Università degli Studi Roma Tre
Dipartimento di Matematica e Fisica

Algebra 2

- MAT/02 AL210 -

Raffaele Di Donna
Matricola: 523997

Indice

Parte I
Teoria dei gruppi

1 Semigruppi, monoidi e gruppi

Definizione 1.1. Sia X un insieme non vuoto. Un'applicazione da $X \times X$ a X viene detta un'*operazione binaria su* X. Un'operazione binaria $\cdot$ su X si dice *associativa* se $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ per ogni $a, b, c \in X$.

(i) Un insieme non vuoto S munito di un'operazione binaria associativa $\cdot$ viene detto un *semigruppo* e si denota $(S, \cdot)$ o più semplicemente S qualora non vi siano ambiguità.

(ii) Un semigruppo M munito di un elemento $e \in M$ tale che $a \cdot e = e \cdot a = a$ per ogni $a \in M$ si dice un *monoide* e si denota $(M, \cdot, e)$ oppure M se non vi sono ambiguità. Inoltre, un elemento $e \in M$ che soddisfi tale proprietà prende il nome di *elemento neutro* (*bilatero*) o *identità*.

(iii) Un monoide G nel quale, per ogni $g \in G$, esiste un elemento $g^{-1} \in G$ tale che $g \cdot g^{-1} = g^{-1} \cdot g = e$ viene detto un *gruppo* e si denota $(G, \cdot, e)$ oppure G purché non vi siano ambiguità. Inoltre, per ogni $g \in G$, un elemento $g^{-1} \in G$ che soddisfi tale proprietà si dice un *inverso bilatero di* g.

Esempio 1.1. L'insieme $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$ munito dell'usuale operazione di somma $+$ è un sottogruppo, ma non è un monoide. L'insieme $\mathbb{N}$ ancora con l'operazione di somma usuale, invece, è un monoide in quanto possiede l'elemento neutro 0, ma non è un gruppo perché ciascun elemento diverso da 0 non ammette un inverso. Gli insiemi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con l'operazione di somma usuale e con elemento neutro 0 sono gruppi.

Esempio 1.2. Gli insiemi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con l'usuale operazione di prodotto $\cdot$ e con elemento neutro 1 sono monoidi, ma non gruppi perché ciascuno di essi contiene l'elemento 0, che non ammette un inverso. Se tali insiemi vengono privati dell'elemento 0 incriminato, allora sono monoidi o gruppi a seconda dei casi. In tal caso, essi si denotano $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$ per semplicità.

Esempio 1.3. Sia $n \in \mathbb{N}^*$ fissato. Si ricordi che la *relazione di congruenza modulo* n è la relazione $\equiv_n$ su $\mathbb{Z}$ definita nel modo seguente: per ogni $a, b \in \mathbb{Z}$, si pone $a \equiv_n b$ oppure $a \equiv b \pmod{n}$ se n divide $b - a$, cioè se esiste $k \in \mathbb{Z}$ tale che $a - b = nk$. È immediato verificare che la relazione di congruenza modulo n è una relazione di equivalenza. Detto questo, la classe di equivalenza di $a \in \mathbb{Z}$ si può denotare $\bar{a}$ anziché $[a]$ se così facendo non si hanno ambiguità, mentre è di uso comune denotare $\mathbb{Z}_n$ l'insieme quoziente $\mathbb{Z}/\equiv_n$. Si ricordi anche che su $\mathbb{Z}_n$ sono ben poste le operazioni di somma $+$ e prodotto $\cdot$ definite da $\bar{a} + \bar{b} := \overline{a + b}$ e da $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$. È dunque immediato verificare che $\mathbb{Z}_n$ munito dell'operazione di somma $+$ e dell'elemento neutro $\bar{0}$ è un gruppo. Se invece si considera $\mathbb{Z}_n$ con l'operazione di prodotto $\cdot$ e con l'elemento neutro $\bar{1}$ si ha un monoide, ma non un gruppo. Se ci si restringe all'insieme $\mathbb{Z}_n^* := \{\, \bar{a} \in \mathbb{Z}_n \mid \mathrm{MCD}(a, n) = 1 \,\}$, allora ogni elemento ammette un inverso bilatero rispetto al prodotto[1] e quindi $\mathbb{Z}_n^*$ con l'operazione di prodotto $\cdot$ e con l'elemento neutro $\bar{1}$ è un gruppo.

Esempio 1.4. Sia X un insieme. L'insieme $\mathcal{P}(X)$, cioè l'insieme delle parti di X, munito dell'operazione di unione $\cup$ e dell'elemento neutro $\varnothing$, oppure dell'operazione di intersezione $\cap$ e dell'elemento neutro X, è un monoide ma non un gruppo. Se invece si considera l'operazione di differenza simmetrica $\triangle$ definita da $A \triangle B := (A \cup B) \setminus (A \cap B)$, allora $\mathcal{P}(X)$ è un gruppo con elemento neutro $\varnothing$. Infatti, per ogni $A \in \mathcal{P}(X)$ è immediato verificare che $A^{-1} = A$.

Esempio 1.5. Sia X un insieme non vuoto. L'insieme $M(X) := \{\, f \colon X \to X \,\}$ munito dell'operazione di composizione di applicazioni $\circ$ e con elemento neutro l'applicazione identità id_X è un monoide ma non un gruppo ed è detto il *monoide delle trasformazioni di* X. L'insieme $A(X) := \{\, f \colon X \to X \mid f \text{ è biiettiva} \,\}$ munito dell'operazione di composizione usuale $\circ$ e dell'elemento neutro id_X è invece un gruppo, noto come il *gruppo delle permutazioni di* X. Si osservi che $M(X)$ e $A(X)$ dipendono soltanto dalla cardinalità di X. In particolare, se X è un insieme finito con $|X| = n$, il monoide delle trasformazioni di X si denota M_n e viene detto il *monoide delle trasformazioni su* n *lettere*, mentre il gruppo delle permutazioni di X viene indicato con S_n e prende il nome di *gruppo simmetrico* (o *gruppo delle permutazioni*) *su* n *lettere*.

[1] Una dimostrazione di questo semplice risultato è reperibile negli appunti del corso AL110.

Esempio 1.6. L'insieme $U_n := \{ z \in \mathbb{C} \mid z^n = 1 \}$ con l'usuale operazione di prodotto $\cdot$ e con elemento neutro 1 è un gruppo, noto come il *gruppo delle radici n-esime dell'unità*. È infatti noto[2] che l'equazione $z^n = 1$ ha n soluzioni complesse distinte, date da $z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ al variare di $0 \leq k \leq n-1$. Per la formula di Eulero $e^{ix} = \cos x + i\sin x$, valida per ogni $x \in \mathbb{R}$, si ha una rappresentazione esponenziale dei numeri complessi e in particolare $z_k = e^{\frac{2k\pi i}{n}}$ per ogni $0 \leq k \leq n-1$. Da questa rappresentazione delle radici n-esime dell'unità si deduce immediatamente che esse formano un gruppo come sopra menzionato.

Esempio 1.7. Sia V uno spazio vettoriale su un campo K, come per esempio $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ oppure $\mathbb{Z}_p$ con p numero primo. L'insieme $\mathrm{End}(V) := \{ f\colon V \to V \mid f \text{ è lineare} \}$ munito dell'operazione di composizione di applicazioni $\circ$ e dell'elemento neutro id_V è un monoide, ma non è un gruppo. Lo stesso insieme munito dell'operazione di somma $+$ definita da $(f+g)(v) := f(v) + g(v)$ e con elemento neutro la funzione nulla o è invece un gruppo, in quanto $f^{-1} = -f$ per ogni $f \in \mathrm{End}(V)$. L'insieme $\mathrm{GL}(V) := \mathrm{End}(V) \cap A(V)$, dove $A(V)$ è definito nell'esempio 1.5, è infine un gruppo con l'operazione di composizione $\circ$ e con l'elemento neutro id_V e viene detto il *gruppo generale lineare di* V.

Esempio 1.8. Sia $n \in \mathbb{N}^*$ e sia K un campo. L'insieme delle matrici quadrate di ordine n a coefficienti in K, denotato $\mathrm{M}_n(K)$, munito dell'operazione di prodotto tra matrici e con elemento neutro la matrice identità I_n è un monoide, ma non è un gruppo. Lo stesso insieme munito dell'usuale operazione di somma tra matrici $+$ e con elemento neutro la matrice nulla O è invece un gruppo. Infine, l'insieme delle matrici invertibili di ordine n a coefficienti in K, denotato $\mathrm{GL}_n(K)$, è un gruppo con l'operazione di prodotto tra matrici e con l'elemento neutro I_n.

Osservazione 1.1. Sia M un monoide. Allora l'elemento neutro è unico.

Dimostrazione. Siano $e, e' \in M$ due elementi neutri. L'asserto segue banalmente dalla definizione 1.1-(ii), in virtù della quale $e = e \cdot e' = e'$ e dall'arbitrarietà nella scelta dei due elementi neutri $e, e' \in M$. □

Proposizione 1.1. *Sia G un gruppo. Allora valgono le seguenti proprietà.*

(i) *L'inverso di g è unico per ogni $g \in G$.*

(ii) $(g^{-1})^{-1} = g$ *per ogni* $g \in G$.

(iii) $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$ *per ogni* $g, h \in G$.

Dimostrazione. Siano $g, h \in G$ due elementi fissati in maniera arbitraria.

(i) Siano $g_1, g_2 \in G$ due inversi di g. Dalle definizioni di elemento neutro, di inverso e dal fatto che l'operazione binaria $\cdot$ su G è associativa deriva immediatamente la relazione seguente:

$$g_1 = e \cdot g_1 = (g_2 \cdot g) \cdot g_1 = g_2 \cdot (g \cdot g_1) = g_2 \cdot e = g_2$$

Dall'arbitrarietà nella scelta degli inversi $g_1, g_2 \in G$ segue dunque che l'inverso di g è unico.

(ii) L'asserto segue banalmente dal fatto che g^{-1} soddisfa la relazione $g \cdot g^{-1} = g^{-1} \cdot g = e$.

(iii) Utilizzando, come nel punto (i) appena dimostrato, le definizioni di elemento neutro, di inverso e l'associatività dell'operazione binaria $\cdot$ su G, si ricava facilmente la condizione seguente:

$$(g \cdot h) \cdot (h^{-1} \cdot g^{-1}) = \big((g \cdot h) \cdot h^{-1}\big) \cdot g^{-1} = \big(g \cdot (h \cdot h^{-1})\big) \cdot g^{-1} = (g \cdot e) \cdot g^{-1} = g \cdot g^{-1} = e$$

Analogamente si dimostra che $(h^{-1} \cdot g^{-1}) \cdot (g \cdot h) = e$, quindi $h^{-1} \cdot g^{-1}$ è per definizione l'inverso di $g \cdot h$. □

[2] Per maggiori dettagli, si rimanda di nuovo agli appunti del corso AL110. Per una dimostrazione della formula di Eulero, si vedano invece le dispense del corso AM210.

1.1 Relazione tra monoidi e gruppi

Definizione 1.2. Sia M un monoide. L'insieme $U(M) := \{\, m \in M \mid m \text{ ammette inverso} \,\}$ viene detto il *gruppo degli elementi invertibili* (o *gruppo delle unità*) *di* M.

Osservazione 1.2. Sia $(M, \cdot, e)$ un monoide. Una conseguenza immediata della definizione 1.1-(iii) e della definizione 1.2 è che $U(M)$ munito dell'operazione binaria $\cdot$ e dell'elemento neutro e è un gruppo.

Osservazione 1.3. La seguente è un'applicazione suriettiva:

$$\begin{aligned} U\colon \{\,\text{Monoidi}\,\} &\longrightarrow \{\,\text{Gruppi}\,\} \\ M &\longmapsto U(M) \end{aligned}$$

Dimostrazione. Basta semplicemente osservare che la mappa inclusione $i\colon \{\,\text{Gruppi}\,\} \to \{\,\text{Monoidi}\,\}$ è per costruzione un'inversa destra di U, cioè soddisfa la condizione $(U \circ i)(G) = G$ per ogni gruppo G. □

Esempio 1.9. Si consideri $\mathbb{N}$ con l'operazione di somma usuale $+$ e con elemento neutro 0. Siccome 0 è l'unico elemento invertibile, si ha che $U(\mathbb{N}) = \{0\}$, cioè il gruppo degli elementi invertibili è banale. Vale lo stesso fatto se si considera $\mathbb{N}$ munito dell'operazione usuale di prodotto $\cdot$ e dell'elemento neutro 1, cioè $U(\mathbb{N}) = \{1\}$. Se invece considero $\mathbb{Z}$ con operazione di prodotto $\cdot$ e con elemento neutro 1, allora il gruppo degli elementi invertibili non è banale. Si vede infatti facilmente che $U(\mathbb{Z}) = \{\pm 1\}$. Si considerino infine gli insiemi $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con l'usuale operazione di prodotto $\cdot$ e con elemento neutro 1. È immediato verificare che $U(\mathbb{Q}) = \mathbb{Q}^*$ e che vale un fatto analogo per gli altri due insiemi numerici $\mathbb{R}$ e $\mathbb{C}$.

Esempio 1.10. Sia $n \in \mathbb{N}^*$ fissato e si consideri $\mathbb{Z}_n$ con l'operazione di prodotto $\cdot$ definita nell'esempio 1.3 e con elemento neutro $\bar{1}$. Da quanto si è osservato nell'esempio appena menzionato segue che $U(\mathbb{Z}_n) = \mathbb{Z}_n^*$.

Esempio 1.11. Sia X un insieme non vuoto. È immediato verificare che $U(M(X)) = A(X)$, in quanto gli elementi invertibili in $M(X)$ sono le applicazioni biiettive.

Esempio 1.12. Sia V uno spazio vettoriale su un campo K e si consideri l'insieme $\mathrm{End}(V)$ con operazione di composizione $\circ$ e con elemento neutro l'applicazione id_V. Esattamente come nell'esempio 1.11, siccome gli elementi invertibili in $\mathrm{End}(V)$ sono le applicazioni biiettive, si ha che $U(\mathrm{End}(V)) = \mathrm{GL}(V)$.

1.2 Concetti di base

Definizione 1.3 (Commutatività)**.** Un semigruppo, monoide o gruppo M si dice *commutativo* (oppure *abeliano*) se l'operazione binaria $\cdot$ su M è commutativa, cioè se $a \cdot b = b \cdot a$ per ogni $a, b \in M$. Si è soliti indicare i semigruppi, monoidi o gruppi abeliani con la notazione additiva, cioè $(M, +)$ oppure $(M, +, 0)$.

Esempio 1.13. È immediato verificare che tutti i semigruppi, monoidi e gruppi costruiti a partire dagli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Z}_n$ con le operazioni usuali di somma $+$ o prodotto $\cdot$ sono commutativi.

Esempio 1.14. Sia X un insieme non vuoto. Si verifica facilmente che $M(X)$ è un monoide abeliano se e solo se $|X| = 1$ e che $A(X)$ è un gruppo abeliano se e solo se $|X| \leq 2$.

Esempio 1.15. Sia V uno spazio vettoriale su un campo K e si considerino gli insiemi $\mathrm{End}(V)$ e $\mathrm{GL}(V)$ muniti dell'operazione di composizione $\circ$ e dell'elemento neutro id_V. Si dimostra facilmente che $\mathrm{End}(V)$ e $\mathrm{GL}(V)$ sono un monoide e un gruppo commutativi se e solo se $\dim V \leq 1$.

Esempio 1.16. Sia $n \in \mathbb{N}^*$ e sia K un campo. È facile vedere che $\mathrm{M}_n(K)$ e $\mathrm{GL}_n(K)$ con l'operazione di prodotto tra matrici e con elemento neutro I_n sono un monoide e un gruppo abeliani se e solo se $n = 1$.

Definizione 1.4 (Ordine)**.** Un semigruppo, monoide o gruppo M si dice *di ordine finito* se $|M| < +\infty$ e in tal caso $|M|$ viene detta l'*ordine del semigruppo, monoide o gruppo* M. Un semigruppo, monoide o gruppo M si dice invece *di ordine infinito* se non è di ordine finito.

Esempio 1.17. Sia $n \in \mathbb{N}^*$ e si consideri $\mathbb{Z}_n$ munito dell'operazione di prodotto $\cdot$ data nell'esempio 1.3 e dell'elemento neutro $\bar{1}$. Chiaramente, vale che $|\mathbb{Z}_n| = n$. Restringendosi a $\mathbb{Z}_n^*$ si ha invece, per definizione, che $|\mathbb{Z}_n^*| = \varphi(n)$, dove $\varphi\colon \mathbb{N} \to \mathbb{N}$ viene detta la *funzione di Eulero*.

Esempio 1.18. Si dimostra facilmente che $|M_n| = n^n$ e che $|S_n| = n!$ utilizzando il calcolo combinatorio.

Definizione 1.5 (Sottosemigruppi, sottomonoidi e sottogruppi)**.**

(i) Sia S un semigruppo. Un *sottosemigruppo* $T < S$ è un sottoinsieme $T \subseteq S$ che è chiuso rispetto all'operazione binaria $\cdot$ su S, cioè tale che $t_1 \cdot t_2 \in T$ per ogni $t_1, t_2 \in T$.

(ii) Sia M un monoide. Un *sottomonoide* $N < M$ è un sottosemigruppo $N < M$ tale che $e \in N$.

(iii) Sia G un gruppo. Un *sottogruppo* $H < G$ è un sottomonoide $H < G$ tale che $h^{-1} \in H$ per ogni scelta di un elemento $h \in H$.

Osservazione 1.4. Sia M un semigruppo, monoide o gruppo. Dalla definizione 1.5 segue immediatamente che ogni sottosemigruppo, sottomonoide o sottogruppo $N < M$ è anche, rispettivamente, un semigruppo, monoide o gruppo.

Esempio 1.19. Si considerino gli insiemi numerici $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ muniti dell'usuale operazione di somma $+$ e dell'elemento neutro 0. Dalla definizione 1.5 segue facilmente che $\mathbb{N} < \mathbb{Z}$ è un sottomonoide, mentre $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ è una catena ascendente di sottogruppi. Si presti attenzione al fatto che $\mathbb{N} < \mathbb{Z}$ non è un sottogruppo poiché, come si è detto nell'esempio 1.1, ogni elemento diverso da 0 non ammette un inverso.

Esempio 1.20. Dato un monoide M, è parecchio evidente che $U(M) < M$ sia un sottomonoide. Non è vero invece che $U(M) < M$ è un sottogruppo a meno che non si assume che M sia anche un gruppo. In tal caso, però, dalla definizione 1.2 segue che $U(M) < M$ è un sottogruppo banale in quanto $U(M) = M$.

Definizione 1.6 (Isomorfismo)**.** Siano M_1 e M_2 semigruppi, monoidi o gruppi, sia $\cdot$ l'operazione binaria su M_1 e sia $\star$ l'operazione binaria su M_2. Si dice che M_1 e M_2 sono *isomorfi* e si scrive $M_1 \simeq M_2$ se esiste una funzione biiettiva $\eta\colon M_1 \to M_2$ tale che $\eta(a \cdot b) = \eta(a) \star \eta(b)$ per ogni $a, b \in M_1$. In caso affermativo, tale applicazione viene detta un *isomorfismo da* M_1 *a* M_2.

Osservazione 1.5. Siano $(M_1, \cdot, e_1)$, $(M_2, \star, e_2)$ monoidi, $\eta\colon M_1 \to M_2$ un isomorfismo. Allora $\eta(e_1) = e_2$.

Dimostrazione. Dalla definizione 1.6 segue banalmente che η è in particolare un'applicazione suriettiva e dunque $\operatorname{Im}\eta = M_2$. Adesso, fissato $a_2 \in M_2$ esiste, per definizione di immagine, un elemento $a_1 \in M_1$ tale che $\eta(a_1) = a_2$ e a questo punto, poiché per ipotesi e_1 è l'elemento neutro di M_1 e η è un isomorfismo, si ha la condizione seguente:

$$a_2 = \eta(a_1) = \eta(a_1 \cdot e_1) = \eta(a_1) \star \eta(e_1) = a_2 \star \eta(e_1)$$

Allo stesso modo si dimostra che $a_2 = \eta(e_1) \star a_2$ e dunque, per arbitrarietà nella scelta di $a_2 \in M_2$ e per unicità dell'elemento neutro in un monoide (osservazione 1.1), posso concludere che $\eta(e_1) = e_2$. □

Osservazione 1.6. Siano $(M_1, \cdot, e_1)$, $(M_2, \star, e_2)$ monoidi, $\eta\colon M_1 \to M_2$ un isomorfismo. Allora la funzione inversa $\eta^{-1}\colon M_2 \to M_1$ esiste ed è un isomorfismo.

Dimostrazione. Innanzitutto, la funzione inversa η^{-1} di η esiste poiché per definizione un isomorfismo è un'applicazione biiettiva, quindi invertibile. Adesso, comunque assegnati $a, b \in M_2$, dall'ipotesi che η sia un isomorfismo deriva la condizione seguente:

$$\eta\big(\eta^{-1}(a) \cdot \eta^{-1}(b)\big) = \eta\big(\eta^{-1}(a)\big) \star \eta\big(\eta^{-1}(b)\big) = a \star b = \eta\big(\eta^{-1}(a \star b)\big)$$

Dato che η è iniettiva per definizione di isomorfismo, si ottiene la relazione $\eta^{-1}(a) \cdot \eta^{-1}(b) = \eta^{-1}(a \star b)$ e posso dunque concludere, per arbitrarietà nella scelta di $a, b \in M_2$, che anche η^{-1} è un isomorfismo. □

Osservazione 1.7. Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ due gruppi e sia $\eta\colon G_1 \to G_2$ un isomorfismo. Allora, per ogni scelta di un elemento $g \in G_1$, vale la condizione $\eta(g)^{-1} = \eta(g^{-1})$.

Dimostrazione. Sia $g \in G_1$ un elemento fissato. Dato che per ipotesi $\eta\colon G_1 \to G_2$ è un isomorfismo e dato che G_1 è un gruppo, utilizzando l'osservazione 1.5 si ricava immediatamente la seguente relazione:

$$\eta(g) \star \eta(g^{-1}) = \eta(g \cdot g^{-1}) = \eta(e_1) = e_2$$

Con un procedimento analogo si dimostra che $\eta(g^{-1}) \star \eta(g) = e_2$ e posso dunque concludere, per unicità dell'inverso in un gruppo (proposizione 1.1-(i)), che vale la condizione $\eta(g)^{-1} = \eta(g^{-1})$. □

Osservazione 1.8. Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ due gruppi e sia $\eta\colon G_1 \to G_2$ un isomorfismo. Se $H < G_1$ è un sottogruppo, allora $\eta(H) < G_2$ è un sottogruppo.

Dimostrazione. Dall'ipotesi che $H < G_1$ sia un sottogruppo e, in particolare, un sottosemigruppo, dalle definizioni di immagine e di isomorfismo segue assai facilmente che $\eta(H) \subseteq G_2$ è un sottoinsieme chiuso rispetto all'operazione binaria $\star$ su G_2. Infatti, dati $h_1, h_2 \in \eta(H)$, esistono $g_1, g_2 \in H$ tali che $\eta(g_1) = h_1$ e $\eta(g_2) = h_2$ e di conseguenza vale la relazione seguente:

$$h_1 \star h_2 = \eta(g_1) \star \eta(g_2) = \eta(g_1 \cdot g_2)$$

Come si è già detto, dalle ipotesi segue che $g_1 \cdot g_2 \in H$ e quindi $h_1 \star h_2 \in \eta(H)$. Ora, dall'osservazione 1.5 e dall'ipotesi che $H < G_1$ sia in particolare un sottomonoide segue immediatamente che $e_2 \in \eta(H)$. Sia infine $h \in \eta(H)$ e sia $g \in H$ l'elemento, che esiste per definizione di immagine, tale che $\eta(g) = h$. Poiché per ipotesi $H < G_1$ è un sottogruppo, si ha che $g^{-1} \in H$. È inoltre possibile applicare l'osservazione 1.7, in virtù della quale vale che $h^{-1} = \eta(g^{-1})$. In particolare, si ha che $h^{-1} \in \eta(H)$ e posso dunque concludere, per arbitrarietà nella scelta dell'elemento $h \in \eta(H)$, che $\eta(H) < G_2$ è un sottogruppo. □

Osservazione 1.9. La relazione di isomorfismo tra semigruppi, monoidi o gruppi è di equivalenza.

Dimostrazione. Siano M_1, M_2, M_3 tre semigruppi, monoidi o gruppi. Basta semplicemente osservare che la relazione di isomorfismo tra semigruppi, monoidi o gruppi è:

- riflessiva: l'applicazione identità id_{M_1} è banalmente un isomorfismo da M_1 in se stesso.
- simmetrica: se esiste un isomorfismo $\eta\colon M_1 \to M_2$, allora è immediato verificare che esiste anche l'applicazione inversa $\eta^{-1}\colon M_2 \to M_1$ e che questa è a sua volta un isomorfismo.
- transitiva: se esistono due isomorfismi $\eta_1\colon M_1 \to M_2$, $\eta_2\colon M_2 \to M_3$, allora si vede facilmente che anche l'applicazione composta $\eta_2 \circ \eta_1\colon M_1 \to M_3$ è un isomorfismo. □

Esempio 1.21. Si considerino $\mathbb{Z}_n$ con l'operazione di somma $+$ definita nell'esempio 1.3 e con elemento neutro $\bar{0}$ e il gruppo delle radici n-esime dell'unità introdotto nell'esempio 1.6. Dalle proprietà di cui gode l'esponenziale complesso segue facilmente che l'applicazione $\eta\colon \mathbb{Z}_n \to U_n$ definita da $\eta(\bar{k}) := e^{\frac{2k\pi i}{n}}$ è ben posta ed è un isomorfismo di gruppi.

Esempio 1.22. Si considerino $\mathbb{R}$ munito dell'operazione usuale di somma usuale $+$ e dell'elemento neutro 0 e la semiretta $(0, +\infty)$ con l'usuale operazione di prodotto $\cdot$ e con elemento neutro 1. Si vede facilmente che $(0, +\infty) < \mathbb{R}^*$ è un sottogruppo e che la funzione $\eta\colon \mathbb{R} \to (0, +\infty)$ data da $\eta(x) := e^x$ è un isomorfismo di gruppi.

1.3 Associatività e commutatività generalizzate

Proposizione 1.2 (Proprietà associativa generalizzata)**.** *Siano S un semigruppo, $a_1, \ldots, a_n \in S$. Allora qualsiasi modo di moltiplicare gli elementi $a_1, \ldots, a_n$ nel dato ordine produce lo stesso risultato.*

Dimostrazione. Si procede per induzione sul numero n di elementi. La base di induzione, corrispondente al caso $n = 1$, è automaticamente verificata. Nel passo induttivo assumo $n \geq 2$, suppongo che l'asserto sia vero nel caso $n - 1$ e ne dimostro la validità per n. Siano $1 \leq i, j \leq n$ indici fissati e si definiscano:

$$g := (a_1 \cdots a_i) \cdot (a_{i+1} \cdots a_n)$$
$$h := (a_1 \cdots a_j) \cdot (a_{j+1} \cdots a_n)$$

Per ipotesi induttiva, gli elementi g e h sono ben definiti. L'obiettivo è dimostrare che $g = h$. Il caso $i = j$ è ovvio, perciò assumo $i \neq j$ e suppongo senza perdita di generalità che $i < j$. Per ipotesi induttiva si ha:

$$g = (a_1 \cdots a_i) \cdot (a_{i+1} \cdots a_n) = (a_1 \cdots a_i) \cdot \big((a_{i+1} \cdots a_j) \cdot (a_{j+1} \cdots a_n)\big)$$
$$h = (a_1 \cdots a_j) \cdot (a_{j+1} \cdots a_n) = \big((a_1 \cdots a_i) \cdot (a_{i+1} \cdots a_j)\big) \cdot (a_{j+1} \cdots a_n)$$

L'asserto segue dunque dalla proprietà associativa della quale gode l'operazione binaria $\cdot$ su S prendendo $a := a_1 \cdots a_i$, $b := a_{i+1} \cdots a_j$, $c := a_{j+1} \cdots a_n$ e dall'arbitrarietà nella scelta degli indici $1 \leq i, j \leq n$. □

In virtù della proposizione 1.2 il risultato di un qualsiasi modo di moltiplicare gli elementi $a_1, \dots, a_n$ di un semigruppo S si può denotare senza ambiguità $a_1 \cdots a_n$.

Definizione 1.7. Siano M un semigruppo, $n \in \mathbb{N}^*$ e sia $a \in M$. Il prodotto di n fattori uguali ad a viene detto la *potenza con base a ed esponente n* e si denota a^n. Se inoltre M è un monoide con identità 1, si pone $a^0 := 1$. Se poi M è anche un gruppo, si definisce $a^n := (a^{-n})^{-1}$ per ogni intero negativo n. Infine, se M è un semigruppo, monoide o gruppo commutativo con operazione binaria $+$, si preferisce utilizzare la notazione na per indicare la potenza con base a ed esponente n.

La definizione 1.7 è ben posta in virtù della proposizione 1.2. Si noti anche che, nel caso in cui M è un gruppo, la definizione 1.7 non produce un conflitto di notazioni con il simbolo dell'inverso di un elemento.

Osservazione 1.10. Sia M un semigruppo. Si dimostra facilmente che, per ogni $n \in \mathbb{N}^*$ e per ogni $a \in M$, valgono le proprietà delle potenze $a^n \cdot a^m = a^{n+m}$ e $(a^n)^m = a^{nm}$. Se inoltre M è un monoide, allora tali proprietà valgono per ogni $n \in \mathbb{N}$. Se infine M è un gruppo, allora tali proprietà valgono per ogni $n \in \mathbb{Z}$.

Proposizione 1.3 (Proprietà commutativa generalizzata)**.** *Siano S un semigruppo commutativo, $\sigma \in S_n$ e siano $a_1, \dots, a_n \in S$. Allora vale la condizione $a_1 \cdots a_n = a_{\sigma(1)} \cdots a_{\sigma(n)}$.*

Dimostrazione. Si procede per induzione sul numero n di elementi. La base di induzione, che corrisponde al caso $n = 1$, è automaticamente soddisfatta. Nel passo induttivo assumo $n \geq 2$, suppongo che l'asserto sia vero nel caso $n - 1$ e dimostro che vale anche per n. Definisco $h := \sigma^{-1}(n)$ e noto che, per definizione di h e per la commutatività dell'operazione binaria $\cdot$ su S applicata $n - h$ volte, vale la relazione seguente:

$$a_{\sigma(1)} \cdots a_{\sigma(n)} = a_{\sigma(1)} \cdots a_{\sigma(h-1)} \cdot a_n \cdot a_{\sigma(h+1)} \cdots a_{\sigma(n)} = a_{\sigma(1)} \cdots a_{\sigma(h-1)} \cdot a_{\sigma(h+1)} \cdots a_{\sigma(n)} \cdot a_n$$

Si consideri ora la permutazione $\sigma' \in S_{n-1}$ definita da $\sigma'(i) := \sigma(i)$ se $i \neq h$, $\sigma'(i) := \sigma(n)$ se $i = h$. Dalla relazione precedente, dalla costruzione di σ', dalla commutatività dell'operazione binaria $\cdot$ su S applicata $n - h - 1$ volte e dall'ipotesi induttiva si ricava la seguente relazione, che implica immediatamente la tesi:

$$\begin{aligned} &a_{\sigma(1)} \cdots a_{\sigma(h-1)} \cdot a_{\sigma(h+1)} \cdots a_{\sigma(n-1)} \cdot a_{\sigma(n)} \cdot a_n \\ &\quad = a_{\sigma'(1)} \cdots a_{\sigma'(h-1)} \cdot a_{\sigma'(h+1)} \cdots a_{\sigma'(n-1)} \cdot a_{\sigma'(h)} \cdot a_n \\ &\quad = a_{\sigma'(1)} \cdots a_{\sigma'(n-1)} \cdot a_n = a_1 \cdots a_{n-1} \cdot a_n = a_1 \cdots a_n \end{aligned}$$

□

Osservazione 1.11. Sia M un semigruppo commutativo. Una conseguenza della proposizione 1.3 è che, per ogni $n \in \mathbb{N}^*$ e per ogni $a \in M$, vale la proprietà delle potenze $(a \cdot b)^n = a^n \cdot b^n$. Se inoltre M è un monoide, allora la medesima proprietà vale per ogni $n \in \mathbb{N}$. Se invece M è un gruppo, allora essa vale per ogni $n \in \mathbb{Z}$.

Osservazione 1.12. La proposizione 1.3 e l'osservazione 1.11 valgono anche, più in generale, in semigruppi, monoidi e gruppi non commutativi purché si assuma che gli elementi considerati commutino a due a due.

1.4 Sottosemigruppi, sottomonoidi e sottogruppi generati da un insieme

Definizione 1.8. Siano M un semigruppo, $S \subseteq M$ un insieme. Si definisce il *sottosemigruppo generato da S* come il più piccolo sottosemigruppo di M contenente S, cioè come il sottosemigruppo $\langle S \rangle < M$ tale che:

(i) $S \subseteq \langle S \rangle$.

(ii) $\langle S \rangle \subseteq H$ per ogni $H < M$ sottosemigruppo con $S \subseteq H$.

Se inoltre M è un monoide, si definisce il *sottomonoide generato da S* come il più piccolo sottomonoide di M contenente S, cioè come il sottomonoide $\langle S \rangle < M$ che soddisfa le proprietà (i) e (ii) per ogni $H < M$ sottomonoide con $S \subseteq H$. Se invece M è un gruppo, si definisce il *sottogruppo generato da S* come il più piccolo sottogruppo di M contenente S, cioè come il sottogruppo $\langle S \rangle < M$ soddisfacente le proprietà (i) e (ii) per ogni $H < M$ sottogruppo con $S \subseteq H$. Infine, se $S = \{s_1, \dots, s_n\}$, per semplificare la notazione si pone $\langle s_1, \dots, s_n \rangle := \langle S \rangle$.

Proposizione 1.4. *Sia M un semigruppo e sia $S \subseteq M$ un insieme. Allora il sottosemigruppo $\langle S \rangle$ esiste ed è unico. Se inoltre M è un monoide, allora il sottomonoide $\langle S \rangle$ esiste ed è unico. Se infine M è anche un gruppo, allora il sottogruppo $\langle S \rangle$ esiste ed è unico.*

Dimostrazione. Si noti innanzitutto che, una volta mostrata l'esistenza del sottosemigruppo $\langle S \rangle$, l'unicità segue immediatamente dalla proprietà (ii). Nel caso in cui M è anche un monoide oppure un gruppo, si può dire lo stesso per quanto riguarda l'unicità del sottomonoide $\langle S \rangle$ o, rispettivamente, del sottogruppo $\langle S \rangle$. Si danno ora due dimostrazioni dell'esistenza del sottosemigruppo $\langle S \rangle$, del sottomonoide $\langle S \rangle$ e del sottogruppo $\langle S \rangle$ sotto le ipotesi assegnate nell'enunciato.

- *Dimostrazione teorica.* Sia $\{H_\alpha\}$ la collezione dei sottosemigruppi di M contenenti S, indicizzata su un insieme A. Definendo semplicemente $\langle S \rangle := \bigcap_{\alpha \in A} H_\alpha$ si ottiene un sottomonoide di M che verifica le proprietà (i) e (ii) per costruzione. Se inoltre M è un monoide oppure un gruppo, allora l'esistenza del sottomonoide $\langle S \rangle$ o, rispettivamente, del sottogruppo $\langle S \rangle$ si dimostra seguendo un procedimento del tutto analogo.

- *Dimostrazione costruttiva.* Definisco $\langle S \rangle := \{ s_1 \cdots s_r \mid r \in \mathbb{N}^*, s_1, \dots, s_r \in S \}$. Si osservi che, a meno di reindicizzare gli elementi di S, il prodotto di due elementi in $\langle S \rangle$ è ancora un elemento di $\langle S \rangle$. Equivalentemente, il sottoinsieme $\langle S \rangle \subseteq M$ è chiuso rispetto all'operazione binaria $\cdot$ su S e quindi $\langle S \rangle < M$ è un sottosemigruppo. Si ha inoltre, per costruzione, che $S \subseteq \langle S \rangle$ poiché ciascun elemento $s \in S$ compare in $\langle S \rangle$ prendendo $r := 1$ e $s_1 := s$. Sia ora $H < M$ un sottosemigruppo con $S \subseteq H$. Essendo $H \subseteq M$ un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su S, per ogni $r \in \mathbb{N}^*$ e per ogni $s_1, \dots, s_r \in S$ vale che $s_1 \cdots s_r \in H$ e di conseguenza $\langle S \rangle \subseteq H$. Questo dimostra quindi che $\langle S \rangle$ è effettivamente il sottosemigruppo generato da S. Se si assume che M sia anche un monoide allora, per dimostrare l'esistenza del sottomonoide generato da S, basta semplicemente definire $\langle S \rangle := \{ s_1 \cdots s_r \mid r \in \mathbb{N}, s_1, \dots, s_r \in S \}$ con la convenzione che l'identità 1 appartiene a $\langle S \rangle$ prendendo $r := 0$. Per costruzione, quindi, si ha che $\langle S \rangle < M$ è un sottomonoide. Per ragioni analoghe a quelle date nel caso dei sottosemigruppi, le proprietà (i) e (ii) sono verificate. Si noti in particolare che ogni sottomonoide $H < M$ contiene l'identità per definizione. Se suppongo infine che M sia un gruppo, allora definisco $\langle S \rangle := \{ s_1^{\pm 1} \cdots s_r^{\pm 1} \mid r \in \mathbb{N}, s_1, \dots, s_r \in S \}$, conservando ovviamente la convenzione che l'identità 1 appartiene a $\langle S \rangle$ scegliendo $r := 0$. È assai evidente che $\langle S \rangle < M$ è un sottogruppo e si dimostra con un procedimento molto simile a quello adottato nei casi precedenti che $\langle S \rangle$ soddisfa le proprietà (i) e (ii). □

Osservazione 1.13. Sia M un semigruppo e sia $S \subseteq M$ un insieme. Dalla dimostrazione costruttiva della proposizione 1.4 segue in particolare che il sottosemigruppo $\langle S \rangle$ è il sottoinsieme di M contenente tutti i possibili prodotti finiti di elementi di S. Se inoltre M è un monoide allora, chiaramente, il sottomonoide $\langle S \rangle$ contiene anche l'identità. Se infine M è un gruppo, allora il sottogruppo $\langle S \rangle$ contiene tutti i possibili prodotti finiti tra gli elementi di S e i loro inversi.

Definizione 1.9. Siano M un semigruppo, monoide o gruppo, $S \subseteq M$ un insieme. Se il sottosemigruppo, sottomonoide o sottogruppo $\langle S \rangle$ coincide con M, si dice che S *è un insieme di generatori di* M o anche che M *è generato da* S. Inoltre, il semigruppo, monoide o gruppo M si dice *ciclico* se è generato da un unico elemento, che viene detto un *generatore di* M.

Osservazione 1.14. Siano M un semigruppo, monoide o gruppo, $S \subseteq M$ un insieme di generatori. Allora vale, rispettivamente, che nessun sottosemigruppo, sottomonoide o sottogruppo proprio di M contiene S.

Esempio 1.23. Sia $n \in \mathbb{N}^*$ fissato. Si considerino $\mathbb{Z}$ e $\mathbb{Q}$ muniti dell'usuale operazione di somma $+$ e con elemento neutro 0 e si consideri $\mathbb{Z}_n$ con l'operazione additiva $+$ definita nell'esempio 1.3 e con elemento neutro $\bar{0}$. Allora è immediato verificare, in virtù dell'osservazione 1.13, che $\mathbb{Z}$ è generato da $\{1\}$, che $\mathbb{Z}_n$ è generato da $\{\bar{1}\}$ e che $\mathbb{Q}$ è generato dall'insieme $\{ \frac{1}{n} \mid n \in \mathbb{N}^* \}$. In particolare, i due gruppi $\mathbb{Z}$ e $\mathbb{Z}_n$ sono ciclici, mentre $\mathbb{Q}$ non è ciclico.

1.5 Teorema di Cayley

Teorema 1.1 (di Cayley)**.** *Sia M un monoide oppure un gruppo. Per ogni $a \in M$, sia $\rho_L(a) \colon M \to M$ la moltiplicazione a sinistra per a, cioè l'applicazione definita da $\rho_L(a)(x) := a \cdot x$.*

(i) *Se M è un monoide, si consideri la seguente applicazione:*

$$\begin{aligned} \rho_L \colon M &\longrightarrow M(M) \\ a &\longmapsto \rho_L(a) \end{aligned}$$

Allora $\operatorname{Im} \rho_L < M(M)$ è un sottomonoide e ρ_L è un isomorfismo da M a $\operatorname{Im} \rho_L$.

(ii) *Se M è un gruppo, si consideri la seguente applicazione:*

$$\begin{aligned} \rho_L \colon M &\longrightarrow A(M) \\ a &\longmapsto \rho_L(a) \end{aligned}$$

Allora $\operatorname{Im}\rho_L < A(M)$ *è un sottogruppo e* ρ_L *è un isomorfismo da* M *a* $\operatorname{Im}\rho_L$.

Dimostrazione. Innanzitutto osservo che, per ogni $a \in M$, l'applicazione $\rho_L(a)$ è ben posta per definizione di operazione binaria, essendo per ipotesi M un monoide oppure un gruppo.

(i) Suppongo che M sia un monoide e osservo che, per costruzione, l'applicazione ρ_L è ben definita. Mostro che $\operatorname{Im}\rho_L < M(M)$ è un sottomonoide. Siano dunque fissati $\alpha, \beta \in \operatorname{Im}\rho_L$. Per definizione di immagine, esistono due elementi $a, b \in M$ tali che $\rho_L(a) = \alpha$ e $\rho_L(b) = \beta$. Dall'associatività di cui gode l'operazione binaria $\cdot$ su M, dalla costruzione delle applicazioni $\rho_L(a)$ e $\rho_L(b)$ deriva, per ogni $x \in M$, la condizione seguente:

$$\big(\rho_L(a) \circ \rho_L(b)\big)(x) = \rho_L(a)\big(\rho_L(b)(x)\big) = \rho_L(a)(b \cdot x) = a \cdot (b \cdot x) = (a \cdot b) \cdot x = \rho_L(a \cdot b)(x) \quad (1)$$

Questo dimostra che $\operatorname{Im}\rho_L \subseteq M(M)$ è un sottoinsieme chiuso rispetto all'operazione binaria $\circ$ su $M(M)$. È immediato verificare che, se M ha elemento neutro 1, allora $\mathrm{id}_M = \rho_L(1)$ e posso quindi affermare che $\operatorname{Im}\rho_L < M(M)$ è un sottomonoide. Ora bisogna mostrare che ρ_L è un isomorfismo da M a $\operatorname{Im}\rho_L$. Poiché si restringe ρ_L alla sua immagine, l'applicazione è banalmente suriettiva. Siano adesso $a, b \in M$ due elementi tali che $\rho_L(a) = \rho_L(b)$. Se tali applicazioni coincidono, dovrà valere in particolare la condizione $\rho_L(a)(1) = \rho_L(b)(1)$, dunque $a = b$ per definizione di elemento neutro. Questo dimostra che ρ_L è un'applicazione biiettiva e dalla relazione (1) segue che è anche un isomorfismo.

(ii) Si assuma ora che M sia un gruppo e si osservi che ρ_L è un'applicazione ben definita in quanto, per ogni $a \in M$, l'applicazione $\rho_L(a)$ è biiettiva. Dalla condizione (1), che continua a valere e dal fatto che M è un gruppo segue infatti che $\rho_L(a)$ ammette un'inversa, come mostrato di seguito:

$$\begin{aligned} \rho_L(a) \circ \rho_L(a^{-1}) &= \rho_L(a \cdot a^{-1}) = \rho_L(1) = \mathrm{id}_M \\ \rho_L(a^{-1}) \circ \rho_L(a) &= \rho_L(a^{-1} \cdot a) = \rho_L(1) = \mathrm{id}_M \end{aligned} \quad (2)$$

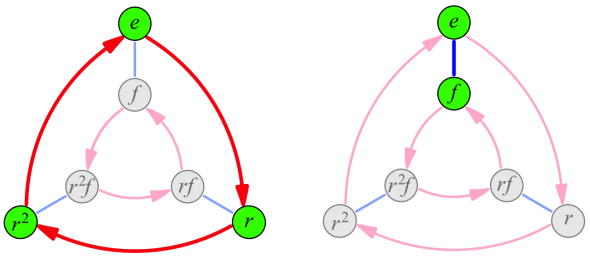
Si dimostra esattamente come nel punto (i) che $\operatorname{Im}\rho_L < M(M)$ è un sottomonoide, mentre dalla condizione (2) e dalla definizione di immagine segue immediatamente che è anche un sottogruppo. Infine, la dimostrazione del fatto che ρ_L è un isomorfismo da M a $\operatorname{Im}\rho_L$ è identica a quella esibita nel punto (i). □

Corollario 1.1. *Sia M un monoide oppure un gruppo e si assuma che M sia finito di ordine n.*

(i) *Se M è un monoide, allora è isomorfo a un sottomonoide di M_n.*

(ii) *Se M è un gruppo, allora è isomorfo a un sottogruppo di S_n.*

Dimostrazione. L'asserto è semplicemente un caso particolare del teorema di Cayley. Si tengano a mente le definizioni di ordine (definizione 1.4), di M_n e di S_n (esempio 1.5). □



Nelle immagini si pone per semplicità $f := (1\,2)$, $r := (1\,2\,3)$. Il diagramma sulla sinistra mostra un sottogruppo del gruppo simmetrico S_3 che è isomorfo al gruppo $(\mathbb{Z}_3, +, \bar{0})$, mentre il diagramma sulla destra, in modo simile, rappresenta una copia isomorfa di $(\mathbb{Z}_2, +, \bar{0})$ all'interno del gruppo simmetrico S_3.

Definizione 1.10. Sia M un monoide. Un elemento $a \in M$ si dice *di ordine finito* se esiste $n \in \mathbb{N}^*$ tale che $a^n = 1$. In caso affermativo, il più piccolo $n \in \mathbb{N}^*$ che soddisfa tale proprietà viene detto l'*ordine di* a e si denota $o(a)$. Un elemento $a \in M$ si dice invece *di ordine infinito* se non è di ordine finito.

Osservazione 1.15. Siano M un monoide, $a \in M$ e sia $k \in \mathbb{N}^*$ tale che $a^k = 1$. Allora si ha che $o(a) \mid k$.

Dimostrazione. Si procede per contrapposizione logica. Sia $n := o(a)$ e si supponga che n non divida k. Per[3] l'algoritmo della divisione euclidea, esistono $q, r \in \mathbb{Z}$ con $0 \leq r \leq n-1$ tali che $k = qn + r$ e inoltre, poiché si assume che n non divida k, deve valere che $r \neq 0$. Di conseguenza, tenendo a mente le proprietà delle potenze (osservazione 1.10) e la definizione 1.10, si ha la relazione seguente, dalla quale deriva la tesi:

$$a^k = a^{qn+r} = (a^n)^q \cdot a^r = (1)^q \cdot a^r = a^r \neq 1 \qquad \square$$

Osservazione 1.16. Siano M_1 e M_2 due semigruppi, monoidi o gruppi, sia $\cdot$ l'operazione binaria su M_1 e sia $\star$ l'operazione binaria su M_2, sia $\eta\colon M_1 \to M_2$ un isomorfismo e si considerino elementi $a_1, \dots, a_n \in M_1$. Dalla definizione 1.6 segue banalmente, per induzione sul numero n degli elementi considerati, che si ha la condizione $\eta(a_1 \cdots a_n) = \eta(a_1) \star \cdots \star \eta(a_n)$.

Osservazione 1.17. Siano $(M_1, \cdot, e_1)$, $(M_2, \star, e_2)$ due monoidi, $\eta\colon M_1 \to M_2$ un isomorfismo e sia $a \in M_1$ un elemento di ordine finito. Allora anche $\eta(a) \in M_2$ è un elemento di ordine finito e vale $o(\eta(a)) = o(a)$.

Dimostrazione. Siano $n := o(a)$, $m := o(\eta(a))$. Per la definizione 1.10, si ha che $a^n = e_1$. Applicando η a primo e secondo membro di tale relazione, si ricava che $\eta(a^n) = \eta(e_1)$ ma questo è equivalente a dire, per le osservazioni 1.5 e 1.16, che $\eta(a)^n = e_2$. Dall'osservazione 1.15 segue dunque che $m \mid n$. A questo punto posso ripetere lo stesso ragionamento considerando l'applicazione inversa η^{-1} e scambiando i ruoli di n e m. Nuovamente in virtù della definizione 1.10, infatti, vale che $\eta(a)^m = e_2$ e se applico η^{-1} a entrambi i membri di tale relazione, tenendo in considerazione le osservazioni 1.6 e 1.16, allora ottengo la relazione:

$$e_2 = \eta^{-1}\big(\eta(a)^m\big) = \eta^{-1}\big(\eta(a)\big)^m = a^m$$

Di nuovo per l'osservazione 1.15, si ha che $n \mid m$. Essendo tuttavia $n, m \in \mathbb{N}^*$ per la definizione 1.10, posso concludere che $n = m$. $\square$

Esempio 1.24. Sia p un numero primo e si consideri $\mathbb{Z}_p$ munito dell'operazione usuale di somma $+$ e con elemento neutro $\bar{0}$. Mi chiedo quale sia il più piccolo $m \in \mathbb{N}^*$ tale che $\mathbb{Z}_p$ sia isomorfo a un sottogruppo di S_m. Sicuramente $m \leq p$ per il corollario 1.1-(ii). Suppongo per assurdo che $m < p$ e osservo che $\bar{1} \in \mathbb{Z}_p$ è un elemento di ordine p. Deve dunque esistere, per l'osservazione 1.17, un elemento $\sigma \in S_m$ di ordine p, ma è noto[4] che l'ordine di una permutazione è dato dal minimo comune multiplo fra le lunghezze dei suoi cicli. Di conseguenza, la permutazione σ ha cicli di lunghezza maggiore o uguale a p e questo contraddice il fatto che $m < p$. In definitiva, l'unica possibilità accettabile è che valga $m = p$.

Osservazione 1.18. Siano $(M_1, \cdot, e_1)$, $(M_2, \star, e_2)$ due monoidi, $\eta\colon M_1 \to M_2$ un isomorfismo e sia $S \subseteq M_1$ un insieme di generatori. Allora $\eta(S) \subseteq M_2$ è un insieme di generatori.

Dimostrazione. Sia $a_2 \in M_2$ un elemento prefissato. Poiché per ipotesi $\eta\colon M_1 \to M_2$ è un isomorfismo, si tratta in particolare di un'applicazione suriettiva e dunque esiste un elemento $a_1 \in M_1$ tale che $\eta(a_1) = a_2$. Dal momento che $S \subseteq M_1$ è per ipotesi un insieme di generatori, applicando la definizione 1.9 e sfruttando l'osservazione 1.13 posso affermare che $a_1 = s_1 \cdots s_r$ per opportuni $s_1, \dots, s_r \in S$ ma allora, dato che per ipotesi $\eta\colon M_1 \to M_2$ è un isomorfismo, posso applicare l'osservazione 1.16 per ottenere la condizione:

$$a_2 = \eta(a_1) = \eta(s_1 \cdots s_r) = \eta(s_1) \star \cdots \star \eta(s_r)$$

Questo dimostra, per arbitrarietà nella scelta dell'elemento $a_2 \in M_2$ e in virtù dell'osservazione 1.13, che $\eta(S) \subseteq M_2$ è un insieme di generatori. $\square$

Naturalmente, l'osservazione 1.18 si estende senza problemi al caso più specifico dei gruppi.

[3] Per una dimostrazione di questo risultato, si rimanda agli appunti del corso AL110.
[4] Maggiori dettagli sono reperibili negli appunti del corso AL110.

1.6 Gruppi ciclici

Proposizione 1.5. *Sia G un gruppo ciclico, $G = \langle a \rangle$. Allora $G = \{ a^n \mid n \in \mathbb{Z} \}$ se a è di ordine infinito, altrimenti $G = \{ 1, a, \dots, a^{n-1} \}$ se $o(a) = n$ e in ambo le descrizioni gli elementi di G sono tutti distinti.*

Dimostrazione. Innanzitutto, dall'osservazione 1.13 segue immediatamente che $G = \{ a^n \mid n \in \mathbb{Z} \}$, ma a priori tale descrizione di G potrebbe ripetere più volte lo stesso elemento. Vi sono in effetti due possibilità: o $a^i \neq a^j$ per ogni $i, j \in \mathbb{Z}$ con $i \neq j$, o $a^i = a^j$ per certi $i, j \in \mathbb{Z}$ con $i \neq j$. Nel primo caso a è un elemento di ordine infinito in quanto, se fosse $o(a) = n$ per un qualche $n \in \mathbb{N}^*$, allora varrebbe la condizione $a^n = a^0$ per definizione e questo è assurdo. Nel secondo caso posso supporre senza perdita di generalità che $i > j$ e dalla condizione $a^i = a^j$ ricavo che $a^{i-j} = 1$, cioè che a è un elemento di ordine finito. Noto che valgono anche le implicazioni inverse per il principio del terzo escluso. Suppongo ora che $o(a) = n$ e osservo che, dato $k \in \mathbb{Z}$, per l'algoritmo della divisione euclidea esistono $q, r \in \mathbb{Z}$ con $0 \leq r \leq n-1$ tali che $k = qn + r$. Di conseguenza, per le proprietà delle potenze (osservazione 1.10) e per la definizione 1.10, si ottiene che:

$$a^k = a^{qn+r} = (a^n)^q \cdot a^r = (1)^q \cdot a^r = a^r \tag{3}$$

Si ottiene dunque che $G = \{ 1, a, \dots, a^{n-1} \}$. Adesso, se a è di ordine infinito, dalla discussione precedente segue anche che gli elementi di $G = \{ a^n \mid n \in \mathbb{Z} \}$ sono a due a due distinti e dunque non vi è nient'altro da dimostrare. Se invece $o(a) = n$, allora suppongo per assurdo che esistano due indici $0 \leq i < j \leq n-1$ tali che $a^i = a^j$. Equivalentemente, si ha la condizione $a^{j-i} = 1$ ma $0 < j - i < n$ e questo contraddice la definizione 1.10. Posso quindi affermare che in ambo le descrizioni di G gli elementi sono tutti distinti. □

Corollario 1.2. *Sia G un gruppo ciclico, $G = \langle a \rangle$ e si considerino i gruppi $(\mathbb{Z}, +, 0)$ e $(\mathbb{Z}_n, +, \bar{0})$. Se a è di ordine infinito, allora l'applicazione $\alpha \colon \mathbb{Z} \to G$ definita da $\alpha(m) := a^m$ è un isomorfismo. Se invece $o(a) = n$, allora l'applicazione $\beta \colon \mathbb{Z}_n \to G$ definita da $\beta(\bar{m}) := a^m$ è un isomorfismo.*

Dimostrazione. Innanzitutto, noto che le applicazioni α e β sono ben definite. Poiché per ipotesi $G = \langle a \rangle$, la prima applicazione è ben posta per l'osservazione 1.13. Per poter affermare che anche β è ben definita, bisogna mostrare che non dipende da una particolare scelta dei rappresentanti delle classi resto modulo n. Siano dunque $m, m' \in \mathbb{Z}$ tali che $\bar{m} = \bar{m}'$, cioè tali che m e m' diano lo stesso resto nella divisione euclidea per n. Formalmente, questo significa che esistono $q, q' \in \mathbb{Z}$ e un intero $0 \leq r \leq n-1$ tali che $m = qn + r$ e $m' = q'n + r$. Allora si vede facilmente che $a^m = a^{m'}$ applicando un argomento simile alla relazione (3). Una volta appurata la buona definizione delle funzioni α e β, la loro biunivocità segue immediatamente dalla proposizione 1.5. Più precisamente, la suriettività deriva, in entrambi i casi, dalla descrizione data del gruppo G, mentre l'iniettività segue dal fatto che, nelle due descrizioni, gli elementi di G sono a due a due distinti. La proprietà delle potenze $a^n \cdot a^m = a^{n+m}$ data nell'osservazione 1.10 mi permette infine di concludere che, se a è di ordine infinito, allora α è un isomorfismo, mentre se $o(a) = n$ allora lo è β. □

Osservazione 1.19. Sia G un gruppo ciclico, $G = \langle a \rangle$. Se a è di ordine infinito, allora ogni sottogruppo di G è della forma $\langle a^m \rangle$ per un qualche $m \in \mathbb{N}$. Se invece $o(a) = n$, allora tutti i sottogruppi di G sono della forma $\langle a^m \rangle$ per un qualche $m \in \mathbb{N}$ tale che $m \mid n$. In particolare, ogni sottogruppo di un gruppo ciclico è a sua volta un gruppo ciclico.

Dimostrazione. Sia $H < G$ un sottogruppo fissato e si considerino le applicazioni $\alpha \colon \mathbb{Z} \to G$ e $\beta \colon \mathbb{Z}_n \to G$ definite da $\alpha(m) := a^m$ e da $\beta(\bar{m}) := a^m$. Se a è di ordine infinito allora, per il corollario 1.2, la funzione α è un isomorfismo e in particolare, per l'osservazione 1.6, lo è anche l'applicazione inversa $\alpha^{-1} \colon G \to \mathbb{Z}$. Ma allora, in virtù dell'osservazione 1.8, l'immagine della restrizione di α^{-1} su H è un sottogruppo di $\mathbb{Z}$. È noto[5] che ogni sottogruppo di $\mathbb{Z}$ è della forma $\langle m \rangle$ per un qualche $m \in \mathbb{N}$ e dunque $\alpha^{-1}(H) = \langle m \rangle$ per un certo $m \in \mathbb{N}$. In particolare, comunque fissato $h \in H$ esiste, per definizione di preimmagine, un elemento $k \in \mathbb{Z}$ tale che $h = \alpha(k \cdot m)$ e questo è del tutto equivalente a dire, per definizione di α e per le proprietà delle potenze (osservazione 1.10), che $h = (a^m)^k$. Posso dunque affermare, per arbitrarietà nella scelta di $h \in H$ e in virtù dell'osservazione 1.13, che $H = \langle a^m \rangle$. Se invece $o(a) = n$, si procede essenzialmente allo stesso modo lavorando con β anziché con α, con la differenza sostanziale che ogni sottogruppo di $\mathbb{Z}_n$ è della forma $\langle \bar{m} \rangle$ per un qualche $m \in \mathbb{N}$ tale che $m \mid n$ e dunque si ha la tesi. □

[5] Si vedano gli appunti del corso AL110 per una dimostrazione di questo risultato. Nel caso di $\mathbb{Z}$ viene spesso utilizzata anche la notazione $m\mathbb{Z}$ al posto di $\langle m \rangle$.

Osservazione 1.20. Sia G un gruppo ciclico, $G = \langle a \rangle$. Se a è di ordine infinito, allora i generatori di G sono a e a^{-1} altrimenti, se $o(a) = n$, essi sono della forma a^k con $0 < k < n$ tale che $\mathrm{MCD}(n, k) = 1$ e in tal caso il numero di generatori è $\varphi(n)$, dove $\varphi\colon \mathbb{N} \to \mathbb{N}$ è la funzione di Eulero.

Dimostrazione. Si assuma che a sia un elemento di ordine infinito e sia b un generatore di G. In virtù del corollario 1.2 l'applicazione $\alpha\colon \mathbb{Z} \to G$ definita da $\alpha(m) := a^m$ è un isomorfismo e in particolare lo è anche l'applicazione inversa $\alpha^{-1}\colon G \to \mathbb{Z}$ in virtù dell'osservazione 1.6. Sia adesso $k \in \mathbb{Z}$ e si osservi che, essendo b un generatore di G, esiste $h \in \mathbb{Z}$ tale che $\alpha(k) = b^h$. Applicando α^{-1} alla relazione ottenuta, si ottiene che $k = \alpha^{-1}(b^h)$ e quindi, ricordando che α^{-1} è un isomorfismo, ci si riduce alla condizione $k = h \cdot \alpha^{-1}(b)$. Non dipendendo il risultato ottenuto da una particolare scelta di $k \in \mathbb{Z}$, posso affermare che $\mathbb{Z} = \langle \alpha^{-1}(b) \rangle$, ma è noto che i generatori di $\mathbb{Z}$ sono soltanto 1 e -1 e di conseguenza, per unicità, deve valere $\alpha^{-1}(b) = 1$ oppure $\alpha^{-1}(b) = -1$. Applicando α a entrambi i membri di tali relazioni e ricordando la definizione di α, si ottiene dunque che $b = a$ oppure $b = a^{-1}$. Se si suppone invece che $o(a) = n$, allora basterà seguire un procedimento analogo con l'applicazione $\beta\colon \mathbb{Z} \to G$ definita da $\beta(\bar{m}) := a^m$, ricordando che i generatori di $\mathbb{Z}_n$ sono tutte le classi di resto modulo n che hanno rappresentanti coprimi con n. Infine, la parte finale dell'enunciato deriva immediatamente dalla definizione della funzione di Eulero (esempio 1.17). □

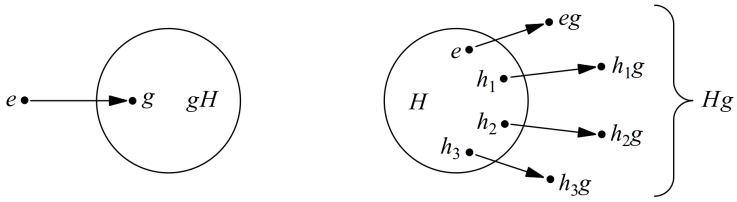
2 Sottogruppi e quozienti

2.1 Classi laterali sinistre e destre

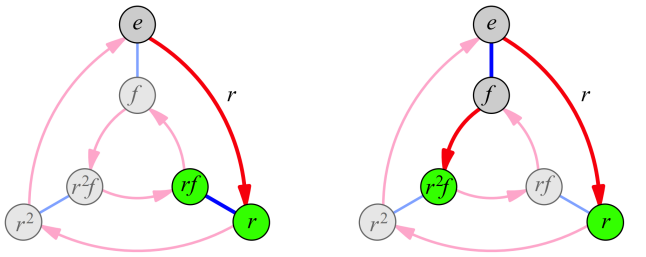
Definizione 2.1. Siano G un gruppo, $H < G$ un sottogruppo e sia $a \in G$.

(i) L'insieme $aH := \{ a \cdot h \mid h \in H \}$ si dice una *classe laterale sinistra di G rispetto a H*. L'elemento a viene detto il rappresentante di aH. L'insieme delle classi laterali sinistre di G rispetto a H si denota G/H.

(ii) L'insieme $Ha := \{ h \cdot a \mid h \in H \}$ si dice una *classe laterale destra di G rispetto a H*. L'elemento a viene detto il rappresentante di Ha. L'insieme delle classi laterali sinistre di G rispetto a H si denota $H\backslash G$.



Ogni classe laterale sinistra gH si può immaginare come una copia di H con punto base g anziché l'identità, come illustrato nella figura a sinistra. La freccia indica la moltiplicazione a destra per g. Nella figura a destra, invece, le frecce rappresentano la moltiplicazione a sinistra per g e ogni classe laterale destra Hg viene vista come l'insieme dei nodi ai quali tali frecce portano gli elementi di H.



Il diagramma a sinistra è una rappresentazione grafica della classe laterale sinistra $r\langle f \rangle$ in S_3. I nodi evidenziati in verde sono quelli che le frecce blu, corrispondenti alla moltiplicazione a sinistra per f, possono raggiungere dopo aver percorso la freccia rossa, che corrisponde invece alla moltiplicazione a destra per r. Il diagramma sulla destra rappresenta, invece, la classe laterale destra $\langle f \rangle r$ di S_3. In questo caso, i nodi evidenziati in verde sono quelli che le frecce rosse, corrispondenti alla moltiplicazione a sinistra per r, possono raggiungere partendo dagli elementi del sottogruppo $\langle f \rangle < S_3$.

Osservazione 2.1. Sia G un gruppo abeliano e sia $H < G$ un sottogruppo. Una conseguenza immediata della definizione 2.1 è che $aH = Ha$ per ogni $a \in G$. In particolare, vale che $G/H = H\backslash G$.

Osservazione 2.2. Sia $(G, \cdot, 1)$ un gruppo e si consideri l'operazione binaria $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$ definita dalla condizione $A \cdot B := \{\, a \cdot b \mid a \in A,\, b \in B \,\}$. Allora l'insieme $\mathcal{P}(G)\setminus\{\varnothing\}$, munito dell'operazione binaria $\cdot$ appena definita e dell'elemento neutro $\{1\}$ è un monoide. Inoltre, per ogni $g \in G$ vale che $\{g\}^{-1} = \{g^{-1}\}$.

Dimostrazione. Innanzitutto, è evidente che l'operazione binaria $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$ sia ben definita. Infatti, se $A, B \neq \varnothing$, allora esistono $a \in A$, $b \in B$ e di conseguenza l'insieme $A \cdot B$ contiene almeno l'elemento $a \cdot b$. Inoltre, dalla chiusura dell'operazione binaria $\cdot$ su G segue banalmente che $A \cdot B \subseteq G$. Si noti ora che dalla proprietà associativa dell'operazione $\cdot$ su G e dall'ipotesi che 1 sia l'elemento neutro di G segue facilmente che l'operazione $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$ è associativa e che $\{1\}$ è l'elemento neutro di $\mathcal{P}(G)\setminus\{\varnothing\}$. La prima parte dell'enunciato è dunque dimostrata. Sia adesso $g \in G$. Si osservi che $\{g\} \cdot \{g^{-1}\} = \{g^{-1}\} \cdot \{g\} = \{1\}$, ma che ciò non è sufficiente per poter affermare che $\{g^{-1}\}$ è l'inverso di $\{g\}$ poiché in un monoide non vale, in generale, l'unicità dell'inverso. Sia dunque $A \in \mathcal{P}(G)\setminus\{\varnothing\}$ tale che $\{g\} \cdot A = A \cdot \{g\} = \{1\}$. Basta notare che, per costruzione e per unicità dell'inverso in G (proposizione 1.1-(i)), devono necessariamente valere le condizioni $|A| = 1$ e $g^{-1} \in A$, dalle quali segue immediatamente che $A = \{g^{-1}\}$ e quindi si ha la tesi. □

Osservazione 2.3. Sia G un gruppo e si consideri il monoide $\mathcal{P}(G)\setminus\{\varnothing\}$ munito dell'operazione binaria $\cdot$ definita nell'osservazione 2.2 e dell'elemento neutro $\{1\}$. Dalla stessa osservazione e dalla definizione 2.1 segue immediatamente che $aH = \{a\} \cdot H$ e che $Ha = H \cdot \{a\}$ per ogni $a \in G$.

Teorema 2.1. *Sia G un gruppo e sia $H < G$ un sottogruppo. Valgono le seguenti affermazioni.*

(i) *Siano $a, b \in G$. Allora $aH = bH$ se e solo se $a^{-1} \cdot b \in H$, invece $Ha = Hb$ se e solo se $a \cdot b^{-1} \in H$.*

(ii) *Le classi laterali sinistre di G rispetto a H formano una partizione di G, cioè esiste un insieme $S \subseteq G$ tale che $G = \coprod_{a \in S} aH$. Equivalentemente, le classi laterali sinistre di G rispetto a H sono o coincidenti o disgiunte e la loro unione è uguale a G. Analogamente, le classi laterali destre di G rispetto a H formano una partizione di G, cioè esiste un insieme $T \subseteq G$ tale che $G = \coprod_{a \in T} Ha$.*

(iii) *Sia $a \in G$. Allora le due applicazioni $\phi_a \colon H \to aH$ e $\psi_a \colon H \to Ha$ definite, rispettivamente, dalle condizioni $\phi_a(h) := a \cdot h$ e $\psi_a(h) := h \cdot a$ sono biiettive. In particolare, le classi laterali sinistre e destre di G rispetto a H hanno tutte la stessa cardinalità di H.*

(iv) *L'applicazione $I \colon G/H \to H\backslash G$ definita da $I(aH) := Ha^{-1}$ è biiettiva. In particolare, gli insiemi G/H e $H\backslash G$ hanno la stessa cardinalità.*

Dimostrazione. La dimostrazione dei punti (i), (ii) e (iii) tratterà delle sole classi laterali sinistre, poiché per quelle destre basta applicare un procedimento del tutto analogo.

(i) Assumo che $aH = bH$. Poiché per ipotesi $H < G$ è un sottogruppo, in particolare $1 \in H$ e quindi $a \in aH$, essendo $a = a \cdot 1$ per definizione di elemento neutro. Ovviamente vale che $a \in bH$, perché si assume che $aH = bH$ e di conseguenza esiste $h \in H$ tale che $a = b \cdot h$. In altre parole, passando all'inverso, si ha che $a^{-1} = h^{-1} \cdot b^{-1}$ per la proposizione 1.1-(iii) e dunque, moltiplicando a destra per b ambo i membri della relazione ottenuta, si ottiene che $a^{-1} \cdot b = h^{-1}$. Questo dimostra, per l'ipotesi che $H < G$ sia un sottogruppo, che $a^{-1} \cdot b \in H$.

Una dimostrazione alternativa dell'implicazione diretta è data utilizzando le osservazioni 2.2 e 2.3. Infatti, moltiplicando a sinistra primo e secondo membro della relazione $aH = bH$ per $\{a^{-1}\}$, si ottiene che $H = (a^{-1} \cdot b)H$. Dato che per ipotesi $H < G$ è un sottogruppo, in particolare $1 \in H$ e di conseguenza, dal momento che $a^{-1} \cdot b = (a^{-1} \cdot b) \cdot 1$ per definizione di elemento neutro, si ricava che $a^{-1} \cdot b \in (a^{-1} \cdot b)H$. Tale condizione, naturalmente, equivale alla tesi perché $H = (a^{-1} \cdot b)H$.

Viceversa, suppongo che $a^{-1} \cdot b \in H$ e pongo $h := a^{-1} \cdot b$. Moltiplicando a sinistra per a, si ricava che $b = a \cdot h$ ma allora, per associatività dell'operazione binaria $\cdot$ su G, per ogni $\tilde{h} \in H$ si ha che:

$$b \cdot \tilde{h} = (a \cdot h) \cdot \tilde{h} = a \cdot (h \cdot \tilde{h})$$

Essendo $H \subseteq G$ un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su G, posso dedurre dalla relazione precedente che $b \cdot \tilde{h} \in aH$ per ogni $\tilde{h} \in H$ e di conseguenza $bH \subseteq aH$. Similmente, dato che la condizione $b = a \cdot h$ è equivalente a richiedere che $a = b \cdot h^{-1}$, per ogni $\tilde{h} \in H$ vale anche che:

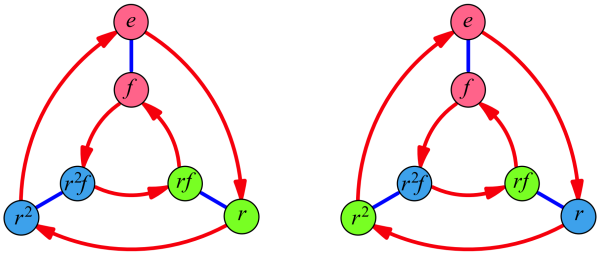
$$a \cdot \tilde{h} = (b \cdot h^{-1}) \cdot \tilde{h} = b \cdot (h^{-1} \cdot \tilde{h})$$

Come prima, dalla condizione ottenuta segue che $a \cdot \tilde{h} \in bH$ per ogni $\tilde{h} \in H$ e dunque $aH \subseteq bH$. Avendo mostrato la doppia inclusione, posso concludere che $aH = bH$.

(ii) Sia $\sim_L$ la relazione su G tale che $a \sim_L b$ se $aH = bH$. È immediato verificare che si tratta di una relazione di equivalenza. È un fatto noto[6] che le relazioni di equivalenza inducono una partizione dell'insieme sulle quali esse sono definite. La tesi segue quindi dal fatto che le classi di equivalenza della relazione $\sim_L$ coincidono con le classi laterali sinistre di G rispetto a H.

(iii) Dimostro che l'applicazione ϕ_a è iniettiva e suriettiva. Per definizione di classe laterale sinistra, se $b \in aH$, allora esiste $h \in H$ tale che $b = a \cdot h$, ma $a \cdot h = \phi_a(h)$ e quindi ϕ_a è suriettiva. Siano ora $h_1, h_2 \in H$ tali che $\phi_a(h_1) = \phi_a(h_2)$. Moltiplicando a sinistra per a^{-1} primo e secondo membro di tale relazione e ricordando come è definita ϕ_a, si ottiene subito che ϕ_a è iniettiva e posso dunque concludere che si tratta di un'applicazione biiettiva. La seconda affermazione deriva banalmente da quanto appena dimostrato e dall'arbitrarietà nella scelta dell'elemento $a \in G$.

(iv) Dimostro che l'applicazione I è iniettiva e suriettiva. Dalla proposizione 1.1-(ii) segue facilmente che, data una classe laterale destra $Hb \in H\backslash G$, vale che $Hb = H(b^{-1})^{-1}$ e dunque $Hb = I(b^{-1}H)$. Questo dimostra che I è suriettiva. Siano adesso $aH, bH \in G/H$ tali che $I(aH) = I(bH)$, cioè tali che $Ha^{-1} = Hb^{-1}$. Dal punto (i) già dimostrato e dalla proposizione 1.1-(ii) segue che $a^{-1} \cdot b \in H$ ma questo equivale a dire, ancora per il punto (i), che $aH = bH$ e di conseguenza I è iniettiva. In definitiva, si tratta di un'applicazione biiettiva. Come per il punto (iii), la seconda affermazione è una conseguenza immediata di quanto si è appena dimostrato. □



Il diagramma a sinistra mostra come il gruppo simmetrico S_3 viene partizionato dalle sue classi laterali sinistre rispetto al sottogruppo $\langle f \rangle < S_3$. Il diagramma a destra, invece, rappresenta la partizione indotta su S_3 dalle sue classi laterali destre rispetto al sottogruppo $\langle f \rangle < S_3$.

Definizione 2.2. Sia G un gruppo e sia $H < G$ un sottogruppo. La cardinalità di G/H oppure di $H\backslash G$ viene detta l'*indice di H in G* e si denota $[G:H]$. Inoltre, se tali insiemi hanno cardinalità finita, si dice anche che *H è di indice finito in G*.

La definizione 2.2 è ben posta in virtù del teorema 2.1-(iv).

Corollario 2.1 (Teorema di Lagrange)**.** *Dati un gruppo G di ordine finito e un sottogruppo $H < G$, vale la formula $|G| = |H|[G:H]$. In particolare, si ha che $|H|$ divide $|G|$.*

Dimostrazione. Innanzitutto, una conseguenza immediata dell'ipotesi che G sia un gruppo di ordine finito e che $H \subseteq G$ è che anche H è un gruppo di ordine finito. Ora, dal teorema 2.1-(ii) e dalla definizione 2.2 segue che G ammette una partizione in $[G:H]$ classi laterali sinistre (o destre) ciascuna delle quali, per il teorema 2.1-(iii), ha cardinalità uguale a $|H|$. Da questa semplice osservazione segue la tesi. □

Corollario 2.2 (Teorema di Cauchy)**.** *Siano G un gruppo di ordine finito, $a \in G$. Allora $o(a)$ divide $|G|$.*

Dimostrazione. Si consideri il sottogruppo $\langle a \rangle < G$ e si osservi che il più piccolo $n \in \mathbb{N}^*$ tale che $a^n = 1$ è lo stesso in $\langle a \rangle$ e in G perché $\langle a \rangle$ è chiuso rispetto all'operazione binaria $\cdot$ su G e ovviamente $a \in \langle a \rangle$. Dalla proposizione 1.5 segue in particolare che $|\langle a \rangle| = o(a)$ e da tale condizione, assieme all'ipotesi che G sia un gruppo di ordine finito e al fatto che $\langle a \rangle \subseteq G$, segue che a è un elemento di ordine finito. Dalla medesima relazione deriva la tesi come caso particolare del teorema di Lagrange (corollario 2.1). □

[6] Per approfondire la questione, si vedano gli appunti del corso AL110.

Esempio 2.1. Sia $n \in \mathbb{N}^*$ fissato, si considerino il gruppo $(\mathbb{Z}, +, 0)$ e il sottogruppo $\langle n \rangle < \mathbb{Z}$. Le classi laterali sinistre e destre di $\mathbb{Z}$ rispetto a $\langle n \rangle$ coincidono per l'osservazione 2.1. Si noti ora che le suddette classi laterali corrispondono alle classi di resto modulo n. Infatti, date due classi $a\langle n \rangle, b\langle n \rangle \in \mathbb{Z}/\langle n \rangle$, per il teorema 2.1-(i) vale che $a\langle n \rangle = b\langle n \rangle$ se e solo se $-a + b \in \langle n \rangle$, vale a dire se e solo se $n \mid -a + b$ e questo equivale a richiedere che $a \equiv b \pmod{n}$, cioè che a e b appartengano alla stessa classe di resto modulo n.

Esempio 2.2. Si consideri il gruppo S_n e si definisca $H := \{ \sigma \in S_n \mid \sigma(n) = n \}$. Si verifica facilmente che $H < S_n$ è un sottogruppo e che $H \simeq S_{n-1}$. In particolare, da quanto si è detto nell'esempio 1.18 segue che $|H| = (n-1)!$ e quindi, per il teorema di Lagrange (corollario 2.1), vale che $[S_n : H] = n$. Posso quindi considerare le applicazioni $\alpha \colon \{1, \dots, n\} \to S_n/H$ e $\beta \colon \{1, \dots, n\} \to H\backslash S_n$ definite da $\alpha(i) := (i\,n) \circ H$ e da $\beta(i) := H \circ (i\,n)$. Si dimostra facilmente che esse sono applicazioni biiettive. Si osservi inoltre che, per costruzione, si ha che $(i\,n) \circ H = \{ \sigma \in S_n \mid \sigma(n) = i \}$, mentre $H \circ (i\,n) = \{ \sigma \in S_n \mid \sigma(i) = n \}$.

Esempio 2.3. Siano $n \in \mathbb{N}^*$ fissato, K un campo e si consideri $\mathrm{GL}_n(K)$ munito dell'usuale operazione di prodotto tra matrici e con elemento neutro la matrice identità I_n. È immediato verificare che il seguente insieme, noto come il *gruppo lineare speciale di ordine n a coefficienti in K*, è un sottogruppo di $\mathrm{GL}_n(K)$:

$$\mathrm{SL}_n(K) := \{ A \in \mathrm{GL}_n(K) \mid \det A = 1 \}$$

Si osservi che in questo caso, anche se $\mathrm{GL}_n(K)$ non è in generale un gruppo abeliano (esempio 1.16) e non è quindi possibile usare l'osservazione 2.1, le classi laterali sinistre e destre di $\mathrm{GL}_n(K)$ rispetto a $\mathrm{SL}_n(K)$ coincidono. Si vede facilmente, infatti, che vale per ogni $A \in \mathrm{GL}_n(K)$ la condizione seguente:

$$A\mathrm{SL}_n(K) = \{ B \in \mathrm{GL}_n(K) \mid \det B = \det A \} = \mathrm{SL}_n(K)A$$

Infine, si dimostra facilmente che la mappa $\alpha \colon \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \to K \setminus \{0\}$ data da $\alpha(A\mathrm{SL}_n(K)) := \det A$ è una funzione ben definita e biiettiva. Questo lo si vedrà con maggior dettaglio in un esempio successivo.

Proposizione 2.1 (Moltiplicatività dell'indice)**.** *Sia G un gruppo e siano $K < H < G$ due sottogruppi. Allora esistono una corrispondenza biunivoca tra G/K e $G/H \times H/K$ e una tra $K\backslash G$ e $H\backslash G \times K\backslash H$. In particolare, se gli indici $[G:K]$, $[G:H]$ e $[H:K]$ sono finiti, allora vale la formula $[G:K] = [G:H][H:K]$.*

Dimostrazione. Verrà trattato soltanto il caso delle classi laterali sinistre, poiché quello delle classi laterali destre si studia con un approccio del tutto analogo. Innanzitutto, dal teorema 2.1-(ii) segue che esistono una collezione $\{a_i\} \subseteq G$, indicizzata su insieme I e una collezione $\{b_j\} \subseteq H$, indicizzata su un insieme J tali che $G = \coprod_{i \in I} a_i H$ e $H = \coprod_{j \in J} b_j K$. Ovviamente, si ha che $|I| = [G:H]$, $|J| = [H:K]$ per costruzione. Si vede facilmente, per doppio contenimento, che il prodotto tra insiemi è distributivo rispetto all'unione e di conseguenza vale la condizione seguente:

$$G = \bigcup_{i \in I} a_i H = \bigcup_{i \in I} a_i \bigcup_{j \in J} b_j K = \bigcup_{i \in I} \bigcup_{j \in J} (a_i \cdot b_j) K$$

In generale, non è detto[7] che una tale unione sia ancora disgiunta, ma in questo caso particolare le unioni disgiunte vengono rispettate. Siano infatti $i, l \in I$, $j, m \in J$ e si supponga che $(a_i \cdot b_j)K$ e $(a_l \cdot b_m)K$ siano classi laterali sinistre di G rispetto a K non disgiunte. Per il teorema 2.1-(ii) si deve avere la condizione $(a_i \cdot b_j)K = (a_l \cdot b_m)K$, mentre in virtù del teorema 2.1-(i) e tenendo a mente la proposizione 1.1-(iii) deve valere, posto $k := b_j^{-1} \cdot a_i^{-1} \cdot a_l \cdot b_m$, la relazione $k \in K$. Moltiplicando a sinistra per b_j e a destra per b_m^{-1} ambo i membri della definizione precedente, si ottiene che $a_i^{-1} \cdot a_l = b_j \cdot k \cdot b_m^{-1}$ ma allora, ricordando che $b_j, b_m \in H$ e che per ipotesi $K < H < G$ sono due sottogruppi, posso affermare che $a_i^{-1} \cdot a_l \in H$. Di nuovo per il teorema 2.1-(i) posso affermare che $a_i H = a_l H$ e quindi, usando il fatto che le classi laterali sinistre di G rispetto a H sono disgiunte, posso affermare che $a_i = a_l$. Dalle relazioni precedenti si ricava quindi che $k = b_j^{-1} \cdot b_m$ e dunque, applicando ancora una volta il teorema 2.1-(i), si ottiene che $b_j K = b_m K$. Da tale relazione e dal fatto che le classi laterali sinistre di H rispetto a K sono disgiunte segue che $b_j = b_m$. Questo mi consente di affermare che $G = \coprod_{(i,j) \in I \times J} (a_i \cdot b_j) K$. A questo punto basta osservare che G/K, G/H e H/K sono in corrispondenza biunivoca, rispettivamente, con gli insiemi $I \times J$, I e J sui quali essi sono indicizzati e quindi, per transitività, è dimostrata la prima parte dell'enunciato. La parte successiva deriva semplicemente dal fatto che la cardinalità del prodotto di due insiemi coincide con il prodotto delle rispettive cardinalità. □

[7] Siano $a, b, c, d \in G$ a due a due distinti tali che $a \cdot b = c \cdot d$. Allora $\{a, c\} \cdot (\{b\} \sqcup \{d\}) = (\{a, c\} \cdot \{b\}) \cup (\{a, c\} \cdot \{d\})$, ma l'unione che compare al secondo membro non è disgiunta, come è immediato verificare.

2.2 Sottogruppi normali e quozienti

Definizione 2.3. Sia G un gruppo. Due elementi $g_1, g_2 \in G$ vengono detti *coniugati* se esiste un terzo elemento $h \in G$ tale che $h \cdot g_1 \cdot h^{-1} = g_2$.

Osservazione 2.4. Sia G un gruppo. Allora la relazione di coniugio è una relazione di equivalenza su G.

Dimostrazione. Siano $g_1, g_2, g_3 \in G$ elementi fissati. È sufficiente osservare che il coniugio è una relazione:

- riflessiva: naturalmente, l'elemento neutro $1 \in G$ è tale che $1 \cdot g_1 \cdot 1^{-1} = g_1$.
- simmetrica: se esiste $h \in G$ tale che $h \cdot g_1 \cdot h^{-1} = g_2$ allora, moltiplicando a sinistra per h^{-1} e a destra per h ambo i membri di tale condizione, si ottiene che $h^{-1} \cdot g_2 \cdot h = g_1$.
- transitiva: se esistono $h, \tilde{h} \in G$ tali che $h \cdot g_1 \cdot h^{-1} = g_2$ e $\tilde{h} \cdot g_2 \cdot \tilde{h}^{-1} = g_3$ allora, tenendo a mente la proposizione 1.1-(iii) e usando l'associatività dell'operazione binaria $\cdot$ su G, si ha la relazione:

$$(\tilde{h} \cdot h) \cdot g_1 \cdot (\tilde{h} \cdot h)^{-1} = (\tilde{h} \cdot h) \cdot g_1 \cdot (h^{-1} \cdot \tilde{h}^{-1}) = \tilde{h} \cdot (h \cdot g_1 \cdot h^{-1}) \cdot \tilde{h}^{-1} = \tilde{h} \cdot g_2 \cdot \tilde{h}^{-1} = g_3 \quad \square$$

Le classi di equivalenza della relazione di coniugio sono dette *classi di coniugio*.

Definizione 2.4. Siano G un gruppo, $H < G$ un sottogruppo e sia $a \in G$. Si consideri inoltre il monoide $\mathcal{P}(G)\setminus\{\varnothing\}$ con l'operazione binaria $\cdot$ definita nell'osservazione 2.2 e con elemento neutro $\{1\}$. L'insieme definito da $aHa^{-1} := \{a\} \cdot H \cdot \{a^{-1}\}$ prende il nome di *sottogruppo coniugato di H rispetto ad a*.

Proposizione 2.2. *Siano G un gruppo, $H < G$ un sottogruppo, $a \in G$. Allora aHa^{-1} è un sottogruppo di G isomorfo a H.*

Dimostrazione. Innanzitutto, dimostro che $aHa^{-1} < G$ è un sottogruppo. Siano dunque $b_1, b_2 \in aHa^{-1}$ elementi prefissati. Per definizione, esistono $h_1, h_2 \in H$ tali che $b_1 = a \cdot h_1 \cdot a^{-1}$ e $b_2 = a \cdot h_2 \cdot a^{-1}$ quindi, dato che $b_1 \cdot b_2 = a \cdot h_1 \cdot h_2 \cdot a^{-1}$ ed essendo $H < G$ un sottogruppo, posso affermare che $b_1 \cdot b_2 \in aHa^{-1}$. Si osservi ora che $1 = a \cdot 1 \cdot a^{-1}$ e di conseguenza $1 \in aHa^{-1}$. Sia infine $b \in aHa^{-1}$. Come prima, esiste un elemento $h \in H$ tale che $b = a \cdot h \cdot a^{-1}$ e di conseguenza $b^{-1} = a \cdot h^{-1} \cdot a^{-1}$ per i punti (ii) e (iii) della proposizione 1.1. In particolare, si ha che $b^{-1} \in aHa^{-1}$ e dunque $aHa^{-1} < G$ è un sottogruppo.

Si consideri adesso l'applicazione $\varphi\colon H \to aHa^{-1}$ definita da $\varphi(h) := a \cdot h \cdot a^{-1}$. Per la definizione 2.4, si tratta di un'applicazione ben definita e suriettiva. Inoltre, dati $h_1, h_2 \in H$ tali che $\varphi(h_1) = \varphi(h_2)$, cioè tali che $a \cdot h_1 \cdot a^{-1} = a \cdot h_2 \cdot a^{-1}$, moltiplicando a sinistra per a^{-1} e a destra per a ambo i membri di tale condizione si ricava che $h_1 = h_2$ e questo mostra che φ è iniettiva. Infine, dati $h_1, h_2 \in H$, vale la relazione:

$$\varphi(h_1 \cdot h_2) = a \cdot (h_1 \cdot h_2) \cdot a^{-1} = (a \cdot h_1 \cdot a^{-1}) \cdot (a \cdot h_2 \cdot a^{-1}) = \varphi(h_1) \cdot \varphi(h_2)$$

Avendo dimostrato che $\varphi\colon H \to aHa^{-1}$ è un isomorfismo, ottengo la tesi. $\square$

Proposizione 2.3. *Siano G un gruppo, $H < G$ un sottogruppo. Le seguenti condizioni sono equivalenti:*

(i) $aHa^{-1} = H$ *per ogni* $a \in G$.

(ii) $aHa^{-1} \subseteq H$ *per ogni* $a \in G$.

(iii) $aHa^{-1} \supseteq H$ *per ogni* $a \in G$.

Dimostrazione. Le implicazioni (i) $\implies$ (ii) e (i) $\implies$ (iii) sono banali. Dimostro dunque che (ii) $\implies$ (iii). Sia $a \in G$. Per la condizione (ii) applicata all'elemento a^{-1} si ha che $a^{-1}Ha \subseteq H$ ma allora, moltiplicando a sinistra per $\{a\}$ e a destra per $\{a^{-1}\}$ entrambi i membri di tale relazione, ricordando la definizione 2.4 e l'osservazione 2.2, si ottiene che $H \subseteq aHa^{-1}$, vale a dire la condizione (iii). Con un procedimento simile si dimostra che (iii) $\implies$ (ii) e quindi vale che (ii) $\iff$ (iii). A questo punto basta notare che, assumendo la condizione (ii), dalla discussione precedente segue che vale anche la (iii) e quindi la (i), perché dal doppio contenimento deriva l'uguaglianza. Con lo stesso ragionamento si deduce che (iii) $\implies$ (i) e posso dunque concludere che le tre condizioni sono equivalenti. $\square$

Definizione 2.5. Sia G un gruppo. Un sottogruppo $H < G$ che soddisfa le condizioni equivalenti della proposizione 2.3 si dice un *sottogruppo normale di G* e si denota $H \lhd G$.

Osservazione 2.5. Sia G un gruppo e sia $H < G$ un sottogruppo. Allora $H \lhd G$ è un sottogruppo normale se e solo se H è unione disgiunta di classi di coniugio.

Dimostrazione. Innanzitutto, per l'osservazione 2.4 la relazione di coniugio è di equivalenza su G e quindi le classi di coniugio formano una partizione di G. Da questo segue in particolare che esse sono disgiunte. Ora se $H \lhd G$ è un sottogruppo normale allora, fissato $h \in H$, anche $a \cdot h \cdot a^{-1} \in H$ per ogni $a \in G$ per la definizione 2.5, ma questo equivale a richiedere che la classe di coniugio di h sia interamente contenuta in H. In particolare, per arbitrarietà nella scelta dell'elemento $h \in H$, l'unione delle classi di coniugio di tutti gli elementi di H è contenuta in H. L'altra inclusione è ovvia. Viceversa, se si assume che H sia unione disgiunta di classi di coniugio, allora per ogni $h \in H$ si ha che $a \cdot h \cdot a^{-1} \in H$ per ogni $a \in G$ in quanto, per ipotesi, la classe di coniugio di h interamente contenuta in H. In particolare, si ottiene che $aHa^{-1} \subseteq H$ per ogni $a \in G$ e di conseguenza $H \lhd G$ è un sottogruppo normale per definizione. □

Osservazione 2.6. Sia G un gruppo abeliano. Allora ogni sottogruppo di G è un sottogruppo normale.

Dimostrazione. Siano $H < G$ un sottogruppo, $a \in G$ e si consideri il monoide $\mathcal{P}(G)\setminus\{\varnothing\}$ con l'operazione binaria $\cdot$ definita nell'osservazione 2.2 e con elemento neutro $\{1\}$. È immediato verificare che, per l'ipotesi che G sia un gruppo abeliano e per come si è definito il prodotto $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$, il monoide $P(G)\setminus\{\varnothing\}$ è commutativo e di conseguenza, per associatività e commutatività dell'operazione $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$, in virtù dell'osservazione 2.2 e della definizione 2.4, vale la condizione seguente:

$$H = \{1\} \cdot H = (\{a\} \cdot \{a^{-1}\}) \cdot H = \{a\} \cdot (\{a^{-1}\} \cdot H) = \{a\} \cdot (H \cdot \{a^{-1}\}) = aHa^{-1}$$

Dall'arbitrarietà nella scelta di $a \in G$ e dalla definizione 2.5 segue che $H \lhd G$ è un sottogruppo normale. Chiaramente, per arbitrarietà nella scelta del sottogruppo $H < G$ si ha la tesi. □

Proposizione 2.4. *Siano G un gruppo, $H < G$ un sottogruppo. Le seguenti condizioni sono equivalenti:*

(i) *$H \lhd G$ è un sottogruppo normale.*

(ii.a) *$G/H = H\backslash G$.*

(ii.b) *$aH = Ha$ per ogni $a \in G$.*

(iii.a) *Il prodotto di classi laterali sinistre è una classe laterale sinistra e, allo stesso modo, il prodotto di classi laterali destre è una classe laterale destra.*

(iii.b) *$aH \cdot bH = (a \cdot b)H$ e $Ha \cdot Hb = H(a \cdot b)$ per ogni $a, b \in G$.*

Dimostrazione. Innanzitutto, si osservi che le implicazioni (ii.b) $\Longrightarrow$ (ii.a) e (iii.b) $\Longrightarrow$ (iii.a) sono banali. Dimostro quindi che (ii.a) $\Longrightarrow$ (ii.b). Fissato un elemento $a \in G$, per la condizione (ii.a) esiste $b \in G$ tale che $aH = Hb$. Si osservi che $a \in aH \cap Ha$ essendo $a = a \cdot 1 = 1 \cdot a$ per definizione di elemento neutro e $1 \in H$ per l'ipotesi che $H < G$ sia un sottogruppo. Dal fatto che $aH = Hb$ segue quindi che $a \in Hb \cap Ha$, ma allora $Hb = Ha$ perché le classi laterali destre di G rispetto a H sono coincidenti oppure disgiunte per il teorema 2.1-(ii). Ho dunque mostrato che $aH = Ha$ per ogni $a \in G$. Ora dimostro che (iii.a) $\Longrightarrow$ (iii.b) nel caso delle classi laterali sinistre. Per le classi laterali destre basta applicare un procedimento analogo. Assegnati due elementi $a, b \in G$, per la condizione (iii.a) esiste $c \in G$ tale che $aH \cdot bH = cH$. Si osservi che $a \cdot b \in (a \cdot b)H \cap (aH \cdot bH)$ poiché, come prima, vale che $a \cdot b = (a \cdot b) \cdot 1 = (a \cdot 1) \cdot (b \cdot 1)$ per definizione di elemento neutro e $1 \in H$ per l'ipotesi che $H < G$ sia un sottogruppo. Ma allora, essendo $aH \cdot bH = cH$, si ottiene che $a \cdot b \in (a \cdot b)H \cap cH$ e di conseguenza $(a \cdot b)H = cH$ in quanto le classi laterali sinistre di G rispetto a H sono coincidenti oppure disgiunte in virtù del teorema 2.1-(ii). Questo dimostra dunque che $aH \cdot bH = (a \cdot b)H$ per ogni $a, b \in H$.

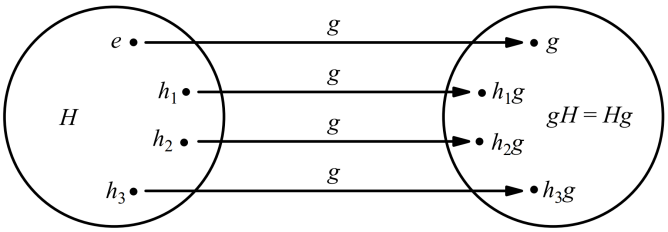
A questo punto sarà sufficiente mostrare che le condizioni (i), (ii.b) e (iii.b) sono equivalenti. È assai evidente che (i) $\Longrightarrow$ (ii.b). Se infatti $H \lhd G$ è un sottogruppo normale allora, per definizione, vale per ogni $a \in G$ la condizione $H = aHa^{-1}$ e quindi, moltiplicando a destra per $\{a\}$ ambo i membri di tale relazione e ricordando l'osservazione 2.2, si ottiene che $aH = Ha$ per ogni $a \in G$. Ora dimostro che (ii.b) $\Longrightarrow$ (iii.b). Fissati $a, b \in G$ osservo che, per la proprietà associativa di cui gode l'operazione binaria $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$ e per l'assunzione della condizione (ii.b), vale la relazione seguente:

$$aH \cdot bH = \{a\} \cdot Hb \cdot H = \{a\} \cdot bH \cdot H = \{a \cdot b\} \cdot (H \cdot H)$$

Dall'ipotesi che $H < G$ sia un sottogruppo e in particolare che H sia chiuso rispetto all'operazione binaria $\cdot$ su G segue che $H \cdot H \subseteq H$. Essendo invece $h = h \cdot 1$ per ogni $h \in H$ e ricordando che $1 \in H$, vale anche l'inclusione $H \subseteq H \cdot H$. Dal doppio contenimento segue che $H \cdot H = H$ e dalla relazione precedente ricavo che $aH \cdot bH = (a \cdot b)H$. Allo stesso modo si dimostra che $Ha \cdot Hb = H(a \cdot b)$. Rimane da dimostrare solo che (iii.b) $\implies$ (i). Sia $a \in G$ un elemento prefissato. Definendo $b := a^{-1}$, dalla condizione (iii.b) segue che $aH \cdot a^{-1}H = (a \cdot a^{-1})H = 1H = H$. Usando tale relazione e ricordando l'osservazione 2.2, si ottiene che:

$$aHa^{-1} = aHa^{-1} \cdot \{1\} \subseteq aHa^{-1} \cdot H = aH \cdot a^{-1}H = H$$

Dalla definizione 2.5 segue dunque che $H \lhd G$ è un sottogruppo normale e in definitiva l'equivalenza delle cinque affermazioni date nell'enunciato è dimostrata. □



Se $H \lhd G$ è un sottogruppo normale, le classi laterali sinistre e destre di G coincidono per la proposizione 2.4-(ii.b).

Osservazione 2.7. La condizione (ii.b) della proposizione 2.4 è più forte dell'affermazione (ii.a) in quanto non si limita a garantire che G abbia le stesse classi laterali sinistre e destre rispetto a H, bensì specifica con quali classi laterali destre coincidono le classi laterali sinistre di G rispetto a H, che vengono dunque considerate singolarmente. Similmente, l'affermazione (iii.b) è più forte della condizione (iii.a) perché non dice soltanto che il prodotto di due classi laterali di G rispetto a H è a sua volta una classe laterale, ma fornisce anche un rappresentante della classe.

Osservazione 2.8. In virtù della proposizione 2.4, una dimostrazione alternativa dell'osservazione 2.6 si può ricavare semplicemente combinando l'osservazione 2.1 con il punto (ii.b) della suddetta proposizione.

Esempio 2.4. Si considerino il gruppo S_n e il sottogruppo $H < S_n$ definito nell'esempio 2.2. Se $n \leq 2$ allora, ricordando l'esempio 1.14, il gruppo simmetrico è abeliano e quindi, in virtù dell'osservazione 2.6, ogni sottogruppo di S_n è normale. In particolare, il sottogruppo $H \lhd S_n$ è normale. Tuttavia, questo non è vero se $n \geq 3$. Si osservi innanzitutto che, per ogni $1 \leq i \leq n$, una descrizione esplicita del sottogruppo coniugato di H rispetto alla permutazione $(i\,n)$ è la seguente:

$$(i\,n) \circ H \circ (i\,n) = \{\, \sigma \in S_n \mid \sigma(i) = i \,\}$$

È infatti immediato verificare che vale il contenimento $\subseteq$ e che i due insiemi in relazione hanno entrambi cardinalità uguale a $(n-1)!$ (si è detto nell'esempio 2.2 che $H \simeq S_{n-1}$). A questo punto, per dimostrare che $H < S_n$ non è un sottogruppo normale, è sufficiente fissare due indici $1 \leq i < j < n$ e considerare la trasposizione $(i\,j) \in S_n$. Si noti che non è possibile fare una tale scelta di indici se $n \leq 2$. Essendo $j < n$, vale che $(i\,j)(n) = n$ e quindi $(i\,j) \in H$. D'altro canto, si ha che $(i\,j)(i) = j$ e quindi, essendo $i \neq j$, posso concludere che $(i\,j) \notin (i\,n) \circ H \circ (i\,n)$. Questo dimostra che $(i\,n) \circ H \circ (i\,n) \neq H$ e per la definizione 2.5 si ha che $H < S_n$ non è un sottogruppo normale.

Esempio 2.5. Sia $n \in \mathbb{N}^*$ fissato e sia K un campo. Si consideri $\mathrm{GL}_n(K)$ munito dell'usuale operazione di prodotto tra matrici e con elemento neutro la matrice identità I_n. Come si è detto nell'esempio 2.3, il gruppo lineare speciale $\mathrm{SL}_n(K)$ è un sottogruppo di $\mathrm{GL}_n(K)$. Dimostro che $\mathrm{SL}_n(K) \lhd \mathrm{GL}_n(K)$ è anche un sottogruppo normale. Sia $B \in \mathrm{GL}_n(K)$ e sia $A \in B\mathrm{SL}_n(K)B^{-1}$. In virtù della definizione 2.4, esiste una matrice $C \in \mathrm{SL}_n(K)$ tale che $A = BCB^{-1}$. Ricordando la definizione di $\mathrm{SL}_n(K)$ nell'esempio 2.3 e utilizzando le ben note proprietà del determinante, si ottiene quindi la condizione seguente:

$$\det A = \det BCB^{-1} = \det B \cdot \det C \cdot \det B^{-1} = \det B \cdot 1 \cdot (\det B)^{-1} = 1$$

Ne segue che $A \in \mathrm{SL}_n(K)$ e dunque, dato che il risultato ottenuto non dipende da una particolare scelta di $A \in B\mathrm{SL}_n(K)B^{-1}$, ottengo che $B\mathrm{SL}_n(K)B^{-1} \subseteq \mathrm{SL}_n(K)$. Posso quindi affermare che $\mathrm{SL}_n(K) \lhd \mathrm{GL}_n(K)$ in virtù della definizione 2.5.

Osservazione 2.9. Sia G un gruppo e sia $N \lhd G$ un sottogruppo normale. Si consideri inoltre il monoide $\mathcal{P}(G)\setminus\{\varnothing\}$ con l'operazione binaria $\cdot$ introdotta nell'osservazione 2.2 e con l'elemento neutro $\{1\}$. Allora l'insieme G/N oppure $N\backslash G$ munito della stessa operazione binaria $\cdot$ è un gruppo con elemento neutro N.

Dimostrazione. Innanzitutto si osservi che, in virtù della proposizione 2.4-(ii.b), è indifferente considerare G/N oppure $N\backslash G$ nel corso della dimostrazione. Inoltre, per il punto (iii.a) della medesima proposizione e per il fatto che l'insieme vuoto non è una classe laterale sinistra né destra di G rispetto a N, deduco che l'operazione binaria $\cdot$ su G/N è ben definita. È immediato verificare che la stessa operazione binaria gode della proprietà associativa utilizzando il fatto che l'operazione binaria $\cdot$ su G è associativa e la definizione dell'operazione binaria $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$. Sia adesso $aN \in G/N$ una classe laterale sinistra prefissata. Per la proposizione 2.4-(iii.b), usando il fatto che 1 è l'elemento neutro di G, si ricavano le relazioni seguenti:

$$aN \cdot N = (a \cdot 1)N = aN$$
$$N \cdot aN = (1 \cdot a)N = aN$$

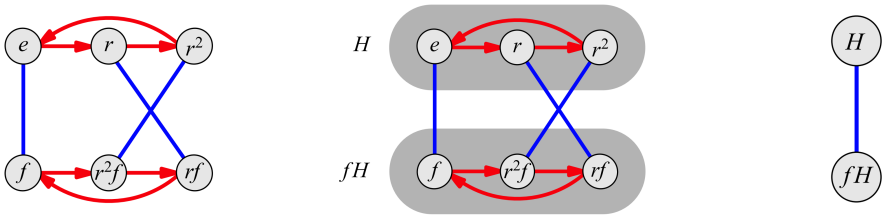
Da tali condizioni segue che N è un elemento neutro di G/N per definizione. Infine, utilizzando di nuovo la proposizione 2.4-(iii.b), si verifica facilmente che $(aN)^{-1} = a^{-1}N$. Si hanno infatti le seguenti relazioni:

$$aN \cdot a^{-1}N = (a \cdot a^{-1})N = N$$
$$a^{-1}N \cdot aN = (a^{-1} \cdot a)N = N$$

Posso dunque concludere che G/N, sotto le ipotesi date, è un gruppo con elemento neutro N. □

Definizione 2.6. Sia G un gruppo e sia $N \lhd G$ un sottogruppo normale. Si consideri inoltre il monoide $\mathcal{P}(G)\setminus\{\varnothing\}$ con l'operazione binaria $\cdot$ definita nell'osservazione 2.2 e con l'elemento neutro $\{1\}$. Il gruppo G/N oppure $N\backslash G$ munito della stessa operazione binaria $\cdot$ e dell'elemento neutro N viene detto il *gruppo quoziente di G rispetto a N*. Inoltre, per ogni $a \in G$, si introduce la notazione $[a]_N$ per indicare la classe laterale $aN = Na$.

La definizione 2.6 è ben posta in virtù dell'osservazione 2.9 e della proposizione 2.4-(ii.b).



I diagrammi rappresentano il passaggio dal gruppo simmetrico S_3 al suo gruppo quoziente $S_3/\langle r\rangle$. Gli elementi che appartengono a una stessa classe laterale vengono raggruppati e nel quoziente vengono considerati come se fossero un unico elemento. Naturalmente, questo si può fare solo in virtù del fatto che $\langle r\rangle \lhd S_3$ è un sottogruppo normale.

Esempio 2.6. Sia $n \in \mathbb{N}^*$ fissato, si considerino il gruppo $(\mathbb{Z}, +, 0)$ e il sottogruppo $\langle n\rangle < \mathbb{Z}$. Essendo $\mathbb{Z}$ un gruppo abeliano, il sottogruppo $\langle n\rangle \lhd \mathbb{Z}$ è normale in virtù dell'osservazione 2.6. Come si è accennato nell'esempio 2.1, esiste una stretta correlazione tra il gruppo $(\mathbb{Z}_n, +, \bar{0})$ e il gruppo quoziente $\mathbb{Z}/\langle n\rangle$. Più precisamente, i due gruppi sono isomorfi. Si consideri infatti l'applicazione $\eta\colon \mathbb{Z}/\langle n\rangle \to \mathbb{Z}_n$ definita dalla condizione $\eta(a\langle n\rangle) := \bar{a}$. Ripetendo l'argomento utilizzato nell'esempio 2.1, si vede immediatamente che, se $b\langle n\rangle = a\langle n\rangle$, allora $a \equiv b \pmod{n}$ e quindi η è un'applicazione ben definita. Poiché tale procedimento consiste solo ed esclusivamente di doppie implicazioni logiche è lecito ripercorrerlo a ritroso, dimostrando così che η è anche iniettiva. Si tratta invece di un'applicazione suriettiva per costruzione e posso dunque affermare che η è un'applicazione biiettiva. Infine, comunque fissati $a\langle n\rangle, b\langle n\rangle \in \mathbb{Z}/\langle n\rangle$, vale in virtù della proposizione 2.4-(iii.b), ricordando la definizione dell'operazione additiva $+$ in $\mathbb{Z}_n$, la condizione seguente:

$$\eta(a\langle n\rangle \cdot b\langle n\rangle) = \eta\big((a+b)\langle n\rangle\big) = \overline{a+b} = \bar{a} + \bar{b} = \eta(a\langle n\rangle) + \eta(b\langle n\rangle)$$

Questo dimostra, in definitiva, che $\eta\colon \mathbb{Z}/\langle n\rangle \to \mathbb{Z}_n$ è un isomorfismo.

Esempio 2.7. Siano $n \in \mathbb{N}^*$ fissato, K un campo e si consideri $\mathrm{GL}_n(K)$ munito dell'usuale operazione di prodotto tra matrici e con elemento neutro la matrice identità I_n. Come si è dimostrato nell'esempio 2.5, il sottogruppo $\mathrm{SL}_n(K) \lhd \mathrm{GL}_n(K)$ è normale e ha dunque senso attribuire al quoziente $\mathrm{GL}_n(K)/\mathrm{SL}_n(K)$ una struttura di gruppo. Si consideri adesso l'applicazione $\alpha\colon \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \to K\setminus\{0\}$ definita dalla condizione $\alpha(A\mathrm{SL}_n(K)) := \det A$. Nella parte finale dell'esempio 2.3 si era accennato che questa funzione fosse biiettiva. Dimostro che α è non solo un'applicazione biiettiva, ma anche un isomorfismo di gruppi. Si noti innanzitutto che α è ben definita. Infatti, per il teorema 2.1-(i) vale che $B\mathrm{SL}_n(K) = A\mathrm{SL}_n(K)$ se e solo se $B^{-1}A \in \mathrm{SL}_n(K)$, ma questo per definizione di $\mathrm{SL}_n(K)$ è equivalente a richiedere che $\det B^{-1}A = 1$ cioè, per le proprietà del determinante, che $\det B = \det A$. Siccome ogni passaggio effettuato è una doppia implicazione logica, posso ripercorrere a ritroso lo stesso ragionamento e da questo ricavo che α è iniettiva. Per mostrare che α è suriettiva, dato un qualsiasi $\lambda \in K\setminus\{0\}$ basta considerare la classe laterale $A\mathrm{SL}_n(K)$ dove A è la matrice definita nella maniera seguente:

$$A := \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

È infatti evidente, per la[8] regola di Laplace sullo sviluppo del determinante, che $\det A = \lambda$. Dato che α è anche suriettiva, posso dunque affermare che essa è un'applicazione biiettiva. Si noti infine che, per ogni $A\mathrm{SL}_n(K), B\mathrm{SL}_n(K) \in \mathrm{GL}_n(K)/\mathrm{SL}_n(K)$, si ha in virtù della proposizione 2.4-(iii.b) e delle proprietà del determinante la condizione seguente:

$$\alpha\big(A\mathrm{SL}_n(K)B\mathrm{SL}_n(K)\big) = \alpha\big(AB\mathrm{SL}_n(K)\big) = \det AB = \det A \cdot \det B = \alpha\big(A\mathrm{SL}_n(K)\big) \cdot \alpha\big(B\mathrm{SL}_n(K)\big)$$

Posso dunque concludere che $\alpha\colon \mathrm{GL}_n(K)/\mathrm{SL}_n(K) \to K\setminus\{0\}$ è un isomorfismo.

Definizione 2.7. Sia G un gruppo. Il seguente insieme viene detto il *centro di* G:

$$Z(G) := \{\, g \in G \mid g \cdot x = x \cdot g \ \ \forall\, x \in G \,\}$$

Osservazione 2.10. Sia G un gruppo. Allora $Z(G) \lhd G$ è un sottogruppo normale.

Dimostrazione. Sia $a \in G$ un elemento arbitrario e sia fissato $g \in aZ(G)a^{-1}$. Dalla definizione 2.4 segue che esiste $h \in Z(G)$ tale che $g = a \cdot h \cdot a^{-1}$ ma allora, essendo $h \cdot a^{-1} = a^{-1} \cdot h$ per la definizione 2.7, vale che $g = h$ e in particolare $g \in Z(G)$. Poiché il risultato ottenuto non dipende da una particolare scelta di $g \in aZ(G)a^{-1}$, posso affermare che $aZ(G)a^{-1} \subseteq Z(G)$. Dall'arbitrarietà nella scelta dell'elemento $a \in G$ e dalla definizione 2.5 segue dunque che $Z(G) \lhd G$ è un sottogruppo normale. □

Osservazione 2.11. Sia G un gruppo. Dalle definizioni 1.3 e 2.7 segue immediatamente che G è un gruppo abeliano se e solo se $Z(G) = G$.

Esempio 2.8. Sia $n \in \mathbb{N}$, $n \geq 3$. È facile verificare, per contrapposizione logica, che $Z(S_n) = \{\mathrm{id}_{\{1,\dots,n\}}\}$. Sia infatti $\sigma \in S_n$, $\sigma \neq \mathrm{id}_{\{1,\dots,n\}}$ una permutazione. Poiché $\sigma \neq \mathrm{id}_{\{1,\dots,n\}}$, esistono $1 \leq a \neq b \leq n$ tali che $\sigma(a) = b$. Sia inoltre $1 \leq c \leq n$ tale che $c \neq a$ e $c \neq b$. Un tale c esiste in virtù dell'assunzione che $n \geq 3$. A questo punto basta semplicemente osservare che $(b\,c) \circ \sigma \neq \sigma \circ (b\,c)$. Si noti infatti che vale la relazione:

$$\big((b\,c) \circ \sigma\big)(a) = (b\,c)\big(\sigma(a)\big) = (b\,c)(b) = c \neq b = \sigma(a) = \sigma\big((b\,c)(a)\big) = \big(\sigma \circ (b\,c)\big)(a)$$

Questo dimostra che, se $n \geq 3$, allora in $Z(S_n)$ non vi è nessun elemento diverso dall'applicazione identità. Il caso $n \leq 2$, invece, non è di particolare interesse. In tal caso, infatti, come si è detto nell'esempio 1.14 il gruppo simmetrico è abeliano e di conseguenza $Z(S_n) = S_n$ in virtù dell'osservazione 2.11.

Definizione 2.8. Sia G un gruppo e siano $a, b \in G$. L'elemento $[a, b] := a \cdot b \cdot a^{-1} \cdot b^{-1}$ prende il nome di *commutatore di* a *e* b. Il sottogruppo generato dai commutatori, invece, si denota $[G, G]$ e viene detto il *sottogruppo commutatore di* G.

La definizione 2.8 è ben posta per definizione di gruppo.

[8] Per maggiori dettagli in merito, si vedano gli appunti del corso GE110.

Osservazione 2.12. Sia G un gruppo e siano $a, b \in G$. Dalla definizione di inverso segue immediatamente la validità della condizione $a \cdot b = [a, b] \cdot b \cdot a$.

Osservazione 2.13. Sia G un gruppo. Allora $[G, G] \lhd G$ è un sottogruppo normale.

Dimostrazione. Innanzitutto si osservi che, per le definizioni 1.8 e 2.8, che $[G, G] < G$ è un sottogruppo. Siano ora $g \in G$ e $h \in g[G, G]g^{-1}$ elementi prefissati. In virtù dell'osservazione 1.13 esistono due collezioni finite $\{a_1, \dots, a_n\}, \{b_1, \dots, b_n\} \subseteq G$, di elementi non necessariamente distinti, tali che valga la condizione:

$$h = g \cdot a_1 \cdot b_1 \cdot a_1^{-1} \cdot b_1^{-1} \cdots a_n \cdot b_n \cdot a_n^{-1} \cdot b_n^{-1} \cdot g^{-1}$$

Dimostro per induzione su $n \in \mathbb{N}$ la validità della seguente formula:

$$h = [g, a_1] \cdot a_1 \cdot [g, b_1] \cdot b_1 \cdot [g, a_1^{-1}] \cdot a_1^{-1} \cdot [g, b_1^{-1}] \cdot b_1^{-1} \cdots [g, a_n^{-1}] \cdot a_n^{-1} \cdot [g, b_n^{-1}] \cdot b_n^{-1} \tag{4}$$

Nella base di induzione, applicando più volte l'osservazione 2.12, si può modificare la posizione di elementi successivi nel prodotto e ottenere così la formula (4) nel caso $n = 1$, come mostra la condizione seguente:

$$\begin{aligned} h &= g \cdot a_1 \cdot b_1 \cdot a_1^{-1} \cdot b_1^{-1} \cdot g^{-1} \\ &= [g, a_1] \cdot a_1 \cdot g \cdot b_1 \cdot a_1^{-1} \cdot b_1^{-1} \cdot g^{-1} \\ &= [g, a_1] \cdot a_1 \cdot [g, b_1] \cdot b_1 \cdot g \cdot a_1^{-1} \cdot b_1^{-1} \cdot g^{-1} \\ &= [g, a_1] \cdot a_1 \cdot [g, b_1] \cdot b_1 \cdot [g, a_1^{-1}] \cdot a_1^{-1} \cdot g \cdot b_1^{-1} \cdot g^{-1} \\ &= [g, a_1] \cdot a_1 \cdot [g, b_1] \cdot b_1 \cdot [g, a_1^{-1}] \cdot a_1^{-1} \cdot [g, b_1^{-1}] \cdot b_1^{-1} \end{aligned}$$

Il passo induttivo si dimostra con un argomento identico. Definisco adesso $c_i := [g, a_i] \cdot a_i$, $d_i := [g, b_i] \cdot b_i$ per ogni $1 \leq i \leq n$ e, ricordando la proposizione 1.1-(iii), osservo che vale per ogni $1 \leq i \leq n$ la relazione:

$$\begin{aligned} c_i^{-1} &= ([g, a_i] \cdot a_i)^{-1} = (g \cdot a_i \cdot g^{-1} \cdot a_i^{-1} \cdot a_i)^{-1} = (g \cdot a_i \cdot g^{-1})^{-1} \\ &= g \cdot a_i^{-1} \cdot g^{-1} = g \cdot a_i^{-1} \cdot g^{-1} \cdot a_i \cdot a_i^{-1} = [g, a_i^{-1}] \cdot a_i^{-1} \end{aligned}$$

Allo stesso modo si dimostra che $d_i^{-1} = [g, b_i^{-1}] \cdot b_i^{-1}$ e dalla formula (4) ricavo quindi la relazione seguente:

$$h = c_1 \cdot d_1 \cdot c_1^{-1} \cdot d_1^{-1} \cdots c_n \cdot d_n \cdot c_n^{-1} \cdot d_n^{-1} = [c_1, d_1] \cdots [c_n, d_n]$$

Questo dimostra che $h \in [G, G]$ e di conseguenza, non dipendendo il risultato ottenuto da una particolare scelta di $h \in g[G, G]g^{-1}$, posso affermare che $g[G, G]g^{-1} \subseteq [G, G]$. Ma allora, per arbitrarietà nella scelta di $g \in G$ e in virtù della definizione 2.5, posso concludere che $[G, G] \lhd G$ è un sottogruppo normale. □

Definizione 2.9. Sia G un gruppo. Il gruppo quoziente $G^{\text{ab}} := G/[G, G]$ munito dell'operazione binaria $\cdot$ introdotta nell'osservazione 2.2 e con elemento neutro $[G, G]$ prende il nome di *abelianizzato di* G.

La definizione 2.9 è ben posta in virtù dell'osservazione 2.13.

Osservazione 2.14. Sia G un gruppo. Allora G^{ab} con l'operazione binaria $\cdot$ definita nell'osservazione 2.2 e con elemento neutro $[G, G]$ è un gruppo abeliano.

Dimostrazione. Innanzitutto, l'osservazione 2.9 garantisce che G^{ab} sia un gruppo con operazione binaria ed elemento neutro dati nelle ipotesi. Basta quindi mostrare che, comunque fissati $g[G, G], h[G, G] \in G^{\text{ab}}$, vale la relazione $g[G, G] \cdot h[G, G] = h[G, G] \cdot g[G, G]$. In virtù della proposizione 2.4-(iii.b), sarà sufficiente dimostrare che vale la condizione $(g \cdot h)[G, G] = (h \cdot g)[G, G]$. Sia $x \in (g \cdot h)[G, G]$ un elemento prefissato. In virtù dell'osservazione 1.13 esistono due collezioni finite $\{a_1, \dots, a_n\}, \{b_1, \dots, b_n\} \subseteq G$, i cui elementi sono a priori non tutti distinti, tali che $x = (g \cdot h) \cdot [a_1, b_1] \cdots [a_n, b_n]$. Adesso, per la proposizione 1.1-(iii), vale la condizione seguente:

$$\begin{aligned} x &= (g \cdot h) \cdot [a_1, b_1] \cdots [a_n, b_n] = (h \cdot g) \cdot (h \cdot g)^{-1} \cdot (g \cdot h) \cdot [a_1, b_1] \cdots [a_n, b_n] \\ &= (h \cdot g) \cdot (g^{-1} \cdot h^{-1} \cdot g \cdot h) \cdot [a_1, b_1] \cdots [a_n, b_n] = (h \cdot g) \cdot [g^{-1}, h^{-1}] \cdot [a_1, b_1] \cdots [a_n, b_n] \end{aligned}$$

Ho dunque mostrato che $x \in (h \cdot g)[G, G]$ e dunque, per arbitrarietà nella scelta di $x \in (g \cdot h)[G, G]$, posso affermare che $(g \cdot h)[G, G] \subseteq (h \cdot g)[G, G]$. L'altra inclusione si dimostra applicando un ragionamento del tutto analogo e quindi, per arbitrarietà nella scelta delle classi laterali $g[G, G], h[G, G] \in G^{\text{ab}}$, ottengo che G^{ab} è un gruppo abeliano. □

Osservazione 2.15. Sia G un gruppo. Allora $[G,G]$ è il più piccolo sottogruppo normale di G tale che il quoziente sia un gruppo abeliano. Più esplicitamente, se $N \lhd G$ è un sottogruppo normale tale che G/N sia un gruppo abeliano, allora $[G,G] \subseteq N$.

Dimostrazione. Sia $g \in [G,G]$ un elemento prefissato. Per l'osservazione 1.13 esistono due collezioni finite $\{a_1,\dots,a_n\},\{b_1,\dots,b_n\} \subseteq G$ tali che $g = [a_1,b_1]\cdots[a_n,b_n]$. Sia adesso $N \lhd G$ un sottogruppo normale tale che G/N sia un gruppo abeliano e sia $1 \leq i \leq n$ un indice fissato. Per l'ipotesi che G/N sia un gruppo abeliano, vale in particolare l'identità $a_i^{-1}N \cdot b_i^{-1}N = b_i^{-1}N \cdot a_i^{-1}N$ e in virtù della proposizione 2.4-(iii.b) ciò equivale a richiedere che $(a_i^{-1}\cdot b_i^{-1})N = (b_i^{-1}\cdot a_i^{-1})N$. Moltiplicando ambo i membri della condizione ottenuta per $\{a_i \cdot b_i\}$ e ricordando la definizione 2.8, si ottiene che $N = [a_i,b_i]N$. Dato che $N < G$ è un sottogruppo, vale in particolare che $1 \in N$ e di conseguenza $[a_i,b_i] \in [a_i,b_i]N$ perché $[a_i,b_i] = [a_i,b_i]\cdot 1$. Ma allora, essendo $N = [a_i,b_i]N$ e ricordando che la scelta dell'indice $1 \leq i \leq n$ è del tutto arbitraria, si può affermare che $[a_i,b_i] \in N$ per ogni $1 \leq i \leq n$. A questo punto basta utilizzare il fatto che N è chiuso rispetto all'operazione binaria $\cdot$ su G per dedurne che $g \in N$. Questo dimostra che $[G,G] \subseteq N$ e dunque, non dipendendo il risultato ottenuto dalla scelta del sottogruppo normale $N \lhd G$, si ha la tesi. □

Osservazione 2.16. Sia G un gruppo e sia $H < G$ un sottogruppo. Se $[G\!:\!H] = 2$, allora $H \lhd G$ è normale.

Dimostrazione. Sia $a \in G$. Si osservi innanzitutto che, se $a \in H$, allora $aH = H$. Se infatti $g \in aH$, allora $g = a \cdot h$ per un qualche $h \in H$ e quindi $g \in H$ per chiusura di H rispetto all'operazione binaria $\cdot$ su G. Se invece $g \in H$ allora, utilizzando il fatto che $g = a\cdot(a^{-1}\cdot h)$ e che $H < G$ è un sottogruppo, si ottiene che $g \in aH$. Chiaramente, ragionando allo stesso modo si dimostra che $Ha = H$ se $a \in H$. Ora, se fosse $H = G$, allora dalla discussione precedente seguirebbe che $[G\!:\!H] = 1$ e questo contraddice le ipotesi. Si può dunque supporre che $a \notin H$. Naturalmente, in tal caso $aH \neq H$ in quanto $a = a\cdot 1$ per definizione di elemento neutro e $a \cdot 1 \in aH$, ma $a \notin H$. Per ragioni del tutto analoghe, si ha anche che $Ha \neq H$. Poiché per ipotesi $[G\!:\!H] = 2$, posso affermare che $G/H = \{\, H, aH \,\}$, mentre $H\backslash G = \{\, H, Ha \,\}$. A questo punto, per il teorema 2.1-(ii) si ha che $G = H \sqcup aH$ e che $G = H \sqcup Ha$. Da queste condizioni segue banalmente che $aH = Ha$. Per le proprietà dell'unione disgiunta, infatti, vale che $g \in aH$ se e solo se $g \notin H$ e questo accade se e solo se $g \in Ha$. Posso dunque concludere, per il teorema 2.4-(ii.a), che $H \lhd G$ è normale. □

Osservazione 2.17. Sia G un gruppo e sia $N \lhd G$ un sottogruppo normale. Se vale che $N \cap [G,G] = \{1\}$, allora si ha la condizione $N \subseteq Z(G)$.

Dimostrazione. Siano $x \in N$ e $a \in G$ due elementi fissati. Per la proposizione 1.1-(iii) e per l'associatività dell'operazione binaria $\cdot$ su G, vale la condizione seguente:

$$x\cdot a = (a\cdot x)\cdot(a\cdot x)^{-1}\cdot(x\cdot a) = (a\cdot x)\cdot(x^{-1}\cdot a^{-1}\cdot x\cdot a)$$

Si osservi ora che $a^{-1}\cdot x\cdot a \in a^{-1}Na$ e che $a^{-1}Na = N$ perché si assume che $N \lhd G$ sia un sottogruppo normale. Essendo in particolare $N < G$ un sottogruppo, si ha che $x^{-1}\cdot a^{-1}\cdot x\cdot a \in N$. D'altra parte, lo stesso elemento non è altro che il commutatore di x^{-1} e a^{-1} e di conseguenza $x^{-1}\cdot a^{-1}\cdot x\cdot a \in [G,G]$. Ma allora, poiché per ipotesi vale che $N \cap [G,G] = \{1\}$, si dovrà avere che $x^{-1}\cdot a^{-1}\cdot x\cdot a = 1$ e dalla relazione precedente si ricava dunque che $x\cdot a = a\cdot x$ per definizione di elemento neutro. Posso dunque affermare, per arbitrarietà nella scelta di $a \in G$, che $x \in Z(G)$. Per arbitrarietà nella scelta di $x \in N$ si ha la tesi. □

2.3 Congruenze e quozienti

Definizione 2.10. Sia G un gruppo. Una relazione di equivalenza $\equiv$ su G tale che, fissati $a,a',b,b' \in G$ con $a \equiv a'$ e $b \equiv b'$, valga la condizione $a\cdot b \equiv a'\cdot b'$ viene detta una *congruenza su* G. Inoltre, l'insieme quoziente $G/\!\equiv$ viene detto il *quoziente di* G *per la congruenza* $\equiv$ e si denota anche $\bar{G}$.

Osservazione 2.18. Sia G un gruppo e sia $\equiv$ una congruenza su G. Allora l'insieme quoziente $\bar{G}$ munito dell'operazione binaria $\cdot$ definita da $[a]\cdot[b] := [a\cdot b]$ è un gruppo con elemento neutro $[1]$.

Dimostrazione. Si noti innanzitutto che, per definizione di congruenza, l'operazione binaria $\cdot$ su $\bar{G}$ è ben posta. Infatti, dati $a,a',b,b' \in G$ tali che $[a] = [a']$ e $[b] = [b']$, vale che $[a\cdot b] = [a'\cdot b']$. Dall'associatività dell'operazione binaria $\cdot$ su G segue immediatamente che anche l'operazione $\cdot$ su $\bar{G}$ gode della proprietà

associativa. Similmente, dal fatto che 1 è l'elemento neutro di G segue che $[1]$ è un elemento neutro di $\bar{G}$, infatti valgono per ogni $[a] \in \bar{G}$ le due condizioni seguenti:

$$[a] \cdot [1] = [a \cdot 1] = [a]$$
$$[1] \cdot [a] = [1 \cdot a] = [a]$$

Altrettanto facilmente si vede che $[a]^{-1} = [a^{-1}]$ per ogni $a \in \bar{G}$. La verifica di questo fatto è immediata:

$$[a] \cdot [a^{-1}] = [a \cdot a^{-1}] = [1]$$
$$[a^{-1}] \cdot [a] = [a^{-1} \cdot a] = [1]$$

Posso dunque concludere che l'insieme quoziente $\bar{G}$ munito dell'operazione binaria $\cdot$ data nelle ipotesi è un gruppo con elemento neutro $[1]$. □

Definizione 2.11. Sia G un gruppo e sia $\equiv$ una congruenza su G. Il gruppo $\bar{G}$ con l'operazione binaria $\cdot$ definita da $[a] \cdot [b] := [a \cdot b]$ e con elemento neutro $[1]$ si dice il *gruppo quoziente di G per la congruenza $\equiv$*.

Teorema 2.2. *Sia G un gruppo. Valgono le seguenti affermazioni.*

(i) *Data una qualunque congruenza $\equiv$ su G, si definisca $N(\equiv) := \{\, g \in G \mid g \equiv 1 \,\}$. Per ogni $N \lhd G$ sottogruppo normale, sia invece $\equiv_N$ la relazione per la quale valga $a \equiv_N b$ se $a \cdot b^{-1} \in N$. Allora la funzione $\Phi\colon \{$ Congruenze su $G \} \to \{$ Sottogruppi normali di $G \}$ data da $\Phi(\equiv) := N(\equiv)$ è una corrispondenza biunivoca la cui inversa $\Psi\colon \{$ Sottogruppi normali di $G \} \to \{$ Congruenze su $G \}$ è definita da $\Psi(N) := \equiv_N$.*

(ii) *Sia $\equiv$ una congruenza su G e sia $N := N(\equiv)$. Allora $G/{\equiv} \simeq G/N$.*

Dimostrazione.

(i) Innanzitutto, dimostro che le applicazioni Φ e Ψ sono ben definite. Fissata quindi una congruenza $\equiv$ su G, dimostro che $N(\equiv) \lhd G$ è un sottogruppo normale. Dalla definizione di congruenza segue che $N(\equiv)$ è chiuso rispetto all'operazione binaria $\cdot$ su G. Infatti, comunque fissati $g, g' \in N(\equiv)$, si ha che $g \equiv 1$ e che $g' \equiv 1$ per definizione di $N(\equiv)$ e di conseguenza vale la condizione seguente:

$$g \cdot g' \equiv 1 \cdot 1 = 1$$

Ancora per definizione di $N(\equiv)$, questo significa che $g \cdot g' \in N(\equiv)$. Adesso, utilizzando il fatto che una congruenza è per definizione una relazione di equivalenza, vale che $1 \equiv 1$ e questo implica, per definizione di $N(\equiv)$, che $1 \in N(\equiv)$. Sia ora $g \in N(\equiv)$, cioè tale che $g \equiv 1$. Ancora per la proprietà riflessiva delle relazioni di equivalenza e per definizione di congruenza, posso moltiplicare a sinistra per g^{-1} ambo i membri della relazione precedente e applicare la definizione di inverso, ottenendo che $g^{-1} \equiv 1$ e quindi che $g^{-1} \in N(\equiv)$. Questo dimostra che $N(\equiv) < G$ è un sottogruppo.

Sia adesso $a \in G$ un elemento fissato e sia $g \in aN(\equiv)a^{-1}$. In virtù della definizione 2.4, esiste un elemento $h \in N(\equiv)$ tale che $g = a \cdot h \cdot a^{-1}$. Utilizzando il fatto, noto per definizione di $N(\equiv)$, che $h \equiv 1$, applicando la proprietà riflessiva e la definizione di inverso, si ottiene la relazione seguente:

$$g = a \cdot h \cdot a^{-1} \equiv a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1$$

Ma allora, sempre per definizione di $N(\equiv)$, si ha che $g \in N(\equiv)$ e questo dimostra, per arbitrarietà nella scelta di $g \in aN(\equiv)a^{-1}$, che vale l'inclusione $aN(\equiv)a^{-1} \subseteq N(\equiv)$. Dato che tale condizione non dipende da una particolare scelta di $a \in G$ posso affermare, in virtù della definizione 2.5, che $N(\equiv) \lhd G$ è un sottogruppo normale e da questo segue che Φ è un'applicazione ben definita.

Sia adesso $N \lhd G$ un sottogruppo normale e siano $a, b, c \in G$ elementi prefissati. Si osservi che la relazione $\equiv_N$ gode delle seguenti proprietà:

- riflessiva: per definizione di inverso, vale la condizione $a \cdot a^{-1} = 1$ e ovviamente $1 \in N$ poiché si sta assumendo che $N < G$ sia un sottogruppo. Di conseguenza, si ha che $a \equiv_N a$.
- simmetrica: se $a \equiv_N b$, allora $a \cdot b^{-1} \in N$ per costruzione di $\equiv_N$. Dal momento che $N < G$ è un sottogruppo, anche $(a \cdot b^{-1})^{-1} \in N$, ma $(a \cdot b^{-1})^{-1} = b \cdot a^{-1}$ per la proposizione 1.1-(iii) e quindi $b \equiv_N a$ per come è definita la relazione $\equiv_N$.

- transitiva: se $a \equiv_N b$ e $b \equiv_N c$, allora $a \cdot b^{-1} \in N$ e $b \cdot c^{-1} \in N$ per definizione di $\equiv_N$. Poiché N è chiuso rispetto all'operazione binaria $\cdot$ su G, anche $(a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in N$ e ovviamente $(a \cdot b^{-1}) \cdot (b \cdot c^{-1}) = a \cdot c^{-1}$ per definizione di inverso. Per costruzione di $\equiv_N$ posso dunque affermare che $a \equiv_N c$.

Questo dimostra che $\equiv_N$ è una relazione di equivalenza. Siano ora $a, b, c, d \in G$ tali che $a \equiv_N b$ e $c \equiv_N d$. Per costruzione di $\equiv_N$, questo significa che $a \cdot b^{-1} \in N$ e che $c \cdot d^{-1} \in N$, ma si noti che questo equivale a richiedere che $\{a \cdot b^{-1}\} \subseteq N$ e che $\{c \cdot d^{-1}\} \subseteq N$ e dunque posso moltiplicare a destra per $\{b\}$ nella prima relazione, per $\{d\}$ nella seconda ottenendo, per l'osservazione 2.2, che $a \in Nb$ e $c \in Nd$. Ne segue in particolare che $a \cdot c \in Nb \cdot Nd$ e quindi $a \cdot c \in N(b \cdot d)$ in virtù della proposizione 2.4-(iii.b). Ma allora, per le stesse motivazioni date in precedenza, moltiplicando a destra per $\{(b \cdot d)^{-1}\}$ si ottiene che $(a \cdot c) \cdot (b \cdot d)^{-1} \in N$, cioè che $a \cdot c \equiv_N b \cdot d$ per la definizione data di $\equiv_N$. Posso affermare, in definitiva, che $\equiv_N$ è una congruenza su G e questo dimostra che Ψ è un'applicazione ben definita.

A questo punto è sufficiente mostrare che Ψ è l'applicazione inversa di Φ, in quanto la biunivocità deriva dall'esistenza di un'inversa bilatera. Sia quindi $M \lhd G$ un sottogruppo normale e si osservi che, per le definizioni date nell'enunciato e per le proprietà dell'elemento neutro, vale la relazione:

$$(\Phi \circ \Psi)(M) = N(\equiv_M) = \{\, g \in G \mid g \equiv_M 1 \,\} = \{\, g \in G \mid g \cdot 1^{-1} \in M \,\} = M$$

Sia invece $\equiv$ una congruenza su G e si consideri la congruenza $(\Psi \circ \Phi)(\equiv) = \equiv_{N(\equiv)}$ su G. Dati $a, b \in G$, per definizione di $\equiv_{N(\equiv)}$ si ha che $a \equiv_{N(\equiv)} b$ se e solo se $a \cdot b^{-1} \in N(\equiv)$. Tale condizione è equivalente a richiedere che $a \cdot b^{-1} \equiv 1$ ma allora, utilizzando il fatto che $\equiv$ è una congruenza su G, posso moltiplicare a destra per b entrambi i membri ottenendo, equivalentemente, che $a \equiv b$. Questo dimostra, per arbitrarietà nella scelta di $a, b \in G$, che le congruenze $\equiv$ e $\equiv_{N(\equiv)}$ coincidono, cioè che $(\Psi \circ \Phi)(\equiv) = \equiv$ e dunque si ha la tesi.

(ii) Si consideri l'applicazione $\phi\colon G/\equiv \to G/N$ definita da $\phi([a]) := aN$. Innanzitutto, osservo che ϕ è ben posta. Per il punto (i) appena dimostrato e per l'ipotesi che $N = N(\equiv)$, vale che $\equiv = \equiv_N$ e di conseguenza, comunque fissate due classi $[a], [b] \in G/\equiv$ tali che $[a] = [b]$, cioè tali che $a \equiv b$, si ha che $a \cdot b^{-1} \in N$. Equivalentemente, in virtù del teorema 2.1-(i), si ha che $Na = Nb$, mentre per la proposizione 2.4-(ii.b) posso affermare che $aN = bN$ e questo dimostra che ϕ è un'applicazione ben definita. Siccome il procedimento seguito consiste soltanto di doppie implicazioni logiche, lo si può ripercorrere a ritroso, ottenendo che ϕ è anche iniettiva. La suriettività di ϕ è invece un fatto ovvio per costruzione e posso dunque affermare che ϕ è biiettiva. Infine si vede facilmente che, per ogni $[a], [b] \in G/\equiv$, vale in virtù dell'ipotesi che $\equiv$ sia una congruenza su G e in virtù del fatto che, in vista del punto (i) appena dimostrato, il sottogruppo $N \lhd G$ è normale, la condizione seguente:

$$\phi([a] \cdot [b]) = \phi([a \cdot b]) = (a \cdot b)N = aN \cdot bN = \phi([a]) \cdot \phi([b])$$

Posso quindi affermare che $\phi\colon G/\equiv \to G/N$ è un isomorfismo e dunque l'asserto è dimostrato. □

Osservazione 2.19. Si noti che, nella dimostrazione del teorema 2.2-(i), il fatto che $\equiv_N$ è una relazione di equivalenza deriva unicamente dall'assunzione che $N < G$ sia un sottogruppo, mentre l'ipotesi che $N \lhd G$ sia un sottogruppo normale viene usata soltanto per dimostrare che $\equiv_N$ è una congruenza su G. Lo stesso procedimento mostra quindi che la funzione $F\colon \{\,\text{Sottogruppi di } G\,\} \to \{\,\text{Relazioni di equivalenza su } G\,\}$ definita da $F(H) := \sim_H$, dove $\sim_H$ è la relazione per la quale valga $a \sim_H b$ se $a \cdot b^{-1} \in N$, è ben definita. Trattasi inoltre di un'applicazione iniettiva. Dati infatti due sottogruppi $H, K < G$ tali che $\sim_H = \sim_K$, si ha che $g \in H$ se e solo se $g \sim_H 1$, ma questo è equivalente a richiedere che $g \sim_K 1$, cioè che $g \in K$. Dalle doppie implicazioni e dall'arbitrarietà nella scelta di $g \in H$ oppure di $g \in K$ deriva la doppia inclusione, quindi $H = K$. In definitiva, si ha il seguente diagramma di applicazioni:

$$\begin{array}{ccc} \{\,\text{Sottogruppi di } G\,\} & \xhookrightarrow{F} & \{\,\text{Relazioni di equivalenza su } G\,\} \\ \uparrow & & \uparrow \\ \{\,\text{Sottogruppi normali di } G\,\} & \xrightarrow[\Psi]{\simeq} & \{\,\text{Congruenze su } G\,\} \end{array}$$

Esempio 2.9. Sia $n \in \mathbb{N}^*$ fissato, si consideri il gruppo $(\mathbb{Z}, +, 0)$ e si osservi che la relazione di congruenza modulo n è in effetti una congruenza. Siano infatti $a, b, c, d \in \mathbb{Z}$ tali che $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Questo significa che esistono $k, h \in \mathbb{Z}$ tali che $a - b = nk$ e $c - d = nh$, ma allora vale la relazione seguente:

$$(a + c) - (b + d) = (a - b) + (c - d) = nk + nh = n(k + h)$$

Di conseguenza, si ha che $a + c \equiv b + d \pmod{n}$ e quindi posso affermare, per arbitrarietà nella scelta di $a, b, c, d \in \mathbb{Z}$, che la relazione di congruenza modulo n è effettivamente una congruenza. Si osservi ora che:

$$N(\equiv_n) = \{\, a \in \mathbb{Z} \mid a \equiv 0 \pmod{n} \,\} = \{\, nk \mid k \in \mathbb{Z} \,\} = \langle n \rangle$$

Dal teorema 2.2-(ii) segue dunque che $\mathbb{Z}_n \simeq \mathbb{Z}/\langle n \rangle$, il che è esattamente quanto si è dimostrato in maniera esplicita nell'esempio 2.6. Si noti anche che, se in particolare $n = 1$ allora, ricordando che $\mathbb{Z}$ è un gruppo ciclico con generatore 1, come si è visto nell'esempio 1.23, vale che $\langle 1 \rangle = \mathbb{Z}$ e quindi $\mathbb{Z}/\mathbb{Z} = \{\mathbb{Z}\}$ è isomorfo al gruppo banale $\{0\}$. Se invece si prende $n = 0$, allora $\langle 0 \rangle = \{0\}$ e dunque $\mathbb{Z}/\{0\} = \{\, a + \{0\} \mid a \in \mathbb{Z} \,\}$ è isomorfo a $\mathbb{Z}$.

Esempio 2.10. Sia $n \in \mathbb{N}^*$ fissato e si consideri il gruppo $(\mathbb{Z}_n, +, \bar{0})$. È un fatto noto che i sottogruppi di $\mathbb{Z}_n$ sono tutti e soli i gruppi ciclici $\langle \bar{m} \rangle$ con $m \in \mathbb{N}$ tale che $m \mid n$. Inoltre, essendo $\mathbb{Z}_n$ un gruppo abeliano, tali sottogruppi sono normali in virtù dell'osservazione 2.6 e ha dunque senso considerare i quozienti di $\mathbb{Z}_n$ rispetto a tali sottogruppi. Ora, fissato $m \in \mathbb{N}$ tale che $m \mid n$, si consideri la congruenza $\equiv_{\langle \bar{m} \rangle}$ definita nel teorema 2.2-(i). Comunque fissate due classi di equivalenza $\bar{a}, \bar{b} \in \mathbb{Z}_n$ tali che $\bar{a} \equiv_{\langle \bar{m} \rangle} \bar{b}$, per definizione di $\equiv_{\langle \bar{m} \rangle}$ si ha che $\bar{a} - \bar{b} \in \langle \bar{m} \rangle$ e questo significa che esiste $k \in \mathbb{Z}$ tale che $\bar{a} - \bar{b} = k\bar{m}$. Dall'uguaglianza delle classi di resto modulo n segue dunque che $a - b \equiv km \pmod{n}$ e in particolare, ricordando le proprietà[9] delle congruenze modulari, vale che $a - b \equiv km \pmod{m}$ perché $m \mid n$. Da questo segue immediatamente che $a \equiv b \pmod{m}$. Viceversa, se $a \equiv b \pmod{m}$, allora esiste $k \in \mathbb{Z}$ tale che $a - b = km$. In particolare, si ha che $\bar{a} - \bar{b} = k\bar{m}$ e questo equivale a richiedere che $\bar{a} - \bar{b} \in \langle \bar{m} \rangle$, cioè che $\bar{a} \equiv_{\langle \bar{m} \rangle} \bar{b}$. Questo dimostra che la congruenza $\equiv_{\langle \bar{m} \rangle}$ è essenzialmente la relazione di congruenza modulo m. Posso dunque concludere, in virtù del teorema 2.2-(ii), che $\mathbb{Z}_n/\langle \bar{m} \rangle \simeq \mathbb{Z}_m$.

2.4 Gruppi diedrali finiti

In questa sezione si daranno tre definizioni più o meno equivalenti del gruppo diedrale finito di ordine n. Qui il simbolo della barretta assumerà un significato diverso dal solito: per ogni $a \in \mathbb{Z}$ si definisce infatti $\bar{a}$ come il più piccolo $k \in \mathbb{N}$ congruo ad a modulo n, cioè si pone $\bar{a} := \min\{\, k \in \mathbb{N} \mid k \equiv a \pmod{n} \,\}$. Tale definizione formale è ben posta per[10] il principio del buon ordinamento.

Osservazione 2.20. Sia $n \in \mathbb{N}^*$ fissato e si consideri l'insieme $D_n := \{\, \sigma^i, \sigma^i\tau \mid 0 \leq i \leq n - 1 \,\}$. Sia inoltre $\cdot$ l'operazione binaria su D_n definita dalle quattro condizioni seguenti:

(i) $\sigma^i \cdot \sigma^j := \sigma^{\overline{i+j}}$

(ii) $\sigma^i \cdot \sigma^j\tau := \sigma^{\overline{i+j}}\tau$

(iii) $\sigma^i\tau \cdot \sigma^j := \sigma^{\overline{i-j}}\tau$

(iv) $\sigma^i\tau \cdot \sigma^j\tau := \sigma^{\overline{i-j}}$

Allora l'insieme D_n munito dell'operazione binaria $\cdot$ è un gruppo con elemento neutro $1 := \sigma^0$.

Dimostrazione. Innanzitutto, osservo che l'operazione binaria $\cdot$ su D_n è ben definita per costruzione e in virtù della premessa fatta prima dell'enunciato. Si osservi che, se $0 \leq a, b \leq n - 1$, allora $\overline{\bar{a} + b} = \overline{a + b}$ in quanto $\bar{a} \equiv a \pmod{n}$. Per questo motivo, infatti, il più piccolo $k \in \mathbb{N}$ tale che $k \equiv \bar{a} + b \pmod{n}$ è anche il più piccolo $h \in \mathbb{N}$ tale che $h \equiv a + b \pmod{n}$. Siano adesso $0 \leq i, j, k \leq n - 1$ indici fissati. Da quanto si è appena osservato e dalle regole di moltiplicazione date nell'enunciato (quelle effettivamente utilizzate verranno indicate a destra di volta in volta) derivano le condizioni seguenti le quali, per arbitrarietà nella scelta degli indici $0 \leq i, j, k \leq n - 1$, dimostrano che l'operazione binaria $\cdot$ su D_n è associativa:

[9] Si vedano a tal proposito gli appunti del corso AL110.

[10] Il principio del buon ordinamento afferma che, se $A \subseteq \mathbb{N}$ è un insieme non vuoto, allora A ammette minimo. Si tratta di un assioma equivalente al principio di induzione e al principio di induzione forte. Una dimostrazione di tale equivalenza è reperibile, come al solito, negli appunti del corso AL110.

1. $(\sigma^i \cdot \sigma^j) \cdot \sigma^k = \sigma^{\overline{i+j}} \cdot \sigma^k = \sigma^{\overline{i+j+k}} = \sigma^i \cdot \sigma^{\overline{j+k}} = \sigma^i \cdot (\sigma^j \cdot \sigma^k)$ (i)
2. $(\sigma^i \cdot \sigma^j) \cdot \sigma^k\tau = \sigma^{\overline{i+j}} \cdot \sigma^k\tau = \sigma^{\overline{i+j+k}}\tau = \sigma^i \cdot \sigma^{\overline{j+k}}\tau = \sigma^i \cdot (\sigma^j \cdot \sigma^k\tau)$ (i), (ii)
3. $(\sigma^i \cdot \sigma^j\tau) \cdot \sigma^k = \sigma^{\overline{i+j}}\tau \cdot \sigma^k = \sigma^{\overline{i+j-k}}\tau = \sigma^i \cdot \sigma^{\overline{j-k}}\tau = \sigma^i \cdot (\sigma^j\tau \cdot \sigma^k)$ (ii), (iii)
4. $(\sigma^i \cdot \sigma^j\tau) \cdot \sigma^k\tau = \sigma^{\overline{i+j}}\tau \cdot \sigma^k\tau = \sigma^{\overline{i+j-k}} = \sigma^i \cdot \sigma^{\overline{j-k}} = \sigma^i \cdot (\sigma^j\tau \cdot \sigma^k\tau)$ (i), (ii), (iv)
5. $(\sigma^i\tau \cdot \sigma^j) \cdot \sigma^k = \sigma^{\overline{i-j}}\tau \cdot \sigma^k = \sigma^{\overline{i-j-k}}\tau = \sigma^i\tau \cdot \sigma^{\overline{j+k}} = \sigma^i\tau \cdot (\sigma^j \cdot \sigma^k)$ (i), (iii)
6. $(\sigma^i\tau \cdot \sigma^j) \cdot \sigma^k\tau = \sigma^{\overline{i-j}}\tau \cdot \sigma^k\tau = \sigma^{\overline{i-j-k}} = \sigma^i\tau \cdot \sigma^{\overline{j+k}}\tau = \sigma^i\tau \cdot (\sigma^j \cdot \sigma^k\tau)$ (ii), (iii), (iv)
7. $(\sigma^i\tau \cdot \sigma^j\tau) \cdot \sigma^k = \sigma^{\overline{i-j}} \cdot \sigma^k = \sigma^{\overline{i-j+k}} = \sigma^i\tau \cdot \sigma^{\overline{j-k}}\tau = \sigma^i\tau \cdot (\sigma^j\tau \cdot \sigma^k)$ (i), (iii), (iv)
8. $(\sigma^i\tau \cdot \sigma^j\tau) \cdot \sigma^k\tau = \sigma^{\overline{i-j}} \cdot \sigma^k\tau = \sigma^{\overline{i-j+k}}\tau = \sigma^i\tau \cdot \sigma^{\overline{j-k}} = \sigma^i\tau \cdot (\sigma^j\tau \cdot \sigma^k\tau)$ (ii), (iii), (iv)

Per dimostrare invece che $1 := \sigma^0$ è un elemento neutro, si fissi un indice $0 \leq i \leq n-1$ e si noti che $\overline{i} = i$. Infatti, se così non fosse, cioè se esistesse $j \in \mathbb{N}$, $j < i$ tale che $j \equiv i \pmod{n}$ allora dovrebbe esistere, per definizione di congruenza modulo n, un numero $k \in \mathbb{Z}$ tale che $i - j = nk$. In tal caso, però, varrebbe che:

$$0 < i - j \leq n - j - 1 < n$$

In particolare, varrebbe che $0 < nk < n$, cioè che $0 < k < 1$ e questo contraddice il fatto che $k \in \mathbb{Z}$. Detto questo, sono giustificate le due condizioni seguenti, in virtù delle quali σ^0 è in effetti un elemento neutro:

1. $\sigma^i \cdot \sigma^0 = \sigma^i = \sigma^0 \cdot \sigma^i$ (i)
2. $\sigma^i\tau \cdot \sigma^0 = \sigma^i\tau = \sigma^0 \cdot \sigma^i\tau$ (ii), (iii)

Dimostro infine che ciascun elemento di D_n ammette un inverso. Utilizzando il fatto che $n \equiv 0 \pmod{n}$ si ricavano facilmente, per ogni $0 \leq i \leq n-1$, le due condizioni seguenti:

1. $\sigma^i \cdot \sigma^{n-i} = \sigma^0 = \sigma^{n-i} \cdot \sigma^i$ (i)
2. $\sigma^i\tau \cdot \sigma^{n-i}\tau = \sigma^0 = \sigma^{n-i}\tau \cdot \sigma^i\tau$ (iv)

Dalla discussione precedente deriva immediatamente la tesi. □

Definizione 2.12 (algebrica)**.** Il gruppo D_n con l'operazione binaria $\cdot$ definita nell'osservazione 2.20 e con elemento neutro 1 viene detto il *gruppo diedrale finito di ordine n*. Inoltre, si pone per semplicità $\sigma := \sigma^1$.

La definizione 2.12 è ben posta in virtù dell'osservazione 2.20.

Osservazione 2.21. Dalla definizione di D_n data nell'osservazione 2.20 e dalle regole di moltiplicazione (i) e (ii) segue immediatamente che, se $n \geq 2$, allora D_n è un gruppo di ordine $2n$ generato da σ e τ. Si noti inoltre che, prendendo in particolare $i := 1$ e $j := 0$ nella regola (iv), si ottiene la condizione $\sigma\tau \cdot \tau = \sigma$, in virtù della quale il gruppo D_n può essere generato anche dagli elementi τ e $\sigma\tau$.

Osservazione 2.22. Ricordando la definizione di D_n come insieme, la definizione 1.10 e prendendo $i := 0$ nella regola di moltiplicazione (iii) si ricava che, se $n \geq 2$, allora il gruppo D_n gode delle seguenti proprietà:

(i) $o(\sigma) = n$

(ii) $o(\tau) = 2$

(iii) $o(\sigma\tau) = 2$

(iv) $\tau \cdot \sigma^j = \sigma^{n-j}\tau$

Osservazione 2.23. Il gruppo D_n è commutativo se e solo se $n \leq 2$.

Dimostrazione. Chiaramente, il gruppo D_1 è commutativo per definizione di elemento neutro. Il gruppo $D_2 = \{\, 1, \sigma, \tau, \sigma\tau \,\}$, invece, è commutativo non soltanto per le proprietà dell'elemento neutro, ma anche in virtù dell'osservazione 2.22 e delle condizioni che seguono, nelle quali è cruciale che valga $-1 \equiv 1 \pmod{2}$:

1. $\sigma \cdot \tau = \sigma\tau = \tau \cdot \sigma$ (ii), (iii)

2. $\sigma \cdot \sigma\tau = \tau = \sigma\tau \cdot \sigma$ (ii), (iii)

3. $\tau \cdot \sigma\tau = \sigma = \sigma\tau \cdot \tau$ (iv)

Se invece $n \geq 3$, allora D_n non è un gruppo commutativo a causa della relazione seguente, nella quale si applica l'osservazione 2.22-(iv) e si utilizza il fatto che $n - 1 \geq 2$:

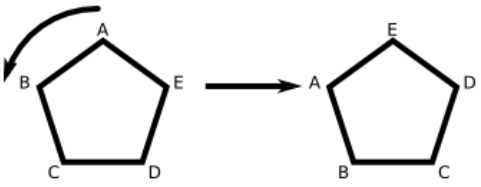
$$\sigma \cdot \tau = \sigma\tau \neq \sigma^{n-1}\tau = \tau \cdot \sigma$$ □

Definizione 2.13 (geometrica)**.** Si consideri il gruppo $\mathrm{GL}_n(\mathbb{R})$ munito dell'usuale operazione di prodotto tra matrici e con elemento neutro la matrice identità. Il seguente sottogruppo di $\mathrm{GL}_n(\mathbb{R})$ prende il nome di *gruppo diedrale finito di ordine n*:

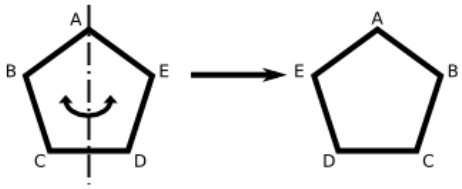
$$D_n := \langle A, B \rangle, \quad \text{dove} \quad A := \begin{pmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

La definizione 2.13 è ben posta in virtù della definizione 1.8.

Osservazione 2.24. Geometricamente, secondo la definizione 2.13 il gruppo D_n è il gruppo delle simmetrie di un poligono regolare con n lati. La matrice A, infatti, si riferisce a una rotazione di angolo $\frac{2\pi}{n}$, mentre la matrice B indica la riflessione attorno a un asse di simmetria prefissato.



Una rotazione del pentagono di $\frac{2\pi}{5} = 72°$.



Una riflessione del pentagono.

Moltiplicando le matrici A e B in tutte le maniere possibili si ottengono tutte le simmetrie del poligono regolare con n lati. Si può osservare che, per n dispari, gli assi di simmetria si trovano sulle mediane, cioè su quei segmenti che congiungono ciascun vertice del poligono al punto medio del lato opposto. Per n pari, invece, gli assi di simmetria giacciono sui segmenti che congiungono i vertici opposti del poligono.

Osservazione 2.25. Chiaramente, l'interpretazione geometrica data del gruppo D_n nell'osservazione 2.24 è significativa soltanto nel caso $n \geq 3$. In tal caso, dalla definizione 2.13 segue banalmente che il gruppo D_n definito geometricamente è un gruppo non abeliano di ordine finito generato dagli elementi B e AB, infatti si ha che $A = (AB)(B)$. Valgono inoltre le due condizioni $o(B) = 2$ e $o(AB) = 2$.

A questo punto, allo scopo di semplificare la notazione nella definizione che segue, è utile definire, per ogni $a \in \mathbb{Z}$, l'intero positivo $\bar{a}^* := \min\{\, k \in \mathbb{N}^* \mid k \equiv a \pmod{n} \,\}$. Esattamente come nel caso di $\bar{a}$ visto a inizio sezione, anche questa definizione è ben posta in virtù del principio del buon ordinamento.

Definizione 2.14 (Sottogruppo del gruppo simmetrico)**.** Sia $n \in \mathbb{N}^*$, $n \geq 3$ fissato e si considerino le due permutazioni $r, s \in S_n$ definite da $r(i) := \overline{i+1}^*$ e $s(i) := \overline{n+2-i}^*$. Il sottogruppo $\langle r, s \rangle < S_n$ prende il nome di *gruppo diedrale finito di ordine n*.

Anche la definizione 2.14 è ben posta in virtù della definizione 1.8.

Osservazione 2.26. In termini meno formali, le applicazioni $r, s \in S_n$ date nella definizione 2.14 si possono indicare con una notazione più familiare nella maniera seguente:

$$r = (1\,2\,\cdots\,n), \quad s = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$$

Osservazione 2.27. Dalla definizione 2.14 segue che il gruppo D_n definito come sottogruppo del gruppo simmetrico è un gruppo non abeliano di ordine finito generato dalle permutazioni s e $r \circ s$. Si ha infatti che $r = (r \circ s) \circ s$. Valgono inoltre le due condizioni $o(s) = 2$ e $o(r \circ s) = 2$.

Definizione 2.15 (Omomorfismo)**.** Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ due gruppi. Un'applicazione $f\colon G_1 \to G_2$ viene detta un *omomorfismo da* G_1 *a* G_2 se verifica la condizione $f(a \cdot b) = f(a) \star f(b)$ per ogni $a, b \in G_1$. Inoltre, un omomorfismo iniettivo prende il nome di *monomorfismo*, mentre un omomorfismo suriettivo si dice un *epimorfismo*.

Osservazione 2.28. Siano G_1 e G_2 gruppi. Combinando le definizioni 1.6 e 2.15 si ottiene che una funzione $f\colon G_1 \to G_2$ è un isomorfismo se e solo se è un omomorfismo biiettivo.

Osservazione 2.29. Sia $(G, \star, e)$ un gruppo e siano $a, b \in G$ elementi che soddisfano le condizioni seguenti:

(i) $a^n = e$ per un qualche $n \geq 3$.

(ii) $b^2 = e$.

(iii) $b \star a \star b^{-1} = a^{-1}$.

Se $G = \langle a, b \rangle$, allora esiste un epimorfismo da D_n a G. Inoltre, se $|G| = 2n$, allora tale epimorfismo è in realtà un isomorfismo.

Dimostrazione. Innanzitutto, si osservi che le ipotesi (i) e (ii) non implicano che $o(a) = n$ e che $o(b) = 2$, bensì che $o(a) \mid n$ e che $o(b) \mid 2$. A titolo di esempio, si può infatti considerare il caso $G := \{e\}$ e prendere $a := b := e$. Trattasi infatti di due elementi di ordine 1 che soddisfano le proprietà (i) e (ii). Si osservi ora che, elevando alla j-esima potenza primo e secondo membro della condizione (iii) si ricava, per ogni $j \in \mathbb{Z}$, la formula $b \star a^j \star b^{-1} = a^{-j}$. Da una proprietà delle potenze (osservazione 1.10) segue infatti la relazione $(a^{-1})^j = a^{-j}$ per ogni $j \in \mathbb{Z}$. La condizione $(b \star a \star b^{-1})^j = b \star a^j \star b^{-1}$ si dimostra, invece, distinguendo i casi $j > 0$, $j = 0$ e $j < 0$ e procedendo per induzione su j. Si noti adesso che, moltiplicando a destra per b primo e secondo membro della formula ottenuta, si ottiene la condizione $b \star a^j = a^{-j} \star b$ per ogni $j \in \mathbb{Z}$. Detto questo si dimostra facilmente la formula $b^k \star a^j = a^{(-1)^k j} \star b^k$, procedendo per induzione su $k \in \mathbb{N}$. Essenzialmente, dato un prodotto qualsiasi con fattori a e b, tale relazione permette di portare tutte le a a sinistra e tutte le b a destra. Tenendo a mente le ipotesi (i) e (ii) e ricordando che per ipotesi $G = \langle a, b \rangle$, dall'osservazione 1.13 e dalla discussione precedente segue che $G = \{\, a^j, a^j \star b \mid 0 \leq j \leq n-1 \,\}$. Questo dimostra, in particolare, che G è un gruppo di ordine finito e che $|G| \leq 2n$. Non è detto che $|G| = 2n$ in quanto gli elementi che compaiono nella descrizione data di G non sono a priori tutti distinti.

A questo punto, si consideri la funzione $f\colon D_n \to G$ definita da $f(\sigma^j) := a^j$ e da $f(\sigma^j\tau) := a^j \star b$ per ogni $0 \leq j \leq n-1$. Per costruzione, trattasi di un'applicazione ben definita e suriettiva. Siano ora fissati due indici $0 \leq i, j \leq n-1$ e si osservi che, per associatività dell'operazione binaria $\star$ su G, in virtù delle ipotesi (i), (ii) e (iii) e in vista della discussione precedente, valgono le seguenti condizioni (come al solito, si indicano sulla destra le regole di moltiplicazione del gruppo D_n che vengono applicate di volta in volta):

1. $f(\sigma^i \cdot \sigma^j) = f(\sigma^{\overline{i+j}}) = a^{\overline{i+j}} = a^i \star a^j = f(\sigma^i) \star f(\sigma^j)$ (i)
2. $f(\sigma^i \cdot \sigma^j\tau) = f(\sigma^{\overline{i+j}}\tau) = a^{\overline{i+j}} \star b = (a^i \star a^j) \star b = a^i \star (a^j \star b) = f(\sigma^i) \star f(\sigma^j\tau)$ (ii)
3. $f(\sigma^i\tau \cdot \sigma^j) = f(\sigma^{\overline{i-j}}\tau) = a^{\overline{i-j}} \star b = (a^i \star a^{-j}) \star b$
   $= a^i \star (a^{-j} \star b) = a^i \star (b \star a^j) = (a^i \star b) \star a^j = f(\sigma^i\tau) \star f(\sigma^j)$ (iii)
4. $f(\sigma^i\tau \cdot \sigma^j\tau) = f(\sigma^{\overline{i-j}}) = a^{\overline{i-j}} = a^i \star a^{-j} = (a^i \star a^{-j}) \star b^2$
   $= a^i \star (a^{-j} \star b) \star b = a^i \star (b \star a^j) \star b = (a^i \star b) \star (a^j \star b) = f(\sigma^i\tau) \star f(\sigma^j\tau)$ (iv)

Tali relazioni mi permettono di affermare che $f\colon D_n \to G$ è un epimorfismo. Se inoltre si ha che $|G| = 2n$ come richiesto nella parte finale dell'enunciato, allora f è un isomorfismo in quanto applicazioni suriettive tra insiemi finiti della stessa cardinalità sono biiettive. □

Osservazione 2.30. Sia $(G, \star, e)$ un gruppo non abeliano di ordine finito generato da due elementi distinti di ordine 2. Allora G è isomorfo a un gruppo diedrale finito.

Dimostrazione. Per ipotesi esistono elementi $x, y \in G$, $x \neq y$ tali che $o(x) = o(y) = 2$ e $G = \langle x, y \rangle$. Poiché per ipotesi G è un gruppo non abeliano e siccome $G = \langle x, y \rangle$, si ha che $x \star y \neq y \star x$. Inoltre, essendo per ipotesi G un gruppo di ordine finito, il prodotto $x \star y$ deve essere un elemento di ordine finito, altrimenti il gruppo ciclico $\langle x \star y \rangle$ sarebbe un sottogruppo di G di ordine infinito, il che è assurdo. Ha dunque senso

definire $n := o(x \star y)$. Siano inoltre $a := x \star y$, $b := y$ e si osservi che $G = \langle a, b \rangle$ poiché, essendo $o(y) = 2$ ed essendo $b = y$, posso ottenere il vecchio generatore x dal prodotto $a \star b = (x \star y) \star y$. Adesso dimostro che $b \notin \langle a \rangle$. Per assurdo, se fosse $b \in \langle a \rangle$, allora esisterebbe $k \in \mathbb{Z}$ tale che $(x \star y)^k = y$ e di conseguenza, moltiplicando a destra per y entrambi i membri di tale relazione e usando il fatto che $o(y) = 2$, si ottiene la condizione $(x \star y)^{k-1} \star x = e$. Per una proprietà delle potenze (osservazione 1.10) e per l'assunzione che $(x \star y)^k = y$, si ha una contraddizione con il fatto che $x \star y \neq y \star x$, come mostra la condizione seguente:

$$y \star x = (x \star y)^k \star x = (x \star y) \star (x \star y)^{k-1} \star x = (x \star y) \star e = x \star y$$

A questo punto, ricordando che $o(a) = n$ e che per ipotesi G è un gruppo di ordine finito, posso applicare il teorema di Cauchy (corollario 2.2), in virtù del quale n divide $|G|$. Ma allora, essendo $|\langle a \rangle| = n$ in virtù della proposizione 1.5, dato che $|a| \subseteq G$ e siccome $b \notin \langle a \rangle$ per la discussione precedente, posso affermare che $|G| > n$ e quindi $|G| \geq 2n$ perché n divide $|G|$.

Si osservi ora che $n \geq 3$. Infatti, se fosse $n \leq 2$, allora $a^2 = e$, vale a dire $(x \star y)^2 = e$ e di conseguenza, moltiplicando a sinistra per $(y \star x)$ ambo i membri di tale relazione e usando il fatto che $o(x) = o(y) = 2$, si contraddice la condizione $x \star y \neq y \star x$, come mostra la relazione seguente:

$$y \star x = (y \star x) \star e = (y \star x) \star (x \star y)^2 = y \star (x \star x) \star y \star x \star y = (y \star y) \star x \star y = x \star y$$

Infine, utilizzando ancora il fatto che $o(x) = o(y) = 2$, si deduce in particolare che $x^{-1} = x$ e che $y^{-1} = y$. Ma allora, applicando la proposizione 1.1-(iii), si ottiene la condizione seguente:

$$b \star a \star b^{-1} = y \star (x \star y) \star y^{-1} = y \star x = y^{-1} \star x^{-1} = (x \star y)^{-1} = a^{-1}$$

Sono dunque soddisfatte tutte le ipotesi dell'osservazione 2.29, in virtù della quale esiste un epimorfismo $f \colon D_n \to G$. Essendo in particolare f una mappa suriettiva ed essendo $|D_n| = 2n$ per l'osservazione 2.21, dovrà necessariamente valere che $|G| \leq 2n$. Dalla discussione precedente si deduce quindi che $|G| = 2n$ e posso dunque concludere, sempre in virtù dell'osservazione 2.29, che $f \colon D_n \to G$ è un isomorfismo. □

Osservazione 2.31. Combinando le osservazioni 2.25, 2.27 e 2.30 si ottiene che, nel caso $n \geq 3$, i gruppi diedrali dati nelle definizioni 2.13 e 2.14 sono isomorfi al gruppo diedrale assegnato nella definizione 2.12. Si può dunque concludere che le definizioni 2.12, 2.13 e 2.14, per $n \geq 3$, sono tutte equivalenti a meno di isomorfismo. A questo punto, è naturale chiedersi che cosa si possa dire nel caso $n \leq 2$. Chiaramente, la definizione 2.14 non si applica al caso $n \leq 2$, ma è possibile dimostrare che le definizioni 2.12 e 2.13 sono ancora equivalenti. Sussistono infatti le due osservazioni seguenti.

Osservazione 2.32. Sia $(G, \star, e)$ un gruppo abeliano generato da due elementi distinti di ordine 2 e sia $+$ l'operazione additiva su $\mathbb{Z}_2$ data nell'esempio 1.3. Allora G è isomorfo al gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ con operazione di somma $+$ data da $(\bar{a}, \bar{b}) + (\bar{c}, \bar{d}) := (\bar{a} + \bar{c}, \bar{b} + \bar{d})$ e con elemento neutro $(\bar{0}, \bar{0})$, detto il *gruppo di Klein*.

Dimostrazione. Innanzitutto, si osservi che il gruppo di Klein è in effetti un gruppo. La buona definizione e l'associatività dell'operazione binaria $+$ su $\mathbb{Z}_2 \times \mathbb{Z}_2$ assegnata nell'enunciato derivano immediatamente da quelle dell'operazione additiva $+$ su $\mathbb{Z}_2$. Similmente, la coppia $(\bar{0}, \bar{0})$ è un elemento neutro di $\mathbb{Z}_2 \times \mathbb{Z}_2$ per il semplice fatto che $\bar{0}$ è l'elemento neutro di $\mathbb{Z}_2$. Infine, anche l'esistenza dell'inverso per ogni elemento di $\mathbb{Z}_2 \times \mathbb{Z}_2$ non è che una conseguenza immediata dell'analoga proprietà di cui gode $\mathbb{Z}_2$.

Detto questo, per ipotesi esistono due elementi $x, y \in G$, $x \neq y$ tali che $o(x) = o(y) = 2$ e $G = \langle x, y \rangle$. In particolare, poiché per ipotesi G è un gruppo abeliano, si ha che $G = \{ e, x, y, x \star y \}$ e in tale descrizione gli elementi di G sono tutti distinti in virtù del fatto che $x \neq y$. Si consideri l'applicazione $f \colon G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ definita dalle relazioni $f(e) := (\bar{0}, \bar{0})$ $f(x) := (\bar{1}, \bar{0})$, $f(y) := (\bar{0}, \bar{1})$ e $f(x \star y) := (\bar{1}, \bar{1})$. È parecchio evidente che si tratti di un'applicazione ben definita e biiettiva per costruzione. È infine immediato verificare che f è un omomorfismo, dunque un isomorfismo da G a $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Osservazione 2.33. Sia $(G, \star, e)$ un gruppo ciclico di ordine 2. Allora G è isomorfo al gruppo $(\mathbb{Z}_2, +, \bar{0})$.

Dimostrazione. Per ipotesi, esiste un elemento $x \in G$ tale che $G = \langle x \rangle$. Essendo G un gruppo di ordine 2, è chiaro che $G = \{ e, x \}$, ma allora la tesi segue banalmente considerando l'applicazione $f \colon G \to \mathbb{Z}_2$ data dalle due condizioni $f(e) := \bar{0}$ e $f(x) := \bar{1}$. Si tratta infatti di un'applicazione ben definita e biiettiva per costruzione e si vede assai facilmente che è anche un omomorfismo, quindi un isomorfismo da G a $\mathbb{Z}_2$. □

Osservazione 2.34. È immediato verificare che i gruppi diedrali D_1 e D_2 sono, rispettivamente, un gruppo ciclico di ordine 2 e un gruppo abeliano generato da due elementi distinti di ordine 2 e che questo è vero sia per la definizione 2.12 che per la definizione 2.13. A questo punto si può dunque concludere, in vista delle osservazioni 2.31, 2.32 e 2.33, che le definizioni 2.12 e 2.13 sono equivalenti per ogni $n \in \mathbb{N}^*$.

Si hanno infine i due risultati seguenti, le cui dimostrazioni[11] non verranno tuttavia trattate.

Osservazione 2.35. Sia $n \in \mathbb{N}$, $n \geq 2$ fissato. Allora ogni sottogruppo di D_n è di una delle seguenti forme:

(i) $\langle \sigma^m \rangle$, dove $m \mid n$, di indice $2m$ in D_n.

(ii) $\langle \sigma^m, \sigma^r \tau \rangle$, dove $m \mid n$ e $0 \leq r \leq m-1$, di indice m in D_n.

Inoltre, i sottogruppi del primo tipo sono isomorfi a $\mathbb{Z}_{\frac{n}{m}}$, quelli del secondo tipo sono invece isomorfi a $D_{\frac{n}{m}}$.

Osservazione 2.36. Sia $n \in \mathbb{N}$, $n \geq 2$ fissato. Allora ogni sottogruppo di D_n della forma $\langle \sigma^m \rangle$ con $m \mid n$, di indice $2m$ in D_n, è normale in D_n. Inoltre, se n è dispari, questi sono tutti e soli i sottogruppi normali non banali di D_n. Se invece n è pari, allora $\langle \sigma^2, \tau \rangle$ e $\langle \sigma^2, \sigma\tau \rangle$ sono gli unici sottogruppi normali aggiuntivi, ciascuno di indice 2 in D_n. Infine, il gruppo quoziente $D_n/\langle \sigma^m \rangle$ è isomorfo a D_m e, nel caso in cui n è pari, i gruppi quoziente $D_n/\langle \sigma^2, \tau \rangle$ e $D_n/\langle \sigma^2, \sigma\tau \rangle$ sono isomorfi a $\mathbb{Z}_2$.

2.5 Gruppo dei quaternioni

Un *quaternione* è un oggetto formale del tipo $a + bi + cj + dk$, dove $a, b, c, d \in \mathbb{R}$ e i, j, k sono simboli che si comportano come l'unità immaginaria dei numeri complessi.

Osservazione 2.37. Si considerino l'insieme $Q := \{ e, \bar{e}, i, \bar{i}, j, \bar{j}, k, \bar{k} \}$ e l'operazione binaria $\cdot$ su Q definita dalla seguente tabella di moltiplicazione:

$\cdot$	$\boldsymbol{e}$	$\boldsymbol{\bar{e}}$	$\boldsymbol{i}$	$\boldsymbol{\bar{i}}$	$\boldsymbol{j}$	$\boldsymbol{\bar{j}}$	$\boldsymbol{k}$	$\boldsymbol{\bar{k}}$
$\boldsymbol{e}$	e	$\bar{e}$	i	$\bar{i}$	j	$\bar{j}$	k	$\bar{k}$
$\boldsymbol{\bar{e}}$	$\bar{e}$	e	$\bar{i}$	i	$\bar{j}$	j	$\bar{k}$	k
$\boldsymbol{i}$	i	$\bar{i}$	$\bar{e}$	e	k	$\bar{k}$	$\bar{j}$	j
$\boldsymbol{\bar{i}}$	$\bar{i}$	i	e	$\bar{e}$	$\bar{k}$	k	j	$\bar{j}$
$\boldsymbol{j}$	j	$\bar{j}$	$\bar{k}$	k	$\bar{e}$	e	i	$\bar{i}$
$\boldsymbol{\bar{j}}$	$\bar{j}$	j	k	$\bar{k}$	e	$\bar{e}$	$\bar{i}$	i
$\boldsymbol{k}$	k	$\bar{k}$	j	$\bar{j}$	$\bar{i}$	i	$\bar{e}$	e
$\boldsymbol{\bar{k}}$	$\bar{k}$	k	$\bar{j}$	j	i	$\bar{i}$	e	$\bar{e}$

Allora l'insieme Q munito dell'operazione binaria $\cdot$ è un gruppo non abeliano con elemento neutro e.

Dimostrazione. Innanzitutto, è chiaro per costruzione che l'operazione binaria $\cdot$ su Q sia ben definita. La dimostrazione del fatto che $\cdot$ gode della proprietà associativa verrà lasciata, dal momento che consiste in una semplice ma dispendiosa verifica di ben 512 relazioni. Detto questo, è immediato verificare che e è un elemento neutro e che ciascun elemento ammette un inverso. Si osservi infatti che la prima riga e la prima colonna della tabella di moltiplicazione non alterano l'ordine prestabilito degli elementi del gruppo e che in ogni riga e in ogni colonna della tabella compare l'elemento neutro e. □

Definizione 2.16. Il gruppo Q con l'operazione binaria $\cdot$ definita nell'osservazione 2.37 e con elemento neutro e prende il nome di *gruppo dei quaternioni*.

Osservazione 2.38. Il gruppo dei quaternioni gode di diverse proprietà interessanti, per le quali non verrà tuttavia esibita una dimostrazione:

(i) $Z(Q) = \{e, \bar{e}\}$.

[11] Tali dimostrazioni e altre utili informazioni sui gruppi diedrali sono reperibili sul seguente sito web: https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral2.pdf

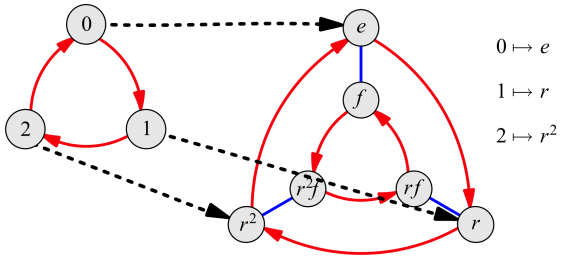
(ii) $Q/Z(Q) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

(iii) I sottogruppi non banali di Q sono $Z(Q)$, $\{e, \bar{e}, i, \bar{i}\}$, $\{e, \bar{e}, j, \bar{j}\}$, $\{e, \bar{e}, k, \bar{k}\}$.

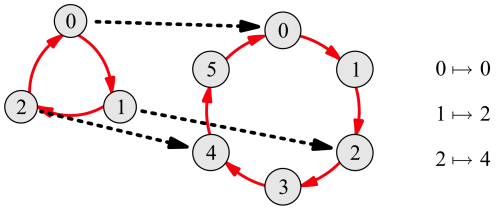
(iv) Tutti i sottogruppi di Q sono sottogruppi normali.

3 Omomorfismi

Si ricordi la definizione 2.15 assieme all'osservazione 2.28. In questa sezione si studieranno nello specifico le proprietà degli omomorfismi tra gruppi.



Nel diagramma, le frecce nere tratteggiate rappresentano un omomorfismo dal gruppo ciclico $(\mathbb{Z}_3, +, \bar{0})$ al gruppo simmetrico S_3. In questo caso particolare si ha un monomorfismo, vale a dire un omomorfismo iniettivo, ma non un epimorfismo, in quanto alcuni elementi di S_3 non vengono raggiunti da nessuna freccia. Si osservi che la stessa applicazione è tuttavia un isomorfismo tra $(\mathbb{Z}_3, +, \bar{0})$ e il sottogruppo $\langle r \rangle < S_3$.



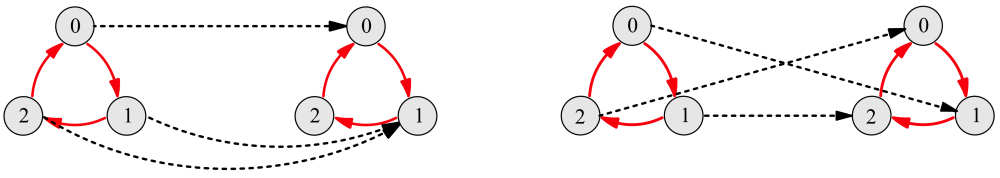
Esattamente come nella figura precedente, anche questo diagramma rappresenta un omomorfismo di gruppi. Più precisamente, si ha un omomorfismo da $(\mathbb{Z}_3, +, \bar{0})$ a $(\mathbb{Z}_6, +, \bar{0})$. Anche stavolta si tratta di un monomorfismo e non di un epimorfismo e si può osservare che la stessa mappa è un isomorfismo tra $(\mathbb{Z}_3, +, \bar{0})$ e il sottogruppo $\langle \bar{2} \rangle < \mathbb{Z}_6$.

Esempio 3.1. Chiaramente, non tutte le applicazioni tra gruppi sono omomorfismi, come mostrano i due seguenti controesempi. Si consideri il gruppo $\mathbb{Z}_3$ con l'usuale operazione additiva $+$ e con elemento neutro $\bar{0}$. L'applicazione $f\colon \mathbb{Z}_3 \to \mathbb{Z}_3$ definita da $f(\bar{0}) := \bar{0}$, $f(\bar{1}) := \bar{1}$, $f(\bar{2}) := \bar{1}$ non è un omomorfismo, infatti:

$$f(\bar{1} + \bar{1}) = f(\bar{2}) = \bar{1} \neq \bar{2} = \bar{1} + \bar{1} = f(\bar{1}) + f(\bar{1})$$

Anche la funzione $g\colon \mathbb{Z}_3 \to \mathbb{Z}_3$ definita da $g(\bar{0}) := \bar{1}$, $g(\bar{1}) := \bar{2}$, $g(\bar{2}) := \bar{0}$ non è un omomorfismo, infatti:

$$g(\bar{0} + \bar{0}) = g(\bar{0}) = \bar{1} \neq \bar{2} = \bar{1} + \bar{1} = g(\bar{0}) + g(\bar{0})$$



Si osservi adesso che l'applicazione g definita nell'esempio 3.1 non è un omomorfismo anche perché non soddisfa la condizione necessaria espressa dall'osservazione che segue.

Osservazione 3.1. Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ gruppi, $f\colon G_1 \to G_2$ un omomorfismo. Allora $f(e_1) = e_2$.

Dimostrazione. Applicando la definizione 2.15 con $a := b := e_1$ e usando il fatto che e_1 è l'elemento neutro di G_1, si ricava facilmente la condizione $f(e_1) \star f(e_1) = f(e_1)$. Utilizzando invece l'ipotesi che G_2 sia un gruppo, l'elemento $f(e_1)$ ammette un inverso e quindi, moltiplicando a destra per $f(e_1)^{-1}$ ambo i membri della relazione precedente, si può concludere che $f(e_1) = e_2$. □

L'osservazione 1.7 si generalizza immediatamente al caso degli omomorfismi nell'enunciato che segue. L'ipotesi di applicazione biunivoca non venne infatti utilizzata nel corso della dimostrazione.

Osservazione 3.2. Siano G_1 e G_2 due gruppi e sia $f\colon G_1 \to G_2$ un omomorfismo. Allora $f(g)^{-1} = f(g^{-1})$ per ogni scelta di un elemento $g \in G_1$.

Osservazione 3.3. Siano G_1, G_2 e G_3 tre gruppi e siano $f\colon G_1 \to G_2$ e $g\colon G_2 \to G_3$ due omomorfismi tali che $\operatorname{Im} f \subseteq G_2$. Si verifica facilmente che anche l'applicazione $g \circ f\colon G_1 \to G_3$ è un omomorfismo.

Vale un risultato analogo all'osservazione 1.16.

Osservazione 3.4. Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ due gruppi, $f\colon G_1 \to G_2$ un omomorfismo e si considerino $a_1, \dots, a_n \in G_1$. Dalla definizione 2.15 segue immediatamente, per induzione sul numero n degli elementi considerati, che si ha la condizione $f(a_1 \cdots a_n) = f(a_1) \star \cdots \star f(a_n)$.

Esempio 3.2. Sia $(G, \cdot, e)$ un gruppo e si consideri $\mathbb{Z}$ con l'usuale operazione di somma $+$ e con elemento neutro 0. Allora, per ogni $a \in G$, l'applicazione $\eta_a\colon \mathbb{Z} \to G$ definita da $\eta_a(n) := a^n$ è un omomorfismo per una proprietà delle potenze (osservazione 1.10).

Esempio 3.3. Sia M un gruppo. Per ogni $a \in M$, sia $\rho_L(a)\colon M \to M$ la moltiplicazione a sinistra per a, cioè l'applicazione definita da $\rho_L(a)(x) := a \cdot x$. Dalla dimostrazione del teorema di Cayley (teorema 1.1) segue immediatamente che la seguente applicazione è un monomorfismo:

$$\begin{aligned} \rho_L\colon M &\longrightarrow A(M) \\ a &\longmapsto \rho_L(a) \end{aligned}$$

Esempio 3.4. Sia G un gruppo e sia $H < G$ un sottogruppo. La mappa $i\colon H \to G$ definita da $i(x) := x$ è banalmente un monomorfismo e prende il nome di *inclusione*.

Esempio 3.5. Sia G un gruppo e sia $N \lhd G$ un sottogruppo normale. La mappa $q\colon G \to G/N$ definita da $q(x) := xN$ è un epimorfismo e prende il nome di *quoziente*. Essa, infatti, è per costruzione suriettiva ed è un omomorfismo in virtù della proposizione 2.4-(iii.b).

Esempio 3.6. Sia $n \in \mathbb{N}^*$ fissato e si considerino i due gruppi $\mathbb{Z}$ e $\mathbb{Z}_n$ con le rispettive operazioni additive e con elementi neutri 0 e $\bar{0}$ rispettivamente.

3.1 Nucleo e immagine

Definizione 3.1. Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ due gruppi e sia $f\colon G_1 \to G_2$ un omomorfismo.

(i) L'insieme $\operatorname{Im} f := \{\, f(a) \mid a \in G_1 \,\}$ prende il nome di *immagine di* f.

(ii) L'insieme $\operatorname{Ker} f := \{\, a \in G_1 \mid f(a) = e_2 \,\}$ viene detto il *nucleo* (o *kernel*) *di* f.

Proposizione 3.1. *Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ gruppi, $f\colon G_1 \to G_2$ un omomorfismo. Allora vale che:*

(i) $\operatorname{Im} f < G_2$ *è un sottogruppo e inoltre* $\operatorname{Im} f = G_2$ *se e solo se* f *è un epimorfismo.*

(ii) $\operatorname{Ker} f \lhd G_1$ *è un sottogruppo normale e inoltre* $\operatorname{Ker} f = \{e_1\}$ *se e solo se* f *è un monomorfismo.*

Dimostrazione.

(i) Innanzitutto, osservo che $\operatorname{Im} f \subseteq G_2$ è un sottoinsieme chiuso rispetto all'operazione binaria $\star$ su G_2. Siano infatti $a_2, b_2 \in \operatorname{Im} f$. Per definizione di immagine, esistono due elementi $a_1, b_1 \in G_1$ tali che $f(a_1) = a_2$ e $f(b_1) = b_2$. Dalla definizione di omomorfismo segue quindi la relazione seguente:

$$a_2 \star b_2 = f(a_1) \star f(b_1) = f(a_1 \cdot b_1)$$

Questo dimostra, come si è detto, che $\operatorname{Im} f \subseteq G_2$ è un sottoinsieme chiuso rispetto all'operazione binaria $\star$ su G_2. Si noti ora che $e_2 \in \operatorname{Im} f$ in virtù dell'osservazione 3.1. Sia infine $g_2 \in \operatorname{Im} f$. Per definizione di immagine, esiste un elemento $g_1 \in G_1$ tale che $f(g_1) = g_2$, ma allora $g_2^{-1} = f(g_1^{-1})$ in virtù dell'osservazione 3.2 e quindi $g_2^{-1} \in \operatorname{Im} f$. Questo mostra che $\operatorname{Im} f < G_2$ è un sottogruppo.

La parte successiva deriva immediatamente dalle definizioni di epimorfismo (definizione 2.15) e di applicazione suriettiva.

(ii) Dimostro che $\operatorname{Ker} f < G_1$ è un sottogruppo. Innanzitutto, è necessario mostrare che esso è chiuso rispetto all'operazione binaria $\cdot$ su G_1. Siano dunque $a_1, b_1 \in \operatorname{Ker} f$. Per la definizione 2.15 e per definizione di nucleo, si ha la condizione seguente:

$$f(a_1 \cdot b_1) = f(a_1) \star f(b_1) = e_2 \star e_2 = e_2$$

Ne segue che $a_1 \cdot b_1 \in \operatorname{Ker} f$ e questo dimostra che $\operatorname{Ker} f \subseteq G_1$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su G_1. Si osservi ora che $e_1 \in \operatorname{Ker} f$ per l'osservazione 3.1. Si fissi infine un elemento $g_1 \in \operatorname{Ker} f$ e si noti che, in virtù della definizione 3.1-(ii) e dell'osservazione 3.2, si ha che:

$$f(g_1^{-1}) = f(g_1)^{-1} = e_2^{-1} = e_2$$

Posso dunque affermare che $\operatorname{Ker} f < G_1$ è un sottogruppo. Sia adesso $a_1 \in G_1$ un elemento fissato e sia $x_1 \in a_1(\operatorname{Ker} f)a_1^{-1}$. Ricordando la definizione 2.4, deve esistere un elemento $b_1 \in \operatorname{Ker} f$ per il quale valga la condizione $x_1 = a_1 \cdot b_1 \cdot a_1^{-1}$ e di conseguenza, per la definizione di nucleo e in virtù delle osservazioni 3.2 e 3.4, si ottiene la relazione seguente:

$$f(x_1) = f(a_1 \cdot b_1 \cdot a_1^{-1}) = f(a_1) \star f(b_1) \star f(a_1^{-1}) = f(a_1) \star f(a_1)^{-1} = e_2$$

Ne segue che $x_1 \in \operatorname{Ker} f$ e quindi, non dipendendo il risultato ottenuto da una particolare scelta di $x_1 \in a_1(\operatorname{Ker} f)a_1^{-1}$, posso affermare che $a_1(\operatorname{Ker} f)a_1^{-1} \subseteq \operatorname{Ker} f$. Dall'arbitrarietà con cui si è scelto l'elemento $a_1 \in G_1$ e dalla definizione 2.5 segue dunque che $\operatorname{Ker} f \lhd G_1$ è un sottogruppo normale.

A questo punto, se f è un monomorfismo allora, fissato $a_1 \in \operatorname{Ker} f$, vale che $f(a_1) = f(e_1)$ in virtù dell'osservazione 3.1. Dall'ipotesi che f sia un'applicazione iniettiva segue dunque che $a_1 = e_1$ e questo dimostra che $\operatorname{Ker} f = \{e_1\}$. Si assuma adesso che $\operatorname{Ker} f = \{e_1\}$ e siano $a_1, b_1 \in G_1$ elementi fissati tali che $f(a_1) = f(b_1)$. Moltiplicando a destra per $f(b_1^{-1})$ ambo i membri di tale relazione, utilizzando l'ipotesi che f sia un omomorfismo e l'osservazione 3.2, si ottiene che $f(a_1 \cdot b_1^{-1}) = e_2$, cioè che $a_1 \cdot b_1^{-1} \in \operatorname{Ker} f$. Poiché si assume per ipotesi che $\operatorname{Ker} f = \{e_1\}$, deve valere la condizione $a_1 \cdot b_1^{-1} = e_1$ e dunque, moltiplicando a destra per b_1 entrambi i membri della relazione ottenuta, si ricava che $a_1 = b_1$. Questo dimostra che f è un monomorfismo e quindi si ha la tesi. □

Definizione 3.2. Siano X, Y insiemi arbitrari, $f\colon X \to Y$ un'applicazione, $y \in Y$ un elemento prefissato. L'insieme $f^{-1}(y) := \{\, x \in X \mid f(x) = y \,\}$ viene detto la *fibra di f in y*.

Osservazione 3.5. Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ due gruppi e sia $f\colon G_1 \to G_2$ un omomorfismo. Allora le fibre non vuote di f sono tutte e sole le classi laterali di G_1 rispetto a $\operatorname{Ker} f$.

Dimostrazione. Dalla definizione 3.2 segue che due elementi $a_1, b_1 \in G_1$ appartengono alla stessa fibra se e solo se $f(a_1) = f(b_1)$. Ripetendo gli stessi passaggi visti nella parte finale della dimostrazione precedente, si vede facilmente che tale condizione equivale a richiedere che $a_1 \cdot b_1^{-1} \in \operatorname{Ker} f$. Equivalentemente, per il teorema 2.1-(i), si deve avere che $(\operatorname{Ker} f)a_1 = (\operatorname{Ker} f)b_1$, vale a dire che a_1 e b_1 appartengono alla stessa classe laterale di G_1 rispetto a $\operatorname{Ker} f$. Dal momento che il procedimento seguito consiste soltanto di doppie implicazioni logiche, si ha la doppia inclusione insiemistica e dunque la tesi. □

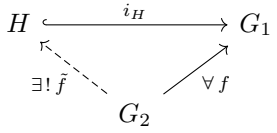
Esempio 3.7. Si osservi che, sotto le ipotesi della proposizione 3.1, non è vero in generale che $\operatorname{Im} f \lhd G_2$ sia un sottogruppo normale, come mostra il seguente controesempio. Si considerino un qualsiasi gruppo G e un suo sottogruppo $H < G$ non normale, come quelli esibiti nell'esempio 2.4 e si definiscano $G_1 := H$, $G_2 := G$ e $f := i$, dove $i\colon H \to G$ denota la mappa inclusione la quale, come si è visto nell'esempio 3.4, è un monomorfismo e quindi un omomorfismo. In questo caso, si ha per costruzione che $\operatorname{Im} i = H$, ma che $H < G$ non è un sottogruppo normale.

Proposizione 3.2 (Proprietà universali delle inclusioni e dei quozienti)**.**

(i) *Siano* $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ *gruppi, sia* $H < G_1$ *un sottogruppo e si consideri la mappa inclusione* $i_H \colon H \to G_1$. *Allora* i_H *verifica la seguente proprietà universale:*

$$\forall\, f \colon G_2 \to G_1 \text{ omomorfismo, con } \operatorname{Im} f \subseteq H \;\; \exists!\, \tilde{f} \colon G_2 \to H \text{ omomorfismo} \;\mid\; i_H \circ \tilde{f} = f$$

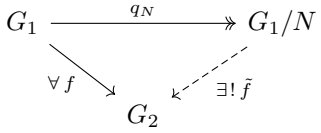
Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



(ii) *Siano* $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ *due gruppi,* $N \lhd G_1$ *un sottogruppo normale e si consideri la mappa quoziente* $q_N \colon G_1 \to G_1/N$. *Allora* q_N *verifica la seguente proprietà universale:*

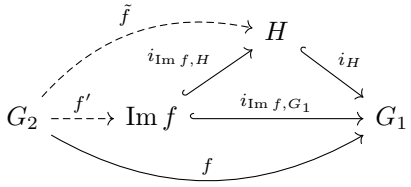
$$\forall\, f \colon G_1 \to G_2 \text{ omomorfismo, con } N \subseteq \operatorname{Ker} f \;\; \exists!\, \tilde{f} \colon G_1/N \to G_2 \text{ omomorfismo} \;\mid\; \tilde{f} \circ q_N = f$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



Dimostrazione.

(i) Sia $f \colon G_2 \to G_1$ un omomorfismo fissato con $\operatorname{Im} f \subseteq H$ e sia $f' \colon G_2 \to \operatorname{Im} f$ la funzione definita da $f'(x) := f(x)$. Si tratta di una funzione ben definita per definizione di immagine. Inoltre, poiché si assume che f sia un omomorfismo, lo è anche f' per costruzione. Si considerino adesso le mappe inclusione $i_{\operatorname{Im} f, G_1} \colon \operatorname{Im} f \to G_1$ e $i_{\operatorname{Im} f, H} \colon \operatorname{Im} f \to H$. Tali applicazioni sono ben definite in quanto $\operatorname{Im} f \subseteq G_1$ per definizione di immagine e $\operatorname{Im} f \subseteq H$ per ipotesi. Per costruzione, dunque, si ha che $f = i_{\operatorname{Im} f, G_1} \circ f'$, mentre $i_{\operatorname{Im} f, G_1} = i_H \circ i_{\operatorname{Im} f, H}$. A questo punto, si può considerare l'applicazione $\tilde{f} \colon G_2 \to H$ data semplicemente da $\tilde{f} := i_{\operatorname{Im} f, H} \circ f'$. Si tratta di una funzione ben definita in virtù della costruzione precedente e anche di un omomorfismo in quanto composizione di omomorfismi (osservazione 3.3). Inoltre, ancora dalla costruzione precedente segue banalmente che $\tilde{f}$ verifica la condizione $f = i_H \circ \tilde{f}$. Quanto discusso finora è riassunto dal seguente diagramma di applicazioni:



Si consideri ora una funzione $\bar{f} \colon G_2 \to H$, possibilmente diversa da $\tilde{f}$, tale che $i_H \circ \bar{f} = f$. Allora si ha, per ogni $x \in G_2$, la condizione che segue, dalla quale deriva immediatamente l'unicità di $\tilde{f}$:

$$\bar{f}(x) = i_H\big(\bar{f}(x)\big) = (i_H \circ \bar{f})(x) = f(x) = (i_H \circ \tilde{f})(x) = i_H\big(\tilde{f}(x)\big) = \tilde{f}(x)$$

(ii) Sia $f \colon G_1 \to G_2$ un omomorfismo fissato con $N \subseteq \operatorname{Ker} f$ e sia $\tilde{f} \colon G_1/N \to G_2$ la funzione definita dalla condizione $\tilde{f}(xN) := f(x)$. Innanzitutto, mostro che $\tilde{f}$ è un'applicazione ben definita. Siano $xN, yN \in G_1/N$ due classi laterali tali che $xN = yN$ vale a dire, in virtù del teorema 2.1-(i), tali che $x^{-1} \cdot y \in N$. Poiché si assume che $N \subseteq \operatorname{Ker} f$, vale in particolare che $x^{-1} \cdot y \in \operatorname{Ker} f$ e dunque, ancora per il teorema 2.1-(i), si può affermare che $x\operatorname{Ker} f = y\operatorname{Ker} f$. Dall'osservazione 3.5 segue quindi che $f(x) = f(y)$ e questo dimostra che $\tilde{f}$ è un'applicazione ben definita. Per costruzione, si ha che $\tilde{f} \circ q_N = f$. Siano ora $xN, yN \in G_1/N$ due classi laterali fissate. Poiché per ipotesi $N \lhd G$

è un sottogruppo normale, posso applicare la proposizione 2.4-(iii.b). In virtù di quel risultato e dell'ipotesi che $f\colon G_1 \to G_2$ sia un omomorfismo, si ottiene la condizione seguente:

$$\tilde{f}(xN \cdot yN) = \tilde{f}\big((x \cdot y)N\big) = f(x \cdot y) = f(x) \star f(y) = \tilde{f}(xN) \star \tilde{f}(yN)$$

Non dipendendo il risultato ottenuto da una particolare scelta degli elementi $xN, yN \in G_1/N$, si può affermare che l'applicazione $\tilde{f}\colon G_1/N \to G_2$ è un omomorfismo. Si consideri ora una funzione $\bar{f}\colon G_1/N \to G_2$, possibilmente diversa da $\tilde{f}$, tale che $\bar{f} \circ q_N = f$. Ricordando la definizione di q_N si ricava, per ogni $xN \in G_1/N$, la relazione seguente, dalla quale deriva l'unicità della funzione $\tilde{f}$:

$$\bar{f}(xN) = \bar{f}\big(q_N(x)\big) = (\bar{f} \circ q_N)(x) = f(x) = (\tilde{f} \circ q_N)(x) = \tilde{f}\big(q_N(x)\big) = \tilde{f}(xN) \qquad \square$$

Osservazione 3.6. Nelle proprietà universali delle inclusioni e dei quozienti, vale in realtà un risultato più forte dell'unicità. Si consideri infatti la proprietà universale delle inclusioni. Dalla dimostrazione appena terminata si evince che, se $\bar{f}\colon G_2 \to H$ è un'applicazione qualsiasi, non necessariamente un omomorfismo, tale che $i_H \circ \bar{f} = f$, allora essa coincide con l'omomorfismo $\tilde{f}$. Vale lo stesso fatto anche per la proprietà universale dei quozienti e per il risultato che segue, la cui dimostrazione fa uso delle proprietà universali appena dimostrate.

Teorema 3.1 (di fattorizzazione degli omomorfismi)**.** *Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ gruppi, si considerino un omomorfismo $f\colon G_1 \to G_2$, la mappa quoziente $q\colon G_1 \to G_1/\mathrm{Ker}\, f$, la mappa inclusione $i\colon \mathrm{Im}\, f \to G_2$. Allora esiste un unico isomorfismo $\tilde{f}\colon G_1/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ che soddisfi la condizione $i \circ \tilde{f} \circ q = f$. In altre parole, esiste una fattorizzazione unica tale che il seguente diagramma di omomorfismi sia commutativo:*

$$\begin{array}{ccc} G_1 & \xrightarrow{\forall\, f} & G_2 \\ {\scriptstyle q}\big\downarrow & & \big\uparrow{\scriptstyle i} \\ G_1/\mathrm{Ker}\, f & \underset{\exists!\, \tilde{f}}{\overset{\cong}{\dashrightarrow}} & \mathrm{Im}\, f \end{array}$$

Dimostrazione. Innanzitutto, applicando la proprietà universale dei quozienti, deduco che esiste un unico omomorfismo $\bar{f}\colon G_1/\mathrm{Ker}\, f \to G_2$ tale che $\bar{f} \circ q = f$. Si osservi ora che $\mathrm{Im}\, f = \mathrm{Im}\, \bar{f}$. Sia infatti $y \in \mathrm{Im}\, f$. Per definizione di immagine, esiste $x \in G_1$ tale che $f(x) = y$, ma allora $\bar{f}(q(x)) = y$, cioè $\bar{f}(x\mathrm{Ker}\, f) = y$ e in particolare $y \in \mathrm{Im}\, \bar{f}$. Se invece $y \in \mathrm{Im}\, \bar{f}$, allora esiste una classe laterale $x\mathrm{Ker}\, f \in G_1/\mathrm{Ker}\, f$ tale che $\bar{f}(x\mathrm{Ker}\, f) = y$. Equivalentemente, si ha che $\bar{f}(q(x)) = y$, cioè $f(x) = y$ e questo dimostra che $y \in \mathrm{Im}\, f$. A questo punto, applicando la proprietà universale delle inclusioni alla funzione $\bar{f}$ e utilizzando il fatto che $\mathrm{Im}\, f = \mathrm{Im}\, \bar{f}$, si ottiene che esiste un unico omomorfismo $\tilde{f}\colon G_1/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ tale che $i \circ \tilde{f} = \bar{f}$. Si può affermare, per costruzione, che $i \circ \tilde{f} \circ q = f$. I seguenti diagrammi riassumono la costruzione precedente:

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle q}\big\downarrow & \nearrow_{\bar{f}} & \\ G_1/\mathrm{Ker}\, f & & \end{array} \qquad \begin{array}{ccc} & & G_2 \\ & \nearrow^{\bar{f}} & \big\uparrow{\scriptstyle i} \\ G_1/\mathrm{Ker}\, f & \underset{\tilde{f}}{\dashrightarrow} & \mathrm{Im}\, f \end{array}$$

Rimane dunque da dimostrare che $\tilde{f}\colon G_1/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ è un isomorfismo. Si osservi innanzitutto che, in virtù della condizione $i \circ \tilde{f} \circ q = f$, si ha per ogni classe laterale $x\mathrm{Ker}\, f \in G_1/\mathrm{Ker}\, f$ la relazione seguente:

$$\tilde{f}(x\mathrm{Ker}\, f) = \tilde{f}(q(x)) = i\big(\tilde{f}(q(x))\big) = (i \circ \tilde{f} \circ q)(x) = f(x)$$

Sia adesso $y \in \mathrm{Im}\, f$ un elemento prefissato. Per definizione di immagine, esiste $x \in G_1$ tale che $f(x) = y$, ma questo equivale a richiedere, in vista della discussione precedente, che $\tilde{f}(x\mathrm{Ker}\, f) = y$. Si può dunque affermare che $\tilde{f}$ è un'applicazione suriettiva. Per l'iniettività, si noti invece che vale la condizione seguente:

$$\begin{aligned} \mathrm{Ker}\, \tilde{f} &= \{\, x\mathrm{Ker}\, f \in G_1/\mathrm{Ker}\, f \mid \tilde{f}(x\mathrm{Ker}\, f) = e_2 \,\} \\ &= \{\, x\mathrm{Ker}\, f \in G_1/\mathrm{Ker}\, f \mid f(x) = e_2 \,\} \\ &= \{\, x\mathrm{Ker}\, f \in G_1/\mathrm{Ker}\, f \mid x \in \mathrm{Ker}\, f \,\} = \{\, \mathrm{Ker}\, f \,\} \end{aligned}$$

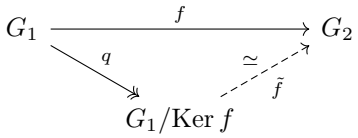
Nell'ultimo passaggio si è usato il teorema 2.1-(i), in virtù del quale $x \in \operatorname{Ker} f$ se e solo se $x\operatorname{Ker} f = \operatorname{Ker} f$. Avendo mostrato che il nucleo di $\tilde{f}$ è banale, posso affermare, per la proposizione 3.1-(ii), che $\tilde{f}$ è iniettiva. In conclusione, l'applicazione $\tilde{f}\colon G_1/\operatorname{Ker} f \to \operatorname{Im} f$ è un isomorfismo e dunque l'asserto è dimostrato. □

Una conseguenza immediata del teorema di fattorizzazione degli omomorfismi è il seguente risultato.

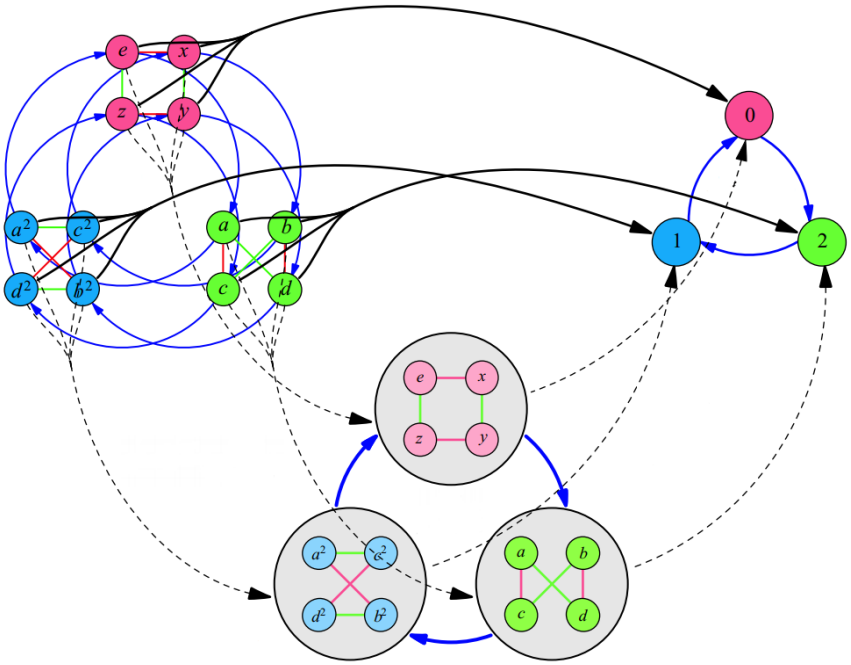
Corollario 3.1 (Primo Teorema di Isomorfismo)**.** *Siano G_1 e G_2 gruppi, $f\colon G_1 \to G_2$ un omomorfismo. Allora vale la condizione $G_1/\operatorname{Ker} f \simeq \operatorname{Im} f$.*

Le due osservazioni che seguono, invece, non sono altro che casi particolari, ma con risvolti significativi, del teorema di fattorizzazione degli omomorfismi.

Osservazione 3.7. Siano G_1 e G_2 gruppi, si considerino un epimorfismo $f\colon G_1 \to G_2$ e la mappa quoziente $q\colon G_1/\operatorname{Ker} f \to G_2$. Allora esiste un unico isomorfismo $\tilde{f}\colon G_1/\operatorname{Ker} f \to G_2$ che soddisfi $\tilde{f} \circ q = f$. In altre parole, esiste una fattorizzazione unica tale che il seguente diagramma di omomorfismi sia commutativo:

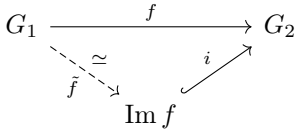


Questo significa che, a meno di identificare i gruppi G_2 e $G_1/\operatorname{Ker} f$, che sono isomorfi, l'applicazione f è essenzialmente una mappa quoziente. Dunque ogni epimorfismo è, a meno di isomorfismo, un quoziente.



Il diagramma rappresenta un esempio intuitivo di applicazione del teorema di fattorizzazione degli omomorfismi nel caso particolare in cui si fattorizzano epimorfismi.

Osservazione 3.8. Siano G_1 e G_2 gruppi, $f\colon G_1 \to G_2$ un monomorfismo e si consideri la mappa inclusione $i\colon \operatorname{Im} f \to G_2$. Allora esiste un unico isomorfismo $\tilde{f}\colon G_1 \to \operatorname{Im} f$ tale che sia soddisfatta $\tilde{f} \circ q = f$. In altre parole, esiste una fattorizzazione unica tale che il seguente diagramma di omomorfismi sia commutativo:



Questo significa che, a meno di identificare il gruppo G_1 e il sottogruppo isomorfo $\operatorname{Im} f < G_2$, la funzione f è essenzialmente una mappa inclusione, quindi ogni monomorfismo è un'inclusione a meno di isomorfismo.

Si considerino adesso un gruppo G, un suo sottogruppo $H < G$ e un suo sottogruppo normale $N \lhd G$. Ci si pone il problema di passare al quoziente rispetto a N partendo dal sottogruppo H. È ben noto ormai che, se $N \lhd H$ è un sottogruppo normale, allora non vi sono problemi, ma adesso si vuole studiare il caso più generale in cui N non è nemmeno un sottogruppo di H. Il teorema che segue propone due soluzioni equivalenti al problema: o si estrae il quoziente rispetto a N dal più piccolo sottogruppo di G contenente N e H, vale a dire $N \cdot H$, oppure si estrae il quoziente rispetto a $N \cap H$ da H. Per semplicità, si introduce inoltre la notazione $NH := N \cdot H$. Si ricordi che in questi casi $\cdot$ indica, come al solito, l'operazione binaria su $\mathcal{P}(G)\setminus\{\varnothing\}$ definita nell'osservazione 2.2.

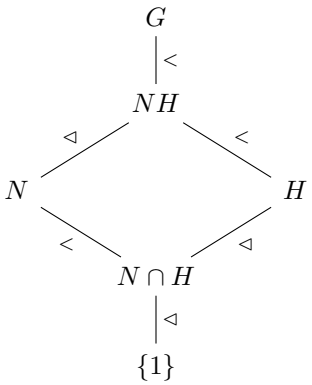
Teorema 3.2 (dei due sottogruppi, del diamante o Secondo Teorema di Isomorfismo)**.** *Sia G un gruppo, sia $H < G$ un sottogruppo e sia $N \lhd G$ un sottogruppo normale. Allora valgono le seguenti affermazioni.*

(i) *$NH = HN$, $NH < G$ è un sottogruppo e $N \lhd NH$ è un sottogruppo normale.*

(ii) *$N \cap H \lhd H$ è un sottogruppo normale.*

(iii) *L'applicazione $\Phi\colon H/(N \cap H) \to (NH)/N$ definita da $\Phi(x(N \cap H)) := xN$ è un isomorfismo.*

In particolare, si ha la condizione $H/(N \cap H) \simeq (NH)/N$.



Il diagramma rappresenta in maniera schematica le relazioni che intercorrono tra i sottogruppi di G che vengono nominati nell'enunciato del teorema. La sua forma particolare, che ricorda quella di un diamante, giustifica uno dei molteplici nomi con cui è conosciuto il teorema.

Dimostrazione.

(i) Innanzitutto, si vede facilmente che $NH = HN$. Infatti, dal momento che per ipotesi $N \lhd G$ è un sottogruppo normale, posso applicare la proposizione 2.4-(ii.a), in virtù della quale $Nh = hN$ per ogni $h \in H$ e quindi, passando all'unione su $h \in H$, si ottiene che $NH = HN$.

Ora dimostro che $NH < G$ è un sottogruppo. Siano quindi $x_1, x_2 \in NH$. Dalla definizione di NH segue che esistono $n_1, n_2 \in N$, $h_1, h_2 \in H$ tali che $x_1 = n_1 \cdot h_1$ e $x_2 = n_2 \cdot h_2$. Adesso, poiché per ipotesi $N \lhd G$ è un sottogruppo normale, vale la proposizione 2.4-(iii.b) e di conseguenza si ha che $Nh_1 \cdot Nh_2 = N(h_1 \cdot h_2)$. Utilizzando invece l'ipotesi che $H < G$ sia un sottogruppo e dunque, in particolare, un sottoinsieme di G chiuso rispetto all'operazione binaria $\cdot$ su G, posso affermare che $h_1 \cdot h_2 \in H$, ma allora $N(h_1 \cdot h_2) \subseteq NH$. Dal fatto che $(n_1 \cdot h_1) \cdot (n_2 \cdot h_2) \in Nh_1 \cdot Nh_2$ si deduce quindi che $x_1 \cdot x_2 \in NH$. Con questo procedimento ho dimostrato che $NH \subseteq G$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su G. È parecchio evidente che $1 \in NH$, infatti $1 = 1 \cdot 1$, $1 \in N$ e $1 \in H$ per definizione di elemento neutro e per l'ipotesi che $N, H < G$ siano sottogruppi. Sia infine $x \in NH$ un elemento fissato. Come prima, esistono $n \in N$, $h \in H$ tali che $x = n \cdot h$ ma allora, poiché per la proposizione 1.1-(iii) vale che $x^{-1} = h^{-1} \cdot n^{-1}$ e poiché si sta supponendo per ipotesi che $N, H < G$ siano due sottogruppi, si ha che $x^{-1} \in HN$. Ovviamente vale, in virtù della parte precedente, che $NH = HN$ e quindi $x^{-1} \in NH$. Quanto si è appena discusso mi permette di affermare che $NH < G$ è un sottogruppo.

Si osservi infine che $N < NH$ è banalmente un sottogruppo in virtù dell'ipotesi che $N < G$ sia un sottogruppo, per il fatto appena dimostrato che $NH < G$ sia un sottogruppo, quindi un gruppo e

per il fatto ovvio che $N \subseteq NH$. Inoltre, poiché per ipotesi $N \lhd G$ è un sottogruppo normale, vale per ogni $a \in G$ una qualsiasi delle proprietà equivalenti date nella proposizione 2.3. In particolare, una qualsiasi di tali proprietà varrà per ogni $a \in NH$ e si può dunque affermare, per definizione, che $N \lhd NH$ è un sottogruppo normale.

(ii) Si osservi che $N \cap H < H$ è banalmente un sottogruppo perché la chiusura rispetto all'operazione binaria, l'appartenenza dell'elemento neutro e degli inversi discende immediatamente dal fatto che N e H, in quanto sottogruppi di G, godono delle medesime proprietà. Sia ora $h \in H$ un elemento fissato e sia $x \in h(N \cap H)h^{-1}$. Dalla definizione di sottogruppo coniugato (definizione 2.4), segue che esiste un elemento $g \in N \cap H$ tale che $x = h \cdot g \cdot h^{-1}$. Si osservi che in particolare $g \in H$ e di conseguenza, essendo $H \subseteq G$ un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su G, posso affermare che $x \in H$. D'altra parte, vale anche che $g \in N$ e, dal momento che per ipotesi $N \lhd G$ è un sottogruppo normale, vale l'inclusione $hNh^{-1} \subseteq N$. Ho ottenuto quindi che $x \in N$ e dunque $x \in N \cap H$. Questo dimostra, per arbitrarietà nella scelta dell'elemento $x \in h(N \cap H)h^{-1}$, che si ha il contenimento $h(N \cap H)h^{-1} \subseteq N \cap H$. Poiché il risultato ottenuto non dipende da una scelta particolare dell'elemento $h \in H$ posso concludere, in virtù della definizione 2.5, che $N \cap H \lhd H$ è un sottogruppo normale.

(iii) Innanzitutto, si osservi che i gruppi quoziente $H/(N \cap H)$ e $(NH)/N$ sono ben definiti in virtù dei punti (i) e (ii) appena dimostrati. Si considerino ora la mappa inclusione $i\colon H \to NH$, la mappa quoziente $q\colon NH \to (NH)/N$ e l'applicazione $f\colon H \to (NH)/N$ data da $f := q \circ i$. Si tratta di un'applicazione ben definita per costruzione e di un omomorfismo in quanto è una composizione di omomorfismi. Per ogni $h \in H$, vale dunque per costruzione che $f(h) = hN$. Si consideri adesso una classe laterale $xN \in (NH)/N$. Per il punto (i) appena dimostrato si ha che $NH = HN$ e di conseguenza, per definizione di HN, esistono $h \in H$, $n \in N$ tali che $x = h \cdot n$. Ma allora, usando il fatto che $N \lhd NH$ è un sottogruppo normale assieme alla proposizione 2.4-(iii.b), si ottiene che:

$$xN = (h \cdot n)N = hN \cdot nN = hN \cdot N = hN = f(h)$$

Va notato che il passaggio intermedio $hN \cdot nN = hN \cdot N$ è giustificato dal teorema 2.1-(i), in virtù del quale $nN = N$ in quanto $n^{-1} \cdot 1 \in N$ essendo $N < G$ un sottogruppo. Il passaggio successivo, cioè $hN \cdot N = hN$, vale invece in virtù del fatto che $N \cdot N = N$. Per dimostrare tale condizione si utilizza soltanto l'ipotesi che $N < G$ e si procede esattamente come si è visto nella dimostrazione della proposizione 2.4. Fatta questa digressione, si osservi che la relazione $xN = f(h)$ dimostra, per arbitrarietà nella scelta della classe laterale $xN \in (NH)/N$ che f è un epimorfismo. A questo punto, si vuole determinare il nucleo di f:

$$\begin{aligned} \operatorname{Ker} f &= \{\, h \in H \mid f(h) = N \,\} \\ &= \{\, h \in H \mid hN = N \,\} \\ &= \{\, h \in H \mid h \in N \,\} = N \cap H \end{aligned}$$

Il penultimo passaggio è valido in virtù del teorema 2.1-(i), per cui vale $h \in N$ se e solo se $hN = N$. Si osservi anche che, per la proposizione 3.1-(ii), questa è una dimostrazione alternativa del fatto che $N \cap H \lhd H$ è un sottogruppo normale.

A questo punto, si consideri l'applicazione $\Phi\colon H/(N \cap H) \to (NH)/N$ assegnata nell'enunciato. Dimostro che Φ è un'applicazione ben definita. Siano infatti $x(N \cap H), y(N \cap H) \in H/(N \cap H)$ due classi laterali tali che $x(N \cap H) = y(N \cap H)$. Dal teorema 2.1-(i) segue che $x^{-1} \cdot y \in N \cap H$ ma allora, in particolare, vale che $x^{-1} \cdot y \in N$ e dunque, riapplicando il teorema 2.1-(i), si ottiene che $xN = yN$. Avendo appurato che Φ è un'applicazione ben definita, posso considerare la mappa quoziente $q'\colon H \to H/(N \cap H)$ e osservare che, per ogni $h \in H$, è verificata la relazione seguente:

$$(\Phi \circ q')(h) = \Phi\big(q'(h)\big) = \Phi\big(h(N \cap H)\big) = hN = f(h)$$

Posso dunque concludere, in virtù delle osservazioni 3.6 e 3.7, che $\Phi\colon H/(N \cap H) \to (NH)/N$ è un isomorfismo. La parte finale dell'enunciato deriva banalmente da quanto appena dimostrato. □

Teorema 3.3 (di corrispondenza)**.** *Siano $(G, \cdot, e)$, $(\bar{G}, \star, \bar{e})$ due gruppi e sia $f\colon G \to \bar{G}$ un epimorfismo. Siano inoltre $\mathcal{G} := \{$ Sottogruppi di G contenenti $\operatorname{Ker} f \,\}$, $\bar{\mathcal{G}} := \{$ Sottogruppi di $\bar{G} \,\}$. Allora f induce una*

corrispondenza biunivoca $\Phi\colon \mathcal{G} \to \bar{\mathcal{G}}$ *definita da* $\Phi(H) := f(H)$*, la cui inversa è l'applicazione* $\Psi\colon \bar{\mathcal{G}} \to \mathcal{G}$ *definita da* $\Psi(\bar{H}) := f^{-1}(\bar{H})$*. Valgono inoltre le due seguenti affermazioni.*

(a) *Siano* $H, H' \in \mathcal{G}$ *due sottogruppi e siano* $\bar{H} := f(H)$*,* $\bar{H}' := f(H')$*. Allora si ha che* $H \subseteq H'$ *se e solo se* $\bar{H} \subseteq \bar{H}'$*. Inoltre, in caso affermativo, vale anche che* $[H' : H] = [\bar{H}' : \bar{H}]$*. In altre parole, la corrispondenza biunivoca preserva le inclusioni e gli indici.*

(b) *Sia* $H \in \mathcal{G}$ *un sottogruppo e sia* $\bar{H} := f(H)$*. Allora* $H \lhd G$ *è un sottogruppo normale se e solo se* $\bar{H} \lhd \bar{G}$ *è un sottogruppo normale, cioè la corrispondenza biunivoca preserva la normalità. Adesso si assuma che tali condizioni equivalenti siano soddisfatte e si considerino le due mappe quoziente* $q\colon G \to G/H$*,* $\bar{q}\colon \bar{G} \to \bar{G}/\bar{H}$*. Allora l'applicazione* $\tilde{f}\colon G/H \to \bar{G}/\bar{H}$ *definita da* $\tilde{f}(xH) := f(x)\bar{H}$ *è l'unico isomorfismo che soddisfa la condizione* $\tilde{f} \circ q = \bar{q} \circ f$*. Equivalentemente, si ha il seguente diagramma di omomorfismi commutativo:*

$$\begin{array}{ccc} G & \xrightarrow{\forall\, f} & \bar{G} \\ {\scriptstyle q}\big\downarrow & & \big\downarrow{\scriptstyle \bar{q}} \\ G/H & \xrightarrow[\exists!\, \tilde{f}]{\simeq} & \bar{G}/\bar{H} \end{array}$$

Dimostrazione. Dimostro, innanzitutto, che Φ e Ψ sono due applicazioni ben definite. Si consideri dunque un sottogruppo $H \in \mathcal{G}$, cioè un sottogruppo $H < G$ tale che $\operatorname{Ker} f \subseteq H$. Dimostro che $f(H) \subseteq \bar{G}$ è chiuso rispetto all'operazione binaria $\star$ su $\bar{G}$. Siano quindi $\bar{h}_1, \bar{h}_2 \in f(H)$. Per definizione di immagine, esistono $h_1, h_2 \in H$ tali che $f(h_1) = \bar{h}_1$ e $f(h_2) = \bar{h}_2$ ma allora, dato che per ipotesi f è un omomorfismo, vale che:

$$\bar{h}_1 \star \bar{h}_2 = f(h_1) \star f(h_2) = f(h_1 \cdot h_2)$$

Essendo $H \subseteq G$ un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su G, dalla condizione precedente si deduce che $\bar{h}_1 \star \bar{h}_2 \in f(H)$ e questo dimostra che $f(H) \subseteq \bar{G}$ è chiuso rispetto all'operazione binaria $\star$ su $\bar{G}$. Si osservi ora che $\bar{e} \in f(H)$ perché, essendo $H < G$ un sottogruppo, vale che $e \in H$ e inoltre $f(e) = \bar{e}$ in virtù dell'osservazione 3.1. Sia infine $\bar{h} \in f(H)$. Di nuovo per definizione di immagine, esiste $h \in H$ tale che $f(h) = \bar{h}$ e quindi, in virtù dell'osservazione 3.2, si ha che $\bar{h}^{-1} = f(h^{-1})$. In particolare, si ottiene che $\bar{h}^{-1} \in f(H)$ e posso dunque affermare che $f(H) < \bar{G}$ è un sottogruppo. Equivalentemente, ho dimostrato che $\Phi(H) \in \bar{\mathcal{G}}$ e quindi, poiché il risultato ottenuto non dipende da una particolare scelta di $H \in \mathcal{G}$, posso affermare che Φ è un'applicazione ben definita. Si consideri adesso un sottogruppo $\bar{H} \in \bar{\mathcal{G}}$, vale a dire un sottogruppo $\bar{H} < \bar{G}$ e siano $h_1, h_2 \in f^{-1}(\bar{H})$ fissati. Per definizione di preimmagine, esistono $\bar{h}_1, \bar{h}_2 \in \bar{H}$ tali che $f(h_1) = \bar{h}_1$ e $f(h_2) = \bar{h}_2$ e dunque, utilizzando l'ipotesi che f sia un omomorfismo, si ottiene che:

$$f(h_1 \cdot h_2) = f(h_1) \star f(h_2) = \bar{h}_1 \star \bar{h}_2$$

Per definizione di preimmagine e per chiusura di $\bar{H}$ rispetto all'operazione binaria $\star$ su $\bar{G}$, posso affermare che $h_1 \cdot h_2 \in f^{-1}(\bar{H})$ e questo dimostra che $f^{-1}(\bar{H}) \subseteq G$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su G. È assai evidente che $e \in f^{-1}(\bar{H})$ in quanto, essendo $\bar{H} < \bar{G}$ un sottogruppo, si ha che $\bar{e} \in \bar{H}$ e inoltre $f(e) = \bar{e}$ per l'osservazione 3.1. Sia adesso $h \in f^{-1}(\bar{H})$. Dalla definizione di preimmagine segue che esiste $\bar{h} \in \bar{H}$ tale che $f(h) = \bar{h}$. In virtù dell'osservazione 3.2, si ha che $\bar{h}^{-1} = f(h^{-1})$ e quindi, usando l'ipotesi che $\bar{H} < \bar{G}$ sia un sottogruppo, posso affermare che $h^{-1} \in f^{-1}(\bar{H})$. Posso dunque concludere che $f^{-1}(\bar{H}) < G$ è un sottogruppo. Sia infine $x \in \operatorname{Ker} f$ cioè, per definizione di nucleo, un elemento di G tale che $f(x) = \bar{e}$. Dato che $\bar{H} < \bar{G}$ è un sottogruppo, si avrà in particolare che $f(x) \in \bar{H}$, ma questo implica che $x \in f^{-1}(\bar{H})$ e quindi, per arbitrarietà nella scelta di $x \in \operatorname{Ker} f$, posso concludere che $\operatorname{Ker} f \subseteq f^{-1}(\bar{H})$. Equivalentemente, ho dimostrato che $\Psi(\bar{H}) \in \mathcal{G}$ e posso dunque affermare, per arbitrarietà nella scelta del sottogruppo $\bar{H} \in \bar{\mathcal{G}}$, che anche Ψ è un'applicazione ben definita.

Adesso si vuole mostrare che Φ è una corrispondenza biunivoca. Per farlo, sarà sufficiente dimostrare che Ψ è un'inversa bilatera di Φ. Sia quindi $\bar{H} \in \bar{\mathcal{G}}$ un sottogruppo. Poiché per ipotesi f è un'applicazione suriettiva, vale la condizione $f(f^{-1}(\bar{H})) = \bar{H}$ per una proprietà nota[12] delle mappe tra insiemi. Ne segue

[12] Ci si riferisce al seguente fatto: dati due insiemi X e Y, un'applicazione $f\colon X \to Y$ è iniettiva se e solo se $f^{-1}(f(A)) = A$ per ogni sottoinsieme $A \subseteq X$, mentre è suriettiva se e solo se $f(f^{-1}(B)) = B$ per ogni sottoinsieme $B \subseteq Y$. Naturalmente, una dimostrazione è reperibile negli appunti del corso AL110.

in modo immediato che Ψ è un'inversa a destra di Φ in quanto $(\Phi \circ \Psi)(\bar{H}) = \bar{H}$ e il risultato ottenuto non dipende da una particolare scelta del sottogruppo $\bar{H} \in \bar{\mathcal{G}}$. Sia adesso $H \in \mathcal{G}$ un sottogruppo, vale a dire un sottogruppo $H < G$ tale che $\operatorname{Ker} f \subseteq H$. L'inclusione $H \subseteq f^{-1}(f(H))$ è sempre vera per le proprietà delle mappe tra insiemi. Sia dunque $x \in f^{-1}(f(H))$ un elemento fissato. Per definizione di preimmagine, si ha che $f(x) \in f(H)$. Per definizione di immagine, invece, esiste $h \in H$ tale che $f(x) = f(h)$. Ricordando ora l'osservazione 3.5, la condizione ottenuta equivale a richiedere che valga $x\operatorname{Ker} f = h\operatorname{Ker} f$. Dai fatti ovvi che $x = x \cdot 1$ e che $1 \in \operatorname{Ker} f$ segue banalmente che $x \in x\operatorname{Ker} f$. Equivalentemente, si ha che $x \in h\operatorname{Ker} f$ e a questo punto è cruciale l'aver assunto che $\operatorname{Ker} f \subseteq H$. In virtù di questo fatto si ha che $h\operatorname{Ker} f \subseteq H \cdot H$ e ovviamente $H \cdot H \subseteq H$ in quanto $H \subseteq G$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su G. In particolare, si ottiene che $x \in H$ e questo dimostra, per arbitrarietà nella scelta di $x \in f^{-1}(f(H))$, che vale l'inclusione $f^{-1}(f(H)) \subseteq H$. Come si è già osservato, l'altro contenimento è banale e di conseguenza $f^{-1}(f(H)) = H$. Da tale relazione segue immediatamente che Ψ è un'inversa a sinistra di Φ poiché vale la condizione $(\Psi \circ \Phi)(H) = H$ e il risultato ottenuto vale indipendentemente dalla scelta del sottogruppo $H \in \mathcal{G}$. La discussione precedente dimostra dunque che Φ è una corrispondenza biunivoca con inversa Ψ, come richiesto nella prima parte dell'enunciato. A questo punto, si procede con la dimostrazione delle due affermazioni (a) e (b).

(a) Si osservi innanzitutto che, se $H \subseteq H'$, allora $\bar{H} \subseteq \bar{H}'$ in quanto il passaggio all'immagine di una funzione preserva le inclusioni. Si supponga invece che $\bar{H} \subseteq \bar{H}'$. In virtù di quanto si è dimostrato nella parte precedente, passando alla preimmagine nelle condizioni $\bar{H} = f(H)$ e $\bar{H}' = f(H')$ note per ipotesi, si ottiene che $H = f^{-1}(\bar{H})$ e che $H' = f^{-1}(\bar{H}')$. Usando quindi il fatto che il passaggio alla preimmagine preserva le inclusioni, posso affermare che $H \subseteq H'$ e questo dimostra dunque che la corrispondenza biunivoca Φ preserva le inclusioni.

Assumo adesso che $H \subseteq H'$ oppure, equivalentemente, che $\bar{H} \subseteq \bar{H}'$. Per il teorema 2.1-(ii), esiste una collezione $\{a_i\} \subseteq H'$, indicizzata su un insieme I, tale che $H' = \coprod_{i \in I} a_i H$ e per definizione si ha che $|I| = [H' : H]$. Adesso, passando all'immagine e utilizzando il fatto noto che le unioni non disgiunte[13] sono rispettate, si ricava che $\bar{H}' = \bigcup_{i \in I} f(a_i H)$. A questo punto si noti che, comunque venga fissato un indice $i \in I$, per definizione di classe laterale sinistra e per l'ipotesi che f sia un omomorfismo vale la condizione seguente:

$$\begin{aligned} f(a_i H) &= \{\, f(x) \mid x \in a_i H \,\} \\ &= \{\, f(x) \mid x = a_i \cdot h\,,\, \exists\, h \in H \,\} \\ &= \{\, f(a_i \cdot h) \mid h \in H \,\} \\ &= \{\, f(a_i) \star f(h) \mid h \in H \,\} \\ &= \{\, f(a_i) \star \bar{h} \mid \bar{h} \in \bar{H} \,\} = f(a_i)\bar{H} \end{aligned} \tag{5}$$

Si ottiene dunque che $\bar{H}' = \bigcup_{i \in I} f(a_i)\bar{H}$. Adesso dimostro che in realtà l'unione è anche disgiunta. Suppongo per assurdo che esistano indici $i, j \in I$, $i \neq j$ tali che $f(a_i)\bar{H} \cap f(a_j)\bar{H} \neq \varnothing$. In virtù del teorema 2.1-(ii), le classi laterali sinistre di $\bar{H}'$ rispetto a $\bar{H}$ sono coincidenti oppure disgiunte e di conseguenza, in questo caso, si deve avere che $f(a_i)\bar{H} = f(a_j)\bar{H}$. Ma allora, per il punto (i) dello stesso teorema e in virtù dell'ipotesi che f sia un omomorfismo, si ottiene la condizione equivalente $f(a_i^{-1} \cdot a_j) \in \bar{H}$. In particolare, utilizzando il fatto che $H = f^{-1}(\bar{H})$, passando alla preimmagine si ricava che $a_i^{-1} \cdot a_j \in H$ e dunque $a_i H = a_j H$ di nuovo per il teorema 2.1-(i), contraddicendo il fatto che $a_i H \cap a_j H = \varnothing$ per indici $i, j \in I$, $i \neq j$. Questo mostra che $\bar{H}' = \coprod_{i \in I} f(a_i)\bar{H}$ e posso quindi affermare che $|I| = [\bar{H}' : \bar{H}]$. In definitiva, la corrispondenza biunivoca Φ preserva gli indici.

(b) Si assuma che $H \lhd G$ sia un sottogruppo normale e sia $\bar{g} \in \bar{G}$ un elemento prefissato. Dato che per ipotesi f è un'applicazione suriettiva, esiste un elemento $g \in G$ tale che $f(g) = \bar{g}$. Dalla normalità di $H \lhd G$ segue che $gHg^{-1} = H$, ma allora la normalità di $\bar{H} \lhd \bar{G}$ deriva dalla relazione seguente:

$$\bar{H} = f(H) = f(gHg^{-1}) = \{f(g)\} \cdot f(H) \cdot \{f(g^{-1})\} = \bar{g}\bar{H}\bar{g}^{-1}$$

[13] Questo si dimostra assai facilmente per doppia inclusione. Si noti, tuttavia, che in generale non sono rispettate le unioni disgiunte. Come controesempio, si possono considerare gli insiemi numerici $\mathbb{Z}$ e $\mathbb{Z}_2$ muniti delle usuali operazioni di somma $+$ e degli elementi neutri 0 e $\bar{0}$ rispettivamente. Si verifica facilmente che l'applicazione $f\colon \mathbb{Z} \to \mathbb{Z}_2$ definita da $f(n) := \bar{0}$ se n è pari, $f(n) := \bar{1}$ se n è dispari è un omomorfismo che non rispetta le unioni disgiunte.

Il penultimo passaggio si giustifica esattamente come si è visto nella relazione (5). Più in generale si può affermare che, se f è un omomorfismo, allora f rispetta l'operazione binaria $\cdot$ su $\mathcal{P}(G)\setminus\{\varnothing\}$.

Ora si supponga invece che $\bar{H} \lhd \bar{G}$ sia un sottogruppo normale. Sia $g \in G$ un elemento prefissato. Per la normalità di $\bar{H} \lhd \bar{G}$, definito $\bar{g} := f(g)$, si ha che $\bar{g}\bar{H}\bar{g}^{-1} \subseteq \bar{H}$ e dunque vale la condizione:

$$f(gHg^{-1}) = \{f(g)\} \cdot f(H) \cdot \{f(g^{-1})\} = \bar{g}\bar{H}\bar{g}^{-1} \subseteq \bar{H}$$

Ma allora, passando alla preimmagine e ricordando che $H = f^{-1}(\bar{H})$, si ottiene che $gHg^{-1} \subseteq H$. Non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $g \in G$, posso dunque affermare che $H \lhd G$ è un sottogruppo normale e quindi la corrispondenza biunivoca Φ preserva la normalità.

Sia adesso $\psi\colon G \to \bar{G}/\bar{H}$ la funzione data da $\psi := \bar{q} \circ f$. Per costruzione, si ha che $\psi(x) := f(x)\bar{H}$. Si noti che, in virtù dell'osservazione 3.3 e per un fatto noto di algebra che è immediato verificare, l'applicazione ψ è un epimorfismo poiché composizione di epimorfismi. Inoltre, si ha la relazione:

$$\begin{aligned}\operatorname{Ker}\psi &= \{\, x \in G \mid \psi(x) = \bar{H} \,\} \\ &= \{\, x \in G \mid f(x)\bar{H} = \bar{H} \,\} \\ &= \{\, x \in G \mid f(x) \in \bar{H} \,\} = f^{-1}(\bar{H}) = H\end{aligned}$$

Al terzo passaggio si è utilizzato, come al solito, il fatto che $f(x) \in \bar{H}$ se e solo se $f(x)\bar{H} = \bar{H}$, la cui validità deriva facilmente dal teorema 2.1-(i). Si consideri infine la funzione $\tilde{f}$ assegnata nelle ipotesi e si osservi che, comunque fissato un elemento $x \in G$, è soddisfatta la condizione seguente:

$$(\tilde{f} \circ q)(x) = \tilde{f}\big(q(x)\big) = \tilde{f}(xH) = f(x)\bar{H} = \psi(x)$$

Posso quindi affermare, in virtù dell'osservazione 3.7 e per costruzione di ψ, che $\tilde{f}\colon G/H \to \bar{G}/\bar{H}$ è l'unico omomorfismo che verifica la relazione $\tilde{f} \circ q = \bar{q} \circ f$. Per poter concludere la dimostrazione, sarà sufficiente dimostrare che $\tilde{f}$ è un'applicazione biiettiva. Comunque fissata una classe laterale sinistra $y\bar{H} \in \bar{G}/\bar{H}$, dall'ipotesi che f sia un epimorfismo e in particolare una funzione suriettiva segue che esiste un elemento $x \in G$ tale che $f(x) = y$ e quindi $\tilde{f}(xH) = y\bar{H}$. Questo dimostra, per arbitrarietà nella scelta della classe laterale $y\bar{H} \in \bar{G}/\bar{H}$, che $\tilde{f}$ è suriettiva. L'iniettività di $\tilde{f}$ deriva invece dal calcolo del nucleo, dal teorema 2.1-(i) e dalla proposizione 3.1-(ii), infatti:

$$\begin{aligned}\operatorname{Ker}\tilde{f} &= \{\, xH \in G/H \mid \tilde{f}(xH) = \bar{H} \,\} \\ &= \{\, xH \in G/H \mid f(x)\bar{H} = \bar{H} \,\} \\ &= \{\, xH \in G/H \mid f(x) \in \bar{H} \,\} \\ &= \{\, xH \in G/H \mid x \in H \,\} = \{H\}\end{aligned}$$

□

Il seguente risultato è un caso particolare del teorema di corrispondenza.

Osservazione 3.9. Siano G un gruppo, $N \lhd G$ un sottogruppo normale e si consideri la mappa quoziente $q\colon G \to G/N$. Siano inoltre $\mathcal{G} := \{\,\text{Sottogruppi di } G \text{ contenenti } N\,\}$, $\bar{\mathcal{G}} := \{\,\text{Sottogruppi di } G/N\,\}$. Allora q induce una corrispondenza biunivoca $\Phi\colon \mathcal{G} \to \bar{\mathcal{G}}$ data da $\Phi(H) := q(H)$. Inoltre, si ha che $q(H) = H/N$ per ogni $H \in \mathcal{G}$. Questo significa che i sottogruppi di G/N sono tutti e soli della forma H/N con $H \in \mathcal{G}$.

Dimostrazione. Chiaramente, la prima parte dell'enunciato non è nient'altro che un caso particolare del teorema di corrispondenza perché la mappa quoziente q è un epimorfismo. Bisogna dunque dimostrare che $q(H) = H/N$ per un fissato $H \in \mathcal{G}$, cioè per un dato sottogruppo $H < G$ tale che $N \subseteq H$. Innanzitutto, si osservi che $N < H$ è banalmente un sottogruppo in virtù dell'ipotesi che $N, H < G$ siano due sottogruppi e per l'assunzione che $N \subseteq H$. Inoltre, poiché si assume che $N \lhd G$ sia un sottogruppo normale, vale per ogni $a \in G$ una qualunque delle proprietà equivalenti date nella proposizione 2.3. Una qualunque di tali proprietà varrà, in particolare, per ogni $a \in H$ e dunque $N \lhd H$ è un sottogruppo normale per definizione. Questo dimostra che il quoziente H/N è ben definito. A questo punto basta semplicemente osservare che:

$$q(H) = \{\, q(x) \mid x \in H \,\} = \{\, xN \mid x \in H \,\} = H/N$$

□

Corollario 3.2 (Terzo Teorema di Isomorfismo)**.** *Sia G un gruppo e siano $K, H \lhd G$ sottogruppi normali tali che $K \subseteq H$. Allora $H/K \lhd G/K$ è un sottogruppo normale e $(G/K)/(H/K) \simeq G/H$.*

Dimostrazione. Si applichi l'osservazione 3.9 con $N := K$. Detti $\mathcal{G} := \{\text{ Sottogruppi di } G \text{ contenenti } K\}$, $\bar{\mathcal{G}} := \{\text{ Sottogruppi di } G/K\}$, per il risultato appena menzionato la mappa quoziente $q\colon G \to G/K$ induce una corrispondenza biunivoca $\Phi\colon \mathcal{G} \to \bar{\mathcal{G}}$ data da $\Phi(H') := q(H')$ e inoltre $q(H') = H'/K$. Dal momento che q è un epimorfismo, vale l'affermazione (b) del teorema di corrispondenza in virtù della quale, essendo per ipotesi $H \lhd G$ un sottogruppo normale, anche $H/K \lhd G/K$ è un sottogruppo normale. Per lo stesso risultato con $\bar{G} := G/K$ e con $\bar{H} := H/K$ si può infine concludere che $(G/K)/(H/K) \simeq G/H$. □

3.2 La funzione segno e il gruppo alterno

L'obiettivo di questa sezione è classificare i sottogruppi normali del gruppo simmetrico S_n. Innanzitutto, si ricordi che la caratteristica di un campo K è il più piccolo $n \in \mathbb{N}^*$ che soddisfa la condizione seguente:

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ volte}} = 0$$

La caratteristica di K si denota $\mathrm{ch}(K)$. Se invece nessun $n \in \mathbb{N}^*$ verifica tale relazione, si pone $\mathrm{ch}(K) := 0$.

Definizione 3.3. Sia K un campo con $\mathrm{ch}(K) \neq 2$, sia $\{E_1, \ldots, E_n\}$ la base canonica di K^n e sia $\sigma \in S_n$. La funzione lineare $T_\sigma\colon K^n \to K^n$ definita da $T_\sigma(E_i) := E_{\sigma(i)}$ al variare dell'indice $1 \leq i \leq n$ viene detta l'*operatore della permutazione* σ. La matrice associata a T_σ rispetto alla base canonica di K^n viene invece detta la *matrice della permutazione* σ.

La definizione 3.3 è ben posta. Infatti, l'applicazione T_σ è ben definita per definizione di base e perché si assume che essa sia lineare.

Osservazione 3.10. Si dimostra facilmente che le matrici di permutazione sono tutte e sole le matrici che hanno entrate uguali a 0 o a 1 e hanno esattamente un'entrata non nulla su ogni riga e su ogni colonna.

Esempio 3.8. Si considerino il campo $\mathbb{R}$ e la permutazione $\sigma := (1\,2\,3)$. In questo caso, l'operatore della permutazione σ è la funzione lineare $T_\sigma\colon \mathbb{R}^3 \to \mathbb{R}^3$ definita da $T_\sigma(E_1) := E_2$, $T_\sigma(E_2) := E_3$, $T_\sigma(E_3) := E_1$, dove E_1, E_2, E_3 sono i vettori della base canonica di $\mathbb{R}^3$. La matrice della permutazione σ è invece data da:

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Osservazione 3.11. Sia K un campo con $\mathrm{ch}(K) \neq 2$ e siano $\sigma, \tau \in S_n$. Allora si ha che $T_{\sigma\circ\tau} = T_\sigma \circ T_\tau$. In altre parole, gli operatori di permutazioni su n lettere rispettano l'operazione di composizione di funzioni. In particolare, vale anche la condizione $M_{\sigma\circ\tau} = M_\sigma M_\tau$.

Dimostrazione. Sia come prima $\{E_1, \ldots, E_n\}$ la base canonica di K^n e sia $1 \leq i \leq n$ un indice prefissato. Dalla definizione 3.3 deriva immediatamente la condizione seguente:

$$T_{\sigma\circ\tau}(E_i) = E_{(\sigma\circ\tau)(i)} = E_{\sigma(\tau(i))} = T_\sigma(E_{\tau(i)}) = T_\sigma\big(T_\tau(E_i)\big) = (T_\sigma \circ T_\tau)(E_i)$$

Non dipendendo il risultato ottenuto da una particolare scelta dell'indice $1 \leq i \leq n$ posso concludere, per definizione di base e per linearità, che $T_{\sigma\circ\tau} = T_\sigma \circ T_\tau$. La seconda parte dell'enunciato deriva da un fatto noto[14] di algebra lineare. □

Osservazione 3.12. Sia K un campo con $\mathrm{ch}(K) \neq 2$ e si consideri il gruppo simmetrico S_n. Una immediata conseguenza della definizione 3.3 è che l'operatore della permutazione identità è l'applicazione identità. In particolare, la matrice della permutazione identità è la matrice identità.

Osservazione 3.13. Si ricordi che[15] una matrice elementare del primo tipo è per definizione una matrice ottenuta dall'identità scambiando due colonne (oppure due righe). È noto che una matrice di questo tipo è invertibile. Si noti anche che, in virtù della definizione 3.3, la matrice di una trasposizione è una matrice

[14] Siano U, V, W spazi vettoriali su un campo K, $u = \{u_1, \ldots, u_s\}$, $v = \{v_1, \ldots, v_n\}$, $w = \{w_1, \ldots, w_m\}$ loro rispettive basi e siano $G\colon U \to V$, $F\colon V \to W$ due applicazioni lineari. Allora la matrice associata a $F \circ G$ rispetto alle basi u e w è uguale al prodotto tra la matrice associata a F rispetto alle basi v e w e la matrice associata a G rispetto alle basi u e v. Per una dimostrazione di questo risultato si vedano gli appunti del corso GE110 oppure le dispense del corso AM210.

[15] Maggiori dettagli sono reperibili negli appunti del corso GE110.

elementare del primo tipo. Si ricordi ora che ogni permutazione si può esprimere come prodotto di due o più trasposizioni e quindi, per l'osservazione 3.11, la matrice di una permutazione è uguale al prodotto di due o più matrici elementari del primo tipo. In particolare, la matrice di una permutazione è invertibile.

Osservazione 3.14. Sia K un campo con $\mathrm{ch}(K) \neq 2$ e sia $\sigma \in S_n$. Allora T_σ è invertibile e $T_\sigma^{-1} = T_{\sigma^{-1}}$. In particolare, vale anche la condizione $M_\sigma^{-1} = M_{\sigma^{-1}}$.

Dimostrazione. Dall'osservazione 3.13 e da un fatto noto di algebra lineare[16] segue immediatamente che T_σ è un'applicazione invertibile. La parte successiva dell'enunciato è invece una conseguenza immediata delle osservazioni 3.11 e 3.12. □

Osservazione 3.15. Combinando le osservazioni 3.11, 3.12 e 3.14 si ottiene che l'insieme degli operatori di permutazioni su n lettere è un sottogruppo di $\mathrm{GL}(K^n)$ e che l'insieme delle matrici di permutazioni su n lettere è un sottogruppo di $\mathrm{GL}_n(K)$. Dall'osservazione 3.11 e dalla definizione 3.3 segue inoltre che, detti $\mathcal{T} := \{\text{ Operatori di permutazioni su } n \text{ lettere }\}$, $\mathcal{M} := \{\text{ Matrici di permutazioni su } n \text{ lettere }\}$, le mappe $T\colon S_n \to \mathcal{T}$, $M\colon S_n \to \mathcal{M}$ definite da $T(\sigma) := T_\sigma$ e da $M(\sigma) := M_\sigma$ sono due isomorfismi. In particolare, si ha che $\mathcal{T} \simeq \mathcal{M}$ e si può affermare che, a meno di isomorfismo, il gruppo simmetrico S^n è un sottogruppo di $\mathrm{GL}(K^n)$ e di $\mathrm{GL}_n(K)$. Si dice che $\mathcal{T}$ e $\mathcal{M}$ sono due realizzazioni del gruppo simmetrico dentro $\mathrm{GL}(K^n)$ e dentro $\mathrm{GL}_n(K)$ rispettivamente.

Definizione 3.4. Sia K un campo con $\mathrm{ch}(K) \neq 2$ e si consideri il gruppo $\{\pm 1\}$ munito dell'operazione di prodotto usuale $\cdot$ e dell'elemento neutro 1. L'applicazione $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ definita da $\mathrm{sgn}(\sigma) := \det M_\sigma$ prende il nome di *funzione segno*.

La definizione 3.4 è ben posta. Si ricordi, infatti, che ogni matrice di permutazione M_σ è il prodotto di un certo numero k di matrici elementari del primo tipo (osservazione 3.13), ciascuna delle quali ammette[17] determinante uguale a -1 in quanto ottenuta dalla matrice identità I_n mediante uno scambio di colonne (oppure di righe). Di conseguenza, il determinante della matrice M_σ è fornito dalla condizione che segue:

$$\det M_\sigma = (-1)^k$$

Esempio 3.9. Si considerino nuovamente il campo $\mathbb{R}$ e la permutazione $\sigma := (1\,2\,3)$. Applicando la regola di Laplace per lo sviluppo del determinante, si ottiene che il segno di σ è dato dalla condizione seguente:

$$\mathrm{sgn}(\sigma) = \begin{vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{vmatrix} = 1$$

Proposizione 3.3. *Siano $n \geq 2$, K un campo con $\mathrm{ch}(K) \neq 2$, e si consideri $\{\pm 1\}$ munito dell'operazione di prodotto usuale $\cdot$ e dell'elemento neutro 1. La funzione $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ è un epimorfismo. Inoltre, si ha che $\{\pm 1\} \simeq \mathbb{Z}_2$ e dunque esiste un epimorfismo dal gruppo simmetrico S_n a $\mathbb{Z}_2$.*

Dimostrazione. La condizione seguente, valida in virtù dell'osservazione 3.11 per ogni scelta di $\sigma, \tau \in S_n$, dimostra che la funzione segno è un omomorfismo:

$$\mathrm{sgn}(\sigma \circ \tau) = \det M_{\sigma\circ\tau} = \det(M_\sigma M_\tau) = (\det M_\sigma) \cdot (\det M_\tau) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau)$$

Si osservi ora che la permutazione identità ha segno uguale a 1 per l'osservazione 3.12 e in virtù del fatto che $\det I_n = 1$. Avendo assunto $n \geq 2$, posso poi considerare la trasposizione $(1\,2)$, la quale ha segno -1 per l'osservazione 3.13, nella quale si è detto che la matrice di una trasposizione è una matrice elementare del primo tipo e in virtù del fatto che queste ultime hanno determinante uguale a -1 in quanto ottenute dalla matrice identità mediante uno scambio di colonne o di righe (leggasi la nota 17). Tali considerazioni mi permettono di concludere che la funzione $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ è un epimorfismo.

Per la seconda parte dell'enunciato, basta considerare l'applicazione $f\colon \{\pm 1\} \to \mathbb{Z}_2$ data da $f(1) := \bar{0}$ e da $f(-1) := \bar{1}$. È immediato verificare che tale applicazione è un isomorfismo. A questo punto la funzione composta $f \circ \mathrm{sgn}\colon S_n \to \mathbb{Z}_2$ è un epimorfismo. Essa infatti è un omomorfismo per l'osservazione 3.3 ed è suriettiva in quanto composizione di applicazioni suriettive. Dunque si ha la tesi. □

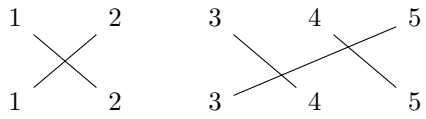
[16] Siano V uno spazio vettoriale su un campo K, $F \in \mathrm{End}(V)$ e siano $v = \{v_1, \ldots, v_n\}$, $w = \{w_1, \ldots, w_n\}$ due basi di V. Allora $F \in \mathrm{GL}(V)$ se e solo se la matrice associata a F rispetto alle basi v e w è invertibile. La dimostrazione è reperibile negli appunti del corso GE110.

[17] Sia K un campo e siano $A, B \in \mathrm{M}_n(K)$. Se la matrice B è ottenuta da A mediante uno scambio di colonne (oppure di righe), allora $\det B = -\det A$. Inoltre, il determinante della matrice identità è uguale a 1. La dimostrazione di tali proprietà fondamentali del determinante è stata già trattata nel corso GE110.

Definizione 3.5. Sia $\sigma \in S_n$. Il seguente insieme viene detto l'*insieme delle inversioni di* σ:

$$\mathrm{inv}(\sigma) := \{\, (i,j) \in \{1,\dots,n\}^2 \;\mid\; i < j \text{ e } \sigma(i) > \sigma(j) \,\}$$

Esempio 3.10. Per calcolare l'insieme delle inversioni di una permutazione può essere utile tracciare un diagramma nel quale, se $\sigma(i) = j$ per certi $i, j \in \{1,\dots,n\}$, allora si connette l'indice i nella prima riga con l'indice j nella seconda riga. Si consideri per esempio la permutazione $\sigma := (1\,2) \circ (3\,4\,5)$ in S_5. In questo caso particolare, il diagramma assume la forma seguente:



Di conseguenza, l'insieme delle inversioni di σ è dato da $\mathrm{inv}(\sigma) = \{\,(1,2),(3,5),(4,5)\,\}$. Geometricamente, esiste una corrispondenza biunivoca tra la cardinalità dell'insieme delle inversioni di una permutazione e il numero di incroci che compaiono nel diagramma.

Teorema 3.4. *Il segno di una permutazione $\sigma \in S_n$ si può calcolare nei seguenti modi equivalenti.*

(i) *Se σ si scrive come prodotto di k trasposizioni, allora* $\mathrm{sgn}(\sigma) = (-1)^k$.

(ii) *Se σ si decompone come prodotto di cicli disgiunti di lunghezze $n_1,\dots,n_s$, allora si ha la formula:*

$$\mathrm{sgn}(\sigma) = \prod_{i=1}^{s} (-1)^{n_i - 1}$$

(iii) *Vale in generale la formula* $\mathrm{sgn}(\sigma) = (-1)^{|\mathrm{inv}(\sigma)|}$.

Dimostrazione.

(i) Se σ si esprime come prodotto di k trasposizioni allora, in virtù dell'osservazione 3.13, la matrice della permutazione σ è uguale al prodotto di k matrici elementari del primo tipo. Di conseguenza, l'asserto deriva immediatamente da quanto si è discusso a seguito della definizione 3.4.

(ii) Innanzitutto dimostro che, data una permutazione costituita da un unico ciclo $(k_1 \cdots k_m)$, si ha la seguente decomposizione come prodotto di $m-1$ trasposizioni:

$$(k_1 \cdots k_m) = (k_1\ k_2) \circ (k_2\ k_3) \circ \cdots \circ (k_{m-1}\ k_m)$$

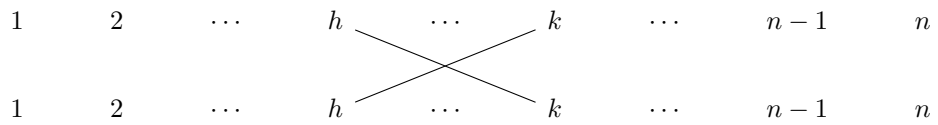
Si procede per induzione sulla lunghezza m del ciclo. La base di induzione, cioè il caso $m = 1$, è banale. Nel passo di induzione assumo $m \geq 2$, suppongo che la formula sia valida per un generico $m-1$ e la dimostro per m. Basta semplicemente osservare che vale la condizione seguente:

$$(k_1 \cdots k_m) = (k_1\ k_2) \circ (k_2 \cdots k_m) = (k_1\ k_2) \circ \big((k_2\ k_3) \circ \cdots \circ (k_{m-1}\ k_m)\big)$$

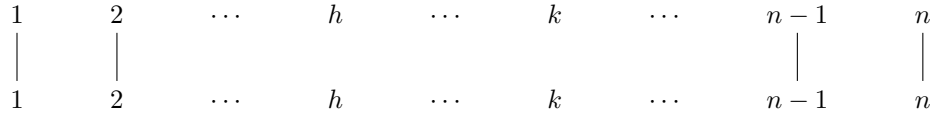
Avendo mostrato che un ciclo di lunghezza m si esprime come prodotto di $m-1$ trasposizioni e poiché per ipotesi σ si decompone come prodotto di cicli disgiunti di lunghezze $n_1,\dots,n_s$, posso affermare che questi cicli si scrivono a loro volta come prodotto di $n_1 - 1,\dots,n_s - 1$ trasposizioni. Ma allora σ si scrive come prodotto di un numero di trasposizioni uguale a $\sum_{i=1}^{s}(n_i - 1)$ e quindi, applicando il punto (i) appena dimostrato e una proprietà delle potenze (osservazione 1.10), si ha la tesi.

(iii) Sia $\widetilde{\mathrm{sgn}}\colon S_n \to \{\pm 1\}$ la mappa definita da $\widetilde{\mathrm{sgn}}(\sigma) := (-1)^{|\mathrm{inv}(\sigma)|}$ e sia $\tau = (h\ k)$ una trasposizione. Posso assumere, senza perdita di generalità, che valga $h < k$. In questo caso particolare, fissato un valore $i \in \{1,\dots,n\}$, si hanno tre possibilità: se $i \neq h$, $i \neq k$, allora $\tau(i) = i$; se invece $i = h$, allora $\tau(i) = k$; se infine $i = k$, allora $\tau(i) = h$. Siano adesso fissati $1 \leq i < j \leq n$ e si distinguano 6 casi:

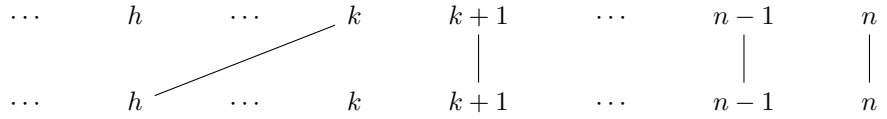
- se $i = h$, $j = k$, allora $\tau(i) = k$, $\tau(j) = h$. In particolare, vale che $\tau(i) > \tau(j)$ e quindi vale, in virtù della definizione 3.5, che $(h, k) \in \mathrm{inv}(\tau)$, come viene mostrato nel seguente diagramma:



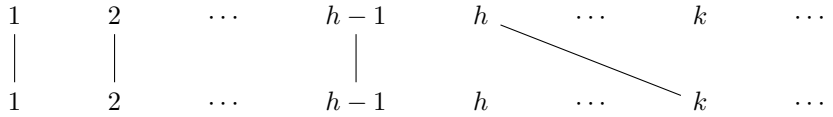
- se $i \neq h$, $j \neq k$, allora $\tau(i) = i$, $\tau(j) = j$. In particolare, si ha che $\tau(i) = \tau(j)$ e dunque, come mostrato anche nel seguente diagramma, vale che $(i, j) \notin \mathrm{inv}(\tau)$ per definizione:



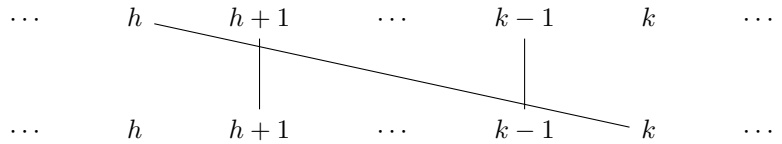
- se $i = k$, allora $j > h$ e dunque $\tau(i) = h$, $\tau(j) = j$. In particolare, si ha che $\tau(i) < \tau(j)$ e di conseguenza vale per definizione che $(i, j) \notin \mathrm{inv}(\tau)$, come fra l'altro si evince dal diagramma:



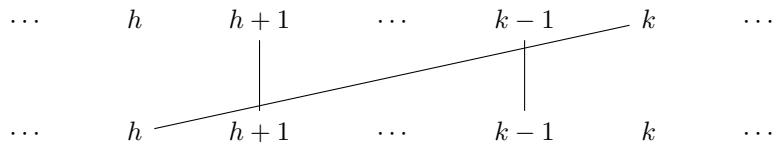
- se $j = h$, allora $i < k$ e dunque $\tau(i) = i$, $\tau(j) = k$. In particolare, si ha che $\tau(i) < \tau(j)$ e di conseguenza vale per definizione che $(i, j) \notin \mathrm{inv}(\tau)$, come si può vedere anche dal diagramma:



- se $i = h$, $j \neq k$, allora $\tau(i) = k$, $\tau(j) = j$. Dalla definizione 3.5 segue che $(i, j) \in \mathrm{inv}(\tau)$ se e solo se $i < j$ e $\tau(i) > \tau(j)$, cioè se e solo se $h < j < k$. Vi sono esattamente $k - h - 1$ scelte possibili di j che soddisfano tale condizione. Il diagramma che segue illustra intuitivamente ciò che accade in questo caso particolare:



- se $i \neq h$, $j = k$, allora $\tau(i) = i$, $\tau(j) = h$. Come prima, in virtù della definizione 3.5 si ha che $(i, j) \in \mathrm{inv}(\tau)$ se e solo se $i < j$ e $\tau(i) > \tau(j)$, cioè se e solo se $h < i < k$. Esattamente come nel caso precedente, vi sono $k - h - 1$ possibili scelte di i che verificano tale relazione. Segue un diagramma che mostra a livello intuitivo cosa accade:



Dall'analisi precedente si deduce che $|\mathrm{inv}(\tau)| = 2(k - h - 1) + 1$. Ricordando la definizione data della funzione $\widetilde{\mathrm{sgn}}$ e utilizzando il fatto che $|\mathrm{inv}(\tau)|$ è un numero dispari, posso dunque affermare che $\widetilde{\mathrm{sgn}}(\tau) = -1$. Si osservi che tale risultato non dipende dalla scelta della trasposizione $\tau \in S_n$.

Sia ora $P := \{ f \colon \mathbb{Q}^n \to \mathbb{Q} \}$. Per ogni $\sigma \in S_n$ e per ogni $f \in P$, sia $\sigma f \in P$ l'applicazione definita da $(\sigma f)(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Si tratta di una funzione ben definita per costruzione.

Si noti adesso che, per ogni $\sigma, \tau \in S_n$ e per ogni $f \in P$, vale la condizione $\sigma(\tau f) = (\tau \circ \sigma)f$. Si ha infatti, per ogni $(x_1, \dots, x_n) \in \mathbb{Q}^n$, la relazione seguente:

$$\begin{aligned}\big(\sigma(\tau f)\big)(x_1, \dots, x_n) &= (\tau f)(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_{\tau(\sigma(1))}, \dots, x_{\tau(\sigma(n))}) \\ &= f(x_{(\tau\circ\sigma)(1)}, \dots, x_{(\tau\circ\sigma)(n)}) = \big((\tau \circ \sigma)f\big)(x_1, \dots, x_n)\end{aligned}$$

A questo punto si consideri l'applicazione $p \in P$ definita da $p(x_1, \dots, x_n) := \prod_{1\le i<j\le n}(x_i - x_j)$. Noto che $\sigma p = \widetilde{\operatorname{sgn}}(\sigma)p$ per ogni scelta di una permutazione $\sigma \in S_n$. Sia infatti $(x_1, \dots, x_n) \in \mathbb{Q}^n$. Allora si ha, in virtù delle definizioni date nel corso della dimostrazione, la condizione che segue:

$$(\sigma p)(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \prod_{1\le i<j\le n}(x_{\sigma(i)} - x_{\sigma(j)})$$

Ora basta osservare che nella produttoria alla fine della relazione precedente compaiono gli stessi fattori presenti in $p(x_1, \dots, x_n)$, con la differenza che si ha una variazione di segno per ogni $i < j$ tale che $\sigma(i) > \sigma(j)$, cioè per ogni $(i, j) \in \operatorname{inv}(\sigma)$. Posso dunque affermare che si ha la condizione:

$$\prod_{1\le i<j\le n}(x_{\sigma(i)} - x_{\sigma(j)}) = (-1)^{|\operatorname{inv}(\sigma)|}\prod_{1\le i<j\le n}(x_i - x_j) = \widetilde{\operatorname{sgn}}(\sigma) \cdot p(x_1, \dots, x_n)$$

Ora dimostro che la funzione $\widetilde{\operatorname{sgn}}$ è un omomorfismo. Noto innanzitutto che, comunque assegnati un elemento $\alpha \in \mathbb{Q}$ e una permutazione $\sigma \in S_n$, vale la relazione $\sigma(\alpha p) = \alpha(\sigma p)$. Infatti, per ogni $x_1, \dots, x_n \in \mathbb{Q}$, si ha la condizione seguente:

$$\begin{aligned}\big(\sigma(\alpha p)\big)(x_1, \dots, x_n) &= (\alpha p)(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \alpha p(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \\ &= \alpha\big((\sigma p)(x_1, \dots, x_n)\big) = \big(\alpha(\sigma p)\big)(x_1, \dots, x_n)\end{aligned}$$

Siano ora $\sigma, \tau \in S_n$ due permutazioni qualsiasi e si osservi che, per le proprietà precedentemente dimostrate, vale la relazione che segue:

$$\widetilde{\operatorname{sgn}}(\sigma \circ \tau)p = (\sigma \circ \tau)p = \tau(\sigma p) = \tau\big(\widetilde{\operatorname{sgn}}(\sigma)p\big) = \widetilde{\operatorname{sgn}}(\sigma)(\tau p) = \widetilde{\operatorname{sgn}}(\sigma)\widetilde{\operatorname{sgn}}(\tau)p$$

Adesso, prendendo $x_1, \dots, x_n \in \mathbb{Q}$ a due a due distinti, dalla condizione precedente si deduce che:

$$\widetilde{\operatorname{sgn}}(\sigma \circ \tau)\prod_{1\le i<j\le n}(x_i - x_j) = \widetilde{\operatorname{sgn}}(\sigma)\widetilde{\operatorname{sgn}}(\tau)\prod_{1\le i<j\le n}(x_i - x_j)$$

Essendo diverse da 0 le quantità espresse sotto il simbolo di produttoria, posso moltiplicare per il loro inverso entrambi i membri della relazione ottenuta, ottenendo che $\widetilde{\operatorname{sgn}}(\sigma \circ \tau) = \widetilde{\operatorname{sgn}}(\sigma)\widetilde{\operatorname{sgn}}(\tau)$. Poiché il risultato ottenuto non dipende da una particolare scelta degli elementi $\sigma, \tau \in S_n$, si può concludere che l'applicazione $\widetilde{\operatorname{sgn}}$ è un omomorfismo di gruppi. A questo punto, si consideri una qualsiasi permutazione $\sigma \in S_n$. È un fatto ben noto che S_n è generato dalle sue trasposizioni, per cui esistono determinate trasposizioni $\tau_1, \dots, \tau_s \in S_n$ tali che $\sigma = \tau_1 \circ \cdots \circ \tau_s$. Ricordando infine che le applicazioni sgn e $\widetilde{\operatorname{sgn}}$ sono omomorfismi per la proposizione 3.3 e in virtù della discussione precedente, applicando l'osservazione 3.4 e utilizzando il fatto che esse assumono valore -1 sulle trasposizioni, si ottiene la relazione seguente:

$$\widetilde{\operatorname{sgn}}(\sigma) = \widetilde{\operatorname{sgn}}(\tau_1) \cdots \widetilde{\operatorname{sgn}}(\tau_s) = (-1)^k = \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_s) = \operatorname{sgn}(\sigma)$$

Questo dimostra, per arbitrarietà nella scelta della permutazione $\sigma \in S^n$, che $\widetilde{\operatorname{sgn}} = \operatorname{sgn}$ e dunque, per definizione di $\widetilde{\operatorname{sgn}}$, si ha la tesi. □

Osservazione 3.16. Siano $\sigma, (i\ j) \in S_n$. Allora vale la formula $\sigma \circ (i\ j) \circ \sigma^{-1} = (\sigma(i)\ \sigma(j))$.

Dimostrazione. Sia $1 \le k \le n$ un indice fissato. Distinguo tre possibilità, a seconda che $k = \sigma(i)$, $k = \sigma(j)$ oppure $k \neq \sigma(i)$ e $k \neq \sigma(j)$. Se $k = \sigma(i)$, allora si ha la seguente condizione:

$$\begin{aligned}\big(\sigma \circ (i\ j) \circ \sigma^{-1}\big)(k) &= \big(\sigma \circ (i\ j) \circ \sigma^{-1}\big)\big(\sigma(i)\big) = \big(\sigma \circ (i\ j)\big)\big((\sigma^{-1} \circ \sigma)(i)\big) \\ &= \big(\sigma \circ (i\ j)\big)(i) = \sigma\big((i\ j)(i)\big) = \sigma(j) \\ &= \big(\sigma(i)\ \sigma(j)\big)\big(\sigma(i)\big) = \big(\sigma(i)\ \sigma(j)\big)(k)\end{aligned}$$

Negli altri casi si procede esattamente allo stesso modo e quindi, non dipendendo il risultato ottenuto da una particolare scelta dell'indice $1 \le k \le n$, si ha la tesi. □

Teorema 3.5. *Si consideri il gruppo* $\{\pm 1\}$ *con l'operazione di prodotto usuale* $\cdot$ *e con elemento neutro* 1. *La funzione segno è l'unico epimorfismo, cioè l'unico omomorfismo non costante, da* S_n *a* $\{\pm 1\}$.

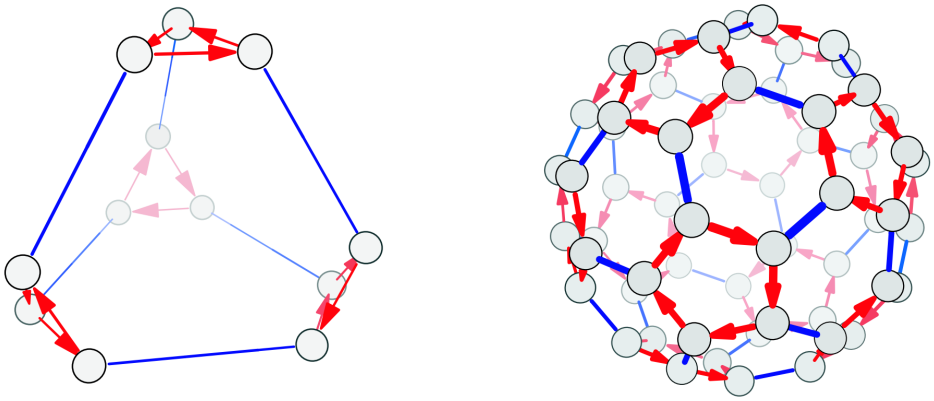
Dimostrazione. Sia $f\colon S_n \to \{\pm 1\}$ un epimorfismo e si osservi, innanzitutto, che richiedere la suriettività equivale a richiedere che f sia non costante. Infatti, tali condizioni sono vere se e solo se esistono $a, b \in S_n$ tali che $f(a) \neq f(b)$. Si noti ora che, se fosse $f(\tau) = 1$ per ogni trasposizione $\tau \in S_n$, allora f non sarebbe suriettiva perché S_n è generato dalle trasposizioni e si assume che f sia un omomorfismo. Si deduce quindi che esiste una trasposizione $\tau := (i\ j)$ tale che $f(\tau) = -1$. Sia ora $\tau' := (h\ k)$ una trasposizione qualsiasi e sia $\sigma := (i\ h) \circ (j\ k)$. Per costruzione vale che $\sigma(i) = h$, $\sigma(j) = k$ e quindi, applicando l'osservazione 3.16, si ottiene che $\sigma \circ \tau \circ \sigma^{-1} = \tau'$. Utilizzando l'assunzione che f sia un omomorfismo, il fatto che $\{\pm 1\}$ con operazione moltiplicativa $\cdot$ ed elemento neutro 1 sia un gruppo abeliano e l'osservazione 3.2, si ricava che:

$$f(\tau') = f(\sigma \circ \tau \circ \sigma^{-1}) = f(\sigma) \cdot f(\tau) \cdot f(\sigma^{-1}) = f(\sigma) \cdot f(\sigma^{-1}) \cdot f(\tau) = f(\tau) = -1$$

Non dipendendo il risultato ottenuto da una particolare scelta della trasposizione τ', posso affermare che f assume valore -1 su tutte le trasposizioni. A questo punto basta semplicemente osservare che il gruppo simmetrico S_n è generato dalle trasposizioni in quanto ogni permutazione si può scrivere come prodotto di trasposizioni. Avendo dimostrato che gli omomorfismi sgn e f coincidono su tali generatori, posso dunque concludere che $f = \operatorname{sgn}$. Per arbitrarietà nella scelta dell'epimorfismo $f\colon S_n \to \{\pm 1\}$, si ha la tesi. □

Osservazione 3.17. Ricordando che, come si è detto nella seconda parte della proposizione 3.3, si ha che $\{\pm 1\} \simeq \mathbb{Z}_2$, una conseguenza immediata del teorema 3.5 è che, a meno di isomorfismo, la funzione segno è l'unico epimorfismo dal gruppo simmetrico S_n a $\mathbb{Z}_2$.

Definizione 3.6. Una permutazione $\sigma \in S_n$ si dice *pari* se $\operatorname{sgn}(\sigma) = 1$, altrimenti si dice *dispari*. Inoltre, se $n \geq 2$, allora l'insieme di tutte le permutazioni pari di S_n prende il nome di *gruppo alterno su n lettere* e si denota A_n.



Il diagramma sulla sinistra, a forma di tetraedro troncato, rappresenta il gruppo alterno A_4. Le frecce rosse stanno a indicare l'operazione di composizione con l'elemento $(2\,4\,3)$, mentre gli spigoli blu rappresentano il prodotto per la permutazione $(1\,2) \circ (3\,4)$. Il diagramma a destra, a forma di icosaedro troncato, mostra invece il gruppo alterno A_6. In questo caso, le frecce rosse indicano la composizione con l'elemento $(1\,2\,3\,4\,5)$, mentre gli spigoli blu indicano il prodotto per la permutazione $(1\,2) \circ (3\,4)$ come nell'altro diagramma.

Osservazione 3.18. Dalla definizione 3.6 segue immediatamente che $A_n = \operatorname{Ker} \operatorname{sgn}$. In particolare, in virtù della proposizione 3.1-(ii), si ha che $A_n \lhd S_n$. Ma allora, ricordando che per la proposizione 3.3 la funzione segno è un epimorfismo e $\operatorname{Im} \operatorname{sgn} \simeq \mathbb{Z}_2$, applicando il primo teorema di isomorfismo (corollario 3.1) si ricava che $S_n/A_n \simeq \mathbb{Z}_2$. In particolare, dalla corrispondenza biunivoca fra i due insiemi segue che $[S_n : A_n] = 2$ e dunque, per il teorema di Lagrange (corollario 2.1), si ottiene che $|A_n| = \frac{n!}{2}$.

Proposizione 3.4. *Sia* $n \geq 2$. *Allora* A_n *è l'unico sottogruppo di indice* 2 *in* S_n.

Dimostrazione. Sia $H < S_n$ un qualsiasi sottogruppo di indice 2. In virtù dell'osservazione 2.16, si ha che $H \lhd S_n$ è un sottogruppo normale. È dunque ben definito il gruppo quoziente S_n/H, che per ipotesi e per definizione di indice (definizione 2.2), ha ordine 2. Deduco quindi che esiste una permutazione $\sigma \notin H$ tale

che $S_n/H = \{ H, \sigma H \}$. A questo punto è evidente che $S_n/H \simeq \mathbb{Z}_2$ perché l'applicazione $f\colon S_n/H \to \mathbb{Z}_2$ definita da $f(H) := \bar{0}$, $f(\sigma H) := \bar{1}$ è un isomorfismo, come è facile verificare. Ma allora, se $q\colon S_n \to S_n/H$ è la mappa quoziente, l'applicazione $f \circ q\colon S_n \to \mathbb{Z}_2$ è un epimorfismo e dall'osservazione 3.17 segue quindi che $f \circ q = \operatorname{sgn}$. In particolare, ricordando che $xH = H$ se e solo se $x \in H$, varrà la condizione seguente:

$$\begin{aligned} A_n = \operatorname{Ker}\operatorname{sgn} = \operatorname{Ker} f \circ q &= \{ x \in S_n \mid (f \circ q)(x) = \bar{0} \} \\ &= \{ x \in S_n \mid f(xH) = \bar{0} \} \\ &= \{ x \in S_n \mid xH = H \} \\ &= \{ x \in S_n \mid x \in H \} = S_n \cap H = H \end{aligned}$$

Dall'arbitrarietà nella scelta del sottogruppo $H < S_n$ di indice 2 segue dunque la tesi. □

Osservazione 3.19. Sia $n \geq 3$. Allora A_n è generato dai cicli di lunghezza 3.

Dimostrazione. Si noti innanzitutto che, come si è visto nella dimostrazione del teorema 3.4-(ii), un ciclo di lunghezza 3 si decompone come prodotto di 2 trasposizioni e quindi è una permutazione pari. Si noti anche che, per il teorema 3.4-(i), ogni permutazione di A_n si può esprimere come prodotto di un numero pari di trasposizioni e sarà quindi sufficiente mostrare che il prodotto di due trasposizioni è sempre uguale a un ciclo di lunghezza 3. Date due trasposizioni $(i\ j), (h\ k) \in S_n$ con $i < j$, $h < k$, si distinguono tre casi:

- se $i = h$ e $j = k$, allora $(i\ j) \circ (h\ k) = \mathrm{id}_{\{1,\dots,n\}} = (1\,2\,3)^0$.
- se $i = h$ e $j \neq k$, allora $(i\ j) \circ (h\ k) = (i\ j) \circ (i\ k) = (i\ k\ j)$.
- se $i \neq h$ e $j \neq k$, allora $(i\ j) \circ (h\ k) = \big((i\ j) \circ (i\ k)\big) \circ \big((i\ k) \circ (h\ k)\big) = (i\ k\ j) \circ (i\ k\ h)$. □

Osservazione 3.20. Il gruppo alterno A_4 è il più piccolo gruppo a dimostrare che, in generale, non vale il viceversa del teorema di Lagrange (corollario 2.1) cioè che, dati un gruppo G e un divisore d di $|G|$, non è detto che esista un sottogruppo di G di ordine d. Il gruppo alterno A_4, di ordine 12, non possiede infatti sottogruppi di ordine 6. Per dimostrarlo, si procede per assurdo: sia $H < A_4$ è un sottogruppo di ordine 6. Se tutti i cicli di lunghezza 3 fossero contenuti in H, allora $H = A_4$ in virtù dell'osservazione 3.19 e questo non è possibile perché $|H| \neq |A_4|$. Posso dunque considerare un ciclo $a \notin H$ di lunghezza 3. In virtù del teorema 2.1-(i) si ha, per contrapposizione logica, che $aH \neq H$. Dal punto (iii) dello stesso risultato segue che $|aH| = 6$ e dunque, per il punto (ii) del medesimo teorema e per il fatto che $|A_4| = 12$, si ottiene che $A_4 = H \sqcup aH$. A questo punto vi sono due possibilità. Se $a^2 \in H$ allora, essendo $H < G$ un sottogruppo, anche $a^4 \in H$ perché $a^4 = a^2 \circ a^2$. Tuttavia, poiché si assume che a sia un ciclo di lunghezza 3, si ha che $a^4 = a$ e questo contraddice il fatto che $a \notin H$. Se invece $a^2 \notin H$, allora in virtù dell'unione disgiunta si deve avere che $a^2 \in aH$. Moltiplicando a sinistra per $\{a^{-1}\}$ si ricava quindi che $a \in H$ e questo è assurdo. In definitiva, il gruppo alterno A_4 non possiede sottogruppi di ordine 6.

Definizione 3.7. Un gruppo G si dice *semplice* se non possiede sottogruppi normali non banali, cioè se i suoi unici sottogruppi normali sono il sottogruppo costituito dal solo elemento neutro e il gruppo stesso.

Sussiste il seguente risultato fondamentale la cui dimostrazione, tuttavia, non verrà trattata.

Teorema 3.6. *Se $n \geq 5$, allora A_n è un gruppo semplice.*

Osservazione 3.21. Il teorema 3.6 vale anche se $n = 2$ e se $n = 3$, ma non se $n = 4$. Il caso $n = 2$ è banale, in quanto $A_2 = \{\mathrm{id}_{\{1,2\}}\}$. Nel caso $n = 3$, invece, si ha che $A_3 = \{\mathrm{id}_{\{1,2,3\}}, (1\,2\,3), (1\,3\,2)\}$ ed è immediato verificare che $A_3 \simeq \mathbb{Z}_3$. Si ricordi adesso che $\mathbb{Z}_p$ con p numero primo non ammette sottogruppi non banali ma allora, dato che per il teorema di corrispondenza i sottogruppi di A_3 e di $\mathbb{Z}_3$ sono in corrispondenza biunivoca, anche A_3 non ammette sottogruppi non banali. In particolare, il gruppo alterno A_3 è semplice. Per mostrare che A_4 non è semplice, basta esibire un sottogruppo normale non banale. Si consideri quindi:

$$V_4 := \{ \mathrm{id}_{\{1,2,3,4\}}, (1\,2) \circ (3\,4), (1\,3) \circ (2\,4), (1\,4) \circ (2\,3) \}$$

È immediato verificare che $V_4 \subseteq A_4$ è chiuso rispetto all'operazione di composizione di funzioni. Inoltre, l'insieme V_4 contiene l'identità e ciascuno dei suoi elementi ha se stesso come inverso. Di conseguenza, si può concludere che $V_4 < A_4$ è un sottogruppo. Per dimostrare che $V_4 \lhd A_4$ è un sottogruppo normale, è

sufficiente osservare che V_4 è uguale all'unione della classe di coniugio dell'applicazione identità con quella costituita dalle coppie di trasposizioni disgiunte, per poi utilizzare l'osservazione 2.5. La classe di coniugio dell'applicazione identità contiene soltanto l'identità perché, se $\sigma \in A_4$ è coniugato all'identità, cioè se si ha che $\sigma = a \circ \mathrm{id}_{\{1,2,3,4\}} \circ a^{-1}$ per un qualche $a \in A_4$, allora $\sigma = \mathrm{id}_{\{1,2,3,4\}}$ per le definizioni di elemento neutro e di inverso. La classe di coniugio di un elemento della forma $(i\ j) \circ (h\ k)$ con i, j, h, k a due a due distinti, invece, è costituita da elementi di A_4 che hanno la medesima struttura in cicli disgiunti in virtù dell'osservazione 3.16. Si ha infatti, per ogni $\sigma \in A_4$, la relazione seguente:

$$\sigma \circ \big((i\ j) \circ (h\ k)\big) \circ \sigma^{-1} = \big(\sigma \circ (i\ j) \circ \sigma^{-1}\big) \circ \big(\sigma \circ (h\ k) \circ \sigma^{-1}\big) = \big(\sigma(i)\ \sigma(j)\big) \circ \big(\sigma(h)\ \sigma(k)\big)$$

Si può verificare esplicitamente che in A_4 non vi sono coppie di trasposizioni disgiunte diverse da quelle già presenti in V_4. Posso dunque concludere che $V_4 \lhd A_4$ è un sottogruppo normale non banale in quanto unione disgiunta di classi di coniugio. Questo dimostra che A_4 non è un gruppo semplice.

Osservazione 3.22. Se $n \geq 4$, allora $Z(A_n) = \{\mathrm{id}_{\{1,\dots,n\}}\}$.

Dimostrazione. Sarà sufficiente mostrare che, fissato $\sigma \in A_n$, $\sigma \neq \mathrm{id}_{\{1,\dots,n\}}$, esiste un elemento $\tau \in A_n$ che non commuta con σ, cioè tale che $\sigma \circ \tau \neq \tau \circ \sigma$. Poiché si assume che $\sigma \neq \mathrm{id}_{\{1,\dots,n\}}$, esistono due elementi $a, b \in \{1, \dots, n\}$ con $a \neq b$ tali che $\sigma(a) = b$. Dal momento che per ipotesi $n \geq 4$, è possibile scegliere altri due elementi $c, d \in \{1, \dots, n\} \setminus \{a, b\}$. A questo punto, posto $\tau := (b\ c\ d)$, si hanno le condizioni seguenti:

$$(\sigma \circ \tau)(a) = \sigma\big(\tau(a)\big) = \sigma(a) = b$$
$$(\tau \circ \sigma)(a) = \tau\big(\sigma(a)\big) = \tau(b) = c$$

Si noti anche che $\tau \in A_n$ in quanto ciclo di lunghezza 3. Dalla discussione precedente segue dunque che ogni permutazione di A_n diversa dall'identità non appartiene al centro di A_n e quindi si ha la tesi. □

Osservazione 3.23. La veridicità dell'osservazione 3.22 nel caso $n \geq 5$ si può dimostrare, in maniera più semplice, come segue. Sotto tali ipotesi, infatti, il gruppo alterno A_n è semplice in virtù del teorema 3.6 e questo significa, per definizione, che non possiede sottogruppi normali non banali. Si ricordi, tuttavia, che $Z(A_n) \lhd A_n$ è un sottogruppo normale per l'osservazione 2.10, dunque le uniche possibilità ammesse sono $Z(A_n) = \{\mathrm{id}_{1,\dots,n}\}$ e $Z(A_n) = A_n$. Se fosse $Z(A_n) = A_n$ allora, per l'osservazione 2.11, varrebbe che A_n è un gruppo abeliano e questo è assurdo. Infatti è facile verificare, per esempio, che vale la condizione:

$$(1\,2\,3) \circ \big((1\,2) \circ (3\,4)\big) \neq \big((1\,2) \circ (3\,4)\big) \circ (1\,2\,3)$$

Per esclusione, dunque, si ha la tesi. L'osservazione 3.22 vale anche, ovviamente, nel caso $n = 2$, ma non nel caso $n = 3$. In tal caso, infatti, il gruppo alterno è abeliano, come è immediato verificare svolgendo i calcoli in maniera esplicita o per isomorfismo con $\mathbb{Z}_3$ e di conseguenza, in virtù dell'osservazione 2.11, si ha che $Z(A_3) = A_3$.

I risultati che seguono sono due corollari fondamentali del teorema 3.6.

Corollario 3.3. *Se $n \geq 5$, allora A_n è l'unico sottogruppo normale non banale di S_n.*

Dimostrazione. Innanzitutto, si noti che $A_n \lhd S_n$ è un sottogruppo normale per l'osservazione 3.18 e che ovviamente è non banale perché si assume $n \geq 5$. Sia quindi $N \lhd S_n$ un sottogruppo normale non banale. Dal teorema dei due sottogruppi (teorema 3.2-(ii)) segue che $N \cap A_n \lhd A_n$ è un sottogruppo normale ma allora, per il teorema 3.6, si dovrà avere che $N \cap A_n = \{\mathrm{id}_{\{1,\dots,n\}}\}$ oppure che $N \cap A_n = A_n$. Suppongo per assurdo che valga la prima di tali condizioni. Dall'isomorfismo $S_n/A_n \simeq \mathbb{Z}_2$ segue assai facilmente che S_n/A_n è un gruppo abeliano ma allora si ha che $[S_n, S_n] \subseteq A_n$ perché $[S_n, S_n]$ è il più piccolo sottogruppo normale di S_n tale che il quoziente sia un gruppo abeliano in virtù dell'osservazione 2.15. In particolare, si ottiene che $N \cap [S_n, S_n] = \{\mathrm{id}_{\{1,\dots,n\}}\}$ quindi, ricordando che $N \lhd S_n$ è un sottogruppo normale e usando l'osservazione 2.17, si ricava che $N \subseteq Z(S_n)$. A questo punto basta ricordare che $Z(S_n) = \{\mathrm{id}_{\{1,\dots,n\}}\}$ per $n \geq 3$, come si è visto nell'esempio 2.8 e di conseguenza, avendo assunto $n \geq 5$, si arriva alla conclusione che $N = \{\mathrm{id}_{\{1,\dots,n\}}\}$. Questo contraddice l'ipotesi che N sia non banale e dunque $N \cap A_n \neq \{\mathrm{id}_{\{1,\dots,n\}}\}$. Per esclusione, dovrà valere quindi che $N \cap A_n = A_n$, vale a dire che $A_n \subseteq N$. Ora, per la moltiplicatività dell'indice (proposizione 2.1) e in virtù dell'osservazione 3.18, si ha la condizione seguente:

$$2 = [S_n : A_n] = [S_n : N][N : A_n]$$

Se fosse $[S_n : N] = 1$, allora varrebbe che $|S_n| = |N|$ per il teorema di Lagrange (corollario 2.1) ma, poiché si assume che $N \subseteq S_n$, questo implicherebbe che $N = S_n$ e si avrebbe una contraddizione con l'assunzione che $N < S_n$ sia un sottogruppo non banale. Di conseguenza, l'unica possibilità è che $[S_n : N] = 2$, mentre $[N : A_n] = 1$. Applicando come prima il teorema di Lagrange, si ottiene quindi che $N = A_n$. Posso dunque concludere, per arbitrarietà nella scelta del sottogruppo normale non banale $N \lhd S_n$, che vale la tesi. □

Osservazione 3.24. Si osservi che la dimostrazione appena terminata vale anche nel caso $n = 3$ e si può dunque affermare che A_3 è l'unico sottogruppo normale non banale di S_3. Il corollario 3.3 non vale invece se $n = 2$ per il semplice fatto che $A_2 \lhd S_2$ è un sottogruppo normale banale. Non vale neppure nel caso in cui $n = 4$ perché l'insieme V_4 definito nell'osservazione 3.21 è un sottogruppo normale non banale di A_4, quindi anche di S_4.

Corollario 3.4 (Teorema di Abel-Ruffini)**.** *Una generica equazione algebrica di grado maggiore o uguale a* 5 *non è risolubile per radicali, cioè non è possibile determinarne le soluzioni in un numero finito di passi, a partire dai coefficienti dell'equazione, usando le quattro operazioni elementari* $+, -, \cdot, \div$ *e le estrazioni di radici.*

La dimostrazione del corollario 3.4 verrà trattata nel corso AL310.

4 Costruzione di gruppi

4.1 Monoidi liberi

Definizione 4.1. Sia $X = \{ a, b, c, \dots \}$ un insieme di simboli possibilmente infinito. In questo contesto, gli elementi di X vengono chiamati *lettere*, mentre X prende il nome di *alfabeto*. Una sequenza finita di lettere di X con ripetizioni ammesse si dice una *parola su* X e l'insieme delle parole su X si denota MX. Inoltre, la sequenza vuota prende il nome di *parola vuota* e viene denotata con il simbolo 1.

Osservazione 4.1. Sia X un alfabeto e sia $*$ l'operazione binaria su MX definita dalla giustapposizione di parole, cioè da $w * w' := ww'$. Allora l'insieme MX munito dell'operazione binaria $*$ è un monoide che ha per elemento neutro la parola vuota 1.

Dimostrazione. È immediato verificare che l'operazione binaria $*$ su MX gode della proprietà associativa. Infatti si ha, per ogni $w, w', w'' \in MX$, la condizione seguente:

$$(w * w') * w'' = ww' * w'' = ww'w'' = w * w'w'' = w * (w' * w'')$$

La parola vuota è un elemento neutro poiché, per definizione, essa è la sequenza vuota e dunque l'asserto è dimostrato. □

Definizione 4.2. Sia X un alfabeto. Il monoide MX con l'operazione binaria $*$ data nell'osservazione 4.1 e con elemento neutro la parola vuota 1 prende il nome di *monoide libero su* X.

Osservazione 4.2. Sia X un alfabeto. Dalla definizione data dell'operazione binaria di giustapposizione $*$ su MX, dalla definizione 1.9 e dall'osservazione 1.13 segue che X è un insieme di generatori per MX.

Definizione 4.3. Siano $(M_1, \cdot, e_1)$, $(M_2, \star, e_2)$ due monoidi. Una funzione $f \colon M_1 \to M_2$ viene detta un *omomorfismo da* M_1 *a* M_2 se verifica la condizione $f(a \cdot b) = f(a) \star f(b)$ per ogni $a, b \in M_1$ e se preserva l'elemento neutro, cioè se $f(e_1) = e_2$.

Vale un fatto analogo all'osservazione 2.28.

Osservazione 4.3. Siano M_1 e M_2 monoidi. Combinando le definizioni 1.6 e 4.3 si ottiene che una funzione $f \colon M_1 \to M_2$ è un isomorfismo se e solo se è un omomorfismo biiettivo.

L'osservazione 1.16 si generalizza senza cambiamenti al caso degli omomorfismi di monoidi.

Osservazione 4.4. Siano $(M_1, \cdot, e_1)$, $(M_2, \star, e_2)$ monoidi, $f \colon M_1 \to M_2$ un omomorfismo e si considerino $a_1, \dots, a_n \in M_1$. Dalla definizione 4.3 segue immediatamente, per induzione sul numero n degli elementi considerati, che si ha la condizione $f(a_1 \cdots a_n) = f(a_1) \star \cdots \star f(a_n)$.

Osservazione 4.5. Negli omomorfismi di monoidi, diversamente da quanto accade con gli omomorfismi di gruppi, la condizione per cui viene preservato l'elemento neutro non è una conseguenza della prima e viene richiesta per definizione. L'esempio che segue dimostra che non si può omettere tale condizione aggiuntiva.

Esempio 4.1. Si considerino il monoide $(\mathbb{Z}, \cdot, 1)$ e l'applicazione identicamente nulla $o\colon \mathbb{Z} \to \mathbb{Z}$. Allora si ha, per ogni $k, h \in \mathbb{Z}$, la condizione seguente:

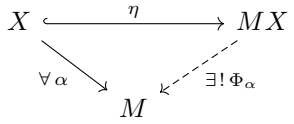
$$o(k \cdot h) = 0 = 0 \cdot 0 = o(k) \cdot o(h)$$

Ciononostante, l'applicazione nulla non è un omomorfismo di monoidi in quanto l'elemento neutro 1 non viene mappato in se stesso, bensì in 0.

Proposizione 4.1 (Proprietà universale dei monoidi liberi)**.** *Sia X un alfabeto, sia M un monoide e si consideri la mappa inclusione $\eta\colon X \to MX$. Allora η soddisfa la seguente proprietà universale:*

$$\forall\, \alpha\colon X \to M \text{ applicazione } \exists!\, \Phi_\alpha\colon MX \to M \text{ omomorfismo } \mid\ \Phi_\alpha \circ \eta = \alpha$$

Equivalentemente, il seguente diagramma di applicazioni è commutativo:



Dimostrazione. Sia $\alpha\colon X \to M$ una qualsiasi applicazione e sia $\Phi_\alpha\colon MX \to M$ la funzione definita dalla condizione $\Phi(abc\dots z) := \alpha(a) \cdot \alpha(b) \cdot \alpha(c) \cdots \alpha(z)$. Si tratta di una mappa ben definita poiché $\alpha(x) \in M$ per ogni $x \in X$ e perché per ipotesi M è un monoide, dunque in particolare è chiuso rispetto all'operazione binaria $\cdot$ su M. Per costruzione, vale banalmente che Φ_α è un omomorfismo e che soddisfa la condizione $\Phi_\alpha \circ \eta = \alpha$. Sia adesso $\Psi_\alpha\colon MX \to M$ un omomorfismo tale che $\Psi_\alpha \circ \eta = \alpha$ e si osservi che, in virtù della condizione appena menzionata, vale per ogni $x \in X$ la relazione seguente:

$$\Psi_\alpha(x) = \Psi_\alpha\big(\eta(x)\big) = (\Psi_\alpha \circ \eta)(x) = \alpha(x)$$

Da tale relazione, dall'assunzione che Ψ_α sia un omomorfismo e dall'osservazione 4.4 deriva dunque, per ogni $abc\dots z \in MX$, la condizione seguente:

$$\Psi_\alpha(abc\dots z) = \Psi_\alpha(a) \cdot \Psi_\alpha(b) \cdot \Psi_\alpha(c) \cdots \Psi_\alpha(z) = \alpha(a) \cdot \alpha(b) \cdot \alpha(c) \cdots \alpha(z) = \Phi_\alpha(abc\dots z)$$

Non dipendendo il risultato ottenuto da una particolare scelta dell'omomorfismo $\Psi_\alpha\colon MX \to M$ tale che $\Psi_\alpha \circ \eta = \alpha$, posso concludere che Φ_α è unico e ottengo quindi la tesi. □

4.2 Gruppi liberi

Definizione 4.4. Siano $X = \{\, a, b, c, \dots \}$, $X^{-1} := \{\, a^{-1}, b^{-1}, c^{-1}, \dots \}$ due alfabeti tali che $|X| = |X^{-1}|$. Sia inoltre $\tilde{X} := X \sqcup X^{-1}$. Una parola in $M\tilde{X}$ si dice *ridotta* se non contiene alcuna coppia consecutiva della forma xx^{-1} oppure $x^{-1}x$ con $x \in X$. Inoltre, assegnata una parola $w \in M\tilde{X}$, una parola ridotta w_0 ottenuta da w mediante un numero finito di cancellazioni di coppie consecutive della forma xx^{-1} oppure $x^{-1}x$ con $x \in X$ si dice una *forma ridotta di* w.

Esempio 4.2. Siano $X, X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4. La parola $aba^{-1}c \in M\tilde{X}$ è ridotta in quanto non contiene coppie consecutive della forma xx^{-1} oppure $x^{-1}x$ con $x \in X$. Deduco quindi che la parola $aba^{-1}c$ è una forma ridotta di se stessa. La parola $baa^{-1}cd \in M\tilde{X}$, invece, non è ridotta. Una sua forma ridotta è bcd, ottenuta cancellando la coppia consecutiva aa^{-1}.

Osservazione 4.6. Siano $X, X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4. Allora, data una parola $w \in M\tilde{X}$, esiste una forma ridotta di w.

Dimostrazione. Posso assumere, senza perdita di generalità, che $w = a_1 a_2 \dots a_n$. Procedo per induzione forte sulla lunghezza n della parola w. La base di induzione forte, corrispondente ai casi $n = 0$ e $n = 1$, è banale. Infatti, la parola vuota 1 e le parole costituite da un'unica lettera non possono contenere coppie

di lettere e di conseguenza sono già una forma ridotta di se stesse. Nel passo di induzione assumo $n \geq 2$, suppongo che la tesi valga per ogni $k \in \{0, \dots, n-1\}$ e dimostro che vale anche per n. Chiaramente, se w è una parola ridotta, allora è una forma ridotta di se stessa. In caso contrario, per la definizione 4.4, essa conterrà almeno una coppia consecutiva della forma $a_i a_i^{-1}$ oppure $a_i^{-1} a_i$ con $i \in \{1, \dots, n-1\}$. Ma allora, cancellando tale coppia, ottengo da w una parola di lunghezza $n-2$ e questa possiede una forma ridotta per ipotesi induttiva. Questo dimostra il passo induttivo e di conseguenza si ha la tesi. □

Proposizione 4.2 (Lemma di cambiamento dell'articolo)**.** *Si considerino alfabeti $X, X^{-1}, \tilde{X}$ come nella definizione 4.4. Allora, data una parola $w \in M\tilde{X}$, la forma ridotta di w è unica.*

Dimostrazione. Assumo senza perdita di generalità che $w = a_1 a_2 \dots a_n$ e procedo per induzione forte sulla lunghezza n della parola w. La base di induzione forte, che corrisponde ai casi $n = 0$ e $n = 1$, deriva dal fatto che la parola vuota 1 e le parole costituite da una sola lettera hanno se stesse come forma ridotta. Nel passo di induzione assumo $n \geq 2$, suppongo che la tesi sia vera per ogni $k \in \{0, \dots, n-1\}$ e dimostro che vale anche per n. Innanzitutto, se w è una parola ridotta, allora la forma ridotta di w è la parola w stessa, che è unica. Mi pongo quindi nel caso non banale in cui w non è una parola ridotta. In tal caso, la parola w contiene per definizione una coppia consecutiva della forma $a_i a_i^{-1}$ oppure $a_i^{-1} a_i$ per qualche $i \in \{1, \dots, n-1\}$. Posso supporre per semplicità che la coppia sia della prima forma, poiché l'argomento che verrà applicato nel corso della dimostrazione è lo stesso in entrambi casi. Si considerino dunque due forme ridotte $w_0^{(1)}, w_0^{(2)} \in M\tilde{X}$ della parola w. Sicuramente, una forma ridotta di w si trova cancellando al primo passo la coppia consecutiva $a_i a_i^{-1}$ e si può dunque supporre che tale forma ridotta sia $w_0^{(1)}$. Ora distinguo tre casi. Innanzitutto, è possibile che anche la parola $w_0^{(2)}$ si ottenga da w cancellando al primo passo la coppia $a_i a_i^{-1}$. Definisco in tal caso $\tilde{w}$ come la parola ottenuta da w eliminando la coppia $a_i a_i^{-1}$. Per costruzione, si ha che $w_0^{(1)}$ e $w_0^{(2)}$ sono forme ridotte della parola $\tilde{w}$, ma questa ha lunghezza $n-2$ e quindi, per ipotesi induttiva, si dovrà avere che $w_0^{(1)} = w_0^{(2)}$. Suppongo ora che il processo di cancellazione dal quale si ottiene la parola $w_0^{(2)}$ preveda la cancellazione della coppia $a_i a_i^{-1}$, ma non necessariamente al primo passo. In questo caso basta semplicemente osservare che, cambiando l'ordine di cancellazione, non cambia $w_0^{(2)}$ e dunque posso assumere, senza perdita di generalità, che la coppia $a_i a_i^{-1}$ venga eliminata al primo passo. Così facendo, mi riconduco al caso precedente, in virtù del quale si ottiene che $w_0^{(1)} = w_0^{(2)}$. Un'ultima possibilità è che il processo di cancellazione dal quale si ottiene $w_0^{(2)}$ non preveda l'eliminazione diretta della coppia $a_i a_i^{-1}$. Si osservi tuttavia che tale coppia non potrà comparire in $w_0^{(2)}$ in quanto una forma ridotta è una parola ridotta per definizione. Da questo segue quindi che a_i oppure a_i^{-1} dovrà essere coinvolto in una qualche cancellazione. Se indico tra parentesi gli elementi che verranno cancellati, allora tale cancellazione sarà necessariamente della forma $(a_i^{-1} a_i) a_i^{-1}$ nel caso in cui viene cancellato almeno a_i, mentre sarà del tipo $a_i (a_i^{-1} a_i)$ nel caso in cui viene cancellato almeno a_i^{-1}. A questo punto basta soltanto notare che, se sostituisco questo passaggio con la cancellazione della coppia $a_i a_i^{-1}$, allora il risultato non cambia. Così facendo si ottiene un nuovo processo che ha ancora come risultato finale la parola $w_0^{(2)}$, ma che coinvolge anche la cancellazione della coppia $a_i a_i^{-1}$. Mi sono dunque ricondotto al caso precedente e posso dunque affermare che si ha in ogni caso la relazione $w_0^{(1)} = w_0^{(2)}$. Per arbitrarietà nella scelta della forma ridotta $w_0^{(2)} \in M\tilde{X}$, si può concludere che ogni forma ridotta di w coincide con $w_0^{(1)}$. In particolare, la forma ridotta di w è unica. □

Osservazione 4.7. Per la proposizione 4.2 ogni parola ammette un'unica forma ridotta, ma il processo di cancellazione non è unico. Si è infatti notato più di una volta, nel corso della dimostrazione, che è possibile apportare modifiche al suddetto processo pur non alterandone il risultato finale. Segue ora un esempio.

Esempio 4.3. Siano $X, X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4. La parola $cabb^{-1}a^{-1}c^{-1}ca \in M\tilde{X}$ ha, in virtù della proposizione 4.2, un'unica forma ridotta. Ciononostante, quelli che seguono sono processi di cancellazione distinti ma ugualmente validi (esattamente come nella dimostrazione della proposizione 4.2, utilizzo le parentesi per indicare gli elementi che verranno cancellati al passaggio successivo):

$$\begin{aligned} ca(bb^{-1})a^{-1}c^{-1}ca &\to c(aa^{-1})c^{-1}ca \to (cc^{-1})ca \to ca \\ cabb^{-1}a^{-1}(c^{-1}c)a &\to cabb^{-1}(a^{-1}a) \to ca(bb^{-1}) \to ca \end{aligned}$$

Definizione 4.5. Siano $X, X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4, siano $w, w' \in M\tilde{X}$ parole e siano $w_0, w_0' \in M\tilde{X}$ le forme ridotte di w e di w' rispettivamente. Le parole w e w' si dicono *equivalenti* e in tal caso si scrive $w \sim w'$ se $w_0 = w_0'$.

La definizione 4.5 è ben posta perché, per la proposizione 4.2, la forma ridotta di una parola è unica.

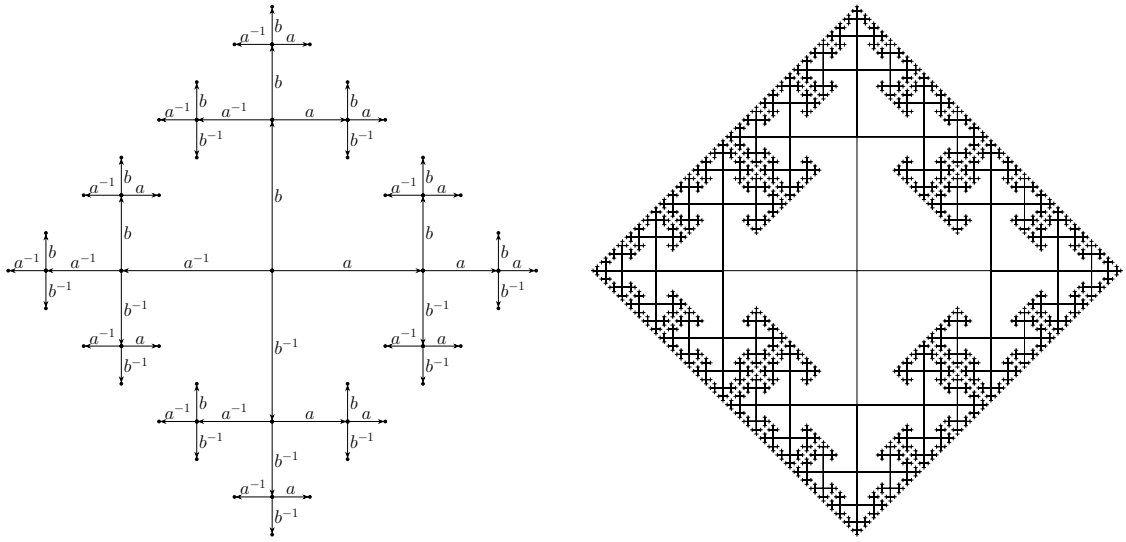
Osservazione 4.8. Si verifica assai facilmente che la relazione di equivalenza di parole $\sim$ su $M\tilde{X}$ introdotta nella definizione 4.5 è in effetti una relazione di equivalenza.

Proposizione 4.3. *Siano $X, X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4 e siano $w, w', v, v' \in M\tilde{X}$ parole. Se $w \sim w'$ e $v \sim v'$, allora $w * v \sim w' * v'$. In altre parole, la relazione di equivalenza di parole $\sim$ su $M\tilde{X}$ è compatibile con l'operazione di giustapposizione di parole $*$ su $M\tilde{X}$.*

Dimostrazione. Poiché per ipotesi $w \sim w'$ e $v \sim v'$, posso supporre senza ambiguità che w_0 sia la forma ridotta di w e di w', che v_0 sia la forma ridotta di v e di v'. Si cancellino da $w * v$ tutte le coppie consecutive della forma xx^{-1} oppure $x^{-1}x$ con $x \in X$ che compaiono interamente in w oppure interamente in v. Così facendo si ottiene per costruzione la parola $w_0 * v_0$ ma questo significa che $w * v$ e $w_0 * v_0$ hanno la stessa forma ridotta, cioè che $w * v \sim w_0 * v_0$. Applicando lo stesso ragionamento con $w' * v'$ al posto di $w * v$, si ottiene che $w' * v' \sim w_0 * v_0$. Usando infine il fatto che $\sim$ è una relazione di equivalenza (osservazione 4.8), vale in particolare la proprietà transitiva, dalla quale deriva immediatamente la tesi. □

Osservazione 4.9. Ricordando la definizione 2.10, diventa possibile riformulare la proposizione 4.3 dicendo semplicemente che la relazione di equivalenza di parole $\sim$ su $M\tilde{X}$ è una congruenza su $M\tilde{X}$. Si noti anche che, in particolare, è ben definito il gruppo quoziente di $M\tilde{X}$ per la congruenza $\sim$, cioè l'insieme $M\tilde{X}/\sim$ munito dell'operazione binaria $\cdot$ definita da $[w] \cdot [w'] := [w * w']$ e con elemento neutro $[1]$.

Definizione 4.6. Siano $X, X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4. Il gruppo quoziente di $M\tilde{X}$ per la congruenza $\sim$ prende il nome di *gruppo libero su X* e si denota FX. Inoltre, un gruppo G si dice *libero* se esiste un alfabeto X tale che $G \simeq FX$. Se infine $X = \{x_1, \dots, x_r\}$ è un alfabeto finito, il gruppo FX si denota $\mathbb{F}_r$ e prende il nome di *gruppo libero su r lettere* (oppure *con r generatori*).



Il diagramma a sinistra rappresenta il gruppo libero sull'alfabeto $\{a, b\}$, vale a dire un gruppo libero su 2 lettere. Partendo dal centro della figura, che corrisponde alla parola vuota, vi sono quattro possibilità dopodiché, a ogni passo, si hanno tre diramazioni anziché quattro. Nei gruppi liberi, infatti, tutte le parole appartenenti a una stessa classe di equivalenza vengono considerate indistinguibili e non avrebbe dunque senso "tornare indietro" applicando l'inverso. Più diramazioni si percorrono, più la parola corrispondente al nodo finale diventa complicata. La figura sulla destra illustra lo stesso diagramma, ma con un maggior numero di diramazioni.

Osservazione 4.10. Sia X un alfabeto. Dalla definizione 4.6, dalle osservazioni 1.13 e 4.2 e dal fatto ovvio che $[x]^{-1} = [x^{-1}]$ per ogni $x \in X$ segue che l'insieme $\{\, [x] \mid x \in X \,\}$ è un insieme di generatori per FX.

Esempio 4.4. Il gruppo banale $\{1\}$ con operazione moltiplicativa $\cdot$ e ovviamente con elemento neutro 1 è libero in quanto $\{1\} \simeq \mathbb{F}_0$. Posso infatti associare la parola vuota 1 all'identità 1. Un caso meno banale è dato dal gruppo $\mathbb{Z}$ munito dell'operazione usuale di somma $+$ e dell'elemento neutro 0. Si consideri la funzione $f\colon \mathbb{Z} \to \mathbb{F}_1$ definita da $f(k) := [a^k]$. Si tratta di una corrispondenza biunivoca per costruzione ed

è immediato verificare, per una proprietà delle potenze (osservazione 1.10), che è anche un omomorfismo, come viene mostrato nella relazione che segue con $k, h \in \mathbb{Z}$ arbitrari:

$$f(k+h) = [a^{k+h}] = [a^k * a^h] = [a^k] \cdot [a^h] = f(k) \cdot f(h)$$

Ne segue che $\mathbb{Z}$ è un gruppo libero in quanto $\mathbb{Z} \simeq \mathbb{F}_1$.

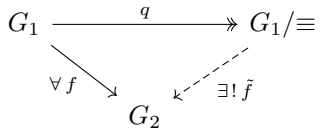
Osservazione 4.11. È immediato verificare che il gruppo libero $\mathbb{F}_r$ è abeliano se e solo se $r \leq 1$. Se infatti $r = 0$, allora non vi è nulla da dimostrare poiché $\mathbb{F}_0$ contiene soltanto l'elemento neutro. Nel caso $r = 1$, invece, la commutatività dell'operazione binaria $\cdot$ su $\mathbb{F}_1$ deriva banalmente dalle definizioni di elemento neutro e di inverso. Se $r \geq 2$, infine, si possono scegliere due lettere $a, b \in \mathbb{F}_r$ con $a \neq b$ e dunque $ab \neq ba$.

Definizione 4.7. Siano X, Y insiemi e sia $\sim$ una relazione di equivalenza su X. Una funzione $f\colon X \to Y$ si dice *invariante rispetto a* $\sim$ se $f(a) = f(b)$ per ogni $a, b \in X$ con $a \sim b$.

Proposizione 4.4 (Proprietà universale delle congruenze)**.** *Siano $(G_1, \cdot, e_1)$, $(G_2, \star, e_2)$ due gruppi, $\equiv$ una congruenza su G_1 e sia $q\colon G_1 \to G_1/\equiv$ la mappa quoziente. Allora q soddisfa la proprietà universale:*

$$\forall\, f\colon G_1 \to G_2 \text{ omomorfismo invariante rispetto a } \equiv\ \exists!\, \tilde{f}\colon G_1/\equiv \to G_2 \text{ omomorfismo } \mid\ \tilde{f} \circ q = f$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



Dimostrazione. Sia $f\colon G_1 \to G_2$ un omomorfismo invariante rispetto a $\equiv$ e sia $\tilde{f}\colon G_1/\equiv \to G_2$ la funzione definita da $\tilde{f}([g]) := f(g)$. Si tratta di un'applicazione ben definita per l'ipotesi che f sia un'applicazione invariante rispetto a $\equiv$. Infatti, comunque assegnati $g, h \in G_1$ tali che $g \equiv h$, vale che $f(g) = f(h)$ in virtù della definizione 4.7. Inoltre, la funzione $\tilde{f}$ così definita rispetta la condizione $\tilde{f} \circ q = f$ per costruzione. Infine, ricordando la definizione del prodotto $\cdot$ su $G_1/\equiv$ data nella definizione 2.11 e utilizzando l'ipotesi che f sia un omomorfismo si ha, per ogni scelta di due classi di equivalenza $[g], [h] \in G_1/\equiv$, la condizione:

$$\tilde{f}([g] \cdot [h]) = \tilde{f}([g \cdot h]) = f(g \cdot h) = f(g) \star f(h) = \tilde{f}([g]) \star \tilde{f}([h])$$

Questo dimostra che $\tilde{f}$ è un omomorfismo. Sia adesso $\bar{f}\colon G_1/\equiv \to G_2$ una funzione, possibilmente diversa da $\tilde{f}$, tale che $\bar{f} \circ q = f$. Allora, comunque venga fissata una classe $[g] \in G_1/\equiv$, vale la relazione seguente:

$$\bar{f}([g]) = \bar{f}\big(q(g)\big) = (\bar{f} \circ q)(g) = f(g) = (\tilde{f} \circ q)(g) = \tilde{f}\big(q(g)\big) = \tilde{f}([g])$$

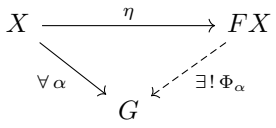
Avendo ottenuto che $\bar{f} = \tilde{f}$ posso concludere, per arbitrarietà nella scelta dell'applicazione $\bar{f}\colon G_1/\equiv \to G_2$ tale che $\bar{f} \circ q = f$, che la funzione $\tilde{f}$ desiderata è unica. □

Per la proprietà universale delle congruenze vale un fatto analogo all'osservazione 3.6. La proposizione che segue si può dedurre come conseguenza delle proprietà universali dei monoidi liberi e delle congruenze.

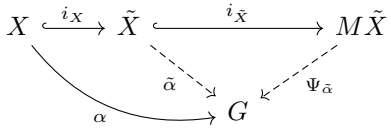
Proposizione 4.5 (Proprietà universale dei gruppi liberi)**.** *Siano X un alfabeto, G un gruppo. Sia inoltre $\eta\colon X \to FX$ l'applicazione definita da $\eta(x) := [x]$. Allora η soddisfa la seguente proprietà universale:*

$$\forall\, \alpha\colon X \to G \text{ applicazione } \exists!\, \Phi_\alpha\colon FX \to G \text{ omomorfismo } \mid\ \Phi_\alpha \circ \eta = \alpha$$

Equivalentemente, il seguente diagramma di applicazioni è commutativo:



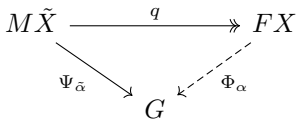
Dimostrazione. Sia $\alpha\colon X \to G$ una funzione e siano $X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4. Considero l'estensione $\tilde{\alpha}\colon \tilde{X} \to G$ di α definita da $\tilde{\alpha}(x) := \alpha(x)$ e da $\tilde{\alpha}(x^{-1}) := \alpha(x)^{-1}$. Si tratta di un'applicazione ben definita in quanto G è per ipotesi un gruppo e quindi gli elementi nell'immagine di α ammettono un inverso. Si considerino adesso le mappe inclusione $i_X\colon X \to \tilde{X}$, $i_{\tilde{X}}\colon \tilde{X} \to M\tilde{X}$ e inoltre, tenendo a mente l'osservazione 4.8 e ricordando che, in virtù della definizione 4.6, si ha che $FX := M\tilde{X}/\!\sim$, dove $\sim$ denota la relazione di equivalenza di parole, si consideri anche la mappa quoziente $q\colon M\tilde{X} \to FX$. Si osservi ora che $\alpha = \tilde{\alpha} \circ i_X$ e che $\eta = q \circ i_{\tilde{X}} \circ i_X$ per costruzione. A questo punto, utilizzando il fatto che un gruppo è in particolare un monoide, posso applicare la proprietà universale dei monoidi liberi (proposizione 4.1), in virtù della quale esiste un unico omomorfismo $\Psi_{\tilde{\alpha}}\colon M\tilde{X} \to G$ tale che $\Psi_{\tilde{\alpha}} \circ i_X = \tilde{\alpha}$. Le mappe coinvolte nella dimostrazione fino a questo punto si possono visualizzare intuitivamente con il seguente diagramma:



Si noti ora che $\Psi_{\tilde{\alpha}}$ è un'applicazione invariante rispetto alla relazione di equivalenza di parole $\sim$. Infatti, date due parole $ab\dots z, ab\dots xx^{-1}\dots z \in M\tilde{X}$ che differiscono soltanto per una qualche coppia xx^{-1} con $x \in X$, ricordando la costruzione di $\Psi_{\tilde{\alpha}}$ data nella dimostrazione della proposizione 4.1 e la definizione di $\tilde{\alpha}$, si ricava la condizione seguente:

$$\begin{aligned}\Psi_{\tilde{\alpha}}(ab\dots xx^{-1}\dots z) &= \tilde{\alpha}(a)\cdot\tilde{\alpha}(b)\cdots\tilde{\alpha}(x)\cdot\tilde{\alpha}(x^{-1})\cdots\tilde{\alpha}(z)\\ &= \alpha(a)\cdot\alpha(b)\cdots\alpha(x)\cdot\alpha(x)^{-1}\cdots\alpha(z)\\ &= \alpha(a)\cdot\alpha(b)\cdots\alpha(z)\\ &= \tilde{\alpha}(a)\cdot\tilde{\alpha}(b)\cdots\tilde{\alpha}(z) = \Psi_{\tilde{\alpha}}(ab\dots z)\end{aligned} \tag{6}$$

Si procede esattamente allo stesso modo se si considerano parole che differiscono soltanto per una qualche coppia $x^{-1}x$ con $x \in X$. A questo punto, poiché per l'osservazione 4.9 la relazione di equivalenza di parole $\sim$ è una congruenza e dato che $\Psi_{\tilde{\alpha}}$ è invariante rispetto a $\sim$, posso applicare la proprietà universale delle congruenze, vale a dire la proposizione 4.4, in virtù della quale esiste un unico omomorfismo $\Phi_\alpha\colon FX \to G$ tale che $\Phi_\alpha \circ q = \Psi_{\tilde{\alpha}}$. Il seguente diagramma di omomorfismi renderà tutto più chiaro:



Basta infine osservare che, per costruzione e per associatività dell'operazione di composizione di funzioni, è soddisfatta la condizione seguente:

$$\Phi_\alpha \circ \eta = \Phi_\alpha \circ (q \circ i_{\tilde{X}} \circ i_X) = \big((\Phi_\alpha \circ q) \circ i_{\tilde{X}}\big) \circ i_X = (\Psi_{\tilde{\alpha}} \circ i_{\tilde{X}}) \circ i_X = \tilde{\alpha} \circ i_X = \alpha$$

L'unicità dell'omomorfismo Φ_α deriva immediatamente da quella dell'estensione $\tilde{\alpha}$, dell'applicazione $\Psi_{\tilde{\alpha}}$ e dalla proprietà universale delle congruenze. □

Alternativamente, posso dare una dimostrazione costruttiva della proprietà universale dei gruppi liberi applicando un argomento del tutto analogo a quello utilizzato per dimostrare la proprietà universale dei monoidi liberi, cioè la proposizione 4.1.

Dimostrazione (*costruttiva*). Si consideri una data applicazione $\alpha\colon X \to G$ e siano $X^{-1}, \tilde{X}$ alfabeti come nella definizione 4.4. Come nella dimostrazione non costruttiva, si consideri l'estensione $\tilde{\alpha}\colon \tilde{X} \to G$ di α definita da $\tilde{\alpha}(x) := \alpha(x)$ e da $\tilde{\alpha}(x^{-1}) := \alpha(x)^{-1}$ e si osservi che è una mappa ben definita poiché si assume che G sia un gruppo e di conseguenza gli elementi nell'immagine di α ammettono un inverso. Si consideri ora la funzione $\Phi_\alpha\colon FX \to G$ definita da $\Phi_\alpha([abc\dots z]) := \tilde{\alpha}(a)\cdot\tilde{\alpha}(b)\cdot\tilde{\alpha}(c)\cdots\tilde{\alpha}(z)$. Per dimostrare che Φ_α è un'applicazione ben definita basta osservare che, date due parole $ab\dots z, ab\dots xx^{-1}\dots z \in M\tilde{X}$ che differiscono soltanto per una qualche coppia xx^{-1} con $x \in X$, vale la condizione (6) con la funzione Φ_α al posto di $\Psi_{\tilde{\alpha}}$ e che, naturalmente, vale lo stesso se si considerano parole che differiscono soltanto per una

qualche coppia $x^{-1}x$ con $x \in X$. Dalla costruzione di Φ_α e dal fatto che $\tilde{\alpha}(x) = \alpha(x)$ per ogni $x \in X$ segue banalmente che Φ_α è un omomorfismo e che soddisfa la condizione $\Phi_\alpha \circ \eta = \alpha$. Sia adesso $\Psi_\alpha \colon FX \to G$ un omomorfismo tale che $\Psi_\alpha \circ \eta = \alpha$. Dato che $\Psi_\alpha \circ \eta = \alpha$ si ha, per ogni $x \in X$, la condizione seguente:

$$\Psi_\alpha([x]) = \Psi_\alpha\big(\eta(x)\big) = (\Psi_\alpha \circ \eta)(x) = \alpha(x) = \tilde{\alpha}(x)$$

Combinando l'ipotesi che Ψ_α sia un omomorfismo, il semplice fatto che $[x^{-1}] = [x]^{-1}$ per ogni $x^{-1} \in X^{-1}$ e la relazione precedente, si ottiene che in effetti $\Psi_\alpha([x]) = \tilde{\alpha}(x)$ per ogni $x \in \tilde{X}$ e di conseguenza, tenendo anche a mente l'osservazione 3.4, comunque fissata una classe $[abc\dots z] \in FX$ si ha la condizione seguente:

$$\Psi_\alpha([abc\dots z]) = \Psi_\alpha([a]) \cdot \Psi_\alpha([b]) \cdot \Psi_\alpha([c]) \cdots \Psi_\alpha([z]) = \tilde{\alpha}(a) \cdot \tilde{\alpha}(b) \cdot \tilde{\alpha}(c) \cdots \tilde{\alpha}(z) = \Phi_\alpha([abc\dots z])$$

Non dipendendo il risultato ottenuto da una particolare scelta dell'omomorfismo $\Psi_\alpha \colon FX \to G$ tale che $\Psi_\alpha \circ \eta = \alpha$, posso concludere che Φ_α è unico e ottengo dunque la tesi. □

Corollario 4.1. *Ogni gruppo è isomorfo al quoziente di un gruppo libero.*

Dimostrazione. Sia G un gruppo e sia X un insieme di generatori per G. Un insieme di generatori per G sicuramente esiste, poiché si può prendere per esempio $X = G$. Si considerino inoltre la mappa inclusione $i \colon X \to G$ e la funzione $\eta \colon X \to FX$ definita da $\eta(x) := [x]$. Per la proprietà universale dei gruppi liberi, cioè la proposizione 4.5, esiste un unico omomorfismo $\Phi_i \colon FX \to G$ tale che $\Phi_i \circ \eta = i$. Si osservi ora che, essendo $\eta(X) \subseteq FX$, varrà in particolare che $\Phi_i(\eta(X)) \subseteq \Phi_i(FX)$. Equivalentemente, per una proprietà elementare della funzione composta e per un cambio di notazione, vale che $(\Phi_i \circ \eta)(X) \subseteq \operatorname{Im} \Phi_i$, ma allora $i(X) \subseteq \operatorname{Im} \Phi_i$ perché $\Phi_i \circ \eta = i$. Si ottiene quindi, per come è definita la mappa inclusione, che $X \subseteq \operatorname{Im} \Phi_i$, ma $\operatorname{Im} \Phi_i < G$ è un sottogruppo in virtù della proposizione 3.1-(i) e quindi, per la definizione 1.8-(ii) nel caso del sottogruppo, si ha che $\langle X \rangle \subseteq \operatorname{Im} \Phi_i$. Poiché si assume che X sia un insieme di generatori per G, la condizione appena ottenuta equivale a richiedere che $G \subseteq \operatorname{Im} \Phi_i$, ma allora si ha doppia inclusione e di conseguenza $\Phi_i \colon FX \to G$ è un epimorfismo. A questo punto è sufficiente applicare l'osservazione 3.7, in virtù della quale ogni epimorfismo è un quoziente a meno di isomorfismo. Più precisamente, si può dire che $FX/\operatorname{Ker} \Phi_i \simeq G$ e dunque si ha la tesi. □

Osservazione 4.12. In virtù del corollario 4.1, ogni gruppo è isomorfo al quoziente di un gruppo libero, ma dalla dimostrazione si evince che tale quoziente non è univocamente determinato. Esso dipende, infatti, dalla scelta di un insieme di generatori X per G. Quanto più grande viene scelto X, tanto più complicato diventa il gruppo libero FX e, di conseguenza, tanto più difficile diventa studiare le proprietà del gruppo G servendosi dell'isomorfismo con un quoziente di FX.

4.3 Gruppi definiti tramite generatori e relazioni

Definizione 4.8. Sia G un gruppo e sia $H < G$ un sottogruppo. Il seguente sottoinsieme di G prende il nome di *chiusura normale di H in G*:

$$\langle H \rangle^G := \langle \bigcup_{a \in G} aHa^{-1} \rangle$$

Sia inoltre $S \subseteq G$ un insieme. Al fine di semplificare la notazione, la chiusura normale di $\langle S \rangle$ in G viene indicata con il simbolo $\langle S \rangle^G$ anziché con $\langle\langle S \rangle\rangle^G$.

Osservazione 4.13. Sia G un gruppo e sia $H < G$ un sottogruppo. Allora la chiusura normale di H in G è il più piccolo sottogruppo normale di G che contiene H.

Dimostrazione. Dalle definizioni 1.8 e 4.8 segue immediatamente che $\langle H \rangle^G < G$ è un sottogruppo. Sarà dunque sufficiente mostrarne la normalità. Siano $g \in G$, $x \in \langle H \rangle^G$ elementi fissati. Per la definizione 4.8 e per l'osservazione 1.13 esistono $x_1, \dots, x_n \in \bigcup_{a \in G} aHa^{-1}$ tali che $x = x_1^{\pm 1} \cdots x_n^{\pm 1}$ e inoltre esistono, per ogni $1 \leq i \leq n$, elementi $a_i \in G$, $h_i \in H$ tali che $x_i = a_i \cdot h_i \cdot a_i^{-1}$. A questo punto basta osservare che, in

virtù della proposizione 1.1-(iii), vale la relazione seguente:

$$\begin{aligned} g\cdot x\cdot g^{-1} &= g\cdot(x_1^{\pm 1}\cdots x_n^{\pm 1})\cdot g^{-1} \\ &= g\cdot\big((a_1\cdot h_1\cdot a_1^{-1})^{\pm 1}\cdots(a_n\cdot h_n\cdot a_n^{-1})^{\pm 1}\big)\cdot g^{-1} \\ &= g\cdot\big((a_1\cdot h_1^{\pm 1}\cdot a_1^{-1})\cdots(a_n\cdot h_n^{\pm 1}\cdot a_n^{-1})\big)\cdot g^{-1} \\ &= \big(g\cdot(a_1\cdot h_1^{\pm 1}\cdot a_1^{-1})\cdot g^{-1}\big)\cdots\big(g\cdot(a_n\cdot h_n^{\pm 1}\cdot a_n^{-1})\cdot g^{-1}\big) \\ &= \big((g\cdot a_1)\cdot h_1^{\pm 1}\cdot(g\cdot a_1)^{-1}\big)\cdots\big((g\cdot a_n)\cdot h_n^{\pm 1}\cdot(g\cdot a_n)^{-1}\big) \end{aligned}$$

Per ogni $1\leq i\leq n$ si ha che $(g\cdot a_i)\cdot h_i^{\pm 1}\cdot(g\cdot a_i)^{-1}\in(g\cdot a_i)H(g\cdot a_i)^{-1}$ poiché si assume per ipotesi che $H<G$ sia un sottogruppo e di conseguenza $(g\cdot a_i)\cdot h_i^{\pm 1}\cdot(g\cdot a_i)^{-1}\in\bigcup_{a\in G}aHa^{-1}$. Nuovamente in virtù dell'osservazione 1.13 e della definizione 4.8, posso affermare che $g\cdot x\cdot g^{-1}\in\langle H\rangle^G$ e quindi deduco, per arbitrarietà nella scelta di $x\in\langle H\rangle^G$, che $g\langle H\rangle^G g^{-1}\subseteq\langle H\rangle^G$. Non dipendendo il risultato ottenuto dalla scelta dell'elemento $g\in G$, posso concludere che $\langle H\rangle^G\lhd G$ è un sottogruppo normale. Naturalmente, il fatto che $H\subseteq\langle H\rangle^G$ è una conseguenza immediata della definizione 4.8.

Sia adesso $N\lhd G$ un sottogruppo normale tale che $H\subseteq N$. In virtù dell'osservazione 2.5, comunque fissato $h\in H$, siccome $h\in N$ essendo $H\subseteq N$, si dovrà avere che anche $a\cdot h\cdot a^{-1}\in N$ per ogni $a\in G$ ma allora, per arbitrarietà nella scelta di $h\in H$, dovrà valere che $aHa^{-1}\subseteq N$ per ogni $a\in G$. In altre parole, si ha che $\bigcup_{a\in G}aHa^{-1}\subseteq N$ e dunque, per le definizioni 1.8-(ii) e 4.8, posso affermare che $\langle H\rangle^G\subseteq N$. □

Osservazione 4.14. Siano G un gruppo, $S\subseteq G$ un insieme. Allora vale la formula $\langle S\rangle^G=\langle\bigcup_{a\in G}aSa^{-1}\rangle$.

Dimostrazione. L'inclusione $\langle\bigcup_{a\in G}aSa^{-1}\rangle\subseteq\langle S\rangle^G$ è banale in quanto $S\subseteq\langle S\rangle$ per la definizione 1.8-(i). Basterà dimostrare che $\langle\bigcup_{a\in G}aSa^{-1}\rangle<G$ è un sottogruppo tale che $\bigcup_{a\in G}a\langle S\rangle a^{-1}\subseteq\langle\bigcup_{a\in G}aSa^{-1}\rangle$. Ovviamente, in virtù della definizione 1.8-(i) si ha che $\langle\bigcup_{a\in G}aSa^{-1}\rangle<G$ è un sottogruppo. Sia adesso $x\in\bigcup_{a\in G}a\langle S\rangle a^{-1}$. Esiste quindi almeno un elemento $g\in G$ tale che $x\in g\langle S\rangle g^{-1}$. Dall'osservazione 1.13 si deduce invece che esistono $s_1,\dots,s_n\in S$ tali che $x=g\cdot s_1^{\pm 1}\cdots s_n^{\pm 1}\cdot g^{-1}$. Equivalentemente si ha che:

$$x=(g\cdot s_1^{\pm 1}\cdot g^{-1})\cdots(g\cdot s_n^{\pm 1}\cdot g^{-1})=(g\cdot s_1\cdot g^{-1})^{\pm 1}\cdots(g\cdot s_n\cdot g^{-1})^{\pm 1}$$

Dal momento che $g\cdot s_i\cdot g^{-1}\in\bigcup_{a\in G}aSa^{-1}$ per ogni $1\leq i\leq n$ posso concludere, per l'osservazione 1.13, che $x\in\langle\bigcup_{a\in G}aSa^{-1}\rangle$. Di conseguenza, per arbitrarietà nella scelta dell'elemento $x\in\bigcup_{a\in G}a\langle S\rangle a^{-1}$, si ha che $\bigcup_{a\in G}a\langle S\rangle a^{-1}\subseteq\langle\bigcup_{a\in G}aSa^{-1}\rangle$. La discussione precedente mi permette dunque di concludere, in virtù delle definizioni 1.8-(ii) e 4.8, che $\langle S\rangle^G\subseteq\langle\bigcup_{a\in G}aSa^{-1}\rangle$. Avendo mostrato la doppia inclusione, si ha la tesi. □

Definizione 4.9. Sia X un alfabeto e sia $R\subseteq FX$ un insieme. Il gruppo quoziente $FX/\langle R\rangle^{FX}$ prende il nome di *gruppo con generatori in X e relazioni in R* e viene denotato $\langle X|R\rangle$. Sia inoltre G un gruppo. Si dice che G *ammette una presentazione* (X,R) se esistono un alfabeto X e un sottoinsieme $R\subseteq FX$ tali che $G\simeq\langle X|R\rangle$. Se infine $X=\{x_1,\dots,x_r\}$ è un alfabeto finito, si definisce $\langle x_1,\dots,x_r|R\rangle:=\langle X|R\rangle$ per semplicità e analogamente, se $R=\{[w_1],\dots,[w_s]\}$ è un insieme finito, si pone $\langle X|w_1,\dots,w_s\rangle:=\langle X|R\rangle$. Al fine di semplificare ulteriormente la notazione, sebbene il gruppo $\langle X|R\rangle$ sia in effetti il quoziente di un quoziente, i suoi elementi verranno indicati senza parentesi quadre anziché con doppie parentesi quadre e l'operazione binaria su $\langle X|R\rangle$ verrà sottintesa.

La definizione 4.9 è ben posta perché $\langle R\rangle^{FX}\lhd FX$ è un sottogruppo normale per l'osservazione 4.13.

Esempio 4.5. Sia X un alfabeto e sia $R:=\{[1]\}$. In virtù dell'osservazione 4.14, si ha che $\langle R\rangle^{FX}=\{[1]\}$ e di conseguenza, per la definizione 4.9, posso affermare che $FX\simeq\langle X|1\rangle$. In altre parole, il gruppo libero su X è un gruppo con generatori in X privo di relazioni. Naturalmente, se $X=\{x_1,\dots,x_r\}$ è un alfabeto finito, allora $\mathbb{F}_r\simeq\langle x_1,\dots,x_r|1\rangle$. Si consideri inoltre il gruppo $\mathbb{Z}$ munito dell'usuale operazione di somma $+$ e dell'elemento neutro 0. Dato che $\mathbb{Z}\simeq\mathbb{F}_1$ come si è dimostrato nell'esempio 4.4, per transitività della relazione di isomorfismo (osservazione 1.9) posso affermare che $\mathbb{Z}\simeq\langle x|1\rangle$. Più in generale, si può dire che un gruppo è libero se e solo se ammette una presentazione priva di relazioni.

Corollario 4.2. *Ogni gruppo ammette una presentazione* (X,R).

Dimostrazione. Si riprenda la dimostrazione del corollario 4.1. È noto che, dati un gruppo G e un insieme di generatori X per G, esiste un epimorfismo $\Phi_i\colon FX \to G$ e quindi, in virtù dell'osservazione 3.7, si ha che $FX/\operatorname{Ker}\Phi_i \simeq G$. Sia ora R un insieme di generatori per $\operatorname{Ker}\Phi_i$. Come si è detto nella dimostrazione del corollario 4.1, un tale insieme di generatori sicuramente esiste poiché, per esempio, si può considerare $R := \operatorname{Ker}\Phi_i$. Per la definizione 1.9 si ha che $\langle R\rangle = \operatorname{Ker}\Phi_i$ ma allora, ricordando la proposizione 3.1-(ii), vale che $\operatorname{Ker}\Phi_i \lhd FX$ è un sottogruppo normale tale che $\langle R\rangle \subseteq \operatorname{Ker}\Phi_i$ e dunque, per l'osservazione 4.13, si ottiene che $\langle R\rangle^{FX} \subseteq \operatorname{Ker}\Phi_i$. D'altra parte, ancora per l'osservazione 4.13, si ha che $\langle R\rangle \subseteq \langle R\rangle^{FX}$ e di conseguenza, tenendo a mente che $\langle R\rangle = \operatorname{Ker}\Phi_i$, si ottiene che $\langle R\rangle^{FX} = \operatorname{Ker}\Phi_i$ per doppia inclusione. A questo punto basta utilizzare il fatto che $FX/\operatorname{Ker}\Phi_i \simeq G$ assieme alla definizione 4.9 per poter concludere che $G \simeq \langle X|R\rangle$. Sempre per la definizione 4.9, questo mi dà la tesi. □

Osservazione 4.15. La dimostrazione costruttiva della proposizione 4.5, cioè della proprietà universale dei gruppi liberi e la dimostrazione del corollario 4.2 forniscono un procedimento algoritmico per determinare la presentazione (X, R) di un dato gruppo G. Si hanno tre passi:

1. Scelgo un insieme di generatori X per G.
2. Considero l'omomorfismo $\Phi_i\colon FX \to G$ definito da $\Phi_i([abc\dots z]) := a\cdot b\cdot c\cdots z$.
3. Calcolo il nucleo di Φ_i e determino un insieme di generatori R per $\operatorname{Ker}\Phi_i$.

Esempio 4.6. Applico la procedura descritta nell'osservazione 4.15 al gruppo $\mathbb{Z}_n$ con l'usuale operazione di somma $+$ e con elemento neutro $\bar 0$. È noto che $\mathbb{Z}_n$ è un gruppo ciclico generato da un qualunque $x \in \mathbb{N}^*$ tale che $\operatorname{MCD}(x, n) = 1$. Posso dunque scegliere $X := \{x\}$. Si consideri ora l'omomorfismo $\Phi_i\colon FX \to \mathbb{Z}_n$ definito dalla condizione $\Phi_i([x^k]) := k\cdot\bar x$ e, ricordando il[18] lemma di Euclide assieme a una proprietà delle potenze, si osservi che il nucleo dell'applicazione Φ_i è dato dalla condizione seguente:

$$\begin{aligned}
\operatorname{Ker}\Phi_i &= \{\,[x^k] \in FX \mid \Phi_i([x^k]) = \bar 0\,\}\\
&= \{\,[x^k] \in FX \mid k\cdot\bar x = \bar 0\,\}\\
&= \{\,[x^k] \in FX \mid n \text{ divide } kx\,\}\\
&= \{\,[x^k] \in FX \mid n \text{ divide } k\,\}\\
&= \{\,[x^k] \in FX \mid k = nh\,,\ \exists\, h \in \mathbb{Z}\,\}\\
&= \{\,[x^n]^h \in FX \mid h \in \mathbb{Z}\,\} = \langle [x^n]\rangle
\end{aligned}$$

Dalla relazione ottenuta deduco in particolare che il nucleo di Φ_i è un gruppo ciclico e che un insieme di generatori per $\operatorname{Ker}\Phi_i$ è dato semplicemente da $R := \{[x^n]\}$. Posso dunque concludere che $\mathbb{Z}_n \simeq \langle x|x^n\rangle$. Inoltre, utilizzando il fatto che $FX = \mathbb{F}_1$, che $\mathbb{F}_1$ è un gruppo abeliano per l'osservazione 4.11 e ricordando l'osservazione 2.6, si ha che $\langle R\rangle \lhd \mathbb{F}_1$ è un sottogruppo normale. Ma allora, in virtù dell'osservazione 4.13, vale per doppio contenimento che $\langle R\rangle^{FX} = \langle R\rangle$ e dunque, passando al quoziente, si ha che la classe di $[x^n]$ coincide con quella di $[1]$. In altre parole nel quoziente, che per la definizione 4.9 è il gruppo $\langle x|x^n\rangle$, si ha la relazione $x^n = 1$. Lo stesso discorso si può ripetere, più in generale, per qualsiasi gruppo $\langle X|R\rangle$.

Esempio 4.7. Il gruppo diedrale finito D_n è isomorfo ai gruppi $\langle x, y|x^2, y^2, (xy)^n\rangle$ e $\langle x, y|x^n, y^2, xyxy\rangle$. Si osservi, innanzitutto, che questi ultimi sono in realtà lo stesso gruppo. Si consideri infatti il primo di tali gruppi. Ponendo $a := xy$, $b := y$, posso ottenere x dal prodotto $(xy)y$ poiché vale la relazione $y^2 = 1$. Di conseguenza, anche a e b sono generatori e quindi $\langle x, y|x^2, y^2, (xy)^n\rangle = \langle a, b|abab, b^2, a^n\rangle$. Si definisca G tale gruppo e si assuma, almeno per il momento, che $n \geq 3$. Si osservi che b è un generatore di ordine 2. Se infatti fosse stato $o(b) = 1$, per esempio, allora b sarebbe apparso nell'insieme delle relazioni del gruppo, sostituendo b^2. Allo stesso modo, si ha che a è un elemento di ordine n. Adesso dalla relazione $abab = 1$ ricavo che $bab = a^{-1}$, ma essendo $b^2 = 1$ ciò equivale a richiedere che $bab^{-1} = a^{-1}$. Sono dunque verificate tutte le ipotesi dell'osservazione 2.29, in virtù della quale esiste un epimorfismo $f\colon D_n \to G$. Deduco in particolare che $|G| \leq 2n$, ma allora si ha la seguente descrizione di G con elementi a due a due distinti:

$$G = \{\,a^i, a^ib \mid 0 \leq i \leq n-1\,\}$$

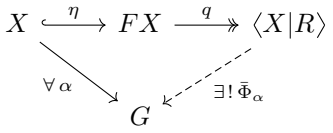
[18] Riporto l'enunciato: siano $a, b, c \in \mathbb{Z}$ tali che $\operatorname{MCD}(a, b) = 1$. Se $a \mid bc$, allora $a \mid c$. La dimostrazione di questo risultato è stata già affrontata nel corso AL110.

Il fatto che gli elementi di tale descrizione siano tutti distinti è una conseguenza immediata delle relazioni sul gruppo G e del fatto che $0 \leq i \leq n-1$. Si può dimostrare più precisamente distinguendo i vari casi e procedendo per assurdo. Alla fine si ottiene che $|G| = 2n$ e l'osservazione 2.29 mi permette di concludere che $f\colon D_n \to G$ è un isomorfismo.

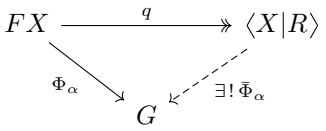
Proposizione 4.6 (Proprietà universale del gruppo $\langle X|R\rangle$)**.** *Sia X un alfabeto e sia G un gruppo. Sia inoltre $\eta\colon X \to FX$ l'applicazione definita da $\eta(x) := [x]$ e, per ogni mappa $\alpha\colon X \to G$, sia $\Phi_\alpha\colon FX \to G$ l'omomorfismo tale che $\Phi_\alpha \circ \eta = \alpha$. Siano infine $R \subseteq FX$ un insieme, $\mathcal{A} := \{\, \alpha\colon X \to G \mid R \subseteq \operatorname{Ker}\Phi_\alpha \,\}$ e sia $q\colon FX \to \langle X|R\rangle$ la mappa quoziente. Allora $q \circ \eta$ soddisfa la seguente proprietà universale:*

$$\forall\, \alpha \in \mathcal{A} \text{ applicazione } \exists!\, \bar{\Phi}_\alpha\colon \langle X|R\rangle \to G \text{ omomorfismo } \mid\ \bar{\Phi}_\alpha \circ (q \circ \eta) = \alpha$$

Equivalentemente, il seguente diagramma di applicazioni è commutativo:



Dimostrazione. Innanzitutto si osservi che, per ogni mappa $\alpha\colon X \to G$, l'omomorfismo $\Phi_\alpha\colon FX \to G$ tale che $\Phi_\alpha \circ \eta = \alpha$ esiste ed è unico per la proprietà universale dei gruppi liberi, vale a dire la proposizione 4.5. Sia adesso $\alpha \in \mathcal{A}$ un'applicazione prefissata. Per definizione di $\mathcal{A}$, si ha che $R \subseteq \operatorname{Ker}\Phi_\alpha$, mentre in virtù della proposizione 3.1-(ii) vale che $\operatorname{Ker}\Phi_\alpha \lhd FX$ è un sottogruppo normale. Dall'osservazione 4.13 segue quindi, per minimalità, che $\langle R\rangle^{FX} \subseteq \operatorname{Ker}\Phi_\alpha$. Posso quindi applicare la proprietà universale dei quozienti (proposizione 3.2-(ii)) all'omomorfismo Φ_α, ottenendo che esiste un'unico omomorfismo $\bar{\Phi}_\alpha\colon \langle X|R\rangle \to G$ tale che $\bar{\Phi}_\alpha \circ q = \Phi_\alpha$. Il diagramma che segue riassume l'utilizzo della proprietà universale dei quozienti:



Infine, per costruzione e per associatività dell'operazione di composizione di applicazioni, vale la relazione:

$$\bar{\Phi}_\alpha \circ (q \circ \eta) = (\bar{\Phi}_\alpha \circ q) \circ \eta = \Phi_\alpha \circ \eta = \alpha$$

L'unicità dell'omomorfismo $\bar{\Phi}_\alpha$ che soddisfi le proprietà desiderate segue immediatamente dall'unicità di Φ_α e dalla proprietà universale dei quozienti. □

Definizione 4.10. Un gruppo G si dice *finitamente generato* se ammette una presentazione (X, R) con $|X| < +\infty$, si dice invece *finitamente presentato* se ammette una presentazione (X, R) con $|X|, |R| < +\infty$.

Osservazione 4.16. Si può mostrare che ogni gruppo finito è finitamente presentato. Si consideri infatti un gruppo finito G e si definiscano $X := G$, $R := \{\, [abc^{-1}] \in FX \mid a \cdot b = c \,\} \cap \{\, [g\hat{g}] \in FX \mid g \in G \,\}$, dove $\hat{g}$ denota l'inverso formale di g in X^{-1} per distinguerlo dall'inverso effettivo in FX. La proposizione 4.6, cioè la proprietà universale del gruppo $\langle X|R\rangle$, garantisce l'esistenza di un epimorfismo dal gruppo $\langle X|R\rangle$ su G. Basta infatti scegliere $\alpha := \mathrm{id}_X$ e osservare che, per la definizione di Φ_α fornita nella dimostrazione costruttiva della proprietà universale dei gruppi liberi (proposizione 4.5), per ogni $[abc^{-1}] \in R$ si ha che:

$$\Phi_\alpha([abc^{-1}]) = \alpha(a) \cdot \alpha(b) \cdot \alpha(c)^{-1} = \mathrm{id}_X(a) \cdot \mathrm{id}_X(b) \cdot \mathrm{id}_X(c)^{-1} = a \cdot b \cdot c^{-1} = c \cdot c^{-1} = 1$$

Sono dunque soddisfatte tutte le ipotesi della proposizione 4.6 e quindi, dette $\eta\colon X \to FX$ l'applicazione data da $\eta(x) := [x]$, $q\colon FX \to \langle X|R\rangle$ la mappa quoziente, esiste un unico omomorfismo $\bar{\Phi}_\alpha\colon \langle X|R\rangle \to G$ tale che $\bar{\Phi}_\alpha \circ (q \circ \eta) = \alpha$, cioè tale che $\bar{\Phi}_\alpha \circ (q \circ \eta) = \mathrm{id}_X$, ma allora $\bar{\Phi}_\alpha$ è un epimorfismo perché ammette un'inversa a destra. La dimostrazione del fatto che $\bar{\Phi}_\alpha$ è un'applicazione iniettiva, dunque un isomorfismo, non verrà invece trattata.

Esempio 4.8. Sia $n \in \mathbb{N}$, $n \geq 2$, si considerino il gruppo simmetrico S_n e un alfabeto $X = \{x_1, \dots, x_{n-1}\}$. Per semplicità, definisco inoltre il seguente sottoinsieme del gruppo libero FX:

$$R := A \cup B \cup C\,, \qquad \text{dove} \qquad \begin{aligned} A &:= \{\, [x_i^2] \mid 1 \leq i \leq n-1 \,\}\,, \\ B &:= \{\, [(x_i x_{i+1})^3] \mid 1 \leq i \leq n-2 \,\}\,, \\ C &:= \{\, [x_i x_j x_i^{-1} x_j^{-1}] \mid 1 \leq i, j \leq n\,,\ j \neq i \pm 1 \,\} \end{aligned}$$

Si considerino ora le due applicazioni $\eta\colon X \to FX$, $\alpha\colon X \to S_n$ definite da $\eta(x_i) := [x_i]$, $\alpha(x_i) := (i\ i+1)$ per ogni $1 \leq i \leq n-1$. Dalla proprietà universale dei gruppi liberi (proposizione 4.5), segue che esiste un unico omomorfismo $\Phi_\alpha\colon FX \to S_n$ tale che $\Phi_\alpha \circ \eta = \alpha$. Per la dimostrazione costruttiva di tale risultato e per definizione di α si ha la condizione $\Phi_\alpha([x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \cdots x_{i_k}^{\pm 1}]) := (i_1\ i_1+1) \circ (i_2\ i_2+1) \circ \cdots \circ (i_k\ i_k+1)$. Dimostro che $R \subseteq \operatorname{Ker} \Phi_\alpha$. Naturalmente, si procede per casi. Innanzitutto, fisso un indice $1 \leq i \leq n-1$ e, ricordando come si è definita l'operazione binaria $\cdot$ su FX, utilizzando il fatto che le trasposizioni sono permutazioni di ordine 2 e usando il fatto che Φ_α è un omomorfismo, noto che vale la condizione seguente:

$$\Phi_\alpha([x_i^2]) = \Phi_\alpha([x_i]^2) = \Phi_\alpha([x_i])^2 = (i\ i+1)^2 = \mathrm{id}_{\{1,\dots,n\}}$$

Sia adesso fissato $1 \leq i \leq n-2$. Per le stesse motivazioni date nel caso precedente, con la differenza che qui utilizzo il fatto che i cicli di lunghezza 3 sono permutazioni di ordine 3, si ricava la relazione seguente:

$$\Phi_\alpha\big([(x_i x_{i+1})^3]\big) = \Phi_\alpha([x_i x_{i+1}])^3 = \big((i\ i+1) \circ (i+1\ i+2)\big)^3 = (i\ i+1\ i+2)^3 = \mathrm{id}_{\{1,\dots,n\}}$$

Siano infine $1 \leq i, j \leq n$, $j \neq i \pm 1$. Usando come al solito il fatto che Φ_α è un omomorfismo, si ricava che:

$$\Phi_\alpha([x_i x_j x_i^{-1} x_j^{-1}]) = (i\ i+1) \circ (j\ j+1) \circ (i\ i+1) \circ (j\ j+1) = \mathrm{id}_{\{1,\dots,n\}}$$

Per arbitrarietà delle relazioni ottenute, posso affermare che $R \subseteq \operatorname{Ker} \Phi_\alpha$. A questo punto si può applicare la proprietà universale del gruppo $\langle X|R\rangle$ e così facendo ottengo un unico omomorfismo $\bar{\Phi}_\alpha\colon \langle X|R\rangle \to S_n$ tale che, detta $q\colon FX \to \langle X|R\rangle$ la mappa quoziente, valga la condizione $\bar{\Phi}_\alpha \circ (q \circ \eta) = \alpha$. Adesso osservo che $(i\ i+1) \in \operatorname{Im} \bar{\Phi}_\alpha$ per ogni $1 \leq i \leq n-1$. Si ha infatti che $\alpha(x_i) = (i\ i+1)$ e di conseguenza, usando il fatto che $\bar{\Phi}_\alpha \circ (q \circ \eta) = \alpha$, vale che $\bar{\Phi}_\alpha\big((q \circ \eta)(x_i)\big) = (i\ i+1)$. Sarà dunque sufficiente dimostrare che $S_n = \langle (1\,2), (2\,3), \dots, (n-1\ n)\rangle$. È noto che S_n è generato dalle trasposizioni e quindi basterà far vedere che una qualsiasi trasposizione si può esprimere come prodotto di trasposizioni della forma $(i\ i+1)$ con $1 \leq i \leq n-1$. Sia $(a\ b) \in S_n$ una trasposizione fissata e si assuma, senza perdita di generalità, che $a < b$. Posto $k := b - a$, si procede per induzione su $k \in \{1, \dots, n-1\}$. La base di induzione, corrispondente al caso $k = 1$, è banale in quanto $(a\ b) = (a\ a+1)$. Assumo quindi $k \geq 2$, suppongo che l'asserto sia vero per $k-1$ e ne dimostro la validità per k. Considero la seguente identità, vera in virtù dell'osservazione 3.16:

$$(a\ b) = (a\ a+1) \circ (a+1\ b) \circ (a\ a+1)$$

Dal momento che $b - (a+1) = k - 1 < k$, per ipotesi induttiva la trasposizione $(a+1\ b)$ si può esprimere come prodotto di trasposizioni della forma $(i\ i+1)$ con $1 \leq i \leq n-1$, ma allora lo stesso vale anche per $(a\ b)$ in virtù della formula precedente. Dalla discussione appena terminata segue che $\bar{\Phi}_\alpha$ è una funzione suriettiva, dunque un epimorfismo. È possibile dimostrare che $\bar{\Phi}_\alpha$ è anche iniettiva, ma la giustificazione di questo fatto verrà tralasciata. In definitiva, dunque, l'applicazione $\bar{\Phi}_\alpha\colon \langle X|R\rangle \to S_n$ è un isomorfismo. In particolare, il gruppo simmetrico S_n è finitamente generato.

Esempio 4.9. Sia $n \in \mathbb{N}^*$ fissato, si consideri un campo K e il gruppo $\mathrm{SL}_n(K)$. È immediato verificare che $\{\pm I_n\} \lhd \mathrm{SL}_n(K)$ e posso quindi considerare il gruppo quoziente $\mathrm{SL}_n(K)/\{\pm I_n\}$, che prende il nome di *gruppo proiettivo lineare speciale di ordine n a coefficienti in K* e si denota $\mathrm{PSL}_n(K)$. Un fatto rilevante in teoria dei numeri e che non verrà dimostrato è che $\mathrm{PSL}_2(\mathbb{Z})$ ammette una presentazione finita anche se è un gruppo infinito. Si può infatti provare che l'applicazione $\Phi\colon \langle x, y | x^2, (xy)^3\rangle \to \mathrm{PSL}_2(\mathbb{Z})$ definita dalle condizioni $\Phi(x) := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $\Phi(y) := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ è un isomorfismo di gruppi.

4.4 Prodotto diretto

Definizione 4.11. Sia $\{X_i\}_{i \in I}$ una collezione, finita oppure infinita, di insiemi. L'insieme delle collezioni $\{x_i\}_{i \in I}$, con $x_i \in X_i$ al variare di $i \in I$, viene detto il *prodotto cartesiano di* $\{X_i\}_{i \in I}$ e si denota $\prod_{i \in I} X_i$. Se poi $I = \{1, \dots, n\}$ è un insieme finito, il prodotto cartesiano di $\{X_i\}_{i \in I}$ si denota anche $X_1 \times \cdots \times X_n$.

Nel risultato che segue si considererà una collezione di gruppi. Per semplicità, le operazioni binarie su tali gruppi verranno indicate con lo stesso simbolo anche se, a priori, esse potranno essere anche distinte.

Osservazione 4.17. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione, finita oppure infinita, di gruppi e sia $\cdot$ l'operazione binaria su $\prod_{i\in I} G_i$ definita dalla condizione $\{g_i\}_{i\in I} \cdot \{g_i'\}_{i\in I} := \{g_i \cdot g_i'\}_{i\in I}$. Allora il prodotto cartesiano $\prod_{i\in I} G_i$ munito dell'operazione binaria $\cdot$ appena definita è un gruppo che ha per elemento neutro $\{e_i\}_{i\in I}$.

Dimostrazione. La buona definizione dell'operazione binaria $\cdot$ su $\prod_{i\in I} G_i$ segue immediatamente dal fatto che le operazioni binarie sui singoli gruppi G_i sono tutte, al variare dell'indice $i \in I$, ben definite. Adesso l'esistenza dell'elemento neutro e degli inversi deriva banalmente dalla definizione dell'operazione binaria $\cdot$ su $\prod_{i\in I} G_i$ e dall'ipotesi che G_i è un gruppo con elemento neutro e_i per ogni $i \in I$. Più esplicitamente si hanno, per ogni scelta di una collezione $\{g_i\}_{i\in I} \in \prod_{i\in I} G_i$, le condizioni seguenti:

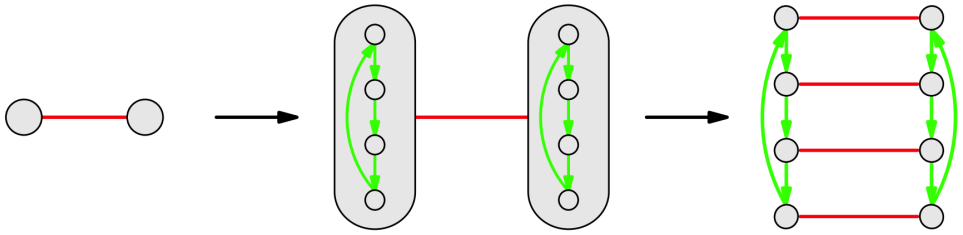
$$\{g_i\}_{i\in I} \cdot \{e_i\}_{i\in I} = \{g_i \cdot e_i\}_{i\in I} = \{g_i\}_{i\in I}$$
$$\{e_i\}_{i\in I} \cdot \{g_i\}_{i\in I} = \{e_i \cdot g_i\}_{i\in I} = \{g_i\}_{i\in I}$$

Questo dimostra che $\{e_i\}_{i\in I}$ è un elemento neutro. Comunque fissata una collezione $\{g_i\}_{i\in I} \in \prod_{i\in I} G_i$ si ha inoltre la condizione $\{g_i\}_{i\in I}^{-1} = \{g_i^{-1}\}_{i\in I}$, come dimostrano le due relazioni che seguono:

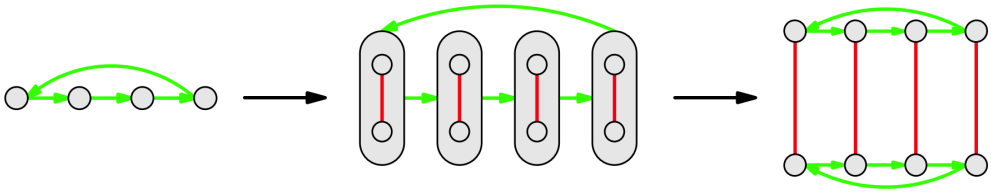
$$\{g_i\}_{i\in I} \cdot \{g_i^{-1}\}_{i\in I} = \{g_i \cdot g_i^{-1}\}_{i\in I} = \{e_i\}_{i\in I}$$
$$\{g_i^{-1}\}_{i\in I} \cdot \{g_i\}_{i\in I} = \{g_i^{-1} \cdot g_i\}_{i\in I} = \{e_i\}_{i\in I}$$

Dalla discussione precedente e dalla definizione di gruppo segue dunque la tesi. □

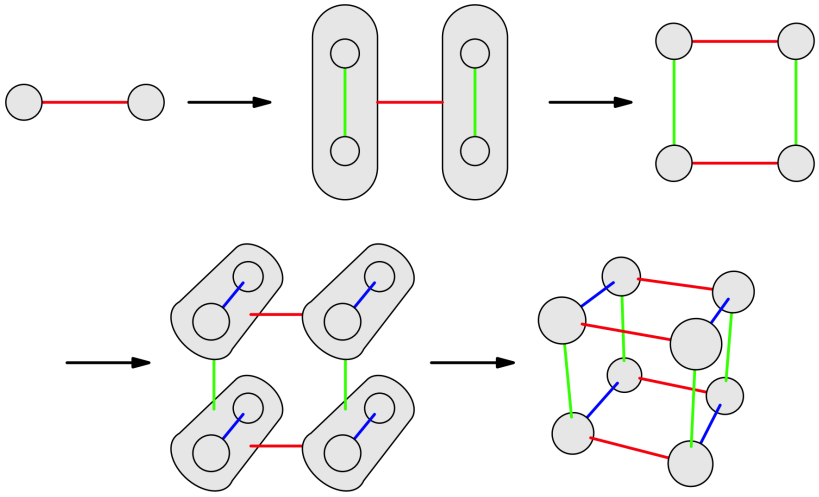
Definizione 4.12. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione, finita oppure infinita, di gruppi. Il gruppo $\prod_{i\in I} G_i$ munito dell'operazione binaria $\cdot$ definita nell'osservazione 4.17 e dell'elemento neutro $\{e_i\}_{i\in I}$ viene detto il *prodotto diretto esterno* (o il *prodotto diretto*, o più semplicemente il *prodotto*) *di* $\{G_i\}_{i\in I}$.



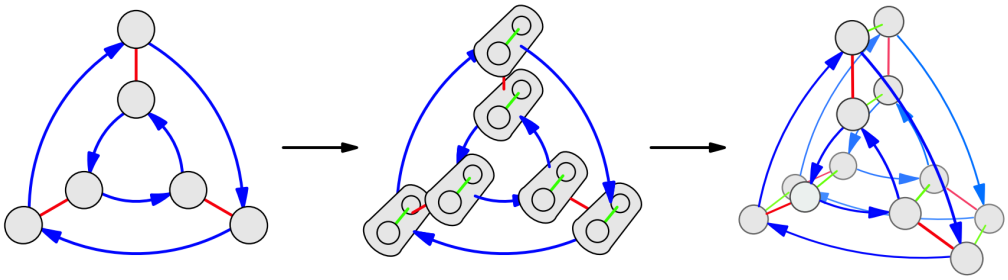
In figura viene visualizzato, in maniera intuitiva, il gruppo dato dal prodotto di $\mathbb{Z}_2$ con $\mathbb{Z}_4$, ambedue considerati con l'usuale operazione additiva $+$ e con elemento neutro $\bar{0}$. Al primo passo si considera semplicemente il gruppo $\mathbb{Z}_2$, dopodiché si sostituisce a ciascun nodo che compare nel diagramma di $\mathbb{Z}_2$ una copia di $\mathbb{Z}_4$. Infine il segmento rosso, che rappresenta la somma per un generatore di $\mathbb{Z}_2$, viene duplicato al fine di connettere i nodi corrispondenti delle due copie di $\mathbb{Z}_4$.



In questo caso, invece, si considera dapprima il gruppo $\mathbb{Z}_4$, poi ciascun nodo viene sostituito da una copia di $\mathbb{Z}_2$ e infine le frecce verdi, che indicano la somma per l'elemento $\bar{1}$ in $\mathbb{Z}_4$, vengono moltiplicate allo scopo di connettere i nodi corrispondenti delle quattro copie di $\mathbb{Z}_2$. Si osservi che il diagramma raffigurante il prodotto diretto $\mathbb{Z}_4 \times \mathbb{Z}_2$ è essenzialmente identico a quello che rappresenta il prodotto $\mathbb{Z}_2 \times \mathbb{Z}_4$. In effetti, sebbene formalmente i due oggetti siano distinti, vi è un isomorfismo naturale tra essi.



Stavolta, prima si applica il prodotto diretto di $\mathbb{Z}_2$ con se stesso, poi il prodotto di $\mathbb{Z}_2 \times \mathbb{Z}_2$ con $\mathbb{Z}_2$. Il procedimento seguito è identico a quello descritto nei casi precedenti. In questo caso, chiaramente, il risultato finale è il prodotto diretto esterno $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.



Infine, viene raffigurato lo stesso processo con il gruppo simmetrico S_3 il quale, diversamente da $\mathbb{Z}_2$ e da $\mathbb{Z}_4$, non è un gruppo ciclico. Ciononostante, l'idea che si cela dietro il prodotto diretto esterno rimane la stessa e pertanto la sequenza può essere interpretata seguendo le stesse indicazioni date nei casi precedenti. Ciò che si ottiene alla fine è il prodotto diretto $S_3 \times \mathbb{Z}_2$.

Osservazione 4.18. Siano $\{G_i\}_{i\in I}$ una collezione di gruppi, $k \in I$ un indice fissato e si consideri la funzione $\pi_k \colon \prod_{i\in I} G_i \to G_k$ definita da $\pi_k(\{g_i\}_{i\in I}) := g_k$, detta la *proiezione canonica sulla componente k-esima*. Si tratta di un omomorfismo di gruppi, poiché soddisfa per ogni $\{g_i\}_{i\in I}, \{g'_i\}_{i\in I} \in \prod_{i\in I} G_i$ la condizione:

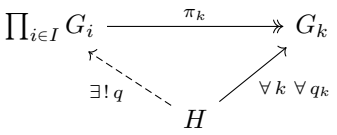
$$\pi_k(\{g_i\}_{i\in I} \cdot \{g'_i\}_{i\in I}) = \pi_k(\{g_i \cdot g'_i\}_{i\in I}) = g_k \cdot g'_k = \pi_k(\{g_i\}_{i\in I}) \cdot \pi_k(\{g'_i\}_{i\in I})$$

Più precisamente, la proiezione canonica π_k è un epimorfismo in quanto applicazione suriettiva. È infatti evidente che, comunque venga fissato $g_k \in G_k$, la collezione $\{x_i\}_{i\in I}$ definita da $x_i := g_k$ se $i = k$, $x_i := e_i$ altrimenti è tale che $\pi_k(\{x_i\}_{i\in I}) = g_k$. Non è invece, in generale, un'applicazione iniettiva, poiché non è detto che la suddetta collezione sia unica.

Proposizione 4.7 (Proprietà universale del prodotto diretto)**.** *Siano $\{(G_i, \cdot, e_i)\}_{i\in I}$ una data collezione di gruppi, $(H, \star, e)$ un gruppo e sia $\{\pi_k \colon \prod_{i\in I} G_i \to G_k\}_{k\in I}$ la famiglia delle proiezioni canoniche. Allora la suddetta famiglia soddisfa la seguente proprietà universale:*

$$\forall\, \{q_k \colon H \to G_k\}_{k\in I} \text{ famiglia di omomorfismi } \exists!\, q \colon H \to \prod_{i\in I} G_i \text{ omomorfismo } \mid \pi_k \circ q = q_k \ \ \forall\, k \in I$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



Dimostrazione. Sia $\{ q_k \colon H \to G_k \}_{k \in I}$ una famiglia di omomorfismi e sia $q \colon H \to \prod_{i \in I} G_i$ l'applicazione definita semplicemente da $q(h) := \{q_i(h)\}_{i \in I}$. Si tratta di una mappa ben definita poiché, per ogni $k \in I$, l'applicazione q_k ha immagine in G_k. Inoltre, dall'ipotesi che q_k sia un omomorfismo per ogni $k \in I$ segue che lo è anche q. Infatti, per ogni $h, h' \in H$, sussiste la condizione seguente:

$$q(h \star h') = \{q_i(h \star h')\}_{i \in I} = \{q_i(h) \cdot q_i(h')\}_{i \in I} = \{q_i(h)\}_{i \in I} \cdot \{q_i(h')\}_{i \in I} = q(h) \cdot q(h')$$

Infine, l'omomorfismo q soddisfa per costruzione la condizione $\pi_k \circ q = q_k$ per ogni $k \in I$. Si consideri ora una qualunque funzione $q' \colon H \to \prod_{i \in I} G_i$ tale che $\pi_k \circ q' = q_k$ per ogni $k \in I$ e si fissi un elemento $h \in H$. Sia inoltre $\{g_i\}_{i \in I} := q'(h)$. Allora, comunque venga fissato un indice $k \in I$, si ha la condizione seguente:

$$g_k = \pi_k\big(q'(h)\big) = (\pi_k \circ q')(h) = q_k(h) = (\pi_k \circ q)(h) = \pi_k\big(q(h)\big) = q_k(h)$$

Di conseguenza, si ha che $q'(h) = \{q_i(h)\}_{i \in I}$, cioè che $q'(h) = q(h)$ e dunque, per arbitrarietà nella scelta dell'elemento $h \in H$, vale che $q' = q$. Non dipendendo il risultato ottenuto da una particolare scelta della funzione $q' \colon H \to \prod_{i \in I} G_i$, posso concludere che l'omomorfismo q è unico e quindi si ha la tesi. □

Anche per la proprietà universale dei prodotti diretti vale un fatto simile all'osservazione 3.6. Segue ora una caratterizzazione del prodotto diretto che permette di cambiare punto di vista. Finora si è visto che, dati due gruppi qualsiasi, è sempre possibile costruire un nuovo gruppo a partire da essi, poiché basta considerarne il prodotto cartesiano e attribuire a questo una naturale struttura di gruppo. Adesso, dato un gruppo, si vuole capire sotto quali condizioni questo si possa esprimere come il prodotto diretto di due suoi sottogruppi.

Proposizione 4.8 (Caratterizzazione interna del prodotto diretto)**.** *Siano $(G_1, \cdot, e_1)$, $(G_2, \cdot, e_2)$, $(G, \star, e)$ gruppi. Allora $G \simeq G_1 \times G_2$ se e solo se esistono sottogruppi $H_1, H_2 < G$ con $H_1 \simeq G_1$, $H_2 \simeq G_2$ tali che:*

(i) $H_1 H_2 = G$.

(ii) $H_1 \cap H_2 = \{e\}$.

(iii.a) *H_1 e H_2 commutano, cioè $h_1 \star h_2 = h_2 \star h_1$ per ogni $h_1 \in H_1$, $h_2 \in H_2$.*

Equivalentemente, si ha che $G \simeq G_1 \times G_2$ se e solo se esistono due sottogruppi $H_1, H_2 < G$ con $H_1 \simeq G_1$, $H_2 \simeq G_2$ che soddisfino le condizioni (i), (ii) e quella che segue al posto della (iii.a):

(iii.b) *$H_1, H_2 \lhd G$ sono sottogruppi normali.*

Dimostrazione. Suppongo che $G \simeq G_1 \times G_2$. In tal caso, esiste un isomorfismo $f \colon G_1 \times G_2 \to G$ e posso considerare le due restrizioni $f_1 \colon G_1 \times \{e_2\} \to G$, $f_2 \colon \{e_1\} \times G_2 \to G$. Tali funzioni ereditano banalmente da f la proprietà di essere omomorfismi di gruppi e l'iniettività. Definisco quindi $H_1 := \operatorname{Im} f_1$, $H_2 := \operatorname{Im} f_2$ e osservo che $H_1, H_2 < G$ sono due sottogruppi in virtù della proposizione 3.1-(i). Si considerino adesso le mappe inclusione $i_1 \colon H_1 \to G$, $i_2 \colon H_2 \to G$. Per la proposizione 3.2-(i), vale a dire la proprietà universale delle inclusioni, esistono e sono unici due omomorfismi $\tilde{f}_1 \colon G_1 \times \{e_2\} \to H_1$, $\tilde{f}_2 \colon \{e_1\} \times G_2 \to H_2$ tali che $i_1 \circ \tilde{f}_1 = f_1$ e $i_2 \circ \tilde{f}_2 = f_2$. Dimostro che $\tilde{f}_1$ è un isomorfismo e con un procedimento del tutto analogo si vede facilmente che lo è anche $\tilde{f}_2$. Dati $x_1, x_2 \in G_1 \times \{e_2\}$ tali che $\tilde{f}_1(x_1) = \tilde{f}_1(x_2)$, vale equivalentemente che $f_1(x_1) = f_1(x_2)$ per la condizione $i_1 \circ \tilde{f}_1 = f_1$, ma allora $x_1 = x_2$ perché f_1 è iniettiva. Dato invece un elemento $h \in H_1$, per definizione di H_1 esiste $x \in G_1 \times \{e_2\}$ tale che $f_1(x) = h$ e quindi anche $\tilde{f}_1(x) = h$ in virtù della condizione $i_1 \circ \tilde{f}_1 = f_1$. Avendo quindi mostrato che l'applicazione $\tilde{f}_1$ è iniettiva e suriettiva, si può affermare che $\tilde{f}_1 \colon G_1 \times \{e_2\} \to H_1$ è un isomorfismo. Dalla discussione precedente e dall'isomorfismo banale $G_1 \times \{e_2\} \simeq G_1$ segue dunque che $H_1 \simeq G_1$. Ragionando esattamente allo stesso modo si ottiene che $H_2 \simeq G_2$. A questo punto bisogna dimostrare la validità delle condizioni (i), (ii), (iii.a) e (iii.b).

(i) Innanzitutto, è evidente che $H_1 H_2 \subseteq G$ in quanto $H_1 H_2 \subseteq GG$ essendo $H_1, H_2 \subseteq G$ e $GG \subseteq G$ per chiusura dell'operazione binaria $\star$ su G. Sia adesso $g \in G$. Usando il fatto che f è un isomorfismo, esiste un elemento $(g_1, g_2) \in G_1 \times G_2$ tale che $f(g_1, g_2) = g$ e inoltre vale la condizione seguente:

$$\begin{aligned} g = f(g_1, g_2) = f(g_1 \cdot e_1, e_2 \cdot g_2) = f\big((g_1, e_2) \cdot (e_1, g_2)\big) = f(g_1, e_2) \star f(e_1, g_2) \\ = f_1(g_1, e_2) \star f_2(e_1, g_2) = \tilde{f}_1(g_1, e_2) \star \tilde{f}_2(e_1, g_2) \end{aligned}$$

Questo dimostra che $g \in H_1 H_2$ e quindi, per arbitrarietà nella scelta di $g \in G$, vale che $G \subseteq H_1 H_2$. Dalla doppia inclusione segue dunque che $H_1 H_2 = G$.

(ii) Innanzitutto, l'inclusione $\{e\} \subseteq H_1 \cap H_2$ è ovvia poiché si è dimostrato che $H_1, H_2 < G$ sono due sottogruppi. Sia quindi $h \in H_1 \cap H_2$. Siccome $h \in H_1$, esiste $g_1 \in G_1$ tale che $f_1(g_1, e_2) = h$ e allo stesso modo, dato che $h \in H_2$, esiste $g_2 \in G_2$ tale che $f_2(e_1, g_2) = h$. Ma allora, in particolare, si ha che $f_1(g_1, e_2) = f_2(e_1, g_2)$ oppure, equivalentemente, che $f(g_1, e_2) = f(e_1, g_2)$ in virtù del fatto che f_1 e f_2 sono restrizioni di f. Per iniettività di f posso quindi affermare che $g_1 = e_1$. A questo punto, basta ricordare che f_1 è un omomorfismo e dunque $f_1(e_1, e_2) = e$ per l'osservazione 3.1, ma al contempo $f_1(e_1, e_2) = h$ in quanto $g_1 = e_1$ e di conseguenza $h = e$. Posso quindi concludere, per arbitrarietà di $h \in H_1 \cap H_2$, che $H_1 \cap H_2 \subseteq \{e\}$ e dunque $H_1 \cap H_2 = \{e\}$ per doppia inclusione.

(iii.a) Siano $h_1 \in H_1$, $h_2 \in H_2$ due elementi prefissati. Dalle definizioni di H_1 e di H_2 segue che esistono $g_1 \in G_1$, $g_2 \in G_2$ tali che $f_1(g_1, e_2) = h_1$, $f_2(e_1, g_2) = h_2$. In particolare, utilizzando come prima il fatto che f_1 e f_2 sono restrizioni di f, si ricava che $f(g_1, e_2) = h_1$, $f(e_1, g_2) = h_2$ e di conseguenza, ricordando che f è un omomorfismo, vale la condizione seguente:

$$\begin{aligned} h_1 \star h_2 &= f(g_1, e_2) \star f(e_1, g_2) = f\big((g_1, e_2) \cdot (e_1, g_2)\big) = f(g_1 \cdot e_1, e_2 \cdot g_2) \\ &= f(e_1 \cdot g_1, g_2 \cdot e_2) = f\big((e_1, g_2) \cdot (g_1, e_2)\big) = f(e_1, g_2) \star f(g_1, e_2) = h_2 \star h_1 \end{aligned}$$

Quanto si è appena dimostrato, naturalmente, non dipende dalla scelta di $h_1 \in H_1$ e di $h_2 \in H_2$.

(iii.b) Dimostro che $H_1 \lhd G$ è un sottogruppo normale. Siano $a \in G$ e $h_1 \in H_1$ fissati. Utilizzando come al solito la definizione di H_1 e il fatto che f è suriettiva, si possono trovare $a_1, g_1 \in G_1$, $a_2 \in G_2$ tali che $f(a_1, a_2) = a$, $f_1(g_1, e_2) = h_1$. A questo punto basta osservare che, per ragioni già discusse nei casi precedenti, si ha anche la condizione $f(g_1, e_2) = h_1$ e dunque, utilizzando il fatto che f è un omomorfismo assieme all'osservazione 3.2, si ottiene la condizione seguente:

$$\begin{aligned} a \star h \star a^{-1} &= f(a_1, a_2) \star f(g_1, e_2) \star f(a_1^{-1}, a_2^{-1}) = f\big((a_1, a_2) \cdot (g_1, e_2) \cdot (a_1^{-1}, a_2^{-1})\big) \\ &= f(a_1 \cdot g_1 \cdot a_1^{-1}, a_2 \cdot e_2 \cdot a_2^{-1}) = f(a_1 \cdot g_1 \cdot a_1^{-1}, e_2) = f_1(a_1 \cdot g_1 \cdot a_1^{-1}, e_2) \end{aligned}$$

Dalla relazione ottenuta segue in particolare che $a \star h \star a^{-1} \in H_1$ e posso dunque affermare, per arbitrarietà nella scelta di $h \in H_1$, che $aH_1a^{-1} \subseteq H_1$. Naturalmente, non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $a \in G$, posso infine concludere che $H_1 \lhd G$ è un sottogruppo normale per definizione. Per dimostrare che anche $H_2 \lhd G$ è un sottogruppo normale si procede esattamente allo stesso modo lavorando con f_2 al posto di f_1.

A questo punto, mi occupo di mostrare il viceversa. Innanzitutto, poiché per ipotesi $H_1 \simeq G_1$, $H_2 \simeq G_2$, si ha che $H_1 \times H_2 \simeq G_1 \times G_2$, come è immediato verificare. Di conseguenza, sarà sufficiente mostrare che $G \simeq H_1 \times H_2$. In un primo momento, assumo le condizioni (i), (ii) e (iii.a). Sia quindi $f\colon H_1 \times H_2 \to G$ l'applicazione definita da $f(h_1, h_2) := h_1 \star h_2$. Si tratta di una mappa ben definita poiché lo è l'operazione binaria $\star$ su G. Si osservi adesso che, fissati $(h_1, h_2), (h_1', h_2') \in H_1 \times H_2$, per la condizione (iii.a) vale che:

$$\begin{aligned} f\big((h_1, h_2) \cdot (h_1', h_2')\big) &= f\big((h_1 \star h_1', h_2 \star h_2')\big) = (h_1 \star h_1') \star (h_2 \star h_2') = h_1 \star (h_1' \star h_2) \star h_2' \\ &= h_1 \star (h_2 \star h_1') \star h_2' = (h_1 \star h_2) \star (h_1' \star h_2') = f(h_1, h_2) \star f(h_1', h_2') \end{aligned}$$

Questo dimostra che f è un omomorfismo. Sia ora $(h_1, h_2) \in \operatorname{Ker} f$. Per definizione, questo significa che $f(h_1, h_2) = e$, cioè che $h_1 \star h_2 = e$. In altre parole, si ha che $h_1 = h_2^{-1}$ e in particolare $h_1, h_2 \in H_1 \cap H_2$. Dunque, ricordando che per ipotesi vale la condizione (ii), si ottiene che $h_1 = h_2 = e$. Non dipendendo il risultato ottenuto da una particolare scelta di $(h_1, h_2) \in \operatorname{Ker} f$, posso affermare che $\operatorname{Ker} f \subseteq \{e\}$. L'altra inclusione è banale perché $\operatorname{Ker} f < H_1 \times H_2$ è un sottogruppo in virtù della proposizione 3.1-(i). Avendo mostrato che $\operatorname{Ker} f = \{e\}$, dalla proposizione 3.1-(ii) ottengo che f è un'applicazione iniettiva. Sia infine $g \in G$ un elemento fissato. Per la condizione (i) si ha che $g \in H_1H_2$ e dunque esistono $h_1 \in H_1$, $h_2 \in H_2$ tali che $g = h_1 \star h_2$. Questo è equivalente a richiedere, per costruzione, che $g = f(h_1, h_2)$ e quindi, siccome l'elemento $g \in G$ è stato scelto in maniera arbitraria, si ottiene che f è un'applicazione suriettiva. Dalla discussione precedente segue dunque che $f\colon H_1 \times H_2 \to G$ è un isomorfismo e questo mi dà la prima parte dell'enunciato.

Adesso suppongo invece che valgano le condizioni (i), (ii) e (iii.b). Sarà sufficiente ricondursi al caso precedente dimostrando che le condizioni (ii) e (iii.b) implicano la (iii.a). Siano quindi $h_1 \in H_1$, $h_2 \in H_2$. Si ricordi innanzitutto che $[h_1, h_2] = h_1 \star h_2 \star h_1^{-1} \star h_2^{-1}$ per definizione. Si noti che $h_2 \star h_1^{-1} \star h_2^{-1} \in H_1$

essendo $H_1 \lhd G$ un sottogruppo normale per l'ipotesi (iii.b) e quindi $[h_1, h_2] \in H_1$ perché vale la relazione $[h_1, h_2] = h_1 \star (h_2 \star h_1^{-1} \star h_2^{-1})$. Analogamente, posso affermare che $h_1 \star h_2 \star h_1^{-1} \in H_2$ perché $H_2 \lhd G$ è un sottogruppo normale per l'ipotesi (iii.b), ma allora $[h_1, h_2] = (h_1 \star h_2 \star h_1^{-1}) \star h_2^{-1}$ e di conseguenza si ha che $[h_1, h_2] \in H_2$. Si ottiene quindi che $[h_1, h_2] \in H_1 \cap H_2$. Equivalentemente, siccome $H_1 \cap H_2 = \{e\}$ in virtù della condizione (ii), posso affermare che $[h_1, h_2] = e$, cioè che $h_1 \star h_2 = h_2 \star h_1$. Per arbitrarietà nella scelta degli elementi $h_1 \in H_1$, $h_2 \in H_2$ si ricava quindi la condizione (iii.a). Essendomi ricondotto al caso precedente, ottengo la tesi. □

Osservazione 4.19. Si dimostra facilmente, per induzione sul numero di fattori nel prodotto diretto, che la proposizione 4.8 vale anche nel caso più generale in cui, anziché considerare solo due gruppi $(G_1, \cdot, e_1)$, $(G_2, \cdot, e_2)$, si considera una collezione $\{(G_i, \cdot, e_i)\}_{i \in I}$ con insieme di indici I numerabile.

Definizione 4.13. Sia G un gruppo. Se esistono sottogruppi $H_1, H_2 < G$ come nella proposizione 4.8, si dice che G è il *prodotto diretto interno di* H_1 *e* H_2.

Osservazione 4.20. Sia $\{G_i\}_{i \in I}$ una data collezione di gruppi e, per ogni $i \in I$, sia $H_i \lhd G_i$ un sottogruppo normale. Allora vale la condizione $\prod_{i \in I} G_i / \prod_{i \in I} H_i \simeq \prod_{i \in I} G_i / H_i$.

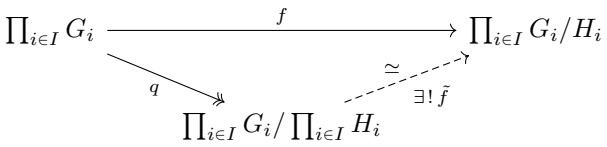
Dimostrazione. Sia $\{ q_i \colon G_i \to G_i/H_i \}_{i \in I}$ la famiglia delle mappe quoziente e si consideri l'applicazione $f \colon \prod_{i \in I} G_i \to \prod_{i \in I} G_i/H_i$ data da $f(\{g_i\}_{i \in I}) := \{q_i(g_i)\}_{i \in I}$. Fissato un elemento $\{y_i\}_{i \in I} \in \prod_{i \in I} G_i/H_i$, per ogni $i \in I$ esiste un elemento $x_i \in G_i$ tale che $q_i(x_i) = y_i$ perché le mappe quoziente sono applicazioni suriettive, ma allora $f(\{x_i\}_{i \in I}) = \{y_i\}_{i \in I}$ e questo dimostra, per arbitrarietà di $\{y_i\}_{i \in I} \in \prod_{i \in I} G_i/H_i$, che f è un'applicazione suriettiva. Date invece due collezioni $\{g_i\}_{i \in I}, \{g_i'\}_{i \in I} \in \prod_{i \in I} G_i$, ricordando come si è definita l'operazione binaria $\cdot$ su $\prod_{i \in I} G_i$ e utilizzando il fatto che le mappe quoziente sono omomorfismi di gruppi, si ottiene la condizione seguente:

$$\begin{aligned} f(\{g_i\}_{i \in I} \cdot \{g_i'\}_{i \in I}) &= f(\{g_i \cdot g_i'\}_{i \in I})_{i \in I} = \{q_i(g_i \cdot g_i')\}_{i \in I} = \{q_i(g_i) \cdot q_i(g_i')\}_{i \in I} \\ &= \{q_i(g_i)\}_{i \in I} \cdot \{q_i(g_i')\}_{i \in I} = f(\{g_i\}_{i \in I}) \cdot f(\{g_i'\}_{i \in I}) \end{aligned}$$

Non dipendendo il risultato ottenuto da una particolare scelta delle collezioni $\{g_i\}_{i \in I}, \{g_i'\}_{i \in I} \in \prod_{i \in I} G_i$, posso affermare che f è un omomorfismo e quindi, essendo f suriettiva, si ottiene che f è un epimorfismo. Calcolo infine il nucleo dell'omomorfismo f:

$$\begin{aligned} \operatorname{Ker} f &= \left\{ \{g_i\}_{i \in I} \in \textstyle\prod_{i \in I} G_i \;\middle|\; f(\{g_i\}_{i \in I}) = \{H_i\}_{i \in I} \right\} \\ &= \left\{ \{g_i\}_{i \in I} \in \textstyle\prod_{i \in I} G_i \;\middle|\; \{q_i(g_i)\}_{i \in I} = \{H_i\}_{i \in I} \right\} \\ &= \left\{ \{g_i\}_{i \in I} \in \textstyle\prod_{i \in I} G_i \;\middle|\; q_i(g_i) = H_i \text{ per ogni } i \in I \right\} \\ &= \left\{ \{g_i\}_{i \in I} \in \textstyle\prod_{i \in I} G_i \;\middle|\; g_i H_i = H_i \text{ per ogni } i \in I \right\} \\ &= \left\{ \{g_i\}_{i \in I} \in \textstyle\prod_{i \in I} G_i \;\middle|\; g_i \in H_i \text{ per ogni } i \in I \right\} \\ &= \left\{ \{g_i\}_{i \in I} \in \textstyle\prod_{i \in I} G_i \;\middle|\; \{g_i\}_{i \in I} \in \prod_{i \in I} H_i \right\} = \textstyle\prod_{i \in I} H_i \end{aligned}$$

Per la proposizione 3.1-(ii) si ha che $\prod_{i \in I} H_i \lhd \prod_{i \in I} G_i$ e dunque il gruppo quoziente $\prod_{i \in I} G_i / \prod_{i \in I} H_i$ è ben definito. A questo punto, se $q \colon \prod_{i \in I} G_i \to \prod_{i \in I} G_i / \prod_{i \in I} H_i$ è la mappa quoziente allora, utilizzando il fatto che f è un epimorfismo, posso applicare l'osservazione 3.7, in virtù della quale esiste uno e un solo isomorfismo $\tilde{f} \colon \prod_{i \in I} G_i / \prod_{i \in I} H_i \to \prod_{i \in I} G_i/H_i$ tale che sia commutativo il diagramma di omomorfismi:



Questo mi dà, in particolare, quanto volevasi dimostrare. □

4.5 Prodotto libero

Per poter definire il prodotto libero di gruppi è indispensabile, innanzitutto, fornire una definizione precisa dell'operatore di unione disgiunta. Il punto cruciale della seguente definizione è che non viene richiesto che

gli insiemi coinvolti nell'unione disgiunta siano effettivamente disgiunti. La disgiunzione, infatti, viene in un certo senso forzata dall'operatore. Nel caso particolare in cui gli insiemi siano disgiunti, poi, vi è una naturale corrispondenza biunivoca tra unione e unione disgiunta.

Definizione 4.14. Sia $\{X_i\}_{i\in I}$ una collezione, finita oppure infinita, di insiemi. Prende il nome di *unione disgiunta di* $\{X_i\}_{i\in I}$ il seguente insieme:

$$\coprod_{i\in I} X_i := \bigcup_{i\in I} \{\, (x,i) \mid x \in X_i \,\}$$

L'idea della definizione 4.14 è che, a differenza dell'unione classica, l'unione disgiunta conserva anche l'informazione sull'insieme dal quale proviene un dato elemento. L'indice ausiliario i permette di risalire, infatti, all'insieme di provenienza X_i di un qualsiasi elemento x.

Definizione 4.15. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione, finita oppure infinita, di gruppi e sia $X := \coprod_{i\in I} G_i$. Una parola $a_1 a_2 \dots a_n$ su X si dice in *forma canonica* se soddisfa le due condizioni seguenti:

(i) Per ogni $1 \leq j \leq n$, se $i_j \in I$ è l'indice tale che $a_j \in G_{i_j}$, allora $a_j \neq e_{i_j}$.

(ii) Per ogni $1 \leq j \leq n-1$, gli elementi a_j e a_{j+1} non provengono dallo stesso gruppo.

L'insieme delle parole in forma canonica su X si denota $\prod^*_{i\in I} G_i$. Se inoltre $I = \{1, \dots, n\}$ è un insieme finito, si pone per semplicità $G_1 * \cdots * G_n := \prod^*_{i\in I} G_i$.

Osservazione 4.21. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione, finita oppure infinita, di gruppi e sia $\cdot$ l'operazione binaria su $\prod^*_{i\in I} G_i$ data dalla giustapposizione di parole seguita dalla riduzione a forma canonica, vale a dire un procedimento che prevede:

(i) Cancellazione degli elementi neutri e_i al variare dell'indice $i \in I$.

(ii) Moltiplicazione delle lettere adiacenti che appartengono allo stesso gruppo.

Allora $\prod^*_{i\in I} G_i$ munito dell'operazione binaria $\cdot$ è un gruppo che ha per elemento neutro la parola vuota 1.

Dimostrazione. Innanzitutto, osservo che l'operazione binaria $\cdot$ su $\prod^*_{i\in I} G_i$ è ben definita in quanto, per costruzione, la giustapposizione di parole seguita dalla riduzione a forma canonica dà luogo a una parola in forma canonica. L'associatività, invece, deriva banalmente dal fatto che l'operazione di giustapposizione di parole è associativa. Si osservi adesso che la parola vuota 1 è una parola in forma canonica, in quanto le condizioni (i) e (ii) sono automaticamente verificate. Ha quindi senso chiedersi se possa essere un elemento neutro per l'operazione binaria $\cdot$ su $\prod^*_{i\in I} G$. È noto per l'osservazione 4.1 che la parola vuota 1 è l'elemento neutro per l'operazione di giustapposizione di parole, ma allora la giustapposizione di una fissata parola $w \in \prod^*_{i\in I} G_i$ con la parola vuota 1 mi restituisce w la quale, essendo già in forma canonica, esce inalterata dal processo di riduzione a forma canonica. Questo dimostra che la parola vuota 1 è anche un elemento neutro per l'operazione binaria $\cdot$ su $\prod^*_{i\in I} G$. Infine, l'inverso di una parola $a_1 a_2 \dots a_n \in \prod^*_{i\in I} G_i$ è dato da $a_n^{-1} \dots a_2^{-1} a_1^{-1}$, come è immediato verificare procedendo per induzione sulla lunghezza della parola. □

Definizione 4.16. Sia $\{G_i\}_{i\in I}$ una collezione, finita oppure infinita, di gruppi. Il gruppo $\prod^*_{i\in I} G_i$ munito dell'operazione binaria $\cdot$ definita nell'osservazione 4.21 e con elemento neutro la parola vuota 1 prende il nome di *prodotto libero* (o *coprodotto*) *di* $\{G_i\}_{i\in I}$.

Esempio 4.10. Siano $(G_1, \cdot, e_1)$, $(G_2, \cdot, e_2)$ gruppi e siano $a_1, b_1, c_1 \in G_1 \setminus \{e_1\}$, $a_2, b_2 \in G_2 \setminus \{e_2\}$. Le due parole $a_1 b_2 c_1, b_1 a_2 \in G_1 * G_2$ sono espresse in forma canonica, ma non lo è la loro giustapposizione. Nelle parole $a_1 b_2 c_1, b_1 a_2$ non può infatti comparire l'elemento neutro poiché questo è stato escluso dalla scelta delle lettere. Inoltre, non compaiono lettere adiacenti appartenenti allo stesso gruppo, come in questo caso suggeriscono gli indici. Sono dunque verificate le condizioni (i) e (ii). Si applichi adesso il procedimento di riduzione a forma canonica alla parola $a_1 b_2 c_1 b_1 a_2$ ottenuta tramite giustapposizione. Innanzitutto, noto che c_1 e b_1 sono lettere adiacenti che appartengono allo stesso gruppo e quindi le moltiplico, ottenendo la parola $a_1 b_2 (c_1 \cdot b_1) a_2$. Se $c_1 \cdot b_1 \neq e_1$, allora ho ottenuto una parola in forma canonica e quindi mi fermo. Se invece $c_1 \cdot b_1 = e_1$, allora dovrò cancellare questo termine, ottenendo la parola $a_1 b_2 a_2$. Adesso osservo che le lettere b_2 e a_2 sono adiacenti e appartenenti allo stesso gruppo, quindi vanno moltiplicate e si trova la parola $a_1 (b_2 \cdot a_2)$. Questa è in forma canonica se $b_2 \cdot a_2 \neq e_2$ altrimenti, se $b_2 \cdot a_2 = e_2$, la lettera deve essere cancellata e si ottiene la parola a_1, che è in forma canonica.

Osservazione 4.22. Siano $\{G_i\}_{i\in I}$ una collezione di gruppi, $k \in I$ un indice fissato e si consideri la funzione $\iota_k \colon G_k \to \prod_{i\in I}^* G_i$ definita da $\iota_k(x) := x$, detta l'*inclusione canonica nella componente k-esima*. Si tratta di un omomorfismo di gruppi in quanto, comunque fissati $x, y \in G_k$, essa soddisfa la condizione seguente:

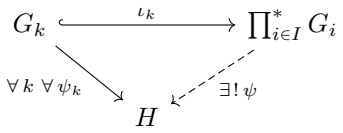
$$\iota_k(x \cdot y) = (x \cdot y) = (x) \cdot (y) = \iota(x) \cdot \iota(y)$$

È importante osservare che il simbolo $\cdot$ denota l'operazione binaria su G_k nei primi due passaggi, denota invece l'operazione binaria su $\prod_{i\in I}^* G_i$ negli altri due passaggi. Dalla definizione di ι_k segue banalmente che è anche un'applicazione iniettiva e dunque è un monomorfismo.

Proposizione 4.9 (Proprietà universale del prodotto libero)**.** *Siano $\{(G_i, \cdot, e_i)\}_{i\in I}$ una data collezione di gruppi, $(H, \star, e)$ un gruppo e sia $\{\, \iota_k \colon G_k \to \prod_{i\in I}^* G_i \,\}_{k\in I}$ la famiglia delle inclusioni canoniche. Allora la suddetta famiglia soddisfa la seguente proprietà universale:*

$$\forall\, \{\, \psi_k \colon G_k \to H \,\}_{k\in I} \text{ famiglia di omomorfismi } \exists!\, \psi \colon \prod_{i\in I}^* G_i \to H \text{ omomorfismo } \mid\ \psi \circ \iota_k = \psi_k \ \ \forall\, k \in I$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



Dimostrazione. Sia $\{\, \psi_k \colon G_k \to H \,\}_{k\in I}$ una famiglia di omomorfismi. Si osservi che, comunque sia fissata una parola in forma canonica $a_1 a_2 \dots a_n \in \prod_{i\in I}^* G_i$, esistono indici $i_1, \dots, i_n \in I$ tali che $a_j \in G_{i_j}$ per ogni $1 \le j \le n$. Si consideri adesso l'applicazione $\psi \colon \prod_{i\in I}^* G_i \to H$ definita dalla condizione seguente:

$$\psi(a_1 a_2 \dots a_n) := \psi_{i_1}(a_1) \star \psi_{i_2}(a_2) \star \cdots \star \psi_{i_n}(a_n)$$

Si tratta di un'applicazione ben definita poiché ciascuna delle mappe ψ_k ha immagine in H e per ipotesi $\star$ è un'operazione binaria su H. Si tratta di un omomorfismo di gruppi per costruzione. Inoltre, comunque fissati un indice $k \in I$ e un elemento $x \in G_k$, vale per costruzione la relazione seguente:

$$(\psi \circ \iota_k)(x) = \psi\big(\iota_k(x)\big) = \psi(x) = \psi_k(x)$$

È dunque verificata la condizione $\psi \circ \iota_k = \psi_k$ per ogni $k \in I$. Sia ora $\psi' \colon \prod_{i\in I}^* G_i \to H$ un omomorfismo, possibilmente diverso da ψ, tale che $\psi' \circ \iota_k = \psi_k$ per ogni $k \in I$. Sia inoltre $a_1 a_2 \dots a_n \in \prod_{i\in I}^* G_i$ fissato. Dall'assunzione che ψ' sia un omomorfismo e dall'osservazione 3.4 segue immediatamente che:

$$\psi'(a_1 a_2 \dots a_n) = \psi'(a_1) \star \psi'(a_2) \star \cdots \star \psi'(a_n)$$

A questo punto, dalla condizione $\psi' \circ \iota_k = \psi_k$ per ogni $k \in I$ e dal fatto che, comunque fissato $1 \le j \le n$, esiste un indice $i_j \in I$ tale che $a_j \in G_{i_j}$ deriva la relazione seguente:

$$\psi'(a_j) = \psi'\big(\iota_{i_j}(a_j)\big) = (\psi' \circ \iota_{i_j})(a_j) = \psi_{i_j}(a_j)$$

Combinando le due relazioni ottenute, si ottiene infine la condizione seguente:

$$\psi'(a_1 a_2 \dots a_n) = \psi'(a_1) \star \psi'(a_2) \star \cdots \star \psi'(a_n) = \psi_{i_1}(a_1) \star \psi_{i_2}(a_2) \star \cdots \star \psi_{i_n}(a_n) = \psi(a_1 a_2 \dots a_n)$$

Non dipendendo il risultato ottenuto dalla particolare scelta di una parola $a_1 a_2 \dots a_n \in \prod_{i\in I}^* G_i$, ottengo che $\psi' = \psi$. Per arbitrarietà nella scelta dell'omomorfismo $\psi' \colon \prod_{i\in I}^* G_i \to H$ tale che si abbia $\psi' \circ \iota_k = \psi_k$ per ogni $k \in I$, posso concludere che ψ è unico e dunque si ha la tesi. □

4.6 Gruppo degli automorfismi

Definizione 4.17. Sia G un gruppo. Un isomorfismo $f \colon G \to G$ si dice un *automorfismo di G*. L'insieme degli automorfismi di G si denota $\mathrm{Aut}(G)$.

Osservazione 4.23. Sia G un gruppo. Allora l'insieme $\mathrm{Aut}(G)$ munito dell'operazione di composizione di applicazioni $\circ$ è un gruppo con elemento neutro l'applicazione identità id_G.

Dimostrazione. Innanzitutto, osservo che l'operazione di composizione di applicazioni $\circ$ è un'operazione binaria su $\mathrm{Aut}(G)$. Infatti, dati due isomorfismi $f, g\colon G \to G$, anche la funzione composta $f \circ g\colon G \to G$ è un isomorfismo. L'associatività dell'operazione di composizione $\circ$ su $\mathrm{Aut}(G)$ segue invece dal fatto che, in generale, la composizione di applicazioni è un'operazione associativa. Inoltre, l'applicazione identità id_G è banalmente un isomorfismo, quindi un automorfismo di G ed è immediato verificare che è un elemento neutro. Infine, dato un qualsiasi isomorfismo $f\colon G \to G$, l'applicazione inversa $f^{-1}\colon G \to G$ esiste ed è un isomorfismo in virtù dell'osservazione 1.6. Questo conclude la dimostrazione. □

Definizione 4.18. Sia G un gruppo. Il gruppo $\mathrm{Aut}(G)$ con l'operazione di composizione di applicazioni $\circ$ e con elemento neutro l'applicazione identità id_G prende il nome di *gruppo degli automorfismi di* G.

Osservazione 4.24. Sia G un gruppo. Per ogni $g \in G$, la funzione $I_g\colon G \to G$ data da $I_g(x) := g \cdot x \cdot g^{-1}$ è un automorfismo di G.

Dimostrazione. Sia $g \in G$ un elemento fissato. Innanzitutto, noto che l'applicazione I_g è un omomorfismo di gruppi in quanto soddisfa, per ogni $x, y \in G$, la condizione seguente:

$$I_g(x \cdot y) = g \cdot (x \cdot y) \cdot g^{-1} = (g \cdot x \cdot g^{-1}) \cdot (g \cdot y \cdot g^{-1}) = I_g(x) \cdot I_g(y)$$

È inoltre immediato verificare che l'applicazione $I_{g^{-1}}\colon G \to G$ è l'inversa di I_g. Questo dimostra che I_g è un'applicazione biiettiva e dunque, in definitiva, un automorfismo di G. □

Definizione 4.19. Sia G un gruppo. Per ogni $g \in G$, la funzione $I_g\colon G \to G$ data da $I_g(x) := g \cdot x \cdot g^{-1}$ prende il nome di *coniugio per* g. L'applicazione $I\colon G \to \mathrm{Aut}(G)$ definita da $I(g) := I_g$ viene invece detta la *mappa di coniugio di* G. Inoltre, l'immagine della mappa di coniugio I si denota $\mathrm{Inn}(G)$ e i suoi elementi vengono detti gli *automorfismi interni di* G. I restanti elementi in $\mathrm{Aut}(G)$ si dicono infine gli *automorfismi esterni di* G e si definisce $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

La definizione 4.19 è ben posta in virtù dell'osservazione 4.24.

Osservazione 4.25. Sia G un gruppo. Nonostante la terminologia introdotta nella definizione 4.19 possa generare confusione, un elemento in $\mathrm{Out}(G)$ non è un automorfismo esterno di G, bensì una classe laterale sinistra di $\mathrm{Aut}(G)$ rispetto a $\mathrm{Inn}(G)$. Gli automorfismi esterni di G sono automorfismi in $\mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$, che non va confuso con l'insieme delle classi laterali sinistre $\mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Proposizione 4.10. *Sia G un gruppo. Allora valgono le seguenti affermazioni.*

(i) *La mappa di coniugio $I\colon G \to \mathrm{Aut}(G)$ è un omomorfismo di gruppi.*

(ii) $\ker I = Z(G)$.

(iii) $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

Dimostrazione.

(i) Siano $g, h \in G$ elementi fissati. Sarà sufficiente mostrare che $I(g \cdot h) = I(g) \circ I(h)$ e questo è come richiedere, per definizione di mappa di coniugio, che valga la condizione $I_{g \cdot h} = I_g \circ I_h$. Tenendo sempre a mente la definizione 4.19 basta osservare che, per ogni $x \in G$, si ha la relazione seguente:

$$I_{g \cdot h}(x) = (g \cdot h) \cdot x \cdot (g \cdot h)^{-1} = g \cdot (h \cdot x \cdot h^{-1}) \cdot g^{-1} = g \cdot I_h(x) \cdot g^{-1} = I_g\big(I_h(x)\big) = (I_g \circ I_h)(x)$$

Questo dimostra dunque che la mappa di coniugio $I\colon G \to \mathrm{Aut}(G)$ è un omomorfismo di gruppi.

(ii) Per ottenere l'asserto, basta semplicemente calcolare il nucleo della mappa di coniugio applicando la definizione 3.1, come mostra la relazione seguente:

$$\begin{aligned}
\ker I &= \{\, g \in G \mid I_g = \mathrm{id}_G \,\} \\
&= \{\, g \in G \mid I_g(x) = \mathrm{id}_G(x) \ \ \forall\, x \in G \,\} \\
&= \{\, g \in G \mid g \cdot x \cdot g^{-1} = x \ \ \forall\, x \in G \,\} \\
&= \{\, g \in G \mid g \cdot x = x \cdot g \ \ \forall\, x \in G \,\} = Z(G)
\end{aligned}$$

(iii) Si noti innanzitutto che, essendo $\mathrm{Inn}(G) = \mathrm{Im}\, I$ per definizione ed essendo la mappa di coniugio I un omomorfismo di gruppi per il punto (i) appena dimostrato, si ha che $\mathrm{Inn}(G) < \mathrm{Aut}(G)$ per la proposizione 3.1-(i). Basterà quindi dimostrare che $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ è un sottogruppo normale. Siano $g \in G$, $\alpha \in \mathrm{Aut}(G)$ due elementi fissati. Dall'assunzione che α sia un automorfismo, dunque un omomorfismo e dall'osservazione 3.2 deriva facilmente, per ogni $x \in G$, la condizione che segue:

$$(\alpha \circ I_g \circ \alpha^{-1})(x) = \alpha\big(I_g(\alpha^{-1}(x))\big) = \alpha\big(g \cdot \alpha^{-1}(x) \cdot g^{-1}\big) = \alpha(g) \cdot x \cdot \alpha(g)^{-1} = I_{\alpha(g)}(x)$$

In particolare, si ha che $\alpha \circ I_g \circ \alpha^{-1} \in \mathrm{Inn}(G)$ e questo, per arbitrarietà nella scelta dell'elemento $g \in G$, dimostra l'inclusione $\alpha\,\mathrm{Inn}(G)\alpha^{-1} \subseteq \mathrm{Inn}(G)$. Non dipendendo il risultato ottenuto da una particolare scelta di $\alpha \in \mathrm{Aut}(G)$, posso dunque concludere che $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ è un sottogruppo normale. □

Osservazione 4.26. Una conseguenza immediata della definizione 4.19 e della proposizione 4.10-(iii) è che l'insieme $\mathrm{Out}(G)$, con l'operazione binaria $\cdot$ definita nell'osservazione 2.2 e con elemento neutro $\mathrm{Inn}(G)$, è il gruppo quoziente di $\mathrm{Aut}(G)$ rispetto a $\mathrm{Inn}(G)$.

Definizione 4.20. Sia G un gruppo. Il sottogruppo normale $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ prende il nome di *gruppo degli automorfismi interni di* G, mentre il gruppo quoziente $\mathrm{Out}(G)$ è detto il *gruppo degli automorfismi esterni di* G.

Osservazione 4.27. Sia G un gruppo. In virtù dei punti (i) e (ii) della proposizione 4.10 posso applicare il primo teorema di isomorfismo alla mappa di coniugio $I\colon G \to \mathrm{Aut}(G)$, ottenendo che $\mathrm{Inn}(G) \simeq G/Z(G)$.

Osservazione 4.28. Sia G un gruppo abeliano. Dalle osservazioni 2.11 e 4.27 segue immediatamente che $\mathrm{Inn}(G) = \{\mathrm{id}_G\}$ e di conseguenza $\mathrm{Out}(G) \simeq \mathrm{Aut}(G)$.

Esempio 4.11. Si consideri il gruppo $\mathbb{Z}$ con l'usuale operazione di somma $+$ e con elemento neutro 0. In virtù dell'osservazione 4.28, l'unico automorfismo interno di $\mathbb{Z}$ è l'applicazione identità $\mathrm{id}_{\mathbb{Z}}$. Ora, siccome $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$, per l'osservazione 1.18 tutti gli automorfismi di $\mathbb{Z}$ dovranno mappare il generatore 1 in se stesso oppure in -1 e quindi vi è, oltre all'applicazione identità $\mathrm{id}_{\mathbb{Z}}$, l'automorfismo esterno $-\mathrm{id}_{\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{Z}$ definito da $-\mathrm{id}_{\mathbb{Z}}(x) := -x$. Ogni altro automorfismo di $\mathbb{Z}$ dovrà coincidere, per l'osservazione 1.18, o con $\mathrm{id}_{\mathbb{Z}}$ o con l'applicazione $-\mathrm{id}_{\mathbb{Z}}$. In altre parole, ho dimostrato che $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}_{\mathbb{Z}}, -\mathrm{id}_{\mathbb{Z}}\}$ e a questo punto è immediato verificare che $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}_2$.

Esempio 4.12. Si consideri il gruppo $\mathbb{Z}_n$ con l'operazione di somma usuale $+$ e con elemento neutro $\bar{0}$. Anche in questo caso si ha a che fare con un gruppo abeliano e dunque l'unico automorfismo interno di $\mathbb{Z}_n$ è l'applicazione identità $\mathrm{id}_{\mathbb{Z}_n}$ in virtù dell'osservazione 4.28. Inoltre, anche $\mathbb{Z}_n$ è un gruppo ciclico e può essere generato dalle classi di resto modulo n i cui rappresentanti sono coprimi con n, cioè $\mathbb{Z}_n = \langle \bar{m}\rangle$ con $m \in \mathbb{N}^*$ tale che $\mathrm{MCD}(n, m) = 1$. Dunque, per l'osservazione 1.18, le applicazioni $f_{\bar{m}}\colon \mathbb{Z}_n \to \mathbb{Z}_n$ definite da $f_{\bar{m}}(\bar{x}) := \bar{m} \cdot \bar{x}$ sono le uniche candidate a essere automorfismi di $\mathbb{Z}_n$ e si verifica assai facilmente che lo sono effettivamente. Riassumendo, si ha che $\mathrm{Aut}(\mathbb{Z}_n) = \{\, f_{\bar{m}}\colon \mathbb{Z}_n \to \mathbb{Z}_n \mid \mathrm{MCD}(n, m) = 1 \,\}$ e a questo punto si dimostra con facilità che $\mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$. In particolare, si ottiene che il gruppo $\mathrm{Aut}(\mathbb{Z}_n)$ è ciclico e che $|\mathrm{Aut}(\mathbb{Z}_n)| = \varphi(n)$, dove la funzione $\varphi\colon \mathbb{N} \to \mathbb{N}$ sta a indicare, come al solito, la funzione di Eulero.

Avendo determinato il gruppo degli automorfismi di $\mathbb{Z}_n$ nell'esempio 4.12, è naturale chiedersi quale possa essere il gruppo degli automorfismi del gruppo $\mathbb{Z}_n^*$ munito dell'operazione usuale di prodotto $\cdot$ e con elemento neutro $\bar{1}$.

Proposizione 4.11. *Sia $n \in \mathbb{N}$, $n \geq 2$ e sia $n = p_1^{r_1} \cdots p_k^{r_k}$ la sua decomposizione in fattori primi. Allora vale la condizione $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ e in particolare si ha che $\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*$.*

Dimostrazione. Si ricordi che, come immediata conseguenza del[19] teorema cinese del resto, l'applicazione $f\colon \mathbb{Z}_n \to \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$ definita da $f(\bar{a}_n) := (\bar{a}_{p_1^{r_1}}, \ldots, \bar{a}_{p_k^{r_k}})$ è biiettiva e induce anche, a sua volta, una

[19] Ricordo l'enunciato: siano $n_1, \ldots, n_s \in \mathbb{N}^*$ tali che $\mathrm{MCD}(n_i, n_j) = 1$ per ogni $1 \leq i \neq j \leq n$. Allora il seguente sistema di congruenze ammette una soluzione che è unica modulo $n_1 + \cdots + n_s$:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_s \pmod{n_s} \end{cases}$$

Per una dimostrazione di questo risultato e delle sue conseguenze si rimanda agli appunti del corso AL110.

corrispondenza biunivoca sugli elementi invertibili, cioè tra $\mathbb{Z}_n^*$ e il prodotto cartesiano $\mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*$. A questo punto basta semplicemente osservare che, per definizione dell'operazione binaria $\cdot$ sul prodotto diretto di gruppi (osservazione 4.17), tale corrispondenza biunivoca è anche un isomorfismo. La verifica esplicita di questo fatto è immediata e pertanto viene omessa. □

Osservazione 4.29. Una conseguenza immediata della proposizione 4.11 è che, per studiare le proprietà di $\mathbb{Z}_n^*$ con $n \in \mathbb{N}$, $n \geq 2$ è sufficiente ridursi al caso di $\mathbb{Z}_{p^r}$ con p numero primo. Si può dimostrare la relazione:

$$\mathbb{Z}_{p^r}^* \simeq \begin{cases} \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{r-1}} & \text{se } p \neq 2,\ r \neq 1 \\ \mathbb{Z}_{p-1} & \text{se } p \neq 2,\ r = 1 \\ \{1\} & \text{se } p = 2,\ r = 1 \\ \mathbb{Z}_2 & \text{se } p = 2,\ r = 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}} & \text{se } p = 2,\ r \geq 3 \end{cases}$$

Secondo, terzo e quarto caso si possono vedere come casi particolari del primo ponendo $\mathbb{Z}_1 := \{\bar{0}\}$, mentre il caso $p = 2$, $r \geq 3$ è una vera e propria eccezione. In ogni caso, vale che $|\mathbb{Z}_{p^r}^*| = \varphi(p^r) = p^{r-1}(p-1)$, dove $\varphi\colon \mathbb{N} \to \mathbb{N}$ è la funzione di Eulero ed è noto che tale applicazione è[20] moltiplicativa. È possibile mostrare, infine, che $\mathbb{Z}_{p^{r-1}} \simeq \langle \overline{1+p} \rangle$ e che $\mathbb{Z}_{2^{r-2}} \simeq \langle \bar{3} \rangle$.

Esempio 4.13. Sia $n \in \mathbb{N}$, $n \geq 3$ fissato e si consideri il gruppo simmetrico S_n. Da quanto si è discusso nell'esempio 2.8 segue che $Z(S_n) = \{\mathrm{id}_{\{1,\dots,n\}}\}$ ma allora, applicando l'osservazione 4.27, posso affermare che $S_n \simeq \mathrm{Inn}(S_n)$. Non verrà invece dimostrata la relazione seguente:

$$\mathrm{Out}(S_n) \simeq \begin{cases} \{1\} & \text{se } n \neq 6 \\ \mathbb{Z}_2 & \text{se } n = 6 \end{cases}$$

Esempio 4.14. Sia $n \in \mathbb{N}$, $n \geq 4$ fissato e si consideri il gruppo alterno A_n. Come si è visto nell'esempio precedente, posso affermare in virtù dell'osservazione 3.22 che $Z(A_n) = \{\mathrm{id}_{\{1,\dots,n\}}\}$ e di conseguenza vale che $A_n \simeq \mathrm{Inn}(A_n)$ per l'osservazione 4.27. Si considerino adesso la mappa di coniugio $I\colon S_n \to \mathrm{Aut}(S_n)$, l'applicazione $r\colon \mathrm{Aut}(S_n) \to \mathrm{Aut}(A_n)$ definita da $r(\alpha) := \alpha\big|_{A_n}$ e la funzione $\tilde{I}\colon S_n \to \mathrm{Aut}(A_n)$ data dalla condizione $\tilde{I} := r \circ I$. La mappa di coniugio è ben definita in virtù dell'osservazione 4.24. L'applicazione r, invece, è ben definita per il teorema di corrispondenza (teorema 3.3-(a)) e in virtù della proposizione 3.4. Infatti, comunque sia fissato $\alpha \in \mathrm{Aut}(S_n)$, per il teorema appena menzionato α induce una corrispondenza biunivoca tra sottogruppi di S_n nel dominio e sottogruppi di S_n nel codominio che preserva gli indici dei sottogruppi. Per la proposizione citata, tuttavia, il gruppo alterno A_n è l'unico sottogruppo di indice 2 in S_n e di conseguenza $\alpha(A_n) = A_n$. Questo dimostra che $\alpha\big|_{A_n} \in \mathrm{Aut}(A_n)$ e dunque r è un'applicazione ben definita. A questo punto, anche $\tilde{I}$ è una mappa ben definita per costruzione.

Adesso mi occupo di dimostrare che $\tilde{I}$ è un omomorfismo di gruppi. Sarà sufficiente mostrare che r è un omomorfismo in quanto I lo è per la proposizione 4.10-(i). Siano dunque $\alpha, \beta \in \mathrm{Aut}(A_n)$ due elementi prefissati e si osservi che, comunque venga fissato $x \in A_n$, è soddisfatta la condizione che segue:

$$(\alpha \circ \beta)\big|_{A_n}(x) = (\alpha \circ \beta)(x) = \alpha\big(\beta(x)\big) = \alpha\big|_{A_n}\big(\beta(x)\big) = \alpha\big|_{A_n}\big(\beta\big|_{A_n}(x)\big) = (\alpha\big|_{A_n} \circ \beta\big|_{A_n})(x)$$

Dalla relazione ottenuta segue, per arbitrarietà nella scelta di $x \in A_n$, che $r(\alpha \circ \beta) = r(\alpha) \circ r(\beta)$. Poiché il risultato ottenuto non dipende da una particolare scelta degli elementi $\alpha, \beta \in \mathrm{Aut}(A_n)$, si può affermare che r è un omomorfismo di gruppi. Di conseguenza, anche $\tilde{I}$ è un omomorfismo in quanto composizione di due omomorfismi.

In realtà si può dire di più sull'applicazione $\tilde{I}$. È possibile dimostrare, infatti, che $\tilde{I}$ è un isomorfismo se $n \neq 6$, un monomorfismo se $n = 6$. La dimostrazione di questo fatto, tuttavia, verrà tralasciata. Poiché nel caso $n \neq 6$ si ha che $\tilde{I}\colon S_n \to \mathrm{Aut}(A_n)$ è un isomorfismo, vale che $S_n \simeq \mathrm{Aut}(A_n)$ ma allora, tenendo a mente la definizione 4.19 e ricordando che $A_n \simeq \mathrm{Inn}(A_n)$ in virtù di quanto si è osservato inizialmente, si può affermare che $\mathrm{Out}(A_n) \simeq S_n/A_n$. Per l'osservazione 3.18, ciò equivale a dire che $\mathrm{Out}(A_n) \simeq \mathbb{Z}_2$. Non verrà invece dimostrato che, nel caso $n = 6$, si ha la relazione $\mathrm{Out}(A_n) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Definizione 4.21. Sia G un gruppo. Un sottogruppo $H < G$ viene detto *caratteristico* se è soddisfatta la condizione $\alpha(H) = H$ per ogni $\alpha \in \mathrm{Aut}(G)$.

[20] Si vedano ancora gli appunti del corso AL110.

Osservazione 4.30. Sia G un gruppo e sia $H < G$ un sottogruppo. Valgono le seguenti affermazioni.

(i) Vale che $H < G$ è un sottogruppo caratteristico se e solo se $\alpha(H) \subseteq H$ per ogni $\alpha \in \mathrm{Aut}(G)$.

(ii) Se $H < G$ è un sottogruppo caratteristico, allora $H \lhd G$ è un sottogruppo normale.

(iii) Sia $N < G$ un sottogruppo. Se $H < N$ e $N < G$ sono due sottogruppi caratteristici, allora anche $H < G$ è un sottogruppo caratteristico.

Dimostrazione.

(i) L'implicazione diretta deriva banalmente dalla definizione 4.21, perciò sarà sufficiente dimostrare il viceversa. Sia $\alpha \in \mathrm{Aut}(G)$. Dato che, per la definizione 4.17, un automorfismo è un isomorfismo, quindi un'applicazione biiettiva, esiste l'applicazione inversa α^{-1} e in virtù dell'osservazione 1.6 anche $\alpha^{-1} \in \mathrm{Aut}(G)$. Dalle ipotesi derivano dunque le due condizioni $\alpha(H) \subseteq H$ e $\alpha^{-1}(H) \subseteq H$. Passando all'immagine tramite α nella seconda relazione e usando il fatto che α^{-1} è l'applicazione inversa di α, si ottiene che $H \subseteq \alpha(H)$ e di conseguenza $\alpha(H) = H$ per doppia inclusione. Poiché il risultato ottenuto non dipende da una particolare scelta di $\alpha \in \mathrm{Aut}(G)$, si può concludere che $H < G$ è un sottogruppo caratteristico.

(ii) Sia $g \in G$ un elemento fissato e si ricordi che $I_g \in \mathrm{Aut}(G)$ in virtù dell'osservazione 4.24. Dato che per ipotesi $H < G$ è un sottogruppo caratteristico, per la definizione 4.21 vale che $I_g(H) = H$ ma allora, per la definizione 4.19, si ha che $gHg^{-1} = H$ e questo dimostra, per arbitrarietà nella scelta dell'elemento $g \in G$, che $H \lhd G$ è un sottogruppo normale.

(iii) Sia $\alpha \in \mathrm{Aut}(G)$. Dato che per ipotesi $N < G$ è un sottogruppo caratteristico, vale che $\alpha(N) = N$, ma allora $\alpha\big|_N \in \mathrm{Aut}(N)$ banalmente. Ora, poiché si assume anche che $H < N$ sia un sottogruppo caratteristico, dovrà valere che $\alpha\big|_N(H) = H$ per la definizione 4.21, ma $\alpha\big|_N(H) = \alpha(H)$ poiché $H \subseteq N$ e per definizione di restrizione. Avendo dunque mostrato che $\alpha(H) = H$ e non dipendendo il risultato ottenuto da una particolare scelta di $\alpha \in \mathrm{Aut}(G)$, si ha che $H < G$ è un sottogruppo caratteristico e questo conclude la dimostrazione. □

4.7 Prodotto semidiretto

Proposizione 4.12. *Siano $(N, \star, e_N)$, $(Q, \star, e_Q)$ due gruppi, sia $\theta\colon Q \to \mathrm{Aut}(N)$ un omomorfismo e sia $\cdot$ l'operazione binaria sul prodotto cartesiano $N \times Q$ data da $(n, q) \cdot (n', q') := \big(n \star \theta(q)(n'), q \star q'\big)$. Allora $N \times Q$ munito dell'operazione binaria $\cdot$ è un gruppo con elemento neutro (e_N, e_Q).*

Dimostrazione. Noto innanzitutto che l'operazione binaria $\cdot$ sul prodotto cartesiano $N \times Q$ è ben definita perché $\theta(q) \in \mathrm{Aut}(N)$ per ogni $q \in Q$ e di conseguenza $\theta(q)(n') \in N$ per ogni $n' \in N$. Si considerino ora tre elementi prefissati $(n, q), (n', q'), (n'', q'') \in N \times Q$. Dalla definizione data dell'operazione binaria $\cdot$ sul prodotto cartesiano $N \times Q$ e dal fatto che θ e $\theta(q)$ siano due omomorfismi deriva facilmente la condizione:

$$\begin{aligned}
\big((n, q) \cdot (n', q')\big) \cdot (n'', q'') &= \big(n \star \theta(q)(n'), q \star q'\big) \cdot (n'', q'') \\
&= \big(n \star \theta(q)(n') \star \theta(q \star q')(n''), (q \star q') \star q''\big) \\
&= \big(n \star \theta(q)(n') \star (\theta(q) \circ \theta(q'))(n''), q \star q' \star q''\big) \\
&= \big(n \star \theta(q)(n') \star \theta(q)(\theta(q')(n'')), q \star q' \star q''\big) \\
&= \big(n \star \theta(q)(n' \star \theta(q')(n'')), q \star (q' \star q'')\big) \\
&= (n, q) \cdot (n' \star \theta(q')(n''), q' \star q'') \\
&= (n, q) \cdot \big((n', q') \cdot (n'', q'')\big)
\end{aligned}$$

Questo dimostra, per arbitrarietà nella scelta di $(n, q), (n', q'), (n'', q'') \in N \times Q$, che l'operazione binaria $\cdot$ su $N \times Q$ è associativa. Si osservi adesso che, applicando l'osservazione 3.1 agli omomorfismi θ e $\theta(q)$ e utilizzando la definizione di elemento neutro, si ricavano le due condizioni seguenti:

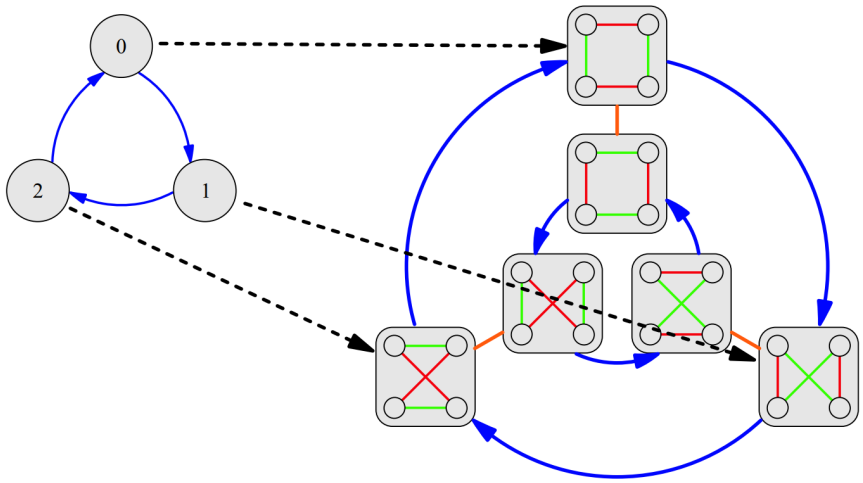
$$\begin{aligned}
(n, q) \cdot (e_N, e_Q) &= \big(n \star \theta(q)(e_N), q \star e_Q\big) = (n \star e_N, q \star e_Q) = (n, q) \\
(e_N, e_Q) \cdot (n, q) &= \big(e_N \star \theta(e_Q)(n), e_Q \star q\big) = (e_N \star n, e_Q \star q) = (n, q)
\end{aligned}$$

Tali condizioni mi permettono di affermare che (e_N, e_Q) è un elemento neutro. Basta infine osservare che, per l'assunzione che θ e $\theta(q)$ siano omomorfismi e per le osservazioni 3.1 e 3.2, valgono le relazioni seguenti:

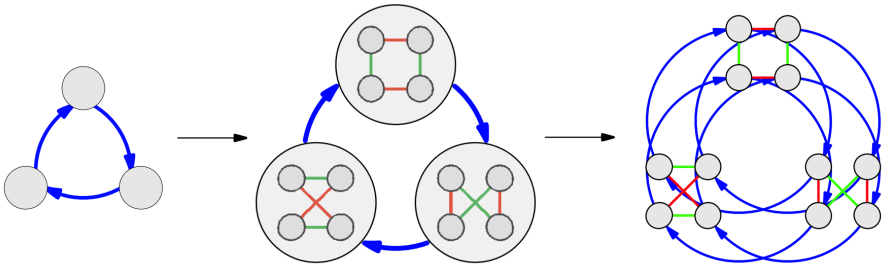
$$\begin{aligned}(n,q)\cdot\big(\theta(q^{-1})(n^{-1}),q^{-1}\big) &= \big(n\star\theta(q)(\theta(q^{-1})(n^{-1})),q\star q^{-1}\big)\\ &= \big(n\star(\theta(q)\circ\theta(q^{-1}))(n^{-1}),e_Q\big)\\ &= (n\star n^{-1},e_Q)=(e_N,e_Q)\\ \big(\theta(q^{-1})(n^{-1}),q^{-1}\big)\cdot(n,q) &= \big(\theta(q^{-1})(n^{-1})\star\theta(q^{-1})(n),q^{-1}\star q\big)\\ &= \big(\theta(q^{-1})(n^{-1}\star n),e_Q\big)\\ &= \big(\theta(q^{-1})(e_N),e_Q\big)=(e_N,e_Q)\end{aligned}$$

Avendo mostrato che ciascun elemento in $N\times Q$ ammette un inverso, posso concludere che $N\times Q$ munito dell'operazione binaria $\cdot$ è un gruppo con elemento neutro (e_N,e_Q). □

Definizione 4.22. Siano $(N,\star,e_N)$, $(Q,\star,e_Q)$ due gruppi, $\theta\colon Q\to\mathrm{Aut}(N)$ un omomorfismo. Il gruppo $N\times Q$ munito dell'operazione binaria $\cdot$ definita nella proposizione 4.12 e dell'elemento neutro (e_N,e_Q) si dice il *prodotto semidiretto di N e Q rispetto a θ* e si denota $N\rtimes_\theta Q$ oppure $N\rtimes Q$ qualora non si volesse specificare l'omomorfismo θ. Inoltre, per ogni $q\in Q$ e per ogni $n\in N$ si pone per semplicità ${}^qn:=\theta(q)(n)$.



La figura mostra un esempio di omomorfismo a valori in un gruppo di automorfismi. In questo caso particolare, si ha che $Q:=\mathbb{Z}_3$, $N:=\mathbb{Z}_2\times\mathbb{Z}_2$ e si dimostra facilmente che $\mathrm{Aut}(N)\simeq S_3$. I segmenti rossi e verdi rappresentano la moltiplicazione per un elemento di N. Intuitivamente, un automorfismo modifica la disposizione di tali segmenti ma non altera la disposizione dei nodi né le relazioni algebriche tra gli elementi del gruppo. Questo significa che il diagramma ottenuto dopo aver applicato l'automorfismo descrive ancora il gruppo N.



In figura viene mostrato il procedimento con cui si può arrivare a costruire il prodotto semidiretto di N e Q per mezzo di un diagramma. Al primo passo si considera il diagramma del gruppo Q, che in questo caso è $\mathbb{Z}_3$. Poi si sostituisce a ciascun nodo una copia di N ma, diversamente da quanto accade nel prodotto diretto, la disposizione dei segmenti rossi e verdi viene modificata dall'azione dell'omomorfismo θ. Infine si duplicano le frecce blu di Q in modo tale da connettere ciascun nodo di N con le sue copie.

Osservazione 4.31. Siano N e Q due gruppi e sia $\theta\colon Q \to \mathrm{Aut}(N)$ l'applicazione definita da $\theta(q) := \mathrm{id}_N$. Allora θ è un omomorfismo banale e il prodotto semidiretto di N e Q rispetto a θ coincide con il prodotto diretto di N e Q. In altre parole, il prodotto semidiretto è una generalizzazione del prodotto diretto.

Osservazione 4.32. Siano $(N, \star, e_N)$, $(Q, \star, e_Q)$ gruppi, $\theta\colon Q \to \mathrm{Aut}(N)$ un omomorfismo. A differenza di quanto accade per il prodotto diretto $N \times Q$, non tutte le proiezioni canoniche del prodotto semidiretto $N \rtimes_\theta Q$ sono, in generale, omomorfismi. Il prodotto semidiretto $N \rtimes_\theta Q$ ammette, infatti, due proiezioni canoniche, date dalle mappe $\pi_N\colon N \rtimes_\theta Q \to N$, $\pi_Q\colon N \rtimes_\theta Q \to Q$ definite dalle condizioni $\pi_N(n, q) := n$, $\pi_Q(n, q) := q$. Si dimostra esattamente come nell'osservazione 4.18 che π_Q è un epimorfismo. Noto invece che, per definizione dell'operazione binaria $\cdot$ su $N \rtimes_\theta Q$, vale per ogni $(n, q), (n', q') \in N \rtimes_\theta Q$ la relazione:

$$\pi_N\big((n, q) \cdot (n', q')\big) = \pi_N(n \star \theta(q)(n'), q \star q') = n \star \theta(q)(n') = \pi_N(n) \star \theta(q)\big(\pi_N(n')\big)$$

Deduco quindi che π_N è un omomorfismo se e solo se $\theta(q)$ è l'applicazione identità per ogni $q \in Q$ e questo accade, in virtù dell'osservazione 4.31, se e solo se il prodotto semidiretto $N \rtimes_\theta Q$ coincide con il prodotto diretto $N \times Q$. Vale invece in generale che π_N è un'applicazione suriettiva, come è immediato verificare.

Proposizione 4.13. *Siano $(N, \star, e_N)$, $(Q, \star, e_Q)$ due gruppi e sia $\theta\colon Q \to \mathrm{Aut}(N)$ un omomorfismo. Sia inoltre $G := N \rtimes_\theta Q$ e si definiscano i due seguenti insiemi:*

$$\tilde{N} := \{\, (n, e_Q) \in N \times Q \mid n \in N \,\}$$
$$\tilde{Q} := \{\, (e_N, q) \in N \times Q \mid q \in Q \,\}$$

Allora valgono le seguenti proprietà:

(i) $\tilde{N}, \tilde{Q} < G$ *sono sottogruppi e inoltre* $\tilde{N} \simeq N$, $\tilde{Q} \simeq Q$.

(ii) $\tilde{N} \cap \tilde{Q} = \{(e_N, e_Q)\}$.

(iii) $\tilde{N}\tilde{Q} = G$.

(iv) $(e_N, q) \cdot (n, e_Q) \cdot (e_N, q)^{-1} = ({}^q n, e_Q)$ *per ogni* $n \in N$, $q \in Q$.

(v) $\tilde{N} \lhd G$ *è un sottogruppo normale.*

Siano ora $f\colon N \to \tilde{N}$, $g\colon Q \to \tilde{Q}$, $\tilde{\theta}\colon \tilde{Q} \to \mathrm{Aut}(\tilde{N})$, $\alpha\colon \mathrm{Aut}(N) \to \mathrm{Aut}(\tilde{N})$ le mappe date dalle condizioni:

$$f(n) := (n, e_Q)\,, \quad g(q) := (e_N, q)\,, \quad \tilde{\theta}(e_N, q) := f \circ \theta(q) \circ f^{-1}\,, \quad \alpha(\phi) := f \circ \phi \circ f^{-1}$$

Si considerino inoltre la mappa inclusione $i\colon \tilde{Q} \to G$, l'applicazione $\tilde{I}\colon G \to \mathrm{Inn}(G)$ definita da $\tilde{I}(g) := I_g$ e la funzione $h\colon \mathrm{Inn}(G) \to \mathrm{Aut}(\tilde{N})$ data dalla relazione $h(\phi) := \phi\big|_{\tilde{N}}$. Allora la condizione (iv) è del tutto equivalente a richiedere che il seguente diagramma di applicazioni sia commutativo, cioè tale che valgano le condizioni $h \circ \tilde{I} \circ i = \tilde{\theta}$ e $\tilde{\theta} \circ g = \alpha \circ \theta$:

$$\begin{array}{ccc} G & \xrightarrow{\tilde{I}} & \mathrm{Inn}(G) \\ {\scriptstyle i}\uparrow & & \downarrow{\scriptstyle h} \\ \tilde{Q} & \xrightarrow{\tilde{\theta}} & \mathrm{Aut}(\tilde{N}) \\ {\scriptstyle g}\uparrow\simeq & & \simeq\uparrow{\scriptstyle \alpha} \\ Q & \xrightarrow[\theta]{} & \mathrm{Aut}(N) \end{array}$$

Dimostrazione.

(i) Si osservi, innanzitutto, che $\tilde{N} = N \times \{e_Q\}$ e che $\tilde{Q} = \{e_N\} \times Q$ per costruzione. Di conseguenza, si ha l'inclusione insiemistica $\tilde{N}, \tilde{Q} \subseteq N \times Q$. Siano adesso fissati $x, x' \in \tilde{N}$. Per definizione di $\tilde{N}$, esistono due elementi $n, n' \in N$ tali che $x = (n, e_Q)$ e $x' = (n', e_Q)$. Ricordando che per ipotesi θ è un omomorfismo, si osservi adesso che, in virtù dell'osservazione 3.1, vale la condizione seguente:

$$(n, e_Q) \cdot (n', e_Q) = (n \star \theta(e_Q)(n'), e_Q \star e_Q) = (n \star n', e_Q) \tag{7}$$

Poiché si assume per ipotesi che $\star$ sia un'operazione binaria su N, posso affermare che $n \star n' \in N$ e di conseguenza $x \cdot x' \in \tilde{N}$. Si osservi poi che $(e_N, e_Q) \in \tilde{N}$ perché $e_N \in N$ essendo N un gruppo. Si ricordi adesso che, come si è visto nella dimostrazione della proposizione 4.12, vale la condizione $(n,q)^{-1} = \big(\theta(q^{-1})(n^{-1}), q^{-1}\big)$ per ogni $(n,q) \in G$. Nel caso particolare di $\tilde{N}$ si ottiene la relazione:

$$(n, e_Q)^{-1} = \big(\theta(e_Q^{-1})(n^{-1}), e_Q^{-1}\big) = (n^{-1}, e_Q) \tag{8}$$

In particolare, si ha che $x^{-1} \in \tilde{N}$. Per arbitrarietà nella scelta di $x, x' \in \tilde{N}$ posso dunque affermare che $\tilde{N} < G$ è un sottogruppo. Si considerino ora due elementi fissati $y, y' \in \tilde{Q}$. Per definizione di $\tilde{Q}$, esistono $q, q' \in Q$ tali che $y = (e_N, q)$ e $y' = (e_N, q')$. Dal momento che $\theta(q)$ è un omomorfismo, posso applicare l'osservazione 3.1 e ottenere la relazione seguente:

$$(e_N, q) \cdot (e_N, q') = \big(e_N \star \theta(q)(e_N), q \star q'\big) = (e_N, q \star q') \tag{9}$$

Dato che per ipotesi $\star$ è un'operazione binaria su Q, vale che $q \star q' \in Q$ e dunque $y \cdot y' \in \tilde{Q}$. Ora osservo che $(e_N, e_Q) \in \tilde{Q}$ perché $e_Q \in Q$ essendo Q un gruppo. Si noti infine che vale la condizione:

$$(e_N, q)^{-1} = \big(\theta(q^{-1})(e_N^{-1}), q^{-1}\big) = (e_N, q^{-1}) \tag{10}$$

Avendo mostrato che $y^{-1} \in \tilde{Q}$ e non dipendendo i risultati ottenuti da una particolare scelta degli elementi $y, y' \in \tilde{Q}$, posso affermare che anche $\tilde{Q} < G$ è un sottogruppo.

Si considerino ora le applicazioni $f\colon N \to \tilde{N}$, $g\colon Q \to \tilde{Q}$ date da $f(n) := (n, e_Q)$, $g(q) := (e_N, q)$. Per costruzione esse sono ben definite e biiettive. Siano adesso $n, n' \in N$, $q, q' \in Q$ e si osservi che, in virtù delle relazioni (7) e (9), valgono le due condizioni seguenti:

$$\begin{aligned} f(n \star n') &= (n \star n', e_Q) = (n, e_Q) \cdot (n', e_Q) = f(n) \cdot f(n') \\ g(q \star q') &= (e_N, q \star q') = (e_N, q) \cdot (e_N, q') = g(q) \cdot g(q') \end{aligned}$$

Tali relazioni dimostrano che f e q sono omomorfismi di gruppi, quindi isomorfismi. Ho appena dimostrato, quindi, che $\tilde{N} \simeq N$ e che $\tilde{Q} \simeq Q$.

(ii) Innanzitutto, è evidente che $(e_N, e_Q) \in \tilde{N} \cap \tilde{Q}$ per il punto (i) appena dimostrato. D'altra parte, comunque fissato $x \in \tilde{N} \cap \tilde{Q}$, esistono $n \in N$, $q \in Q$ tali che $x = (n, e_Q) = (e_N, q)$. In particolare, si ha che $n = e_N$ e dunque $x = (e_N, e_Q)$. Per arbitrarietà nella scelta dell'elemento $x \in \tilde{N} \cap \tilde{Q}$ si può concludere che $\tilde{N} \cap \tilde{Q} \subseteq \{(e_N, e_Q)\}$ e dalla doppia inclusione segue che $\tilde{N} \cap \tilde{Q} = \{(e_N, e_Q)\}$.

(iii) Si osservi, innanzitutto, che $\tilde{N}, \tilde{Q} \subseteq G$ per costruzione. Dato che per definizione $\cdot$ è un'operazione binaria su G (proposizione 4.12), vale l'inclusione $\tilde{N}\tilde{Q} \subseteq GG \subseteq G$. Adesso, fissato $x \in G$, esistono per definizione di G due elementi $n \in N$, $q \in Q$ tali che $x = (n, q)$. Si osservi che vale la relazione:

$$(n, e_Q) \cdot (e_N, q) = \big(n \star \theta(e_Q)(e_N), e_Q \star q\big) = (n, q) \tag{11}$$

Questa semplice considerazione mostra che $x \in \tilde{N}\tilde{Q}$. Non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $x \in G$, posso affermare che $G \subseteq \tilde{N}\tilde{Q}$ e dunque $\tilde{N}\tilde{Q} = G$ per doppio contenimento.

(iv) Si ricordi che $(e_N, q)^{-1} = (e_N, q^{-1})$ per ogni $q \in Q$ in virtù della relazione (10). Comunque fissati $n \in N$, $q \in Q$, la formula che si vuole dimostrare deriva immediatamente dalla relazione seguente:

$$\begin{aligned} \big((e_N, q) \cdot (n, e_Q)\big) \cdot (e_N, q)^{-1} &= \big(e_N \star \theta(q)(n), q \star e_Q\big) \cdot (e_N, q^{-1}) \\ &= \big(\theta(q)(n), q\big) \cdot (e_N, q^{-1}) \\ &= \big(\theta(q)(n) \star \theta(q)(e_N), q \star q^{-1}\big) = \big(\theta(q)(n), e_Q\big) \end{aligned}$$

(v) Innanzitutto, per il punto (i) appena dimostrato, si ha che $\tilde{N} < G$ è un sottogruppo. Siano quindi fissati $x \in G$, $y \in \tilde{N}$. Come si è già visto nei punti precedenti, per definizione di G e di $\tilde{N}$ esistono

$n, n' \in N$, $q \in Q$ tali che $x = (n, q)$, $y = (n', e_Q)$. Per le relazioni (8), (10), (11) e per il punto (iv) appena dimostrato, si ha la condizione seguente:

$$\begin{aligned} x \cdot y \cdot x^{-1} &= (n, q) \cdot (n', e_Q) \cdot (n, q)^{-1} \\ &= \big((n, e_Q) \cdot (e_N, q)\big) \cdot (n', e_Q) \cdot \big((n, e_Q) \cdot (e_N, q)\big)^{-1} \\ &= (n, e_Q) \cdot \big((e_N, q) \cdot (n', e_Q) \cdot (e_N, q^{-1})\big) \cdot (n^{-1}, e_Q) \\ &= (n, e_Q) \cdot \big(\theta(q)(n), e_Q\big) \cdot (n^{-1}, e_Q) \end{aligned}$$

In particolare, dato che $\tilde{N} < G$ è un sottogruppo e dunque un sottoinsieme di G chiuso rispetto all'operazione binaria $\cdot$ su G, posso affermare che $x \cdot y \cdot x^{-1} \in \tilde{N}$. Poiché il risultato ottenuto non dipende da una particolare scelta di $y \in \tilde{N}$, posso affermare che $x\tilde{N}x^{-1} \subseteq \tilde{N}$. Per arbitrarietà di $x \in G$ posso invece concludere che $\tilde{N} \lhd G$ è un sottogruppo normale per definizione.

Per quanto riguarda la parte finale dell'enunciato, bisogna innanzitutto mostrare che tutte le applicazioni presenti nel diagramma sono ben definite. Nella dimostrazione del punto (i) si è già visto che f e g sono isomorfismi di gruppi ben definiti. Per costruzione e per il fatto noto che f è un isomorfismo, anche $\tilde{\theta}$ e α sono applicazioni ben definite. La funzione I è ben posta in virtù della definizione 4.19, mentre h lo è in virtù del punto (v) appena dimostrato. Data infatti un'applicazione $\phi \in \mathrm{Inn}(G)$, esiste un elemento $g \in G$ tale che $\phi = I_g$. Essendo $\tilde{N} \lhd G$ un sottogruppo normale per il punto (v) già menzionato, però, si ha che:

$$\phi(\tilde{N}) = I_g(\tilde{N}) = g\tilde{N}g^{-1} = \tilde{N}$$

Posso dunque affermare che $\phi\big|_{\tilde{N}} \in \mathrm{Aut}(\tilde{N})$ e questo dimostra che h è un'applicazione ben definita. Dalle definizioni fornite nell'enunciato segue immediatamente che, per ogni $q \in Q$, si ha la condizione seguente:

$$(\tilde{\theta} \circ g)(q) = \tilde{\theta}\big(g(q)\big) = \tilde{\theta}(e_N, q) = f \circ \theta(q) \circ f^{-1} = \alpha\big(\theta(q)\big) = (\alpha \circ \theta)(q)$$

Siano adesso $n \in N$, $q \in Q$ due elementi prefissati. Pongo per semplicità $x := (e_N, q)$ e osservo che, ancora in virtù delle definizioni date nell'enunciato, si hanno le seguenti relazioni:

$$\begin{aligned} \tilde{\theta}(x)(n, e_Q) &= \big(f \circ \theta(q) \circ f^{-1}\big)(n, e_Q) \\ &= f\big(\theta(q)(f^{-1}(n, e_Q))\big) \\ &= f\big(\theta(q)(n)\big) = f({}^q n) \\ &= ({}^q n, e_Q) \end{aligned} \qquad \begin{aligned} (h \circ \tilde{I} \circ i)(x)(n, e_Q) &= h\big(\tilde{I}(i(x))\big)(n, e_Q) \\ &= h\big(\tilde{I}(x)\big)(n, e_Q) = h(I_x)(n, e_Q) \\ &= I_x\big|_{\tilde{N}}(n, e_Q) = I_x(n, e_Q) \\ &= (e_N, q) \cdot (n, e_Q) \cdot (e_N, q)^{-1} \end{aligned}$$

A questo punto è evidente, per arbitrarietà nella scelta di $n \in N$, $q \in Q$, l'equivalenza della condizione (iv) con la commutatività del diagramma assegnato. Questo conclude la dimostrazione. □

Osservazione 4.33. Il punto (v) della proposizione 4.13 giustifica la scelta della notazione utilizzata per il prodotto semidiretto: si scrive $N \rtimes Q$ in quanto il gruppo $\tilde{N}$ isomorfo a N è un sottogruppo normale di G.

Esempio 4.15. Sotto le ipotesi della proposizione 4.13 si è visto che $\tilde{N} \lhd G$ è un sottogruppo normale ma non è vero, in generale, che lo è anche $\tilde{Q} \lhd G$, come mostra il seguente controesempio. Si consideri il caso particolare in cui $N := \mathbb{Z}_3$ e $Q := \mathbb{Z}_2$, entrambi con operazione usuale di somma $+$ ed elemento neutro $\bar{0}$. Da quanto si è detto nell'esempio 4.12 segue che gli unici automorfismi di $\mathbb{Z}_3$ sono l'applicazione identità $\mathrm{id}_{\mathbb{Z}_3}$ e la funzione $f\colon \mathbb{Z}_3 \to \mathbb{Z}_3$ definita da $f(\bar{x}) := \bar{2} \cdot \bar{x}$. Considero dunque l'applicazione $\theta\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ data da $\theta(\bar{0}) := \mathrm{id}_{\mathbb{Z}_3}$, $\theta(\bar{1}) := f$, che è chiaramente un omomorfismo. Si verifica assai facilmente, tenendo a mente la definizione dell'operazione binaria $\cdot$ su $\mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2$, che la seguente applicazione è un isomorfismo:

$$\begin{aligned} \eta\colon \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2 &\longrightarrow S_3 \\ (\bar{0}, \bar{0}) &\longmapsto \mathrm{id}_{\{1,2,3\}} \\ (\bar{1}, \bar{0}) &\longmapsto (1\,2\,3) \\ (\bar{2}, \bar{0}) &\longmapsto (1\,3\,2) \\ (\bar{0}, \bar{1}) &\longmapsto (1\,2) \\ (\bar{1}, \bar{1}) &\longmapsto (1\,3) \\ (\bar{2}, \bar{1}) &\longmapsto (2\,3) \end{aligned}$$

Altrettanto facilmente si può osservare che $\eta(\{\bar{0}\} \times \mathbb{Z}_2) = \{\mathrm{id}_{\{1,2,3\}}, (1\,2)\}$. Il controesempio voluto è dato dal fatto che $\{\bar{0}\} \times \mathbb{Z}_2 < \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2$ non è un sottogruppo normale. Per dimostrarlo, basterà osservare che $\{\mathrm{id}_{\{1,2,3\}}, (1\,2)\} < S_3$ non è un sottogruppo normale. Per il teorema di corrispondenza (teorema 3.3-(b)), infatti, l'isomorfismo η induce una corrispondenza biunivoca tra i sottogruppi di $\mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2$ e i sottogruppi di S_3 e inoltre tale corrispondenza biunivoca preserva la normalità. Detto questo si noti che, prendendo $\sigma := (2\,3)$, vale la relazione $\sigma \circ (1\,2) \circ \sigma^{-1} = (1\,3)$ e chiaramente $(1\,3) \notin \{\mathrm{id}_{\{1,2,3\}}, (1\,2)\}$. Questo dimostra che $\sigma\{\mathrm{id}_{\{1,2,3\}}, (1\,2)\}\sigma^{-1} \not\subseteq \{\mathrm{id}_{\{1,2,3\}}, (1\,2)\}$ e non è quindi possibile che $\{\mathrm{id}_{\{1,2,3\}}, (1\,2)\} < S_3$ sia normale.

Proposizione 4.14 (Caratterizzazione interna del prodotto semidiretto)**.** *Siano $(N, \star, e_N)$, $(Q, \star, e_Q)$, $(G, \cdot, e)$ gruppi e sia $\theta\colon Q \to \mathrm{Aut}(N)$ un omomorfismo. Allora vale che $G \simeq N \rtimes_\theta Q$ se e solo se esistono due sottogruppi $\bar{N}, \bar{Q} < G$ con $\bar{N} \simeq N$, $\bar{Q} \simeq Q$ tali che siano soddisfatte le seguenti condizioni:*

(i) $\bar{N}\bar{Q} = G$.

(ii) $\bar{N} \cap \bar{Q} = \{e\}$.

(iii) $\bar{N} \lhd G$ *è un sottogruppo normale.*

(iv) *Siano $f\colon N \to \bar{N}$, $g\colon Q \to \bar{Q}$ gli isomorfismi noti e sia $\bar{\theta}\colon \bar{Q} \to \mathrm{Aut}(\bar{N})$ l'applicazione definita da:*

$$\bar{\theta}(q) := f \circ \theta\big(g^{-1}(q)\big) \circ f^{-1}$$

Sia inoltre $i\colon \bar{Q} \to G$ la mappa inclusione e si considerino le applicazioni $\alpha\colon \mathrm{Aut}(N) \to \mathrm{Aut}(\bar{N})$, $\tilde{I}\colon G \to \mathrm{Inn}(G)$, $h\colon \mathrm{Inn}(G) \to \mathrm{Aut}(\bar{N})$ date da $\alpha(\phi) := f \circ \phi \circ f^{-1}$, $\tilde{I}(g) := I_g$, $h(\phi) := \phi\big|_{\bar{N}}$ come nella proposizione 4.13. Allora il seguente diagramma di applicazioni è commutativo, cioè tale che siano soddisfatte le due condizioni $h \circ \tilde{I} \circ i = \bar{\theta}$ e $\bar{\theta} \circ g = \alpha \circ \theta$:

$$\begin{array}{ccc} G & \xrightarrow{\tilde{I}} & \mathrm{Inn}(G) \\ {\scriptstyle i}\uparrow & & \downarrow{\scriptstyle h} \\ \bar{Q} & \xrightarrow{\bar{\theta}} & \mathrm{Aut}(\bar{N}) \\ {\scriptstyle g}\uparrow{\scriptstyle \simeq} & & {\scriptstyle \simeq}\uparrow{\scriptstyle \alpha} \\ Q & \xrightarrow[\theta]{} & \mathrm{Aut}(N) \end{array}$$

Dimostrazione. Si considerino i sottogruppi $\tilde{N}, \tilde{Q} < N \rtimes_\theta Q$ dati nella proposizione 4.13 e si supponga che $G \simeq N \rtimes_\theta Q$. In tal caso, esiste un isomorfismo $\eta\colon N \rtimes_\theta Q \to G$. Definisco $\bar{N} := \eta(\tilde{N})$, $\bar{Q} := \eta(\tilde{Q})$ e noto che $\bar{N}, \bar{Q} < G$ sono sottogruppi in virtù dell'osservazione 1.8. Per costruzione e per la proposizione 4.13-(i) si ha che $\bar{N} \simeq N$, $\bar{Q} \simeq Q$. A questo punto va dimostrata la validità delle condizioni fornite nell'enunciato.

(i) Dal momento che per ipotesi η è un isomorfismo, in particolare si ha che η è suriettiva e dunque, in virtù della proposizione 4.13-(iii), vale la condizione seguente:

$$\eta(\tilde{N}\tilde{Q}) = \eta(N \rtimes_\theta Q) = G$$

Basterà quindi dimostrare che $\bar{N}\bar{Q} = \eta(\tilde{N}\tilde{Q})$. Sia $y \in \bar{N}\bar{Q}$ un elemento prefissato. Allora esistono $y_N \in \bar{N}$, $y_Q \in \bar{Q}$ tali che valga $y = y_N \cdot y_Q$. Tuttavia, per costruzione di $\bar{N}$ e $\bar{Q}$, esistono $x_N \in \tilde{N}$, $x_Q \in \tilde{Q}$ tali che $\eta(x_N) = y_N$, $\eta(x_Q) = y_Q$. Ora basterà utilizzare il fatto che η è un omomorfismo per ottenere la seguente relazione:

$$y = y_N \cdot y_Q = \eta(x_N) \cdot \eta(x_Q) = \eta(x_N \cdot x_Q)$$

Questo dimostra che $y \in \eta(\tilde{N}\tilde{Q})$ e vale quindi, per arbitrarietà nella scelta di $y \in \bar{N}\bar{Q}$, l'inclusione $\bar{N}\bar{Q} \subseteq \eta(\tilde{N}\tilde{Q})$. Sia adesso fissato $y \in \eta(\tilde{N}\tilde{Q})$. Per definizione di immagine esiste $x \in \tilde{N}\tilde{Q}$ tale che valga $\eta(x) = y$ e inoltre, come prima, esistono $x_N \in \tilde{N}$, $x_Q \in \tilde{Q}$ tali che $x = x_N \cdot x_Q$. Utilizzando nuovamente il fatto che η è un omomorfismo, posso affermare che $y \in \bar{N}\bar{Q}$ in virtù della relazione:

$$y = \eta(x) = \eta(x_N \cdot x_Q) = \eta(x_N) \cdot \eta(x_Q)$$

Poiché il risultato ottenuto non dipende da una particolare scelta dell'elemento $y \in \eta(\tilde{N}\tilde{Q})$, posso affermare che $\eta(\tilde{N}\tilde{Q}) \subseteq \bar{N}\bar{Q}$ e di conseguenza si ha che $\bar{N}\bar{Q} = \eta(\tilde{N}\tilde{Q})$ per doppio contenimento.

(ii) L'asserto segue immediatamente dal fatto che l'immagine di una funzione rispetta le intersezioni, dalla proposizione 4.13-(ii) e dal fatto che η è un isomorfismo assieme all'osservazione 1.5, infatti:

$$\bar{N} \cap \bar{Q} = \eta(\tilde{N}) \cap \eta(\tilde{Q}) = \eta(\tilde{N} \cap \tilde{Q}) = \eta\big(\{(e_N, e_Q)\}\big) = \{e\}$$

(iii) Quanto si vuole mostrare è una conseguenza immediata della proposizione 4.13-(v) e del teorema di corrispondenza (teorema 3.3-(b)).

(iv) Gli isomorfismi impliciti nelle condizioni $\bar{N} \simeq N$, $\bar{Q} \simeq Q$ sono, per la proposizione 4.13 e in virtù della costruzione precedente, le applicazioni $f\colon N \to \bar{N}$, $g\colon Q \to \bar{Q}$ definite da $f(n) := \eta(n, e_Q)$, $g(q) := \eta(e_N, q)$. La buona definizione delle funzioni che compaiono nel diagramma si dimostra esattamente come nella proposizione 4.13. Si vede facilmente che, per ogni $q \in Q$, vale la relazione:

$$(\bar{\theta} \circ g)(q) = \bar{\theta}\big(g(q)\big) = f \circ \theta\big(g^{-1}(g(q))\big) \circ f^{-1} = f \circ \theta(q) \circ f^{-1} = \alpha\big(\theta(q)\big) = (\alpha \circ \theta)(q)$$

Siano adesso $n' \in \bar{N}, q' \in \bar{Q}$ elementi fissati. Per costruzione, esistono elementi $n \in N, q \in Q$ tali che $n' = \eta(n, e_Q)$, $q' = \eta(e_N, q)$ oppure, equivalentemente, tali che $n' = f(n)$, $q' = g(q)$ e dunque, in virtù delle definizioni fornite nell'enunciato, si hanno le seguenti condizioni:

$$\begin{aligned}
\bar{\theta}(q')(n') &= \big(f \circ \theta(g^{-1}(q')) \circ f^{-1}\big)(n') \\
&= f\big(\theta(g^{-1}(q'))(f^{-1}(n'))\big) \\
&= f\big(\theta(q)(n)\big) = f({}^{q}n) \\
&= \eta({}^{q}n, e_Q)
\end{aligned}
\qquad
\begin{aligned}
(h \circ \tilde{I} \circ i)(q')(n') &= h\big(\tilde{I}(i(q'))\big)(n') \\
&= h\big(\tilde{I}(q')\big)(n') = h(I_{q'})(n') \\
&= I_{q'}\big|_{\bar{N}}(n') = I_{q'}(n') \\
&= \eta(e_N, q) \cdot \eta(n, e_Q) \cdot \eta(e_N, q)^{-1}
\end{aligned}$$

Per la proposizione 4.13-(iv) e in virtù del fatto che η è un omomorfismo di gruppi, ma anche per arbitrarietà nella scelta degli elementi $n' \in \bar{N}$, $q' \in \bar{Q}$, si può concludere che il diagramma fornito nell'enunciato è commutativo.

Adesso bisogna dimostrare che vale anche il viceversa. Per ipotesi, esistono due sottogruppi $\bar{N}, \bar{Q} < G$ con $\bar{N} \simeq N$, $\bar{Q} \simeq Q$ tali che siano verificate le condizioni assegnate nell'enunciato. Sarà sufficiente dimostrare che $N \rtimes_\theta Q \simeq \bar{N} \rtimes_{\bar{\theta}} \bar{Q}$ e che $\bar{N} \rtimes_{\bar{\theta}} \bar{Q} \simeq G$. Bisogna innanzitutto dimostrare che l'applicazione $\bar{\theta}$ assegnata nell'enunciato è un omomorfismo affinché il prodotto semidiretto $\bar{N} \rtimes_{\bar{\theta}} \bar{Q}$ sia ben definito. Si noti dunque che, assegnati due elementi $q_1, q_2 \in \bar{Q}$, in virtù del fatto che θ e g^{-1} sono omomorfismi (osservazione 1.6) si ha la condizione seguente:

$$\begin{aligned}
\bar{\theta}(q_1 \cdot q_2) &= f \circ \theta\big(g^{-1}(q_1 \cdot q_2)\big) \circ f^{-1} \\
&= f \circ \theta\big(g^{-1}(q_1) \star g^{-1}(q_2)\big) \circ f^{-1} \\
&= f \circ \theta\big(g^{-1}(q_1)\big) \circ \theta\big(g^{-1}(q_2)\big) \circ f^{-1} \\
&= f \circ \theta\big(g^{-1}(q_1)\big) \circ f^{-1} \circ f \circ \theta\big(g^{-1}(q_2)\big) \circ f^{-1} = \bar{\theta}(q_1) \circ \bar{\theta}(q_2)
\end{aligned}$$

Posso dunque affermare, per arbitrarietà nella scelta degli elementi $q_1, q_2 \in \bar{Q}$, che $\bar{\theta}$ è un omomorfismo e si può quindi considerare senza ambiguità l'applicazione $\phi\colon N \rtimes_\theta Q \to \bar{N} \rtimes_{\bar{\theta}} \bar{Q}$ definita dalla condizione $\phi(n, q) := (f(n), g(q))$. Buona definizione, iniettività e suriettività di ϕ derivano dalle analoghe proprietà di cui godono gli isomorfismi f e g. Adesso, tenendo a mente come si è definita l'operazione binaria $\cdot$ sul prodotto semidiretto di due gruppi, usando la costruzione di ϕ assieme al fatto che f e g sono isomorfismi di gruppi, ma soprattutto la definizione di $\bar{\theta}$ fornita dalla condizione (iv) si ottiene, per ogni $n_1, n_2 \in N$, $q_1, q_2 \in Q$, la condizione seguente, in virtù della quale posso concludere che ϕ è un isomorfismo di gruppi:

$$\begin{aligned}
\phi\big((n_1, q_1) \cdot (n_2, q_2)\big) &= \phi\big(n_1 \star \theta(q_1)(n_2), q_1 \star q_2\big) \\
&= \big(f(n_1 \star \theta(q_1)(n_2)), g(q_1 \star q_2)\big) \\
&= \big(f(n_1) \cdot f(\theta(q_1)(n_2)), g(q_1) \cdot g(q_2)\big) \\
&= \big(f(n_1) \cdot (f \circ \theta(q_1) \circ f^{-1})(f(n_2)), g(q_1) \cdot g(q_2)\big) \\
&= \big(f(n_1) \cdot \bar{\theta}(g(q_1))(f(n_2)), g(q_1) \cdot g(q_2)\big) \\
&= \big(f(n_1), g(q_1)\big) \cdot \big(f(n_2), g(q_2)\big) = \phi(n_1, q_1) \cdot \phi(n_2, q_2)
\end{aligned}$$

Si consideri ora l'applicazione $\psi\colon \bar{N} \rtimes_{\bar{\theta}} \bar{Q} \to G$ definita da $f(n,q) := n \cdot q$. È assai evidente che ψ sia una funzione ben definita, in quanto $\bar{N}, \bar{Q} < G$ sono sottogruppi. Dalla condizione (i) segue immediatamente che ψ è una mappa suriettiva. Si consideri adesso un elemento $(n,q) \in \operatorname{Ker}\psi$. Per definizione di nucleo, si ha la condizione $\psi(n,q) = 1$, cioè $n \cdot q = 1$ ma allora, moltiplicando a destra per q^{-1} ambedue i membri di tale relazione, si ottiene che $n = q^{-1}$. In particolare, si ha che $n, q \in \bar{N} \cap \bar{Q}$, ma $\bar{N} \cap \bar{Q} = \{e\}$ in virtù della condizione (ii) e di conseguenza vale che $(n,q) = (e,e)$. Poiché il risultato ottenuto non dipende da una particolare scelta dell'elemento $(n,q) \in \operatorname{Ker}\psi$, si ricava che $\operatorname{Ker}\psi \subseteq \{(e,e)\}$, mentre l'altra inclusione è ovvia. Avendo mostrato che $\operatorname{Ker}\psi$ è banale, posso affermare che ψ è iniettiva per la proposizione 3.1-(ii), purché si dimostri che è anche un omomorfismo. Si osservi dunque che, fissati $(n_1,q_1),(n_2,q_2) \in \bar{N} \rtimes_{\bar{\theta}} \bar{Q}$, in virtù della condizione $h \circ \tilde{I} \circ i = \bar{\theta}$ garantita dalla condizione (iv) si può ottenere la relazione che segue:

$$\begin{aligned}
\psi\big((n_1,q_1)\cdot(n_2,q_2)\big) &= \psi\big(n_1 \cdot \bar{\theta}(q_1)(n_2), q_1 \cdot q_2\big) \\
&= \psi\big(n_1 \cdot (h \circ \tilde{I} \circ i)(q_1)(n_2), q_1 \cdot q_2\big) \\
&= \psi\big(n_1 \cdot h(\tilde{I}(i(q_1)))(n_2), q_1 \cdot q_2\big) \\
&= \psi\big(n_1 \cdot h(\tilde{I}(q_1))(n_2), q_1 \cdot q_2\big) \\
&= \psi\big(n_1 \cdot h(I_{q_1})(n_2), q_1 \cdot q_2\big) \\
&= \psi\big(n_1 \cdot I_{q_1}\big|_{\bar{N}}(n_2), q_1 \cdot q_2\big) \\
&= \psi\big(n_1 \cdot I_{q_1}(n_2), q_1 \cdot q_2\big) \\
&= \psi\big(n_1 \cdot q_1 \cdot n_2 \cdot q_1^{-1}, q_1 \cdot q_2\big) \\
&= n_1 \cdot q_1 \cdot n_2 \cdot q_1^{-1} \cdot q_1 \cdot q_2 \\
&= n_1 \cdot q_1 \cdot n_2 \cdot q_2 = \psi(n_1,q_1) \cdot \psi(n_2,q_2)
\end{aligned}$$

Questo dimostra che ψ è un isomorfismo di gruppi e dunque si ha la tesi. □

Osservazione 4.34. Sebbene nella dimostrazione del viceversa della proposizione 4.14 non venga utilizzata esplicitamente, la condizione (iii) non può essere rimossa poiché garantisce che l'applicazione h definita nel punto (iv) sia ben definita. Si noti, a tal proposito, che per giustificare lo stesso fatto nella dimostrazione della proposizione 4.13 è stata cruciale la validità del punto (v), in virtù del quale $\tilde{N} \lhd G$ è un sottogruppo normale.

Osservazione 4.35. La proposizione 4.14 si può indebolire non assegnando l'omomorfismo $\theta\colon Q \to \operatorname{Aut}(N)$ coinvolto nel prodotto semidiretto $N \rtimes_\theta Q$ e cancellando la condizione (iv). Infatti, è parecchio evidente che la dimostrazione dell'implicazione diretta continui a valere senza specificare l'omomorfismo θ poiché, se non si considera la parte relativa al punto (iv), l'omomorfismo θ non viene coinvolto. Nel viceversa si può invece recuperare la condizione (iv), non assunta per ipotesi, definendo $\theta\colon Q \to \operatorname{Aut}(N)$ come segue:

$$\theta(q) := f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(q)\big) \circ f$$

Pongo per semplicità $x := g(q)$ e osservo che vale la relazione seguente:

$$(h \circ \tilde{I} \circ i)(x) = h\big(\tilde{I}(i(x))\big) = h\big(\tilde{I}(x)\big) = h(I_x) = I_x\big|_{\bar{N}}$$

Come si è già osservato nella dimostrazione della proposizione 4.13, per la condizione (iii) si può affermare che $I_x\big|_{\bar{N}}$ è un automorfismo di $\bar{N}$ e di conseguenza θ è un'applicazione ben definita. Applicando lo stesso procedimento utilizzato nella dimostrazione della proposizione 4.10-(i), si dimostra assai facilmente che $\tilde{I}$ è un omomorfismo di gruppi. Per dimostrare che h è un omomorfismo basta invece osservare che, per ogni $\phi, \psi \in \operatorname{Inn}(G)$ e per ogni $n \in \bar{N}$, vale per definizione di restrizione di un'applicazione la relazione seguente:

$$(\phi \circ \psi)\big|_{\bar{N}}(n) = (\phi \circ \psi)(n) = \phi\big(\psi(n)\big) = \phi\big|_{\bar{N}}\big(\psi(n)\big) = \phi\big|_{\bar{N}}\big(\psi\big|_{\bar{N}}(n)\big) = (\phi\big|_{\bar{N}} \circ \psi\big|_{\bar{N}})(n)$$

Dalla relazione ottenuta, che non dipende dalla scelta di $n \in \bar{N}$, si deduce che $h(\phi \circ \psi) = h(\phi) \circ h(\psi)$ e si può dunque affermare, per arbitrarietà nella scelta degli elementi $\phi, \psi \in \operatorname{Inn}(G)$, che h è un omomorfismo. Questo dimostra che anche $h \circ \tilde{I} \circ i$ è un omomorfismo di gruppi in quanto composizione di omomorfismi (osservazione 3.3). A questo punto, dati $q_1, q_2 \in Q$, posso usare il fatto che g e $h \circ \tilde{I} \circ i$ sono omomorfismi

per ottenere la condizione che segue:

$$\begin{aligned}\theta(q_1 \star q_2) &= f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(q_1 \star q_2)\big) \circ f \\ &= f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(q_1) \cdot g(q_2)\big) \circ f \\ &= f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(q_1)\big) \circ (h \circ \tilde{I} \circ i)\big(g(q_2)\big) \circ f \\ &= f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(q_1)\big) \circ f \circ f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(q_2)\big) \circ f = \theta(q_1) \circ \theta(q_2)\end{aligned}$$

La relazione precedente mi permette di concludere, per arbitrarietà nella scelta degli elementi $q_1, q_2 \in Q$, che θ è un omomorfismo di gruppi. Adesso bisogna mostrare che il diagramma di applicazioni dato dalla condizione (iv) è commutativo. Dalla definizione della mappa $\bar{\theta}$ segue che, per ogni $q \in \bar{Q}$, vale l'identità:

$$\bar{\theta}(q) = f \circ \theta\big(g^{-1}(q)\big) \circ f^{-1} = f \circ f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(g^{-1}(q))\big) \circ f \circ f^{-1} = (h \circ \tilde{I} \circ i)(q)$$

Questo dimostra che $h \circ \tilde{I} \circ i = \bar{\theta}$. Utilizzando la relazione precedente e ricordando come è stata definita l'applicazione θ si deduce facilmente che, comunque fissato un elemento $q \in Q$, vale la seguente condizione:

$$(\bar{\theta} \circ g)(q) = \bar{\theta}\big(g(q)\big) = f \circ f^{-1} \circ (h \circ \tilde{I} \circ i)\big(g(q)\big) \circ f \circ f^{-1} = f \circ \theta(q) \circ f^{-1} = \alpha\big(\theta(q)\big) = (\alpha \circ \theta)(q)$$

Per arbitrarietà nella scelta di $q \in Q$ si ottiene quindi che $\bar{\theta} \circ g = \alpha \circ \theta$ e posso dunque concludere che il diagramma fornito dalla condizione (iv) è commutativo.

4.8 Caratterizzazione dei prodotti semidiretti in termini di estensioni

Definizione 4.23. Siano N, Q e G tre gruppi. Se esiste un sottogruppo normale $M \lhd G$ tale che $N \simeq M$ e tale che $Q \simeq G/M$, si dice che G è un'*estensione di Q tramite N*.

Nella definizione che segue si pone $1 := \{1\}$ con un piccolo abuso di notazione.

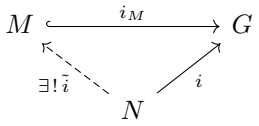
Definizione 4.24. Siano N, Q e G tre gruppi, $i\colon N \to G$, $\pi\colon G \to Q$ due omomorfismi e si consideri la sequenza di gruppi e omomorfismi che segue:

$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } Q \longrightarrow 1$$

Una tale sequenza si dice una *successione esatta corta* oppure, più semplicemente, una *successione esatta* se i è un monomorfismo, se π è un epimorfismo e se $\operatorname{Im} i = \operatorname{Ker} \pi$. Per semplicità, una successione esatta si denota anche $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$.

Osservazione 4.36. Siano N, Q e G gruppi. Allora G è un'estensione di Q tramite N se e solo se esistono due omomorfismi $i\colon N \to G$, $\pi\colon G \to Q$ tali che la sequenza $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ sia una successione esatta.

Dimostrazione. Suppongo che G sia un'estensione di Q tramite N. Per definizione, esiste un sottogruppo normale $M \lhd G$ tale che $N \simeq M$ e tale che $Q \simeq G/M$. In particolare, vi sono due isomorfismi $\eta\colon N \to M$, $f\colon G/M \to Q$. Si considerino adesso la mappa inclusione $i_M\colon M \to G$, la mappa quoziente $q\colon G \to G/M$ e le applicazioni $i\colon N \to G$, $\pi\colon G \to Q$ definite da $i := i_M \circ \eta$, $\pi := f \circ q$. Per costruzione, la funzione i è iniettiva in quanto composizione di applicazioni iniettive e similmente π è suriettiva poiché definita come composizione di mappe suriettive. È inoltre immediato verificare che $\operatorname{Im} i = \operatorname{Ker} \pi$ e questo dimostra che la sequenza $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ è una successione esatta. Viceversa, se esistono due omomorfismi $i\colon N \to G$, $\pi\colon G \to Q$ tali che $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ sia una successione esatta corta, allora i è un monomorfismo, π è un epimorfismo e $\operatorname{Im} i = \operatorname{Ker} \pi$ per definizione. Definisco ora $M := \operatorname{Ker} \pi$, cosicché $M \lhd G$ sia un sottogruppo normale per la proposizione 3.1-(ii). Si consideri ancora la mappa inclusione $i_M\colon M \to G$ e si osservi che, per la proprietà universale delle inclusioni (proposizione 3.2-(i)), esiste un unico omomorfismo $\tilde{i}\colon N \to M$ tale che $i_M \circ \tilde{i} = i$, cioè tale che il seguente diagramma di omomorfismi sia commutativo:



Utilizzando il fatto che $i_M \circ \tilde{i} = i$, ricordando che i è una funzione iniettiva e che $M = \operatorname{Im} i$, si dimostra facilmente che $\tilde{i}$ è un'applicazione iniettiva e suriettiva, dunque un isomorfismo e quindi $N \simeq M$. Usando invece il fatto che π è un epimorfismo, si può applicare l'osservazione 3.7 e dunque esiste un isomorfismo $\tilde{\pi}\colon G/M \to Q$. In particolare, si ha che $G/M \simeq Q$ e quindi G è un'estensione di Q tramite N. □

Una questione interessante che permette di comprendere meglio il concetto di estensione di un gruppo è il cosiddetto "problema dell'estensione". Fissati due gruppi G e H e dato un omomorfismo $f\colon G \to H$, è noto che il nucleo di f è un sottogruppo normale di G per la proposizione 3.1-(ii) e che $G/\operatorname{Ker} f \simeq \operatorname{Im} f$ per il primo teorema di isomorfismo (corollario 3.1). In altre parole, se $i\colon \operatorname{Ker} f \to G$ è la mappa inclusione e se $\pi\colon G \to G/\operatorname{Ker} f$ è la mappa quoziente, quanto si è detto può esprimersi in termini di successioni esatte corte come segue:

$$1 \longrightarrow \operatorname{Ker} f \xrightarrow{i} G \xrightarrow{\pi} G/\operatorname{Ker} f \longrightarrow 1$$

Il "problema dell'estensione" è, in un certo senso, il problema opposto: dati due gruppi N e Q, si vogliono determinare due gruppi G e H e un omomorfismo $f\colon G \to H$ tali che $N \simeq \operatorname{Ker} f$ e $Q \simeq G/\operatorname{Ker} f$. In altre parole, si vuole trovare un'estensione di Q tramite N, cioè una "soluzione" alla seguente successione esatta:

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

Definizione 4.25. Siano N, Q e G tre gruppi. Si dice che una successione esatta corta $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ *spezza* se esiste un omomorfismo $s\colon Q \to G$, che viene detto una *sezione di* Q, tale che $\pi \circ s = \mathrm{id}_Q$.

Osservazione 4.37. Siano N, Q e G tre gruppi, sia $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ una successione esatta e sia $s\colon Q \to G$ una sezione di Q. Dalla definizione 4.25 segue banalmente che s è un monomorfismo poiché omomorfismo e inversa a destra di π.

Osservazione 4.38. Siano N, Q e G tre gruppi e sia $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ una successione esatta corta. Allora tale successione esatta spezza se e solo se esiste un sottogruppo $Q' < G$ tale che la restrizione di π su Q' a valori in Q sia un isomorfismo di gruppi.

Dimostrazione. Per definizione, se la successione esatta $N \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ spezza, allora esiste una sezione di Q, vale a dire un omomorfismo $s\colon Q \to G$ tale che $\pi \circ s = \mathrm{id}_Q$. Definisco $Q' := \operatorname{Im} s$ e noto che $Q' < G$ è un sottogruppo in virtù della proposizione 3.1-(i). Siano ora fissati $p', q' \in Q'$ tali che $\pi\big|_{Q'}(p') = \pi\big|_{Q'}(q')$. Per definizione di restrizione, si ha che $\pi(p') = \pi(q')$ e inoltre, essendo $Q' = \operatorname{Im} s$, esistono $p, q \in Q$ tali che $s(p) = p'$, $s(q) = q'$. Combinando le relazioni precedenti si ottiene che $\pi\big(s(p)\big) = \pi\big(s(q)\big)$ e quindi, usando il fatto che $\pi \circ s = \mathrm{id}_Q$, si ricava che $p = q$. Questo dimostra che la restrizione di π su Q' è un'applicazione iniettiva. Dato invece $q \in Q$, per la relazione $\pi \circ s = \mathrm{id}_Q$ vale che $\pi\big(s(q)\big) = q$. Ricordando che $Q' = \operatorname{Im} s$ e utilizzando il fatto che $\pi\big|_{Q'}(q') = \pi(q')$ per ogni $q' \in Q'$, si ottiene dunque che la restrizione di π su Q' a valori in Q è anche suriettiva. Siccome la restrizione di un omomorfismo è ancora un omomorfismo, si può concludere che $\pi\big|_{Q'}$ è un isomorfismo di gruppi. Viceversa, suppongo che esista un sottogruppo $Q' < G$ tale che la restrizione di π su Q' sia un isomorfismo. Un isomorfismo è in particolare una mappa biiettiva, quindi invertibile, ma allora la restrizione di π su Q' ammette un'inversa bilatera $\tilde{s}\colon Q \to Q'$ la quale, per l'osservazione 1.6, è anch'essa un isomorfismo di gruppi. Sia adesso $i_{Q'}\colon Q' \to G$ la mappa inclusione e sia $s\colon Q \to G$ l'applicazione data da $s := i_{Q'} \circ \tilde{s}$. Si tratta di un omomorfismo di gruppi poiché composizione di omomorfismi. Inoltre, ricordando che $\tilde{s}$ è l'inversa di π, per ogni $q \in Q$ si ricava la condizione seguente:

$$(\pi \circ s)(q) = \pi\big(s(q)\big) = \pi\big((i_{Q'} \circ \tilde{s})(q)\big) = \pi\big(i_{Q'}(\tilde{s}(q))\big) = \pi\big(\tilde{s}(q)\big) = (\pi \circ \tilde{s})(q) = \mathrm{id}_Q(q)$$

Avendo mostrato che $\pi \circ s = \mathrm{id}_Q$, posso concludere che s è una sezione di Q e dunque si ha la tesi. □

Esempio 4.16. Non tutte le successioni esatte corte spezzano, come dimostra il seguente controesempio. Sia p un numero primo e si considerino le applicazioni $i\colon \mathbb{Z}_p \to \mathbb{Z}_{p^2}$, $\pi\colon \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ definite da $i(\bar{x}) := \bar{p}\bar{x}$, $\pi(\bar{x}) := \bar{x}$. Dimostro innanzitutto che $\mathbb{Z}_p \overset{i}{\hookrightarrow} \mathbb{Z}_{p^2} \overset{\pi}{\twoheadrightarrow} \mathbb{Z}_p$ è una successione esatta corta. Si verifica assai facilmente che i e π sono omomorfismi di gruppi. Sia adesso $\bar{x} \in \operatorname{Ker} i$ fissato. Per la definizione 3.1-(ii), si ha che $i(\bar{x}) = \bar{0}$, cioè che $\bar{p}\bar{x} = \bar{0}$ e questo vuol dire, per definizione di relazione di congruenza modulo p^2, che esiste $k \in \mathbb{Z}$ tale che $px = p^2k$. Poiché in $\mathbb{Z}$ valgono le[21] leggi di cancellazione, la relazione precedente implica che $x = pk$, cioè che $\bar{x} = \bar{0}$. Siccome il risultato ottenuto non dipende da una particolare scelta di $\bar{x} \in \operatorname{Ker} i$, si ottiene che $\operatorname{Ker} i \subseteq \{\bar{0}\}$ ed essendo l'altro contenimento ovvio posso affermare che $\operatorname{Ker} i = \{\bar{0}\}$ quindi, per la proposizione 3.1-(ii), che i è un monomorfismo. Per costruzione, si ha inoltre che $\operatorname{Im} i = \langle \bar{p} \rangle$. Si consideri ora un elemento $x \in \operatorname{Ker} \pi$. Ancora per la definizione 3.1-(ii) vale che $\pi(\bar{x}) = \bar{0}$, cioè che $\bar{x} = \bar{0}$ e questo significa che $x = pk$ per un opportuno $k \in \mathbb{Z}$. In particolare, passando alla congruenza modulo p^2, si ottiene che $\bar{x} \in \langle \bar{p} \rangle$. Viceversa, fissato un elemento $\bar{x} \in \langle \bar{p} \rangle$, siccome $\langle \bar{p} \rangle = \{\bar{0}, \bar{p}\}$ vale che $\bar{x} = \bar{0}$ oppure

[21] È un risultato noto che, comunque assegnati $n, m, k \in \mathbb{Z}$, con $k \neq 0$, tali che $kn = km$ oppure $nk = mk$, vale che $n = m$.

$\bar{x} = \bar{p}$. In ambo i casi, passando alla congruenza modulo p, si ottiene che $\bar{x} = \bar{0}$, cioè che $\pi(\bar{x}) = \bar{0}$, quindi $\bar{x} \in \operatorname{Ker}\pi$. Posso dunque affermare, per doppia inclusione, che $\operatorname{Ker}\pi = \langle \bar{p} \rangle$. Si ha infine, per costruzione, che π è un epimorfismo e posso dunque affermare che $\mathbb{Z}_p \xhookrightarrow{i} \mathbb{Z}_{p^2} \xrightarrow{\pi} \!\!\!\rightarrow \mathbb{Z}_p$ è una successione esatta corta. In virtù dell'osservazione 4.38, tale successione esatta spezza se e solo se esiste un sottogruppo $Q' < \mathbb{Z}_{p^2}$ tale che la restrizione di π su Q' a valori in $\mathbb{Z}_p$ sia un isomorfismo di gruppi. È noto che i sottogruppi di $\mathbb{Z}_n$ sono tutti e soli i gruppi ciclici $\langle \bar{m} \rangle$ con $m \in \mathbb{N}$ tale che $m \mid n$ e di conseguenza i sottogruppi di $\mathbb{Z}_{p^2}$ sono $\{\bar{0}\}$, $\langle \bar{p} \rangle$ e $\mathbb{Z}_{p^2}$. Per poter affermare che π non induce un isomorfismo da nessuno di tali sottogruppi a $\mathbb{Z}_p$, basta semplicemente osservare che $|\mathbb{Z}_p| = p$, mentre $|\{\bar{0}\}| = 1$, $|\langle \bar{p} \rangle| = 2$ e $|\mathbb{Z}_{p^2}| = p^2$. Non è dunque possibile costruire, in generale, un'applicazione biiettiva da un sottogruppo di $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p$ e ciò mi permette di concludere che la successione esatta $\mathbb{Z}_p \xhookrightarrow{i} \mathbb{Z}_{p^2} \xrightarrow{\pi} \!\!\!\rightarrow \mathbb{Z}_p$ non spezza.

Proposizione 4.15. *Siano $(N, \star, e_N)$, $(Q, \star, e_Q)$ e $(G, \cdot, e)$ gruppi. Allora $G \simeq N \rtimes_\theta Q$ per un qualche omomorfismo $\theta \colon Q \to \operatorname{Aut}(N)$ se e solo se esiste una successione esatta corta $N \xhookrightarrow{i} G \xrightarrow{\pi} \!\!\!\rightarrow Q$ che spezza.*

Dimostrazione. Assumo che esista un omomorfismo $\theta \colon Q \to \operatorname{Aut}(N)$ tale che $G \simeq N \rtimes_\theta Q$. Esiste dunque un isomorfismo $f \colon N \rtimes_\theta Q \to G$. Si consideri adesso la proiezione canonica $\pi_Q \colon N \rtimes_\theta Q \to Q$ assieme alle tre mappe $i \colon N \to G$, $\pi \colon G \to Q$, $s \colon Q \to G$ definite da $i(n) := f(n, e_Q)$, $\pi := \pi_Q \circ f^{-1}$, $s(q) := f(e_N, q)$. Usando la relazione (7) e ricordando che f è un omomorfismo, si ottiene per ogni $n, n' \in N$ la condizione:

$$i(n \star n') = f(n \star n', e_Q) = f\big((n, e_Q) \cdot (n', e_Q)\big) = f(n, e_Q) \cdot f(n', e_Q) = i(n) \cdot i(n')$$

Questo dimostra che i è un omomorfismo di gruppi. Adesso, usando il fatto che f è un isomorfismo assieme all'osservazione 3.1, posso calcolare il nucleo dell'omomorfismo i:

$$\begin{aligned} \operatorname{Ker} i &= \{\, n \in N \mid i(n) = e \,\} \\ &= \{\, n \in N \mid f(n, e_Q) = f(e_N, e_Q) \,\} \\ &= \{\, n \in N \mid n = e_N \,\} = \{e_N\} \end{aligned}$$

Posso dunque affermare che i è un monomorfismo in virtù della proposizione 3.1-(ii). Si osservi ora che π è banalmente un epimorfismo in quanto composizione di epimorfismi. La proiezione canonica π_Q è infatti un epimorfismo per l'osservazione 4.32, mentre l'applicazione f^{-1} è un isomorfismo per l'osservazione 1.6. A questo punto, si osservi che $\operatorname{Im} i = f(N \times \{e_Q\})$. Se infatti $y \in f(N \times \{e_Q\})$, allora esiste $n \in N$ tale che $f(n, e_Q) = y$ e quindi $i(n) = y$. Se invece $y \in \operatorname{Im} i$, allora esiste $n \in N$ tale che $i(n) = y$, ma questo è come richiedere che $f(n, e_Q) = y$, quindi si ha la doppia inclusione. Calcolo infine il nucleo della mappa π:

$$\begin{aligned} \operatorname{Ker}\pi &= \{\, x \in G \mid \pi(x) = e_Q \,\} \\ &= \{\, x \in G \mid \pi_Q(f^{-1}(x)) = e_Q \,\} \\ &= \{\, x \in G \mid x = f(n, q)\,,\ \pi_Q(n, q) = e_Q\,,\ \exists\, (n, q) \in N \rtimes_\theta Q \,\} \\ &= \{\, x \in G \mid x = f(n, q)\,,\ q = e_Q\,,\ \exists\, (n, q) \in N \rtimes_\theta Q \,\} \\ &= \{\, x \in G \mid x = f(n, e_Q)\,,\ \exists\, n \in N \,\} = f(N \times \{e_Q\}) \end{aligned}$$

Posso dunque affermare che $\operatorname{Im} i = \operatorname{Ker}\pi$ e quindi $N \xhookrightarrow{i} G \xrightarrow{\pi} \!\!\!\rightarrow Q$ è una successione esatta corta. Adesso dimostro che tale successione esatta spezza. Per farlo, sarà sufficiente mostrare che s è una sezione di Q. Noto che, per la relazione (9) e per il fatto che f è un omomorfismo, vale per ogni $q, q' \in Q$ la relazione:

$$s(q \star q') = f(e_N, q \star q') = f\big((e_N, q) \cdot (e_N, q')\big) = f(e_N, q) \cdot f(e_N, q') = s(q) \cdot s(q')$$

La relazione ottenuta dimostra che s è un omomorfismo. Infine osservo che, comunque fissato $q \in Q$, vale la relazione seguente, in virtù della quale è possibile concludere che s è effettivamente una sezione di Q:

$$(\pi \circ s)(q) = \pi\big(s(q)\big) = (\pi_Q \circ f^{-1})\big(f(e_N, q)\big) = \pi_Q\big(f^{-1}(f(e_N, q))\big) = \pi_Q(e_N, q) = q = \mathrm{id}_Q(q)$$

L'implicazione diretta è dunque dimostrata.

Suppongo adesso che esista una successione esatta $N \xhookrightarrow{i} G \xrightarrow{\pi} \!\!\!\rightarrow Q$ che spezza. Per definizione, esiste dunque un omomorfismo $s \colon Q \to G$ con $\pi \circ s = \mathrm{id}_Q$. Definisco $\bar{N} := i(N)$, $\bar{Q} := s(Q)$ e dimostro, usando la proposizione 4.14 con l'osservazione 4.35, che $G \simeq N \rtimes Q$. Innanzitutto, per la proposizione 3.1-(i), vale che $\bar{N}, \bar{Q} < G$ sono due sottogruppi. Si osservi inoltre che, per la definizione 4.24 e per l'osservazione 4.37, le applicazioni i e s sono monomorfismi e dunque le funzioni $\tilde{i} \colon N \to \bar{N}$, $\tilde{s} \colon Q \to \bar{Q}$ definite da $\tilde{i}(n) := i(n)$ e da $\tilde{s}(q) := s(q)$ sono isomorfismi di gruppi per costruzione. Sono dunque verificate le condizioni $N \simeq \bar{N}$, $Q \simeq \bar{Q}$. Adesso basterà mostrare che $\bar{N}$ e $\bar{Q}$ soddisfano le condizioni (i), (ii) e (iii) della proposizione 4.14.

(i) L'inclusione $\bar{N}\bar{Q} \subseteq G$ è ovviamente soddisfatta. Sia ora $x \in G$ un elemento fissato e sia $q := \pi(x)$. Usando il fatto che π è un epimorfismo per la definizione 4.24, quindi un omomorfismo e tenendo a mente la definizione 4.25, si ottiene la condizione seguente:

$$\pi\big(x \cdot s(q)^{-1}\big) = \pi(x) \star \pi\big(s(q^{-1})\big) = \pi(x) \star (\pi \circ s)(q^{-1}) = \pi(x) \star \pi(x)^{-1} = e_Q$$

Dalla definizione 3.1-(ii) segue quindi che $x \cdot s(q)^{-1} \in \operatorname{Ker}\pi$ ma, poiché $\operatorname{Ker}\pi = \operatorname{Im} i$ in virtù della definizione 4.24, è equivalente richiedere che esista $n \in N$ tale che $i(n) = x \cdot s(q)^{-1}$. Moltiplicando a destra per $s(q)$ primo e secondo membro della relazione precedente, si ottiene che $x = i(n) \cdot s(q)$ e in particolare $x \in \bar{N}\bar{Q}$. Posso dunque affermare, per arbitrarietà nella scelta di $x \in G$, che vale l'inclusione $G \subseteq \bar{N}\bar{Q}$ e dal doppio contenimento segue che $\bar{N}\bar{Q} = G$.

(ii) Sia $x \in \bar{N} \cap \bar{Q}$ un elemento fissato. Ricordando le definizioni di $\bar{N}$ e di $\bar{Q}$, esistono $n \in N$, $q \in Q$ tali che $x = i(n)$, $x = s(q)$. Da tali condizioni, dalla definizione 4.25 e dal fatto che $\operatorname{Im} i = \operatorname{Ker}\pi$ si ricava la condizione che segue:

$$q = (\pi \circ s)(q) = \pi\big(s(q)\big) = \pi(x) = \pi\big(i(n)\big) = e_Q$$

Ma allora, usando il fatto che $x = s(q)$, ricordando che s è un omomorfismo per la definizione 4.25 e applicando l'osservazione 3.1, dalla relazione ottenuta deduco che $x = e$. Non dipendendo questo risultato da una particolare scelta dell'elemento $x \in \bar{N} \cap \bar{Q}$, posso affermare che $\bar{N} \cap \bar{Q} \subseteq \{e\}$ ed essendo l'altra inclusione banale posso concludere che $\bar{N} \cap \bar{Q} = \{e\}$.

(iii) Per mostrare che $\bar{N} \lhd G$ è un sottogruppo normale basta osservare che $\bar{N} = \operatorname{Im} i$, che $\operatorname{Im} i = \operatorname{Ker}\pi$ per la definizione 4.24 e che $\operatorname{Ker}\pi \lhd G$ è un sottogruppo normale per la proposizione 3.1-(ii).

Posso dunque concludere, in vista della proposizione 4.14 e dell'osservazione 4.35 già citate in precedenza, che $G \simeq N \rtimes Q$, cioè che esiste un omomorfismo $\theta\colon Q \to \operatorname{Aut}(N)$ tale che $G \simeq N \rtimes_\theta Q$. □

Esempio 4.17. Sia $n \in \mathbb{N}$, $n \geq 2$ fissato. Si considerino il gruppo simmetrico S_n, il gruppo alterno A_n e il gruppo $\{\pm 1\}$ munito dell'usuale operazione di prodotto $\cdot$ e dell'elemento neutro 1. Per la proposizione 3.3, la funzione $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ è un epimorfismo. Un monomorfismo, invece, è dato dalla mappa inclusione $i\colon A_n \to S_n$. Dato che $A_n = \operatorname{Ker}\operatorname{sgn}$ come conseguenza immediata della definizione 3.6, vale la condizione $\operatorname{Im} i = \operatorname{Ker}\operatorname{sgn}$ e questo dimostra che $A_n \overset{i}{\hookrightarrow} S_n \overset{\operatorname{sgn}}{\twoheadrightarrow} \{\pm 1\}$ è una successione esatta corta. Si consideri ora l'applicazione $s\colon \{\pm 1\} \to S_n$ definita da $s(1) := \mathrm{id}_{\{1,\dots,n\}}$, $s(-1) := (1\,2)$. Tale funzione è chiaramente un omomorfismo di gruppi ed è immediato verificare che $\operatorname{sgn} \circ s = \mathrm{id}_{\{\pm 1\}}$. Si tratta dunque di una sezione di $\{\pm 1\}$. Questo mi permette di affermare che la successione esatta $A_n \overset{i}{\hookrightarrow} S_n \overset{\operatorname{sgn}}{\twoheadrightarrow} \{\pm 1\}$ spezza. Dunque, per la proposizione 4.15 e per l'osservazione 4.35, si ha che $S_n \simeq A_n \rtimes_\theta \{\pm 1\}$, dove $\theta\colon \{\pm 1\} \to \operatorname{Aut}(A_n)$ può essere scelto come l'omomorfismo dato da $\theta(1) := \mathrm{id}_{A_n}$, $\theta(-1) := I_\tau$, mentre la funzione $I_\tau\colon A_n \to A_n$ è la restrizione del coniugio per $\tau := (1\,2)$ su A_n. Tale applicazione è effettivamente a valori in A_n perché, comunque assegnata una permutazione $\sigma \in A_n$, vale in virtù della proposizione 3.3 la relazione seguente:

$$\operatorname{sgn}\big(I_\tau(\sigma)\big) = \operatorname{sgn}(\tau \circ \sigma \circ \tau^{-1}) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau^{-1}) = (-1) \cdot 1 \cdot (-1) = 1$$

Si può inoltre osservare che I_τ è un automorfismo esterno di A_n. Per dimostrare questo fatto, è necessario innanzitutto distinguere due casi. Se $n = 3$ allora, come si è già notato nell'osservazione 3.23, il gruppo A_3 è abeliano e dunque non ammette automorfismi interni non banali per l'osservazione 4.28. In questo caso sarà quindi sufficiente osservare che I_τ è non banale:

$$I_\tau(2\,3) = (1\,2) \circ (2\,3) \circ (1\,2) = (1\,3) \neq (2\,3)$$

Nel caso $n = 2$ oppure $n \geq 4$ si procede, invece, per assurdo. Se infatti esistesse una permutazione $\rho \in A_n$ tale che $I_\tau = I_\rho$ allora, per ogni $\sigma \in A_n$, si avrebbe che $\tau \circ \sigma \circ \tau^{-1} = \rho \circ \sigma \circ \rho^{-1}$. Moltiplicando a sinistra per ρ^{-1}, a destra per τ entrambi i membri di tale relazione, si ottiene che $(\rho^{-1} \circ \tau) \circ \sigma = \sigma \circ (\rho^{-1} \circ \tau)$ per ogni $\sigma \in A_n$, cioè che $\rho^{-1} \circ \tau \in Z(A_n)$. A questo punto posso applicare l'osservazione 3.22, che continua a valere nel caso $n = 2$ per l'osservazione 3.23, in modo tale da ottenere che $\rho^{-1} \circ \tau = \mathrm{id}_{\{1,\dots,n\}}$. Passando al segno e usando il fatto che la funzione segno è un omomorfismo (proposizione 3.3), tuttavia, si ottiene la seguente contraddizione, in virtù della quale posso concludere che I_τ è un automorfismo esterno di A_n:

$$1 = \operatorname{sgn}(\mathrm{id}_{\{1,\dots,n\}}) = \operatorname{sgn}(\rho^{-1} \circ \tau) = \operatorname{sgn}(\rho^{-1}) \cdot \operatorname{sgn}(\tau) = 1 \cdot (-1) = -1$$

Esempio 4.18. Sia $n \in \mathbb{N}$, $n \geq 2$ e si consideri il gruppo diedrale D_n. Per le osservazioni 2.35 e 2.36 nel caso $m := 1$, si ha che $\langle\sigma\rangle \lhd D_n$ è un sottogruppo normale isomorfo a $\mathbb{Z}_n$ e inoltre $D_n/\langle\sigma\rangle \simeq D_1$. In virtù delle osservazioni 2.33 e 2.34, vale anche che $D_1 \simeq \mathbb{Z}_2$ e dunque $D_n/\langle\sigma\rangle \simeq \mathbb{Z}_2$ per transitività. Se adesso $i\colon \langle\sigma\rangle \to D_n$ denota la mappa inclusione e se $\pi\colon D_n \to D_n/\langle\sigma\rangle$ indica la mappa quoziente, usando il fatto che $\operatorname{Im} i = \operatorname{Ker}\pi$ posso affermare che $\langle\sigma\rangle \overset{i}{\hookrightarrow} D_n \overset{\pi}{\twoheadrightarrow} D_n/\langle\sigma\rangle$ è una successione esatta corta. Si consideri ora l'applicazione $s\colon D_n/\langle\sigma\rangle \to D_n$ definita da $s(\langle\sigma\rangle) := 1$, $s(\tau\langle\sigma\rangle) := \tau$. È immediato verificare che s è un omomorfismo di gruppi e che $\pi \circ s = \mathrm{id}_{D_n/\langle\sigma\rangle}$, ma allora la successione esatta $\langle\sigma\rangle \overset{i}{\hookrightarrow} D_n \overset{\pi}{\twoheadrightarrow} D_n/\langle\sigma\rangle$ spezza in quanto s è una sezione di $D_n/\langle\sigma\rangle$. Esattamente come nell'esempio 4.17, dalla proposizione 4.15 e dall'osservazione 4.35 segue che $D_n \simeq \langle\sigma\rangle \rtimes_\theta D_n/\langle\sigma\rangle$, dove $\theta\colon D_n/\langle\sigma\rangle \to \mathrm{Aut}(\langle\sigma\rangle)$ può essere selezionato come l'omomorfismo definito da $\theta(\langle\sigma\rangle) := \mathrm{id}_{\langle\sigma\rangle}$, $\theta(\tau\langle\sigma\rangle) := I_\tau$, con $I_\tau\colon \langle\sigma\rangle \to \langle\sigma\rangle$ che è la restrizione del coniugio per τ su $\langle\sigma\rangle$. Si tratta di un'applicazione ben definita in quanto, per l'osservazione 2.22, vale per ogni $k \in \mathbb{Z}$ la condizione seguente:

$$I_\tau(\sigma^k) = \tau \cdot \sigma^k \cdot \tau^{-1} = \sigma^{n-k} \cdot \tau \cdot \tau = \sigma^{n-k}$$

Osservazione 4.39. Sia G un gruppo finito non semplice. In virtù della definizione 3.7, esiste almeno un sottogruppo normale $N \lhd G$ non banale, cioè tale che $N \neq \{1\}$ e $N \neq G$. Di conseguenza, anche il gruppo quoziente G/N è non banale. In particolare, ricordando il teorema di Lagrange (corollario 2.1), si ha che:

$$|N| < |N|[G:N] = |G|$$
$$[G:N] < |N|[G:N] = |G|$$

In virtù dell'osservazione 4.39, per studiare le proprietà di un gruppo finito non semplice G può essere utile analizzare un suo sottogruppo normale $N \lhd G$ non banale e il gruppo quoziente G/N. Questi ultimi due, infatti, sono gruppi di ordine più piccolo di G e dunque, a priori, è più facile studiarli. Ci si può porre il problema di classificare tutti i gruppi finiti, vale a dire:

(i) I gruppi semplici:

- $\mathbb{Z}_p$ con p numero primo.
- il gruppo alterno A_n con $n \geq 5$.
- gruppi di matrici su campi finiti, come $\mathrm{PSL}_n(\mathbb{Z}_p)$.
- 26 gruppi sporadici il più grande dei quali, di ordine pari a circa $8 \cdot 10^{53}$, è il "gruppo mostro".

(ii) Le estensioni non banali, utilizzando tecniche coomologiche.

La dimostrazione di questo risultato ha occupato 500 articoli per un totale di circa 15.000 pagine.

5 Gruppi abeliani

5.1 Prodotto diretto debole e somma diretta

Osservazione 5.1. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione, finita oppure infinita, di gruppi. Allora l'insieme che segue è un sottogruppo normale del prodotto diretto esterno della collezione $\{G_i\}_{i\in I}$:

$$\prod_{i\in I}^{\mathrm{w}} G_i := \left\{ \{g_i\}_{i\in I} \in \prod_{i\in I} G_i \;\middle|\; g_i = e_i \text{ per ogni } i \in I\setminus\{i_1,\dots,i_k\},\, \exists\, i_1,\dots,i_k \in I \right\}$$

Dimostrazione. Siano $\{g_i\}_{i\in I}, \{g_i'\}_{i\in I} \in \prod_{i\in I}^{\mathrm{w}} G_i$ due elementi fissati. Per definizione di $\prod_{i\in I}^{\mathrm{w}} G_i$ esistono $i_1,\dots,i_k,j_1,\dots,j_h \in I$ tali che $g_i = e_i$ per ogni $i \in I\setminus\{i_1,\dots,i_k\}$ e $g_i' = e_i$ per ogni $i \in I\setminus\{j_1,\dots,j_h\}$, ma allora per ogni $i \in I\setminus\{i_1,\dots,i_k,j_1,\dots,j_h\}$ varrà che $g_i \cdot g_i' = e_i$ e di conseguenza, utilizzando il fatto che $\{g_i\}_{i\in I} \cdot \{g_i'\}_{i\in I} = \{g_i \cdot g_i'\}_{i\in I}$ per definizione dell'operazione binaria $\cdot$ sul prodotto diretto $\prod_{i\in I} G_i$, si può concludere che $\{g_i\}_{i\in I} \cdot \{g_i'\}_{i\in I} \in \prod_{i\in I}^{\mathrm{w}} G_i$. Questo dimostra, per arbitrarietà di $\{g_i\}_{i\in I}, \{g_i'\}_{i\in I} \in \prod_{i\in I}^{\mathrm{w}} G_i$, che $\prod_{i\in I}^{\mathrm{w}} G_i \subseteq \prod_{i\in I} G_i$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su $\prod_{i\in I} G_i$. Si osservi ora che $\{e_i\}_{i\in I} \in \prod_{i\in I}^{\mathrm{w}}$ ovviamente e si noti anche che, per ogni $\{g_i\}_{i\in I} \in \prod_{i\in I}^{\mathrm{w}} G_i$, vale che $\{g_i^{-1}\}_{i\in I} \in \prod_{i\in I}^{\mathrm{w}} G_i$ in quanto $g_i^{-1} = e_i^{-1} = e_i$ per ogni $i \in I$ tranne che per un numero finito di indici. Ho dunque mostrato che $\prod_{i\in I}^{\mathrm{w}} G_i < \prod_{i\in I} G_i$ è un sottogruppo. Adesso, comunque fissati $\{a_i\}_{i\in I} \in \prod_{i\in I} G_i$, $\{g_i\}_{i\in I} \in \prod_{i\in I}^{\mathrm{w}} G_i$, per

definizione di $\prod^{\mathrm{w}}_{i\in I} G_i$ esistono $i_1, \dots, i_k \in I$ tali che $g_i = e_i$ per ogni $i \in I \setminus \{i_1, \dots, i_k\}$ e dunque, per tali indici i, si ha che $a_i \cdot g_i \cdot a_i^{-1} = a_i \cdot a_i^{-1} = e_i$. Questo dimostra, per definizione dell'operazione binaria $\cdot$ su $\prod_{i\in I} G_i$, che vale la condizione $\{a_i\}_{i\in I} \cdot \{g_i\}_{i\in I} \cdot \{a_i\}^{-1}_{i\in I} \in \prod^{\mathrm{w}}_{i\in I} G_i$. Per arbitrarietà nella scelta delle due collezioni $\{a_i\}_{i\in I} \in \prod_{i\in I} G_i$, $\{g_i\}_{i\in I} \in \prod^{\mathrm{w}}_{i\in I} G_i$ si ottiene dunque la tesi. □

Definizione 5.1. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione di gruppi, finita oppure infinita. Considero il prodotto diretto esterno di $\{G_i\}_{i\in I}$. Il sottogruppo normale $\prod^{\mathrm{w}}_{i\in I} G_i \lhd \prod_{i\in I} G_i$ viene detto il *prodotto diretto debole esterno* (o il *prodotto diretto debole*) *di* $\{G_i\}_{i\in I}$. Se inoltre $\{(A_i, +, e_i)\}_{i\in I}$ è una collezione, finita oppure infinita, di gruppi abeliani, il prodotto diretto debole di $\{A_i\}_{i\in I}$ viene detto la *somma diretta di* $\{A_i\}_{i\in I}$ e si denota $\bigoplus_{i\in I} A_i$.

Osservazione 5.2. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione finita di gruppi. Dalla definizione del prodotto diretto debole $\prod^{\mathrm{w}}_{i\in I} G_i$ come insieme, data nell'osservazione 5.1, segue immediatamente che $\prod^{\mathrm{w}}_{i\in I} G_i = \prod_{i\in I} G_i$.

Osservazione 5.3. Sia $\{(G_i, \cdot, e_i)\}_{i\in I}$ una collezione di gruppi. Assegnato un elemento $a_1 \cdots a_k \in \prod^{*}_{i\in I} G_i$, per ogni $1 \leq j \leq k$ esiste un indice $i_j \in I$ tale che $a_j \in G_{i_j}$ ed è dunque ragionevole considerare la funzione $\xi\colon \prod^{*}_{i\in I} G_i \to \prod^{\mathrm{w}}_{i\in I} G_i$ definita dalla condizione $\xi(a_1 \cdots a_k) := \{b_i\}_{i\in I}$, dove per ogni indice $i \in I$ si pone:

$$b_i := \begin{cases} \prod_{\substack{1\leq j\leq k \\ i_j = i}} a_j & \text{se esiste } 1 \leq j \leq k \text{ tale che } i_j = i \\ e_j & \text{se } i_j \neq i \text{ per ogni } 1 \leq j \leq k \end{cases}$$

Si tratta di un'applicazione ben definita in quanto gli elementi di $\prod^{*}_{i\in I} G_i$ sono parole, vale a dire sequenze finite di lettere. Più precisamente, dato che $k \in \mathbb{N}^*$, vi è al più un numero finito di indici $1 \leq j \leq k$ e in particolare vi è al più un numero finito di tali indici che soddisfino la condizione $i_j = i$. Di conseguenza, per la costruzione precedente, vi è al più un numero finito di indici $i \in I$ tali che $b_i \neq e_j$ e questo dimostra che ξ è in effetti un'applicazione a valori in $\prod^{\mathrm{w}}_{i\in I} G_i$. Inoltre, è immediato verificare che ξ è un'applicazione suriettiva. Infatti, assegnata una collezione $\{a_i\}_{i\in I} \in \prod^{\mathrm{w}}_{i\in I} G_i$, per come si è definito a livello insiemistico il prodotto diretto debole (osservazione 5.1) esistono indici $i_1, \dots, i_k \in I$ tali che si abbia $a_i = e_i$ per ogni $i \in I \setminus \{i_1, \dots, i_k\}$. È assai evidente che tali indici possano essere scelti a due a due distinti senza perdita di generalità. Si consideri dunque l'elemento $a_{i_1} \cdots a_{i_k} \in \prod^{*}_{i\in I} G_i$ e si osservi che $\xi(a_{i_1} \cdots a_{i_k}) = \{a_i\}_{i\in I}$. In questo caso particolare, infatti, se fisso un indice $i \in \{i_1, \dots, i_k\}$, cioè se $i = i_j$ per un certo $1 \leq j \leq k$, allora $b_i = a_{i_j} = a_i$. Se invece viene assegnato un indice $i \in I \setminus \{i_1, \dots, i_k\}$, cioè tale che si abbia $i \neq i_j$ per ogni $1 \leq j \leq k$, allora $b_i = e_i = a_i$. Non dipendendo il risultato ottenuto da una particolare scelta degli indici considerati, né di una collezione $\{a_i\}_{i\in I} \in \prod^{\mathrm{w}}_{i\in I} G_i$, posso concludere che ξ è una mappa suriettiva. Ovviamente, in generale ξ non è una funzione iniettiva in quanto parole con lettere scambiate di posizione vengono mappate nella medesima collezione del prodotto diretto debole. Nel caso in cui $I = \{1, 2\}$ si ha, per esempio, che $\xi(a_1 a_2) = \xi(a_2 a_1) = (a_1, a_2)$. È inoltre immediato verificare che ξ è un omomorfismo di gruppi. Se infine $i\colon \prod^{\mathrm{w}}_{i\in I} G_i \to \prod_{i\in I} G_i$ denota la mappa inclusione allora, combinando la presente con le osservazioni 4.18 e 4.22, si hanno i seguenti omomorfismi di gruppi:

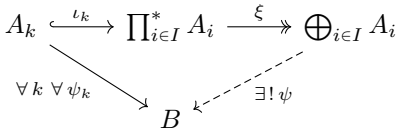
$$G_k \xhookrightarrow{\iota_k} \prod^{*}_{i\in I} G_i \xrightarrow{\xi} \prod^{\mathrm{w}}_{i\in I} G_i \xhookrightarrow{i} \prod_{i\in I} G_i \xrightarrow{\pi_k} G_k$$

Osservazione 5.4. Sia $\{(A_i, +, e_i)\}_{i\in I}$ una collezione, finita oppure infinita, di gruppi abeliani. Per come si è definita l'operazione binaria $\cdot$ sul prodotto cartesiano $\prod_{i\in I} A_i$, il prodotto diretto e la somma diretta della collezione $\{A_i\}_{i\in I}$ sono gruppi abeliani. Il prodotto libero $\prod^{*}_{i\in I} A_i$, invece, non è necessariamente un gruppo abeliano ed è parecchio facile esibire un controesempio. Si considerino infatti il gruppo banale $\{0\}$ e il prodotto libero $\{0\} * \{0\}$. Per poter distinguere l'elemento 0 nelle due copie del gruppo banale, utilizzo dei pedici ausiliari. Tenendo a mente la definizione, data nell'osservazione 4.21, dell'operazione binaria $\cdot$ su $\prod^{*}_{i\in I} A_i$, basta osservare che $0_1 \cdot 0_1 0_2 = 0_1 0_2$, mentre $0_1 0_2 \cdot 0_1 = 0_1 0_2 0_1$.

Proposizione 5.1 (Proprietà universale della somma diretta)**.** *Siano* $\{(A_i, +, e_i)\}_{i\in I}$ *una data collezione di gruppi abeliani,* $(B, +, 0)$ *un gruppo abeliano e si consideri la collezione* $\{\, \iota_k\colon A_k \to \prod^{*}_{i\in I} A_i \,\}_{k\in I}$ *delle inclusioni canoniche assieme alla funzione* $\xi\colon \prod^{*}_{i\in I} A_i \to \bigoplus_{i\in I} A_i$ *definita nell'osservazione 5.3. Allora è verificata la seguente proprietà universale:*

$$\forall\, \{\, \psi_k\colon A_k \to B \,\}_{k\in I} \text{ omomorfismi } \exists!\, \psi\colon \bigoplus_{i\in I} A_i \to B \text{ omomorfismo } \mid\ \psi \circ (\xi \circ \iota_k) = \psi_k \ \ \forall\, k \in I$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



Dimostrazione. Sia $\{\,\psi_k\colon A_k \to B\,\}_{k\in I}$ una famiglia di omomorfismi e sia $\psi\colon \bigoplus_{i\in I} A_i \to B$ l'applicazione definita da $\psi(\{a_i\}_{i\in I}) := \sum_{i\in I} \psi_i(a_i)$. Si tratta di una funzione ben definita in quanto, per definizione di somma diretta, vale la condizione $a_i = e_i$ per ogni $i \in I$ tranne al più per un numero finito di indici e per tali indici $\psi_i(a_i) = 0$ in virtù dell'osservazione 3.1. Questo mostra che la somma $\sum_{i\in I} \psi_i(a_i)$ è una somma finita di elementi di B. Appurata la buona definizione della mappa ψ, si considerino due collezioni fissate $\{a_i\}_{i\in I}, \{b_i\}_{i\in I} \in \bigoplus_{i\in I} A_i$ e si noti che, in vista della definizione data dell'operazione binaria $\cdot$ su $\bigoplus_{i\in I} A_i$ nell'osservazione 4.17, per costruzione di ψ, in virtù del fatto che ψ_i è un omomorfismo per ogni $i \in I$ e per l'ipotesi che B sia un gruppo abeliano, vale la condizione seguente:

$$\begin{aligned}\psi(\{a_i\}_{i\in I} \cdot \{b_i\}_{i\in I}) = \psi(\{a_i + b_i\}_{i\in I}) &= \sum_{i\in I} \psi_i(a_i + b_i)\\ &= \sum_{i\in I} \big(\psi_i(a_i) + \psi_i(b_i)\big)\\ &= \sum_{i\in I} \psi_i(a_i) + \sum_{i\in I} \psi_i(b_i)\\ &= \psi(\{a_i\}_{i\in I}) + \psi(\{b_i\}_{i\in I})\end{aligned}$$

Per arbitrarietà nella scelta degli elementi $\{a_i\}_{i\in I}, \{b_i\}_{i\in I} \in \bigoplus_{i\in I} A_i$, posso dunque affermare che ψ è un omomorfismo di gruppi. Siano adesso $k \in I$, $a \in A_k$ e si consideri la collezione $\{a_i\}_{i\in I} \in \bigoplus_{i\in I} A_i$ definita da $a_i := a$ se $i = k$, $a_i := e_i$ altrimenti. Tenendo a mente le definizioni date degli omomorfismi ι_k e ξ nelle osservazioni 4.22 e 5.3 e ricordando che ψ_i è un omomorfismo per ogni $i \in I$ assieme all'osservazione 3.1, si ottiene la seguente relazione:

$$(\psi \circ \xi \circ \iota_k)(a) = \psi\big(\xi(\iota_k(a))\big) = \psi\big(\xi(a)\big) = \psi(\{a_i\}_{i\in I}) = \sum_{i\in I} \psi_i(a_i) = \psi_k(a)$$

Questo dimostra, per arbitrarietà nella scelta dell'indice $k \in I$ e dell'elemento $a \in A_k$, che vale l'identità $\psi \circ (\xi \circ \iota_k) = \psi_k$ per ogni $k \in I$. Sia adesso $\phi\colon \bigoplus_{i\in I} A_i \to B$ un omomorfismo tale che $\phi \circ (\xi \circ \iota_k) = \psi_k$ per ogni $k \in I$ e si consideri un elemento $\{a_i\}_{i\in I} \in \bigoplus_{i\in I} A_i$. Come si è già discusso nell'osservazione 5.3, per definizione di somma diretta esistono indici $i_1, \dots, i_k \in I$ tali che $a_i = e_i$ per ogni $i \in I \setminus \{i_1, \dots, i_k\}$ e di conseguenza si ha che $\xi(a_{i_1} \cdots a_{i_k}) = \{a_i\}_{i\in I}$. Ma allora, usando il fatto che ϕ e ξ sono omomorfismi, ricordando di nuovo come sono state definite le inclusioni canoniche nelle componenti del prodotto libero (osservazione 4.22), utilizzando la relazione $\phi \circ (\xi \circ \iota_k) = \psi_k$ per ogni $k \in I$ e tenendo sempre a mente che ψ_i è un omomorfismo per ogni $i \in I$ con l'osservazione 3.1, si ottiene la condizione seguente:

$$\begin{aligned}\phi(\{a_i\}_{i\in I}) &= \phi\big(\xi(a_{i_1} \cdots a_{i_k})\big) = \phi\big(\xi(a_{i_1}) \cdots \xi(a_{i_k})\big) = \phi\big(\xi(a_{i_1})\big) + \cdots + \phi\big(\xi(a_{i_k})\big)\\ &= \phi\big(\xi(\iota_{i_1}(a_{i_1}))\big) + \cdots + \phi\big(\xi(\iota_{i_k}(a_{i_k}))\big) = \psi_{i_1}(a_{i_1}) + \cdots + \psi_{i_k}(a_{i_k})\\ &= \sum_{i\in I} \psi_i(a_i) = \psi(\{a_i\}_{i\in I})\end{aligned}$$

Poiché il risultato ottenuto non dipende da una particolare scelta della collezione $\{a_i\}_{i\in I} \in \bigoplus_{i\in I} A_i$, posso affermare che $\phi = \psi$ e quindi, per arbitrarietà nella scelta dell'omomorfismo $\phi\colon \bigoplus_{i\in I} A_i \to B$ che soddisfi $\phi \circ (\xi \circ \iota_k) = \psi_k$ per ogni $k \in I$, posso concludere che l'applicazione ψ è unica. □

Ricapitolando, se si considerano gruppi qualsiasi, allora valgono le affermazioni seguenti:

- Il *prodotto diretto* soddisfa la proprietà universale rispetto alle proiezioni canoniche.
- Il *prodotto libero* soddisfa la proprietà universale rispetto alle inclusioni canoniche.
- Il *prodotto diretto debole* non soddisfa alcuna proprietà universale.

Se invece ci si restringe ai soli gruppi abeliani, allora valgono le seguenti considerazioni:

- Il *prodotto diretto* verifica la proprietà universale rispetto alle proiezioni canoniche.
- Il *prodotto libero* non è di particolare rilievo per quanto si è discusso nell'osservazione 5.4.
- La *somma diretta* soddisfa la proprietà universale data dalla proposizione 5.1.

5.2 Gruppi abeliani liberi

Si introduce questa sezione con un commento preliminare. Dato un gruppo abeliano G e dato un insieme $X \subseteq G$, l'osservazione 1.13 nel caso dei gruppi si traduce in notazione additiva dicendo che il sottogruppo $\langle X \rangle$ consiste di ogni combinazione lineare del tipo $n_1x_1 + \cdots + n_kx_k$ con $n_1, \dots, n_k \in \mathbb{Z}$, $x_1, \dots, x_k \in X$. In particolare, per ogni $x \in G$ si ha che $\langle x \rangle = \{\, nx \mid n \in \mathbb{Z} \,\}$.

Definizione 5.2. Sia X un insieme non vuoto. Il gruppo $\mathbb{Z}^X := \bigoplus_{x \in X} \mathbb{Z}$ con l'operazione binaria $+$ data nell'osservazione 4.17 e con elemento neutro $\{0\}_{x \in X}$ prende il nome di *gruppo abeliano libero su* X. Se poi $|X| < +\infty$ e se $n := |X|$, si definisce per semplicità $\mathbb{Z}^n := \mathbb{Z}^X$. Si pone infine $\mathbb{Z}^\varnothing := \{0\}$ per convenzione.

La definizione 5.2 è ben posta perché $\mathbb{Z}^X$ è un gruppo in virtù dell'osservazione 5.1. Inoltre, il gruppo $\mathbb{Z}^X$ dipende soltanto da $|X|$ e dunque non vi è ambiguità nell'utilizzare la notazione $\mathbb{Z}^n$ qualora $|X| = n$.

Osservazione 5.5. Sia X un insieme non vuoto. Essendo $\mathbb{Z}^X$ definito come una somma diretta tra copie di $\mathbb{Z}$, esso è un gruppo abeliano in virtù dell'osservazione 5.4. Se inoltre $|X| < +\infty$ e se si definisce $n := |X|$, allora $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ (n volte) in quanto la somma diretta di una collezione finita di gruppi coincide, per l'osservazione 5.2, con il prodotto diretto della medesima collezione.

Definizione 5.3. Siano A un gruppo abeliano, $X \subseteq A$ un insieme, $x_1, \dots, x_k \in X$ a due a due distinti. Si dice che $x_1, \dots, x_k$ sono *linearmente indipendenti* se, dati $n_1, \dots, n_k \in \mathbb{Z}$ tali che $n_1x_1 + \cdots + n_kx_k = 0$, si ha che $n_j = 0$ per ogni $1 \leq j \leq k$. Inoltre, se $X \subseteq A$ è un insieme di generatori, cioè se $\langle X \rangle = A$ e se, per ogni $x_1, \dots, x_k \in X$, vale che $x_1, \dots, x_k$ sono linearmente indipendenti, si dice che X è una *base per* A.

Osservazione 5.6. Sia X un insieme e si consideri la funzione $\theta\colon X \to \mathbb{Z}^X$ definita da $\theta(x) := \{\theta_i(x)\}_{i \in X}$, dove $\theta_i(x) := 1$ se $i = x$, $\theta_i(x) := 0$ altrimenti. Allora $\operatorname{Im}\theta$ è una base per $\mathbb{Z}^X$.

Dimostrazione. Innanzitutto, osservo che $\langle \operatorname{Im}\theta \rangle = \mathbb{Z}^X$. Data infatti una collezione $\{a_i\}_{i \in X}$ è immediato verificare, passando alla componente i-esima con $i \in X$ indice fissato, che $\{a_i\}_{i \in X} = \sum_{x \in X} a_x \{\theta_i(x)\}_{i \in X}$. Siano adesso $y_1, \dots, y_k \in \operatorname{Im}\theta$ a due a due distinti. Per definizione di immagine, esistono $x_1, \dots, x_k \in X$ tali che $\theta(x_j) = y_j$ per ogni $1 \leq j \leq k$. Equivalentemente, si ha che $y_j = \{\theta_i(x_j)\}_{i \in X}$ per ogni $1 \leq j \leq k$. Se fosse $x_j = x_h$ per certi $1 \leq j \neq h \leq k$, allora varrebbe la condizione seguente:

$$y_j = \{\theta_i(x_j)\}_{i \in X} = \{\theta_i(x_h)\}_{i \in X} = y_h$$

Questo contraddice l'assunzione che $y_1, \dots, y_k$ fossero a due a due distinti e dunque anche $x_1, \dots, x_k$ sono a due a due distinti. Ho quindi mostrato che θ è un'applicazione iniettiva. Siano adesso $n_1, \dots, n_k \in \mathbb{Z}$ tali che $n_1y_1 + \cdots + n_ky_k = 0$. In altre parole, si ha che $n_1\{\theta_i(x_1)\}_{i \in X} + \cdots + n_k\{\theta_i(x_k)\}_{i \in X} = 0$ ma allora, passando alla componente x_j-esima con indice $1 \leq j \leq k$ fissato e utilizzando il fatto che $x_1, \dots, x_k$ sono a due a due distinti, si ottiene la relazione seguente:

$$0 = n_1\theta_{x_j}(x_1) + \cdots + n_j\theta_{x_j}(x_j) + \cdots + n_k\theta_{x_j}(x_k) = n_j$$

Posso dunque affermare, per arbitrarietà nella scelta dell'indice $1 \leq j \leq k$ e degli elementi $n_1, \dots, n_k \in \mathbb{Z}$, che $y_1, \dots, y_k$ sono linearmente indipendenti. In definitiva, non dipendendo il risultato ottenuto da una particolare scelta degli elementi $y_1, \dots, y_k \in \operatorname{Im}\theta$ a due a due distinti, si ha la tesi. □

Osservazione 5.7. Sia A un gruppo abeliano e sia $X \subseteq A$, $X = \{x_i\}_{i \in I}$ un insieme. Allora X è una base per A se e solo se ogni $a \in A$ si esprime in maniera unica come combinazione lineare finita a coefficienti interi di elementi di X vale a dire, più precisamente, se e solo se esiste un'unica collezione $\{n_i\}_{i \in I} \subseteq \mathbb{Z}$, con $n_i = 0$ per ogni $i \in I$ tranne che per un numero finito di indici, tale che $a = \sum_{i \in I} n_ix_i$.

Dimostrazione. Si assuma che X sia una base per A e si consideri un elemento $a \in A$ fissato. In virtù della definizione 5.3 si ha che $\langle X \rangle = A$ e di conseguenza esistono $i_1, \dots, i_k \in I$, $n_{i_1}, \dots, n_{i_k} \in \mathbb{Z}$ tali che valga la condizione $a = n_{i_1}x_{i_1} + \cdots + n_{i_k}x_{i_k}$. Ponendo $n_i := 0$ per ogni $i \in I \setminus \{i_1, \dots, i_k\}$, si trova una collezione $\{n_i\}_{i\in I}$ tale che $a = \sum_{i\in I} n_i x_i$. Sia adesso $\{m_i\}_{i\in I} \subseteq \mathbb{Z}$, con $m_i = 0$ per ogni $i \in I \setminus \{j_1, \dots, j_h\}$, per certi $j_1, \dots, j_h \in I$, tale che $a = \sum_{i\in I} m_i x_i$. Sottraendo membro a membro le due relazioni note, si ottiene che $\sum_{i\in I}(m_i - n_i)x_i = 0$ e dunque, essendo $n_i = m_i = 0$ per ogni $i \in I \setminus (\{i_1, \dots, i_k\} \cup \{j_1, \dots, j_h\})$, vale che:

$$\sum_{i\in\{i_1,\dots,i_k\}\cup\{j_1,\dots,j_k\}} (m_i - n_i)x_i = 0$$

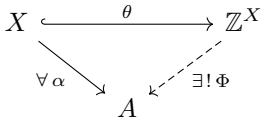
Poiché per ipotesi X è una base per A, in virtù della definizione 5.3 gli elementi di X coinvolti nella somma precedente sono linearmente indipendenti e di conseguenza dovrà valere che $m_i = n_i$ per ogni scelta di un indice $i \in \{i_1, \dots, i_k\} \cup \{j_1, \dots, j_k\}$. In definitiva, si ottiene che $\{m_i\}_{i\in I} = \{n_i\}_{i\in I}$ e questo dimostra, per arbitrarietà nella scelta di $\{m_i\}_{i\in I} \subseteq \mathbb{Z}$, che la collezione $\{n_i\}_{i\in I}$ è unica.

Viceversa, se ogni $a \in A$ si può scrivere in maniera unica come combinazione lineare finita a coefficienti interi di elementi di X, allora in particolare $\langle X \rangle = A$ per l'osservazione 1.13. Siano adesso $i_1, \dots, i_k \in I$ indici fissati e siano $n_{i_1}, \dots, n_{i_k} \in \mathbb{Z}$ tali che valga $n_{i_1}x_{i_1} + \cdots + n_{i_k}x_{i_k} = 0$. Come nella parte precedente, definendo $n_i := 0$ per ogni $i \in I \setminus \{i_1, \dots, i_k\}$, si ottiene una collezione $\{n_i\}_{i\in I} \subseteq \mathbb{Z}$ tale che $\sum_{i\in I} n_i x_i = 0$ e per ipotesi la suddetta collezione è unica. A questo punto basta notare che anche $\sum_{i\in I} 0x_i = 0$ e dunque, per unicità, si dovrà avere che $n_i = 0$ per ogni $i \in I$. In particolare, si ha che $n_{i_j} = 0$ per ogni $1 \le j \le k$ e questo dimostra che $x_{i_1}, \dots, x_{i_k}$ sono linearmente indipendenti. Per arbitrarietà nella scelta degli indici $i_1, \dots, i_k \in I$ e in virtù della definizione 5.3, posso concludere che X è una base per A. □

Proposizione 5.2 (Proprietà universale dei gruppi abeliani liberi)**.** *Sia A un gruppo abeliano e sia X un insieme. Allora la mappa $\theta\colon X \to \mathbb{Z}^X$ data nell'osservazione 5.6 soddisfa la seguente proprietà universale:*

$$\forall\, \alpha\colon X \to A \text{ applicazione } \exists!\, \Phi\colon \mathbb{Z}^X \to A \text{ omomorfismo } \mid\ \Phi \circ \theta = \alpha$$

Equivalentemente, il seguente diagramma di applicazioni è commutativo:



Dimostrazione. Sia innanzitutto $\alpha\colon X \to A$ un'applicazione fissata. Per l'osservazione 5.6 si ha che $\operatorname{Im}\theta$ è una base per $\mathbb{Z}^X$. Equivalentemente, per l'osservazione 5.7, posso supporre che $X = \{x_i\}_{i\in I}$ cosicché ogni elemento $\{y_x\}_{x\in X} \in \mathbb{Z}^X$ si possa scrivere in maniera unica come combinazione lineare finita a coefficienti interi di elementi in $\operatorname{Im}\theta$. Esplicitamente, questo equivale a richiedere che esista una e una sola collezione $\{n_i\}_{i\in I} \subseteq \mathbb{Z}$, con $n_i = 0$ per ogni $i \in I$ tranne che per un numero finito di indici, tale che valga la relazione $\{y_x\}_{x\in X} = \sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}$. Non vi è quindi ambiguità nel considerare la mappa $\Phi\colon \mathbb{Z}^X \to A$ data da:

$$\Phi\left(\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}\right) := \sum_{i\in I} n_i\alpha(x_i)$$

Siano ora $\{n_i\}_{i\in I}, \{m_i\}_{i\in I} \subseteq \mathbb{Z}$ collezioni qualunque. Per una proprietà delle potenze (osservazione 1.10) e per l'osservazione 5.5 si ha la condizione che segue e posso dunque affermare che Φ è un omomorfismo:

$$\begin{aligned}\Phi\left(\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} + \sum_{i\in I} m_i\{\theta_x(x_i)\}_{x\in X}\right) &= \Phi\left(\sum_{i\in I}(n_i + m_i)\{\theta_x(x_i)\}_{x\in X}\right)\\ &= \sum_{i\in I}(n_i + m_i)\alpha(x_i)\\ &= \sum_{i\in I} n_i\alpha(x_i) + \sum_{i\in I} m_i\alpha(x_i)\end{aligned}$$

Si consideri ora un indice fissato $i \in I$. Dalla costruzione di Φ segue immediatamente la relazione seguente:

$$(\Phi \circ \theta)(x_i) = \Phi\big(\theta(x_i)\big) = \Phi\big(\{\theta_x(x_i)\}_{x\in X}\big) = \alpha(x_i)$$

Sia infine $\Psi\colon \mathbb{Z}^X \to A$ un omomorfismo tale che $\Psi \circ \theta = \alpha$. Comunque fissata una collezione $\{n_i\}_{i\in I} \subseteq \mathbb{Z}$, vale in virtù dell'osservazione 3.4 e delle assunzioni fatte la condizione seguente:

$$\begin{aligned}\Psi\Big(\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}\Big) &= \sum_{i\in I} n_i\Psi\big(\{\theta_x(x_i)\}_{x\in X}\big)\\ &= \sum_{i\in I} n_i\Psi\big(\theta(x_i)\big)\\ &= \sum_{i\in I} n_i(\Psi\circ\theta)(x_i)\\ &= \sum_{i\in I} n_i\alpha(x_i)\end{aligned}$$

Questo dimostra che le applicazioni Φ e Ψ coincidono e quindi, non dipendendo il risultato ottenuto dalla scelta dell'omomorfismo $\Psi\colon \mathbb{Z}^X \to A$ tale che $\Psi \circ \theta = \alpha$, posso concludere che Φ è unico. □

Corollario 5.1. *Sia A un gruppo abeliano e sia $X \subseteq A$ un insieme di generatori. Allora esiste almeno un epimorfismo $\Phi\colon \mathbb{Z}^X \to A$. Da questo segue che ogni gruppo abeliano è isomorfo al quoziente di un gruppo abeliano libero.*

Dimostrazione. Si considerino la mappa inclusione $i\colon X \to A$ e un elemento fissato $a \in A$. Dalla proprietà universale dei gruppi abeliani liberi, vale a dire la proposizione 5.2, segue che esiste un unico omomorfismo $\Phi\colon \mathbb{Z}^X \to A$ tale che $\Phi \circ \theta = i$. Dal momento che per ipotesi $X \subseteq A$ è un insieme di generatori, esistono $x_1, \dots, x_k \in X$, $n_1, \dots, n_k \in \mathbb{Z}$ tali che $a = n_1x_1 + \cdots + n_kx_k$. Equivalentemente, utilizzando il fatto che $\Phi \circ \theta = i$, che Φ è un omomorfismo e applicando l'osservazione 3.4, si ha la condizione seguente:

$$\begin{aligned}a &= n_1x_1 + \cdots + n_kx_k\\ &= n_1i(x_1) + \cdots + n_ki(x_k)\\ &= n_1(\Phi\circ\theta)(x_1) + \cdots + n_k(\Phi\circ\theta)(x_k)\\ &= n_1\Phi\big(\theta(x_1)\big) + \cdots + n_k\Phi\big(\theta(x_k)\big)\\ &= \Phi\big(n_1\theta(x_1) + \cdots + n_k\theta(x_k)\big)\end{aligned}$$

Questo mostra che $a \in \operatorname{Im}\Phi$ e quindi, per arbitrarietà nella scelta di $a \in A$, posso affermare che $A \subseteq \operatorname{Im}\Phi$. L'altro contenimento è banale e di conseguenza Φ è un epimorfismo in quanto omomorfismo suriettivo. La parte successiva deriva immediatamente dall'osservazione 3.7, in virtù della quale $\mathbb{Z}^X/\operatorname{Ker}\Phi \simeq A$. □

Proposizione 5.3 (Caratterizzazione dei gruppi abeliani liberi come gruppi abeliani che ammettono una base)**.** *Sia A un gruppo abeliano e sia X una base per A. Allora $A \simeq \mathbb{Z}^X$.*

Dimostrazione. Per la definizione 5.3, se X è una base per A, allora $X \subseteq A$ è in particolare un insieme di generatori. Posso dunque applicare il corollario 5.1, in virtù del quale esiste un epimorfismo $\Phi\colon \mathbb{Z}^X \to A$. Dalla dimostrazione del corollario 5.1 segue inoltre che posso scegliere Φ tale che $\Phi \circ \theta = i$, dove $i\colon X \to A$ è la mappa inclusione. Come si è osservato invece nella dimostrazione della proposizione 5.2, se si assume che $X = \{x_i\}_{i\in I}$, allora per ogni $\{y_x\}_{x\in X} \in \mathbb{Z}^X$ esiste un'unica collezione $\{n_i\}_{i\in I} \subseteq \mathbb{Z}$, con $n_i = 0$ per ogni $i \in I$ tranne che per un numero finito di indici, tale che valga la relazione $\{y_x\}_{x\in X} = \sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}$. Utilizzando la condizione precedente, il fatto che Φ è un omomorfismo, che $\Phi \circ \theta = i$, l'osservazione 3.4 e soprattutto l'ipotesi che X sia una base per A, si ricava la condizione seguente:

$$\begin{aligned}\operatorname{Ker}\Phi &= \big\{ \textstyle\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} \in \mathbb{Z}^X \;\big|\; \Phi\big(\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}\big) = 0 \big\}\\ &= \big\{ \textstyle\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} \in \mathbb{Z}^X \;\big|\; \sum_{i\in I} n_i\Phi\big(\{\theta_x(x_i)\}_{x\in X}\big) = 0 \big\}\\ &= \big\{ \textstyle\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} \in \mathbb{Z}^X \;\big|\; \sum_{i\in I} n_i\Phi\big(\theta(x_i)\big) = 0 \big\}\\ &= \big\{ \textstyle\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} \in \mathbb{Z}^X \;\big|\; \sum_{i\in I} n_i(\Phi\circ\theta)(x_i) = 0 \big\}\\ &= \big\{ \textstyle\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} \in \mathbb{Z}^X \;\big|\; \sum_{i\in I} n_ii(x_i) = 0 \big\}\\ &= \big\{ \textstyle\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} \in \mathbb{Z}^X \;\big|\; \sum_{i\in I} n_ix_i = 0 \big\}\\ &= \big\{ \textstyle\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X} \in \mathbb{Z}^X \;\big|\; n_i = 0 \text{ per ogni } i \in I \big\} = \big\{\{0\}_{x\in X}\big\}\end{aligned}$$

Posso dunque affermare, in virtù della proposizione 3.1-(ii), che Φ è un'applicazione iniettiva, quindi un isomorfismo di gruppi. In particolare, posso concludere che $A \simeq \mathbb{Z}^X$ e dunque si ha la tesi. □

Il risultato che segue è essenzialmente il viceversa della proposizione 5.3.

Osservazione 5.8. Sia A un gruppo, con $A \simeq \mathbb{Z}^X$. Allora A è un gruppo abeliano che ammette una base.

Dimostrazione. Per ipotesi, esiste un isomorfismo $\eta\colon \mathbb{Z}^X \to A$. È immediato verificare che, essendo $\mathbb{Z}_X$ un gruppo abeliano per le definizioni 5.1 e 5.2 ed essendo $\mathbb{Z}^X \simeq A$, anche A è un gruppo abeliano. Basterà dunque mostrare che A ammette una base. Per l'osservazione 5.6, il gruppo abeliano libero $\mathbb{Z}^X$ ammette una base B. In virtù della definizione 5.3, si ha che $B \subseteq \mathbb{Z}^X$ è un insieme di generatori e che, comunque assegnati elementi $x_1, \dots, x_k \in B$, tali $x_1, \dots, x_k$ sono linearmente indipendenti. Essendo $\eta\colon \mathbb{Z}^X \to A$ un isomorfismo, per l'osservazione 1.18 si ha che $\eta(B) \subseteq A$ è un insieme di generatori. Si considerino adesso elementi $y_1, \dots, y_k \in \eta(B)$ e siano $n_1, \dots, n_k \in \mathbb{Z}$ tali che $n_1y_1 + \cdots + n_ky_k = 0$. Naturalmente, esistono per definizione di immagine elementi $x_1, \dots, x_k \in B$ tali che $\eta(x_j) = y_j$ per ogni indice $1 \leq j \leq k$ e quindi, essendo η un omomorfismo, posso applicare le osservazioni 3.1 e 3.4 per ottenere la relazione che segue:

$$\eta(\{0\}_{x\in X}) = 0 = n_1y_1 + \cdots + n_ky_k = n_1\eta(x_1) + \cdots + n_k\eta(x_k) = \eta(n_1x_1 + \cdots + n_kx_k)$$

A questo punto, usando il fatto che η è una funzione iniettiva e che B è una base per $\mathbb{Z}^X$, posso concludere che $n_j = 0$ per ogni $1 \leq j \leq k$ e questo dimostra, per arbitrarietà nella scelta degli elementi $n_1, \dots, n_k \in \mathbb{Z}$ tali che $n_1y_1 + \cdots + n_ky_k = 0$, che $y_1, \dots, y_k$ sono linearmente indipendenti. In definitiva, l'insieme $\eta(B)$ è una base per A in virtù della definizione 5.3 e questo conclude la dimostrazione. □

Teorema 5.1 (Invarianza del rango)**.** *Siano X e Y due insiemi. Allora $\mathbb{Z}^X \simeq \mathbb{Z}^Y$ se e solo se $|X| = |Y|$.*

Dimostrazione. Si osservi innanzitutto che, in virtù della definizione 5.2, il gruppo $\mathbb{Z}^X$ dipende soltanto da $|X|$ e quindi il viceversa è banale. Più precisamente, se $|X| = |Y|$, allora esiste un'applicazione biiettiva $f\colon X \to Y$ e posso quindi considerare l'applicazione $\Phi\colon \mathbb{Z}^X \to \mathbb{Z}^Y$ definita da $\Phi(\{y_x\}_{x\in X}) := \{y_{f(x)}\}_{x\in X}$, la quale è ovviamente un isomorfismo di gruppi. Si assuma adesso che $\mathbb{Z}^X \simeq \mathbb{Z}^Y$ e si distinguano due casi. La prima possibilità è che $|X| < +\infty$. Si consideri il gruppo $2\mathbb{Z}^X := \bigoplus_{x\in X} \langle 2\rangle$, dove ovviamente $\langle 2\rangle < \mathbb{Z}$. In virtù dell'osservazione 2.6, vale che $\langle 2\rangle \lhd \mathbb{Z}$ è un sottogruppo normale perché $\mathbb{Z}$ è un gruppo abeliano, ma allora posso applicare l'osservazione 4.20 e, ricordando l'esempio 2.6, si ottiene la condizione seguente:

$$\mathbb{Z}^X/2\mathbb{Z}^X \simeq \bigoplus_{x\in X} \mathbb{Z}/\langle 2\rangle \simeq \bigoplus_{x\in X} \mathbb{Z}_2$$

In particolare, dalla corrispondenza biunivoca tra insiemi segue immediatamente che $|\mathbb{Z}^X/2\mathbb{Z}^X| = 2^{|X|}$ e a questo punto, ripetendo lo stesso argomento con Y, si ricava che anche $|\mathbb{Z}^Y/2\mathbb{Z}^Y| = 2^{|Y|}$. Utilizzando ora l'ipotesi che $\mathbb{Z}^X \simeq \mathbb{Z}^Y$ posso affermare che $2^{|X|} = 2^{|Y|}$ e usando l'assunzione che $|X| < +\infty$ posso passare al logaritmo nella relazione precedente, ottenendo che $|X| = |Y|$. Se invece $|X| = +\infty$ allora, riapplicando l'argomento usato nella parte precedente della dimostrazione, si ottiene che $2^{|X|} = 2^{|Y|}$ e di conseguenza anche $|Y| = +\infty$. Adesso, non potendo passare al logaritmo, bisognerà dimostrare che $|X| = |\mathbb{Z}^X|$. Allo stesso modo, si dimostrerà che $|Y| = |\mathbb{Z}^Y|$ e usando infine l'ipotesi che $\mathbb{Z}^X \simeq \mathbb{Z}^Y$ sarà possibile concludere che $|X| = |Y|$. La dimostrazione dell'identità $|X| = |\mathbb{Z}^X|$ richiede la conoscenza di risultati particolari[22] di teoria degli insiemi e pertanto verrà tralasciata. □

Definizione 5.4. Sia X un insieme. La cardinalità di X viene detta il *rango di* $\mathbb{Z}^X$ e si denota $\mathrm{rk}(\mathbb{Z}^X)$.

La definizione 5.4 è ben posta per il teorema di invarianza del rango (teorema 5.1). Se infatti $\mathbb{Z}^X = \mathbb{Z}^Y$, allora in particolare varrà che $\mathbb{Z}^X \simeq \mathbb{Z}^Y$ e quindi $|X| = |Y|$. Adesso il teorema di invarianza del rango può essere riformulato dicendo che due gruppi abeliani liberi sono isomorfi se e solo se hanno lo stesso rango.

Corollario 5.2. *Sia A un gruppo abeliano e siano X e Y due basi per A. Allora $|X| = |Y|$.*

Dimostrazione. Essendo per ipotesi X e Y due basi per A, si può applicare la proposizione 5.3, in virtù della quale $A \simeq \mathbb{Z}^X$ e $A \simeq \mathbb{Z}^Y$. In particolare, si ottiene che $\mathbb{Z}^X \simeq \mathbb{Z}^Y$ e quindi l'asserto segue dal teorema di invarianza del rango (teorema 5.1). □

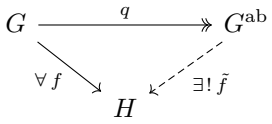
[22] Primo fra tutti il teorema di Schroeder-Bernstein, del quale si riporta l'enunciato: siano A e B insiemi. Se $|A| \leq |B|$ e $|B| \leq |A|$, allora $|A| = |B|$. Per una dimostrazione di questo risultato e per la parte finale di quella del teorema di invarianza del rango, si rimanda al libro *Algebra* di Thomas W. Hungerford.

A questo punto, si vogliono mettere in relazione gruppi liberi e gruppi abeliani liberi.

Osservazione 5.9 (Proprietà universale degli abelianizzati). Siano $(G, \cdot, e)$ un gruppo, $(H, +, 0)$ un gruppo abeliano e si consideri la mappa quoziente $q\colon G \to G^{\mathrm{ab}}$. Allora q soddisfa la seguente proprietà universale:

$$\forall\, f\colon G \to H \text{ omomorfismo } \exists!\, \tilde{f}\colon G^{\mathrm{ab}} \to H \text{ omomorfismo } \mid\ \tilde{f} \circ q = f$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



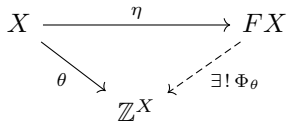
Dimostrazione. Ricordo, innanzitutto, che $G^{\mathrm{ab}} = G/[G,G]$ per la definizione 2.9 e considero una qualsiasi applicazione $f\colon G \to H$. Per la proprietà universale dei quozienti, vale a dire la proposizione 3.2-(ii), sarà sufficiente mostrare che $[G,G] \subseteq \operatorname{Ker} f$. Sia dunque $x \in [G,G]$ un elemento fissato. Per la definizione 2.8, esistono $a, b \in G$ tali che $x = a \cdot b \cdot a^{-1} \cdot b^{-1}$ ma allora, in virtù del fatto che f è un omomorfismo, posso applicare le osservazioni 3.2 e 3.4 per ottenere la condizione seguente, nella quale si rivela cruciale l'ipotesi che H sia un gruppo abeliano:

$$f(x) = f(a \cdot b \cdot a^{-1} \cdot b^{-1}) = f(a) + f(b) - f(a) - f(b) = 0$$

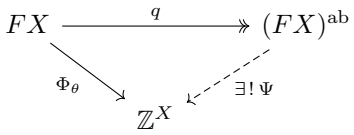
Per la definizione 3.1-(ii) si può dunque affermare che $x \in \operatorname{Ker} f$ e questo dimostra, per arbitrarietà nella scelta dell'elemento $x \in [G,G]$, che vale l'inclusione $[G,G] \subseteq \operatorname{Ker} f$. A questo punto, l'asserto non è altro che un caso particolare della proprietà universale dei quozienti. □

Osservazione 5.10. Sia X un insieme. Allora $\mathbb{Z}^X \simeq (FX)^{\mathrm{ab}}$.

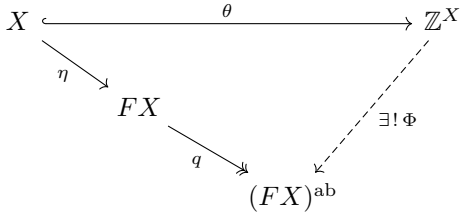
Dimostrazione. Si considerino l'applicazione $\eta\colon X \to FX$ definita da $\eta(x) := [x]$ e la funzione $\theta\colon X \to \mathbb{Z}^X$ definita nell'osservazione 5.6. Per la proprietà universale dei gruppi liberi, vale a dire la proposizione 4.5, esiste un unico omomorfismo $\Phi_\theta\colon FX \to \mathbb{Z}^X$ tale che $\Phi_\theta \circ \eta = \theta$, cioè tale che il seguente diagramma di applicazioni sia commutativo:



Sia ora $q\colon FX \to (FX)^{\mathrm{ab}}$ la mappa quoziente. Per la proprietà universale degli abelianizzati, vale a dire l'osservazione 5.9, esiste un unico omomorfismo $\Psi\colon (FX)^{\mathrm{ab}} \to \mathbb{Z}^X$ tale che $\Psi \circ q = \Phi_\theta$ oppure, in termini equivalenti, tale che il seguente diagramma di omomorfismi sia commutativo:



D'altra parte, per la proprietà universale dei gruppi abeliani liberi, cioè per la proposizione 5.2, esiste un unico omomorfismo $\Phi\colon \mathbb{Z}^X \to (FX)^{\mathrm{ab}}$ che soddisfi la relazione $\Phi \circ \theta = q \circ \eta$, cioè tale che sia commutativo il seguente diagramma di applicazioni:



A questo punto sarà sufficiente mostrare che Φ e Ψ sono l'una l'applicazione inversa dell'altra. Per farlo, si definiscano gli insiemi X^{-1}, $\tilde{X}$ come nella definizione 4.4 e si considerino le due estensioni $\tilde{\theta}\colon \tilde{X} \to \mathbb{Z}^X$,

$\tilde{\eta}\colon \tilde{X} \to FX$ delle funzioni θ e η date da $\tilde{\theta}(x) := \theta(x)$, $\tilde{\theta}(x^{-1}) := \theta(x)^{-1}$, $\tilde{\eta}(x) := \eta(x)$, $\tilde{\eta}(x^{-1}) := \eta(x)^{-1}$. Tali applicazioni sono ben definite perché $\mathbb{Z}^X$ e FX sono gruppi. Detto questo, dalle dimostrazioni delle proposizioni 3.2-(ii), 5.2 e dalla dimostrazione costruttiva della proposizione 4.5 si deduce facilmente che:

$$\Phi\left(\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}\right) = \sum_{i\in I} n_i(q\circ\eta)(x_i)\,, \quad \Psi\big([abc\dots z][G,G]\big) = \tilde{\theta}(a)+\tilde{\theta}(b)+\tilde{\theta}(c)+\cdots+\tilde{\theta}(z)$$

Come si è già osservato nella dimostrazione della proposizione 5.2, in virtù dell'osservazione 5.7, comunque assegnato un elemento $\{y_x\}_{x\in X} \in \mathbb{Z}^X$ esiste un'unica collezione $\{n_i\} \subseteq \mathbb{Z}$, con $n_i = 0$ per ogni $i \in I$ tranne che per un numero finito di indici, tale che valga la relazione $\{y_x\}_{x\in X} = \sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}$. Fatta questa premessa, usando il fatto che Ψ è un omomorfismo assieme all'osservazione 3.4, applicando le condizioni $\Psi\circ q = \Phi_\theta$, $\Phi_\theta\circ\eta = \theta$ e ricordando come si è definita l'applicazione θ nell'osservazione 5.6, si ottiene che:

$$\begin{aligned}\Psi\left(\Phi\left(\sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}\right)\right) &= \Psi\left(\sum_{i\in I} n_i(q\circ\eta)(x_i)\right)\\ &= \sum_{i\in I} n_i(\Psi\circ q\circ\eta)(x_i)\\ &= \sum_{i\in I} n_i\theta(x_i) = \sum_{i\in I} n_i\{\theta_x(x_i)\}_{x\in X}\end{aligned}$$

Questo dimostra che Ψ è un'inversa a sinistra di Φ. Sia adesso $[abc\dots z][G,G] \in G^{\mathrm{ab}}$ una qualsiasi classe laterale e si noti che, utilizzando il fatto che Φ e q sono omomorfismi assieme all'osservazione 3.4, usando la condizione $\Phi\circ\theta = q\circ\eta$ dalla quale segue immediatamente, per costruzione e per unicità dell'inverso, che $\Phi\circ\tilde{\theta} = q\circ\tilde{\eta}$ e tenendo a mente la definizione data dell'applicazione $\tilde{\eta}$, si ottiene la relazione seguente:

$$\begin{aligned}\Phi\big(\Psi([abc\dots z][G,G])\big) &= \Phi\big(\tilde{\theta}(a)+\tilde{\theta}(b)+\tilde{\theta}(c)+\cdots+\tilde{\theta}(z)\big)\\ &= \Phi\big(\tilde{\theta}(a)\big)\cdot\Phi\big(\tilde{\theta}(b)\big)\cdot\Phi\big(\tilde{\theta}(c)\big)\cdots\Phi\big(\tilde{\theta}(z)\big)\\ &= q\big(\tilde{\eta}(a)\big)\cdot q\big(\tilde{\eta}(b)\big)\cdot q\big(\tilde{\eta}(c)\big)\cdots q\big(\tilde{\eta}(z)\big)\\ &= q\big([a]\big)\cdot q\big([b]\big)\cdot q\big([c]\big)\cdots q\big([z]\big)\\ &= q\big([a]\cdot[b]\cdot[c]\cdots\big)\\ &= q\big([abc\dots z]\big) = [abc\dots z][G,G]\end{aligned}$$

Avendo dunque mostrato che Ψ è anche un'inversa a destra di Φ, posso concludere che Φ è un isomorfismo di gruppi in quanto omomorfismo biiettivo e da questo discende immediatamente la tesi. □

5.3 Gruppi abeliani finitamente generati

Sia A è un gruppo abeliano finitamente generato. Per la definizione 4.10, esiste un insieme di generatori $X \subseteq A$ tale che $|X| < +\infty$. Posto $n := |X|$ esiste, in virtù del corollario 5.1, un sottogruppo $H < \mathbb{Z}^n$ tale che $A \simeq \mathbb{Z}^n/H$. Si osservi che il gruppo quoziente $\mathbb{Z}^n/H$ è ben definito in quanto, essendo $\mathbb{Z}^n$ un gruppo abeliano (osservazione 5.4), ogni suo sottogruppo è normale (osservazione 2.6). Questa semplice premessa mostra che le proprietà dei gruppi abeliani finitamente generati si possono dedurre riducendosi allo studio dei sottogruppi di $\mathbb{Z}^n$ e giustifica quindi l'importanza del seguente risultato. Prima occorre dare tuttavia una definizione.

Definizione 5.5. Un gruppo F viene detto un *gruppo abeliano libero* se esiste $n \in \mathbb{N}^*$ tale che $F \simeq \mathbb{Z}^n$. Un tale $n \in \mathbb{N}^*$ si dice inoltre il *rango di* F e si denota $\mathrm{rk}(F)$.

La definizione 5.5 è ben posta per il teorema di invarianza del rango (teorema 5.1).

Teorema 5.2 (Sottogruppi di $\mathbb{Z}^n$)**.** *Sia F un gruppo abeliano libero di rango n e sia $G < F$ un sottogruppo non banale. Allora esistono una base $\{x_1,\dots,x_n\}$ per F, un intero $1 \le r \le n$ ed elementi $d_1,\dots,d_r \in \mathbb{N}^*$ con $d_1 \mid d_2 \mid \cdots \mid d_r$ tali che G sia un gruppo abeliano libero con base $\{d_1x_1,\dots,d_rx_r\}$.*

Dimostrazione. Si procede per induzione su $n \in \mathbb{N}^*$. La base di induzione, corrispondente al caso $n = 1$, si dimostra come segue. Innanzitutto, vale naturalmente che $\mathbb{Z}^1 \simeq \mathbb{Z}$ e quindi, per ipotesi e in virtù della

definizione 5.5, si ha che $F \simeq \mathbb{Z}$. In altre parole, esiste un isomorfismo $\eta\colon \mathbb{Z} \to F$. Dato che $\mathbb{Z} = \langle 1 \rangle$, vale che $F = \langle \eta(1) \rangle$ per l'osservazione 1.18, mentre l'osservazione 1.5 e il fatto che η sia una funzione iniettiva garantiscono che $\eta(1) \neq 0$. Sia adesso $k \in \mathbb{Z}$ tale che $k\eta(1) = 0$. Per le osservazioni 1.5 e 1.16, la suddetta condizione equivale a richiedere che $\eta(k \cdot 1) = \eta(0)$ e quindi, per iniettività di η, dovrà valere che $k \cdot 1 = 0$. Tale relazione implica che $k = 0$ e posso dunque affermare, per arbitrarietà nella scelta di $k \in \mathbb{Z}$, che $\eta(1)$ è linearmente indipendente. Questo dimostra che $\{\eta(1)\}$ è una base per F e di conseguenza posso scegliere $x_1 := \eta(1)$ nell'enunciato del teorema. Ora, essendo F un gruppo ciclico, posso usare l'osservazione 1.19 per ottenere che esiste $m \in \mathbb{N}$ tale che $G = \langle m\eta(1) \rangle$ e inoltre $m \neq 0$ poiché si sta assumendo che G sia non banale. Applicando un argomento sostanzialmente identico a quello utilizzato per dimostrare che $\eta(1)$ è linearmente indipendente, si vede facilmente che lo è anche $m\eta(1)$ e posso quindi concludere che $\{m\eta(1)\}$ è una base per G, cioè che vale quanto riportato nell'enunciato prendendo $r := 1$ e $d_1 := m$.

Nel passo di induzione assumo quindi $n \geq 2$, suppongo che il teorema sia vero per un generico $n-1$ e ne dimostro la validità per n. Si consideri il seguente sottoinsieme di $\mathbb{Z}$:

$$S := \left\{ s \in \mathbb{Z} \;\middle|\; sy_1 + k_2y_2 + \cdots + k_ny_n \in G\,,\, \exists \{y_1, \ldots, y_n\} \text{ base per } F\,,\, k_2, \ldots, k_n \in \mathbb{Z} \right\}$$

Per la definizione 5.5 e in virtù dell'osservazione 5.8, il gruppo abeliano libero F ammette sicuramente una base $\{y_1, \ldots, y_n\}$ dunque, prendendo $k_i := 0$ per ogni $2 \leq i \leq n$ e usando il fatto che $0 \in G$ essendo $G < F$ un sottogruppo, posso affermare che $0 \in S$. In particolare, deduco che S è un insieme non vuoto. Adesso osservo che, comunque assegnato un elemento $s \in S$, per costruzione esistono una base $\{y_1, \ldots, y_n\}$ per F ed elementi $k_2, \ldots, k_n \in \mathbb{Z}$ tali che $sy_1 + k_2y_2 + \cdots + k_ny_n \in G$, ma ovviamente anche $\{y_2, y_1, y_3, \ldots, y_n\}$ è una base per F e $k_2y_2 + sy_1 + k_3y_3 + \cdots + k_ny_n \in G$ essendo G un gruppo abeliano. Questo dimostra che anche $k_2 \in S$ e analogamente $k_3, \ldots, k_n \in S$. A questo punto distinguo due possibilità, a seconda che $S \cap \mathbb{N}^*$ sia o no un insieme non vuoto. Se tale insieme è vuoto, allora $S = \langle d_1 \rangle$ con $d_1 := 0$, mentre posso definire $d_1 := \min(S \cap \mathbb{N}^*)$ se $S \cap \mathbb{N}^*$ è non vuoto. Dimostro che, anche in questo caso, si ha che $S = \langle d_1 \rangle$. Assegnato un elemento $d \in \langle d_1 \rangle$ osservo che, in virtù dell'osservazione 1.13, esiste un elemento $k \in \mathbb{Z}$ tale che $d = kd_1$. Inoltre, notando che $d_1 \in S$ per costruzione, esistono una base $\{y_1, \ldots, y_n\}$ per F ed elementi $k_2, \ldots, k_n \in \mathbb{Z}$ tali che $g \in G$, dove $g := d_1y_1 + k_2y_2 + \cdots + k_ny_n$. Ma allora, dato che per ipotesi $G < F$ è un sottogruppo, posso affermare che anche $kg \in G$ e questo dimostra che $kd_1 \in S$, cioè che $d \in S$. Posso dunque concludere che $\langle d_1 \rangle \subseteq S$. Adesso suppongo per assurdo che esista un certo indice $2 \leq j \leq n$ tale che $d_1 \nmid k_j$. In tal caso, per l'algoritmo della divisione euclidea, esisterebbero $q, t \in \mathbb{Z}$ con $0 < t < d_1$ tali che $k_j = qd_1 + t$. Ora, posto $y_1' := y_1 + qy_j$, osservo che $\{y_1', y_2, \ldots, y_n\}$ è ancora una base per F. Si noti infatti che $y_1 = y_1' - qy_j$ e che, per ogni $m_1, \ldots, m_n \in \mathbb{Z}$ tali che $m_1y_1' + m_2y_2 + \cdots + m_ny_n = 0$, cioè tali che $m_1y_1 + \cdots + (m_j + qm_1)y_j + \cdots + m_ny_n = 0$, per indipendenza lineare degli elementi $y_1, \ldots, y_n$ vale che $m_i = 0$ per ogni $1 \leq i \leq n$ e dunque anche $y_1', y_2, \ldots, y_n$ sono linearmente indipendenti. Detto questo, nella base $\{y_1', y_2, \ldots, y_n\}$ si ha che $g = d_1y_1' + \cdots + ty_j + \cdots + k_ny_n$ e ricordando quanto si è discusso in precedenza anche $t \in S$, contraddicendo la minimalità di d_1. Di conseguenza, vale per ogni $2 \leq i \leq n$ che $d_1 \mid k_i$. Sia adesso $h \in G$ un elemento qualsiasi. Essendo $G \subseteq \langle y_1, \ldots, y_n \rangle$, esistono $l_1, \ldots, l_n \in \mathbb{Z}$ tali che $h = l_1y_1 + \cdots + l_ny_n$. Suppongo per assurdo che $d_1 \nmid l_1$ e noto che, applicando l'algoritmo della divisione euclidea, si ottengono elementi $q, t \in \mathbb{Z}$ con $0 < t < d_1$ tali che $l_1 = qd_1 + t$ e dunque si ha la condizione:

$$h - qg = ty_1 + (l_2 - qk_2)y_2 + \cdots + (l_n - qk_n)y_n$$

Essendo $G < F$ un sottogruppo, vale che $h - qg \in G$ e quindi $t \in S$, contraddicendo la minimalità di d_1. Posso dunque affermare che $d_1 \mid l_1$, cioè che esiste un elemento $q \in \mathbb{Z}$ tale che $l_1 = qd_1$. Si osservi ora che:

$$h - (q-1)g = d_1y_1 + \big(l_2 - (q-1)k_2\big)y_2 + \cdots + \big(l_n - (q-1)k_n\big)y_n$$

Ripetendo lo stesso argomento utilizzato per dimostrare che $d_1 \mid k_i$ per ogni $2 \leq i \leq n$ posso affermare che, fissato un indice $2 \leq i \leq n$, vale che $d_1 \mid l_i - (q-1)k_i$, cioè che esiste $a_i \in \mathbb{Z}$ tale che $l_i - (q-1)k_i = a_id_1$. Siccome $d_1 \mid k_i$, esiste $b_i \in \mathbb{Z}$ tale che $k_i = b_id_1$, ma allora $l_i = \big((q-1)b_i + a_i\big)d_1$ e questo mi permette di affermare che $d_1 \mid l_i$ per ogni $2 \leq i \leq n$. Si consideri ora una qualunque base $\{z_1, \ldots, z_n\}$ per F. Essendo $G \subseteq \langle z_1, \ldots, z_n \rangle$, comunque fissato un indice $1 \leq i \leq n$ esistono elementi $\alpha_{i1}, \ldots, \alpha_{in} \in \mathbb{Z}$ tali che valga la condizione $y_i = \sum_{j=1}^{n} \alpha_{ij}z_j$. Si ricava quindi la relazione seguente:

$$h = \sum_{i=1}^{n} l_iy_i = \sum_{i=1}^{n} l_i\left(\sum_{j=1}^{n} \alpha_{ij}z_j\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} \alpha_{ij}l_i\right)z_j$$

Poiché $d_1 \mid l_i$ per ogni $1 \leq i \leq n$, esistono $c_i \in \mathbb{Z}$ tali che $l_i = c_i d_1$, ma allora $\sum_{i=1}^{n} \alpha_{ij} l_i = (\sum_{i=1}^{n} \alpha_{ij} c_i) d_1$ per ogni $1 \leq j \leq n$ e posso quindi affermare che, data una qualsiasi base per F, l'elemento d_1 divide tutti i coefficienti di una combinazione lineare di h in quella determinata base. A questo punto, comunque fissato un elemento $s \in S$, per definizione di S esistono una base $\{z_1, \dots, z_n\}$ per F ed elementi $l_2, \dots, l_n \in \mathbb{Z}$ tali che $sz_1 + l_2 z_2 + \cdots + l_n z_n \in G$ e quindi, in vista della discussione precedente, vale che $d_1 \mid s$. Ciò significa che esiste $k \in \mathbb{Z}$ tale che $s = kd_1$, cioè che $s \in \langle d_1 \rangle$. Avendo mostrato anche l'inclusione $S \subseteq \langle d_1 \rangle$, posso concludere che $S = \langle d_1 \rangle$.

Adesso dimostro che esiste un elemento $x_1 \in G$ tale che $\{x_1, y_2, \dots, y_n\}$ sia una base per F e $d_1 x_1 \in G$. Per farlo, considero l'elemento $g \in G$ e ricordo che $k_i = b_i d_1$ per ogni $2 \leq i \leq n$. Di conseguenza, ponendo $x_1 := y_1 + b_2 y_2 + \cdots + b_n y_n$, vale che $d_1 x_1 \in G$ per costruzione. Rimane da mostrare che $\{x_1, y_2, \dots, y_n\}$ è una base per F. Innanzitutto, è evidente che $F = \langle x_1, y_2, \dots, y_n \rangle$ in quanto $y_1 = x_1 - b_2 y_2 - \cdots - b_n y_n$. D'altra parte, comunque assegnati $m_1, \dots, m_n \in \mathbb{Z}$ tali che $m_1 x_1 + m_2 y_2 + \cdots + m_n y_n = 0$, cioè tali che $m_1 y_1 + (m_2 + b_2 m_1) y_2 + \cdots + (m_n + b_n m_1) y_n = 0$, per l'indipendenza lineare degli elementi $y_1, \dots, y_n$ si ha che $m_i = 0$ per ogni $1 \leq i \leq n$ e dunque anche $x_1, y_2, \dots, y_n$ sono linearmente indipendenti. Concludo che $\{x_1, y_2, \dots, y_n\}$ è effettivamente una base per F.

Sia ora $H := \langle y_2, \dots, y_n \rangle$ e si osservi che $y_2, \dots, y_n$ sono linearmente indipendenti come conseguenza immediata del fatto che lo sono $y_1, \dots, y_n$. Si può dunque affermare che $\{y_2, \dots, y_n\}$ è una base per H e quindi $H \simeq \mathbb{Z}^{n-1}$ in virtù della proposizione 5.3. Per la definizione 5.5 questo è equivalente a dire che H è un gruppo abeliano libero di rango $n-1$. Adesso, ricordando che il prodotto diretto di una collezione finita di gruppi coincide con la somma diretta, dimostro che $F \simeq \langle x_1 \rangle \oplus H$. Per farlo, basterà applicare la proposizione 4.8. Noto innanzitutto che la condizione (iii.b) è automaticamente verificata in virtù del fatto che ogni sottogruppo di un gruppo abeliano è un sottogruppo normale (osservazione 2.6). Sia adesso $v \in \langle x_1 \rangle \cap H$. In tal caso, esistono $l_1, \dots, l_n \in \mathbb{Z}$ tali che $v = l_1 x_1$, $v = l_2 y_2 + \cdots + l_n y_n$ e di conseguenza, sottraendo membro a membro le due relazioni precedenti, si ottiene che $l_1 x_1 - l_2 y_2 - \cdots - l_n y_n = 0$. Per indipendenza lineare degli elementi $x_1, y_2, \dots, y_n$ dovrà quindi valere che $l_i = 0$ per ogni indice $1 \leq i \leq n$ e in particolare $v = 0$. Questo dimostra, per arbitrarietà di $v \in \langle x_1 \rangle \cap H$, il contenimento $\langle x_1 \rangle \cap H \subseteq \{0\}$, mentre l'altra inclusione è immediata. Inoltre, si vede assai facilmente che $F = \langle x_1 \rangle + H$ in quanto la base $\{x_1, y_2, \dots, y_n\}$ è data dall'unione delle basi $\{x_1\}$ e $\{y_2, \dots, y_n\}$. A tal proposito, va notato che l'elemento x_1 è linearmente indipendente. Assegnato infatti $n \in \mathbb{Z}$ tale che $nx_1 = 0$, è del tutto equivalente richiedere che valga $nx_1 + 0y_2 + \cdots + 0y_n = 0$ e quindi $n = 0$ per indipendenza lineare di $x_1, y_2, \dots, y_n$. Fatte queste considerazioni posso affermare, per la proposizione 4.8 già menzionata, che $F \simeq \langle x_1 \rangle \oplus H$. Con lo stesso metodo si vuole dimostrare che $G \simeq \langle d_1 x_1 \rangle \oplus (G \cap H)$. Come prima, la condizione (iii.b) è un'immediata conseguenza del fatto che F è un gruppo abeliano. Stavolta, anche la condizione (ii) è automaticamente verificata in quanto $\langle d_1 x_1 \rangle \cap (G \cap H) \subseteq \langle x_1 \rangle \cap H \subseteq \{0\}$, mentre l'altra inclusione è banale. Si consideri adesso un elemento $v \in G$. Dal momento che $G \subseteq \langle x_1, y_2, \dots, y_n \rangle$, esistono elementi $t_1, \dots, t_n \in \mathbb{Z}$ tali che $v = t_1 x_1 + t_2 y_2 + \cdots + t_n y_n$. Adesso, se $d_1 = 0$ allora, comunque fissato un indice $1 \leq i \leq s$, si deve avere che $t_i = 0$ in quanto $t_i \in S$ per costruzione e $S = \langle d_1 \rangle$. In particolare, si ottiene che $v = 0$ e di conseguenza $v \in \langle d_1 x_1 \rangle + (G \cap H)$ banalmente. Se invece $d_1 \neq 0$ allora, comunque vengano scelti una base per F e un elemento $h \in G$, l'elemento d_1 divide i coefficienti di una combinazione lineare di h nella base assegnata. In questo caso, dunque, si ha che $d_1 \mid t_1$, cioè esiste un elemento $q_1 \in \mathbb{Z}$ tale che $t_1 = q_1 d_1$. Detto questo, osservo che $q_1 d_1 x_1 \in \langle d_1 x_1 \rangle$, mentre $t_2 y_2 + \cdots + t_n y_n \in G \cap H$ in quanto $t_2 y_2 + \cdots + t_n y_n = v - q_1 d_1 x_1$, $v - q_1 d_1 x_1 \in G$ e $H = \langle y_2, \dots, y_n \rangle$. Di conseguenza $v \in \langle d_1 x_1 \rangle + (G \cap H)$ e quindi, per arbitrarietà nella scelta di $v \in G$, posso affermare che $G \subseteq \langle d_1 x_1 \rangle + (G \cap H)$. Ovviamente, l'altra inclusione è banale, per cui posso riapplicare la proposizione 4.8 ottenendo che $G \simeq \langle d_1 x_1 \rangle \oplus (G \cap H)$.

A questo punto, se $G \cap H = \{0\}$, allora $G = \langle d_1 x_1 \rangle$ per la discussione precedente. È inoltre immediato verificare che $d_1 x_1$ è linearmente indipendente come conseguenza del fatto che lo è l'elemento x_1 e in virtù dell'ipotesi che $G < F$ sia un sottogruppo non banale, per cui $d_1 \neq 0$. Questo mi consente di affermare che $\{d_1 x_1\}$ è una base per G e di conseguenza vale precisamente quanto si voleva dimostrare con $r := 1$. Se invece si ha $G \cap H \neq \{0\}$, allora sarà sufficiente applicare l'ipotesi induttiva al gruppo abeliano libero H di rango $n-1$ e al suo sottogruppo $G \cap H < H$. Così facendo, si deduce che esistono $x_2, \dots, x_n \in G$ tali che $\{x_2, \dots, x_n\}$ sia una base per H, un elemento $2 \leq r \leq n$ e certi $d_2, \dots, d_r \in \mathbb{N}^*$ tali che $d_2 \mid d_3 \mid \cdots \mid d_r$ e tali che $G \cap H$ sia un gruppo abeliano libero con base $\{d_2 x_2, \dots, d_r x_r\}$. Si osservi adesso che, essendo $F = \langle x_1 \rangle + H$ ed essendo $H = \langle x_2, \dots, x_n \rangle$, vale banalmente la relazione $F = \langle x_1, \dots, x_n \rangle$. Siano inoltre $m_1, \dots, m_n \in \mathbb{Z}$ tali che $m_1 x_1 + \cdots + m_n x_n = 0$. In altre parole, si ha che $m_2 x_2 + \cdots + m_n x_n = -m_1 x_1$ e in particolare tale elemento appartiene a $\langle x_1 \rangle \cap H$. Ricordo però che $\langle x_1 \rangle \cap H = \{0\}$ e dunque vale che $-m_1 x_1 = 0$, $m_2 x_2 + \cdots + m_n x_n = 0$. Per indipendenza lineare di x_1 e di $x_2, \dots, x_n$ si può affermare che

$m_i = 0$ per ogni $1 \leq i \leq n$ e questo mostra che gli elementi $x_1, \ldots, x_n$ sono linearmente indipendenti. Si deduce quindi che $\{x_1, \ldots, x_n\}$ è una base per F e analogamente, essendo $G \simeq \langle d_1 x_1 \rangle \oplus (G \cap H)$, vale che $\{d_1 x_1, \ldots, d_r x_r\}$ è una base per G. In particolare, per dimostrare il fatto che $d_1 x_1, \ldots, d_r x_r$ sono elementi linearmente indipendenti, bisognerà scartare il caso $d_1 = 0$. Se infatti fosse $d_1 = 0$ allora, ricordando che $G = \langle d_1 x_1 \rangle + (G \cap H)$, si dovrebbe avere che $G = G \cap H$, cioè che $G \subseteq H$, ma allora $x_1 \in \langle y_2, \ldots, y_n \rangle$ in quanto $x_1 \in G$ e $H = \langle y_2, \ldots, y_n \rangle$. In particolare, varrebbe la condizione $x_1 = l_2 y_2 + \cdots + l_n y_n$ e questo contraddice il fatto che $x_1, y_2, \ldots, y_n$ sono linearmente indipendenti. L'unica possibilità accettabile è che valga $d_1 \neq 0$ e dunque, essendo $d_1 x_1$ linearmente indipendente sotto tale condizione, per dimostrare che gli elementi $d_1 x_1, \ldots, d_r x_r$ sono linearmente indipendenti sarà sufficiente riapplicare l'argomento usato prima per dimostrare l'indipendenza lineare di $x_1, \ldots, x_n$. Per concludere la dimostrazione, si noti che $d_2 x_2 \in G$ per costruzione e si ricordi che, assegnati una base per F e un elemento $h \in G$, l'elemento d_1 divide ciascun coefficiente di una combinazione lineare di h nella base fissata. In particolare, posso affermare che $d_1 \mid d_2$ e dunque si ha la tesi. □

Dal teorema 5.2 e dalla proposizione 5.3 deriva immediatamente il seguente risultato.

Corollario 5.3. *Ogni sottogruppo non banale $G < \mathbb{Z}^n$ è un gruppo abeliano libero di rango $r \leq n$.*

A questo punto, si vogliono classificare tutti i gruppi abeliani finitamente generati. Per farlo, tuttavia, sarà necessario introdurre la seguente definizione.

Definizione 5.6. Siano A un gruppo abeliano, $m \in \mathbb{N}^*$ e sia p un numero primo.

(i) L'insieme $mA := \{\, ma \mid a \in A \,\}$ viene detto il *sottogruppo dei multipli di m in A*.

(ii) L'insieme $A[m] := \{\, a \in A \mid ma = 0 \,\}$ prende il nome di *m-torsione di A*.

(iii) L'insieme $A(p) := \{\, a \in A \mid p^k a = 0 \text{ per qualche } k \in \mathbb{N} \,\}$ è detto il *p-sottogruppo di A*.

(iv) L'insieme $A_{\text{tor}} := \{\, a \in A \mid a \text{ è un elemento di ordine finito} \,\}$ si dice la *torsione di A*.

Osservazione 5.11. Sia A un gruppo abeliano e sia p un numero primo. Allora vale la seguente relazione:

$$A(p) = \{\, a \in A \mid o(a) = p^k \text{ per qualche } k \in \mathbb{N} \,\}$$

Dimostrazione. Sia $a \in A$ un elemento prefissato. Chiaramente, se $o(a) = p^k$ per un qualche $k \in \mathbb{N}$, allora $p^k a = 0$ per la definizione 1.10. Se invece assumo che $p^k a = 0$ per un certo $k \in \mathbb{N}$, allora $o(a) \mid p^k$ in virtù dell'osservazione 1.15 e di conseguenza esiste $h \in \mathbb{Z}$ tale che $p^k = o(a)h$. Dato che in $\mathbb{Z}$ vale l'unicità della fattorizzazione in primi, dovrà necessariamente valere che $o(a)$ è una potenza di p, cioè che $o(a) = p^l$ per un certo $l \in \mathbb{N}$ e dunque si ha la tesi. □

Osservazione 5.12. Siano A un gruppo abeliano, $m \in \mathbb{N}^*$ e sia p un numero primo. Allora ciascun insieme introdotto nella definizione 5.6 è un sottogruppo di A.

Dimostrazione.

(i) Siano $x, y \in mA$ due elementi prefissati e si osservi che, per la definizione 5.6-(i), esistono $a, b \in A$ tali che $x = ma$, $y = mb$. Dato che per ipotesi A è un gruppo abeliano, posso usare la proprietà delle potenze data dall'osservazione 1.11, ottenendo la condizione seguente:

$$x + y = ma + mb = m(a + b)$$

Ne segue che $x + y \in A$ e questo dimostra, per arbitrarietà nella scelta degli elementi $x, y \in mA$, che $mA \subseteq A$ è un sottoinsieme chiuso rispetto all'operazione binaria $+$ su A. Si osservi adesso che $0 \in mA$ in quanto $0 \in A$ e $m0 = 0$ per definizione di gruppo e di elemento neutro. Si noti infine che $-x \in mA$ poiché $-ma = m(-a)$ per una proprietà delle potenze (osservazione 1.10) e $-a \in A$ essendo A un gruppo. Non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $x \in mA$, posso concludere che $mA < A$ è un sottogruppo.

(ii) Siano $a, b \in A[m]$ elementi fissati. Ricordando la definizione 5.6-(ii) e applicando la proprietà delle potenze fornita dall'osservazione 1.11, si ottiene la condizione seguente:

$$m(a+b) = ma + mb = 0 + 0 = 0$$

Questo dimostra che $a + b \in A[m]$ ma allora, poiché il risultato ottenuto non dipende dalla scelta degli elementi $a, b \in A$, posso affermare che $A[m] \subseteq A$ è chiuso rispetto all'operazione binaria $+$ su A. Si noti adesso che $0 \in A[m]$ banalmente, in quanto $m0 = 0$ per definizione di elemento neutro. Infine, per una proprietà delle potenze (osservazione 1.10) posso affermare che $m(-a) = -ma = 0$ e di conseguenza $-a \in A[m]$. Per arbitrarietà nella scelta dell'elemento $a \in A$, si può concludere che $A[m] < A$ è un sottogruppo.

(iii) Siano $a, b \in A(p)$ due elementi fissati. Per la definizione 5.6-(iii) esistono $k, h \in \mathbb{N}$ tali che $p^k a = 0$, $p^h b = 0$ e quindi, assumendo senza perdita di generalità $k \geq h$, per le proprietà delle potenze si ha:

$$p^k(a+b) = p^k a + p^k b = p^k a + p^{k-h}(p^h b) = 0 + p^{k-h}0 = 0$$

Posso dunque affermare che $a + b \in A(p)$ e siccome il risultato ottenuto non dipende dalla scelta degli elementi $a, b \in A(p)$ posso affermare che $A(p) \subseteq A$ è chiuso rispetto all'operazione binaria $+$ su A. Si noti ora che $p^k 0 = 0$ per ogni $k \in \mathbb{N}$ e quindi $0 \in A(p)$. Infine, poiché $p^k(-a) = -p^k a = 0$, vale che $-a \in A(p)$ e posso quindi concludere, per arbitrarietà nella scelta dell'elemento $a \in A(p)$, che $A(p) < A$ è un sottogruppo.

(iv) Siano $a, b \in A_{\text{tor}}$ elementi prefissati. In virtù della definizione 5.6-(iv) esistono $n, m \in \mathbb{N}^*$ tali che $na = 0$, $mb = 0$ ma allora, applicando le proprietà delle potenze, si ottiene la condizione seguente:

$$nm(a+b) = (nm)a + (nm)b = m(na) + n(mb) = m0 + n0 = 0$$

Di conseguenza, vale che $a + b \in A_{\text{tor}}$ e da questo posso dedurre, per arbitrarietà nella scelta degli elementi $a, b \in A_{\text{tor}}$, che $A_{\text{tor}} \subseteq A$ è un sottoinsieme chiuso rispetto all'operazione binaria $+$ su A. Si osservi adesso che $0 \in A_{\text{tor}}$ in quanto 0 è banalmente un elemento di ordine 1 e che $-a \in A_{\text{tor}}$ perché $n(-a) = -na = 0$ per una proprietà delle potenze (osservazione 1.10). Si può concludere quindi che $A_{\text{tor}} < A$ è un sottogruppo e questo conclude la dimostrazione. □

Osservazione 5.13. Siano A un gruppo abeliano, $m \in \mathbb{N}^*$ e sia p un numero primo. Valgono le proprietà:

(i) $A[m] < A_{\text{tor}}$.

(ii) $A(p) = \bigcup_{k=0}^{\infty} A[p^k]$ e in particolare $A(p) < A_{\text{tor}}$.

(iii) $A_{\text{tor}} \simeq \bigoplus_{p \text{ primo}} A(p)$.

Dimostrazione.

(i) In vista dell'osservazione 5.12, basterà mostrare che $A[m] \subseteq A_{\text{tor}}$. Fissato un elemento $a \in A[m]$, per la definizione 5.6-(ii) si ha la condizione $ma = 0$, ma allora $o(a) \mid m$ per l'osservazione 1.15 e in particolare a è un elemento di ordine finito, cioè $a \in A_{\text{tor}}$. Non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $a \in A[m]$, posso concludere che $A[m] \subseteq A_{\text{tor}}$ e di conseguenza $A[m] < A_{\text{tor}}$ è un sottogruppo.

(ii) La prima affermazione deriva banalmente dalla definizione 5.6, la seconda invece è un'immediata conseguenza della prima e del punto (i) appena dimostrato. Infatti, comunque fissato un elemento $a \in A(p)$, esiste $k \in \mathbb{N}$ tale che $a \in A[p^k]$ e di conseguenza $a \in A_{\text{tor}}$ per il punto (i) già dimostrato.

(iii) Si consideri l'applicazione $\Phi \colon \bigoplus_{p \text{ primo}} A(p) \to A_{\text{tor}}$ data da $\Phi(\{x_p\}_{p \text{ primo}}) = \sum_{p \text{ primo}} x_p$ e si noti che la somma è finita in quanto $x_p = 0$ per ogni primo p tranne che per un numero finito di primi. Osservo anche che, comunque assegnato un primo p, per costruzione vale che $x_p \in A(p)$ e dunque esiste un certo $k_p \in \mathbb{N}$ tale che $p^{k_p} x_p = 0$. Inoltre, se $x_p = 0$, allora posso scegliere in particolare $k_p := 1$. In virtù di questo fatto, l'elemento $\sum_{p \text{ primo}} x_p$ ha ordine finito per costruzione in quanto:

$$\prod_{p \text{ primo}} p^{k_p} \sum_{p \text{ primo}} x_p = 0$$

Ne segue che Φ è una mappa ben definita. È immediato verificare che Φ è un omomorfismo perché si assume che A sia un gruppo abeliano. Per dimostrare che Φ è un'applicazione iniettiva, pongo:

$$\sum_{p\,\text{primo}} A(p) := \{\, x_1 + \cdots + x_h \mid x_i \in A(p_i) \text{ per ogni } 1 \leq i \leq h\,, \text{ per certi primi } p_1, \ldots, p_h \,\}$$

Si considerino quindi un numero primo p prefissato e un elemento $x \in A(p) \cap (\sum_{q\,\text{primo},\, q\neq p} A(q))$. Dalla definizione precedente segue assai facilmente che esistono $q_1, \ldots, q_h$ primi con $q_i \neq p$ per ogni $1 \leq i \leq h$ e certi $x_1 \in A(q_1), \ldots, x_h \in A(q_h)$ tali che $x = x_1 + \cdots + x_h$. Si può dunque applicare l'osservazione 5.11, in virtù della quale esistono $k, k_1, \ldots, k_h \in \mathbb{N}$ tali che $o(x) = p^k$, $o(x_i) = q_i^{k_i}$ per ogni $1 \leq i \leq h$. Ora dimostro, per induzione su $1 \leq h \leq n$, che $o(x_1 + \cdots + x_h) = \prod_{i=1}^{h} q_i^{k_i}$. La base di induzione, che corrisponde al caso $h = 1$, è banalmente verificata. Nel passo induttivo assumo dunque $h \geq 2$ e suppongo che $o(x_1 + \cdots + x_{h-1}) = \prod_{i=1}^{h-1} q_i^{k_i}$. Inoltre, si può definire per semplicità $y := x_1 + \cdots + x_{h-1}$. Sarà sufficiente dimostrare che $o(y + x_h) = o(y)o(x_h)$. Si osservi che, in virtù dell'ipotesi che A sia un gruppo abeliano, posso applicare le proprietà delle potenze date dalle osservazioni 1.10 e 1.11 per ottenere la condizione seguente:

$$\big(o(y)o(x_h)\big)(y + x_h) = \big(o(y)o(x_h)\big)y + \big(o(y)o(x_h)\big)x_h = o(x_h)\big(o(y)y\big) + o(y)\big(o(x_h)x_h\big) = 0$$

Dall'osservazione 1.15 deriva quindi la condizione $o(y + x_h) \mid o(y)o(x_h)$. D'altra parte, ancora per le proprietà delle potenze prima menzionate, vale anche la relazione che segue:

$$\begin{aligned} 0 &= o(x_h)\big(o(y + x_h)(y + x_h)\big) = \big(o(x_h)o(y + x_h)\big)(y + x_h) \\ &= \big(o(x_h)o(y + x_h)\big)y + \big(o(x_h)o(y + x_h)\big)x_h \\ &= \big(o(x_h)o(y + x_h)\big)y + o(y + x_h)\big(o(x_h)x_h\big) = \big(o(x_h)o(y + x_h)\big)y \end{aligned}$$

Di nuovo per l'osservazione 1.15, ottengo che $o(y) \mid o(x_h)o(y + x_h)$. Poiché $\text{MCD}(o(y), o(x_h)) = 1$ per l'ipotesi che $q_1, \ldots, q_h$ siano numeri primi i quali, naturalmente, possono essere scelti a due a due distinti senza perdita di generalità, si può applicare il lemma di Euclide (si veda la nota 18) per ottenere che $o(y) \mid o(y + x_h)$. Ripetendo lo stesso argomento, ma scambiando i ruoli di $o(x_h)$ e $o(y)$, posso affermare che anche $o(x_h) \mid o(y + x_h)$ e di conseguenza, tenendo a mente la definizione di minimo comune multiplo e utilizzando il fatto che $\text{mcm}(o(y), o(x_h)) = o(y)o(x_h)$ per un fatto[23] noto di divisibilità in $\mathbb{Z}$, si ricava la condizione $o(y)o(x_h) \mid o(y + x_h)$. Ricordando infine che, per la definizione 1.10, l'ordine di un elemento è un valore strettamente positivo, si può concludere che $o(y + x_h) = o(y)o(x_h)$, cioè che $o(x_1 + \cdots + x_h) = \prod_{i=1}^{h} q_i^{k_i}$. A questo punto, utilizzando il fatto che $x = x_1 + \cdots + x_h$ e che $o(x)$ è unico per minimalità, si dovrà avere che $p^k = \prod_{i=1}^{h} q_i^{k_i}$. Se fosse $k \neq 0$, allora si avrebbe una contraddizione con l'assunzione che $q_i \neq p$ per ogni $1 \leq i \leq h$, oppure con l'ipotesi che p sia un numero primo. Di conseguenza, dovrà necessariamente valere che $k = 0$, quindi $o(x) = 1$ e posso dunque concludere che $x = 0$ per la definizione 1.10. Ho così dimostrato l'inclusione $A(p) \cap (\sum_{q\,\text{primo},\, q\neq p} A(q)) \subseteq \{0\}$. L'altro contenimento è un'immediata conseguenza dell'osservazione 5.12. Detto questo, si può utilizzare questo risultato per dimostrare che Φ è una funzione iniettiva. Data infatti una collezione $\{x_p\}_{p\,\text{primo}} \in \text{Ker}\,\Phi$, per definizione di nucleo si ha che $\Phi(\{x_p\}_{p\,\text{primo}}) = 0$, cioè che $\sum_{p\,\text{primo}} x_p = 0$. In particolare, per ogni primo p vale la relazione $x_p = \sum_{q\,\text{primo},\, q\neq p}(-x_q)$, ma allora $x_p \in A(p) \cap (\sum_{q\,\text{primo},\, q\neq p} A(q))$ e quindi $x_p = 0$ in virtù della discussione precedente. Questo dimostra che il nucleo dell'omomorfismo Φ è banale e dunque, per la proposizione 3.1-(ii), posso concludere che Φ è un monomorfismo.

Per poter concludere che Φ è anche una mappa suriettiva, quindi un isomorfismo, sarà sufficiente dimostrare che $A_{\text{tor}} \subseteq \sum_{p\,\text{primo}} A(p)$. Assegnato un elemento $x \in A_{\text{tor}}$, per la definizione 5.6-(iv) esiste un qualche $n \in \mathbb{N}$ tale che $nx = 0$. Poiché in $\mathbb{Z}$ ogni elemento ammette una fattorizzazione in primi, esistono numeri primi $p_1, \ldots, p_s$ ed elementi $k_1, \ldots, k_s \in \mathbb{N}^*$ tali che $n = p_1^{k_1} \cdots p_s^{k_s}$. Nel caso banale in cui $s = 1$, si ha che $p_1^{k_1} x = 0$ e dunque $x \in A(p_1)$ in virtù della definizione 5.6-(iii). In particolare, vale che $x \in \sum_{p\,\text{primo}} A(p)$. Si assuma quindi $s \geq 2$ e si ponga $n' := p_2^{k_2} \cdots p_s^{k_s}$ per semplicità, cosicché valga la condizione $n = p_1^{k_1} n'$. Potendo scegliere $p_1, \ldots, p_s$ a due a due distinti senza perdita di generalità ed essendo $p_1, \ldots, p_s$ numeri primi, si ha che $\text{MCD}(p_1^{k_1}, n') = 1$. Adesso

[23] Dati $a, b \in \mathbb{Z}$ con $\text{MCD}(a, b) = 1$, vale che $\text{mcm}(a, b) = |ab|$. Più in generale, vale la formula $\text{MCD}(a, b)\,\text{mcm}(a, b) = |ab|$ per ogni $a, b \in \mathbb{Z}$. Tali risultati sono dimostrati negli appunti del corso AL110.

applico[24] l'identità di Bezout, in virtù della quale esistono $a, b \in \mathbb{Z}$ tali che si abbia $1 = ap_1^{k_1} + bn'$ e definisco $x_1 := bn'x$, $x_2 := ap_1^{k_1}x$ in modo tale che, moltiplicando per x entrambi i membri della relazione precedente, si ottenga la condizione $x = x_1 + x_2$. Si noti dunque che $x_1 \in A(p_1)$ poiché:

$$p_1^{k_1}x_1 = p_1^{k_1}(bn'x) = b(p_1^{k_1}n')x = b(nx) = 0$$

D'altra parte, vale anche la condizione seguente:

$$n'x_2 = n'(ap_1^{x_1}x) = a(p_1^{k_1}n')x = a(nx) = 0$$

A questo punto distinguo due possibilità. Se n' è potenza di un numero primo, cioè se $n' = p_2^{k_2}$, allora $x_2 \in A(p_2)$, quindi $x \in A(p_1) + A(p_2)$ e in particolare $x \in \sum_{p\,\text{primo}} A(p)$. In caso contrario, essendo $s \geq 3$, si può iterare la costruzione precedente con n' al posto di n e dopo esattamente s iterazioni ottengo che $x = x_1 + \cdots + x_s$ con $x_i \in A(p_i)$ per ogni $1 \leq i \leq s$. Ne segue in particolare che $x \in A(p_1) + \cdots + A(p_s)$ e quindi $x \in \sum_{p\,\text{primo}} A(p)$. Non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $x \in A_{\text{tor}}$, l'inclusione $A_{\text{tor}} \subseteq \sum_{p\,\text{primo}} A(p)$ è dimostrata e mi permette di concludere che Φ è un isomorfismo di gruppi. □

Osservazione 5.14. Siano A un gruppo abeliano, $m \in \mathbb{N}^*$ e sia p un numero primo. Si vede facilmente che i sottogruppi dati nella definizione 5.6 sono compatibili con le somme dirette, cioè che valgono le proprietà:

(i) $m(A \oplus B) = mA \oplus mB$.

(ii) $(A \oplus B)[m] = A[m] \oplus B[m]$.

(iii) $(A \oplus B)(p) = A(p) \oplus B(p)$.

(iv) $(A \oplus B)_{\text{tor}} = A_{\text{tor}} \oplus B_{\text{tor}}$.

Osservazione 5.15. Sia A un gruppo abeliano finito. In questo caso particolare si deduce facilmente, come conseguenza immediata del teorema di Cauchy (corollario 2.2), che vale la condizione $A_{\text{tor}} = A$.

Osservazione 5.16. Siano A, B due gruppi abeliani tali che $A \simeq B$. Allora vale la condizione $A_{\text{tor}} \simeq B_{\text{tor}}$.

Dimostrazione. Per ipotesi, esiste un isomorfismo $\eta\colon A \to B$. Sarà sufficiente mostrare che $\eta(A_{\text{tor}}) = B_{\text{tor}}$ in modo tale che, restringendo η su A_{tor}, si abbia l'isomorfismo voluto. Sia dunque $a \in A_{\text{tor}}$ un elemento fissato. Per la definizione 5.6-(iv), esiste $k \in \mathbb{N}^*$ tale che $ka = 0$ ma allora, applicando η a primo e secondo membro, utilizzando il fatto che η è un omomorfismo con le osservazioni 3.1 e 3.4, si ottiene che $k\eta(a) = 0$ e questo mi permette di affermare che $\eta(a) \in B_{\text{tor}}$. Per arbitrarietà nella scelta dell'elemento $a \in A_{\text{tor}}$ vale quindi l'inclusione $\eta(A_{\text{tor}}) \subseteq B_{\text{tor}}$. Si consideri adesso un elemento $b \in B_{\text{tor}}$. In virtù dell'osservazione 1.6, anche l'applicazione inversa $\eta^{-1}\colon B \to A$ è un omomorfismo di gruppi e posso quindi ripetere l'argomento precedente con η^{-1} al posto di η, ottenendo l'inclusione $\eta^{-1}(B_{\text{tor}}) \subseteq A_{\text{tor}}$. Passando all'immagine tramite η e utilizzando il fatto che η^{-1} è l'applicazione inversa di η, si può infine concludere che $B_{\text{tor}} \subseteq \eta(A_{\text{tor}})$ e dalla doppia inclusione deriva immediatamente la tesi. □

Similmente si dimostra che, dati due gruppi abeliani A, B tali che $A \simeq B$, comunque assegnati $m \in \mathbb{N}^*$ e un numero primo p, valgono isomorfismi $mA \simeq mB$, $A[m] \simeq B[m]$ e infine $A(p) \simeq B(p)$.

Esempio 5.1. Si consideri il gruppo abeliano $\mathbb{Z}$ munito dell'usuale operazione di somma $+$ e con elemento neutro 0. Siccome $\mathbb{Z}$ non ammette elementi di ordine finito non banali, per la definizione 5.6-(iv) vale che $\mathbb{Z}_{\text{tor}} = \{0\}$ e di conseguenza, in virtù dell'osservazione 5.13, comunque fissati $m \in \mathbb{N}^*$ e un numero primo p, anche $\mathbb{Z}[m] = \{0\}$, $\mathbb{Z}(p) = \{0\}$. Infine, dalla definizione 5.6-(i) segue immediatamente che $m\mathbb{Z} = \langle m \rangle$.

Nei risultati seguenti le classi di resto modulo n verranno indicate alternativamente con una barretta oppure con parentesi quadre al fine di migliorare la leggibilità del testo.

Esempio 5.2. Si consideri il gruppo abeliano $\mathbb{Z}_n$ con operazione di somma usuale ed elemento neutro $\bar{0}$.

[24] Comunque assegnati $n, m \in \mathbb{Z}$, esistono $a, b \in \mathbb{Z}$ tali che $\text{MCD}(n, m) = an + bm$. Una dimostrazione di questo risultato, noto come l'identità di Bezout, è reperibile negli appunti del corso AL110.

(i) Si osservi innanzitutto che, comunque assegnato un elemento $m \in \mathbb{N}^*$, vale la seguente condizione:

$$m\mathbb{Z}_n = \{\, m\bar{a} \mid \bar{a} \in \mathbb{Z}_n \,\} = \{\, \bar{m}\bar{a} \mid \bar{a} \in \mathbb{Z}_n \,\} = \{\, a\bar{m} \mid a \in \mathbb{Z} \,\} = \langle \bar{m} \rangle$$

Dimostro che $\langle \bar{m} \rangle = \langle [\mathrm{MCD}(n,m)] \rangle$. Ricordando la definizione di massimo comune divisore, vale che $\mathrm{MCD}(n,m) \mid m$, cioè esiste $h \in \mathbb{Z}$ tale che $m = h\,\mathrm{MCD}(n,m)$. Passando ora alla congruenza modulo n, ottengo che $\bar{m} = h[\mathrm{MCD}(n,m)]$ e in particolare $\bar{m} \in \langle [\mathrm{MCD}(n,m)] \rangle$. Tenendo a mente che, per la definizione 1.8-(ii), il sottogruppo generato da un elemento è il più piccolo sottogruppo che lo contiene, si può dunque affermare che $\langle \bar{m} \rangle \subseteq \langle [\mathrm{MCD}(n,m)] \rangle$. Per poter dimostrare l'altra inclusione, è necessario utilizzare l'identità di Bezout, in virtù della quale esistono $a, b \in \mathbb{Z}$ tali che $\mathrm{MCD}(n,m) = an + bm$. In particolare, passando alla congruenza modulo n, ricavo la condizione $[\mathrm{MCD}(n,m)] = b\bar{m}$ e di conseguenza $[\mathrm{MCD}(n,m)] \in \langle \bar{m} \rangle$. Posso dunque concludere, per le stesse ragioni di prima, che $\langle [\mathrm{MCD}(n,m)] \rangle \subseteq \langle \bar{m} \rangle$ e per doppio contenimento si ottiene quanto volevasi dimostrare.

Ora mi occupo di dimostrare che $\langle [\mathrm{MCD}(n,m)] \rangle \simeq \mathbb{Z}_c$ con $c := \frac{n}{\mathrm{MCD}(n,m)}$. Va notato che $c \in \mathbb{Z}$ in quanto $\mathrm{MCD}(n,m) \mid n$. In virtù del corollario 1.2, basterà mostrare che $o([\mathrm{MCD}(n,m)]) = c$. Vale ovviamente che $c[\mathrm{MCD}(n,m)] = \bar{0}$. Fissato invece $k \in \mathbb{N}^*$ tale che $k[\mathrm{MCD}(n,m)] = \bar{0}$, per come si è definita la relazione di congruenza modulo n si ha che $n \mid k\,\mathrm{MCD}(n,m)$, cioè esiste $h \in \mathbb{Z}$ tale che $k\,\mathrm{MCD}(n,m) = nh$ ma allora, utilizzando il fatto che $\mathrm{MCD}(n,m) \neq 0$, posso dividere in $\mathbb{Q}$ ambo i membri della relazione precedente per $\mathrm{MCD}(n,m)$, ottenendo che $k = ch$ e in particolare $c \mid k$. Questo dimostra che $o([\mathrm{MCD}(n,m)]) = c$ per la definizione 1.10 e dunque $\langle \mathrm{MCD}(n,m) \rangle \simeq \mathbb{Z}_c$ per il corollario 1.2 già menzionato.

(ii) Dimostro che $\mathbb{Z}_n[m] = \mathbb{Z}_n[\mathrm{MCD}(n,m)]$. Dato un qualsiasi elemento $\bar{x} \in \mathbb{Z}_n[\mathrm{MCD}(n,m)]$, in virtù della definizione 5.6-(ii) si ha che $\mathrm{MCD}(n,m)\bar{x} = \bar{0}$. Per definizione di massimo comune divisore si ha che $\mathrm{MCD}(n,m) \mid m$, cioè esiste un elemento $k \in \mathbb{Z}$ tale che $m = k\,\mathrm{MCD}(n,m)$ ma allora, se moltiplico per k entrambi i membri della relazione $\mathrm{MCD}(n,m)\bar{x} = \bar{0}$, per definizione di elemento neutro ottengo che $m\bar{x} = \bar{0}$ e posso dunque affermare che $\bar{x} \in \mathbb{Z}_n[m]$. Poiché il risultato ottenuto non dipende da una particolare scelta di $\bar{x} \in \mathbb{Z}_n[\mathrm{MCD}(n,m)]$, vale che $\mathbb{Z}_n[\mathrm{MCD}(n,m)] \subseteq \mathbb{Z}_n[m]$. Si consideri ora un elemento $\bar{x} \in \mathbb{Z}_n[m]$, cioè tale che $m\bar{x} = \bar{0}$. Applicando l'identità di Bezout, si ottengono $a, b \in \mathbb{Z}$ tali che $\mathrm{MCD}(n,m) = an + bm$ ma allora, moltiplicando ambo i membri per x e passando alla congruenza modulo n, si ricava che $\mathrm{MCD}(n,m)\bar{x} = \bar{0}$, per cui posso affermare che $\bar{x} \in \mathbb{Z}_n[\mathrm{MCD}(n,m)]$ e dunque anche l'inclusione $\mathbb{Z}_n[m] \subseteq \mathbb{Z}_n[\mathrm{MCD}(n,m)]$ è dimostrata.

Dimostro che $\mathbb{Z}_n[\mathrm{MCD}(n,m)] = \langle [\frac{n}{\mathrm{MCD}(n,m)}] \rangle$. Come è già stato osservato nel punto (i), si ha che $\frac{n}{\mathrm{MCD}(n,m)} \in \mathbb{Z}$ perché $\mathrm{MCD}(n,m) \mid n$. Adesso si vede facilmente che $\mathrm{MCD}(n,m)[\frac{n}{\mathrm{MCD}(n,m)}] = \bar{0}$ e di conseguenza $[\frac{n}{\mathrm{MCD}(n,m)}] \in \mathbb{Z}_n[\mathrm{MCD}(n,m)]$ per la definizione 5.6-(ii). Tenendo invece a mente la definizione 1.8-(ii), si può affermare che $\langle [\frac{n}{\mathrm{MCD}(n,m)}] \rangle \subseteq \mathbb{Z}_n[\mathrm{MCD}(n,m)]$. Si consideri adesso un elemento $\bar{x} \in \mathbb{Z}_n[\mathrm{MCD}(n,m)]$, cioè tale che valga la condizione $\mathrm{MCD}(n,m)\bar{x} = \bar{0}$. Per definizione di relazione di congruenza modulo n, si ha che $n \mid \mathrm{MCD}(n,m)x$, cioè esiste un elemento $k \in \mathbb{Z}$ tale che $\mathrm{MCD}(n,m)x = kn$. Effettuando ora la divisione in $\mathbb{Q}$ per $\mathrm{MCD}(n,m)$, resa possibile dal fatto che $\mathrm{MCD}(n,m) \neq 0$, si ottiene che $x = k\frac{n}{\mathrm{MCD}(n,m)}$ e dunque, passando alla congruenza modulo n, vale che $\bar{x} = k[\frac{n}{\mathrm{MCD}(n,m)}]$. In particolare, si ha che $\bar{x} \in \langle [\frac{n}{\mathrm{MCD}(n,m)}] \rangle$ e dunque, non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $\bar{x} \in \mathbb{Z}_n[\mathrm{MCD}(n,m)]$, posso concludere che $\mathbb{Z}_n[\mathrm{MCD}(n,m)] \subseteq \langle [\frac{n}{\mathrm{MCD}(n,m)}] \rangle$. Per doppia inclusione, si ottiene quanto volevasi dimostrare.

Infine, mostro che $\langle [\frac{n}{\mathrm{MCD}(n,m)}] \rangle \simeq \mathbb{Z}_{\mathrm{MCD}(n,m)}$. Per farlo, sarà sufficiente applicare il corollario 1.2 dopo aver dimostrato che $o([\frac{n}{\mathrm{MCD}(n,m)}]) = \mathrm{MCD}(n,m)$. Si osservi dunque che vale banalmente la condizione $\mathrm{MCD}(n,m)[\frac{n}{\mathrm{MCD}(n,m)}] = 0$. Fissato invece $k \in \mathbb{N}^*$ tale che $k[\frac{n}{\mathrm{MCD}(n,m)}] = 0$, per come è stata definita la relazione di congruenza modulo n si ha che $n \mid k\frac{n}{\mathrm{MCD}(n,m)}$, cioè esiste $h \in \mathbb{Z}$ tale che $k\frac{n}{\mathrm{MCD}(n,m)} = hn$. Moltiplicando entrambi i membri della relazione ottenuta per $\mathrm{MCD}(n,m)$, ricordando che $n \neq 0$ e che in $\mathbb{Z}$ valgono le leggi di cancellazione (si veda la nota 21), si ottiene che $k = h\,\mathrm{MCD}(n,m)$. In particolare, vale che $\mathrm{MCD}(n,m) \mid k$ e posso quindi concludere, in vista della definizione 1.10, che $o([\frac{n}{\mathrm{MCD}(n,m)}]) = \mathrm{MCD}(n,m)$. Come si è già accennato prima, il corollario 1.2 implica che valga $\langle [\frac{n}{\mathrm{MCD}(n,m)}] \rangle \simeq \mathbb{Z}_{\mathrm{MCD}(n,m)}$ come volevasi dimostrare.

(iii) Si assuma che $n = p^r n'$ con p numero primo, $r, n' \in \mathbb{N}$ tali che $p \nmid n'$ e dimostro che $\mathbb{Z}_n(p) = \langle \bar{n}' \rangle$. Innanzitutto vale ovviamente, per ipotesi, che $p^r \bar{n}' = \bar{0}$ e quindi, ricordando la definizione 5.6-(iii),

si ha che $\bar{n}' \in \mathbb{Z}_n(p)$. Questo dimostra, in vista della definizione 1.8-(ii), che $\langle \bar{n}' \rangle \subseteq \mathbb{Z}_n(p)$. Sia ora $\bar{x} \in \mathbb{Z}_n(p)$ un elemento fissato. Ancora per la definizione 5.6-(iii) si ha che $p^k \bar{x} = \bar{0}$ per un qualche $k \in \mathbb{N}$. Dimostro che $\mathrm{MCD}(p^k, n') = 1$. Le condizioni $1 \mid p^k$ e $1 \mid n'$ sono banalmente vere, per cui considero un elemento $d \in \mathbb{N}^*$ tale che $d \mid p^k$ e $d \mid n'$. In particolare, esiste $a \in \mathbb{Z}$ tale che $p^k = da$. Poiché si assume che p sia un numero primo, dovrà valere che $d = 1$ oppure $a = 1$. Se fosse $a = 1$, allora $p^k = d$ e di conseguenza $p^k \mid n'$, contraddicendo le ipotesi. Questo dimostra che $d = 1$, ma il risultato ottenuto non dipende dalla scelta dell'elemento $d \in \mathbb{N}^*$ tale che $d \mid p^k$ e $d \mid n'$ e dunque $\mathrm{MCD}(p^k, n') = 1$ per definizione. A questo punto applico l'identità di Bezout, in virtù della quale esistono $a, b \in \mathbb{Z}$ tali che $1 = ap^k + bn'$. Moltiplicando adesso per x primo e secondo membro della relazione precedente, passando alla congruenza modulo n e usando il fatto che $p^k \bar{x} = 0$, si ottiene che $\bar{x} = bx\bar{n}'$. In particolare, si ha che $\bar{x} \in \langle \bar{n}' \rangle$ e quindi vale l'inclusione $\mathbb{Z}_n(p) \subseteq \langle \bar{n}' \rangle$. La doppia inclusione implica quanto volevasi dimostrare.

Dimostro infine che $\langle \bar{n}' \rangle \simeq \mathbb{Z}_{p^r}$ e per farlo, come al solito, dimostro che $o(\bar{n}') = p^r$ per poi ricorrere al corollario 1.2. Innanzitutto, dalle ipotesi segue banalmente che $p^r \bar{n}' = \bar{0}$. Considero quindi un elemento $k \in \mathbb{N}^*$ tale che $k\bar{n}' = \bar{0}$. Per come è definita la relazione di congruenza modulo n, vale che $n \mid kn'$ e questo significa che esiste $h \in \mathbb{Z}$ tale che $kn' = hn$. Ricordando le ipotesi, è del tutto equivalente richiedere che valga la relazione $kn' = hp^r n'$ ma allora, utilizzando il fatto che $n' \neq 0$ e tenendo a mente che in $\mathbb{Z}$ valgono le leggi di cancellazione, si ottiene che $k = hp^r$ e in particolare $p^r \mid k$. Per la definizione 1.10 si può concludere che $o(n') = p^r$ e dunque l'isomorfismo $\langle \bar{n}' \rangle \simeq \mathbb{Z}_{p^r}$ deriva dal corollario 1.2 già menzionato.

Lemma 5.1. *Siano $n \in \mathbb{N}$, $m \in \mathbb{N}^*$ e sia p un numero primo. Vale la condizione seguente:*

$$(p^n \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p]) / (p^{n+1} \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p]) \simeq \begin{cases} \mathbb{Z}_p & \text{se } n = m-1 \\ \{0\} & \text{se } n \neq m-1 \end{cases}$$

Dimostrazione. Si osservi innanzitutto che, in vista dei punti (i) e (ii) dell'esempio 5.2 e in virtù del fatto che $\mathrm{MCD}(p^k, p^h) = p^{\min\{k,h\}}$, $\mathrm{mcm}(p^k, p^h) = p^{\max\{k,h\}}$ per ogni $k, h \in \mathbb{N}$, utilizzando inoltre il fatto noto che $\langle [a] \rangle \cap \langle [b] \rangle = \langle [\mathrm{mcm}(a,b)] \rangle$ comunque fissate due classi $[a], [b] \in \mathbb{Z}_n$, si ricava la condizione seguente:

$$\begin{aligned} p^n \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p] &= \langle [\mathrm{MCD}(p^m, p^n)] \rangle \cap \left\langle \left[\frac{p^m}{\mathrm{MCD}(p^m, p)} \right] \right\rangle \\ &= \langle [p^{\min\{m,n\}}] \rangle \cap \left\langle \left[\frac{p^m}{p} \right] \right\rangle = \langle [p^{\min\{m,n\}}] \rangle \cap \langle [p^{m-1}] \rangle \\ &= \langle [\mathrm{mcm}(p^{\min\{m,n\}}, p^{m-1})] \rangle = \langle [p^{\max\{\min\{m,n\}, m-1\}}] \rangle \end{aligned}$$

Posso quindi distinguere due casi e riapplicare lo stesso argomento con $n+1$ al posto di n, ottenendo che:

$$p^n \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p] = \begin{cases} \langle [p^{m-1}] \rangle & \text{se } n \leq m-1 \\ \langle [p^m] \rangle & \text{se } n \geq m \end{cases}, \quad p^{n+1} \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p] = \begin{cases} \langle [p^{m-1}] \rangle & \text{se } n \leq m-2 \\ \langle [p^m] \rangle & \text{se } n \geq m-1 \end{cases}$$

A questo punto, usando il fatto che ogni sottogruppo di un gruppo abeliano è normale (osservazione 2.6), posso passare al quoziente e ottenere quindi la relazione che segue:

$$(p^n \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p]) / (p^{n+1} \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p]) = \begin{cases} \langle [p^{m-1}] \rangle / \langle [p^{m-1}] \rangle & \text{se } n \leq m-2 \\ \langle [p^{m-1}] \rangle / \langle [p^m] \rangle & \text{se } n = m-1 \\ \langle [p^m] \rangle / \langle [p^m] \rangle & \text{se } n \geq m \end{cases}$$

Si osservi infine che $\langle [p^{m-1}] \rangle$ è un gruppo ciclico generato da un elemento di ordine p e dunque, in virtù del corollario 1.2, si ha che $\langle [p^{m-1}] \rangle \simeq \mathbb{Z}_p$. Tenendo a mente che le classi di equivalenza considerate sono classi di resto modulo p^m, si ha la condizione $\langle [p^{m-1}] \rangle / \langle [p^m] \rangle \simeq \mathbb{Z}_p / \{\bar{0}\} \simeq \mathbb{Z}_p$. D'altra parte, vale banalmente che $\langle [p^{m-1}] \rangle / \langle [p^{m-1}] \rangle \simeq \{0\}$, $\langle [p^m] \rangle / \langle [p^m] \rangle \simeq \{0\}$ e dunque l'asserto è dimostrato. □

Teorema 5.3 (Classificazione dei gruppi abeliani finitamente generati)**.** *Si consideri un gruppo abeliano A finitamente generato. Valgono le seguenti affermazioni.*

(i) *Il gruppo A si esprime come somma diretta finita di gruppi ciclici, cioè esistono $r, n_1, \dots, n_s \in \mathbb{N}$, con $n_1, \dots, n_s \geq 2$, tali che $A \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$.*

(ii) *L'intero non negativo r è unico.*

(iii) *Gli interi $n_1, \dots, n_s \geq 2$ si possono scegliere in modo tale che valga una delle seguenti condizioni:*

  (a) *$n_1 \mid n_2 \mid \cdots \mid n_s$ e in questo caso $n_1, \dots, n_s$ sono unici.*

  (b) *$n_1, \dots, n_s$ sono potenze di primi, cioè esistono $p_1, \dots, p_s$ numeri primi, $\alpha_1, \dots, \alpha_s \in \mathbb{N}^*$ tali che $n_i = p_i^{\alpha_i}$ per ogni $1 \leq i \leq s$ e in questo caso $n_1, \dots, n_s$ sono unici a meno di permutazioni degli indici.*

Dimostrazione. Innanzitutto, dato che per ipotesi A è un gruppo finitamente generato, esiste un insieme di generatori finito $X \subseteq A$. Posto per semplicità $n := |X|$, usando l'ipotesi che A sia un gruppo abeliano posso applicare il corollario 5.1, dal quale deduco l'esistenza di un epimorfismo $\Phi \colon \mathbb{Z}^n \to A$. Applicando quindi l'osservazione 3.7, si ottiene in particolare che $A \simeq \mathbb{Z}^n / \operatorname{Ker} \Phi$. Inoltre, dato che $\operatorname{Ker} \Phi < \mathbb{Z}^n$ è un sottogruppo, si può usare il teorema 5.2 per ottenere una base $\{x_1, \dots, x_n\}$ per $\mathbb{Z}^n$, un intero $1 \leq t \leq n$, $d_1, \dots, d_t \in \mathbb{N}^*$ con $d_1 \mid d_2 \mid \cdots \mid d_t$ tali che $\operatorname{Ker} \Phi$ sia un gruppo abeliano libero con base $\{d_1 x_1, \dots, d_t x_t\}$. In particolare, si ha che $\mathbb{Z}^n = \langle x_1, \dots, x_n \rangle$, $\operatorname{Ker} \Phi = \langle d_1 x_1, \dots, d_t x_t \rangle$. Si vede facilmente, per induzione sul numero degli elementi, che $\langle x_1, \dots, x_n \rangle \simeq \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$. Infatti, la base induttiva è ovvia, mentre il passo di induzione si dimostra esattamente come si è giustificato che $F \simeq \langle x_1 \rangle \oplus H$ nella dimostrazione del teorema 5.2. Vale dunque che $\mathbb{Z}^n \simeq \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$ e analogamente $\operatorname{Ker} \Phi \simeq \langle d_1 x_1 \rangle \oplus \cdots \oplus \langle d_t x_t \rangle$. Si osservi adesso che $\langle d_1 x_1 \rangle \oplus \cdots \oplus \langle d_t x_t \rangle \simeq \langle d_1 x_1 \rangle \oplus \cdots \oplus \langle d_t x_t \rangle \oplus \{0\} \oplus \cdots \oplus \{0\}$ per cui, applicando l'osservazione 4.20, si ottiene la condizione seguente:

$$\begin{aligned}
\mathbb{Z}^n / \operatorname{Ker} \Phi &\simeq (\langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle) / (\langle d_1 x_1 \rangle \oplus \cdots \oplus \langle d_t x_t \rangle) \\
&\simeq (\langle x_1 \rangle \oplus \cdots \oplus \langle x_t \rangle \oplus \langle x_{t+1} \rangle \oplus \cdots \oplus \langle x_n \rangle) / (\langle d_1 x_1 \rangle \oplus \cdots \oplus \langle d_t x_t \rangle \oplus \{0\} \oplus \cdots \oplus \{0\}) \\
&\simeq (\langle x_1 \rangle / \langle d_1 x_1 \rangle) \oplus \cdots \oplus (\langle x_t \rangle / \langle d_t x_t \rangle) \oplus (\langle x_{t+1} \rangle / \{0\}) \oplus \cdots \oplus (\langle x_n \rangle / \{0\}) \\
&\simeq (\langle x_1 \rangle / \langle d_1 x_1 \rangle) \oplus \cdots \oplus (\langle x_t \rangle / \langle d_t x_t \rangle) \oplus \langle x_{t+1} \rangle \oplus \cdots \oplus \langle x_n \rangle
\end{aligned}$$

Si osservi che, per ogni $1 \leq i \leq n$, l'applicazione $f_i \colon \langle x_i \rangle \to \mathbb{Z}$ definita da $f_i(k x_i) := k$ è un isomorfismo di gruppi per costruzione e che f_i induce per restrizione un isomorfismo $\langle d_i x_i \rangle \simeq \langle d_i \rangle$ per ogni $1 \leq i \leq t$. Di conseguenza, ricordando la relazione precedente e utilizzando l'esempio 2.6, si ottiene quindi la condizione:

$$\begin{aligned}
\mathbb{Z}^n / \operatorname{Ker} \Phi &\simeq (\mathbb{Z} / \langle d_1 \rangle) \oplus \cdots \oplus (\mathbb{Z} / \langle d_t \rangle) \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \\
&\simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t} \oplus \mathbb{Z}^{n-t}
\end{aligned}$$

Questo dimostra l'affermazione (i) e la parte concernente l'esistenza nel punto (a) della condizione (iii). La parte riguardante l'esistenza nel punto (b) dell'affermazione (iii) è fornita invece dalla proposizione 4.11 e dall'esistenza della decomposizione in fattori primi in $\mathbb{Z}$. Infatti, comunque assegnato un indice $1 \leq i \leq n$ esistono $p_{i1}, \dots, p_{ik}$ numeri primi, $\alpha_{i1}, \dots, \alpha_{ik} \in \mathbb{N}^*$ tali che $\mathbb{Z}_{d_i} \simeq \mathbb{Z}_{p_{i1}^{\alpha_{i1}}} \oplus \cdots \oplus \mathbb{Z}_{p_{ik}^{\alpha_{ik}}}$ e di conseguenza si ha proprio quanto volevasi dimostrare.

Ora, data una qualsiasi decomposizione $A \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$, mi occupo di mostrare che l'intero non negativo r è unico. Combinando le osservazioni 5.14-(iv), 5.15, 5.16 con l'esempio 5.1, si può affermare che $A_{\text{tor}} \simeq \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$ e dunque $A / A_{\text{tor}} \simeq \mathbb{Z}^r$ in virtù dell'osservazione 4.20. Questo dimostra, per la definizione 5.5, che A / A_{tor} è un gruppo abeliano libero di rango r. In particolare, l'intero non negativo r dipende soltanto da A nel senso che, ripetendo lo stesso argomento con una decomposizione in cui r viene sostituito da un intero non negativo s, si ottiene che $s = r$ per unicità del rango. In altre parole, l'intero non negativo r è unico e quindi il punto (ii) è dimostrato.

Si consideri ora una decomposizione $A \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$ con $n_1, \dots, n_s \geq 2$ scelti in modo tale che sia soddisfatto il punto (a) della condizione (iii), cioè tali che $n_1 \mid n_2 \mid \cdots \mid n_s$. Per dimostrare l'unicità di tali $n_1, \dots, n_s$ sarà sufficiente darne una caratterizzazione che li determini in maniera univoca. Osservo innanzitutto che $A_{\text{tor}} \simeq \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$ per le stesse ragioni di prima. Detto questo, dimostro che n_s è il più piccolo intero positivo tale che $n_s A_{\text{tor}} = \{0\}$. Poiché si assume che $n_1 \mid n_2 \mid \cdots \mid n_s$, vale banalmente che $n_s A_{\text{tor}} = \{0\}$. Si consideri ora un intero positivo k tale che $k A_{\text{tor}} = \{0\}$. In particolare, si dovrà avere la condizione $k \mathbb{Z}_{n_s} = \{\bar{0}\}$ la quale, in vista dell'esempio 5.2-(i), equivale a richiedere che valga $\langle \bar{k} \rangle = \{\bar{0}\}$. Da questo si deduce che $n_s \mid k$ e dunque la minimalità di n_s è dimostrata. Adesso, comunque assegnato un

indice $1 \leq i \leq s$, si vuole mostrare che n_{s-i} è il più piccolo intero positivo tale che $n_{s-i}A_{\text{tor}}$ sia isomorfo alla somma diretta di i gruppi ciclici finiti. Osservo innanzitutto che, per l'osservazione 5.14-(i) e in virtù del fatto che $n_1 \mid n_2 \mid \cdots \mid n_{s-i}$, si ha che $n_{s-i}A_{\text{tor}} \simeq n_{s-i}\mathbb{Z}_{n_{s-i+1}} \oplus \cdots \oplus n_{s-i}\mathbb{Z}_{n_s}$ e dunque $n_{s-i}A_{\text{tor}}$ è isomorfo alla somma diretta di i gruppi ciclici finiti. Si consideri adesso un intero positivo k tale che kA_{tor} sia isomorfo alla somma diretta di i gruppi ciclici finiti. Di nuovo in virtù dell'osservazione 5.14-(i) e per le assunzioni fatte sugli interi positivi $n_1, \ldots, n_s \geq 2$, si dovrà avere che $kA_{\text{tor}} \simeq k\mathbb{Z}_{n_{s-i+1}} \oplus \cdots \oplus k\mathbb{Z}_{n_s}$, cioè che $k\mathbb{Z}_{n_j} = \{\bar{0}\}$ comunque sia fissato un indice $1 \leq j \leq s-i$. In virtù dell'esempio 5.2-(i), è equivalente richiedere che valga $\langle \bar{k} \rangle = \{\bar{0}\}$ e di conseguenza $n_j \mid k$. In particolare, si dovrà avere che $n_{s-i} \mid k$ e questo dimostra la minimalità di n_{s-i}. Avendo caratterizzato $n_1, \ldots, n_s$ come i più piccoli interi non negativi che soddisfano determinate proprietà, la loro unicità è dimostrata e deriva dall'unicità del minimo.

Considero infine una decomposizione $A \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$ con $n_1, \ldots, n_s \geq 2$ scelti come potenze di primi, cioè tali che sia verificato il punto (b) dell'affermazione (iii). Più esplicitamente, esistono numeri primi $p_1, \ldots, p_s$ ed elementi $\alpha_{11}, \ldots, \alpha_{1k_1}, \ldots, \alpha_{s1}, \ldots, \alpha_{sk_s} \in \mathbb{N}$ con $k_1, \ldots, k_s \in \mathbb{N}^*$ per cui si abbia che:

$$A \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{{p_1}^{\alpha_{11}}} \oplus \cdots \oplus \mathbb{Z}_{{p_1}^{\alpha_{1k_1}}} \oplus \cdots \oplus \mathbb{Z}_{{p_s}^{\alpha_{s1}}} \oplus \cdots \oplus \mathbb{Z}_{{p_s}^{\alpha_{sk_s}}}$$

Adesso si osservi che, fissati due indici $1 \leq i \leq s$, $1 \leq h_i \leq k_i$ e un primo p, vale che $\mathbb{Z}_{{p_i}^{\alpha_{ih_i}}}(p) = \mathbb{Z}_{{p_i}^{\alpha_{ih_i}}}$ se $p = p_i$, $\mathbb{Z}_{{p_i}^{\alpha_{ih_i}}}(p) = \{\bar{0}\}$ altrimenti. Se infatti $p = p_i$, allora si può applicare facilmente l'esempio 5.2-(iii). Se invece $p \neq p_i$ allora, fissato $\bar{x} \in \mathbb{Z}_{{p_i}^{\alpha_{ih_i}}}(p)$, per il teorema di Cauchy (corollario 2.2) vale che $o(\bar{x}) \mid p_i^{\alpha_{ih_i}}$, mentre per la definizione 5.6-(iii) assieme all'osservazione 1.15 si ha che $o(\bar{x}) \mid p^k$ per un qualche $k \in \mathbb{N}$. Equivalentemente, esistono $h, l \in \mathbb{Z}$ tali che $p_i^{\alpha_{ih_i}} = o(\bar{x})h$, $p^k = o(\bar{x})l$ e di conseguenza, se fosse $o(\bar{x}) \neq 1$, l'elemento $o(\bar{x})$ dovrebbe essere una potenza non banale di p_i oppure di p, contraddicendo il fatto che in $\mathbb{Z}$ la fattorizzazione in primi è unica. Si deduce che $o(\bar{x}) = 1$ cioè, per la definizione 1.10, che $\bar{x} = \bar{0}$. Fatta questa considerazione, applicando l'osservazione 5.14-(iii) e tenendo a mente l'esempio 5.1 si ottiene, per ogni numero primo p, la relazione seguente:

$$A(p) \simeq \begin{cases} \mathbb{Z}_{{p_i}^{\alpha_{i1}}} \oplus \cdots \oplus \mathbb{Z}_{{p_i}^{\alpha_{ik_i}}} & \text{se } p = p_i \text{ per un qualche } 1 \leq i \leq s \\ \{0\} & \text{se } p \neq p_i \text{ per ogni } 1 \leq i \leq s \end{cases}$$

Si osservi che $A(p)$ è banale per ogni primo p tranne che per un numero finito di primi e di conseguenza è ben definita la somma diretta $\bigoplus_{p \text{ primo}} A(p)$. Dalla discussione precedente deriva la seguente condizione:

$$A \simeq \mathbb{Z}^r \oplus \bigoplus_{p \text{ primo}} A(p)$$

Basterà dunque mostrare che ciascun fattore $A(p)$ con p numero primo si esprime in maniera unica come somma di gruppi ciclici di ordine una potenza di p, cioè che $A(p) \simeq \bigoplus_{m \in \mathbb{N}^*} (\mathbb{Z}_{p^m})^{\gamma_m}$ con $\gamma_m \in \mathbb{N}$ unico. Ricordando dunque l'osservazione 5.14 e che il prodotto cartesiano di insiemi rispetta le intersezioni, si ha per ogni $n \in \mathbb{N}$ la condizione seguente:

$$\big(p^n A(p) \cap A(p)[p]\big) \big/ \big(p^{n+1} A(p) \cap A(p)[p]\big) = \bigoplus_{m \in \mathbb{N}^*} \big((p^n \mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p]) / (p^{n+1}\mathbb{Z}_{p^m} \cap \mathbb{Z}_{p^m}[p])\big)^{\gamma_m}$$

Applicando ora il lemma 5.1, posso affermare che gli unici fattori non banali nella somma diretta si hanno per $m = n+1$ e di conseguenza si ha la relazione che segue:

$$\big(p^n A(p) \cap A(p)[p]\big) \big/ \big(p^{n+1} A(p) \cap A(p)[p]\big) \simeq (\mathbb{Z}_p)^{\gamma_{n+1}}$$

Questo dimostra che, per $m \in \mathbb{N}^*$ fissato, l'elemento γ_m dipende soltanto da A e da p, dunque è unico. Se infatti si dovesse ripetere l'argomento precedente con un qualunque $\gamma'_m \in \mathbb{N}$ al posto di γ_m, si otterrebbe la condizione $(\mathbb{Z}_p)^{\gamma_m} \simeq (\mathbb{Z}_p)^{\gamma'_m}$. Passando alle cardinalità, si ricava che $p^{\gamma_m} = p^{\gamma'_m}$ e quindi, per unicità della fattorizzazione in primi in $\mathbb{Z}$, si può affermare che $\gamma_m = \gamma'_m$. Questo conclude la dimostrazione. □

Definizione 5.7. Sia A un gruppo abeliano finitamente generato e si consideri una sua decomposizione in gruppi ciclici $A \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$. L'intero non negativo r viene detto il *rango di* A e si denota $\text{rk}(A)$, mentre gli interi $n_1, \ldots, n_s$ prendono il nome di *fattori invarianti di* A se soddisfano il punto (a) del teorema 5.3-(iii), si dicono invece i *divisori elementari di* A se verificano il punto (b) del teorema 5.3-(iii).

Ovviamente, la definizione 5.7 è ben posta per il teorema 5.3. Inoltre, dal teorema appena menzionato e dalla terminologia introdotta con la definizione 5.7 deriva immediatamente il seguente risultato.

Corollario 5.4. *Siano A e B due gruppi abeliani finitamente generati. Allora vale che $A \simeq B$ se e solo se $\mathrm{rk}(A) = \mathrm{rk}(B)$ e hanno gli stessi fattori invarianti, oppure gli stessi divisori elementari.*

Parte II
Teoria degli anelli

6 Anelli e omomorfismi

Definizione 6.1. Un insieme non vuoto R munito di due operazioni binarie $+$ e $\cdot$ è detto un *anello* se:

(i) Esiste un elemento $0 \in R$ tale che $(R, +, 0)$ sia un gruppo abeliano.

(ii) Vale che $(R, \cdot)$ è un semigruppo. Equivalentemente, l'operazione binaria $\cdot$ su R è associativa, cioè $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ per ogni $a, b, c \in R$.

(iii) Valgono le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$, cioè $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ per ogni $a, b, c \in R$.

In caso affermativo, l'anello R si denota $(R, +, \cdot, 0)$ o più semplicemente R qualora non vi siano ambiguità. Inoltre, si dice che R è un anello *commutativo* se $(R, \cdot)$ è un semigruppo commutativo, cioè se $a \cdot b = b \cdot a$ per ogni $a, b \in R$. Se infine esiste un elemento $1 \in R$ tale che $(R, \cdot, 1)$ sia un monoide, cioè tale che valga $a \cdot 1 = 1 \cdot a = a$ per ogni $a \in R$, si dice che R è un anello *con identità* e R si denota anche $(R, +, \cdot, 0, 1)$.

Dato un anello R, si pone per semplicità $a - b := a + (-b)$ per ogni $a, b \in R$.

Proposizione 6.1. *Sia R un anello. Allora valgono le seguenti proprietà.*

(i) $a \cdot 0 = 0 \cdot a = 0$ *per ogni* $a \in R$.

(ii) $(\sum_{i=1}^{n} a_i) \cdot (\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} (a_i \cdot b_j)$ *per ogni* $a_1, \dots, a_n, b_1, \dots, b_m \in R$.

(iii) $(na) \cdot b = n(a \cdot b) = a \cdot nb$ *per ogni* $a, b \in R$, $n \in \mathbb{Z}$.

(iv) *Se R è un anello con identità, allora si ha per ogni $a, b \in R$ con $a \cdot b = b \cdot a$, $n \in \mathbb{N}$ la condizione:*

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}$$

Dimostrazione.

(i) Sia $a \in R$ un elemento fissato. Usando il fatto che 0 è un elemento neutro rispetto all'operazione di somma $+$, cioè la definizione 6.1-(i), assieme alla proprietà distributiva sinistra di $\cdot$ rispetto a $+$, vale a dire la definizione 6.1-(iii), si ottiene la condizione seguente:

$$a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0)$$

Sottraendo a entrambi i membri della relazione ottenuta la quantità $a \cdot 0$, si ricava che $a \cdot 0 = 0$. Procedendo esattamente allo stesso modo, ma utilizzando la proprietà distributiva destra anziché quella sinistra, si ottiene che $0 \cdot a = 0$.

(ii) In un primo momento, assumo $n := 1$ e procedo per induzione su $m \in \mathbb{N}$. La base di induzione, che corrisponde al caso $m = 1$, è banale. Nel passo di induzione assumo dunque $m \geq 2$, suppongo che $a_1 \cdot \sum_{j=1}^{m-1} b_j = \sum_{j=1}^{m-1} (a_1 \cdot b_j)$ e noto che, per la proprietà distributiva sinistra di $\cdot$ rispetto a $+$, cioè per la definizione 6.1-(iii), vale la relazione seguente:

$$\begin{aligned} a_1 \cdot \sum_{j=1}^{m} b_j &= a_1 \cdot \left(\sum_{j=1}^{m-1} b_j + b_m \right) \\ &= \left(a_1 \cdot \sum_{j=1}^{m-1} b_i \right) + (a_1 \cdot b_m) \\ &= \sum_{j=1}^{m-1} (a_1 \cdot b_j) + (a_1 \cdot b_m) = \sum_{j=1}^{m} (a_1 \cdot b_j) \end{aligned}$$

Questo dimostra che l'asserto è vero per $n := 1$, $m \in \mathbb{N}$. Si procede ora per induzione su $n \in \mathbb{N}$. La base di induzione è il caso $n = 1$ dato dalla discussione precedente. Nel passo induttivo assumo $n \geq 2$ e suppongo che la formula da dimostrare valga per un generico $n - 1$, per ogni $m \in \mathbb{N}$ e ne dimostro la validità per n. Per la proprietà distributiva destra di $\cdot$ rispetto a $+$, vale a dire per la definizione 6.1-(iii), si ha la condizione seguente, in virtù della quale si ha la tesi:

$$\begin{aligned}\left(\sum_{i=1}^{n} a_i\right) \cdot \left(\sum_{j=1}^{m} b_j\right) &= \left(\sum_{i=1}^{n-1} a_i + a_n\right) \cdot \left(\sum_{j=1}^{m} b_j\right) \\ &= \left(\left(\sum_{i=1}^{n-1} a_i\right) \cdot \left(\sum_{j=1}^{m} b_j\right)\right) + \left(a_n \cdot \sum_{j=1}^{m} b_j\right) \\ &= \sum_{i=1}^{n-1}\sum_{j=1}^{m}(a_i \cdot b_j) + \sum_{j=1}^{m}(a_n \cdot b_j) = \sum_{i=1}^{n}\sum_{j=1}^{m}(a_i \cdot b_j)\end{aligned}$$

(iii) Siano $a, b \in R$, $n \in \mathbb{Z}$ e si assuma per adesso $n > 0$. Per definizione di potenza (definizione 1.7) e per il punto (ii) appena dimostrato, si ha la condizione seguente:

$$(na) \cdot b = \left(\sum_{i=1}^{n} a\right) \cdot b = \sum_{i=1}^{n}(a \cdot b) = n(a \cdot b)$$

Si dimostra con un procedimento analogo che $a \cdot (nb) = n(a \cdot b)$. Il caso $n = 0$ deriva banalmente dalla definizione di potenza con esponente 0 e dal punto (i) appena dimostrato, infatti si ha che:

$$(0a) \cdot b = 0 \cdot b = 0 = 0(a \cdot b)$$

Chiaramente, con un ragionamento identico si ottiene che $a \cdot (0b) = 0(a \cdot b)$. Mi pongo ora nel caso $n = -1$. Si vuole mostrare che $(-a) \cdot b = -(a \cdot b)$. Si noti che, per la proprietà distributiva destra di $\cdot$ rispetto a $+$, cioè per la definizione 6.1-(iii) e per il punto (i) già dimostrato, vale la relazione:

$$(a \cdot b) + \big((-a) \cdot b\big) = (a - a) \cdot b = 0 \cdot b = 0$$

Per unicità dell'inverso in un gruppo (proposizione 1.1-(i)) posso affermare che $(-a) \cdot b = -(a \cdot b)$. Si procede in modo simile, utilizzando la proprietà distributiva sinistra anziché quella destra, per dimostrare che $a \cdot (-b) = -(a \cdot b)$. Assumo ora $n \leq -2$. Per definizione di potenza con esponente negativo, per il punto (ii) già dimostrato e per il caso $n = -1$ appena discusso, si ha la relazione:

$$(na) \cdot b = \left(\sum_{i=1}^{-n} -a\right) \cdot b = \sum_{i=1}^{-n}\big((-a) \cdot b\big) = (-n)\big((-a) \cdot b\big) = (-n)\big(-(a \cdot b)\big) = n(a \cdot b)$$

Avendo esaurito tutti i possibili casi per $n \in \mathbb{Z}$, si ottiene la tesi.

(iv) Si osservi innanzitutto che, per il punto (iii) appena dimostrato, non vi è ambiguità nello scrivere $\binom{n}{k}a^k \cdot b^{n-k}$ senza parentesi. Detto questo, si procede per induzione su $n \in \mathbb{N}$. La base induttiva, che corrisponde al caso $n = 0$, segue immediatamente dalla definizione di potenza con esponente 0. Nel passo di induzione assumo $n \geq 1$, suppongo che la tesi valga per $n - 1$ e dimostro che vale anche per n. Per una proprietà delle potenze (osservazione 1.10), per il punto (ii) già dimostrato, per l'ipotesi cruciale che $a \cdot b = b \cdot a$ e per le proprietà del coefficiente binomiale, si ha la relazione:

$$\begin{aligned}(a + b)^n &= (a + b) \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} a^k \cdot b^{n-k-1} \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} a^{k+1} \cdot b^{n-k-1} + \sum_{k=0}^{n-1} \binom{n-1}{k} b \cdot a^k \cdot b^{n-k-1} \\ &= \sum_{h=1}^{n} \binom{n-1}{h-1} a^h \cdot b^{n-h} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k \cdot b^{n-k} \\ &= a^n + b^n + \sum_{k=1}^{n-1} \binom{n}{k} a^k \cdot b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\end{aligned}$$

Avendo ottenuto la formula desiderata, la dimostrazione si conclude. □

Le asserzioni (ii) e (iv) della proposizione 6.1 sono note, rispettivamente, come la proprietà distributiva generalizzata e il teorema binomiale.

6.1 Alcune classi notevoli di anelli

Definizione 6.2. Sia R un anello. Un elemento $a \in R$ viene detto un *divisore dello zero sinistro* se esiste $b \in R$, $b \neq 0$ tale che $a \cdot b = 0$, viene invece detto un *divisore dello zero destro* se esiste $c \in R$, $c \neq 0$ tale che $c \cdot a = 0$. Infine, un divisore dello zero sinistro e destro si dice semplicemente un *divisore dello zero*.

Osservazione 6.1. Sia R un anello non banale. Dalla definizione 6.2 segue che 0 è un divisore dello zero.

Definizione 6.3. Sia R un anello con identità. Un elemento $a \in R$ si dice *invertibile a sinistra* se esiste $b \in R$ tale che $b \cdot a = 1$ e in tal caso b prende il nome di *inverso sinistro di* a, è invece detto *invertibile a destra* se esiste $c \in R$ tale che $a \cdot c = 1$ e in caso affermativo c prende il nome di *inverso destro di* a. Infine, un elemento invertibile a sinistra e a destra viene semplicemente detto un elemento *invertibile*.

Osservazione 6.2. Sia R un anello con identità e sia $a \in R$. Valgono le seguenti affermazioni.

(i) Se a è invertibile a sinistra, allora a non è un divisore dello zero sinistro. Allo stesso modo, se a è invertibile a destra, allora a non è un divisore dello zero destro.

(ii) Se b è un inverso sinistro di a e c è un inverso destro di a, allora $b = c$.

Dimostrazione.

(i) Dimostro soltanto la prima asserzione, in quanto la seconda si dimostra con un procedimento del tutto analogo. Poiché per ipotesi a è invertibile a sinistra, per definizione esiste un elemento $c \in R$ tale che $c \cdot a = 1$. Sia $b \in R$ un elemento tale che $a \cdot b = 0$. Allora si ha, per definizione di elemento neutro, per l'associatività dell'operazione binaria $\cdot$ su R garantita dalla definizione 6.1-(ii) e per la proposizione 6.1-(i), la condizione seguente:

$$b = 1 \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$$

Poiché il risultato ottenuto non dipende dalla scelta dell'elemento $b \in R$ tale che $a \cdot b = 0$ si può affermare, per contrapposizione logica, che ogni elemento $b \in R$, $b \neq 0$ è tale che $a \cdot b \neq 0$ e questo equivale a dire, per definizione, che a non è un divisore dello zero sinistro.

(ii) Per definizione, si hanno le condizioni $b \cdot a = 1$ e $a \cdot c = 1$. Per definizione di elemento neutro e per l'associatività dell'operazione binaria $\cdot$ su R data dalla definizione 6.1-(ii) si ricava la condizione seguente, dalla quale discende immediatamente la tesi:

$$b = b \cdot 1 = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1 \cdot c = c$$ □

Definizione 6.4. Sia R un anello con identità e sia $a \in R$ un elemento invertibile. Un inverso sinistro o destro di a si dice semplicemente un *inverso di* a e si denota a^{-1}.

Osservazione 6.3. Sia R un anello con identità e sia $a \in R$ un elemento invertibile. Dalle definizioni 6.3 e 6.4 e dall'osservazione 6.2-(ii) segue immediatamente che l'inverso di a è unico. Infatti, siccome a è un elemento invertibile, esso ammette almeno un inverso sinistro e un inverso destro, per cui posso applicare l'osservazione prima menzionata per ottenere che tutti gli inversi di a coincidono.

Si ricordi adesso che, dato un monoide M, il gruppo delle unità di M, introdotto nella definizione 1.2, è effettivamente un gruppo per l'osservazione 1.2. Per semplicità, si dà la seguente definizione.

Definizione 6.5. Sia R un anello con identità. Il gruppo delle unità del monoide $(R, \cdot, 1)$ prende il nome di *gruppo delle unità di* R e si denota $U(R)$.

Osservazione 6.4. Sia R un anello con identità. Se $1 = 0$, allora R è un anello banale, cioè $R = \{0\}$. Dato infatti un elemento $a \in R$, per definizione di elemento neutro e per la proposizione 6.1-(i) si ha la relazione:

$$a = a \cdot 1 = a \cdot 0 = 0$$

Definizione 6.6. Un anello con identità $1 \neq 0$ viene detto un *dominio* se non ammette divisori dello zero sinistri o destri non banali, cioè diversi da 0. Un dominio commutativo prende il nome di *dominio integrale* oppure *di integrità*). Un anello con identità $1 \neq 0$ è detto un *corpo* (o un *anello di divisione*) se ogni suo elemento non banale, cioè diverso da 0, è invertibile. Un corpo commutativo prende il nome di *campo*.

Osservazione 6.5. Dalla definizione 6.3 e dall'osservazione 6.2-(i) segue immediatamente che tutti i corpi sono domini. In particolare, tutti i campi sono domini integrali.

Osservazione 6.6. Sia R un anello con identità $1 \neq 0$. Valgono le seguenti affermazioni.

(i) R è un corpo se e solo se $U(R) = R \setminus \{0\}$.

(ii) R è un dominio se e solo se valgono le leggi di cancellazione, cioè se e solo se per ogni $a, b, c \in R$ con $a \neq 0$, la relazione $a \cdot b = a \cdot c$ implica $b = c$ e la relazione $b \cdot a = c \cdot a$ implica $b = c$.

Dimostrazione. La prima affermazione segue banalmente dalle definizioni 6.5 e 6.6, perciò sarà sufficiente dimostrare soltanto la seconda asserzione.

(ii) La dimostrazione del viceversa è immediata. Se infatti si assumono le leggi di cancellazione allora, prendendo $c := 0$, si ottiene che $a \cdot b = a \cdot 0$ implica $b = 0$ e che $b \cdot a = 0 \cdot a$ implica $b = 0$. In virtù della proposizione 6.1-(i) ciò equivale a dire che $a \cdot b = 0$ implica $b = 0$ e che $b \cdot a = 0$ implica $b = 0$. Per contrapposizione logica, ogni elemento $b \in R$, $b \neq 0$ non soddisfa né la condizione $a \cdot b = 0$, né $b \cdot a = 0$ e questo è come dire, per definizione, che a non è un divisore dello zero sinistro né destro. Siccome le leggi di cancellazione valgono per ogni $a \in R$ con $a \neq 0$, posso affermare che R non ha divisori dello zero non banali, cioè che R è un dominio.

L'implicazione diretta si dimostra, invece, come segue. Siano $a, b, c \in R$ con $a \neq 0$ elementi fissati tali che $a \cdot b = a \cdot c$. Sottraendo la quantità $a \cdot c$ a primo e secondo membro, usando la proprietà distributiva sinistra di $\cdot$ rispetto a $+$, vale a dire la definizione 6.1-(iii) e la proposizione 6.1-(iii), si ottiene la condizione seguente:

$$0 = (a \cdot b) - (a \cdot c) = (a \cdot b) + \big(a \cdot (-c)\big) = a \cdot (b - c)$$

Dato che per ipotesi R è un dominio, l'elemento a non può essere un divisore dello zero perché si assume $a \neq 0$. In particolare, dovrà valere che $b - c = 0$ altrimenti si avrebbe una contraddizione con l'affermazione precedente. Equivalentemente, si ha che $b = c$. Con un procedimento simile si dimostra che $b \cdot a = c \cdot a$ implica $b = c$ e posso dunque concludere, per arbitrarietà nella scelta di $a, b, c \in R$ con $a \neq 0$, che valgono le leggi di cancellazione. □

Osservazione 6.7. Sia R un dominio e sia $a \in R$. Se a è un elemento invertibile a sinistra oppure a destra, allora a è un elemento invertibile.

Dimostrazione. Si assuma che a sia un elemento invertibile a sinistra, cioè che esista un elemento $b \in R$ tale che $b \cdot a = 1$. Si osservi che, se fosse $b = 0$, allora si avrebbe che $1 = 0$ per la proposizione 6.1-(i), ma questo contraddice l'ipotesi che R sia un dominio (definizione 6.6) e dunque $b \neq 0$. Adesso, moltiplicando a destra per b entrambi i membri della relazione $b \cdot a = 1$, ottengo che $b \cdot (a \cdot b) = b$ ma allora, utilizzando l'ipotesi che R sia un dominio assieme al fatto che $b \neq 0$, posso applicare la legge di cancellazione sinistra data dall'osservazione 6.6-(ii) per ottenere che $a \cdot b = 1$ e questo dimostra che a è invertibile. Nel caso in cui si assume che a sia un elemento invertibile a destra anziché a sinistra, la dimostrazione è analoga. □

Osservazione 6.8. Sia R un dominio finito. Allora R è un corpo.

Dimostrazione. Sia $a \in R$, $a \neq 0$ un elemento prefissato e sia $f \colon R \to R$ la mappa definita da $f(b) := a \cdot b$. Si tratta di un'applicazione ben definita poiché si assume che R sia un dominio e in particolare un anello. Inoltre, essendo R un dominio, la suddetta funzione è iniettiva. Dati infatti due elementi $b_1, b_2 \in R$ tali che $f(b_1) = f(b_2)$, cioè tali che $a \cdot b_1 = a \cdot b_2$, ricordando che $a \neq 0$ si può applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)) per ottenere che $b_1 = b_2$. A questo punto, poiché si assume che R sia finito, posso affermare che f è anche un'applicazione suriettiva, ma allora deve esistere un elemento $b \in R$ tale che $f(b) = 1$ perché, essendo R un dominio, vale che $1 \in R$. In altre parole, esiste $b \in R$ tale che $a \cdot b = 1$ e questo dimostra, in virtù dell'osservazione 6.7, che a è un elemento invertibile. Posso dunque concludere, per la definizione 6.6 e per arbitrarietà nella scelta dell'elemento $a \in R$ con $a \neq 0$, che R è un corpo. □

Definizione 6.7. Sia R un anello. Un insieme $S \subseteq R$ si dice un *sottoanello di* R e si indica con $S < R$ se $(S, +, 0)$ è un sottogruppo di $(R, +, 0)$ e se $S \subseteq R$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su R, cioè se soddisfa la condizione $s_1 \cdot s_2 \in S$ per ogni $s_1, s_2 \in S$.

Osservazione 6.9. Sia $(R, +, 0, \cdot)$ un anello e sia $S < R$ un sottoanello. Dalle definizioni 1.5-(i) e 6.7 segue banalmente che $(S, \cdot)$ è un sottosemigruppo di $(R, \cdot)$. Dall'osservazione 1.4 segue dunque che $(S, +, 0)$ è un gruppo, mentre $(S, \cdot)$ è un semigruppo. Inoltre, poiché si assume che $(R, +, 0)$ sia un gruppo abeliano, lo è anche $(S, +, 0)$. Infine, le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$ in S discendono dal fatto che R è un anello. Queste facili considerazioni mostrano quindi che $(S, +, 0, \cdot)$ è un anello.

Esempio 6.1. Si consideri l'insieme numerico $\mathbb{Z}$ con le usuali operazioni di somma e prodotto. Dato che $(\mathbb{Z}, +, 0)$ e $(\mathbb{Z}, \cdot, 1)$ sono, rispettivamente, un gruppo abeliano e un monoide (esempi 1.1, 1.2 e 1.13) e dato che sono soddisfatte le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$, in virtù della definizione 6.1 vale che $(\mathbb{Z}, +, 0, \cdot, 1)$ è un anello con identità. Siccome $\mathbb{Z}$ è commutativo e non possiede divisori dello zero non banali, per la definizione 6.6 è anche un dominio integrale. Essendo però $U(\mathbb{Z}) = \{\pm 1\}$ come si è detto nell'esempio 1.9, per l'osservazione 6.6-(i) il dominio integrale $\mathbb{Z}$ non è un campo. È immediato verificare che $\langle n \rangle < \mathbb{Z}$ è un sottoanello per ogni $n \in \mathbb{N}$. Questo dimostra anche che un sottoanello di un anello con identità non è, in generale, un anello con identità.

Esempio 6.2. Si considerino gli insiemi numerici $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con le usuali operazioni di somma e prodotto. Proprio come nel caso di $\mathbb{Z}$, in virtù degli esempi 1.1, 1.2 e 1.13 vale che $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$ e $(\mathbb{C}, +, 0)$ sono gruppi abeliani, mentre $(\mathbb{Q}, \cdot, 1)$, $(\mathbb{R}, \cdot, 1)$ e $(\mathbb{C}, \cdot, 1)$ sono monoidi. Inoltre, valgono in tutti questi casi le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$ e di conseguenza $(\mathbb{Q}, +, 0, \cdot, 1)$, $(\mathbb{R}, +, 0, \cdot, 1)$ e $(\mathbb{C}, +, 0, \cdot, 1)$ sono anelli con identità per la definizione 6.1. Si ricordi adesso che $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$ e $U(\mathbb{C}) = \mathbb{C}^*$ in virtù dell'esempio 1.9 e quindi, utilizzando l'osservazione 6.6-(i) assieme al fatto che $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono anelli commutativi, si ottiene che essi sono campi.

Esempio 6.3. Sia $n \in \mathbb{N}^*$ fissato e si consideri $\mathbb{Z}_n$ con le usuali operazioni di somma e prodotto. In virtù degli esempi 1.3 e 1.13, si ha che $(\mathbb{Z}_n, +, \bar{0})$ è un gruppo abeliano, mentre $(\mathbb{Z}_n, \cdot, \bar{1})$ è un monoide. Inoltre, le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$ sono una conseguenza delle analoghe proprietà di $\mathbb{Z}$ e posso dunque affermare che $(\mathbb{Z}_n, +, \bar{0}, \cdot, \bar{1})$ è un anello con identità. Infine, si può dimostrare che $\mathbb{Z}_n$ è un dominio integrale se e solo se n è un numero primo. Si assuma infatti che n sia un numero primo e si considerino due classi $\bar{a}, \bar{b} \in \mathbb{Z}_n$ tali che $\bar{a}\bar{b} = \bar{0}$. Per come è definita la relazione di congruenza modulo n, vale che $n \mid ab$ ma allora, per definizione di numero primo, si ha che $n \mid a$ oppure $n \mid b$, cioè che $\bar{a} = \bar{0}$ oppure $\bar{b} = \bar{0}$. Questo dimostra, per arbitrarietà nella scelta delle classi $\bar{a}, \bar{b} \in \mathbb{Z}_n$ tali che $\bar{a}\bar{b} = \bar{0}$, che $\mathbb{Z}_n$ è un dominio integrale. Nel viceversa si procede per contrapposizione logica, assumendo che n non sia un numero primo. In tal caso, esistono $a, b \in \mathbb{Z}$ tali che $n \mid ab$ ma $n \nmid a$ e $n \nmid b$. Equivalentemente, passando alla congruenza modulo n, vale che $\bar{a}\bar{b} = \bar{0}$ con $\bar{a} \neq \bar{0}$ e $\bar{b} \neq \bar{0}$ e di conseguenza $\bar{a}$ e $\bar{b}$ sono divisori dello zero non banali in $\mathbb{Z}_n$. Questo dimostra che $\mathbb{Z}_n$ non è un dominio integrale.

Esempio 6.4. Sia V uno spazio vettoriale su un campo K. Come si è osservato negli esempi 1.7 e 1.12, vale che $(\mathrm{End}(V), +, o)$ e $(\mathrm{End}(V), \circ, \mathrm{id}_V)$ sono un gruppo e un monoide rispettivamente. Inoltre, si ha che $(\mathrm{End}(V), +, o)$ è un gruppo abeliano poiché la proprietà commutativa della somma $+$ vale per un[25] assioma degli spazi vettoriali. Inoltre, dato che le applicazioni in $\mathrm{End}(V)$ sono lineari, valgono le proprietà distributive sinistra e destra di $\circ$ rispetto a $+$ e si può dunque affermare che $(\mathrm{End}(V), +, o, \circ, \mathrm{id}_V)$ è un anello con identità. Dall'esempio 1.15 segue che $\mathrm{End}(V)$ è un anello commutativo se e solo se $\dim V \leq 1$. Si ricordi inoltre che $U(\mathrm{End}(V)) = \mathrm{GL}(V)$ per l'esempio 1.12.

Esempio 6.5. Sia $n \in \mathbb{N}^*$ fissato e sia K un campo. In virtù dell'esempio 1.8, si ha che $(\mathrm{M}_n(K), +, O)$ e $(\mathrm{M}_n(K), \cdot, I_n)$ sono un gruppo e un monoide rispettivamente. Inoltre, per una[26] delle proprietà basilari delle matrici valgono le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$ e posso dunque affermare che $(\mathrm{M}_n(K), +, O, \cdot, I_n)$ è un anello con identità. Chiaramente, si tratta di un anello non commutativo. L'anello $\mathrm{M}_n(K)$ non è un dominio, in quanto ammette divisori dello zero non banali. Infatti un esempio di divisore dello zero è dato dalla matrice $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, che è nilpotente di ordine 2, cioè tale che $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Esempio 6.6. Sia A un gruppo abeliano e sia $\mathrm{End}(A) := \{\, f \colon A \to A \mid f \text{ è un omomorfismo di gruppi} \,\}$. Sia inoltre $+$ l'operazione binaria su $\mathrm{End}(A)$ definita da $(f + g)(a) := f(a) + g(a)$. Si verifica facilmente

[25] Si vedano a tal proposito gli appunti del corso GE110, oppure le dispense del corso AM210.
[26] Per ottenere maggiori informazioni al riguardo, si vedano gli appunti del corso GE110.

che $(\mathrm{End}(A), +, o)$ e $(\mathrm{End}(A), \circ, \mathrm{id}_A)$ sono un gruppo e un monoide rispettivamente e che valgono anche le proprietà distributive sinistra e destra di $\circ$ rispetto a $+$, per cui $(\mathrm{End}(A), +, o, \circ, \mathrm{id}_A)$ è un anello con identità. Gli elementi invertibili in $\mathrm{End}(A)$ sono le applicazioni biiettive, quindi gli automorfismi di A. In altre parole, vale la condizione $U(\mathrm{End}(A)) = \mathrm{Aut}(A)$.

Esempio 6.7. Siano i, j, k simboli formali e sia $\mathbb{H} := \{\, a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \,\}$. Per semplicità, è convenzione che i termini con coefficiente 0 vengano omessi. Sia $+$ l'operazione binaria su $\mathbb{H}$ che consiste nell'operazione di somma usuale effettuata termine a termine. Sia invece $\cdot$ l'operazione binaria su $\mathbb{H}$ che viene definita a partire dalle proprietà distributive sinistra e destra rispetto a $+$ e dalle relazioni seguenti:

(i) $i^2 = j^2 = k^2 = -1$

(ii) $i \cdot j = -j \cdot i = k$

(iii) $j \cdot k = -k \cdot j = i$

(iv) $k \cdot i = -i \cdot k = j$

Si dimostra facilmente che $(\mathbb{H}, +, 0, \cdot, 1)$ è un anello con identità, detto l'*anello dei quaternioni*. Inoltre, fissato un quaternione $q = a + bi + cj + dk$ si definisce il *quaternione coniugato di* q come il quaternione $\bar{q} := a - bi - cj - dk$. Il quaternione coniugato soddisfa le seguenti proprietà, la cui verifica è immediata:

(a) $\overline{q_1 + q_2} = \bar{q}_1 + \bar{q}_2$ per ogni $q_1, q_2 \in \mathbb{H}$.

(b) $\overline{q_1 \cdot q_2} = \bar{q}_2 \cdot \bar{q}_1$ per ogni $q_1, q_2 \in \mathbb{H}$.

Si definisce invece la *norma di* q come il numero reale non negativo $|q| := \sqrt{q\bar{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$, che soddisfa la cosiddetta proprietà di "non degenerazione", cioè $|q| = 0$ se e solo se $q = 0$. A questo punto è immediato verificare che $q^{-1} = \frac{\bar{q}}{|q|^2}$ per ogni $q \in \mathbb{H}$, $q \neq 0$. Questo dimostra che $U(\mathbb{H}) = \mathbb{H} \setminus \{0\}$ e dunque, per l'osservazione 6.6-(i), posso concludere che $\mathbb{H}$ è un corpo. L'anello $\mathbb{H}$ non è tuttavia un campo perché non è commutativo, come mostrano per esempio le relazioni (ii), (iii) e (iv). Si può infine dimostrare che l'insieme $\{\pm 1, \pm i, \pm j, \pm k\} < U(H)$ è un sottogruppo isomorfo al gruppo dei quaternioni Q, introdotto con la definizione 2.16.

Esempio 6.8. Siano $(G, \star, e)$ un gruppo, $(R, +, 0, \cdot)$ un anello commutativo e sia $R(G) := \bigoplus_{g \in G} R$. Per semplicità, ciascun elemento $\{r_g\}_{g \in G} \in R(G)$ può essere indicato utilizzando una somma formale finita del tipo $\sum_{g \in G} r_g g$. Si tratta di una somma finita in quanto, per definizione di somma diretta (definizione 5.1), esistono $g_1, \ldots, g_k \in G$ tali che $r_g = 0$ per ogni $g \in G \setminus \{g_1, \ldots, g_k\}$. Utilizzando la notazione delle somme formali e denotando $+$ l'operazione binaria usuale per somme dirette, si ha la seguente condizione:

$$\left(\sum_{g \in G} r_g g\right) + \left(\sum_{g \in G} s_g g\right) = \sum_{g \in G} (r_g + s_g) g$$

Sia inoltre $\cdot$ l'operazione binaria su $R(G)$ definita dalla condizione seguente:

$$\left(\sum_{g \in G} r_g g\right) \cdot \left(\sum_{h \in G} r_h h\right) := \sum_{l \in G} \left(\sum_{\substack{g,h \in G \\ g \star h = l}} r_g \cdot r_h \right) l$$

In altre parole, l'operazione binaria $\cdot$ è univocamente determinata dalla distributività rispetto alla somma assieme alla regola $(r_g g) \cdot (r_h h) := (r_g \cdot r_h)(g \star h)$. Poiché per ipotesi R è un anello, vale in particolare che $(R, +, 0)$ è un gruppo abeliano e quindi lo è anche $(R(G), +, 0)$ in virtù dell'osservazione 5.4. Inoltre, si vede facilmente che l'operazione binaria $\cdot$ su $R(G)$ appena definita è associativa e che valgono le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$ e si può dunque concludere che $(R(G), +, 0, \cdot)$ è un anello. Tale anello prende il nome di *anello gruppale associato a* G *e* R. È infine immediato verificare che l'anello $R(G)$ è commutativo se e solo se G è un gruppo abeliano e che $R(G)$ è un anello con identità $\sum_{g \in G} 1g$ se e solo se R è un anello con identità 1.

Definizione 6.8. Un anello R viene detto *booleano* se $a^2 = a$ per ogni $a \in R$.

Esempio 6.9. Sia X un insieme. Come si è detto nell'esempio 1.4, vale che $(\mathcal{P}(X), \triangle, \varnothing)$ e $(\mathcal{P}(X), \cap, X)$ sono un gruppo e un monoide rispettivamente. È possibile dimostrare che valgono le proprietà distributive sinistra e destra di $\cap$ rispetto a $\triangle$ e dunque $(\mathcal{P}(X), \triangle, \varnothing, \cap, X)$ è un anello con identità. Inoltre, per le proprietà dell'intersezione $\cap$ è ovviamente un anello commutativo e booleano.

Esempio 6.10. Siano X un insieme non vuoto, R un anello e sia $R^X := \{ f \colon X \to R \}$. Siano inoltre $+$ e $\cdot$ le operazioni binarie su R^X definite dalle due condizioni seguenti:

$$(f+g)(x) := f(x) + g(x)$$
$$(f \cdot g)(x) := f(x) \cdot g(x)$$

Utilizzando il fatto che R è un anello, si vede facilmente che $(R^X, +, o)$ e $(R^X, \cdot)$ sono un gruppo abeliano e un semigruppo rispettivamente. Inoltre, valgono le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$ e dunque $(R^X, +, o, \cdot)$ è un anello. Se inoltre R è un anello con identità e $u \colon X \to R$ è l'applicazione data da $u(x) := 1$, allora $(R^X, +, o, \cdot, u)$ è un anello con identità. Vi è un naturale isomorfismo di gruppi tra $(R^X, +, 0)$ e il prodotto diretto $\prod_{x \in X} R$. In particolare, se $|X| < +\infty$ e se $n := |X|$, allora l'anello R^S si denota R^n ed è essenzialmente l'insieme delle n-uple a coefficienti in R.

Esempio 6.11. Sia $(R, +, 0, \cdot)$ un anello e sia $\circ$ l'operazione binaria su R definita da $a \circ b := b \cdot a$. Allora si dimostra con estrema facilità che anche $(R, +, 0, \circ)$ è un anello, detto l'*anello opposto di* R e denotato R^{opp}. Altrettanto facilmente si possono dimostrare le seguenti proprietà:

(i) R^{opp} è un anello con identità se e solo se lo è R e in tal caso le identità coincidono.

(ii) R^{opp} e R sono lo stesso anello se e solo se R è un anello commutativo.

(iii) I divisori dello zero sinistri di R^{opp} sono i divisori dello zero destri di R. Analogamente, i divisori dello zero destri di R^{opp} sono i divisori dello zero sinistri di R.

(iv) Gli elementi invertibili a sinistra e gli inversi sinistri di R^{opp} sono gli elementi invertibili a destra e gli inversi destri di R. Analogamente, gli elementi invertibili a destra e gli inversi destri di R^{opp} sono gli elementi invertibili a sinistra e gli inversi sinistri di R.

(v) R^{opp} è un dominio se e solo se R un dominio.

(vi) R^{opp} è un corpo se e solo se R un corpo.

(vii) L'anello opposto di R^{opp} è R.

Esempio 6.12. Siano $n \in \mathbb{N}^*$ fissato, R un anello e si consideri il seguente insieme:

$$R[X_1, \dots, X_n] := \left\{ \sum_{I \in \mathbb{N}^n} r_I X^I \;\middle|\; r_I \in R\,,\ r_I = 0 \text{ per ogni } I \in \mathbb{N}^n \setminus \{I_1, \dots, I_k\},\ \exists\, I_1, \dots, I_k \in \mathbb{N}^n \right\}$$

Qui il simbolo di sommatoria sta a indicare una somma formale finita, $I = (i_1, \dots, i_n)$ è un vettore, mentre $X^I := X_1^{i_1} \cdots X_n^{i_n}$ è un simbolo formale che semplifica la notazione. Siano ora $+$ e $\cdot$ le operazioni binarie su $R[X_1, \dots, X_n]$ definite dalle due condizioni seguenti:

$$\left(\sum_{I \in \mathbb{N}^n} r_I X^I \right) + \left(\sum_{I \in \mathbb{N}^n} s_I X^I \right) := \sum_{I \in \mathbb{N}^n} (r_I + s_I) X^I$$
$$\left(\sum_{I \in \mathbb{N}^n} r_I X^I \right) \cdot \left(\sum_{J \in \mathbb{N}^n} s_J X^J \right) := \sum_{K \in \mathbb{N}^n} \left(\sum_{\substack{I, J \in \mathbb{N}^n \\ I+J=K}} r_I \cdot s_J \right) X^K$$

Ragionando come nell'esempio 6.8, si dimostra facilmente che $(R[X_1, \dots, X_n], +, 0, \cdot)$ è un anello, detto l'*anello dei polinomi su* R *in* n *variabili*. Un elemento della forma $r_I X^I$ per un qualche $I \in \mathbb{N}^n$ si dice un *monomio*, mentre una combinazione lineare di monomi prende il nome di *polinomio*. Per convenzione, se $n = 0$, si pone inoltre $R[X_1, \dots, X_n] := R$. Si noti anche che, alternativamente, si può dare una definizione induttiva dell'anello dei polinomi su R in n variabili. Basta infatti definire $R[X_1]$ e, per ogni $n \in \mathbb{N}$, $n \geq 2$, porre $R[X_1, \dots, X_n] := (R[X_1, \dots, X_{n-1}])[X_n]$. Si può infine osservare che, generalizzando la definizione

di anello gruppale data nell'esempio 6.8, l'anello $R[X_1, \dots, X_n]$ si può anche definire come l'anello $R(\mathbb{N}^n)$ associato al monoide $\mathbb{N}^n$ e a R. Se si utilizza questa definizione, dall'esempio 6.8 segue immediatamente che l'anello $R[X_1, \dots, X_n]$ è commutativo in quanto $\mathbb{N}^n$ è un monoide abeliano e inoltre $R[X_1, \dots, X_n]$ è un anello con identità $1 \cdot X^{\mathbf{0}}$, dove $\mathbf{0} \in \mathbb{N}^n$ denota la n-upla nulla, se e solo se R è un anello con identità 1.

Esempio 6.13. Siano $n \in \mathbb{N}^*$ fissato, R un anello e si consideri il seguente insieme:

$$R[\![X_1, \dots, X_n]\!] := \left\{ \sum_{I \in \mathbb{N}^n} r_I X^I \;\middle|\; r_I \in R \right\}$$

In questo caso, il simbolo di sommatoria denota una somma formale possibilmente infinita. Esattamente come nell'esempio 6.12, $I = (i_1, \dots, i_n)$ è un vettore, mentre $X^I := X_1^{i_1} \cdots X_n^{i_n}$ è un simbolo formale atto a semplificare la notazione. Si definiscono inoltre su $R[\![X_1, \dots, X_n]\!]$ le stesse operazioni binarie $+$ e $\cdot$ date nell'esempio 6.12. Anche stavolta basterà ripetere un argomento simile a quello adottato nell'esempio 6.8 per dimostrare che $(R[\![X_1, \dots, X_n]\!], +, 0, \cdot)$ è un anello. Quest'ultimo prende il nome di *anello delle serie di potenze su* R. A questo punto, si vede facilmente che $R[X_1, \dots, X_n] < R[\![X_1, \dots, X_n]\!]$ è un sottoanello.

6.2 Omomorfismi e caratteristica

Definizione 6.9. Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ due anelli. Un'applicazione $f \colon R \to S$ viene detta un *omomorfismo da* R *a* S se soddisfa le condizioni $f(a+b) = f(a) + f(b)$ e $f(a \cdot b) = f(a) \star f(b)$ per ogni $a, b \in R$. Inoltre, un omomorfismo iniettivo prende il nome di *monomorfismo*, un omomorfismo suriettivo si dice un *epimorfismo*, mentre un omomorfismo biiettivo viene detto un *isomorfismo*. Infine, si dice che R e S sono *isomorfi* e si scrive $R \simeq S$ se esiste un isomorfismo da R a S.

Osservazione 6.10. Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ due anelli e si consideri un omomorfismo $f \colon R \to S$. Una conseguenza parecchio banale delle definizioni 2.15 e 6.9 è che f è anche un omomorfismo di gruppi da $(R, +, 0_R)$ a $(S, +, 0_S)$.

Dall'osservazione 6.10 e dalle proprietà note degli omomorfismi di gruppi derivano immediatamente i risultati seguenti.

Osservazione 6.11. Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ due anelli e si consideri un omomorfismo $f \colon R \to S$. Allora $f(0_R) = 0_S$.

Osservazione 6.12. Siano R e S anelli e sia $f \colon R \to S$ un omomorfismo. Allora si ha che $-f(g) = f(-g)$ per ogni scelta di un elemento $g \in G_1$.

Osservazione 6.13. Siano $(R, +, 0_R, \cdot, 1_R)$, $(S, +, 0_S, \star, 1_S)$ due anelli con identità. In generale, non vale un risultato analogo all'osservazione 6.11 con gli elementi neutri rispetto al prodotto, cioè non vale che, se $f \colon R \to S$ è un omomorfismo, allora $f(1_R) = 1_S$. Un controesempio è dato dalla funzione identicamente nulla $o \colon R \to S$ la quale, pur essendo un omomorfismo come è immediato verificare, è tale che $o(1_R) = 0_S$.

Osservazione 6.14. Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ anelli, $f \colon R \to S$ un omomorfismo e si considerino elementi $a_1, \dots, a_n \in R$. Dalla definizione 6.9 segue facilmente, per induzione sul numero n degli elementi considerati, che valgono le due condizioni seguenti:

$$f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n)$$
$$f(a_1 \cdots a_n) = f(a_1) \star \cdots \star f(a_n)$$

Definizione 6.10. Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ due anelli e si consideri un omomorfismo $f \colon R \to S$. L'insieme $\operatorname{Ker} f := \{\, a \in R \mid f(a) = 0_S \,\}$ prende il nome di *nucleo* (o *kernel*) *di* f.

Osservazione 6.15. Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ anelli, $f \colon R \to S$ un omomorfismo. Allora si ha che:

(i) $\operatorname{Im} f < S$ è un sottoanello e inoltre $\operatorname{Im} f = S$ se e solo se f è un epimorfismo.

(ii) $\operatorname{Ker} f < R$ è un sottoanello e inoltre $\operatorname{Ker} f = \{0_R\}$ se e solo se f è un monomorfismo.

Dimostrazione.

(i) Per la proposizione 3.1-(i) assieme all'osservazione 6.10 vale che $\operatorname{Im} f < S$ è un sottogruppo. Siano adesso $s_1, s_2 \in \operatorname{Im} f$ due elementi prefissati. Per definizione di immagine, esistono $r_1, r_2 \in R$ tali che $f(r_1) = s_1$, $f(r_2) = s_2$. Dato che per ipotesi f è un omomorfismo, vale la seguente condizione:

$$s_1 \star s_2 = f(r_1) \star f(r_2) = f(r_1 \cdot r_2)$$

Poiché per ipotesi R è un anello, vale in particolare che $\cdot$ è un'operazione binaria su R e dunque $r_1 \cdot r_2 \in R$. In particolare, per definizione di immagine, si ha che $s_1 \star s_2 \in \operatorname{Im} f$ e questo dimostra, per arbitrarietà nella scelta di $s_1, s_2 \in \operatorname{Im} f$, che $\operatorname{Im} f \subseteq S$ è chiuso rispetto all'operazione binaria $\star$ su S. Per la definizione 6.7 posso quindi concludere che $\operatorname{Im} f < S$ è un sottoanello.

La seconda parte deriva banalmente dal fatto che $\operatorname{Im} f = S$ se e solo se f è una mappa suriettiva, assieme alla definizione 6.9 e all'ipotesi che f sia un omomorfismo.

(ii) Per la proposizione 3.1-(ii) con l'osservazione 6.10 si ha che $\operatorname{Ker} f < R$ è un sottogruppo. Siano ora $a_1, a_2 \in \operatorname{Ker} f$ elementi fissati e si noti che, per l'ipotesi che f sia un omomorfismo e in virtù della definizione 6.10, vale la condizione seguente:

$$f(a_1 \cdot a_2) = f(a_1) \star f(a_2) = 0_S \star 0_S = 0_S$$

Questo dimostra che anche $a_1 \cdot a_2 \in \operatorname{Ker} f$. Non dipendendo il risultato ottenuto dalla scelta degli elementi $a_1, a_2 \in \operatorname{Ker} f$, posso dunque affermare che $\operatorname{Ker} f \subseteq R$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su R. Di conseguenza, vale che $\operatorname{Ker} f < R$ è un sottoanello.

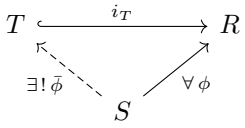
La seconda parte deriva immediatamente dalla proposizione 3.1-(ii), dall'osservazione 6.10 e dalla definizione 6.9. □

Esempio 6.14. Sia R un anello e sia $S < R$ un sottoanello. Allora è immediato verificare che la funzione $i\colon S \to R$ definita da $i(x) := x$, nota come la mappa *inclusione*, è un omomorfismo di anelli. Ovviamente, si tratta di un'applicazione iniettiva, dunque di un monomorfismo.

Proposizione 6.2 (Proprietà universale delle inclusioni per anelli)**.** *Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ due anelli, sia $T < R$ un sottoanello. Allora la mappa inclusione $i_T\colon T \to R$ soddisfa la proprietà universale:*

$$\forall\, \phi\colon S \to R \text{ omomorfismo, con } \operatorname{Im}\phi \subseteq T \;\; \exists!\, \bar{\phi}\colon S \to T \text{ omomorfismo} \;\mid\; i_T \circ \bar{\phi} = \phi$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



Dimostrazione. Si fissi un omomorfismo $\phi\colon S \to R$. Per la proprietà universale delle inclusioni per gruppi, vale a dire la proposizione 3.2-(i), esiste un unico omomorfismo di gruppi $\bar{\phi}\colon S \to T$ tale che $i_T \circ \bar{\phi} = \phi$. Bisogna però osservare che tale applicazione è anche un omomorfismo di anelli. Dalla dimostrazione della proposizione 3.2-(i) segue che l'applicazione $\bar{f}$ è definita semplicemente da $\bar{f}(x) := f(x)$ e di conseguenza $\bar{f}$ è un omomorfismo di anelli perché lo è f. □

Esempio 6.15. Si consideri la mappa quoziente $q\colon \mathbb{Z} \to \mathbb{Z}_n$ definita da $q(x) := \bar{x}$. È facile verificare che q è un omomorfismo di anelli. Essendo inoltre q una funzione suriettiva per costruzione, è un epimorfismo.

Esempio 6.16. Siano G, H gruppi, R un anello commutativo e sia $\phi\colon G \to H$ un omomorfismo. Allora si vede facilmente, utilizzando le definizioni date nell'esempio 6.8 e l'assunzione che ϕ sia un omomorfismo di gruppi, che l'applicazione $R(\phi)\colon R(G) \to R(H)$ definita dalla relazione $R(\phi)(\sum_{g\in G} r_g g) := \sum_{g\in G} r_g \phi(g)$ è un omomorfismo di anelli.

Definizione 6.11. Sia R un anello.

(i) Si dice che R ha *caratteristica positiva* (o *finita*) se esiste $n \in \mathbb{N}^*$ tale che $na = 0$ per ogni $a \in R$. In caso affermativo, il più piccolo $n \in \mathbb{N}^*$ che soddisfa tale proprietà viene detto la *caratteristica di R e si denota* $\operatorname{car}(R)$.

(ii) Si dice che R ha *caratteristica zero* (o *infinita*) se non ha caratteristica positiva. In tal caso, si pone $\mathrm{car}(R) := 0$ per convenzione.

Proposizione 6.3 (Caratteristica di un anello con identità)**.** *Sia $(R, +, 0_R, \cdot, 1_R)$ un anello con $1_R \neq 0_R$ e sia $n := \mathrm{car}(R)$. Valgono le seguenti affermazioni.*

(i) *Esiste un unico omomorfismo di anelli $\Phi\colon \mathbb{Z} \to R$ tale che $\Phi(1) = 1_R$.*

(ii) *Se $n > 0$, allora n è il più piccolo intero positivo tale che $n1_R = 0_R$. Si ha invece che $n = 0$ se e solo se $k1_R \neq 0_R$ per ogni $k \in \mathbb{N}^*$.*

(iii) *Vale che $\mathrm{Ker}\,\Phi = \langle n \rangle$.*

(iv) *Se R è un dominio, allora $n = 0$ oppure n è un numero primo.*

Dimostrazione.

(i) Sia $\Phi\colon \mathbb{Z} \to R$ l'applicazione definita da $\Phi(k) := k1_R$. Ovviamente, vale che $\Phi(1) = 1_R$ e inoltre, dati $k, h \in \mathbb{Z}$ si hanno, per due proprietà delle potenze (osservazione 1.10) e per la distributività generalizzata di $\cdot$ rispetto a $+$ (proposizione 6.1-(ii)), le condizioni seguenti:

$$\Phi(k+h) = (k+h)1_R = k1_R + h1_R = \Phi(k) + \Phi(h)$$

$$\Phi(kh) = (kh)1_R = k(h1_R) = \sum_{i=1}^{k}\sum_{j=1}^{h} 1_R = \left(\sum_{i=1}^{k} 1_R\right) \cdot \left(\sum_{j=1}^{h} 1_R\right) = k1_R \cdot h1_R = \Phi(k) \cdot \Phi(h)$$

Tali relazioni dimostrano, per arbitrarietà nella scelta di $k, h \in \mathbb{Z}$, che Φ è un omomorfismo. Sia adesso $\Psi\colon \mathbb{Z} \to R$ un omomorfismo tale che $\Psi(1) = 1_R$. Allora, in virtù dell'osservazione 6.14, si ha per ogni $k \in \mathbb{Z}$ la relazione seguente:

$$\Psi(k) = \Psi(k1) = k\Psi(1) = k1_R = \Phi(k)$$

Non dipendendo il risultato ottenuto da una particolare scelta dell'omomorfismo $\Psi\colon \mathbb{Z} \to R$ tale che $\Psi(1) = 1_R$, posso concludere che Φ è unico.

(ii) Si supponga che $n > 0$ e sia $k \in \mathbb{N}^*$ il più piccolo intero positivo tale che $k1_R = 0_R$. In virtù della definizione 6.11-(i) si ha, in particolare, che $n1_R = 0_R$ e di conseguenza $k \leq n$ per la minimalità di k. D'altra parte, per definizione di elemento neutro, per i punti (i) e (iii) della proposizione 6.1, vale per ogni $a \in R$ la condizione seguente:

$$ka = k(1_R \cdot a) = (k1_R) \cdot a = 0_R \cdot a = 0_R$$

Per la minimalità di n dovuta alla definizione 6.11-(i), posso affermare che $n \leq k$ e in definitiva si ha che $n = k$. La seconda affermazione è una facile conseguenza della prima. Si supponga infatti che $n = 0$. Se esistesse $k \in \mathbb{N}^*$ tale che $k1_R = 0_R$ allora, ragionando esattamente come prima, si otterrebbe che $ka = 0_R$ per ogni $a \in R$. Questo tuttavia equivale a dire, per la definizione 6.11-(i), che R ha caratteristica positiva, contraddicendo il fatto che $n = 0$. Viceversa, suppongo che valga $k1_R \neq 0_R$ per ogni $k \in \mathbb{N}^*$. Se fosse $n > 0$ allora, per la definizione 6.11-(i), esisterebbe $k \in \mathbb{N}^*$ tale che $k1_R = 0_R$ e questo è assurdo. Queste semplici considerazioni mi danno la tesi.

(iii) Si ricordi, innanzitutto, che tutti i sottogruppi di $\mathbb{Z}$ sono del tipo $\langle k \rangle$ con $k \in \mathbb{N}$ e che $\mathrm{Ker}\,\Phi < \mathbb{Z}$ è un sottogruppo per la proposizione 3.1-(ii). Di conseguenza, esiste $k \in \mathbb{N}$ tale che $\mathrm{Ker}\,\Phi = \langle k \rangle$. A questo punto distinguo due possibilità. Se $n > 0$, allora sarà sufficiente mostrare che k è il più piccolo intero positivo tale che $k1_R = 0_R$. Essendo $\mathrm{Ker}\,\Phi = \langle k \rangle$, varrà in particolare che $k \in \mathrm{Ker}\,\Phi$ e questo implica, per definizione di nucleo e per costruzione di Φ, che $k1_R = 0_R$. Inoltre, vale che $k > 0$ perché $n > 0$ e $n \in \mathrm{Ker}\,\Phi$ per costruzione di Φ e per definizione di caratteristica. Sia adesso $h \in \mathbb{N}^*$ tale che $h1_R = 0_R$. Ancora per costruzione di Φ, si ha che $h \in \mathrm{Ker}\,\Phi$ e dunque $h \in \langle k \rangle$ in quanto $\mathrm{Ker}\,\Phi = \langle k \rangle$. In particolare, si ha che $k \leq h$ e questo dimostra la minimalità di k. Posso dunque affermare che $k = n$ in virtù del punto (ii) appena dimostrato. Se invece $n = 0$ allora, di nuovo per il punto (ii) già dimostrato, vale che $h1_R \neq 0_R$ per ogni $h \in \mathbb{N}^*$. Di conseguenza, si ha che $h \in \mathrm{Ker}\, f$ se e solo se $h = 0$. Utilizzando il fatto che $\mathrm{Ker}\, f = \langle k \rangle$, dalla condizione precedente si deduce in particolare che $k = 0$. Posso dunque concludere che $\mathrm{Ker}\, f = \langle n \rangle$.

(iv) Se $n = 0$, allora non vi è nulla da dimostrare, perciò assumo $n > 0$ e dimostro che n è un numero primo. Per farlo, sarà sufficiente dimostrare che ogni fattorizzazione di n è banale. Siano dunque $k_1, k_2 \in \mathbb{N}^*$ due elementi prefissati tali che $n = k_1 k_2$. Dalla definizione 6.11-(i), da una proprietà delle potenze (osservazione 1.10) e dalla proprietà distributiva generalizzata (proposizione 6.1-(ii)) deriva la condizione seguente:

$$0_R = n1_R = (k_1k_2)1_R = k_1(k_2 1_R) = \sum_{i=1}^{k_1}\sum_{j=1}^{k_2} 1_R = \left(\sum_{i=1}^{k_1} 1_R\right) \cdot \left(\sum_{j=1}^{k_2} 1_R\right) = (k_1 1_R) \cdot (k_2 1_R)$$

Se $k_1 1_R = 0_R$ e $k_2 1_R = 0_R$ allora, per la minimalità di n data dal punto (ii) già dimostrato, si ha che $n \leq k_1$ e $n \leq k_2$. Dalla relazione $n \leq k_1$, equivalente a $k_1 k_2 \leq k_1$, si ricava che $k_1(k_2 - 1) \leq 0$. Essendo $k_1 \in \mathbb{N}^*$, dovrà valere che $k_1 \geq 0$ e di conseguenza $k_2 - 1 \leq 0$. Essendo $k_2 \in \mathbb{N}^*$, si deduce che $k_2 = 1$. Ragionando allo stesso modo, dalla condizione $n \leq k_2$ si ricava che $k_1 = 1$. Ma allora anche $n = 1$ e quindi $1_R = 0_R$ per definizione di caratteristica. Questo contraddice le ipotesi, per cui dovrà valere che $k_1 1_R \neq 0_R$ oppure $k_2 1_R \neq 0_R$. Mi limito a studiare il caso in cui $k_1 1_R \neq 0_R$, in quanto l'altra possibilità si tratta con un procedimento analogo. Per la condizione precedente e per la definizione 6.2, si ha che $k_2 1_R$ è un divisore dello zero. A questo punto utilizzo l'ipotesi che R sia un dominio per affermare che $k_2 1_R = 0$. Di nuovo per la minimalità di n nel punto (ii) già dimostrato, posso affermare che $n \leq k_2$. D'altra parte, ricordando che $k_1 \in \mathbb{N}^*$, dovrà valere anche la condizione $k_2 \leq n$ e dunque $k_2 = n$. Questo dimostra che la fattorizzazione $n = k_1 k_2$ è banale ma allora, poiché il risultato ottenuto non dipende da una particolare scelta di $k_1, k_2 \in \mathbb{N}^*$, posso affermare che n è un numero primo e questo conclude la dimostrazione. □

Definizione 6.12. Sia $(R, +, 0_R, \cdot, 1_R)$ un anello con $1_R \neq 0_R$. L'omomorfismo di anelli $\Phi\colon \mathbb{Z} \to R$ dato dalla condizione $\Phi(k) := k1_R$ prende il nome di *omomorfismo caratteristico*.

La definizione 6.12 è ben posta in quanto, come si è visto nella dimostrazione della proposizione 6.3-(i), l'applicazione Φ è effettivamente un omomorfismo di anelli.

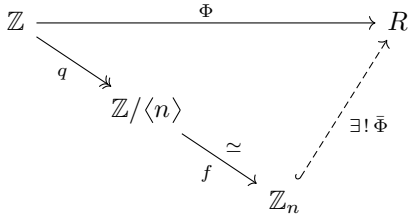
Corollario 6.1. *Sia $(R, +, 0_R, \cdot, 1_R)$ un anello con $1_R \neq 0_R$ e sia $n := \mathrm{car}(R)$. Allora, per ogni $k \in \mathbb{N}^*$ tale che $k1_R = 0_R$, vale che $n \mid k$.*

Dimostrazione. Sia $k \in \mathbb{N}^*$ un elemento fissato tale che $k1_R = 0_R$. Dalle definizioni 6.10 e 6.12 segue che $k \in \mathrm{Ker}\,\Phi$, ma per la proposizione 6.3-(iii) vale che $\mathrm{Ker}\,\Phi = \langle n \rangle$ e di conseguenza $k \in \langle n \rangle$. In particolare, si ha la tesi. □

Osservazione 6.16. Sia $(R, +, 0_R, \cdot, 1_R)$ un anello con $1_R \neq 0_R$ e sia $n := \mathrm{car}(R)$. Valgono le proprietà:

(i) $n = 0$ se e solo se l'omomorfismo caratteristico Φ è un monomorfismo.

(ii) Se $n > 0$, sia $q\colon \mathbb{Z} \to \mathbb{Z}/\langle n \rangle$ la mappa quoziente e sia $f\colon \mathbb{Z}/\langle n \rangle \to \mathbb{Z}_n$ l'isomorfismo definito dalla condizione $f(k\langle n \rangle) := \bar{k}$. Allora esiste un unico monomorfismo $\bar{\Phi}\colon \mathbb{Z}_n \to R$ tale che $\bar{\Phi} \circ f \circ q = \Phi$ oppure, equivalentemente, tale che il seguente diagramma di omomorfismi sia commutativo:

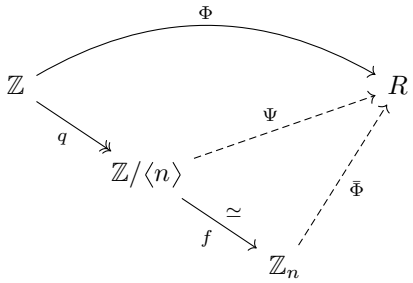


Dimostrazione.

(i) L'asserto deriva immediatamente dalla proposizione 6.3-(iii) e dall'osservazione 6.15-(ii).

(ii) Si osservi, innanzitutto, che il gruppo quoziente $\mathbb{Z}/\langle n \rangle$ è ben definito perché, essendo $\mathbb{Z}$ un gruppo abeliano, tutti i suoi sottogruppi sono normali. Inoltre, la mappa f è ben posta in virtù di quanto si è detto nell'esempio 2.6. Per la proposizione 6.3-(iii) posso applicare la proprietà universale dei

quozienti (proposizione 3.2-(ii)), in virtù della quale esiste uno e un solo omomorfismo di gruppi $\Psi\colon \mathbb{Z}/\langle n\rangle \to R$ tale che $\Psi \circ q = \Phi$. Essendo f un isomorfismo, esiste l'applicazione inversa f^{-1} e questa è a sua volta un isomorfismo per l'osservazione 1.6. Posso dunque considerare la funzione $\bar{\Phi}\colon \mathbb{Z}_n \to R$ definita da $\bar{\Phi} := \Psi \circ f^{-1}$. Il seguente diagramma sintetizza la costruzione precedente:



In virtù dell'osservazione 3.3, la mappa $\bar{\Phi}$ è un omomorfismo di gruppi in quanto composizione di omomorfismi. Per la dimostrazione della proprietà universale dei quozienti e per costruzione si ha che $\bar{\Phi}(\bar{k}) = k1_R$ per ogni $\bar{k} \in \mathbb{Z}_n$. A questo punto si vede assai facilmente che $\bar{\Phi}$ è un omomorfismo di anelli. Infatti, comunque fissati $\bar{k}, \bar{h} \in \mathbb{Z}_n$, per una proprietà delle potenze (osservazione 1.10) e per la proprietà distributiva generalizzata (proposizione 6.1-(ii)) si ha la condizione che segue:

$$\bar{\Phi}(\bar{k}\cdot\bar{h}) = (kh)1_R = k(h1_R) = \sum_{i=1}^{k}\sum_{j=1}^{h} 1_R = \left(\sum_{i=1}^{k} 1_R\right)\cdot\left(\sum_{j=1}^{h} 1_R\right) = k1_R \cdot h1_R = \bar{\Phi}(\bar{k})\cdot\bar{\Phi}(\bar{h})$$

Tenendo a mente che $\Psi \circ q = \Phi$ per la proprietà universale dei quozienti e che $\operatorname{Ker}\Phi = \langle n\rangle$ per la proposizione 6.3-(iii), calcolo infine il nucleo dell'omomorfismo Ψ:

$$\begin{aligned}\operatorname{Ker}\Psi &= \{\, k\langle n\rangle \in \mathbb{Z}/\langle n\rangle \mid \Psi(k\langle n\rangle) = 0_R \,\}\\ &= \{\, k\langle n\rangle \in \mathbb{Z}/\langle n\rangle \mid (\Psi\circ q)(k) = 0_R \,\}\\ &= \{\, k\langle n\rangle \in \mathbb{Z}/\langle n\rangle \mid \Phi(k) = 0_R \,\} = \operatorname{Ker}\Phi = \langle n\rangle\end{aligned}$$

Posso dunque concludere, per la proposizione 3.1-(ii), che Ψ è un monomorfismo. In particolare, l'omomorfismo di anelli $\bar{\Phi}$ è un monomorfismo poiché composizione di mappe iniettive. L'unicità è una conseguenza immediata del fatto che Ψ è unica per la proprietà universale dei quozienti, f^{-1} è unica per l'unicità dell'applicazione inversa e in virtù della discussione precedente. □

Proposizione 6.4 (Immersione in anelli con identità)**.** *Sia* $(R, +, 0_R, \cdot)$ *un anello. Allora esiste un anello* S *con identità, con* $\operatorname{car}(S) = 0$ *oppure con* $\operatorname{car}(S) = \operatorname{car}(R)$*, ed esiste un sottoanello* $T < S$ *tale che* $R \simeq T$*.*

Dimostrazione. Nel corso della dimostrazione verranno presentate due costruzioni. La prima costruzione dà luogo a un anello S tale che $\operatorname{car}(S) = 0$ e vale in generale, mentre la seconda costruzione dà origine a un anello S con $\operatorname{car}(S) = \operatorname{car}(R)$ e vale soltanto nel caso in cui $\operatorname{car}(R) > 0$.

- *Prima costruzione.* Pongo $S := R \oplus \mathbb{Z}$ e considero l'operazione binaria $\cdot$ su S data dalla relazione:

$$(r_1, k_1)\cdot(r_2, k_2) := (r_1\cdot r_2 + k_1 r_2 + k_2 r_1, k_1 k_2)$$

Per costruzione, tale operazione binaria su S è ben definita. Si vede facilmente che $\cdot$ è associativa e che $(0_R, 1)$ è un elemento neutro. In altre parole, l'insieme S munito dell'operazione binaria $\cdot$ è un monoide con elemento neutro $(0_R, 1)$. Si ricordi che S con l'operazione binaria usuale della somma diretta (osservazione 4.17), che in questo contesto verrà denotata con il simbolo $+$, è un gruppo abeliano con elemento neutro $(0_R, 0)$. Si osservi infine che vale la proprietà distributiva sinistra di $\cdot$ rispetto a $+$, poiché per ogni $(r_1, k_1), (r_2, k_2), (r_3, k_3) \in S$ si ha, in virtù dell'ipotesi che R sia un anello e del fatto che $\mathbb{Z}$ sia un anello, per le proprietà delle potenze (osservazioni 1.10 e 1.11) e per

definizione dell'operazione binaria $+$ su S, la condizione seguente:

$$\begin{aligned}(r_1,k_1)\cdot\big((r_2,k_2)+(r_3,k_3)\big) &= (r_1,k_1)\cdot(r_2+r_3,k_2+k_3)\\ &= \big(r_1\cdot(r_2+r_3)+k_1(r_2+r_3)+(k_2+k_3)r_1, k_1(k_2+k_3)\big)\\ &= (r_1\cdot r_2+r_1\cdot r_3+k_1r_2+k_1r_3+k_2r_1+k_3r_1, k_1k_2+k_1k_3)\\ &= (r_1\cdot r_2+k_1r_2+k_2r_1,k_1k_2)+(r_1\cdot r_3+k_1r_3+k_3r_1,k_1k_3)\\ &= \big((r_1,k_1)\cdot(r_2,k_2)\big)+\big((r_1,k_1)\cdot(r_3,k_3)\big)\end{aligned}$$

Con un procedimento sostanzialmente identico si dimostra che vale anche la proprietà distributiva destra di $\cdot$ rispetto a $+$ e posso dunque concludere che $(S,+,(0_R,0),\cdot,(0_R,1))$ è un anello. Si noti che $\mathrm{car}(S)=0$ in quanto $k(0_R,1)=(0_R,k)\neq(0_R,0)$ per ogni $k\in\mathbb{N}^*$. Ora, posto $T:=R\oplus\{0\}$, è immediato verificare che $T<S$ è un sottoanello e che la funzione $f\colon R\to T$ data da $f(r):=(r,0)$ è un isomorfismo di anelli.

- *Seconda costruzione.* Pongo per semplicità $n:=\mathrm{car}(R)$, assumo che $n>0$ e pongo $S:=R\oplus\mathbb{Z}_n$. Si consideri l'operazione binaria $\cdot$ su S definita dalla seguente condizione:

$$(r_1,\bar{k}_1)\cdot(r_2,\bar{k}_2):=(r_1\cdot r_2+k_1r_2+k_2r_1,\bar{k}_1\bar{k}_2)$$

Dimostro che $\cdot$ è un'operazione binaria ben definita, vale a dire che non dipende da una particolare scelta dei rappresentanti delle classi di resto modulo n. Siano $\bar{k}_1,\bar{h}_1,\bar{k}_2,\bar{h}_2\in\mathbb{Z}_n$ tali che valgano le due condizioni $\bar{k}_1=\bar{h}_1$ e $\bar{k}_2=\bar{h}_2$. Allora, per come è definita la relazione di congruenza modulo n, si ha che $k_1=h_1+l_1n$ e che $k_2=h_2+l_2n$ per opportuni $l_1,l_2\in\mathbb{Z}$. Ricordando che $n=\mathrm{car}(R)$ e applicando le proprietà delle potenze (osservazione 1.10), si ricava quindi la relazione seguente:

$$k_1r_2=(h_1+l_1n)r_2=h_1r_2+l_1(nr_2)=h_1r_2+l_10_R=h_1r_2$$

Analogamente si dimostra che $k_2r_1=h_2r_1$ e posso quindi affermare che $\cdot$ è un'operazione binaria ben definita. Ragionando esattamente come si è visto nella parte precedente della dimostrazione, si dimostra facilmente che $(S,+,(0_R,\bar{0}),\cdot,(0_R,\bar{1}))$ è un anello. Stavolta però si ha che $\mathrm{car}(S)=n$. Infatti, vale che $n(0_R,\bar{1})=(0_R,\bar{n})=(0_R,\bar{0})$ e inoltre, se $k\in\mathbb{N}^*$ è tale che $k(0_R,\bar{1})=(0_R,\bar{0})$, cioè tale che $\bar{k}=\bar{0}$, allora $n\mid k$ e in particolare $n\leq k$. In altre parole, vale che n è il più piccolo intero positivo tale che $n(0_R,\bar{1})=(0_R,\bar{0})$ e quindi, per la proposizione 6.3-(ii), si ottiene che $\mathrm{car}(S)=n$. A questo punto basta semplicemente definire $T:=R\oplus\{\bar{0}\}$ e considerare l'applicazione $f\colon R\to T$ definita da $f(r):=(r,\bar{0})$. È infatti immediato verificare che $T<S$ è un sottoanello e che la mappa f è un isomorfismo di anelli. □

Osservazione 6.17. Si osservi che gli isomorfismi di anelli definiti nel corso della dimostrazione precedente non preservano l'identità rispetto al prodotto. L'isomorfismo dato nella prima costruzione, per esempio, non lo è in virtù del fatto che $f(1_R)=(1_R,0)\neq(0_R,1)$.

Osservazione 6.18. Sia $(S,+,0_S,\cdot)$ un anello e sia $R<S$ un sottoanello.

(i) Se $\mathrm{car}(S)>0$, allora $0<\mathrm{car}(R)\leq\mathrm{car}(S)$.

(ii) Se S è un anello con identità $1_S\neq0_S$ e vale che $1_S\in R$, allora $\mathrm{car}(R)=\mathrm{car}(S)$.

Dimostrazione. Definisco per semplicità $n:=\mathrm{car}(S)$.

(i) Se $n>0$ allora, in virtù della definizione 6.11-(i), vale che $na=0_S$ per ogni $a\in S$. In particolare, essendo $R\subseteq S$, si ha che $na=0_S$ per ogni $a\in R$. Tenendo a mente l'osservazione 6.9, la relazione precedente equivale a richiedere che $\mathrm{car}(R)>0$. Infine, per minimalità della caratteristica, si ha anche la condizione $\mathrm{car}(R)\leq\mathrm{car}(S)$.

(ii) Sotto le ipotesi assegnate, per definizione di elemento neutro, si ha che R è un anello con identità $1_S\neq0_S$. A questo punto basta semplicemente osservare che $\mathrm{car}(R)$ è, per la proposizione 6.3-(ii), il più piccolo $k\in\mathbb{N}^*$ tale che $k1_S=0_S$ perché R ha gli stessi elementi neutri di S e di conseguenza $\mathrm{car}(R)=\mathrm{car}(S)$. □

7 Ideali

Proprio come i sottogruppi normali giocano un ruolo cruciale nella teoria dei gruppi, così gli ideali hanno un ruolo fondamentale nello studio degli anelli.

Definizione 7.1. Sia R un anello. Un sottoanello $I < R$ prende il nome di *ideale sinistro di* R se $r \cdot x \in I$ per ogni $x \in I$, $r \in R$. Similmente, un sottoanello $I < R$ si dice un *ideale destro di* R se $x \cdot r \in I$ per ogni $x \in I$, $r \in R$. Un ideale sinistro e destro viene semplicemente detto un *ideale* (*bilatero*) e si denota $I \lhd R$.

Esempio 7.1. Sia R un anello. I sottoanelli banali $\{0\}$ e R sono ovviamente ideali. Tali ideali sono detti *banali* per distinguerli da tutti gli altri, detti *propri* o *non banali*.

Osservazione 7.1. Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ anelli, $f\colon R \to S$ un omomorfismo. Allora $\operatorname{Ker} f \lhd R$ è un ideale.

Dimostrazione. Siano $x \in \operatorname{Ker} f$, $r \in R$ due elementi fissati. Usando l'ipotesi che f sia un omomorfismo, la definizione 6.10 e la proposizione 6.1-(i), si ottiene la condizione seguente:

$$f(r \cdot x) = f(r) \star f(x) = f(r) \star 0_S = 0_S$$

Questo dimostra che $r \cdot x \in \operatorname{Ker} f$ e quindi, non dipendendo il risultato ottenuto da una particolare scelta degli elementi $x \in \operatorname{Ker} f$, $r \in R$, posso affermare che $\operatorname{Ker} f$ è un ideale sinistro di R. Con un procedimento simile si dimostra che $\operatorname{Ker} f$ è un ideale destro di R e posso dunque concludere che $I \lhd R$ è un ideale. □

Esempio 7.2. Sotto le ipotesi assegnate nell'osservazione 7.1, non è vero in generale che $\operatorname{Im} f \lhd S$ è un ideale, come mostra il seguente controesempio. Si consideri la mappa inclusione $i\colon \mathbb{Z} \to \mathbb{R}$, la quale è un omomorfismo di anelli per quanto si è detto nell'esempio 6.14. È facile verificare che $\operatorname{Im} i = \mathbb{Z}$ e a questo punto si può prendere in esame il seguente controesempio: vale che $1 \in \mathbb{Z}$ e che $\sqrt{2} \in \mathbb{R}$, ma $\sqrt{2} \cdot 1 = \sqrt{2}$ e $\sqrt{2} \notin \mathbb{Z}$, dunque $\mathbb{Z}$ non può essere un ideale sinistro di $\mathbb{R}$.

I risultati che seguono verranno enunciati, per semplicità, solo nel caso degli ideali sinistri, ma valgono con piccoli aggiustamenti anche per gli ideali destri e bilateri.

Osservazione 7.2. Sia R un anello con identità 1 e sia I un ideale sinistro di R. Allora si ha che $I = R$ se e solo se $1 \in I$.

Dimostrazione. L'implicazione diretta è ovvia, per cui basterà dimostrare il viceversa. L'inclusione $I \subseteq R$ deriva banalmente dall'ipotesi che $I < R$ sia un sottoanello. Dato invece $r \in R$, posso utilizzare le ipotesi che I sia un ideale sinistro di R e che $1 \in I$ per poter affermare che $r \in I$ e posso dunque concludere, per doppia inclusione, che $I = R$. □

Osservazione 7.3. Sia R un anello con identità 1 e sia I un ideale sinistro di R con $I \neq \{0\}$. Allora I è un ideale proprio di R, cioè $I \neq R$, se e solo se non possiede elementi invertibili, cioè $u \notin I$ per ogni $u \in U(R)$.

Dimostrazione. Si procede per contrapposizione logica in ambedue le implicazioni. Se esiste un elemento $u \in I$ tale che $u \in U(R)$ allora, usando l'ipotesi che I sia un ideale sinistro di R, posso affermare che $1 \in I$ perché $u^{-1} \cdot u = 1$ con $u^{-1} \in R$ e con $u \in I$. Dall'osservazione 7.2 segue dunque che $I = R$. Viceversa, se $I = R$, allora vale ovviamente che $1 \in I$ e che $1 \in U(R)$. □

Osservazione 7.4. Sia R un anello e sia $\{I_i\}_{i \in I}$ una collezione di ideali sinistri di R. Allora è immediato verificare che $\bigcap_{i \in I} I_i$ è un ideale sinistro di R.

Definizione 7.2. Siano R un anello e sia $X \subseteq R$ un insieme. La seguente intersezione prende il nome di *ideale sinistro generato da* X:

$$(X) := \bigcap_{\substack{I \text{ ideale sinistro} \\ \text{di } R \text{ tale che } X \subseteq I}} I$$

In modo analogo si definiscono l'*ideale destro generato da* X e l'*ideale* (*bilatero*) *generato da* X. Se inoltre $X = \{x_1, \ldots, x_n\}$, si pone per semplicità $(x_1, \ldots, x_n) := (X)$. Infine, un ideale sinistro, destro o bilatero I di R viene detto *finitamente generato* se esistono $x_1, \ldots, x_n \in I$ tali che $I = (x_1, \ldots, x_n)$, prende invece il nome di *ideale principale* se esiste $x \in I$ tale che $I = (x)$.

Osservazione 7.5. Sia R un anello e sia $X \subseteq R$ un insieme. Per la definizione 7.2 e per l'osservazione 7.4 si ha che (X) è il più piccolo ideale sinistro contenente X.

Osservazione 7.6. Sia R un anello con identità 1 e si consideri un elemento $x \in R$. Allora, nel caso degli ideali sinistri, l'ideale principale (x) è dato dalla seguente descrizione esplicita:

$$(x) = \{\, r \cdot x \mid r \in R \,\} \tag{12}$$

Dimostrazione. Sarà sufficiente mostrare la doppia inclusione. Dato $y \in \{\, r \cdot x \mid r \in R \,\}$, esiste $r \in R$ tale che $y = r \cdot x$, ma allora $y \in I$ per ogni ideale sinistro I di R tale che $x \in I$ e dunque, per la definizione 7.2, si ha che $y \in (x)$. Questo dimostra che $\{\, r \cdot x \mid r \in R \,\} \subseteq (x)$. Si noti ora che $\{\, r \cdot x \mid r \in R \,\}$ è un ideale sinistro di R per costruzione e che $x \in \{\, r \cdot x \mid r \in R \,\}$ perché $x = 1 \cdot x$. Dall'osservazione 7.5 segue quindi che $(x) \subseteq \{\, r \cdot x \mid r \in R \,\}$. L'asserto deriva dunque dal doppio contenimento. □

L'osservazione 7.6 si generalizza parecchio facilmente al caso degli ideali sinistri finitamente generati:

$$(x_1, \ldots, x_n) = \{\, r_1 \cdot x_1 + \cdots + r_n \cdot x_n \mid r_1, \ldots, r_n \in R \,\}$$

Osservazione 7.7. Sia R un anello commutativo con identità 1 e si consideri un elemento $x \in R$. Allora, nel caso degli ideali bilateri, l'ideale principale (x) è dato dalla descrizione (12).

Dimostrazione. Noto innanzitutto che, per le osservazioni 7.5, 7.6 e in virtù del fatto che gli ideali bilateri sono ideali sinistri particolari, vale banalmente l'inclusione $\{\, r \cdot x \mid r \in R \,\} \subseteq (x)$. Adesso sarà sufficiente osservare che $\{\, r \cdot x \mid r \in R \,\}$ è un ideale bilatero contenente x per poi applicare l'osservazione 7.5 nel caso degli ideali bilateri. Quanto si vuole dimostrare è in realtà un'ovvia conseguenza del fatto che $r \cdot x = x \cdot r$ per ogni $r \in R$, essendo per ipotesi R un anello commutativo. Di conseguenza, infatti, si ha la condizione:

$$\{\, r \cdot x \mid r \in R \,\} = \{\, x \cdot r \mid r \in R \,\}$$

In particolare, in virtù dell'osservazione 7.6 nel caso degli ideali destri, posso affermare che $\{\, r \cdot x \mid r \in R \,\}$ è anche un ideale destro e di conseguenza, per minimalità (osservazione 7.5), si ha anche il contenimento $(x) \subseteq \{\, r \cdot x \mid r \in R \,\}$. La doppia inclusione mi dà dunque la tesi. □

Osservazione 7.8. Sia R un anello con identità 1. Allora R è un corpo se e solo se R non possiede ideali sinistri propri né ideali destri propri.

Dimostrazione. Assumo che R sia un corpo e che I sia un ideale sinistro di R con $I \neq \{0\}$. Poiché $I \neq \{0\}$, esiste un elemento $x \in I$, $x \neq 0$, ma allora $x \in U(R)$ perché R è un corpo e quindi per l'osservazione 6.6-(i) si ha che $U(R) = R \setminus \{0\}$. Applicando l'osservazione 7.3 per contrapposizione logica si ottiene che $I = R$ e posso dunque concludere, per arbitrarietà nella scelta dell'ideale sinistro I di R con $I \neq \{0\}$, che R non ha ideali sinistri propri. Ragionando allo stesso modo, si dimostra che R non ha ideali destri propri.

Viceversa, suppongo che R non abbia ideali sinistri propri né ideali destri propri e fisso $x \in R$, $x \neq 0$. Essendo l'ideale principale $(x) = \{\, r \cdot x \mid r \in R \,\}$ un ideale sinistro diverso da $\{0\}$ per l'osservazione 7.5 si dovrà avere, per ipotesi, che $(x) = R$. In particolare, deve esistere $r \in R$ tale che $r \cdot x = 1$. Si consideri ora l'ideale principale $(r) = \{\, s \cdot r \mid s \in R \,\}$ e si noti che $(r) = R$ per le stesse ragioni di prima. In particolare, esiste $s \in R$ tale che $s \cdot r = 1$. A questo punto basta soltanto osservare che $s = x$ in virtù della relazione:

$$s = s \cdot 1 = s \cdot (r \cdot x) = (s \cdot r) \cdot x = 1 \cdot x = x$$

Questo dimostra che $x \in U(R)$ e posso dunque concludere, per arbitrarietà nella scelta di $x \in R$, $x \neq 0$, che tutti gli elementi non nulli di R sono invertibili, cioè che R è un corpo. □

Esempio 7.3. Sia R un anello con identità 1 e sia $n \in \mathbb{N}^*$, $n \geq 2$ fissato. Per ogni $1 \leq i \leq n$, si utilizzano le notazioni $A^{(i)}$ e $A_{(i)}$ per indicare, rispettivamente, la i-esima riga e la i-esima colonna della matrice A. Per ogni $1 \leq k \leq n$ posso quindi definire i due seguenti insiemi di matrici:

$$I_k := \{\, A \in \mathrm{M}_n(R) \mid A_{(k)} \neq {}^t(0 \cdots 0),\ A_{(i)} = {}^t(0 \cdots 0) \text{ per ogni } 1 \leq i \leq n \text{ con } i \neq k \,\}$$
$$J_k := \{\, A \in \mathrm{M}_n(R) \mid A^{(k)} \neq (0 \cdots 0),\ A^{(i)} = (0 \cdots 0) \text{ per ogni } 1 \leq i \leq n \text{ con } i \neq k \,\}$$

Utilizzando tecniche di algebra lineare si può facilmente dimostrare che I_k e J_k sono, rispettivamente, un ideale sinistro e un ideale destro di $\mathrm{M}_n(R)$ per ogni $1 \leq k \leq n$. Si può anche osservare che I_k e J_k non sono, rispettivamente, un ideale destro e un ideale sinistro di $\mathrm{M}_n(R)$ per ogni $1 \leq k \leq n$ e per ogni $n \geq 2$. Per dimostrare questa affermazione, basterà esibire un controesempio. Comunque fissati $n \geq 2$, $1 \leq k \leq n$, si considerino le matrici $A, B \in \mathrm{M}_n(R)$, $A = (a_{ij})$, $B = (b_{ij})$ definite da $a_{ij} := 1$ se $j = k$, $a_{ij} := 0$ altrimenti e da $b_{ij} := 1$ se $i = k$, $b_{ij} := 0$ altrimenti. Per costruzione vale che $A \in I_k$, $B \in J_k$ e, se $AB = (c_{ij})$, allora:

$$c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj} = a_{ik} b_{kj} = 1$$

Essendo AB la matrice con tutte le entrate uguali a 1, essa non appartiene né a I_k né a J_k e di conseguenza I_k non può essere un ideale destro di $\mathrm{M}_n(R)$, mentre J_k non può essere un ideale sinistro di $\mathrm{M}_n(R)$.

Esempio 7.4. Sia R un corpo e sia $n \in \mathbb{N}^*$ fissato. Allora $\mathrm{M}_n(R)$ non ha ideali propri. Si consideri infatti un ideale $I \lhd \mathrm{M}_n(R)$, $I \neq \{O\}$. Poiché si assume che $I \neq \{O\}$, deve esistere una matrice $A \in I$, $A = (a_{ij})$ tale che $A \neq \{O\}$, cioè tale che $a_{st} \neq 0$ per opportuni indici $1 \leq s, t \leq n$. Per ogni $1 \leq k, h \leq n$, sia adesso $E_{kh} \in \mathrm{M}_n(R)$, $E_{kh} = (e_{ij})$ la matrice definita da $e_{ij} := 1$ se $i = k$ e $j = h$, $e_{ij} := 0$ altrimenti. Allora, per ogni $1 \leq k \leq n$, usando il fatto che ogni elemento non banale in R è invertibile per la definizione 6.6, si ha:

$$a_{st}^{-1} E_{ks} A E_{tk} = E_{kk}$$

Utilizzando l'assunzione che $I \lhd \mathrm{M}_n(R)$, posso affermare che $E_{kk} \in I$ per ogni $1 \leq k \leq n$. In particolare, si ha che $I_n \in I$ perché $I_n = \sum_{k=1}^{n} E_{kk}$ e posso dunque concludere, per l'osservazione 7.2, che $I = \mathrm{M}_n(R)$. Questo dimostra, appunto, che $\mathrm{M}_n(R)$ non possiede ideali propri.

Esempio 7.5. Siano $n, m \in \mathbb{N}$ fissati e si considerino gli anelli $\mathbb{Z}$ e $\mathbb{Z}_n$. Come accennato nell'esempio 6.1 nel caso di $\mathbb{Z}$, si vede facilmente che $\langle m \rangle < \mathbb{Z}$ e che $\langle \bar{m} \rangle < \mathbb{Z}_n$ sono sottoanelli. Altrettanto facilmente si dimostra che essi sono ideali bilateri. Siano infatti $r \in \mathbb{Z}$, $x \in \langle m \rangle$ due elementi fissati. Per definizione di $\langle m \rangle$ esiste $k \in \mathbb{Z}$ tale che $x = km$, ma allora $rx = rkm$ e dunque $rx \in \langle m \rangle$. Questo dimostra che $\langle m \rangle$ è un ideale sinistro di $\mathbb{Z}$ ma, essendo $\mathbb{Z}$ un anello commutativo, non vi è alcuna distinzione tra ideali destri e sinistri, per cui posso concludere che $\langle m \rangle \lhd \mathbb{Z}$ è un ideale bilatero. Allo stesso modo si può dimostrare che $\langle \bar{m} \rangle \lhd \mathbb{Z}_n$ è un ideale bilatero.

7.1 Teoremi di isomorfismo

I teoremi di isomorfismo per gruppi si estendono a teoremi di isomorfismo per anelli utilizzando gli ideali bilateri anziché i sottogruppi normali. In questa sezione le classi laterali verranno indicate con notazione additiva per evitare di creare confusione con le vecchie definizioni, cioè si preferirà la notazione $a + I$ alla più comune aI.

Proposizione 7.1 (Anello quoziente)**.** *Sia R un anello e sia $I \lhd R$ un ideale. Sia inoltre $\cdot$ l'operazione binaria sul gruppo quoziente R/I definita da $(a + I) \cdot (b + I) := (a \cdot b) + I$. Allora R/I munito dell'usuale operazione additiva $+$ introdotta nell'osservazione 2.2 e dell'operazione moltiplicativa $\cdot$ appena definita è un anello che ha per elemento neutro rispetto alla somma I. Valgono inoltre le due affermazioni seguenti:*

(i) *Se R è un anello commutativo, allora lo è anche R/I.*

(ii) *Se R è un anello con identità 1, allora R/I è un anello con identità $1 + I$.*

Dimostrazione. Poiché per ipotesi R è un anello, in particolare $(R, +, 0)$ è un gruppo abeliano. Da questo si deduce innanzitutto che il gruppo quoziente R/I è ben definito. Si noti infatti che il sottoanello $I < R$ è, in particolare, un sottogruppo di $(R, +, 0)$ e di conseguenza $I \lhd R$ è un sottogruppo normale in quanto tutti i sottogruppi di un gruppo abeliano sono normali (osservazione 2.6). Inoltre, è immediato verificare che R/I è un gruppo abeliano ricorrendo alla definizione 2.1-(i) e all'osservazione 2.9. Adesso mostro che l'operazione binaria $\cdot$ su R/I data nell'enunciato è ben posta. Siano $a + I, a' + I, b + I, b' + I \in R/I$ classi laterali sinistre tali che $a + I = a' + I$, $b + I = b' + I$. In virtù del teorema 2.1-(i) si ha che $a - a' \in I$ e che $b - b' \in I$. Definisco per semplicità $x := a - a'$, $y := b - b'$ dopodiché, applicando la proposizione 6.1-(ii), ottengo la condizione seguente:

$$a \cdot b = (a' + x) \cdot (b' + y) = (a' \cdot b') + (a' \cdot y) + (x \cdot b') + (x \cdot y)$$

Poiché si assume che $I \lhd R$ sia un ideale si ha la condizione $(a' \cdot y) + (x \cdot b') + (x \cdot y) \in I$, dalla quale si deduce che $(a \cdot b) - (a' \cdot b') \in I$. Usando di nuovo il teorema 2.1-(i) si ottiene che $(a \cdot b) + I = (a' \cdot b') + I$ e questo dimostra, per arbitrarietà nella scelta delle classi laterali coinvolte, che l'operazione binaria $\cdot$ su R/I è ben definita. Adesso, l'associatività di tale operazione binaria e le proprietà distributive sinistra e destra rispetto alla somma $+$ derivano immediatamente dalle analoghe proprietà di cui gode l'operazione binaria $\cdot$ su R. Questo dimostra che R/I è un anello come richiesto nell'enunciato. Anche le affermazioni aggiuntive non sono altro che una conseguenza immediata della definizione data dell'operazione binaria $\cdot$ su R/I e delle proprietà di cui gode, per ipotesi, l'operazione binaria $\cdot$ su R. □

Definizione 7.3. Sia R un anello e sia $I \lhd R$ un ideale. L'anello R/I munito dell'operazione additiva $+$ data nell'osservazione 2.2, dell'operazione moltiplicativa $\cdot$ introdotta nella proposizione 7.1 e dell'elemento neutro rispetto alla somma I prende il nome di *anello quoziente di R rispetto a I*.

La definizione 7.3 è ben posta in virtù della proposizione 7.1.

Proposizione 7.2 (Mappa quoziente)**.** *Sia R un anello e sia $I \lhd R$ un ideale. La funzione $\pi\colon R \to R/I$ definita da $\pi(a) := a + I$ è un epimorfismo tale che* $\operatorname{Ker}\pi = I$.

Dimostrazione. Si è già osservato nell'esempio 3.5 che π è un omomorfismo di gruppi suriettivo. Si osservi che, per come si è definita l'operazione $\cdot$ su R/I nella proposizione 7.1, vale per ogni $a, b \in R$ la relazione:

$$\pi(a \cdot b) = (a \cdot b) + I = (a + I) \cdot (b + I) = \pi(a) \cdot \pi(b)$$

Questo dimostra che π è un omomorfismo di anelli. A questo punto, bisogna solo calcolare il nucleo di π:

$$\begin{aligned} \operatorname{Ker}\pi &= \{\, a \in R \mid \pi(a) = I \,\} \\ &= \{\, a \in R \mid a + I = I \,\} \\ &= \{\, a \in R \mid a \in I \,\} = I \end{aligned}$$

□

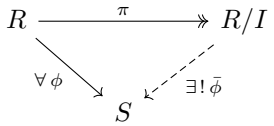
Definizione 7.4. Sia R un anello e sia $I \lhd R$ un ideale. L'epimorfismo $\pi\colon R \to R/I$ dato dalla condizione $\pi(a) := a + I$ si dice la *mappa quoziente* (oppure la *proiezione canonica*, o anche l'*epimorfismo canonico*).

La definizione 7.4 è ben posta in virtù della proposizione 7.2.

Proposizione 7.3 (Proprietà universale dei quozienti per anelli)**.** *Siano $(R, +, 0_R, \cdot)$, $(S, +, 0_S, \star)$ due anelli, $I \lhd R$ un ideale. Allora la mappa quoziente $\pi\colon R \to R/I$ soddisfa la seguente proprietà universale:*

$$\forall\, \phi\colon R \to S \text{ omomorfismo, con } I \subseteq \operatorname{Ker}\phi \;\; \exists!\, \bar{\phi}\colon R/I \to S \text{ omomorfismo} \mid \bar{\phi} \circ \pi = \phi$$

Equivalentemente, il seguente diagramma di omomorfismi è commutativo:



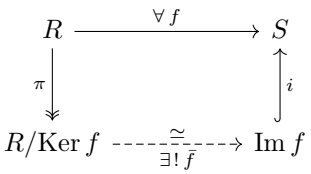
Dimostrazione. Sia $\phi\colon R \to S$ un omomorfismo. Per la proprietà universale dei quozienti per gruppi, cioè per la proposizione 3.2-(ii), esiste un unico omomorfismo di gruppi $\bar{\phi}\colon R/I \to S$ tale che $\bar{\phi} \circ \pi = \phi$. Dalla dimostrazione di quel risultato segue inoltre che $\bar{\phi}$ è l'applicazione definita da $\bar{\phi}(a + I) := \phi(a)$. Basterà dunque dimostrare che $\bar{\phi}$ è un omomorfismo di anelli. Questo però deriva immediatamente dalla relazione seguente la quale, per come si è definita l'operazione binaria $\cdot$ su R/I nella proposizione 7.1 e per l'ipotesi che ϕ sia un omomorfismo di anelli, è valida per qualunque scelta di due classi laterali $a + I, b + I \in R/I$:

$$\bar{\phi}\big((a + I) \cdot (b + I)\big) = \bar{\phi}\big((a \cdot b) + I\big) = \phi(a \cdot b) = \phi(a) \star \phi(b) = \bar{\phi}(a + I) \star \bar{\phi}(b + I)$$

□

Teorema 7.1 (di fattorizzazione degli omomorfismi)**.** *Siano R e S anelli, si considerino un omomorfismo $f\colon R \to S$, la mappa quoziente $\pi\colon R \to R/\operatorname{Ker} f$, la mappa inclusione $i\colon \operatorname{Im} f \to S$. Allora esiste un unico*

isomorfismo $\bar{f}\colon R/\operatorname{Ker} f \to \operatorname{Im} f$ *che verifichi la condizione* $i \circ \bar{f} \circ \pi = f$ *oppure, equivalentemente, esiste una fattorizzazione unica tale che il seguente diagramma di omomorfismi sia commutativo:*



Dimostrazione. Per il teorema di fattorizzazione degli omomorfismi di gruppi, cioè il teorema 3.1, esiste un unico isomorfismo di gruppi $\bar{f}\colon R/\operatorname{Ker} f \to \operatorname{Im} f$ tale che $i \circ \bar{f} \circ \pi = f$. Basterà dunque mostrare che $\bar{f}$ è un omomorfismo di anelli. Si ricordi che la costruzione di $\bar{f}$ realizzata nel corso della dimostrazione del teorema 3.1 prevedeva di applicare le proprietà universali delle inclusioni e dei quozienti. Di conseguenza, ripetendo passo dopo passo la stessa costruzione ma utilizzando le analoghe proprietà universali per anelli, fornite dalle proposizioni 6.2 e 7.3, si ottiene che $\bar{f}$ è un omomorfismo di anelli. □

Proprio come nel caso degli omomorfismi di gruppi, dal teorema di fattorizzazione degli omomorfismi deriva immediatamente il seguente risultato.

Corollario 7.1 (Primo Teorema di Isomorfismo)**.** *Siano* R *e* S *anelli e sia* $f\colon R \to S$ *un omomorfismo. Allora vale la condizione* $R/\operatorname{Ker} f \simeq \operatorname{Im} f$*.*

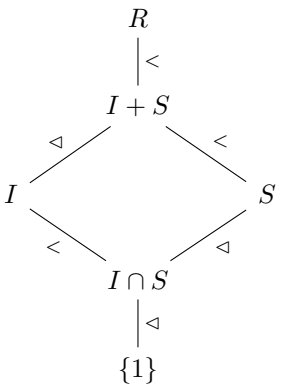
Teorema 7.2 (dell'ideale e del sottoanello, del diamante o Secondo Teorema di Isomorfismo)**.** *Siano* R *un anello,* $S < R$ *un sottoanello e sia* $I \lhd R$ *un ideale. Allora valgono le seguenti affermazioni.*

(i) $I + S = S + I$*,* $I + S < R$ *è un sottoanello e* $I \lhd I + S$ *è un ideale.*

(ii) $I \cap S \lhd S$ *è un ideale.*

(iii) *L'applicazione* $\Phi\colon S/(I \cap S) \to (I + S)/I$ *definita da* $\Phi(a + (I \cap S)) := a + I$ *è un isomorfismo.*

In particolare, si ha la condizione $S/(I \cap S) \simeq (I + S)/I$*.*



Dimostrazione.

(i) Innanzitutto, in virtù del teorema 3.2-(i) è noto che $I + S = S + I$, $I + S < R$ è un sottogruppo e $I \lhd I + S$ è un sottogruppo normale. Per dimostrare che $I + S < R$ è un sottoanello, considero elementi $r_1, r_2 \in I + S$. Ricordo la definizione dell'operazione binaria $+$ su $\mathcal{P}(R)\setminus\{\varnothing\}$ introdotta nell'osservazione 2.2, per cui esistono $x_1, x_2 \in I$, $s_1, s_2 \in S$ tali che $r_1 = x_1 + s_1$, $r_2 = x_2 + s_2$. In virtù della proposizione 6.1-(ii), si ha la condizione seguente:

$$r_1 \cdot r_2 = (x_1 + s_1) \cdot (x_2 + s_2) = (x_1 \cdot x_2) + (x_1 \cdot s_2) + (s_1 \cdot x_2) + (s_1 \cdot s_2)$$

Poiché per ipotesi $I, S < R$ sono sottoanelli essi sono, in particolare, sottoinsiemi chiusi rispetto all'operazione binaria $\cdot$ su R e di conseguenza $x_1 \cdot x_2 \in I$, mentre $s_1 \cdot s_2 \in S$. Dato che per ipotesi $I \lhd R$ è un ideale bilatero, si ha che $x_1 \cdot s_2, s_1 \cdot x_2 \in I$. In particolare, tutti questi sono elementi

di $I + S$, ma quest'ultimo è un sottogruppo per il teorema 3.2-(i) e quindi dovrà contenerne anche la somma perché è un sottoinsieme chiuso rispetto all'operazione binaria $+$ su R. Ho dimostrato che $r_1 \cdot r_2 \in I + S$ e questo mi permette di concludere, per arbitrarietà nella scelta degli elementi $r_1, r_2 \in I + S$, che $I + S < R$ è un sottoanello in quanto trattasi di un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su R.

Si osservi ora che $I < I + S$ è banalmente un sottoanello perché si assume per ipotesi che $I < R$ sia un sottoanello e dunque la chiusura rispetto all'operazione binaria $\cdot$ ristretta agli elementi di $I + S$ discende banalmente dalla chiusura rispetto all'operazione $\cdot$ su R. Siano adesso $r \in I + S$, $x \in I$ elementi fissati. Come prima, esistono $y \in I$, $s \in S$ tali che $r = y + s$ e quindi, applicando la proprietà distributiva destra di $\cdot$ rispetto a $+$ valida in virtù dell'ipotesi che R sia un anello, ricavo la condizione seguente:

$$r \cdot x = (y + s) \cdot x = (y \cdot x) + (s \cdot x)$$

Poiché si assume che $I \lhd R$ sia un ideale, vale che $y \cdot x, s \cdot x \in I$ e dunque anche la somma di tali elementi appartiene a I. In altre parole, si ottiene la condizione $r \cdot x \in I$. Applicando la proprietà distributiva sinistra di $\cdot$ rispetto a $+$ e ripercorrendo un ragionamento analogo si ottiene anche la condizione $x \cdot r \in I$ e posso dunque affermare, per arbitrarietà nella scelta degli elementi $r \in R$, $x \in I$, che $I \lhd I + S$ è un ideale.

(ii) Per il teorema 3.2-(ii), è noto che $I \cap S \lhd S$ è un sottogruppo normale. La chiusura di $I \cap S \subseteq S$ rispetto all'operazione binaria $\cdot$ su R ristretta agli elementi di S discende banalmente dalle ipotesi che $I, S < R$ siano sottoanelli e, in particolare, sottoinsiemi chiusi rispetto all'operazione binaria $\cdot$ su R. Posso dunque affermare che $I \cap S < S$ è un sottoanello. Siano adesso $r \in S$, $x \in I \cap S$ due elementi prefissati. Allora $r \cdot x, x \cdot r \in S$ in quanto $S \subseteq R$ è chiuso rispetto all'operazione binaria $\cdot$ su R, mentre $r \cdot x, x \cdot r \in I$ perché per ipotesi $I \lhd R$ è un ideale bilatero. Ma allora tali elementi appartengono a $I \cap S$ e posso dunque concludere, per arbitrarietà nella scelta di $r \in S$, $x \in I \cap S$, che $I \cap S \lhd S$ è un ideale.

(iii) Innanzitutto, per i punti (i) e (ii) già dimostrati, i due anelli quoziente $S/(I \cap S)$ e $(I + S)/I$ sono ben definiti. Per il teorema 3.2-(iii), l'applicazione Φ assegnata nell'enunciato è un isomorfismo di gruppi. Sarà quindi sufficiente mostrare che è anche un omomorfismo di anelli. Per farlo, fisso due classi laterali $x + (I \cap S), y + (I \cap S) \in S/(I \cap S)$ e osservo che, per come si è definita l'operazione binaria $\cdot$ su un anello quoziente nella proposizione 7.1, vale la condizione seguente:

$$\begin{aligned}\Phi\big((x + (I \cap S)) \cdot (y + (I \cap S))\big) &= \Phi\big((x \cdot y) + (I \cap S)\big) \\ &= (x \cdot y) + I \\ &= (x + I) \cdot (y + I) \\ &= \Phi\big(x + (I \cap S)\big) \cdot \Phi\big(y + (I \cap S)\big)\end{aligned}$$

Non dipendendo il risultato ottenuto dalla scelta degli elementi coinvolti, posso concludere che Φ è un isomorfismo di anelli. La parte finale dell'enunciato è una conseguenza immediata di quanto si è già dimostrato. □

Teorema 7.3 (di corrispondenza). *Siano $(R, +, 0, \cdot)$, $(\bar{R}, +, \bar{0}, \star)$ due anelli, $f\colon R \to \bar{R}$ un epimorfismo. Pongo inoltre $\mathcal{R} := \{$ Sottoanelli di R contenenti $\operatorname{Ker} f \}$, $\bar{\mathcal{R}} := \{$ Sottoanelli di $\bar{R} \}$. Allora f induce una corrispondenza biunivoca $\Phi\colon \mathcal{R} \to \bar{\mathcal{R}}$ definita da $\Phi(S) := f(S)$, la cui inversa è l'applicazione $\Psi\colon \bar{\mathcal{R}} \to \mathcal{R}$ definita da $\Psi(\bar{S}) := f^{-1}(\bar{S})$. Valgono inoltre le due seguenti affermazioni.*

(a) *Siano $S, S' \in \mathcal{R}$ due sottoanelli e siano $\bar{S} := f(S)$, $\bar{S}' := f(S')$. Allora si ha che $S \subseteq S'$ se e solo se vale che $\bar{S} \subseteq \bar{S}'$. In altre parole, la corrispondenza biunivoca preserva le inclusioni.*

(b) *Sia $S \in \mathcal{R}$ un sottoanello e sia $\bar{S} := f(S)$. Allora $S \lhd R$ è un ideale se e solo se vale che $\bar{S} \lhd \bar{R}$ è un ideale, cioè la corrispondenza biunivoca preserva gli ideali. Ora si assuma che tali condizioni equivalenti siano soddisfatte e si considerino le due mappe quoziente $\pi\colon R \to R/S$, $\bar{\pi}\colon \bar{R} \to \bar{R}/\bar{S}$. Allora l'applicazione $\tilde{f}\colon R/S \to \bar{R}/\bar{S}$ definita da $\tilde{f}(x + S) := f(x) + \bar{S}$ è l'unico isomorfismo tale*

che $\tilde{f} \circ \pi = \bar{\pi} \circ f$*. Equivalentemente, si ha il seguente diagramma di omomorfismi commutativo:*

$$\begin{array}{ccc} R & \xrightarrow{\forall\, f} & \bar{R} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\bar{\pi}} \\ R/S & \xrightarrow[\exists!\, \tilde{f}]{\simeq} & \bar{R}/\bar{S} \end{array}$$

Dimostrazione. Se $\mathcal{G} := \{\,\text{Sottogruppi di } (R, +, 0) \text{ contenenti Ker } f\,\}$ e $\bar{\mathcal{G}} := \{\,\text{Sottogruppi di } (\bar{R}, +, \bar{0})\,\}$ allora f induce, per il teorema di corrispondenza, vale a dire il teorema 3.3, una corrispondenza biunivoca $\Phi\colon \mathcal{G} \to \bar{\mathcal{G}}$ definita da $\Phi(H) := f(H)$ la cui inversa è l'applicazione $\Psi\colon \bar{\mathcal{G}} \to \mathcal{G}$ data da $\Psi(\bar{H}) := f^{-1}(\bar{H})$. Dimostro che Φ si restringe a una corrispondenza biunivoca tra $\mathcal{R}$ e $\bar{\mathcal{R}}$. Sia dunque $S \in \mathcal{R}$ un sottoanello e sia $\bar{S} := f(S)$. Per il teorema di corrispondenza è noto che $(\bar{S}, +, \bar{0})$ è un sottogruppo di $(\bar{R}, +, \bar{0})$, per cui basterà dimostrare che $\bar{S} \subseteq \bar{R}$ è un sottoinsieme chiuso rispetto all'operazione binaria $\star$ su $\bar{R}$. Comunque fissati $y_1, y_2 \in \bar{S}$, per definizione di immagine esistono $x_1, x_2 \in S$ tali che $f(x_1) = y_1$, $f(x_2) = y_2$. Usando quindi l'ipotesi che f sia un omomorfismo di anelli, si ottiene con estrema facilità la condizione seguente:

$$y_1 \star y_2 = f(x_1) \star f(x_2) = f(x_1 \cdot x_2)$$

Essendo $S < R$ un sottoanello, esso è in particolare un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su R e quindi $x_1 \cdot x_2 \in S$, ma allora dalla condizione precedente deduco che $y_1 \star y_2 \in \bar{S}$ e questo dimostra, per arbitrarietà nella scelta degli elementi $y_1, y_2 \in \bar{S}$, che $\bar{S} < \bar{R}$ è un sottoanello in quanto sottoinsieme chiuso rispetto all'operazione binaria $\star$ su $\bar{R}$. Si consideri adesso un sottoanello $\bar{S} \in \bar{\mathcal{R}}$ e sia $S := f^{-1}(\bar{S})$. Come prima, è noto per il teorema di corrispondenza di gruppi che $(S, +, 0)$ è un sottogruppo di $(R, +, 0)$ e che Ker $f \subseteq S$ e quindi sarà sufficiente mostrare che $S \subseteq R$ è chiuso rispetto all'operazione binaria $\cdot$ su R. Fissati $x_1, x_2 \in S$, per definizione di preimmagine esistono $y_1, y_2 \in \bar{S}$ tali che $f(x_1) = y_1$, $f(x_2) = y_2$. Utilizzando proprio come prima l'ipotesi che f sia un omomorfismo di anelli, si trova la relazione seguente:

$$f(x_1 \cdot x_2) = f(x_1) \star f(x_2) = y_1 \star y_2$$

Dato che $\bar{S} < \bar{R}$ è un sottoanello, quindi un sottoinsieme chiuso rispetto all'operazione binaria $\star$ su $\bar{R}$, si può affermare che $y_1 \star y_2 \in \bar{S}$. Dalla relazione precedente si deduce allora che $x_1 \cdot x_2 \in S$ e posso dunque concludere, per arbitrarietà nella scelta di $x_1, x_2 \in S$, che $S < R$ è un sottoanello in quanto sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su R. La discussione precedente esaurisce quindi quanto richiesto nella prima parte nell'enunciato. L'asserzione (a) deriva immediatamente dal teorema di corrispondenza per gruppi, per cui basterà dimostrare l'affermazione (b).

(b) Suppongo che $S \lhd R$ sia un ideale e dimostro che lo è anche $\bar{S} \lhd \bar{R}$. Siano dunque $x \in \bar{R}$, $y \in \bar{S}$ due elementi fissati. Usando il fatto che $\bar{R} = f(R)$, $\bar{S} = f(S)$ posso affermare che esistono $r \in R$, $s \in S$ tali che $f(r) = x$, $f(s) = y$. Poiché si assume che f sia un omomorfismo di anelli, si ha che:

$$x \star y = f(r) \star f(s) = f(r \cdot s)$$

Ora, essendo per ipotesi $S \lhd R$ un ideale, si ha che $r \cdot s \in S$, ma allora dalla relazione precedente si ricava che $x \star y \in \bar{S}$. Con un procedimento analogo si dimostra che anche $y \star x \in \bar{S}$ e posso quindi affermare, per arbitrarietà nella scelta degli elementi $x \in \bar{R}$, $y \in \bar{S}$, che $\bar{S} \lhd \bar{R}$ è un ideale bilatero. Viceversa, assumo che $\bar{S} \lhd \bar{R}$ sia un ideale e dimostro che anche $S \lhd R$ è un ideale. Fisso dunque due elementi $r \in R$, $s \in S$. Definisco $x := f(r)$, $y := f(s)$ cosicché si abbia che $r \in \bar{R}$, $s \in \bar{S}$ e noto che, per l'ipotesi che f sia un omomorfismo di anelli, vale la condizione seguente:

$$f(r \cdot s) = f(r) \star f(s) = x \star y$$

Dato che per ipotesi $\bar{S} \lhd \bar{R}$ è un ideale, vale che $x \star y \in \bar{S}$ e posso quindi affermare, in virtù della relazione precedente, che $r \cdot s \in S$. Analogamente si dimostra che $s \cdot r \in S$ e questo mi permette di concludere che $S \lhd R$ è un ideale.

Avendo dimostrato che la corrispondenza biunivoca preserva gli ideali, posso assumere che $S \lhd R$ oppure, equivalentemente, che $\bar{S} \lhd \bar{R}$ sia un ideale. In particolare, siccome $(R, +, 0)$ è un gruppo

abeliano per l'ipotesi che R sia un anello, ogni suo sottogruppo è normale per l'osservazione 2.6 e in particolare $(S, +, 0)$ è un suo sottogruppo normale. Questo tuttavia comporta, per il teorema di corrispondenza per gruppi, che $(\bar{S}, +, \bar{0})$ è un sottogruppo normale di $(\bar{R}, +, \bar{0})$ e che la funzione $\tilde{f}$ definita nell'enunciato è l'unico isomorfismo di gruppi tale che $\tilde{f} \circ \pi = \bar{\pi} \circ f$. Per concludere la dimostrazione, basterà dimostrare che $\tilde{f}$ è un omomorfismo di anelli, ma questo segue facilmente dalla definizione dell'operazione binaria $\cdot$ su un anello quoziente data nella proposizione 7.1. Dati infatti $x + S, y + S \in R/S$, per l'ipotesi che f sia un omomorfismo di anelli si ricava la condizione:

$$\begin{aligned}\tilde{f}\big((x+S)\cdot(y+S)\big) &= \tilde{f}\big((x\cdot y)+S\big)\\ &= f(x\cdot y)+\bar{S}\\ &= \big(f(x)\star f(y)\big)+\bar{S}\\ &= \big(f(x)+S\big)\cdot\big(f(y)+S\big)\\ &= \tilde{f}(x+S)\cdot\tilde{f}(y+S)\end{aligned}$$ □

Come nel caso dei gruppi, il risultato che segue deriva immediatamente dal teorema di corrispondenza.

Osservazione 7.9. Siano R un anello, $I \lhd R$ un ideale e sia $\pi\colon R \to R/I$ la mappa quoziente. Siano inoltre $\mathcal{R} := \{\,\text{Sottoanelli di } R \text{ contenenti } I\,\}$ e $\bar{\mathcal{R}} := \{\,\text{Sottoanelli di } R/I\,\}$. Allora π induce una corrispondenza biunivoca $\Phi\colon \mathcal{R} \to \bar{\mathcal{R}}$ definita dalla relazione $\Phi(S) := \pi(S)$. Inoltre, si ha che $\pi(S) = S/I$ per ogni $S \in \mathcal{R}$. Questo significa che i sottoanelli di R/I sono tutti e soli della forma S/I con $S \in \mathcal{R}$.

Dimostrazione. Ovviamente, la prima parte dell'enunciato segue dal teorema di corrispondenza applicato alla mappa quoziente $\pi\colon R \to R/I$ la quale, per la proposizione 7.2, è un epimorfismo con $\operatorname{Ker}\pi = I$. Ora osservo che, per ogni $S \in \mathcal{R}$, l'anello quoziente S/I è ben definito in quanto $I \lhd S$ è un ideale. Questo però deriva facilmente dal fatto che $S < R$ è un sottoanello e che $I \lhd R$ è un ideale. Per ottenere la tesi basta dunque osservare che vale, per ogni $S \in \mathcal{R}$, la condizione seguente:

$$\pi(S) = \{\,\pi(a) \mid a \in S\,\} = \{\,a + I \mid a \in S\,\} = S/I$$ □

Corollario 7.2 (Terzo Teorema di Isomorfismo)**.** *Sia R un anello e siano $I, J \lhd R$ ideali tali che $I \subseteq J$. Allora $J/I \lhd R/I$ è un ideale e vale la condizione $(R/I)/(J/I) \simeq R/J$.*

Dimostrazione. Siano $\mathcal{R} := \{\,\text{Sottoanelli di } R \text{ contenenti } I\,\}$, $\bar{\mathcal{R}} := \{\,\text{Sottoanelli di } R/I\,\}$ e si consideri la mappa quoziente $\pi\colon R \to R/I$. In virtù dell'osservazione 7.9, tale applicazione induce una corrispondenza biunivoca $\Phi\colon \mathcal{R} \to \bar{\mathcal{R}}$ data da $\Phi(S) := \pi(S)$ e inoltre $\pi(S) = S/I$ per ogni $S \in \mathcal{R}$. Per la proposizione 7.2, la mappa quoziente è un epimorfismo e posso dunque usare l'asserzione (b) del teorema di corrispondenza per affermare che $J/I \lhd R/I$ è un ideale. In virtù dello stesso risultato con $R := R$, $S := J$, $\bar{R} := R/I$ e con $\bar{S} := J/I$ posso concludere che $(R/I)/(J/I) \simeq R/J$. □

7.2 Ideali primi e massimali

Proposizione 7.4. *Sia R un anello. Siano $+$ e $\cdot$ le operazioni binarie su $\mathcal{P}(R)\setminus\{\varnothing\}$ date dalle relazioni:*

$$A + B := \{\,a + b \mid a \in A,\, b \in B\,\},\quad A \cdot B := \left\{ \sum_{i\in I}(a_i \cdot b_i) \;\middle|\; \{a_i\}_{i\in I} \subseteq A,\, \{b_i\}_{i\in I} \subseteq B,\, |I| < +\infty \right\}$$

Le operazioni binarie appena definite godono delle seguenti proprietà:

(i) *Soddisfano la proprietà associativa, cioè $(A + B) + C = A + (B + C)$ e $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ per ogni $A, B, C \in \mathcal{P}(R)\setminus\{\varnothing\}$.*

(ii) *Valgono le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$, cioè soddisfano le due relazioni $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$ e $(A + B) \cdot C = (A \cdot C) + (B \cdot C)$ per ogni $A, B, C \in \mathcal{P}(R)\setminus\{\varnothing\}$.*

(iii) *Siano $A, B \in \mathcal{P}(R)\setminus\{\varnothing\}$ prefissati. Se $A, B \lhd R$ sono ideali, allora $A + B, A \cdot B \lhd R$ sono ideali.*

Dimostrazione. Le affermazioni (i) e (ii) derivano immediatamente dal fatto che R è un anello, per cui R possiede operazioni binarie $+$ e $\cdot$ associative e gode delle proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$. Sarà dunque sufficiente dimostrare la terza asserzione per poter concludere la dimostrazione.

(iii) Innanzitutto, bisogna mostrare che $(A+B,+,0)$ è un sottogruppo di $(R,+,0)$. Comunque fissati due elementi $x_1, x_2 \in A+B$, per come si è definita l'operazione binaria $+$ su $\mathcal{P}(R)\setminus\{\varnothing\}$ esistono $a_1, a_2 \in A$, $b_1, b_2 \in B$ tali che $x_1 = a_1 + b_1$, $x_2 = a_2 + b_2$. Ora, dato che per ipotesi R è un anello, si ha che $(R,+,0)$ è un gruppo abeliano e in virtù di questo fatto si ottiene la condizione seguente:

$$x_1 + x_2 = (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2)$$

Poiché per ipotesi $A, B < R$ sono sottoanelli, essi sono in particolare chiusi rispetto all'operazione binaria $+$ su R e di conseguenza $a_1 + a_2 \in A$, $b_1 + b_2 \in B$. Dalla condizione precedente si deduce quindi che $x_1 + x_2 \in A+B$ e questo dimostra, per arbitrarietà nella scelta di $x_1, x_2 \in A+B$, che $A+B \subseteq R$ è un sottoinsieme chiuso rispetto all'operazione binaria $+$ su R. Si noti ora che $0 \in A$ e $0 \in B$ perché si assume che $A, B < R$ siano sottoanelli, quindi $0 \in A+B$ essendo $0 = 0+0$ per definizione di elemento neutro. Infine, fissato $x \in A+B$, esistono $a \in A$, $b \in B$ tali che $x = a+b$. Dall'ipotesi che $A, B < R$ siano sottoanelli segue in particolare che $(A,+,0)$ e $(B,+,0)$ sono due sottogruppi di $(R,+,0)$ e di conseguenza $-a \in A$, $-b \in B$. Ma allora si ottiene che $-x \in A+B$ perché $-x = -b - a$ per la proposizione 1.1-(iii) e vale che $-b - a = -a - b$ essendo $(R,+,0)$ un gruppo abeliano. Posso dunque concludere, per arbitrarietà nella scelta dell'elemento $x \in A+B$, che $(A+B,+,0)$ è un sottogruppo di $(R,+,0)$. Sia ora fissato $r \in R$. Per le proprietà distributive sinistra e destra di $\cdot$ rispetto a $+$ valide per l'ipotesi che R sia un anello, si ha la relazione seguente:

$$r \cdot x = r \cdot (a+b) = (r \cdot a) + (r \cdot b)$$
$$x \cdot r = (a+b) \cdot r = (a \cdot r) + (b \cdot r)$$

Dall'assunzione che $A, B \lhd R$ siano ideali segue che $r \cdot a, a \cdot r \in A$, $r \cdot b, b \cdot r \in B$ e posso dunque affermare che $r \cdot x, x \cdot r \in A+B$. Questo dimostra, nel caso particolare in cui si ha $r \in A+B$, che $A+B \subseteq R$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su R, quindi $A+B < R$ è un sottoanello. Nel caso generale in cui $r \in R$, invece, le relazioni ottenute mi consentono di affermare che $A+B \lhd R$ è un ideale.

A questo punto, bisogna ripetere l'intero procedimento per dimostrare che anche $A \cdot B \lhd R$ è un ideale. Innanzitutto, va dimostrato che $(A \cdot B,+,0)$ è un sottogruppo di $(R,+,0)$. Fissati quindi due elementi $x, x' \in A \cdot B$, per come si è definita l'operazione binaria $\cdot$ su $\mathcal{P}(R)\setminus\{\varnothing\}$ esistono due insiemi di indici I, J con $|I|, |J| < +\infty$ e collezioni $\{a_i\}_{i\in I}, \{a'_j\}_{j\in J} \subseteq A$, $\{b_i\}_{i\in I}, \{b'_j\}_{j\in J} \subseteq B$ tali che $x = \sum_{i\in I}(a_i \cdot b_i)$, $x' = \sum_{j\in J}(a'_j \cdot b'_j)$. Dato che $|I| + |J| < +\infty$, l'elemento $x + x'$ appartiene ad $A \cdot B$ per costruzione e posso quindi affermare, per arbitrarietà nella scelta di $x, x' \in A \cdot B$, che $A \cdot B \subseteq R$ è un sottoinsieme chiuso rispetto all'operazione binaria $+$ su R. Naturalmente, poi, si ha che $0 \in A \cdot B$ perché $0 \in A$, $0 \in B$ essendo per ipotesi $A, B < R$ sottoanelli e $0 = 0 \cdot 0$ in virtù della proposizione 6.1-(i). Sia infine fissato $x \in A \cdot B$. Come prima, esistono un insieme di indici I con $|I| < +\infty$ e due collezioni $\{a_i\}_{i\in I} \subseteq A$, $\{b_i\}_{i\in I} \subseteq B$ tali che $x = \sum_{i\in I}(a_i \cdot b_i)$. Si osservi che, per la proprietà distributiva generalizzata (proposizione 6.1-(ii)) e per la proposizione 6.1-(iii), si ha la condizione seguente:

$$-x = -\sum_{i\in I}(a_i \cdot b_i) = \sum_{i\in I}\big(-(a_i \cdot b_i)\big) = \sum_{i\in I}\big((-a_i) \cdot b_i\big)$$

Poiché per ipotesi $A < R$ è un sottoanello, vale in particolare che $\{-a_i\}_{i\in I} \subseteq A$ e di conseguenza $-x \in A \cdot B$ in virtù della relazione precedente. Dato che il risultato ottenuto non dipende da una particolare scelta dell'elemento $x \in A \cdot B$, si può concludere che $(A \cdot B,+,0)$ è un sottogruppo di $(R,+,0)$. Sia ora $r \in R$. Ancora per la proprietà distributiva generalizzata si hanno le relazioni:

$$r \cdot x = r \cdot \sum_{i\in I}(a_i \cdot b_i) = \sum_{i\in I}\big(r \cdot (a_i \cdot b_i)\big) = \sum_{i\in I}\big((r \cdot a_i) \cdot b_i\big)$$
$$x \cdot r = \left(\sum_{i\in I}(a_i \cdot b_i)\right) \cdot r = \sum_{i\in I}\big((a_i \cdot b_i) \cdot r\big) = \sum_{i\in I}\big(a_i \cdot (b_i \cdot r)\big)$$

Dalle ipotesi che $A, B \lhd R$ siano ideali segue che $\{r \cdot a_i\}_{i\in I} \subseteq A$, $\{b_i \cdot r\}_{i\in I} \subseteq B$ e si può dunque affermare, grazie alle relazioni precedenti, che $r \cdot x, x \cdot r \in A \cdot B$. Questo dimostra, se si sceglie in particolare $r \in A \cdot B$, che $A \cdot B \subseteq R$ è un sottoinsieme chiuso rispetto all'operazione binaria $\cdot$ su R e di conseguenza ottengo che $A \cdot B < R$ è un sottoanello. Prendendo in generale $r \in R$, invece, si ottiene che $A \cdot B \lhd R$ è un ideale e questo conclude la dimostrazione. □

Osservazione 7.10. Sia R un anello. Si noti che l'operazione binaria $+$ su $\mathcal{P}(R)\setminus\{\varnothing\}$ data nell'enunciato della proposizione 7.4 coincide con quella introdotta nell'osservazione 2.2. Di conseguenza, è noto in virtù della suddetta osservazione che $(\mathcal{P}(R)\setminus\{\varnothing\}, +, \{0\})$ è un monoide.

Osservazione 7.11. Sia R un anello con identità 1. Allora vale la condizione $R^2 = R$.

Dimostrazione. Si osservi, innanzitutto, che l'inclusione $R^2 \subseteq R$ deriva banalmente dal fatto che R è un anello, per cui $+$ e $\cdot$ sono operazioni binarie su R. L'inclusione $R \subseteq R^2$ segue invece dall'ipotesi che R sia un anello con identità 1, per cui ciascun elemento $r \in R$ si può esprimere come $r = r \cdot 1$. Queste semplici considerazioni mi danno la tesi. □

Osservazione 7.12. Sia R un anello e siano $A, B, P \lhd R$ ideali. Se $A \subseteq P$ oppure $B \subseteq P$, allora $A \cdot B \subseteq P$.

Dimostrazione. Dimostro il risultato solo nel caso in cui $A \subseteq P$, perché nel caso speculare in cui $B \subseteq P$ si ragiona esattamente allo stesso modo. Sia $x \in A \cdot B$ un elemento prefissato. Per come è stata definita l'operazione binaria $\cdot$ su $\mathcal{P}(R)\setminus\{\varnothing\}$ nella proposizione 7.4, esistono un insieme di indici I con $|I| < +\infty$ e due collezioni $\{a_i\}_{i\in I} \subseteq A$, $\{b_i\}_{i\in I} \subseteq B$ tali che $x = \sum_{i\in I}(a_i \cdot b_i)$. Poiché per ipotesi $A \subseteq P$ e $P \lhd R$ è un ideale, posso affermare che $a_i \cdot b_i \in P$ per ogni $i \in I$, ma allora anche $x \in P$ in quanto $P \subseteq R$ è chiuso rispetto all'operazione binaria $+$ su R. Per arbitrarietà nella scelta di $x \in A \cdot B$ si ha la tesi. □

Definizione 7.5. Sia R un anello.

(i) Un ideale $P \lhd R$ viene detto *primo* se $P \neq R$ e se, comunque vengano fissati due ideali $A, B \lhd R$ tali che $A \cdot B \subseteq P$, vale che $A \subseteq P$ oppure $B \subseteq P$.

(ii) Un ideale $M \lhd R$ viene detto *massimale* se $M \neq R$ e se, comunque venga fissato un ideale $I \lhd R$ tale che $M \subseteq I$, vale che $I = M$ oppure $I = R$.

L'importanza di queste classi di ideali risiede nel fatto che i rispettivi quozienti possono essere domini o corpi, come verrà meglio specificato nelle successive proposizioni grazie anche alla seguente definizione.

Definizione 7.6. Sia R un anello con identità $1 \neq 0$.

(i) Un ideale $P \lhd R$ si dice *fortemente primo* se l'anello quoziente R/P è un dominio e se $R/P \neq \{P\}$.

(ii) Un ideale $M \lhd R$ viene detto *fortemente massimale* se l'anello R/M è un corpo e se $R/M \neq \{M\}$.

Osservazione 7.13. Una conseguenza banale della definizione 7.6 e dell'osservazione 6.5 è che ogni ideale fortemente massimale è anche un ideale fortemente primo.

Proposizione 7.5 (Caratterizzazione degli ideali primi attraverso il quoziente)**.** *Siano R un anello con identità $1 \neq 0$, $P \lhd R$ un ideale. Valgono le seguenti affermazioni.*

(i) *Si ha che P è un ideale fortemente primo se e solo se $P \neq R$ e, comunque vengano fissati $a, b \in R$ tali che $a \cdot b \in P$, vale che $a \in P$ oppure $b \in P$.*

(ii) *Se P è un ideale fortemente primo, allora P è primo.*

(iii) *Se P è un ideale primo e R è un anello commutativo, allora P è fortemente primo.*

Dimostrazione.

(i) Per la definizione 7.6-(i), dire che P è un ideale fortemente primo significa che l'anello quoziente R/P è un dominio e che $R/P \neq \{P\}$. La condizione $R/P \neq \{P\}$ equivale banalmente a richiedere che $P \neq R$. D'altra parte, per la definizione 6.6 si ha che R/P è un dominio se e solo se R/P non possiede divisori dello zero sinistri o destri non banali e questo è equivalente a dire, ragionando per contrapposizione logica dalla definizione 6.2, che comunque fissate due classi $a + P, b + P \in R/P$ tali che $(a + P) \cdot (b + P) = P$, cioè $(a \cdot b) + P = P$, vale alternativamente che $a + P = P$ oppure che $b + P = P$. Quanto si è appena detto equivale tuttavia a richiedere, per il teorema 2.1-(i), che comunque vengano fissati $a, b \in R$ tali che $a \cdot b \in P$ vale che $a \in P$ oppure $b \in P$. Quanto volevasi dimostrare segue dunque dalla catena di doppie implicazioni.

(ii) Dal momento che per ipotesi $P \lhd R$ è un ideale fortemente primo, si ha la condizione $P \neq R$ per il punto (i) appena dimostrato. Siano dunque $A, B \lhd R$ due ideali prefissati tali che $A \cdot B \subseteq P$ e si osservi che, se $A \subseteq P$, allora $P \lhd R$ è banalmente un ideale primo in virtù della definizione 7.5-(i). Assumo quindi $A \nsubseteq P$ e dimostro che $B \subseteq P$. Siccome $A \nsubseteq P$, esiste un elemento $a \in A$ tale che $a \notin P$. Tuttavia, per come si sono scelti gli ideali $A, B \lhd R$, comunque fissato un elemento $b \in R$ si ha che $a \cdot b \in P$. Adesso, dato che per ipotesi $P \lhd R$ è un ideale fortemente primo, si può usare l'equivalenza fornita dal punto (i) appena dimostrato in virtù della quale, essendo $a \notin P$, si dovrà avere che $b \in P$. Posso quindi affermare, per arbitrarietà nella scelta dell'elemento $b \in B$, che vale l'inclusione $B \subseteq P$ e questo mi permette di concludere che $P \lhd R$ è un ideale primo.

(iii) Innanzitutto, poiché per ipotesi $P \lhd R$ è un ideale primo, si ha che $P \neq R$ per definizione. Siano adesso $a, b \in R$ elementi fissati tali che $a \cdot b \in P$. L'obiettivo è dimostrare che $a \in P$ oppure $b \in P$ per poi applicare il punto (i) già dimostrato. Si osservi che, per come è stata definita l'operazione binaria $\cdot$ su $\mathcal{P}(R) \setminus \{\varnothing\}$ nella proposizione 7.4, per le osservazioni 7.7 e 7.11, per l'ipotesi che R sia un anello commutativo e in virtù della proprietà distributiva generalizzata (proposizione 6.1-(ii)), vale la condizione seguente:

$$\begin{aligned}
(a) \cdot (b) &= \left\{ \sum_{i \in I} (x_i \cdot y_i) \;\middle|\; \{x_i\}_{i \in I} \subseteq (a),\, \{y_i\}_{i \in I} \subseteq (b),\, |I| < +\infty \right\} \\
&= \left\{ \sum_{i \in I} \big((r_i \cdot a) \cdot (s_i \cdot b)\big) \;\middle|\; \{r_i\}_{i \in I}, \{s_i\}_{i \in I} \subseteq R,\, |I| < +\infty \right\} \\
&= \left\{ \sum_{i \in I} \big((r_i \cdot s_i) \cdot (a \cdot b)\big) \;\middle|\; \{r_i\}_{i \in I}, \{s_i\}_{i \in I} \subseteq R,\, |I| < +\infty \right\} \\
&= \left\{ \left(\sum_{i \in I} (r_i \cdot s_i) \right) \cdot (a \cdot b) \;\middle|\; \{r_i\}_{i \in I}, \{s_i\}_{i \in I} \subseteq R,\, |I| < +\infty \right\} \\
&= \{\, r \cdot (a \cdot b) \mid r \in R \,\} = (a \cdot b)
\end{aligned}$$

Adesso, usando il fatto che $a \cdot b \in P$, l'ipotesi che $P \lhd R$ sia un ideale bilatero e l'osservazione 7.5, posso affermare che $(a \cdot b) \subseteq P$. In vista della condizione precedente, ciò equivale a richiedere che $(a) \cdot (b) \subseteq P$ ma allora si ottiene, in virtù dell'ipotesi che $P \lhd R$ sia un ideale primo, che $(a) \subseteq P$ oppure $(b) \subseteq P$. In particolare, si dovrà avere che $a \in P$ oppure che $b \in P$ e questo dimostra, per arbitrarietà nella scelta degli elementi $a, b \in R$ con $a \cdot b \in P$ e in virtù del punto (i) già dimostrato, che $P \lhd R$ è un ideale fortemente primo. □

Proposizione 7.6 (Caratterizzazione degli ideali massimali tramite il quoziente)**.** *Siano R un anello con identità $1 \neq 0$, $M \lhd R$ un ideale. Valgono le seguenti affermazioni.*

(i) *Si ha che M è un ideale fortemente massimale se e solo se $M \neq R$ e, comunque sia fissato $a \in R$ con $a \notin M$, esiste un elemento $b \in R$ tale che $(a \cdot b) - 1, (b \cdot a) - 1 \in M$.*

(ii) *Se M è un ideale fortemente massimale, allora M è massimale.*

(iii) *Se M è un ideale massimale e R è un anello commutativo, allora M è fortemente massimale.*

Dimostrazione.

(i) Si ricordi che, per la definizione 7.6-(ii), dire che $M \lhd R$ è un ideale fortemente massimale significa che l'anello quoziente R/M è un corpo e inoltre $R/M \neq \{M\}$. Ovviamente, è del tutto equivalente richiedere che $R/M \neq \{M\}$ oppure che $M \neq R$. Adesso ricordo che, in virtù della definizione 6.6, se R/M è un corpo allora ogni suo elemento non banale è invertibile. Equivalentemente, per ogni $a + M \in R/M$ con $a + M \neq M$ esiste, in virtù dell'osservazione 6.3 e della proposizione 7.1, una classe laterale $b + M \in R/M$ tale che $(a \cdot b) + M = 1 + M$ e $(b \cdot a) + M = 1 + M$. In altre parole, per il teorema 2.1-(i), comunque venga fissato $a \in R$ con $a \notin M$, esiste un elemento $b \in R$ tale che $(a \cdot b) - 1 \in M$ e $(b \cdot a) - 1 \in M$. La catena di doppie implicazioni appena costruita mi dà la tesi.

(ii) Si noti innanzitutto che, per il punto (i) appena dimostrato e per l'ipotesi che $M \lhd R$ sia un ideale fortemente massimale, vale che $M \neq R$. Sia ora $I \lhd R$ un ideale tale che $M \subseteq I$. Se $I = M$, allora

$M \lhd R$ è banalmente un ideale massimale, perciò assumo $I \neq M$ e dimostro che $I = R$. Dato che $I \neq M$, deve esistere un elemento $a \in I$ tale che $a \notin M$. Di nuovo per il punto (i) già dimostrato, posso affermare che esiste $b \in R$ tale che $(a \cdot b) - 1 \in M$. Equivalentemente, esiste $m \in M$ tale che $1 = (a \cdot b) - m$ ma da questo si deduce che $1 \in I$ in quanto $a, m \in I$, $b \in R$ e $I \lhd R$ è un ideale. In particolare, vale che $I = R$ in virtù dell'osservazione 7.2 e posso dunque concludere che $M \lhd R$ è un ideale massimale.

(iii) Per l'ipotesi che $M \lhd R$ sia un ideale massimale, si ha che $M \neq R$. In particolare, posso scegliere $a \in R$ tale che $a \notin M$. Per il punto (i) appena dimostrato e in virtù dell'ipotesi che R sia un anello commutativo, sarà sufficiente trovare un elemento $b \in R$ tale che $(a \cdot b) - 1 \in M$. A tale scopo, si consideri l'insieme $M + (a)$. Per la proposizione 7.4, si tratta di un ideale in quanto somma di due ideali e per costruzione $M \subseteq M + (a)$. Vale inoltre che $M + (a) \neq M$ perché $a \in M + (a)$ mentre $a \notin M$. Siccome $M \lhd R$ è un ideale massimale, dovrà valere che $M + (a) = R$ e in particolare si ha che $1 \in M + (a)$. Per la definizione data dell'operazione binaria $+$ su $\mathcal{P}(R) \setminus \{\varnothing\}$, esistono due elementi $m \in M$, $b \in R$ tali che $1 = m + (a \cdot b)$. Di conseguenza, si ottiene che $(a \cdot b) - 1 \in M$ e si può dunque concludere, per arbitrarietà nella scelta dell'elemento $a \in R$ con $a \notin M$, che $M \lhd R$ è un ideale fortemente massimale. □

Proposizione 7.7. *Siano R un anello con $R^2 = R$, $M \lhd R$ un ideale massimale. Allora $M \lhd R$ è primo.*

Dimostrazione. Si osservi che la condizione $M \neq R$ è automaticamente verificata per l'ipotesi che $M \lhd R$ sia un ideale massimale. Adesso si procede per contrapposizione logica: si vuole dimostrare che, dati due ideali $A, B \lhd R$ tali che $A \nsubseteq M$ e $B \nsubseteq M$, vale che $A \cdot B \nsubseteq M$. Si osservi che, se $A \nsubseteq M$ e $B \nsubseteq M$, allora $M \subseteq A + M$ e $M \subseteq B + M$, ma $A + M \neq M$ e $B + M \neq M$. Poiché si assume che $M \lhd R$ sia un ideale massimale, si dovrà avere che $A + M = R$ e $B + M = R$. Di conseguenza, dall'ipotesi che $R^2 = R$ e dalla proposizione 7.4-(ii) deriva immediatamente la condizione seguente:

$$R = R^2 = (A + M) \cdot (B + M) = (A \cdot B) + (A \cdot M) + (M \cdot B) + (M \cdot M)$$

Dato che per ipotesi $M \lhd R$ è un ideale, per come sono definite le operazioni binarie $+$ e $\cdot$ su $\mathcal{P}(R) \setminus \{\varnothing\}$, vale banalmente l'inclusione $(A \cdot M) + (M \cdot B) + (M \cdot M) \subseteq M$ e quindi $R \subseteq (A \cdot B) + M$. Ora, se fosse $A \cdot B \subseteq M$, allora varrebbe che $R \subseteq M$ e di conseguenza $R = M$, ma questo è assurdo. L'unica possibilità accettabile, dunque, è che $A \cdot B \nsubseteq M$ e questo mi permette di concludere, per contrapposizione logica, che $M \lhd R$ è un ideale primo. □

Esempio 7.6. Le proposizioni 7.5-(iii) e 7.6-(iii) sono in generale false se non si assume l'ipotesi che R sia un anello commutativo, come mostra il seguente controesempio. Considero, per un certo $n \in \mathbb{N}$ con $n \geq 2$ e per un qualche corpo R, l'anello $\mathrm{M}_n(R)$ con l'ideale banale $\{O\}$. Quanto si è osservato negli esempi 6.5 e 7.1 implica che $\mathrm{M}_n(R)$ è un anello con identità $I_n \neq O$, mentre $\{O\} \lhd \mathrm{M}_n(R)$ è un ideale banale. Le altre ipotesi delle proposizioni 7.5 e 7.6 sono dunque verificate. Ora, poiché si assume che R sia un corpo posso affermare, in vista dell'esempio 7.4, che $\mathrm{M}_n(R)$ non ha ideali propri e quindi $\{O\} \lhd \mathrm{M}_n(R)$ è banalmente un ideale massimale. Per l'osservazione 7.11 sono verificate le ipotesi della proposizione 7.7, in virtù della quale $\{O\} \lhd \mathrm{M}_n(R)$ è anche un ideale primo. Ciononostante l'anello quoziente $\mathrm{M}_n(R)/\{O\}$, banalmente isomorfo a $\mathrm{M}_n(R)$, non è un dominio. La matrice $A \in \mathrm{M}_n(R)$, $A = (a_{ij})$ data da $a_{ij} := 1$ se $i = 1$ e $j = n$, $a_{ij} := 0$ altrimenti, è infatti una matrice nilpotente di ordine 2 e quindi $A + \{O\}$ è un divisore dello zero non banale in $\mathrm{M}_n(R)/\{O\}$. Posso quindi affermare che $\mathrm{M}_n(R)/\{O\}$ non è un dominio e in particolare, per l'osservazione 6.5, non è neanche un corpo. Questo dimostra che $\{O\} \lhd \mathrm{M}_n(R)$ non è un ideale fortemente primo e dunque, in virtù dell'osservazione 7.13, non è neppure fortemente massimale.

Esempio 7.7. In generale, la proposizione 7.7 è falsa se non si assume l'ipotesi che $R^2 = R$, come mostra il seguente controesempio. In questo contesto, denoto $n\mathbb{Z} := \langle n \rangle$ per una maggiore chiarezza e considero l'anello $2\mathbb{Z}$. Da quanto si è detto nell'esempio 7.5 segue in particolare che $4\mathbb{Z} \lhd 2\mathbb{Z}$ è un ideale. In questo caso, l'ipotesi che $R^2 = R$ non è verificata. Infatti, ricordando che $\mathbb{Z}$ è un anello con identità per quanto si

è discusso nell'esempio 6.1 e applicando l'osservazione 7.11, si ottiene la condizione seguente:

$$\begin{aligned} 2\mathbb{Z}\cdot 2\mathbb{Z} &= \left\{ \sum_{i\in I}(2n_i)(2m_i) \;\middle|\; \{n_i\}_{i\in I},\{m_i\}_{i\in I}\subseteq\mathbb{Z},\, |I|<+\infty \right\} \\ &= \left\{ 4\sum_{i\in I} n_i m_i \;\middle|\; \{n_i\}_{i\in I},\{m_i\}_{i\in I}\subseteq\mathbb{Z},\, |I|<+\infty \right\} \\ &= \{\, 4k \mid k\in\mathbb{Z}\,\} = 4\mathbb{Z} \end{aligned}$$

Dalla relazione precedente segue inoltre che $4\mathbb{Z}\lhd 2\mathbb{Z}$ non è un ideale primo, perché $2\mathbb{Z}\lhd 2\mathbb{Z}$ è banalmente un ideale, vale che $2\mathbb{Z}\cdot 2\mathbb{Z}\subseteq 4\mathbb{Z}$ ma non è vero che $2\mathbb{Z}\subseteq 4\mathbb{Z}$. Adesso sarà sufficiente mostrare che $4\mathbb{Z}\lhd 2\mathbb{Z}$ è un ideale massimale. Dimostro, innanzitutto, che ogni ideale di $\mathbb{Z}$ è un ideale principale vale a dire, per l'osservazione 7.7, un ideale della forma $n\mathbb{Z}$ per qualche $n\in\mathbb{N}$. Sia dunque $I\lhd\mathbb{Z}$ un ideale prefissato. Se $I=\{0\}$, allora $I=(0)$ banalmente in virtù della già citata osservazione 7.7. Assumo quindi $I\neq\{0\}$, per cui esiste un certo $m\in I$ con $m\neq 0$. Posso assumere senza perdita di generalità che $m>0$ in quanto, se fosse $m<0$, allora potrei considerare $-m$ al posto di m perché $I\lhd\mathbb{Z}$ è un ideale e quindi, in particolare, è un sottoanello. Posso dunque definire $n:=\min\{\,k\in I\mid k>0\,\}$ essendo tale insieme non vuoto. Noto che l'inclusione $(n)\subseteq I$ discende immediatamente dall'osservazione 7.5. Sia ora $x\in I$ un elemento prefissato. Se $x=0$, allora $x\in(n)$ poiché $x=0n$ per la proposizione 6.1-(i). Se invece $x\neq 0$ allora, per l'algoritmo euclideo della divisione, esistono $q,r\in\mathbb{Z}$ con $0\leq r<n$ tali che $x=nq+r$. Equivalentemente, si ha che $r=x-nq$, ma allora $r\in I$ in quanto $x,n\in I$ e $I\lhd\mathbb{Z}$ è un ideale. Ricordando che n è definito come il più piccolo intero positivo appartenente ad I e che $0\leq r<n$, si dovrà necessariamente avere che $r=0$ e da questo segue che $x\in(n)$ essendo $x=nq$. Posso dunque affermare, per arbitrarietà nella scelta di $x\in I$, che $I\subseteq(n)$, quindi $I=(n)$ per doppia inclusione. Non dipendendo il risultato ottenuto da una particolare scelta dell'ideale $I\lhd\mathbb{Z}$, posso concludere che ogni ideale di $\mathbb{Z}$ è un ideale principale.

A questo punto, per dimostrare che $4\mathbb{Z}\lhd 2\mathbb{Z}$ è un ideale massimale, bisognerà utilizzare il fatto noto[27] che, per ogni $a,b\in\mathbb{Z}$, vale il contenimento $b\mathbb{Z}\subseteq a\mathbb{Z}$ se e solo se $a\mid b$. Sia $I\lhd 2\mathbb{Z}$ un ideale tale che $4\mathbb{Z}\subseteq I$. Naturalmente, varrà in particolare che $I\lhd\mathbb{Z}$ è un ideale e dunque, in vista della discussione precedente, deve esistere $n\in\mathbb{N}$ tale che $I=n\mathbb{Z}$. Per il fatto noto prima menzionato, essendo $n\mathbb{Z}\subseteq 2\mathbb{Z}$ e $4\mathbb{Z}\subseteq n\mathbb{Z}$, si dovrà avere che $2\mid n$ e che $n\mid 4$. Sotto tali condizioni, le uniche possibilità ammesse sono $n=2$ e $n=4$. In altre parole, si dovrà avere che $I=2\mathbb{Z}$ oppure $I=4\mathbb{Z}$ e posso dunque concludere, per arbitrarietà nella scelta dell'ideale $I\lhd 2\mathbb{Z}$ con $4\mathbb{Z}\subseteq I$, che $4\mathbb{Z}\lhd 2\mathbb{Z}$ è un ideale massimale.

7.3 Tre assiomi equivalenti nella teoria degli insiemi

Per dimostrare la successiva proposizione si usa il lemma di Zorn, vale a dire un assioma nella teoria degli insiemi equivalente all'assioma della scelta e al teorema del buon ordinamento. Si può dimostrare che non è possibile derivare il lemma di Zorn da altri assiomi e di conseguenza si possono avere teorie degli insiemi che includono il lemma di Zorn e altre che lo escludono.

Definizione 7.7. Sia X un insieme non vuoto e sia $\mathcal{C}$ una collezione di sottoinsiemi di X. Una collezione $\mathcal{F}$ di elementi di $\mathcal{C}$ tale che valga $A\subseteq B$ oppure $B\subseteq A$ per ogni $A,B\in\mathcal{F}$ prende il nome di *catena in* $\mathcal{C}$.

Osservazione 7.14. Siano X un insieme non vuoto, $\mathcal{C}$ una collezione di sottoinsiemi di S e sia $\mathcal{F}=\{A_i\}_{i\in I}$ una catena in C. Dato che per la definizione 7.7 tutti gli elementi di $\mathcal{F}$ sono confrontabili, si può sempre supporre che siano contenuti gli uni negli altri. Si possono considerare, per esempio, le seguenti possibilità:

$$\begin{aligned} &\mathcal{F}=\{\,A_1\subseteq A_2\subseteq\cdots\subseteq A_{n-1}\subseteq A_n\,\} && \text{se } |I|=n \text{ con } n\in\mathbb{N}^* \\ &\mathcal{F}=\{\,A_1\subseteq A_2\subseteq\cdots\,\} && \text{se } |I|=|\mathbb{N}| \\ &\mathcal{F}=\{\,A_i\subseteq A_j \mid i,j\in\mathbb{R} \text{ con } i\leq j\,\} && \text{se } |I|=|\mathbb{R}| \end{aligned}$$

Definizione 7.8. Sia X un insieme non vuoto e sia $\mathcal{C}$ una collezione di sottoinsiemi di X.

(i) Un elemento $M\in X$ tale che $A\subseteq M$ per ogni $A\in\mathcal{C}$ viene detto un *maggiorante per* $\mathcal{C}$.

(ii) Un elemento $M\in\mathcal{C}$ tale che M sia un maggiorante per $\mathcal{C}$ viene detto un *massimo di* $\mathcal{C}$.

[27] Per una dimostrazione di questo risultato, si rimanda agli appunti del corso AL110.

(iii) Un elemento $M \in \mathcal{C}$ tale che, comunque venga fissato un elemento $A \in \mathcal{C}$ con $M \subseteq A$, si abbia che $A = M$ viene detto un *elemento massimale di* $\mathcal{C}$.

Si possono definire in maniera speculare un *minorante per* $\mathcal{C}$, un *minimo di* $\mathcal{C}$, un *elemento minimale di* $\mathcal{C}$.

Osservazione 7.15. Siano X un insieme non vuoto, $\mathcal{C}$ una collezione di sottoinsiemi di X e sia $M \in \mathcal{C}$ un massimo di $\mathcal{C}$. Una facile conseguenza della definizione 7.8 è che M è sia un maggiorante che un elemento massimale di $\mathcal{C}$.

Osservazione 7.16. Siano X un insieme non vuoto, $\mathcal{C}$ una collezione di sottoinsiemi di X e sia $M \in \mathcal{C}$ un massimo di $\mathcal{C}$. Allora M è l'unico massimo di $\mathcal{C}$.

Dimostrazione. Sia $N \in \mathcal{C}$ un massimo di $\mathcal{C}$ possibilmente diverso da M. Dalla definizione 7.8 segue che N è un maggiorante per $\mathcal{C}$ e quindi dovrà valere che $A \subseteq N$ per ogni $A \in \mathcal{C}$. In particolare, si ottiene che $M \subseteq N$ perché $M \in \mathcal{C}$. Similmente, poiché per ipotesi M è un massimo di $\mathcal{C}$, si deve avere che $N \subseteq M$. Dato che l'inclusione è una relazione d'ordine parziale e in particolare una relazione antisimmetrica, posso concludere che $N = M$ e questo dimostra, per arbitrarietà nella scelta del massimo $N \in \mathcal{C}$, che M è l'unico massimo di $\mathcal{C}$. □

Esempio 7.8. Sia X un insieme non vuoto e sia $\mathcal{C}$ una collezione di sottoinsiemi di X. Diversamente da quanto accade per il massimo, non è vero in generale che esistono un unico maggiorante per $\mathcal{C}$ e un unico elemento massimale di $\mathcal{C}$, come mostra il seguente controesempio. Pongo $X := \{a, b, c\}$ e $\mathcal{C} := \{\{a\}, \{b\}\}$. Allora $\{a, b\}$ e X sono maggioranti distinti per $\mathcal{C}$, mentre $\{a\}$ e $\{b\}$ sono due elementi massimali distinti per $\mathcal{C}$. Si noti inoltre che non vi sono altri maggioranti o elementi massimali e dunque, venendo a mancare la condizione necessaria espressa dall'osservazione 7.15, si deduce che $\mathcal{C}$ non ammette massimo, quindi il massimo non sempre esiste.

Osservazione 7.17. Siano X un insieme non vuoto, $\mathcal{C}$ una collezione di sottoinsiemi di S, $\mathcal{F}$ una catena in $\mathcal{C}$ e sia $M \in \mathcal{F}$ un elemento massimale di $\mathcal{F}$. Allora M è il massimo di $\mathcal{F}$.

Dimostrazione. Sia $A \in \mathcal{F}$ un elemento fissato. Dato che per ipotesi $\mathcal{F}$ è una catena, dalla definizione 7.7 segue che $A \subseteq M$ oppure $M \subseteq A$. Se $M \subseteq A$ allora, utilizzando l'ipotesi che M sia un elemento massimale di $\mathcal{F}$, si ottiene che $M = A$. Dal momento che l'inclusione è una relazione d'ordine parziale e in particolare una relazione riflessiva, dovrà valere che $A \subseteq M$. Questo dimostra, per arbitrarietà nella scelta di $A \in \mathcal{F}$, che M è il massimo di $\mathcal{F}$. □

Osservazione 7.18. Nell'enunciato dell'osservazione 7.17, l'ipotesi che $\mathcal{F}$ sia una catena non può essere in alcun modo indebolita. Se non si fa questa assunzione, infatti, un controesempio è dato dall'esempio 7.8, nel quale viene esibito un caso particolare in cui sono presenti due elementi massimali distinti ma non un massimo. Naturalmente, non vi è alcuna contraddizione con l'osservazione 7.17 appena dimostrata perché nell'esempio sopra citato $\mathcal{C}$ non è una catena.

Nel caso particolare in cui si considera una collezione di sottoinsiemi di un insieme ambiente assegnato, dunque, l'enunciato del lemma di Zorn è il seguente:

"Sia X un insieme non vuoto e sia $\mathcal{C}$ una collezione di sottoinsiemi di X.
Se ogni catena in $\mathcal{C}$ ammette un maggiorante, allora $\mathcal{C}$ ammette un elemento massimale."

Esiste tuttavia una formulazione più generale del lemma di Zorn. Si ricordi che una relazione binaria su un insieme non vuoto è detta una *relazione d'ordine parziale* (o più semplicemente una *relazione d'ordine*) se gode delle proprietà riflessiva, simmetrica e transitiva. Inoltre, la coppia costituita da un insieme e da una relazione d'ordine su di esso viene detta un *insieme parzialmente ordinato*. Le definizioni e i risultati precedenti, enunciati e dimostrati nel caso particolare in cui la relazione d'ordine è quella di inclusione, si generalizzano con estrema facilità al caso di relazioni d'ordine qualsiasi. Di fatto, i risultati ottenuti con le relative dimostrazioni non dipendono in alcun modo dalla relazione d'ordine scelta.

Assioma 1 (Lemma di Zorn)**.** Sia $(X, \leq)$ un insieme parzialmente ordinato. Se ogni catena in X ammette un maggiorante, allora X possiede un elemento massimale.

Come si è già anticipato, il lemma di Zorn è equivalente ad altri due assiomi nella teoria degli insiemi, cioè l'assioma della scelta e il teorema del buon ordinamento, noto anche come il teorema di Zermelo. Tali assiomi vengono di seguito enunciati, ma la loro equivalenza non verrà dimostrata. Ricordo che, dato un insieme X, una relazione d'ordine $\leq$ su X si dice *totale* se vale che $a \leq b$ oppure $b \leq a$ per ogni $a, b \in X$.

Assioma 2 (della scelta)**.** Sia $\{X_i\}_{i \in I}$ una collezione, possibilmente infinita, di insiemi non vuoti. Allora il prodotto cartesiano $\prod_{i \in I} X_i$ è non vuoto, cioè è possibile scegliere un elemento $x_i \in X_i$ per ogni $i \in I$.

Assioma 3 (Teorema del buon ordinamento)**.** Sia X un insieme non vuoto. Allora X ammette un buon ordinamento, vale a dire che esiste una relazione d'ordine $\leq$ tale che U ammetta minimo per ogni $U \subseteq X$.

Osservazione 7.19. Sia X un insieme non vuoto. Se $\leq$ è un buon ordinamento su X, allora è anche una relazione d'ordine totale su X. Se infatti $a, b \in X$ sono due elementi fissati allora, per definizione di buon ordinamento l'insieme $\{a, b\} \subseteq X$ deve ammettere minimo. In particolare, dovrà valere che $a \leq b$ oppure che $b \leq a$ e questo mi permette di concludere, per arbitrarietà nella scelta degli elementi $a, b \in X$, che $\leq$ è una relazione d'ordine totale su X.

Un risultato che si può dimostrare grazie all'assioma della scelta è il paradosso di Banach-Tarski, cioè il celebre risultato del "raddoppiamento della sfera" con cui si afferma che è possibile prendere una sfera nello spazio tridimensionale, suddividerla in un numero finito di pezzi non misurabili e, usando solo rotazioni e traslazioni, riassemblare i pezzi in modo da ottenere due sfere dello stesso raggio dell'originale.

Questi assiomi equivalenti permettono di dimostrare risultati importanti in diverse aree della matematica:

- In algebra lineare, l'esistenza di una base per ogni spazio vettoriale, anche di dimensione infinita.
- In topologia, il teorema di Tychonoff, in virtù del quale il prodotto di una collezione anche infinita di spazi topologici compatti è compatto.
- In teoria dei campi, il fatto che ogni campo possiede una chiusura algebrica, cioè che ogni campo è essenzialmente un sottoanello di un campo algebricamente chiuso.
- In teoria degli anelli, l'esistenza di ideali massimali.

Proposizione 7.8 (Esistenza di ideali massimali)**.** *Sia R un anello con identità $1 \neq 0$ e sia $A \lhd R$, $A \neq R$ un ideale. Allora esiste un ideale massimale $M \lhd R$ tale che $A \subseteq M$. In particolare R ammette un ideale massimale.*

Dimostrazione. Chiaramente, una volta dimostrata la prima parte dell'enunciato, la seconda parte deriva banalmente dalla precedente prendendo $I := \{0\}$. Per dimostrare la prima parte, si usa il lemma di Zorn. Definisco $\mathcal{X} := \{\, I \lhd R \text{ ideale} \mid A \subseteq I,\ I \neq R \,\}$ e noto, innanzitutto, che $\mathcal{X}$ è non vuoto in quanto $A \in \mathcal{X}$. Si consideri la relazione d'ordine parziale su $\mathcal{X}$ data semplicemente dall'inclusione, cosicché $(\mathcal{X}, \subseteq)$ sia un insieme parzialmente ordinato. Sia adesso $\mathcal{F}$ una catena in $\mathcal{X}$ e sia $F := \bigcup_{I \in \mathcal{F}} I$. L'obiettivo è dimostrare che F è un maggiorante per $\mathcal{F}$. Vale ovviamente, per costruzione, che $I \subseteq F$ per ogni $I \in \mathcal{F}$. Sarà quindi sufficiente mostrare che $F \in \mathcal{X}$. Per costruzione, si ha che $A \subseteq F$. Siano adesso $a, b \in F$ elementi fissati. Per come si è definito F, esistono $I, J \in \mathcal{F}$ tali che $a \in I$, $b \in J$. Tuttavia, poiché si assume che $\mathcal{F}$ sia una catena in $\mathcal{X}$, dovrà valere che $I \subseteq J$ oppure $J \subseteq I$. Assumo che $I \subseteq J$, mentre l'altro caso si tratta con un procedimento identico. Da questa supposizione segue che $a, b \in J$ ma, essendo $J \lhd R$ un ideale in quanto elemento di $\mathcal{X}$, si può affermare che $a + b, a \cdot b \in J$. In particolare, si ottiene che $a + b, a \cdot b \in F$ e questo dimostra, per arbitrarietà nella scelta degli elementi $a, b \in F$, che $F \subseteq R$ è un sottoinsieme chiuso rispetto alle operazioni binarie $+$ e $\cdot$ su R. Ora osservo che $0 \in F$ perché, per un qualsiasi $I \in \mathcal{F}$, si ha che $I \lhd R$ è un ideale e di conseguenza $0 \in I$. Infine, assegnato un elemento $a \in F$, per costruzione esiste $I \in \mathcal{F}$ tale che $a \in I$. Come prima, utilizzando il fatto che $I \lhd R$ è un ideale, posso affermare anche che $-a \in I$ e in particolare $-a \in F$. Non dipendendo il risultato ottenuto da una particolare scelta dell'elemento $a \in F$, si può affermare che $F < R$ è un sottoanello. Siano infine $r \in R$, $a \in F$ due elementi fissati. Ragionando

esattamente come prima, esiste $I \in \mathcal{F}$ tale che $a \in I$, ma $I \lhd R$ è un ideale e quindi $r \cdot a, a \cdot r \in I$. Ricavo dunque che $r \cdot a, a \cdot r \in F$ e questo dimostra, per arbitrarietà nella scelta degli elementi $r \in R$, $a \in F$, che $F \lhd R$ è un ideale. Osservo infine che, per ogni $I \in \mathcal{F}$, si ha che $1 \notin I$ in quanto, se così non fosse, allora dall'osservazione 7.2 seguirebbe che $I = R$, contraddicendo la definizione di $\mathcal{X}$. Ottengo quindi che $1 \notin F$ ma questo è equivalente a richiedere, per contrapposizione logica dall'osservazione 7.2, che $F \neq R$. Posso dunque affermare che $F \in \mathcal{X}$ e di conseguenza F è un maggiorante per $\mathcal{F}$. Poiché il risultato ottenuto non dipende da una particolare scelta della catena $\mathcal{F}$ in $\mathcal{X}$ posso applicare il lemma di Zorn, in virtù del quale esiste un elemento massimale $M \in \mathcal{X}$. Per definizione di $\mathcal{X}$ si ha che $M \lhd R$ è un ideale tale che $A \subseteq M$ e $M \neq R$. A questo punto, dato un ideale $I \lhd R$ tale che $M \subseteq I$, in particolare anche $A \subseteq I$ e quindi, se $I \neq R$, allora $I \in \mathcal{X}$. Essendo tuttavia M un elemento massimale di $\mathcal{X}$, si dovrà avere che $I = M$. Posso dunque concludere che $M \lhd R$ è un ideale massimale e quindi si ha la tesi. □

Esempio 7.9. La proposizione 7.8 diventa falsa se non si assume l'ipotesi che R sia un anello con identità, come mostra il seguente controesempio. Si consideri il gruppo $\mathbb{Q}$ munito dell'operazione additiva $+$ usuale. Sia inoltre p un numero primo. Si dimostra facilmente, ricordando la definizione 5.6-(iii) e procedendo per doppia inclusione, che vale la relazione seguente:

$$(\mathbb{Q}/\mathbb{Z})(p) = \left\{ \frac{a}{p^k}\mathbb{Z} \in \mathbb{Q}/\mathbb{Z} \;\middle|\; a \in \mathbb{Z}\,,\ k \in \mathbb{N} \right\}$$

Si noti infatti che, per ogni $a \in \mathbb{Z}$, $k \in \mathbb{N}$, vale che $p^k \frac{a}{p^k}\mathbb{Z} = a\mathbb{Z}$ e ovviamente $a\mathbb{Z} = \mathbb{Z}$ per il teorema 2.1-(i) e in virtù del fatto che $a - 1 \in \mathbb{Z}$. Viceversa, fisso $a, b \in \mathbb{Z}$ con $\mathrm{MCD}(a, b) = 1$ senza perdita di generalità e suppongo che esista $k \in \mathbb{N}$ tale che $p^k \frac{a}{b}\mathbb{Z} = \mathbb{Z}$ cioè, come si è appena visto, tale che $p^k \frac{a}{b}\mathbb{Z} = a\mathbb{Z}$. Ancora per il teorema 2.1-(i), è necessario che valga $p^k \frac{a}{b} - a \in \mathbb{Z}$ oppure, in altre parole, che si abbia $\frac{a(p^k - b)}{b} \in \mathbb{Z}$, cioè che $b \mid a(p^k - b)$. Dal lemma di Euclide (si veda la nota 18) si deduce quindi che $b \mid p^k - b$, cioè che esiste $h \in \mathbb{Z}$ tale che $p^k - b = hb$, ma allora $p^k = (h + 1)b$ e dunque, ricordando che in $\mathbb{Z}$ vale l'unicità della fattorizzazione in numeri primi, posso affermare che b è una potenza di p.

Si consideri adesso l'operazione moltiplicativa banale su $(\mathbb{Q}/\mathbb{Z})(p)$, cioè l'operazione binaria $\cdot$ definita da $\frac{a}{p^k}\mathbb{Z} \cdot \frac{b}{p^k}\mathbb{Z} := \mathbb{Z}$, cosicché $(\mathbb{Q}/\mathbb{Z})(p)$ sia banalmente un anello. Si usa indicare l'anello appena costruito con la notazione $\mathbb{Z}(p^\infty)$. Trattasi di un anello senza identità, poiché comunque assegnati $a \in \mathbb{Z}$, $k \in \mathbb{N}$ vale la relazione $\frac{1}{p}\mathbb{Z} \cdot \frac{a}{p^k}\mathbb{Z} = \mathbb{Z}$ e $\mathbb{Z} \neq \frac{1}{p}\mathbb{Z}$ in virtù del teorema 2.1-(i) assieme al fatto che $\frac{1}{p} \notin \mathbb{Z}$.

Si osservi inoltre che, per come si è definita l'operazione binaria $\cdot$ su $\mathbb{Z}(p^\infty)$, tutti i suoi sottoanelli sono banalmente ideali. Detto questo dimostro che, comunque assegnato $n \in \mathbb{N}$, si ha la seguente descrizione:

$$\left(\frac{1}{p^n}\mathbb{Z}\right) = J\,, \quad \text{dove} \quad J := \left\{ \frac{a}{p^n}\mathbb{Z} \in \mathbb{Q}/\mathbb{Z} \;\middle|\; a \in \mathbb{Z} \right\}$$

Innanzitutto, si vede assai facilmente che $J < \mathbb{Z}(p^\infty)$ è un sottoanello. Dati infatti $\frac{a}{p^n}\mathbb{Z}, \frac{b}{p^n}\mathbb{Z} \in J$, vale che:

$$\frac{a}{p^n}\mathbb{Z} + \frac{b}{p^n}\mathbb{Z} = \frac{a+b}{p^n}\mathbb{Z}\,, \quad \frac{a}{p^n}\mathbb{Z} \cdot \frac{b}{p^n}\mathbb{Z} = \frac{0}{p^n}\mathbb{Z}$$

Ne segue che $J \subseteq \mathbb{Z}(p^\infty)$ è un sottoinsieme chiuso rispetto alle operazioni binarie $+$ e $\cdot$ su $\mathbb{Z}(p^\infty)$. Inoltre, vale banalmente che $\mathbb{Z} \in J$ in quanto $\mathbb{Z} = \frac{0}{p^n}\mathbb{Z}$ per il teorema 2.1-(i) e altrettanto facilmente si verifica che $-\frac{a}{p^n}\mathbb{Z} \in J$. Posso dunque affermare che $J < \mathbb{Z}(p^\infty)$ è un sottoanello, ma allora $J \lhd \mathbb{Z}(p^\infty)$ è un ideale per quanto osservato prima. Si osservi adesso che $\frac{1}{p^n}\mathbb{Z} \in J$ essendo $1 \in \mathbb{Z}$ e di conseguenza $\left(\frac{1}{p^n}\mathbb{Z}\right) \subseteq J$ in virtù dell'osservazione 7.5. Dato invece un elemento $\frac{a}{p^n}\mathbb{Z} \in J$, posso utilizzare il fatto che $\left(\frac{1}{p^n}\mathbb{Z}\right) < \mathbb{Z}(p^\infty)$ è un sottoanello assieme alla relazione $\frac{a}{p^n}\mathbb{Z} = a\frac{1}{p^n}\mathbb{Z}$ per poter affermare che $\frac{a}{p^n}\mathbb{Z} \in \left(\frac{1}{p^n}\mathbb{Z}\right)$ e dunque, siccome il risultato ottenuto non dipende dalla scelta dell'elemento $\frac{a}{p^n}\mathbb{Z} \in J$, si ha anche il contenimento $J \subseteq \left(\frac{1}{p^n}\mathbb{Z}\right)$.

Adesso si vuole mostrare che, comunque fissato un ideale $I \lhd \mathbb{Z}(p^\infty)$, esiste $n \in \mathbb{N}$ tale che $I = \left(\frac{1}{p^n}\mathbb{Z}\right)$. Il caso $I = \{0\}$ è immediato in quanto basta scegliere $n := 0$. Suppongo quindi che $I \neq \{0\}$, cioè che esista un elemento $\frac{a}{p^k}\mathbb{Z} \in I$ con $a \in \mathbb{Z}$, $k \in \mathbb{N}^*$ e con $\mathrm{MCD}(a, p^k) = 1$ senza perdita di generalità. Per l'identità di Bezout, esistono $x, y \in \mathbb{Z}$ tali che $1 = ax + p^k y$ e in particolare, usando il fatto che $p^k \neq 0$ in quanto p è un numero primo, in $\mathbb{Q}$ posso dividere per p^k entrambi i membri della relazione precedente, ottenendo che $\frac{1}{p^k} = x\frac{a}{p^k} + y$. Passando ora alle classi laterali sinistre e applicando la proposizione 2.4-(iii.b) si deduce la condizione $\frac{1}{p^k}\mathbb{Z} = x\frac{a}{p^k}\mathbb{Z} + y\mathbb{Z}$ e di conseguenza $\frac{1}{p^k}\mathbb{Z} \in I$ in quanto $I < \mathbb{Z}(p^\infty)$ è un sottoanello, $y\mathbb{Z} = \mathbb{Z}$ per il teorema 2.1-(i) e $\mathbb{Z}$ è l'elemento neutro rispetto all'operazione additiva $+$ su $\mathbb{Z}(p^\infty)$. Definisco dunque:

$$n := \max\left\{ h \in \mathbb{Z} \;\middle|\; \frac{1}{p^h}\mathbb{Z} \in I \right\}$$

Per costruzione vale che $\frac{1}{p^n}\mathbb{Z} \in I$ e dunque $(\frac{1}{p^n}\mathbb{Z}) \subseteq I$ in virtù dell'osservazione 7.5. Si consideri adesso un elemento $\frac{b}{p^m}\mathbb{Z} \in I$. Ripetendo l'argomento di prima con l'identità di Bezout si evince che anche $\frac{1}{b^m}\mathbb{Z} \in I$. Dalla massimalità di n si deduce quindi che $m \leq n$ e di conseguenza $\frac{b}{p^m}\mathbb{Z} = bp^{n-m}\frac{1}{p^n}\mathbb{Z}$. Questo dimostra che $\frac{b}{p^m} \in (\frac{1}{p^n}\mathbb{Z})$ e dunque, per arbitrarietà nella scelta di $\frac{b}{p^m} \in I$, si può concludere che $I \subseteq (\frac{1}{p^n}\mathbb{Z})$. Dalla doppia inclusione e dall'arbitrarietà nella scelta dell'ideale $I \lhd R$ segue quindi che ciascun ideale di $\mathbb{Z}(p^\infty)$ è della forma $(\frac{1}{p^n}\mathbb{Z})$ con $n \in \mathbb{N}$.

A questo punto, comunque sia fissato un ideale $M \lhd \mathbb{Z}(p^\infty)$ con $M \neq \mathbb{Z}(p^\infty)$, in vista della discussione precedente esiste $n \in \mathbb{N}$ tale che $M = (\frac{1}{p^n}\mathbb{Z})$. Definisco $I := (\frac{1}{p^{n+1}}\mathbb{Z})$ e noto che, per l'osservazione 7.5 e in virtù del fatto che $\frac{1}{p^n} = \frac{p}{p^{n+1}}$, vale l'inclusione $M \subseteq I$. Ora, per mostrare che tale contenimento è stretto, suppongo per assurdo che $\frac{1}{p^{n+1}}\mathbb{Z} \in (\frac{1}{p^n}\mathbb{Z})$ cioè, ricordando la descrizione fornita in precedenza per l'ideale principale $(\frac{1}{p^n}\mathbb{Z})$, che esista $a \in \mathbb{Z}$ tale che $\frac{1}{p^{n+1}} = \frac{a}{p^n}$. Moltiplicando per p^{n+1} i due membri della relazione precedente, si ottiene che $ap = 1$, ma questo è assurdo in quanto p non è invertibile essendo p un numero primo. Questo dimostra che $(\frac{1}{p^n}\mathbb{Z}) \subsetneq (\frac{1}{p^{n+1}}\mathbb{Z})$. Infine, ripetendo lo stesso argomento con $n+1$ al posto di n, si ottiene la condizione $(\frac{1}{p^{n+1}}\mathbb{Z}) \subsetneq (\frac{1}{p^{n+2}}\mathbb{Z})$ e in particolare $I \neq \mathbb{Z}(p^\infty)$. Si può dunque concludere, data l'arbitrarietà nella scelta dell'ideale $M \lhd \mathbb{Z}(p^\infty)$ con $M \neq \mathbb{Z}(p^\infty)$, che $\mathbb{Z}(p^\infty)$ non ammette nessun ideale massimale. Si può anche osservare che la dimostrazione della proposizione 7.8 non può essere applicata al caso di $\mathbb{Z}(p^\infty)$ in quanto si ricorre all'osservazione 7.2, valida solamente nel caso degli anelli con identità.

8 Campo dei quozienti di un dominio integrale

Si considerino un corpo F e un suo sottoanello $R < F$. Se $1 \in R$, allora non è vero a priori che anche R è un corpo perché nulla garantisce che ogni elemento di R ammetta un inverso in R. Un controesempio è dato semplicemente dal caso particolare in cui si pone $F := \mathbb{Q}$, $R := \mathbb{Z}$. Sicuramente si può dire, tuttavia, che R è un dominio in quanto sottoinsieme di F, che per l'osservazione 6.5 è un dominio.

In questa sezione, ci si pone il problema opposto: assegnato un dominio D, è sempre possibile trovare un corpo F tale che D sia isomorfo a un sottoanello di F contenente l'identità? In generale, la risposta[28] a questa domanda non è affermativa. Tuttavia, se ci si restringe al caso commutativo, vale a dire al caso dei domini integrali, è possibile costruire un campo $Q(D)$, detto il *campo dei quozienti di* D, che gode delle proprietà desiderate.

8.1 Campo dei quozienti

L'idea di base è imitare la costruzione di $\mathbb{Q}$ a partire da $\mathbb{Z}$. Posto per semplicità $D^* := D \setminus \{0\}$, da qui in poi considero quindi la relazione $\sim$ su $D \times D^*$ tale che, per definizione, valga $(a, b) \sim (c, d)$ se $a \cdot d = b \cdot c$.

Proposizione 8.1. *La relazione $\sim$ su $D \times D^*$ è una relazione di equivalenza.*

Dimostrazione. Siano $(a, b), (c, d), (e, f) \in D \times D^*$ tre elementi prefissati. Basta semplicemente verificare che la relazione $\sim$ gode delle seguenti proprietà:

- riflessiva: poiché si assume che D sia un dominio integrale, per la proprietà commutativa vale che $a \cdot b = b \cdot a$ ma questo equivale a richiedere, per come si è definita la relazione $\sim$, che $(a, b) \sim (a, b)$.
- simmetrica: se $(a, b) \sim (c, d)$ allora, per definizione di $\sim$, vale che $a \cdot d = b \cdot c$. Utilizzando ancora l'ipotesi che D sia un dominio integrale, quindi un anello commutativo, la condizione precedente diventa $c \cdot b = d \cdot a$ e posso dunque affermare che $(c, d) \sim (a, b)$.
- transitiva: se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, cioè se $a \cdot d = b \cdot c$ e se $c \cdot f = d \cdot e$ allora, in virtù del fatto che D è un dominio integrale e in particolare un anello commutativo, si ricava la condizione:

  $$(a \cdot f) \cdot d = (a \cdot d) \cdot f = (b \cdot c) \cdot f = b \cdot (c \cdot f) = b \cdot (d \cdot e) = (b \cdot e) \cdot d$$

  Utilizzando il fatto che $d \neq 0$ in quanto elemento di D^*, posso applicare le leggi di cancellazione, vale a dire l'osservazione 6.5-(ii), ottenendo che $a \cdot f = b \cdot e$. Questo dimostra che $(a, b) \sim (e, f)$ e dunque si ha la tesi. □

Da questo punto in poi, al fine di semplificare la notazione, l'operazione binaria $\cdot$ su D verrà omessa.

[28] Per approfondire la questione, un buon riferimento è il libro *Basic Algebra I* di N. Jacobson.

Definizione 8.1. La classe di equivalenza di un elemento $(a, b) \in D \times D^*$ rispetto alla relazione $\sim$ viene detta una *frazione* (oppure un *quoziente*) e si denota $\frac{a}{b}$. Il quoziente $D \times D^*/\sim$ prende il nome di *insieme dei quozienti di* D e si denota $Q(D)$. Inoltre, su $Q(D)$ si considerano le operazioni binarie $+$ e $\cdot$ definite dalle condizioni seguenti e si pongono per semplicità le seguenti convenzioni:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}, \quad 0 := \frac{0}{1}, \quad 1 := \frac{1}{1}, \quad -\frac{a}{b} := \frac{-a}{b}$$

La definizione 8.1 è ben posta perché le operazioni binarie $+$ e $\cdot$ sono ben definite. Esse non dipendono, cioè, dalla particolare scelta di un rappresentante in $D \times D^*$. Siano infatti $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in Q(D)$ frazioni tali che $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$. Per come sono state definite le operazioni binarie $+$ e $\cdot$ su $Q(D)$ basterà dimostrare che valgono le condizioni $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ e $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. Per farlo, è cruciale l'ipotesi che D sia un dominio integrale e in particolare un anello commutativo, in virtù della quale si ottengono le due relazioni seguenti:

$$\begin{aligned}(ad + bc)b'd' &= adb'd' + bcb'd' \\ &= (ab')dd' + bb'(cd') \\ &= (ba')dd' + bb'(dc') \\ &= bda'd' + bdb'c' = bd(a'd' + b'c')\end{aligned} \qquad \begin{aligned}(ac)(b'd') &= (ab')(cd') \\ &= (ba')(dc') \\ &= (bd)(a'c')\end{aligned}$$

Per come è definita la relazione $\sim$ su $D \times D^*$, le suddette condizioni implicano quanto volevasi dimostrare.

Proposizione 8.2. *L'insieme dei quozienti $Q(D)$ munito delle operazioni binarie $+$ e $\cdot$ introdotte nella definizione 8.1 è un campo con elemento neutro rispetto alla somma 0 e con identità 1.*

Dimostrazione. Bisogna innanzitutto mostrare che $Q(D)$ munito dell'operazione di somma $+$ è un gruppo abeliano con elemento neutro 0. Siano $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(D)$ elementi fissati. Dato che per ipotesi D è un anello si può affermare, in virtù delle due relazioni seguenti, che l'operazione $+$ gode della proprietà associativa:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{(ad + bc)f + (bd)e}{(bd)f} = \frac{adf + bcf + bde}{bdf}$$
$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{a(df) + b(cf + de)}{b(df)} = \frac{adf + bcf + bde}{bdf}$$

È immediato verificare, per l'ipotesi che D sia un anello commutativo, che l'operazione binaria additiva $+$ gode anche della proprietà commutativa. Di conseguenza, per poter affermare che 0 è un elemento neutro rispetto alla somma sarà sufficiente osservare che, per la proposizione 6.1-(i), vale la condizione seguente:

$$\frac{a}{b} + \frac{0}{1} = \frac{a1 + 0b}{b1} = \frac{a}{b}$$

Altrettanto facilmente si dimostra che l'opposto della frazione $\frac{a}{b}$ è $-\frac{a}{b}$. Osservando infatti che $\frac{0}{1} = \frac{0}{b^2}$ per come si è definita la relazione $\sim$ su $D \times D^*$ e in virtù della proposizione 6.1-(i), si ottiene la condizione:

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{b^2} = \frac{0}{b^2} = 0$$

Non dipendendo il risultato ottenuto dalla scelta degli elementi $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(D)$, posso affermare che $Q(D)$ munito dell'operazione di somma $+$ è un gruppo abeliano con elemento neutro 0. Ora dimostro che $Q(D)$ è un anello commutativo con identità 1. Si vede facilmente che l'operazione binaria $\cdot$ su $Q(D)$ è associativa:

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$$

Come nel caso dell'operazione binaria $+$ su $Q(D)$, anche l'operazione moltiplicativa $\cdot$ gode della proprietà commutativa in virtù dell'ipotesi che D sia un anello commutativo. È dunque immediato verificare che 1 è l'identità rispetto al prodotto, infatti:

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{a1}{b1} = \frac{a}{b}$$

Si può dunque affermare, per arbitrarietà nella scelta delle frazioni $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(D)$, che $Q(D)$ è un anello commutativo con identità 1. Per dimostrare che $Q(D)$ è un campo, per la definizione 6.6 basterà mostrare

che ogni suo elemento non banale è invertibile. Sia dunque $\frac{a}{b} \in Q(D)$, $\frac{a}{b} \neq 0$ un elemento fissato. Poiché si assume che $\frac{a}{b} \neq 0$ dovrà valere, per come è stata definita la relazione $\sim$ su $D \times D^*$, che $a1 \neq 0b$. In altre parole, per definizione di identità e in virtù della proposizione 6.1-(i), si ha che $a \neq 0$ e di conseguenza si può considerare la frazione $\frac{b}{a} \in Q(D)$. Per l'ipotesi che D sia un anello commutativo, si ha che $ab = ba$ e si ricava quindi la seguente condizione:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$$

Posso dunque affermare che $\frac{b}{a}$ è l'inverso di $\frac{a}{b}$. Poiché il risultato ottenuto non dipende da una particolare scelta della frazione $\frac{a}{b} \in Q(D)$, $\frac{a}{b} \neq 0$, si può infine concludere che $Q(D)$ è un campo. □

Definizione 8.2. Siano R e S anelli con identità 1_R e 1_S rispettivamente. Un omomorfismo $f\colon R \to S$ si dice *unitario* (oppure *identitario*) se $f(1_R) = 1_S$.

Osservazione 8.1. Dalla definizione 8.2 e da quanto si è discusso nell'osservazione 6.13 segue banalmente che non tutti gli omomorfismi di anelli sono unitari.

Osservazione 8.2. Siano R e S anelli con identità 1_R e 1_S rispettivamente, sia $f\colon R \to S$ un omomorfismo unitario e sia $x \in R$. Se $x \in U(R)$, allora $f(x) \in U(S)$ e vale che $f(x)^{-1} = f(x^{-1})$.

Dimostrazione. Innanzitutto, dato che per ipotesi $x \in U(R)$, esiste un certo $y \in R$ tale che $xy = yx = 1_R$. Applicando f su tale relazione e utilizzando l'ipotesi che f sia un omomorfismo di anelli unitario, si ottiene la condizione $f(x)f(y) = f(y)f(x) = 1_S$ e da questo segue immediatamente la tesi. □

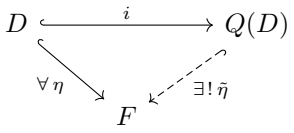
Proposizione 8.3 (Proprietà universale del campo dei quozienti)**.** *Sia D un dominio integrale.*

(i) *L'applicazione $i\colon D \to Q(D)$ definita da $i(a) := \frac{a}{1}$ è un monomorfismo unitario.*

(ii) *Sia F un campo. L'applicazione i definita nel punto (i) soddisfa la seguente proprietà universale:*

$$\forall\, \eta\colon D \to F \text{ monomorfismo unitario } \exists!\, \tilde{\eta}\colon Q(D) \to F \text{ monomorfismo unitario } \mid\ \tilde{\eta} \circ i = \eta$$

Equivalentemente, il seguente diagramma di monomorfismi è commutativo:



Dimostrazione.

(i) Siano $a, b \in D$ elementi fissati. Per la definizione 8.1 e per costruzione, si hanno le due condizioni:

$$i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)\,, \quad i(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = i(a) \cdot i(b)$$

Poiché tali relazioni non dipendono dalla scelta degli elementi $a, b \in D$, posso affermare che i è un omomorfismo di anelli. È inoltre immediato verificare che i è unitario. Calcolo infine il nucleo di i:

$$\operatorname{Ker} i = \{\, a \in D \mid i(a) = 0 \,\} = \left\{\, a \in D \;\middle|\; \frac{a}{1} = \frac{0}{1} \,\right\} = \{\, a \in D \mid a = 0 \,\} = \{0\}$$

Posso dunque concludere, in virtù dell'osservazione 6.15-(ii), che i è un monomorfismo.

(ii) Siano $\eta\colon D \to F$ un monomorfismo unitario, $\tilde{\eta}\colon Q(D) \to F$ la mappa data da $\tilde{\eta}(\frac{a}{b}) := \eta(a)\eta(b)^{-1}$. Innanzitutto, bisogna mostrare che si tratta di un'applicazione ben definita. La prima potenziale ambiguità riguarda l'esistenza di $\eta(b)^{-1}$. A tal proposito si noti che, data una frazione $\frac{a}{b} \in Q(D)$, il rappresentante della frazione scelta corrisponde a una coppia $(a, b) \in D \times D^*$ e in particolare si ha che $b \neq 0$. Poiché si assume che η sia un monomorfismo, per l'osservazione 6.15-(ii) dovrà valere che $b \notin \operatorname{Ker} \eta$ e dunque $\eta(b) \neq 0$. Di conseguenza, essendo per ipotesi F un campo, l'elemento $\eta(b)$ è invertibile. Ora dimostro, invece, che la funzione $\tilde{\eta}$ non dipende dai rappresentanti delle frazioni scelte. Siano dunque fissate due frazioni $\frac{a}{b}, \frac{a'}{b'} \in Q(D)$ tali che $\frac{a}{b} = \frac{a'}{b'}$, cioè tali che valga $ab' = ba'$.

In particolare, si ha che $\eta(ab') = \eta(ba')$ e quindi, usando il fatto che η è un omomorfismo, si ricava che $\eta(a)\eta(b') = \eta(b)\eta(a')$. In vista della discussione precedente, posso moltiplicare ambo i membri della relazione ottenuta per $\eta(b)^{-1}\eta(b')^{-1}$. Usando adesso l'ipotesi che D sia un dominio integrale e quindi un anello commutativo, ottengo che $\eta(a)\eta(b^{-1}) = \eta(a')\eta(b')^{-1}$ e questo, per come è stata definita la mappa $\tilde{\eta}$, implica che $\tilde{\eta}(\frac{a}{b}) = \tilde{\eta}(\frac{a'}{b'})$. In definitiva, posso affermare che l'applicazione $\tilde{\eta}$ è ben definita.

Siano adesso $\frac{a}{b}, \frac{c}{d} \in Q(D)$ due frazioni. Ricordando come sono state definite le operazioni binarie $+$ e $\cdot$ su $Q(D)$, usando la definizione di $\tilde{\eta}$, l'osservazione 8.2, l'ipotesi che η sia un omomorfismo, il fatto che l'operazione moltiplicativa su F gode della proprietà distributiva destra e infine l'ipotesi che F sia un campo quindi, in particolare, un anello commutativo, si ottengono le due condizioni:

$$\begin{aligned}\tilde{\eta}\Big(\frac{a}{b} + \frac{c}{d}\Big) &= \tilde{\eta}\Big(\frac{ad+bc}{bd}\Big)\\ &= \eta(ad+bc)\eta(bd)^{-1}\\ &= \big(\eta(a)\eta(d) + \eta(b)\eta(c)\big)\eta(d)^{-1}\eta(b)^{-1}\\ &= \eta(a)\eta(b)^{-1} + \eta(c)\eta(d)^{-1}\\ &= \tilde{\eta}\Big(\frac{a}{b}\Big) + \tilde{\eta}\Big(\frac{c}{d}\Big)\end{aligned} \qquad \begin{aligned}\tilde{\eta}\Big(\frac{a}{b} \cdot \frac{c}{d}\Big) &= \tilde{\eta}\Big(\frac{ac}{bd}\Big)\\ &= \eta(ac)\eta(bd)^{-1}\\ &= \eta(a)\eta(c)\eta(d)^{-1}\eta(b)^{-1}\\ &= \eta(a)\eta(b)^{-1}\eta(c)\eta(d)^{-1}\\ &= \tilde{\eta}\Big(\frac{a}{b}\Big)\tilde{\eta}\Big(\frac{c}{d}\Big)\end{aligned}$$

Questo dimostra, per arbitrarietà nella scelta delle frazioni $\frac{a}{b}, \frac{c}{d} \in Q(D)$, che l'applicazione $\tilde{\eta}$ è un omomorfismo di anelli. Si verifica assai facilmente che si tratta anche di un omomorfismo unitario. Infatti, poiché per ipotesi η è unitario e per le proprietà dell'identità, si ha la relazione seguente:

$$\tilde{\eta}\Big(\frac{1}{1}\Big) = \eta(1)\eta(1)^{-1} = 1$$

Si noti adesso che, data una frazione $\frac{a}{b} \in Q(D)$, la condizione $\eta(a)\eta(b)^{-1} = 0$ implica che $\eta(a) = 0$ per l'ipotesi che D sia un dominio integrale, cioè che D non ammetta divisori dello zero sinistri o destri non banali, assieme al fatto che l'inverso di un elemento in un anello è sempre non banale. In virtù di questo fatto, per l'ipotesi che η sia un monomorfismo assieme all'osservazione 6.11 ed essendo $\frac{0}{b} = \frac{0}{1}$ per ogni $b \in D^*$ per la proposizione 6.1-(i), il nucleo dell'omomorfismo $\tilde{\eta}$ è dato da:

$$\begin{aligned}\operatorname{Ker}\tilde{\eta} &= \Big\{ \frac{a}{b} \in Q(D) \;\Big|\; \tilde{\eta}\Big(\frac{a}{b}\Big) = 0 \Big\}\\ &= \Big\{ \frac{a}{b} \in Q(D) \;\Big|\; \eta(a)\eta(b)^{-1} = 0 \Big\}\\ &= \Big\{ \frac{a}{b} \in Q(D) \;\Big|\; \eta(a) = 0 \Big\}\\ &= \Big\{ \frac{a}{b} \in Q(D) \;\Big|\; a = 0 \Big\} = \Big\{ \frac{0}{1} \Big\}\end{aligned}$$

Posso dunque affermare, in virtù dell'osservazione 6.15-(ii), che $\tilde{\eta}$ è un monomorfismo. Rimane da verificare soltanto che $\tilde{\eta}$ soddisfa la condizione $\tilde{\eta} \circ i = \eta$. Per farlo basta semplicemente osservare che, comunque fissato $a \in D$, per l'ipotesi che η sia un omomorfismo unitario si ha la condizione:

$$(\tilde{\eta} \circ i)(a) = \tilde{\eta}\big(i(a)\big) = \tilde{\eta}\Big(\frac{a}{1}\Big) = \eta(a)\eta(1)^{-1} = \eta(a)$$

Sia infine $\bar{\eta}\colon Q(D) \to F$ un omomorfismo unitario tale che $\bar{\eta} \circ i = \eta$ e sia $\frac{a}{b} \in Q(D)$ un elemento fissato. Utilizzando il fatto, noto dalla dimostrazione della proposizione 8.2, che $\frac{1}{b}$ è l'inverso di $\frac{b}{1}$, ricordando come è stata definita l'applicazione i nel punto (i) già dimostrato, usando le assunzioni fatte su $\bar{\eta}$ e applicando l'osservazione 8.2, si ricava la relazione seguente:

$$\begin{aligned}\bar{\eta}\Big(\frac{a}{b}\Big) = \bar{\eta}\Big(\frac{a1}{1b}\Big) = \bar{\eta}\Big(\frac{a}{1} \cdot \frac{1}{b}\Big) &= \bar{\eta}\Big(\frac{a}{1} \cdot \Big(\frac{b}{1}\Big)^{-1}\Big)\\ = \bar{\eta}\big(i(a) \cdot i(b)^{-1}\big) = \bar{\eta}\big(i(a)\big)\bar{\eta}\big(i(b)\big)^{-1} &= \eta(a)\eta(b)^{-1} = \tilde{\eta}\Big(\frac{a}{b}\Big)\end{aligned}$$

Poiché il risultato ottenuto non dipende da una particolare scelta della frazione $\frac{a}{b} \in Q(D)$, si può affermare che $\bar{\eta} = \tilde{\eta}$ e questo dimostra, per arbitrarietà nella scelta dell'omomorfismo unitario $\bar{\eta}$ che verifichi le proprietà richieste, l'unicità di $\tilde{\eta}$. L'asserto è dunque dimostrato. □

Osservazione 8.3. Dalla dimostrazione della proposizione 8.3-(ii) segue immediatamente che, in effetti, si ha un risultato più forte dell'unicità. Nella parte conclusiva della dimostrazione, infatti, non si assume che $\bar{\eta}$ sia un'applicazione iniettiva e di conseguenza anche omomorfismi unitari che a priori non sono iniettivi ma che soddisfano la condizione $\bar{\eta} \circ i = \eta$ dovranno coincidere con $\tilde{\eta}$.

Osservazione 8.4. Siano D un dominio integrale, F un campo, $\eta\colon D \to F$ un monomorfismo unitario. Per la proprietà universale del campo dei quozienti, vale a dire la proposizione 8.3-(ii), esiste un monomorfismo unitario $\tilde{\eta}\colon Q(D) \to F$. In particolare, essendo $\tilde{\eta}$ un'applicazione iniettiva, dovrà valere che $|Q(D)| \leq |F|$. In virtù di questo fatto e della proposizione 8.3-(i), che garantisce l'esistenza di un monomorfismo unitario da D a $Q(D)$, posso affermare che il campo dei quozienti $Q(D)$ di un dominio integrale D è il più piccolo campo in cui D si può immergere in maniera unitaria, vale a dire rispettando le identità.

Osservazione 8.5. Sia D un dominio integrale e sia $i\colon D \to Q(D)$ la mappa data nella proposizione 8.3-(i). Il risultato appena menzionato garantisce che i sia un monomorfismo e quindi, per l'osservazione 6.15-(ii), si ha che $\operatorname{Ker} i = \{0\}$. Dal primo teorema di isomorfismo si ricava dunque che $D \simeq \operatorname{Im} i$, dove $\operatorname{Im} i < Q(D)$ è un sottoanello in virtù dell'osservazione 6.15-(i). Inoltre, per la proposizione 8.3-(i) si ha che $1 \in \operatorname{Im} i$ e quindi è possibile finalmente dare una risposta alla domanda posta a inizio sezione: il campo dei quozienti $Q(D)$ di un dominio integrale D è un campo tale che D sia isomorfo a un sottoanello di $Q(D)$ contenente l'identità. Dall'osservazione 8.4 segue inoltre che $Q(D)$ è il più piccolo campo che gode di tale proprietà.

Esempio 8.1. Poiché la costruzione del campo dei quozienti di un dominio integrale imita, come si è già detto a inizio sezione, la costruzione di $\mathbb{Q}$ a partire da $\mathbb{Z}$, vale banalmente che $\mathbb{Q} = Q(\mathbb{Z})$. Dunque $\mathbb{Q}$ è il più piccolo campo che contiene $\mathbb{Z}$ come sottoanello contenente l'identità.

9 Teoria della divisibilità in anelli commutativi

L'idea è estendere la teoria della fattorizzazione in numeri primi da $\mathbb{Z}$ ad anelli commutativi con identità $1 \neq 0$ più generali, come per esempio agli anelli di polinomi in più variabili.

Definizione 9.1 (Divisibilità)**.** Sia R un anello commutativo con identità $1 \neq 0$ e siano $a, b \in R$.

(i) Si dice che a *divide* b e si scrive $a \mid b$ se $a \neq 0$ e se esiste un elemento $c \in R$ tale che $b = a \cdot c$.

(ii) Si dice che a *e* b *sono associati* e si scrive $a \sim b$ se $a \mid b$ e $b \mid a$.

(iii) Un elemento $c \in R$ tale che $c \mid a$ viene detto un *fattore* (oppure un *divisore*) *di* a.

(iv) Un fattore c di a tale che $c \not\sim a$ e $c \notin U(R)$ viene detto un *fattore proprio di* a.

Proposizione 9.1. *Siano R un anello commutativo con identità $1 \neq 0$, $a, b, u \in R$. Valgono le proprietà:*

(i) *$a \mid b$ se e solo se $(b) \subseteq (a)$ con $a \neq 0$.*

(ii) *$a \sim b$ se e solo se $(a) = (b)$ con $a, b \neq 0$.*

(iii) *$u \in U(R)$ se e solo se $u \mid x$ per ogni $x \in R$.*

(iv) *L'essere elementi associati è una relazione di equivalenza su R.*

(v) *Se esiste un elemento $v \in U(R)$ tale che $a = b \cdot v$ e se $a, b \neq 0$, allora $a \sim b$.*

(vi) *Se R è un dominio integrale e $a \sim b$, allora $a, b \neq 0$ ed esiste un certo $v \in U(R)$ tale che $a = b \cdot v$.*

Dimostrazione.

(i) Per la definizione 9.1-(i), dire che $a \mid b$ significa che $a \neq 0$ e che esiste un elemento $c \in R$ tale che $b = a \cdot c$ e questo è equivalente a richiedere, per l'osservazione 7.7, che $b \in (a)$ con $a \neq 0$. In altre parole, per l'osservazione 7.5, si ha la condizione $(b) \subseteq (a)$ con $a \neq 0$ per minimalità, ma questo è proprio quanto volevasi dimostrare.

(ii) Per la definizione 9.1-(ii), si ha che $a \sim b$ se e solo se $a \mid b$ e $b \mid a$ ma questo equivale a richiedere, per il punto (i) già dimostrato, che $(b) \subseteq (a)$ con $a \neq 0$ e che $(a) \subseteq (b)$ con $b \neq 0$, cioè che $(a) = (b)$ con $a, b \neq 0$ e dunque si ha la tesi.

(iii) Anche in questo caso basterà esibire una catena di doppie implicazioni. Per la definizione 6.5 e per l'ipotesi che R sia un anello commutativo, vale che $u \in U(R)$ se e solo se esiste un elemento $r \in R$ tale che $r \cdot u = 1$ ma questo equivale a richiedere, in virtù dell'osservazione 7.7, che $1 \in (u)$. Per l'osservazione 7.2, questo è come dire che $(u) = R$, ma siccome una delle due inclusioni è sempre verificata per definizione di ideale, è del tutto equivalente richiedere che $R \subseteq (u)$. In altre parole, vale la condizione $a \in (u)$ per ogni $a \in R$. In virtù dell'osservazione 7.5, la suddetta condizione è a sua volta equivalente a richiedere che $(a) \subseteq (u)$ per ogni $a \in R$. Ora, se fosse $u = 0$ allora, per la proposizione 6.1-(i), varrebbe che $r \cdot u = 0$, contraddicendo l'ipotesi che $1 \neq 0$. Di conseguenza, si dovrà avere che $u \neq 0$ e quindi, usando la relazione precedente con il punto (i) appena dimostrato, ottengo che $u \mid a$ per ogni $a \in R$. Viceversa, se si assume che $u \mid a$ per ogni $a \in R$, allora si ha per ogni $a \in R$ il contenimento $(a) \subseteq (u)$ grazie al punto (i) già dimostrato. Ma allora, ripercorrendo a ritroso la catena delle doppie implicazioni si ricava che $u \in U(R)$ e dunque si ottiene la tesi.

(iv) L'asserto segue banalmente dall'equivalenza espressa nel punto (ii) già dimostrato.

(v) Se $a = b \cdot v$, allora $b \mid a$ per la definizione 9.1-(i) e per l'ipotesi che $b \neq 0$. Al contempo, utilizzando l'assunzione che $v \in U(R)$, posso moltiplicare a destra per v^{-1} entrambi i membri della condizione precedente, ottenendo che $b = a \cdot v^{-1}$ e quindi vale che $a \mid b$ perché per ipotesi anche $a \neq 0$. Per la definizione 9.1-(ii), si può dunque concludere che $a \sim b$.

(vi) Se $a \sim b$, allora $a \mid b$ e $b \mid a$ per la definizione 9.1-(ii) e quindi, in virtù della definizione 9.1-(i), vale che $a, b \neq 0$ ed esistono due elementi $c, d \in R$ tali che $b = a \cdot c$ e $a = b \cdot d$. Mettendo assieme tali relazioni, si ricava che:

$$b = a \cdot c = (b \cdot d) \cdot c = b \cdot (d \cdot c)$$

Poiché per ipotesi R è un dominio integrale ed essendo $b \neq 0$, posso usare la legge di cancellazione sinistra fornita dall'osservazione 6.6-(ii), ottenendo che $d \cdot c = 1$. Questo dimostra, in particolare, che $d \in U(R)$. Ricordando infine che $a = b \cdot d$, si ottiene dunque la tesi. □

Osservazione 9.1. Sia R un dominio integrale e sia $a \in R$. Dalla proposizione 9.1 segue immediatamente, come caso particolare, che $a \sim 1$ se e solo se $a \in U(R)$.

Osservazione 9.2. Sia R un anello commutativo con identità $1 \neq 0$. Si vede parecchio facilmente che, per la definizione 9.1-(i), la divisibilità è una relazione su R riflessiva e transitiva. Ciononostante, essa non è in generale una relazione d'ordine su R in quanto potrebbe non essere antisimmetrica. Si consideri infatti il caso particolare in cui $R = \mathbb{Z}$. Se si assume che $a \mid b$ e $b \mid a$, allora $a \sim b$ per la definizione 9.1-(ii). Siccome $\mathbb{Z}$ è un dominio integrale, posso applicare la proposizione 9.1-(vi), in virtù della quale $a = b \cdot v$ per un certo $v \in U(\mathbb{Z})$. Ma allora, essendo $U(\mathbb{Z}) = \{\pm 1\}$ come si è visto nell'esempio 1.9, posso concludere che $a = \pm b$.

Definizione 9.2 (Primi e irriducibili)**.** Sia R un anello commutativo con identità $1 \neq 0$.

(i) Un elemento $p \in R$ è detto *primo* se $p \neq 0$, se $p \notin U(R)$ e se, comunque vengano fissati elementi $a, b \in R$ tali che $p \mid a \cdot b$, si ha che $p \mid a$ oppure $p \mid b$.

(ii) Un elemento $c \in R$ viene detto *irriducibile* se $c \neq 0$, se $c \notin U(R)$ e se, comunque vengano fissati due elementi $a, b \in R$ tali che $a \cdot b = c$, vale che $a \in U(R)$ oppure $b \in U(R)$.

Esempio 9.1. Nel caso particolare dell'anello $\mathbb{Z}$ è possibile dimostrare[29] che elementi primi e irriducibili coincidono. Si tratta, infatti, di tutti gli elementi della forma $\pm p$ con p numero primo. Tuttavia, dato un qualsiasi anello commutativo R con identità $1 \neq 0$, in generale non è vero né che tutti gli elementi primi sono irriducibili, né che tutti gli elementi irriducibili sono primi, come mostrano i seguenti controesempi.

Si consideri l'anello $\mathbb{Z}_6$ con le usuali operazioni di somma e di prodotto. Si verifica facilmente che $\mathbb{Z}_6$ è un anello commutativo con identità $\bar{1} \neq \bar{0}$. Asserisco che $\bar{2}$ è un elemento primo ma non irriducibile di $\mathbb{Z}_6$. Innanzitutto, è parecchio evidente che $\bar{2} \neq \bar{0}$ e che $\bar{2} \notin U(\mathbb{Z}_6)$ in quanto $U(\mathbb{Z}_6) = \mathbb{Z}_6^*$ per l'esempio 1.10 e $\mathrm{MCD}(2, 6) \neq 1$. Siano adesso $\bar{a}, \bar{b} \in \mathbb{Z}_6$ elementi fissati tali che $\bar{2} \mid \bar{a} \cdot \bar{b}$. Per la definizione 9.1-(i), esiste un elemento $\bar{c} \in \mathbb{Z}_6$ tale che $\bar{a} \cdot \bar{b} = \bar{2} \cdot \bar{c}$ ma questo equivale a richiedere, per come è stata definita la relazione di congruenza modulo 6, che esista $k \in \mathbb{Z}$ tale che $ab = 2c + 6k$ oppure, equivalentemente, tale che valga la condizione $ab = 2(c + 3k)$. In particolare, si deduce che ab è un numero pari e dunque deve essere pari a

[29] L'argomento è stato trattato con maggiore dettaglio negli appunti del corso AL110.

oppure b. Posso assumere senza perdita di generalità che a sia pari, cioè che esista $h \in \mathbb{Z}$ tale che $a = 2h$. A questo punto basta osservare che $\bar{2} \mid \bar{a}$ in quanto $\bar{a} = \bar{2} \cdot \bar{h}$ e da questo segue, per arbitrarietà nella scelta delle classi $\bar{a}, \bar{b} \in \mathbb{Z}_6$ tali che $\bar{2} \mid \bar{a} \cdot \bar{b}$, che $\bar{2}$ è un elemento primo di $\mathbb{Z}_6$. Si noti ora che $\bar{2}$ non è un elemento irriducibile di $\mathbb{Z}_6$ in quanto $\bar{2} = \bar{2} \cdot \bar{4}$, mentre $\bar{2}, \bar{4} \notin U(\mathbb{Z}_6)$ non essendo 2 e 4 numeri coprimi con 6. Questo dimostra che non tutti gli elementi primi sono irriducibili.

Si consideri adesso l'insieme $\mathbb{Z} + \mathbb{Z}\sqrt{-5} := \{ n + m\sqrt{-5} \mid n, m \in \mathbb{Z} \}$. Si vede con estrema facilità che $\mathbb{Z} + \mathbb{Z}\sqrt{-5} < \mathbb{C}$ è un sottoanello. Sia ora $N \colon \mathbb{Z} + \mathbb{Z}\sqrt{-5} \to \mathbb{N}$ la restrizione della norma complessa usuale sul sottoanello $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ e si noti che tale funzione è a valori in $\mathbb{N}$ essendo $N(n + m\sqrt{-5}) = n^2 + 5m^2$. Dimostro che 2 è un elemento irriducibile ma non primo di $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Per farlo, dimostro innanzitutto che, comunque assegnato un elemento $x \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$, vale che $x \in U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$ se e solo se $N(x) = 1$. Per definizione, se $x \in U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$, allora esiste un elemento $y \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ tale che $xy = 1$ ma allora, passando alla norma e sfruttandone la[30] moltiplicatività, si ricava che $N(x)N(y) = 1$ e quindi $N(x) = 1$. Se invece si assume che $N(x) = 1$, allora $x^{-1} = \bar{x}$ e ovviamente $\bar{x} \in U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$. Si ricordi, infatti, che:

$$x^{-1} = \frac{\bar{x}}{N(x)}$$

Fatta questa premessa, si osservi che $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ in quanto $(2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$ e si supponga, per assurdo, che $2 \mid 1 + \sqrt{-5}$ oppure $2 \mid 1 - \sqrt{-5}$. In entrambi i casi, passando alla norma e usandone la moltiplicatività si ricava che $N(2)$ divide $N(1 \pm \sqrt{-5})$, ma $N(2) = 4$ mentre $N(1 \pm \sqrt{-5}) = 6$ e dunque si ha una contraddizione in quanto $4 \nmid 6$. Questo dimostra che $2 \nmid 1 \pm \sqrt{-5}$ e di conseguenza 2 non è un elemento primo di $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Siano adesso $x, y \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ due elementi fissati tali che $xy = 2$. Passando alla norma nella relazione precedente, si ottiene che $N(x)N(y) = 4$. Suppongo per assurdo che $N(x) = 2$. In tal caso, se $x = n + m\sqrt{-5}$, allora dovrà valere che $n^2 + 5m^2 = 2$ ma è immediato verificare che tale equazione non ammette soluzioni intere e questo è assurdo. Le uniche possibilità ammesse sono dunque $N(x) = 1$ oppure $N(x) = 4$, cioè $x \in U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$ oppure $y \in U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$. In definitiva, per arbitrarietà nella scelta di $x, y \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ tali che $xy = 2$, si ottiene che 2 è un elemento irriducibile di $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ e questo dimostra che non tutti gli elementi irriducibili sono primi.

Proposizione 9.2. *Siano R un anello commutativo con identità $1 \neq 0$, $c, p \in R$. Valgono le proprietà:*

(i) *Si ha che $p \in R$ è un elemento primo se e solo se $(p) \lhd R$ è un ideale primo non nullo.*

(ii) *Se $c \in R$ è un elemento irriducibile, allora (c) è un elemento massimale nell'insieme degli ideali principali propri di R cioè tale che, comunque venga fissato un ideale principale proprio $(d) \lhd R$ con $(c) \subseteq (d)$, valga la condizione $(d) = (c)$.*

(iii) *Se R è un dominio integrale e se (c) è un elemento massimale nell'insieme degli ideali principali propri di R, allora $c \in R$ è un elemento irriducibile.*

(iv) *Se R è un dominio integrale e $p \in R$ è un elemento primo, allora $p \in R$ è un elemento irriducibile.*

(v) *Se $c \in R$ è un elemento irriducibile, allora $c \neq 0$, $c \notin U(R)$ e c non ha fattori propri, vale a dire che i divisori di c sono elementi invertibili di R oppure elementi associati a c.*

(vi) *Se R è un dominio integrale, se $c \neq 0$, se $c \notin U(R)$ e se c non ha fattori propri, allora $c \in R$ è un elemento irriducibile.*

Dimostrazione.

(i) Dato che per ipotesi R è un anello commutativo con identità $1 \neq 0$, per la proposizione 7.5 si ha che $(p) \lhd R$ è un ideale primo se e solo se è un ideale fortemente primo ma questo, in virtù della proposizione 7.5-(i), è equivalente a richiedere che $(p) \neq R$ e che, comunque assegnati $a, b \in R$ tali che $a \cdot b \in (p)$, vale che $a \in (p)$ oppure $b \in (p)$. In virtù di quanto si è già visto nella dimostrazione della proposizione 9.1-(iii), vale che $(p) \neq R$ se e solo se $p \notin U(R)$. La seconda condizione è invece equivalente a richiedere, per l'osservazione 7.5, che per ogni $a, b \in R$ tali che $(a \cdot b) \subseteq (p)$ si abbia che $(a) \subseteq (p)$ oppure $(b) \subseteq (p)$. Ricordando tuttavia che per ipotesi $(p) \neq (0)$, cioè che $p \neq 0$, per

[30] Si ricordi che la norma di un numero complesso è moltiplicativa, cioè verifica la condizione $N(zw) = N(z)N(w)$ per ogni $z, w \in \mathbb{C}$. Questa e altre proprietà dei numeri complessi sono state già trattate nel corso AL110.

la proposizione 9.1-(i) è del tutto equivalente richiedere che, comunque assegnati $a, b \in R$ tali che $p \mid a \cdot b$, valga che $p \mid a$ oppure $p \mid b$. Posso quindi affermare, in vista della discussione precedente e della definizione 9.2-(i), che $(p) \lhd R$ è un ideale primo non nullo se e solo se $p \in R$ è un elemento primo e questo è esattamente quanto volevasi dimostrare.

(ii) Innanzitutto, poiché si assume che $c \in R$ sia un elemento irriducibile, si dovrà avere in particolare che $c \neq 0$ e che $c \notin U(R)$. Come si è già osservato nella dimostrazione del punto (i), la condizione $c \notin U(R)$ è equivalente a richiedere che $(c) \neq R$ e quindi, essendo $c \neq 0$, posso affermare che (c) è un ideale principale proprio. Sia ora $(d) \lhd R$ un ideale principale proprio con $(c) \subseteq (d)$. Poiché si assume che $(d) \lhd R$ sia un ideale proprio, dovrà valere che $d \neq 0$ e di conseguenza posso applicare la proposizione 9.1-(i), in virtù della quale $d \mid c$. Dalla definizione 9.1-(i), segue che esiste un certo $x \in R$ tale che $c = d \cdot x$ ma allora, dal momento che per ipotesi $c \in R$ è un elemento irriducibile, per la definizione 9.2-(ii) si dovrà avere che $d \in U(R)$ oppure $x \in U(R)$. Se fosse $d \in U(R)$ allora, come si è già osservato prima per l'ideale (c), dovrebbe valere che $(d) = R$, ma questo contraddice l'ipotesi che $(d) \lhd R$ sia un ideale proprio. Per esclusione, si deve avere che $x \in U(R)$ ma allora, ricordando che $c = d \cdot x$, dalla proposizione 9.1-(v) segue che $c \sim d$. Per la proposizione 9.1-(ii) si può dunque affermare che $(c) = (d)$ e questo permette di concludere, per arbitrarietà nella scelta dell'ideale principale proprio $(d) \lhd R$ con $(c) \subseteq (d)$, che (c) è un elemento massimale nell'insieme di tutti gli ideali principali propri di R.

(iii) Innanzitutto, le condizioni $c \neq 0$ e $c \notin U(R)$ derivano dall'ipotesi che $(c) \lhd R$ sia un ideale proprio perché, come al solito, vale che $c \neq R$ se e solo se $c \notin U(R)$. Siano ora $a, b \in R$ due elementi fissati tali che $c = a \cdot b$. Se fosse $a = 0$, allora anche $c = 0$ per la proposizione 6.1-(i), ma questo è assurdo e quindi $a \neq 0$. Adesso, applicando la definizione 9.1-(i), si deduce che $a \mid c$ e in particolare, per la proposizione 9.1-(i) segue in particolare la condizione $(c) \subseteq (a)$. A questo punto, poiché si assume che (c) sia un elemento massimale nell'insieme degli ideali principali propri di R ed essendo $a \neq 0$, si possono distinguere due possibilità, a seconda che $(a) = R$ oppure che $(a) = (c)$. Nel primo caso si ha, come al solito, che $a \in U(R)$. Se invece $(a) = (c)$ allora, per la proposizione 9.1-(ii), vale che $a \sim c$. Ricordando che, per la proposizione 9.1-(iv), l'essere elementi associati è una relazione di equivalenza, è equivalente richiedere che valga $c \sim a$ anziché $a \sim c$ e dunque, utilizzando l'ipotesi che R sia un dominio integrale assieme alla proposizione 9.1-(vi), si ottiene che $a, c \neq 0$ e che esiste un elemento $v \in U(R)$ tale che $c = a \cdot v$. Adesso, usando nuovamente il fatto che R è un dominio integrale assieme alle relazioni $c = a \cdot b$, $a \neq 0$ e applicando infine la legge di cancellazione sinistra (osservazione 6.6-(ii)), si ottiene che $b = v$ e in particolare $b \in U(R)$. Ricapitolando, assegnati in maniera arbitraria due elementi $a, b \in R$ tali che $c = a \cdot b$, si ha che $a \in U(R)$ oppure $b \in U(R)$ e posso dunque concludere, in virtù della definizione 9.2-(ii), che $c \in R$ è un elemento irriducibile.

(iv) Innanzitutto, dato che per ipotesi $p \in R$ è un elemento primo, per la definizione 9.2-(i) si hanno le condizioni $p \neq 0$ e $p \notin U(R)$. Siano dunque fissati $a, b \in R$ tali che $p = a \cdot b$. Naturalmente, si ha in particolare che $p \mid a \cdot b$ e quindi, per l'ipotesi che $p \in R$ sia un elemento primo, dovrà valere che $p \mid a$ oppure $p \mid b$. Posso supporre, senza perdita di generalità, che $p \mid a$, cioè che esista un qualche elemento $c \in R$ tale che $a = p \cdot c$. A questo punto, combinando le due relazioni $p = a \cdot b$ e $a = p \cdot c$, si ottiene che $p = p \cdot (c \cdot b)$. Usando l'ipotesi che R sia un dominio integrale assieme alla condizione $p \neq 0$ e alla legge di cancellazione sinistra (osservazione 6.6-(ii)), posso affermare che $c \cdot b = 1$ e in particolare si ottiene che $b \in U(R)$. Questo dimostra, per arbitrarietà nella scelta di $a, b \in R$ tali che $p = a \cdot b$, che $p \in R$ è un elemento irriducibile.

(v) Sia $d \in R$ un fattore di c cioè, secondo la definizione 9.1-(iii), un elemento tale che $d \mid c$. In virtù della definizione 9.1-(i), esiste $x \in R$ tale che $c = d \cdot x$. Dato che per ipotesi $c \in R$ è un elemento irriducibile vi sono due possibilità, a seconda che $d \in U(R)$ oppure che $x \in U(R)$. Osservo che, se $x \in U(R)$, allora $c \sim d$ per la proposizione 9.1-(v). In definitiva, poiché il risultato ottenuto non dipende da una particolare scelta del fattore $d \in R$ di c, posso concludere che ogni fattore di c è un elemento invertibile di R oppure un elemento associato a c. Le due condizioni $c \neq 0$ e $c \notin U(R)$ derivano banalmente dall'ipotesi che $c \in R$ sia un elemento irriducibile e dalla definizione 9.2-(ii).

(vi) Innanzitutto, le condizioni $c \neq 0$ e $c \notin U(R)$ sono date per ipotesi. Siano dunque $a, b \in R$ elementi fissati tali che $c = a \cdot b$. Noto che, se fosse $a = 0$ allora, in virtù della proposizione 6.1-(i), dovrebbe valere anche che $c = 0$, ma questo è assurdo e di conseguenza $a \neq 0$. Dalla relazione $c = a \cdot b$ ricavo

quindi che $a \mid c$, ma per ipotesi c non possiede fattori propri e quindi $a \in U(R)$ oppure $a \sim c$. Nel secondo caso, per la definizione 9.1-(ii), si ha in particolare che $c \mid a$ cioè, per la definizione 9.1-(i), esiste un elemento $x \in R$ tale che $a = c \cdot x$. Ma allora, combinando le relazioni $c = a \cdot b$ e $a = c \cdot x$, si ottiene che $c = c \cdot (x \cdot b)$. Dato che per ipotesi R è un dominio integrale e $c \neq 0$, posso applicare la legge di cancellazione sinistra, in virtù della quale $x \cdot b = 1$ e in particolare $b \in U(R)$. Ottengo quindi che, comunque assegnati due elementi $a, b \in R$ tali che $c = a \cdot b$, vale che $a \in U(R)$ oppure $b \in U(R)$ e questo dimostra, per la definizione 9.2-(ii), che $c \in R$ è un elemento irriducibile. □

Esempio 9.2. La proposizione 9.2-(iv) è in generale falsa se non si assume che R sia un dominio integrale. Basta infatti considerare l'anello $\mathbb{Z}_6$ come nell'esempio 9.1, nel quale si è dimostrato che $\bar{2}$ è un elemento primo ma non irriducibile di $\mathbb{Z}_6$. Si osservi che $\mathbb{Z}_6$ non è un dominio integrale e dunque l'esempio 9.1 non contraddice la proposizione 9.2-(iv). Si vede facilmente, infatti, che $\bar{2}$ è un divisore dello zero non banale.

Osservazione 9.3. Sia R un anello commutativo con identità $1 \neq 0$ e siano $x, y \in R$ con $x \sim y$.

(i) Se $x \in R$ è un elemento primo, allora anche $y \in R$ è un elemento primo.

(ii) Se $x \in R$ è un elemento irriducibile, allora anche $y \in R$ è un elemento irriducibile.

Dimostrazione.

(i) In virtù della proposizione 9.2-(i), se $x \in R$ è un elemento primo, allora $(x) \lhd R$ è un ideale primo non nullo. Poiché si assume che $x \sim y$, dalla proposizione 9.1-(ii) segue la condizione $(x) = (y)$. In particolare, anche $(y) \lhd R$ è un ideale primo non nullo quindi, di nuovo per la proposizione 9.2, posso concludere che $y \in R$ è un elemento primo.

(ii) Siano $a, b \in R$ elementi fissati tali che $y = a \cdot b$. Poiché per ipotesi $x \sim y$, dalla definizione 9.1-(ii) segue in particolare che $y \mid x$ e quindi, per la definizione 9.1-(i), esiste un elemento $c \in R$ tale che $x = y \cdot c$. Poiché si assume che $y = a \cdot b$, dalla relazione precedente si deduce che $x = a \cdot (b \cdot c)$ ma, essendo $x \in R$ un elemento irriducibile, dovrà valere che $a \in U(R)$ oppure $b \cdot c \in U(R)$. Dunque, se $a \notin U(R)$, ricordando che per ipotesi R è un anello commutativo, deve esistere un certo $d \in R$ tale che $(b \cdot c) \cdot d = 1$. In particolare, anche $b \in U(R)$ perché $b^{-1} = c \cdot d$ e posso quindi concludere, per arbitrarietà nella scelta degli elementi $a, b \in R$, che $y \in R$ è un elemento irriducibile. □

9.1 Domini a fattorizzazione unica

Definizione 9.3. Un dominio integrale R viene detto un *dominio a fattorizzazione* se ogni suo elemento non banale e non invertibile ammette una decomposizione (o fattorizzazione) in irriducibili cioè se, fissato $a \in R$ con $a \neq 0$ e con $a \notin U(R)$, esistono elementi irriducibili $c_1, \ldots, c_n \in R$ tali che $a = c_1 \cdots c_n$. Si dice invece che in R vale l'*unicità della fattorizzazione* se la decomposizione in irriducibili di un suo elemento fissato, qualora essa esista, è unica a meno di riordinamento e relazioni di associazione. Più precisamente questo significa che, dato un elemento $a \in R$, se $a = c_1 \cdots c_n$, $a = d_1 \cdots d_m$ sono due fattorizzazioni di a in irriducibili, allora $n = m$ ed esiste una permutazione $\sigma \in S_n$ tale che $c_i \sim d_{\sigma(i)}$ per ogni indice $1 \leq i \leq n$. Inoltre, un dominio a fattorizzazione nel quale vale l'unicità della fattorizzazione viene detto un *dominio a fattorizzazione unica*.

Definizione 9.4. Siano R un dominio a fattorizzazione unica, $a \in R$, $a \neq 0$, $a \notin U(R)$ e sia $a = c_1 \cdots c_n$ una decomposizione di a in irriducibili. L'intero positivo n viene detto la *lunghezza della fattorizzazione*, mentre gli elementi $c_1, \ldots, c_n \in R$ prendono il nome di *fattori irriducibili di* a.

Osservazione 9.4. Siano R un dominio a fattorizzazione unica, $a \in R$, $a \neq 0$, $a \notin U(R)$ e sia $a = c_1 \cdots c_n$ una decomposizione di a in irriducibili. Combinando le definizioni 9.3 e 9.4 si ricava che la lunghezza della fattorizzazione considerata è unica, mentre i fattori irriducibili lo sono a meno di relazioni di associazione.

Osservazione 9.5. Sia R un dominio a fattorizzazione unica e sia $a \in R$, $a \neq 0$, $a \notin U(R)$. Allora esistono $u \in U(R)$, elementi irriducibili $p_1, \ldots, p_s \in R$ a due a due non associati, $e_1, \ldots, e_s \in \mathbb{N}^*$ tali che si abbia:

$$a = u \cdot p_1^{e_1} \cdots p_s^{e_s}$$

Dimostrazione. Poiché si assume che R sia un dominio a fattorizzazione unica, che $a \neq 0$ e che $a \notin U(R)$, l'elemento a ammette una decomposizione in irriducibili $a = c_1 \cdots c_n$. Procedo quindi per induzione sulla lunghezza $n \in \mathbb{N}^*$ della fattorizzazione. La base di induzione, che corrisponde al caso $n = 1$, è ovvia perché $a = c_1$ è una fattorizzazione di a in irriducibili. Per la precisione, l'asserto vale prendendo $u := 1$, $p_1 := c_1$, $e_1 := 1$. Nel passo di induzione, assumo $n \geq 2$ e suppongo che ogni elemento non banale e non invertibile di R con una fattorizzazione di lunghezza $n-1$ si possa esprimere nella forma desiderata. Pongo dunque $b := c_1 \cdots c_{n-1}$ in modo tale che $b = c_1 \cdots c_n$ sia, per costruzione, una decomposizione di b in irriducibili. Dall'ipotesi induttiva segue quindi che esistono $v \in U(R)$, elementi irriducibili $p_1, \ldots, p_r \in R$ a due a due non associati, $d_1, \ldots, d_r \in \mathbb{N}^*$ tali che valga la relazione $b = v \cdot p_1^{d_1} \cdots p_r^{d_r}$. Adesso, essendo $a = b \cdot c_n$ per costruzione, basta distinguere due casi, a seconda che c_n sia associato o meno a un fattore irriducibile di b. Se $c_n \not\sim p_i$ per ogni $1 \leq i \leq n$ allora, definendo $u := v$, $s := r+1$, $p_s := c_n$, $e_i := d_i$ per ogni $1 \leq i \leq r$ e $e_s := 1$, ricordando che per ipotesi R è un dominio a fattorizzazione unica, quindi un anello commutativo, si ha la tesi. Se invece $c_n \sim p_i$ per un certo $1 \leq i \leq n$ allora, per la proposizione 9.1-(vi), esiste $u_i \in U(R)$ tale che $c_n = p_i \cdot u_i$. Anche in questo caso l'asserto discende immediatamente dal fatto che R è un anello commutativo, ponendo $u := v \cdot u_i$, $s := r$, $e_j := d_j$ per ogni $1 \leq j \leq s$ con $j \neq i$ e $e_i := d_i + 1$. □

Definizione 9.5. Siano R un dominio a fattorizzazione unica, $a \in R$, $a \neq 0$, $a \notin U(R)$, $a = u \cdot p_1^{e_1} \cdots p_s^{e_s}$ con $u \in U(R)$, $p_1, \ldots, p_s \in R$ elementi irriducibili a due a due non associati e con $e_1, \ldots, e_s \in \mathbb{N}^*$. Per ogni scelta di un indice $1 \leq i \leq s$, l'intero positivo e_i prende il nome di *molteplicità di p_i in a* e si denota $m_a(p_i)$.

Esempio 9.3. Un esempio di dominio a fattorizzazione unica è fornito dall'anello $\mathbb{Z}$. Tenendo a mente gli esempi 1.9 e 9.1 e applicando l'osservazione 9.5 si ottiene che, comunque assegnato $n \in \mathbb{Z}$, esistono numeri primi $p_1, \ldots, p_s$ a due a due distinti ed esistono $e_1, \ldots, e_s \in \mathbb{N}^*$ tali che $n = \pm p_1^{e_1} \cdots p_s^{e_s}$.

Definizione 9.6. Sia R un dominio integrale e siano $a, b \in R$ non entrambi nulli. Un elemento $d \in R$ si dice un *massimo comune divisore di a e b* e si denota $\mathrm{MCD}(a, b)$ se sono verificate le condizioni seguenti:

D1 $d \mid a$ e $d \mid b$.

D2 Per ogni $d' \in R$ tale che $d' \mid a$ e $d' \mid b$, vale che $d' \mid d$.

Un elemento $m \in R$ è invece detto un *minimo comune multiplo di a e b* e si denota $\mathrm{mcm}(a, b)$ se soddisfa:

M1 $a \mid m$ e $b \mid m$.

M2 Per ogni $m' \in R$ tale che $a \mid m'$ e $b \mid m'$, vale che $m \mid m'$.

Per ogni $a \in R$, si definiscono inoltre per convenzione $\mathrm{MCD}(0, 0) := 0$ e $\mathrm{mcm}(a, 0) := 0$.

Osservazione 9.6. Sia R un dominio integrale e siano $a, b \in R$. Dalla definizione 9.6 segue assai facilmente che il massimo comune divisore e il minimo comune multiplo di a e b, qualora esistano, sono unici a meno di relazioni di associazione. Siano infatti c e d due massimi comuni divisori di a e b. Siccome $c \mid a$ e $c \mid b$, si deve avere che $c \mid d$ ma allora, scambiando i ruoli di c e d, si ottiene anche che $d \mid c$ e quindi $c \sim d$ per la definizione 9.1-(ii). Per il minimo comune multiplo di a e b basta applicare un ragionamento identico.

Osservazione 9.7. Sia R un dominio integrale tale che, comunque siano fissati $a, b \in R$, esista $\mathrm{MCD}(a, b)$.

(i) Per ogni $a, a', b, b' \in R$ con $a \sim a'$, $b \sim b'$ vale che $\mathrm{MCD}(a, b) \sim \mathrm{MCD}(a', b')$.

(ii) Per ogni $a, x \in R$ con $a \neq 0$ vale che $\mathrm{MCD}(a, a \cdot x) \sim a$.

Dimostrazione.

(i) Siano $a, a', b, b' \in R$ con $a \sim a'$, $b \sim b'$ e siano $d := \mathrm{MCD}(a, b)$, $d' := \mathrm{MCD}(a', b')$. Una immediata conseguenza delle ipotesi è che d e d' sono due elementi di R ben definiti. Inoltre, poiché si assume che $a \sim a'$, $b \sim b'$, per la definizione 9.1 vale in particolare che $a, a', b, b' \neq 0$ e di conseguenza, per la definizione 9.6, anche $d, d' \neq 0$. Dalla definizione 9.6-D1 segue dunque che $d \mid a$ e $d \mid b$, mentre $a \mid a'$ e $b \mid b'$ in virtù della definizione 9.1-(ii), ma allora $d \mid a'$ e $d \mid b'$ in quanto la divisibilità è una relazione transitiva (osservazione 9.2). Dalla definizione 9.6-D2 si deduce quindi che $d \mid d'$. Con un procedimento essenzialmente identico si dimostra che $d' \mid d$ e posso dunque concludere che $d \sim d'$.

(ii) Siano $a, x \in R$ con $a \neq 0$ due elementi fissati e sia $d := \mathrm{MCD}(a, a \cdot x)$. Innanzitutto, dalle ipotesi segue che $d \in R$ è un elemento ben definito. Inoltre, poiché si assume che $a \neq 0$, anche $d \neq 0$ per la definizione 9.6. In particolare, per la definizione 9.6-D1 si ha che $d \mid a$. Si osservi adesso che $a \mid a$ e $a \mid a \cdot x$ banalmente, infatti $a = a \cdot 1$ e $a \cdot x = a \cdot x$, ma allora $a \mid d$ in virtù della definizione 9.6-D2 e posso dunque concludere che $d \sim a$ per la definizione 9.1-(ii). □

Proposizione 9.3 (Proprietà di un dominio a fattorizzazione unica)**.** *Sia R un dominio a fattorizzazione unica. Valgono le seguenti affermazioni.*

(i) *Siano $a, b \in R$, $a, b \neq 0$, $a, b \notin U(R)$ e siano $a = c_1 \cdots c_n$, $b = d_1 \cdots d_m$ due decomposizioni di a e b in irriducibili. Se $b \mid a$, allora $m \leq n$ ed esiste una permutazione $\sigma \in S_n$ tale che $d_i \sim c_{\sigma(i)}$ per ogni $1 \leq i \leq m$. In altre parole, ciascun fattore irriducibile di b è associato a un fattore irriducibile di a.*

(ii.a) (Condizione sulla catena discendente di fattori propri)**.** *Non esistono catene discendenti infinite di fattori propri in R, cioè non esiste una catena infinita $\{ \cdots \mid a_3 \mid a_2 \mid a_1 \} \subseteq R$ tale che a_{i+1} sia un fattore proprio di a_i per ogni $i \in \mathbb{N}^*$.*

(ii.b) (Condizione sulla catena ascendente di ideali principali)**.** *Non esistono catene ascendenti proprie infinite di ideali principali in R, cioè non esiste una catena infinita $\{ (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \}$.*

(iii) *Sia $c \in R$ un elemento irriducibile. Allora $c \in R$ è un elemento primo.*

(iv) *Comunque vengano assegnati due elementi $a, b \in R$, esiste* $\mathrm{MCD}(a, b)$.

Dimostrazione.

(i) Se $b \mid a$ allora, per la definizione 9.1-(i), esiste un elemento $x \in R$ tale che $a = b \cdot x$. Distinguo due possibilità, a seconda che x sia o meno un elemento invertibile di R. Se $x \in U(R)$, allora definisco $d'_m := d_m \cdot x$, in modo tale che $a = c_1 \cdots c_n$ e $a = d_1 \cdots d'_m$ siano fattorizzazioni di a in irriducibili. Dato che per ipotesi R è un dominio a fattorizzazione unica, in virtù della definizione 9.3 vale che $n = m$ ed esiste una permutazione $\sigma \in S_n$ tale che $d_i \sim c_{\sigma(i)}$ per ogni $1 \leq i \leq m-1$, $d'_m \sim c_{\sigma(m)}$. Ricordando ora che $x \in U(R)$, per la proposizione 9.1-(v) si ha che $d'_m \sim d_m$ e dunque, usando il fatto che l'essere elementi associati è una relazione di equivalenza, quindi simmetrica e transitiva (proposizione 9.1-(iv)), si può concludere che $d_m \sim c_{\sigma(m)}$ e si ottiene la tesi. Se invece $x \notin U(R)$, noto che $x \neq 0$. Infatti, se fosse $x = 0$, allora anche $a = 0$ per la proposizione 6.1-(i) e in virtù della relazione $a = b \cdot x$, dunque si ha una contraddizione con le ipotesi. Essendo $x \neq 0$, $x \notin U(R)$, per la definizione 9.3 esiste una decomposizione in irriducibili $x = e_1 \cdots e_s$ ma allora, usando il fatto che $a = b \cdot x$, posso affermare che $a = c_1 \cdots c_n$ e $a = d_1 \cdots d_m \cdot e_1 \cdots e_s$ sono decomposizioni di a in irriducibili. Nuovamente per l'ipotesi che R sia un dominio a fattorizzazione unica, si ricava che $n = m + s$ ed esiste una permutazione $\sigma \in S_n$ tale che $d_i \sim c_{\sigma(i)}$ per ogni $1 \leq i \leq m$, $e_i \sim c_{\sigma(m+i)}$ per ogni $1 \leq i \leq s$. In particolare, si ottiene la tesi.

(ii.a) Suppongo per assurdo che esista una catena infinita $\{ \cdots \mid a_3 \mid a_2 \mid a_1 \} \subseteq R$ tale che a_{i+1} sia un fattore proprio di a_i per ogni $i \in \mathbb{N}^*$. In virtù della definizione 9.1, si ha che $a_{i+1} \neq 0$, $a_{i+1} \notin U(R)$ per ogni $i \in \mathbb{N}^*$ e dunque, dato che per ipotesi R è un dominio a fattorizzazione unica, ciascuno di tali elementi ammette una decomposizione in irriducibili. Per ogni $i \in \mathbb{N}^*$, sia dunque $n(i+1)$ la lunghezza della fattorizzazione di a_{i+1}. Poiché si assume che a_{i+1} sia un fattore proprio di a_i per ogni $i \in \mathbb{N}^*$, per la definizione 9.1 si ha che $a_{i+1} \mid a_i$ e quindi esiste un elemento $x_{i+1} \in R$ tale che $a_i = a_{i+1} \cdot x_{i+1}$. Inoltre, in virtù del punto (i) appena dimostrato, vale che $n(i+2) \leq n(i+1)$ per ogni $i \in \mathbb{N}^*$. Ora si osservi che, se fosse $x_{i+1} \in U(R)$ per un qualche $i \in \mathbb{N}^*$, allora si avrebbe che $a_i \sim a_{i+1}$ per la proposizione 9.1-(v), ma questo contraddice l'assunzione che a_{i+1} sia un fattore proprio di a_i e quindi $x_{i+1} \notin U(R)$. Similmente, se fosse $x_{i+2} = 0$ per un qualche $i \in \mathbb{N}^*$ allora, per la proposizione 6.1-(i) applicata alla relazione $a_{i+1} = a_{i+2} \cdot x_{i+2}$, varrebbe che $a_{i+1} = 0$ e questo è assurdo. Deduco dunque che $x_{i+2} \neq 0$, $x_{i+2} \notin U(R)$ per ogni $i \in \mathbb{N}^*$. Ripetendo il ragionamento fatto nella parte finale della dimostrazione del punto (i) si ottiene che $n(i+2) < n(i+1)$ per ogni $i \in \mathbb{N}^*$. Adesso, posto $n := n(2)$, dalla relazione precedente si ricava assai facilmente, ragionando per induzione su $i \in \mathbb{N}^*$, la formula $n(i+2) < n - i + 1$. Si osservi però che $n(n+2) < 1$ e questo è assurdo in quanto la lunghezza di una fattorizzazione in irriducibili è sempre un intero positivo (definizione 9.4). Dalla contraddizione segue che vale necessariamente quanto volevasi dimostrare.

(ii.b) Suppongo per assurdo che esista una catena infinita $\{ (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \}$ e osservo che, se esistesse un indice $j \in \mathbb{N}^*$ tale che $a_{j+1} = 0$, cioè tale che $(a_{j+1}) = \{0\}$, allora dovrebbe valere che $(a_{j+1}) \subseteq (a_j)$ in quanto $0 \in (a_j)$ essendo $(a_j) \lhd R$ un ideale. Questo contraddice però il fatto che $(a_i) \subsetneq (a_{i+1})$ per ogni $i \in \mathbb{N}^*$ e dunque si dovrà avere che $a_{i+1} \neq 0$ per ogni $i \in \mathbb{N}^*$. Si noti adesso che, comunque assegnato un indice $i \in \mathbb{N}^*$, la condizione $(a_i) \subseteq (a_{i+1})$ con $a_{i+1} \neq 0$ è equivalente a richiedere, in virtù della proposizione 9.1-(i), che $a_{i+1} \mid a_i$. Posso quindi affermare che la catena $\{ \cdots \mid a_3 \mid a_2 \mid a_1 \} \subseteq R$ è una catena discendente infinita di fattori in R. A questo punto, fissato un indice $i \in \mathbb{N}^*$, dimostro che a_{i+1} è un fattore proprio di a_i. Innanzitutto, poiché si assume che $(a_{i+1}) \neq (a_i)$ posso affermare, per la proposizione 9.1-(ii), che $a_{i+1} \not\sim a_i$. Si osservi adesso che, se fosse $a_{i+1} \in U(R)$, allora $1 \in (a_{i+1})$ perché $1 = a_{i+1}^{-1} \cdot a_{i+1}$. Dall'osservazione 7.3 si deduce quindi che $(a_{i+1}) = R$ e in particolare si ottiene la condizione $(a_{i+2}) \subseteq (a_{i+1})$, contraddicendo il fatto che $(a_{i+1}) \subsetneq (a_{i+2})$. Dalla discussione precedente segue che $a_{i+1} \notin U(R)$ e posso quindi affermare che a_{i+1} è un fattore proprio di a_i. Siccome il risultato ottenuto non dipende da una particolare scelta dell'indice $i \in \mathbb{N}^*$, posso infine concludere che $\{ \cdots \mid a_3 \mid a_2 \mid a_1 \}$ è una catena discendente infinita di fattori propri in R, ma questo è assurdo in quanto contraddice il punto (ii.a) appena dimostrato.

(iii) Innanzitutto, poiché per ipotesi $c \in R$ è un elemento irriducibile, valgono per la definizione 9.2-(ii) le condizioni $c \neq 0$ e $c \notin U(R)$. Siano adesso $a, b \in R$ due elementi fissati tali che $c \mid a \cdot b$. In virtù della definizione 9.1-(i), questo significa che esiste un elemento $x \in R$ tale che $a \cdot b = c \cdot x$. Se fosse $x = 0$ allora, per la proposizione 6.1-(i), si avrebbe che $a \cdot b = 0$ ma allora, tenendo a mente che per ipotesi R è un dominio a fattorizzazione unica e quindi, in particolare, un dominio integrale, dovrà valere che $a = 0$ oppure $b = 0$. In particolare, si avrebbe che $c \mid a$ oppure $c \mid b$ in quanto $a = c \cdot 0$ o $b = c \cdot 0$ di nuovo per la proposizione 6.1-(i). Si consideri dunque il caso meno banale in cui $x \neq 0$ e si distinguano due casi, a seconda che x sia o meno un elemento invertibile di R. Se $x \in U(R)$, allora $c \sim c \cdot x$ banalmente e quindi, applicando l'osservazione 9.3-(ii), ottengo che anche $c \cdot x \in R$ è un elemento irriducibile. Essendo $a \cdot b = c \cdot x$, posso affermare che $a \in U(R)$ oppure $b \in U(R)$. Suppongo che $a \in U(R)$ e moltiplico per a^{-1} primo e secondo membro della relazione precedente, ottenendo la condizione $b = c \cdot (x \cdot a^{-1})$. In particolare, dalla definizione 9.1-(i) deduco che $c \mid b$. Se invece $b \in U(R)$ allora, con un procedimento del tutto analogo, si ottiene che $c \mid a$.

Resta ora da analizzare il caso in cui $x \neq 0$ e $x \notin U(R)$. Innanzitutto, se fosse $a = 0$ oppure $b = 0$ allora, in virtù della proposizione 6.1-(i), varrebbe che $c \cdot x = 0$. Poiché si assume che $c, x \neq 0$, per la relazione precedente c e x sono divisori dello zero non banali e quindi si ha una contraddizione con l'ipotesi che R sia un dominio integrale. Si deduce quindi che $a, b \neq 0$. Si osservi adesso che se $a \in U(R)$ allora, procedendo esattamente come nel caso in cui $x \in U(R)$, si ottiene che $c \mid b$ e analogamente, se $b \in U(R)$, allora $c \mid a$. Suppongo dunque che $a, b \notin U(R)$. In questo caso, dato che per ipotesi R è un dominio a fattorizzazione unica, esistono delle fattorizzazioni in irriducibili $a = d_1 \cdots d_n$, $b = e_1 \cdots e_m$, $x = f_1 \cdots f_r$. Dalla condizione $a \cdot b = c \cdot x$ ricavo la relazione seguente:

$$d_1 \cdots d_n \cdot e_1 \cdots e_m = c \cdot f_1 \cdots f_r$$

Dall'unicità della fattorizzazione (definizione 9.3) segue quindi che $n + m = r + 1$ e che $c \sim d_i$ per un qualche $1 \leq i \leq n$ oppure $c \sim e_i$ per un certo $1 \leq i \leq m$. Se $c \sim d_i$ per un opportuno $1 \leq i \leq n$, allora per la definizione 9.1-(ii) si ha che $c \mid d_i$. Dal momento che d_i è un fattore di a cioè, secondo la definizione 9.1-(iii), un elemento tale che $d_i \mid a$ e ricordando che la divisibilità è una relazione transitiva (osservazione 9.2), posso affermare che $c \mid a$. Se invece $c \sim e_i$ per un qualche $1 \leq i \leq m$ allora, con un ragionamento del tutto analogo, si deduce che $c \mid b$. Avendo ottenuto in tutti i casi esaminati che $c \mid a$ oppure $c \mid b$ si può concludere, per arbitrarietà nella scelta di $a, b \in R$ tali che $c \mid a \cdot b$, che $c \in R$ è un elemento primo.

(iv) Siano $a, b \in R$ due elementi fissati e si osservi innanzitutto che, se $a, b = 0$, allora $\mathrm{MCD}(a, b) = 0$ per definizione. Se invece $a = 0$ e $b \neq 0$, allora $b \in R$ è un elemento tale che $b \mid 0$ e $b \mid b$ in quanto $0 = b \cdot 0$ per la proposizione 6.1-(i), mentre $b = b \cdot 1$ per definizione di identità. Inoltre, di nuovo per la proposizione 6.1-(i), ogni elemento non banale di R divide 0, mentre se un dato $d \in R$ divide b, allora $d \mid b$ tautologicamente e posso dunque affermare, in virtù della definizione 9.6, che b è un massimo comune divisore di a e b. Se $a \neq 0$ e $b = 0$ allora, applicando un ragionamento analogo, si può concludere che a è un massimo comune divisore di a e b. Assumo quindi che $a, b \neq 0$ e faccio un'ulteriore distinzione di casi. Suppongo che $a \in U(R)$. In tal caso, valgono le condizioni $a \mid a$ e

$a \mid b$ perché $a = a \cdot 1$, mentre $b = a \cdot (a^{-1} \cdot b)$. Inoltre, assegnato un elemento $d \in R$ tale che $d \mid a$ e $d \mid b$, si ha in particolare che $d \mid a$ e ottengo dunque, per la definizione 9.6, che a è un massimo comune divisore di a e b. Analogamente, se $b \in U(R)$, allora b è un massimo comune divisore di a e b. Si consideri adesso il caso in cui $a, b \neq 0$, $a, b \notin U(R)$. Dal momento che per ipotesi R è un dominio a fattorizzazione unica, per l'osservazione 9.5 esistono $u, v \in U(R)$, elementi irriducibili $p_1, \dots, p_s \in R$ a due a due non associati, $d_1, \dots, d_s, e_1, \dots, e_s \in \mathbb{N}$ tali che valgano le condizioni:

$$a = u \cdot p_1^{d_1} \cdots p_s^{d_s}, \quad b = v \cdot p_1^{e_1} \cdots p_s^{e_s}$$

Per ogni $1 \leq i \leq s$, definisco $f_i := \min\{d_i, e_i\}$ e pongo $c := p_1^{f_1} \cdots p_s^{f_s}$. In questo modo, l'elemento c è per costruzione il massimo comune divisore di a e b. Si noti infatti che $c \mid a$ in quanto vale che:

$$a = u \cdot p_1^{d_1} \cdots p_s^{d_s} = (p_1^{f_1} \cdots p_s^{f_s}) \cdot (u \cdot p_1^{d_1 - f_1} \cdots p_s^{d_s - f_s}) = c \cdot (u \cdot p_1^{d_1 - f_1} \cdots p_s^{d_s - f_s})$$

Analogamente, si ha che $c \mid b$. Sia ora $d \in R$ un elemento fissato tale che $d \mid a$ e $d \mid b$. In virtù della definizione 9.1-(i), si ha che $d \neq 0$. Se fosse $d \in U(R)$, allora varrebbe la condizione $d \mid c$ in quanto $c = d \cdot (d^{-1} \cdot c)$. Suppongo quindi che $d \notin U(R)$. Ricordando che R è un dominio a fattorizzazione unica, in virtù dell'osservazione 9.5 esistono $w \in U(R)$, elementi irriducibili $q_1, \dots, q_r \in R$ a due a due non associati, $g_1, \dots, g_r \in \mathbb{N}^*$ tali che $d = w \cdot q_1^{g_1} \cdots q_r^{g_r}$. Adesso, siccome $d \mid a$, per il punto (i) già dimostrato $r \leq s$ e ogni fattore irriducibile di d è associato a un certo fattore irriducibile di a. Essendo R un anello commutativo posso assumere, a meno di permutare gli indici, che $q_i \sim p_i$ per ogni $1 \leq i \leq r$. Si osservi inoltre che, siccome $p_1, \dots, p_r$ sono elementi a due a due non associati, per ogni $1 \leq i \leq r$ l'elemento q_i è associato soltanto a p_i e di conseguenza $g_i \leq d_i$. Analogamente, dalla condizione $d \mid b$ si ricava, per un fissato indice $1 \leq i \leq r$, che $g_i \leq e_i$ e quindi, ricordando la definizione di f_i, vale che $g_i \leq f_i$. A questo punto, se $q_i \sim p_i$ allora, per la definizione 9.1-(ii), si ha che $q_i \mid p_i$ cioè, per la definizione 9.1-(i), esiste un elemento $x_i \in R$ tale che $p_i = q_i \cdot x_i$. Ricavo che:

$$\begin{aligned} c &= (p_1^{f_1} \cdots p_r^{f_r}) \cdot (p_{r+1}^{f_{r+1}} \cdots p_s^{f_s}) \\ &= \big((q_1^{f_1} \cdot x_1^{f_1}) \cdots (q_r^{f_r} \cdot x_r^{f_r})\big) \cdot (p_{r+1}^{f_{r+1}} \cdots p_s^{f_s}) \\ &= d \cdot (q_1^{f_1 - g_1} \cdots q_r^{f_r - g_r}) \cdot (x_1^{f_1} \cdots x_r^{f_r}) \cdot (p_{r+1}^{f_{r+1}} \cdots p_s^{f_s}) \cdot w^{-1} \end{aligned}$$

Questo dimostra che $d \mid c$. Non dipendendo il risultato ottenuto dalla scelta di $d \in R$ tale che $d \mid a$ e $d \mid b$, si può concludere che c è un massimo comune divisore di a e b per la definizione 9.6. □

Osservazione 9.8. Sia R un dominio a fattorizzazione unica. Tenendo a mente che R è anche un dominio integrale per la definizione 9.3, posso combinare le proposizioni 9.2-(iv) e 9.3-(iii), ottenendo che in R un elemento è primo se e solo se è un elemento irriducibile.

Lemma 9.1. *Sia R un dominio integrale tale che, comunque fissati elementi $a, b \in R$, esista* $\mathrm{MCD}(a, b)$.

(i) *Ogni numero finito di elementi di R non tutti nulli ha un massimo comune divisore cioè, fissati $a_1, \dots, a_n \in R$ non tutti nulli, esiste un elemento $d \in R$ tale che siano verificate le due condizioni:*

  (a) $d \mid a_i$ *per ogni* $1 \leq i \leq n$.

  (b) *Comunque assegnato $d' \in R$ tale che $d' \mid a_i$ per ogni $1 \leq i \leq n$, vale che $d' \mid d$.*

(ii) *Per ogni $a, b, c \in R$ non tutti nulli vale che* $\mathrm{MCD}(\mathrm{MCD}(a, b), c) \sim \mathrm{MCD}(a, \mathrm{MCD}(b, c))$.

(iii) *Per ogni $a, b, c \in R$ con a e b non entrambi nulli, $c \neq 0$ vale che* $\mathrm{MCD}(c \cdot a, c \cdot b) \sim c \cdot \mathrm{MCD}(a, b)$.

(iv) *Per ogni $a, b, c \in R$, se* $\mathrm{MCD}(a, b) \sim 1$ *e se* $\mathrm{MCD}(a, c) \sim 1$, *allora anche* $\mathrm{MCD}(a, b \cdot c) \sim 1$.

Dimostrazione.

(i) Si procede per induzione sul numero $n \in \mathbb{N}$, $n \geq 2$ degli elementi considerati. La base di induzione, cioè il caso $n = 2$, segue banalmente dalle ipotesi. Nel passo di induzione assumo $n \geq 3$, suppongo che la tesi sia vera per un generico $n - 1$ e la dimostro per n. Siano dunque fissati $a_1, \dots, a_n \in R$ non tutti nulli. Per ipotesi induttiva, esiste un certo $a \in R$ tale che $a \mid a_i$ per ogni $1 \leq i \leq n - 1$ e tale che, comunque assegnato $a' \in R$ con $a' \mid a_i$ per ogni $1 \leq i \leq n - 1$, si abbia che $a' \mid a$. Pongo

$b := a_n$ e noto che, per ipotesi, deve esistere $\mathrm{MCD}(a, b)$. Definisco per semplicità $d := \mathrm{MCD}(a, b)$ e noto che $d \neq 0$ in virtù della definizione 9.1-(i). Per costruzione e per transitività della relazione di divisibilità (osservazione 9.2), l'elemento d appena definito soddisfa la condizione (a). Sia adesso $d' \in R$ un elemento prefissato tale che $d' \mid a_i$ per ogni $1 \leq i \leq n$. Siccome in particolare $d' \mid a_i$ per ogni $1 \leq i \leq n-1$, dalle condizioni imposte su a per ipotesi induttiva segue immediatamente che $d' \mid a$, mentre $d' \mid b$ per definizione di b. Di conseguenza, si ha che $d' \mid d$ per la definizione 9.6-D2 e dunque l'elemento d soddisfa anche la condizione (b). Non dipendendo il risultato ottenuto da una particolare scelta degli elementi $a_1, \ldots, a_n \in R$, si ha la tesi.

(ii) Siano $a, b, c \in R$ non tutti nulli e siano $d := \mathrm{MCD}(\mathrm{MCD}(a, b), c)$, $d' := \mathrm{MCD}(a, \mathrm{MCD}(b, c))$. Dalle ipotesi segue che d e d' sono elementi di R ben definiti. Poiché si assume che $a, b, c \in R$ siano non tutti nulli, vale che $d, d' \neq 0$ e dunque, in virtù della definizione 9.6-D1, si ha che $d \mid \mathrm{MCD}(a, b)$ e $d \mid c$. Dal momento che la divisibilità è una relazione transitiva (osservazione 9.2), posso affermare che $d \mid a$ e $d \mid b$, ma allora $d \mid \mathrm{MCD}(b, c)$ per la definizione 9.6-D2 e per la medesima ragione $d \mid d'$. Applicando un procedimento del tutto analogo si dimostra che $d' \mid d$ e si può dunque concludere, per la definizione 9.1-(ii), che $d \sim d'$.

(iii) Siano $a, b, c \in R$ con a e b non entrambi nulli, $c \neq 0$ e siano $d := \mathrm{MCD}(a, b)$, $d' := \mathrm{MCD}(c \cdot a, c \cdot b)$. Per ipotesi, gli elementi d e d' sono ben definiti e inoltre, per le assunzioni fatte su $a, b, c \in R$, essi sono anche non nulli. Dalla definizione 9.6-D1 segue dunque che $d \mid a$ e $d \mid b$ ma questo significa, per la definizione 9.1-(i), che esistono $x, y \in R$ tali che $a = d \cdot x$, $b = d \cdot y$. Moltiplicando a sinistra per c ambo i membri di tali relazioni, si ottiene in particolare che $c \cdot a = (c \cdot d) \cdot x$, $c \cdot b = (c \cdot d) \cdot y$ e dunque, essendo $c, d \neq 0$, si ha che $c \cdot d \mid c \cdot a$ e $c \cdot d \mid c \cdot b$ nuovamente per la definizione 9.1-(i). Dalla definizione 9.6-D2 segue allora che $c \cdot d \mid d'$, cioè che esiste $u \in R$ tale che $d' = (c \cdot d) \cdot u$. A questo punto sarà sufficiente mostrare che $u \in U(R)$. Per la definizione 9.6-D1 si ha che $d' \mid c \cdot a$ e $d' \mid c \cdot b$ quindi, in virtù della definizione 9.1-(i), esistono $r, s \in R$ tali che $c \cdot a = d' \cdot r$, $c \cdot b = d' \cdot s$. Combinando ora le relazioni precedenti e usando l'ipotesi che R sia un dominio integrale, dunque un anello commutativo, si ottengono le due condizioni seguenti:

$$c \cdot a = c \cdot (d \cdot u \cdot r)$$
$$c \cdot b = c \cdot (d \cdot u \cdot s)$$

Tenendo a mente che R è un dominio integrale e che $c \neq 0$, posso applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)), ottenendo che $a = (d \cdot u) \cdot r$, $b = (d \cdot u) \cdot s$. Si osservi che, se fosse $u = 0$, allora $d' = 0$ per la proposizione 6.1-(i) applicata alla relazione $d' = (c \cdot d) \cdot u$, ma questo è assurdo. Di conseguenza, si deve avere che $u \neq 0$. Dato che per ipotesi R è un dominio integrale, in R non esistono divisori dello zero non banali e quindi anche $d \cdot u \neq 0$. Dalla definizione 9.1-(i) segue dunque che $d \cdot u \mid a$ e $d \cdot u \mid b$, ma allora $d \cdot u \mid d$ per la definizione 9.6-D2. Nuovamente per la definizione 9.1-(i), esiste un elemento $v \in R$ tale che $d = (d \cdot u) \cdot v$, ma $d \neq 0$ e per ipotesi R è un dominio integrale, per cui posso applicare di nuovo la legge di cancellazione sinistra ottenendo che $u \cdot v = 1$. In particolare, posso affermare che $u \in U(R)$ e, ricordando che $d' = (c \cdot d) \cdot u$, posso concludere che $d' \sim c \cdot d$ per la proposizione 9.1-(v).

(iv) Siano $a, b, c \in R$ elementi fissati tali che $\mathrm{MCD}(a, b) \sim 1$ e $\mathrm{MCD}(a, c) \sim 1$. Come al solito, è noto per ipotesi che il massimo comune divisore di due elementi qualunque di R esiste. Innanzitutto, si osservi che l'asserto è banale se $a = 0$. In tal caso, infatti, in virtù dell'osservazione 9.7-(ii) si ha che $\mathrm{MCD}(a, b) \sim b$, $\mathrm{MCD}(a, c) \sim c$ e $\mathrm{MCD}(a, b \cdot c) \sim b \cdot c$ per cui bisogna mostrare che, se $b \sim 1$ e se $c \sim 1$, allora anche $b \cdot c \sim 1$, ma questo è ovvio per l'osservazione 9.1. Si può dunque supporre che $a \neq 0$. Ora, tenendo a mente l'ipotesi che R sia un anello commutativo e che $\mathrm{MCD}(a, b) \sim 1$, $\mathrm{MCD}(a, c) \sim 1$, posso usare l'osservazione 9.7 con i punti (ii) e (iii) già dimostrati per ottenere che:

$$\mathrm{MCD}(a, b \cdot c) \sim \mathrm{MCD}\big(\mathrm{MCD}(a, a \cdot c), b \cdot c\big) \sim \mathrm{MCD}\big(a, \mathrm{MCD}(a \cdot c, b \cdot c)\big)$$
$$\sim \mathrm{MCD}\big(a, c \cdot \mathrm{MCD}(a, b)\big) \sim \mathrm{MCD}(a, c) \sim 1$$ □

Teorema 9.1. *Sia R un dominio integrale. Valgono le seguenti affermazioni.*

(i) *Se R soddisfa la condizione sulla catena ascendente di ideali principali, vale a dire se è verificata la proposizione 9.3-(ii.b), allora R è un dominio a fattorizzazione.*

(ii) *Se, comunque vengano assegnati due elementi $a, b \in R$, esiste* $\mathrm{MCD}(a, b)$*, allora in R un elemento è primo se e solo se è un elemento irriducibile.*

(iii) *Se in R un elemento è primo se e solo se è un elemento irriducibile, allora in R vale l'unicità della fattorizzazione.*

Dimostrazione.

(i) Sia $a \in R$, $a \neq 0$, $a \notin U(R)$ un elemento fissato. Innanzitutto, dimostro che a ammette un fattore irriducibile c_1. Chiaramente, se a è irriducibile allora, ponendo $c_1 := a$, si ottiene in modo banale un fattore irriducibile di a. Suppongo quindi che $a \in R$ non sia un elemento irriducibile. In virtù della definizione 9.2-(ii), esistono due elementi $a_1, b_1 \in R$, $a_1, b_1 \notin U(R)$ tali che $a = a_1 \cdot b_1$. Noto che, se fosse $a_1 = 0$, allora anche $a = 0$ per la proposizione 6.1-(i), ma questo è assurdo e dunque $a_1 \neq 0$. Posso quindi affermare, per la definizione 9.1-(i), che $a_1 \mid a$ e questo equivale a richiedere, in virtù della proposizione 9.1-(i), che valga l'inclusione $(a) \subseteq (a_1)$. Si osservi inoltre che, se fosse $(a_1) \subseteq (a)$ allora, di nuovo per la proposizione 9.1-(i) e per il fatto che $a \neq 0$, si avrebbe che $a \mid a_1$ cioè esisterebbe, secondo la definizione 9.1-(i), un elemento $x_1 \in R$ tale che $a_1 = a \cdot x_1$. Ma allora, combinando le relazioni $a = a_1 \cdot b_1$ e $a_1 = a \cdot x_1$, ricavo che $a = a \cdot (x_1 \cdot b_1)$ mentre l'ipotesi che R sia un dominio integrale permette di usare la legge di cancellazione sinistra (osservazione 6.6-(ii)) per ottenere che $x_1 \cdot b_1 = 1$. In particolare, si dovrebbe avere che $b_1 \in U(R)$, ma questo è assurdo. Ho dunque mostrato che $(a) \subsetneq (a_1)$ e che $a_1 \neq 0$. A questo punto, se a_1 è un elemento irriducibile allora, definendo $c_1 := a_1$, ottengo un fattore irriducibile di a. Se invece $a_1 \in R$ non è un elemento irriducibile allora, utilizzando il fatto che $a_1 \neq 0$, posso ripetere la costruzione precedente con a_1 al posto di a, ottenendo che esiste un elemento $a_2 \in R$ con $a_2 \neq 0$ e $a_2 \notin U(R)$ tale che $(a_1) \subsetneq (a_2)$. Suppongo per assurdo che, iterando questo procedimento all'infinito, non esista un indice $i \in \mathbb{N}^*$ tale che $a_i \in R$ sia un elemento irriducibile. Sotto tale condizione, è possibile costruire una catena infinita $\{ (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \}$ e questo contraddice l'ipotesi che R soddisfi la condizione sulla catena ascendente di ideali principali. Deve dunque esistere un indice $N \in \mathbb{N}^*$ tale che $a_N \in R$ sia un elemento irriducibile. Per costruzione, basta dunque definire $c_1 := a_N$ per ottenere un fattore irriducibile di a.

Ora bisogna dimostrare che a ammette una decomposizione in irriducibili. Dalla parte precedente segue che esistono $a_1, c_1 \in R$, con c_1 elemento irriducibile, tali che $a = c_1 \cdot a_1$. Distinguo due casi, a seconda che a_1 sia o meno un elemento invertibile di R. Se $a_1 \in U(R)$, allora $a \sim c_1$ in virtù del fatto che, essendo $a, c_1 \neq 0$, si può utilizzare la proposizione 9.1-(v). Per l'osservazione 9.3-(ii) si può quindi affermare che $a \in R$ è un elemento irriducibile e di conseguenza la decomposizione di a in irriducibili è banale. Si assuma invece che $a_1 \notin U(R)$. Dalla relazione $a = c_1 \cdot a_1$ si ricava assai facilmente che $a_1 \mid a$ in quanto $a_1 \neq 0$. Infatti, se fosse $a_1 = 0$ allora, per la proposizione 6.1-(i), anche $a = 0$ e questo è assurdo. Si osservi adesso che, se fosse $a \sim a_1$, allora dovrebbe esistere, per la proposizione 9.1-(vi), un elemento $v \in U(R)$ tale che $a = a_1 \cdot v$. Combinando tale relazione con $a = c_1 \cdot a_1$ e usando il fatto che R è un anello commutativo, si ottiene che $a_1 \cdot c_1 = a_1 \cdot v$. Poiché per ipotesi R è un dominio integrale ed essendo $a_1 \neq 0$, si può applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)), ottenendo la relazione $c_1 = v$ e in particolare $c_1 \in U(R)$, ma questo è assurdo e di conseguenza si deve necessariamente avere che $a \not\sim a_1$. Si osservi adesso che le due condizioni $a_1 \mid a$ e $a_1 \not\sim a$ sono equivalenti a richiedere, per la proposizione 9.1, che $(a) \subsetneq (a_1)$ con $a_1 \neq 0$. A questo punto osservo che, per la prima parte della dimostrazione con a_1 al posto di a, esistono $a_2, c_2 \in R$, con c_2 elemento irriducibile, tali che $a_1 = c_2 \cdot a_2$. Posso distinguere di nuovo due possibilità: se $a_2 \in U(R)$ allora, ragionando esattamente come prima, si ottiene che $a_1 \in R$ è un elemento irriducibile e dunque $a = c_1 \cdot a_1$ è una decomposizione di a in irriducibili. Se invece $a_2 \notin U(R)$ allora, dal momento che $a_1 \neq 0$, posso ripetere l'argomento seguito prima, ottenendo la condizione $(a_1) \subsetneq (a_2)$ con $a_2 \neq 0$. Ora suppongo per assurdo che, iterando questo procedimento all'infinito, nessun indice $i \in \mathbb{N}^*$ sia tale che $a_i \in U(R)$. In tal caso, si può considerare una catena infinita $\{ (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \}$, ma questo contraddice l'ipotesi che R verifichi la condizione sulla catena ascendente di ideali principali. Deduco quindi l'esistenza di un indice $N \in \mathbb{N}^*$ tale che $a_N \in U(R)$. Dalla costruzione precedente segue che $a = c_1 \cdots c_{N-1} \cdot a_{N-1}$ è una decomposizione di a in irriducibili e dunque si ha la tesi.

(ii) Innanzitutto, poiché per ipotesi R è un dominio integrale, in virtù della proposizione 9.2-(iv) ogni elemento primo in R è anche un elemento irriducibile. Sarà quindi sufficiente mostrare che ciascun

elemento irriducibile in R è primo. Fissato un elemento irriducibile $c \in R$, si intende procedere per contrapposizione logica. Assegnati quindi $a, b \in R$ tali che $c \nmid a$ e $c \nmid b$, l'obiettivo è dimostrare che $c \nmid a \cdot b$. Innanzitutto, se fosse $a = 0$ oppure $b = 0$, allora varrebbe che $c \mid a$ oppure $c \mid b$ in quanto $0 = c \cdot 0$ per la proposizione 6.1-(i) e quindi si ha una contraddizione. Di conseguenza, deve valere necessariamente che $a, b \neq 0$. Volendo mostrare che $\text{MCD}(a, c) \sim 1$, noto che l'identità soddisfa la definizione 9.6-D1 perché, essendo $a = 1 \cdot a$, $c = 1 \cdot c$ con $1 \neq 0$, per la definizione 9.1-(i) valgono le condizioni $1 \mid a$ e $1 \mid c$. Sia adesso $d \in R$ un elemento fissato tale che $d \mid a$ e $d \mid c$. Di nuovo per la definizione 9.1-(i), esistono due elementi $x, y \in R$ tali che $a = d \cdot x$, $c = d \cdot y$. Poiché si assume che $c \in R$ sia un elemento irriducibile, dovrà valere che $d \in U(R)$ oppure $y \in U(R)$. Se $y \in U(R)$, allora $d = c \cdot y^{-1}$ e posso quindi affermare, in virtù del fatto che $c \neq 0$ essendo $c \in R$ un elemento irriducibile, che $c \mid d$. Ma allora, per transitività della relazione di divisibilità (osservazione 9.2), si ottiene che $c \mid a$ e questo è assurdo. Non essendo dunque $y \in U(R)$, si deve necessariamente avere che $d \in U(R)$. In particolare, vale che $d \mid 1$ in quanto $1 = d \cdot d^{-1}$ e posso quindi affermare, per la definizione 9.6-D2, che $\text{MCD}(a, c) \sim 1$. Applicando un argomento del tutto analogo e utilizzando l'ipotesi che $c \nmid b$, si dimostra anche che $\text{MCD}(b, c) \sim 1$ e dunque, in virtù del lemma 9.1-(iv) e per l'ovvia simmetria del massimo comune divisore, si ha che $\text{MCD}(a \cdot b, c) \sim 1$. Ora, se per assurdo $c \mid a \cdot b$ allora, per la definizione 9.1-(i), esiste un qualche $z \in R$ tale che $a \cdot b = c \cdot z$ ma allora, per l'osservazione 9.7-(ii) e in virtù del fatto che $c \neq 0$, si ha che $\text{MCD}(a \cdot b, c) \sim c$. Tenendo a mente che, per la proposizione 9.1-(iv), l'essere associati è una relazione di equivalenza e, in particolare, una relazione transitiva, ottengo che $c \sim 1$ ma questo, per l'osservazione 9.1, equivale a richiedere che $c \in U(R)$. Questo contraddice l'ipotesi che $c \in R$ sia un elemento irriducibile e di conseguenza dovrà necessariamente valere la condizione $c \nmid a \cdot b$. Posso quindi concludere, per arbitrarietà nella scelta dei due elementi $a, b \in R$ tali che $c \nmid a$ e $c \nmid b$ e per contrapposizione logica, che $c \in R$ è un elemento primo. Siccome il risultato ottenuto non dipende da una particolare scelta dell'elemento irriducibile $c \in R$, si ha la tesi.

(iii) Sia $a \in R$ un fissato elemento che ammette una decomposizione in irriducibili e siano $a = c_1 \cdots c_n$, $a = d_1 \cdots d_m$ fattorizzazioni di a in irriducibili. Si procede per induzione sulla lunghezza $n \in \mathbb{N}^*$ della prima fattorizzazione. Nella base di induzione, corrispondente al caso $n = 1$, vale che $a = c_1$ e in particolare $a \in R$ è un elemento irriducibile. Se fosse $m > 1$ allora, poiché $a = d_1 \cdot (d_2 \cdots d_m)$, per la definizione 9.2-(ii) si dovrebbe avere che $d_1 \in U(R)$ oppure $d_2 \cdots d_m \in U(R)$. La possibilità che $d_1 \in U(R)$ va scartata in quanto $d_1 \in R$ è un elemento irriducibile e dunque $d_2 \cdots d_m \in U(R)$. Essendo R un anello commutativo, questo significa che esiste $x \in R$ tale che $(d_2 \cdots d_m) \cdot x = 1$, ma allora anche $d_2 \in U(R)$ e questo contraddice il fatto che $d_2 \in R$ è un elemento irriducibile. Deduco quindi che $m = 1$ e che $c_1 = d_1$. Nel passo induttivo assumo $n \geq 2$ e suppongo che ogni elemento di R con una decomposizione in irriducibili di lunghezza $n - 1$ ammetta una fattorizzazione unica a meno di riordinamento e relazioni di associazione. Si osservi che $d_1 \mid a$ in quanto $d_1 \neq 0$ per la definizione 9.2-(ii) e $a = d_1 \cdot (d_2 \cdots d_m)$ ma, dato che per ipotesi un elemento in R è primo se e solo se è un elemento irriducibile e dal momento che $a = c_1 \cdots c_n$, deve esistere un indice $1 \leq i \leq n$ tale che $d_1 \mid c_i$. A meno di riordinare i fattori irriducibili $c_1, \ldots, c_n$ di a, posso supporre senza perdita di generalità che $d_1 \mid c_1$ e questo significa, per la definizione 9.1-(i), che esiste un elemento $u \in R$ tale che $c_1 = d_1 \cdot u$. Essendo $c_1 \in R$ un elemento irriducibile, si dovrà avere che $d_1 \in U(R)$ oppure $u \in U(R)$, ma anche $d_1 \in R$ è un elemento irriducibile e dunque, in virtù della definizione 9.2-(ii), deve necessariamente valere che $u \in U(R)$. Dalle decomposizioni in irriducibili di a si deduce che:

$$d_1 \cdot (d_2 \cdots d_m) = a = c_1 \cdot (c_2 \cdots c_n) = d_1 \cdot (u \cdot c_2 \cdots c_n)$$

Dal momento che per ipotesi R è un dominio integrale ed essendo $d_1 \neq 0$, posso applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)) per ottenere che $u \cdot c_2 \cdots c_n = d_2 \cdots d_m$. Posto ora $c_2' := c_2 \cdot u$, per la proposizione 9.1-(v) si ha che $c_2' \sim c_2$ e quindi, per l'osservazione 9.3-(ii), anche $c_2' \in R$ è un elemento irriducibile. Si noti adesso che l'elemento $c_2' \cdots c_n$ ammette banalmente una decomposizione in irriducibili di lunghezza $n - 1$ e quindi, per ipotesi induttiva, vale la condizione $n - 1 = m - 1$ ed esiste una permutazione $\sigma \in S_{n-1}$ tale che $c_i \sim d_{\sigma(i)}$ per ogni indice $3 \leq i \leq n$ e tale che $c_2' \sim d_{\sigma(2)}$. Tenendo a mente che l'essere elementi associati è una relazione di equivalenza per la proposizione 9.1-(iv), anche $c_2 \sim d_{\sigma(2)}$, mentre $c_1 \sim d_1$ in virtù del fatto che $c_1 = d_1 \cdot u$ con $u \in U(R)$ assieme alla proposizione 9.1-(v). Questo permette di concludere la dimostrazione. □

Dal teorema 9.1 deriva immediatamente il seguente corollario.

Corollario 9.1. *Sia R un dominio integrale. Allora R è un dominio a fattorizzazione unica se e solo se:*

(i) *R soddisfa la condizione sulla catena ascendente di ideali principali, cioè la proposizione 9.3-(ii.b).*

(ii) *In R un elemento è primo se e solo se è un elemento irriducibile oppure, comunque vengano fissati due elementi $a, b \in R$, esiste* $\mathrm{MCD}(a, b)$.

Osservazione 9.9. Molti anelli di interesse in geometria algebrica e aritmetica soddisfano la proprietà della catena ascendente su tutti gli ideali, non solo su quelli principali. Un anello che goda di tale proprietà si dice un "anello noetheriano". Dal teorema 9.1-(i) segue immediatamente che ogni dominio noetheriano è un dominio a fattorizzazione, nel quale tuttavia non si ha necessariamente l'unicità della fattorizzazione. Un esempio è dato dai cosiddetti "anelli di tipo finito" su un campo K oppure su $\mathbb{Z}$, vale a dire anelli della forma $K[X_1, \ldots, X_n]/I$ oppure $\mathbb{Z}[X_1, \ldots, X_n]/I$, dove I è un ideale di $K[X_1, \ldots, X_n]$ o di $\mathbb{Z}[X_1, \ldots, X_n]$.

Osservazione 9.10. Siano R un dominio integrale, $a, b \in R$. Allora le seguenti condizioni sono equivalenti:

(i) Esiste $\mathrm{mcm}(a, b)$.

(ii) Per ogni $r \in R$ con $r \neq 0$, esiste $\mathrm{MCD}(r \cdot a, r \cdot b)$.

Se inoltre una di tali condizioni equivalenti è soddisfatta e se $a, b \neq 0$, allora $\mathrm{MCD}(a, b) \cdot \mathrm{mcm}(a, b) \sim a \cdot b$.

Dimostrazione. Si osservi innanzitutto che, se $a = 0$ e $b = 0$ allora, per la definizione 9.6 e in virtù della proposizione 6.1-(i), esiste $\mathrm{mcm}(a, b)$ e, per ogni $r \in R$ con $r \neq 0$, esiste $\mathrm{MCD}(r \cdot a, r \cdot b)$, dunque non vi è nulla da dimostrare. Se invece $a = 0$ oppure $b = 0$ allora posso supporre, per l'ovvia simmetria del minimo comune multiplo e del massimo comune divisore, che $b = 0$. Sotto tale condizione, vale per definizione che $\mathrm{mcm}(a, b) = 0$. Si osservi ora che $a \mid a$ e $a \mid 0$ banalmente, in quanto $a = a \cdot 1$ e $0 = a \cdot 0$ per definizione di identità e in virtù della proposizione 6.1-(i). D'altra parte, comunque fissato un elemento $d \in R$ tale che $d \mid a$ e $d \mid 0$, in particolare $d \mid a$ e posso quindi affermare, per la definizione 9.6, che a è un massimo comune divisore di a e b.

Si consideri adesso il caso non banale in cui $a, b \neq 0$. Innanzitutto, dimostro l'implicazione (i) $\implies$ (ii). Pongo per semplicità $m := \mathrm{mcm}(a, b)$ e osservo che m è un elemento di R ben definito per ipotesi. Dalla definizione 9.6-M1 e dall'assunzione che $a, b \neq 0$ segue che $a \mid m$ e $b \mid m$ e quindi, per la definizione 9.1-(i), esistono due elementi $x, y \in R$ tali che $m = a \cdot x$, $m = b \cdot y$. Siccome $a \mid a \cdot b$ e $b \mid a \cdot b$ banalmente, per la definizione 9.6-M2 si ha che $m \mid a \cdot b$ e questo, nuovamente per la definizione 9.1-(i), significa che esiste un elemento $d \in R$ tale che $a \cdot b = m \cdot d$. Si osservi adesso che valgono le due condizioni seguenti:

$$a \cdot m = a \cdot (b \cdot y) = (a \cdot b) \cdot y = (m \cdot d) \cdot y = (d \cdot y) \cdot m$$
$$b \cdot m = b \cdot (a \cdot x) = (a \cdot b) \cdot x = (m \cdot d) \cdot x = (d \cdot x) \cdot m$$

Utilizzando l'ipotesi che R sia un dominio integrale assieme al fatto che $m \neq 0$, posso applicare la legge di cancellazione destra (osservazione 6.6-(ii)) per ottenere che $a = d \cdot y$, $b = d \cdot x$. Ovviamente, se fosse $d = 0$ allora, per la proposizione 6.1-(i), si avrebbe che $a = 0$ e $b = 0$, ma questo è assurdo e dunque $d \neq 0$. Sono quindi verificate, in virtù della definizione 9.1-(i), le condizioni $d \mid a$ e $d \mid b$. Sia adesso $d' \in R$ un elemento tale che $d' \mid a$ e $d' \mid b$. Sempre per la definizione 9.1-(i), esistono due elementi $x', y' \in R$ tali che $a = d' \cdot x'$, $b = d' \cdot y'$. Inoltre, siccome $a \mid a \cdot b$ e $b \mid a \cdot b$ e la divisibilità è una relazione transitiva (osservazione 9.2), si ha che $d' \mid a \cdot b$ cioè, ancora per la definizione 9.1-(i), esiste un elemento $c \in R$ tale che $a \cdot b = d' \cdot c$. Si noti adesso che valgono le due relazioni seguenti:

$$d' \cdot (a \cdot y') = a \cdot (d' \cdot y') = a \cdot b = d' \cdot c$$
$$d' \cdot (b \cdot x') = b \cdot (d' \cdot x') = b \cdot a = d' \cdot c$$

Usando nuovamente l'ipotesi che R sia un dominio integrale e notando che $d' \neq 0$ per la definizione 9.1-(i), posso applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)), dalla quale derivano le condizioni $c = a \cdot y'$, $c = b \cdot x'$. In particolare, essendo $a, b \neq 0$, si ha che $a \mid c$ e $b \mid c$. Dalla definizione 9.6-M2 segue quindi che $m \mid c$ cioè, per la definizione 9.1-(i), che esiste un elemento $z \in R$ tale che $c = m \cdot z$. Dunque:

$$m \cdot (d' \cdot z) = d' \cdot (m \cdot z) = d' \cdot c = a \cdot b = m \cdot d$$

Applicando ancora una volta la legge di cancellazione sinistra, si ottiene quindi che $d = d' \cdot z$. Ovviamente questo implica, per la definizione 9.1-(i), che $d' \mid d$. Siccome il risultato ottenuto non dipende dalla scelta

dell'elemento $d' \in R$, posso concludere che d è un massimo comune divisore di a e b. Si osservi ora che la formula $\mathrm{MCD}(a,b) \cdot \mathrm{mcm}(a,b) \sim a \cdot b$ discende immediatamente dalla relazione $a \cdot b = m \cdot d$ e dal fatto che il minimo comune multiplo e il massimo comune divisore di a e b sono definiti solo a meno di relazioni di associazione (osservazione 9.6). Sia infine $r \in R$ con $r \neq 0$ un elemento fissato. Moltiplicando a sinistra per r le relazioni $a = d \cdot y$, $b = d \cdot x$ e utilizzando il fatto che $r \neq 0$, si ottiene facilmente che $r \cdot d \mid r \cdot a$ e $r \cdot d \mid r \cdot b$. Sia ora $s \in R$ un qualunque elemento tale che $s \mid r \cdot a$ e $s \mid r \cdot b$ cioè, per la definizione 9.1-(i), tale che $r \cdot a = s \cdot x''$, $r \cdot b = s \cdot y''$ per opportuni $x'', y'' \in R$. Sia ora $t := x'' \cdot b$ e si consideri la relazione:

$$r \cdot t = r \cdot (x'' \cdot b) = x'' \cdot (r \cdot b) = x'' \cdot (s \cdot y'') = (s \cdot x'') \cdot y'' = (r \cdot a) \cdot y'' = r \cdot (a \cdot y'')$$

Utilizzando nuovamente la legge di cancellazione sinistra assieme all'ipotesi che $r \neq 0$, posso affermare che $t = a \cdot y''$. A questo punto vale ovviamente che $a \mid t$ e $b \mid t$ e quindi, per la definizione 9.6-M2, anche $m \mid t$. Come al solito, questo significa che esiste un elemento $z \in R$ tale che $t = m \cdot z$, ma allora vale la relazione:

$$m \cdot (s \cdot z) = s \cdot (m \cdot z) = s \cdot t = s \cdot (x'' \cdot b) = (s \cdot x'') \cdot b = (r \cdot a) \cdot b = r \cdot (a \cdot b) = r \cdot (m \cdot d) = m \cdot (r \cdot d)$$

Dato che $m \neq 0$, posso applicare nuovamente la legge di cancellazione sinistra per ottenere che $r \cdot d = s \cdot z$. In particolare, vale che $s \mid r \cdot d$ e questo dimostra, per arbitrarietà nella scelta dell'elemento $s \in R$ tale che $s \mid r \cdot a$ e $s \mid r \cdot b$, che $r \cdot d$ è un massimo comune divisore di $r \cdot a$ e di $r \cdot b$.

Viceversa, dimostro che (ii) $\Longrightarrow$ (i). Pongo per semplicità $d := \mathrm{MCD}(a,b)$ e noto che d è un elemento di R ben definito in quanto per ipotesi esiste $\mathrm{MCD}(1 \cdot a, 1 \cdot b)$. In virtù della definizione 9.6-D2, si ha che $d \mid a$ e $d \mid b$ cioè, per la definizione 9.1-(i), si ha che $d \neq 0$ ed esistono elementi $x, y \in R$ tali che $a = d \cdot x$, $b = d \cdot y$. Inoltre, tenendo a mente che la divisibilità è una relazione transitiva (osservazione 9.2), dato che valgono banalmente le relazioni $a \mid a \cdot b$ e $b \mid a \cdot b$, si ha che $d \mid a \cdot b$, quindi esiste un elemento $m \in R$ tale che $a \cdot b = d \cdot m$. Dalle condizioni precedenti derivano assai facilmente le due relazioni che seguono:

$$d \cdot m = a \cdot b = a \cdot (d \cdot y) = d \cdot (a \cdot y)$$
$$d \cdot m = a \cdot b = (d \cdot x) \cdot b = d \cdot (b \cdot x)$$

Ricordando che per ipotesi R è un dominio integrale e usando il fatto che $d \neq 0$, si può applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)) per ottenere che $m = a \cdot y$, $m = b \cdot x$. Poiché si assume che $a, b \neq 0$ posso affermare, in virtù della definizione 9.1-(i), che $a \mid m$ e $b \mid m$. Sia adesso $m' \in R$ un elemento fissato tale che $a \mid m'$ e $b \mid m'$. Nuovamente per la definizione 9.1-(i) esistono $x', y' \in R$ tali che $m' = a \cdot x'$, $m' = b \cdot y'$. Segue in particolare che $a \cdot b \mid m' \cdot b$ e $a \cdot b \mid m' \cdot a$. Adesso definisco $d' := \mathrm{MCD}(m' \cdot a, m' \cdot b)$ e osservo che d' è un elemento di R ben definito per ipotesi, ma allora $a \cdot b \mid d'$ per la definizione 9.6-D2. A questo punto basta ricordare che, per il lemma 9.1-(iii) e in virtù del fatto che $m' \neq 0$, vale che $d' \sim m' \cdot d$ e in particolare, per la definizione 9.1-(ii), si ha che $d' \mid m' \cdot d$. Ricordando che la divisibilità è una relazione riflessiva (osservazione 9.2), si ottiene dunque che $a \cdot b \mid m' \cdot d$ cioè, per la definizione 9.1-(i), che esiste un elemento $c \in R$ tale che $m' \cdot d = (a \cdot b) \cdot c$. Adesso si ottiene con estrema facilità la condizione che segue:

$$m' \cdot d = (a \cdot b) \cdot c = (d \cdot m) \cdot c = (m \cdot c) \cdot d$$

Applicando stavolta la legge di cancellazione destra (osservazione 6.6-(ii)), si ricava che $m' = m \cdot c$ quindi, essendo $m \neq 0$ per l'ipotesi che $a, b \neq 0$, si ha che $m \mid m'$. Poiché il risultato ottenuto non dipende da una particolare scelta dell'elemento $m' \in R$ tale che $a \mid m'$ e $b \mid m'$, posso infine concludere che m è un minimo comune multiplo di a e b. La validità della formula $\mathrm{MCD}(a,b) \cdot \mathrm{mcm}(a,b) \sim a \cdot b$ si giustifica esattamente come si è visto nella dimostrazione dell'implicazione diretta e dunque si ha la tesi. □

9.2 Due classi notevoli di domini a fattorizzazione unica

L'obiettivo di questa sezione è quello di dare una generalizzazione per l'algoritmo della divisione euclidea.

Definizione 9.7. Un dominio integrale R prende il nome di *dominio a ideali principali* se per ogni ideale $I \lhd R$ esiste un qualche $a \in R$ tale che $I = (a)$. Un dominio integrale R si dice invece un *dominio euclideo* se esiste un'applicazione $\delta \colon R \setminus \{0\} \to \mathbb{N}$, detta *funzione euclidea*, soddisfacente le due seguenti proprietà:

(1) Per ogni $a, b \in R$ con $a, b \neq 0$, vale che $\delta(a) \leq \delta(ab)$.

(2) Per ogni $a, b \in R$ con $b \neq 0$, esistono due elementi $q, r \in R$ tali che si abbia $a = b \cdot q + r$ e tali che $r = 0$ oppure $r \neq 0$ e $\delta(r) < \delta(b)$.

Esempio 9.4. Naturalmente, un classico esempio di dominio euclideo è dato dall'anello $\mathbb{Z}$, la cui funzione euclidea è la mappa $\delta\colon \mathbb{Z}^* \to \mathbb{N}$ definita da $\delta(x) := |x|$. Si ricordi infatti che, per l'algoritmo della divisione euclidea, comunque fissati elementi $a, b \in \mathbb{Z}$ con $b \neq 0$, esistono $q, r \in \mathbb{Z}$ con $0 \leq r < |b|$ tali che $a = bq + r$.

Teorema 9.2. *Sia R un dominio integrale. Valgono le seguenti affermazioni.*

(i) *Se R è un dominio euclideo, allora R è un dominio a ideali principali.*

(ii) *Se R è un dominio a ideali principali, allora R è un dominio a fattorizzazione unica.*

Dimostrazione.

(i) Innanzitutto, poiché si assume che R sia un dominio euclideo, esiste una funzione $\delta\colon R\setminus\{0\} \to \mathbb{N}$ come nella definizione 9.7. Sia $I \lhd R$ un ideale qualsiasi. Chiaramente, se $I = \{0\}$, allora $I = (0)$, per cui posso assumere che $I \neq \{0\}$. In tal caso si ha che $I\setminus\{0\}$ è non vuoto e di conseguenza, per il principio del buon ordinamento (leggasi la nota 10), è ben definito il seguente numero naturale:

$$\beta := \min\{\, \delta(x) \mid x \in I\,,\, x \neq 0\,\}$$

Per definizione di minimo, vale che β appartiene all'insieme di cui è minimo e dunque esiste $b \in I$, $b \neq 0$ tale che $\delta(b) = \beta$. Sia adesso $a \in I$. Dal momento che per ipotesi R è un dominio euclideo, si ha che $a = b \cdot q + r$ per opportuni $q, r \in R$ con $r = 0$ oppure con $r \neq 0$ e $\delta(r) < \delta(b)$. Suppongo per assurdo che $r \neq 0$ e che $\delta(r) < \delta(b)$. Poiché si assume che $I \lhd R$ sia un ideale, che $b \in I$ e che $q \in R$, per la definizione 7.1 vale che anche $b \cdot q \in I$. Essendo in particolare $I < R$ un sottoanello, siccome anche $a \in I$ e $r = a - b \cdot q$, posso affermare che $r \in I$. Dalla minimalità di β segue dunque che $\beta \leq \delta(r)$, ma questo è in evidente contraddizione con la condizione $\delta(r) < \delta(b)$ e quindi questa possibilità va scartata. Per esclusione, dovrà valere che $r = 0$ e dunque $a = b \cdot q$. Tenendo a mente l'osservazione 7.7, da tale condizione segue immediatamente che $a \in (b)$. A questo punto, poiché il risultato ottenuto non dipende da una particolare scelta dell'elemento $a \in I$, posso affermare che $I \subseteq (b)$. L'altro contenimento è invece una conseguenza immediata dell'osservazione 7.5 e del fatto che $b \in I$. Avendo mostrato che $I = (b)$ posso concludere, per arbitrarietà nella scelta dell'ideale $I \lhd R$ con $I \neq \{0\}$, che R è un dominio a ideali principali come volevasi dimostrare.

(ii) Per avere la tesi sarà sufficiente mostrare, in virtù del corollario 9.1, che R soddisfa la condizione sulla catena ascendente di ideali principali, vale a dire la proposizione 9.3-(ii.b) e che, comunque vengano assegnati due elementi $a, b \in R$, esiste $\mathrm{MCD}(a, b)$. Suppongo per assurdo che esista una catena infinita $\{\, (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots\,\}$ e definisco $I := \bigcup_{i\in\mathbb{N}^*}(a_i)$, quindi dimostro che $I \lhd R$ è un ideale. Siano innanzitutto $x, y \in I$ due elementi fissati. Per costruzione, esistono $i, j \in \mathbb{N}^*$ tali che $x \in (a_i)$, $y \in (a_j)$. Siccome (a_i) e (a_j) sono elementi di una catena, per la definizione 7.7 dovrà valere, alternativamente, che $(a_i) \subseteq (a_j)$ oppure $(a_j) \subseteq (a_i)$. Naturalmente posso assumere, senza perdita di generalità, che valga $(a_i) \subseteq (a_j)$. In particolare, si ricava che $x, y \in (a_j)$ e dunque anche $x + y \in (a_j)$ perché $(a_j) \lhd R$ è un ideale, quindi un sottoanello. Si noti ora che $0 \in I$ banalmente in quanto, comunque scelto un indice $i \in \mathbb{N}^*$, si ha che $0 \in (a_i)$. Inoltre, se $x \in (a_i)$ allora, essendo $(a_i) \lhd R$ un ideale, anche $-x \in (a_i)$ e quindi $-x \in I$. Dato infine un elemento $r \in R$, in virtù della definizione 7.1 si ha che $r \cdot x \in (a_i)$ e in particolare $r \cdot x \in I$. Poiché si assume che R sia un anello commutativo, scegliendo $r \in I$ posso affermare che $I \subseteq R$ è chiuso rispetto all'operazione binaria $\cdot$ su R. Questo dimostra che $I < R$ è un sottoanello. Invece, prendendo più in generale $r \in R$, posso concludere che $I \lhd R$ è un ideale. Dal momento che per ipotesi R è un dominio a ideali principali, per la definizione 9.7 esiste un elemento $b \in R$ tale che $I = (b)$. In particolare, vale che $b \in I$ cioè, per costruzione, esiste un indice $N \in \mathbb{N}^*$ tale che $b \in (a_N)$. In virtù dell'osservazione 7.5, si ha che $(b) \subseteq (a_N)$, cioè che $I \subseteq (a_N)$ e dato che l'altra inclusione è banale posso affermare che $I = (a_N)$. Per costruzione, però, si ha che $(a_{N+1}) \subseteq I$, cioè che $(a_{N+1}) \subseteq (a_N)$ e questo contraddice il fatto che $(a_i) \subsetneq (a_{i+1})$ per ogni $i \in \mathbb{N}^*$. Posso quindi affermare che R verifica la condizione sulla catena ascendente di ideali principali.

Siano adesso $a, b \in R$ due elementi fissati e si ricordi la definizione di ideale finitamente generato (definizione 7.2). Poiché si assume che R sia un dominio a ideali principali, esiste un qualche $d \in R$

tale che $(a,b)=(d)$. Da questo segue immediatamente che $a,b\in(d)$ quindi, per l'osservazione 7.5, valgono le inclusioni $(a)\subseteq(d)$ e $(b)\subseteq(d)$. Naturalmente, se fosse $d=0$ allora anche $a=0$ e $b=0$, ma in tal caso il massimo comune divisore di a e b esiste per definizione, dunque si può assumere che $d\neq 0$. Per la proposizione 9.1-(i), le relazioni ottenute sono equivalenti a richiedere che $d\mid a$ e $d\mid b$. Sia adesso $c\in R$ un elemento fissato tale che $c\mid a$ e $c\mid b$. Ancora per la proposizione 9.1-(i), si ha che $c\neq 0$ e valgono le inclusioni $(a)\subseteq(c)$ e $(b)\subseteq(c)$. In particolare, si ha che $a,b\in(c)$ ma allora, per l'osservazione 7.5, vale anche il contenimento $(a,b)\subseteq(c)$, cioè $(d)\subseteq(c)$. Nuovamente in virtù della proposizione 9.1-(i), posso dunque affermare che $c\mid d$. In definitiva, per arbitrarietà nella scelta dell'elemento $c\in R$ tale che $c\mid a$ e $c\mid b$ e in virtù della definizione 9.6, si ottiene che d è un massimo comune divisore di a e b. Non dipendendo il risultato ottenuto da una particolare scelta degli elementi $a,b\in R$ si può concludere, in virtù del corollario 9.1, che R è un dominio a fattorizzazione unica e quindi si ha la tesi. □

10 Anelli di polinomi

La definizione degli anelli di polinomi è stata già data nell'esempio 6.12. In questa sezione ci si restringerà soltanto al caso in cui R è un anello commutativo con identità $1\neq 0$ e di conseguenza, in vista dell'esempio sopra citato, per ogni $n\in\mathbb{N}$ anche $R[X_1,\dots,X_n]$ è un anello commutativo con identità $1\cdot X^{\mathbf{0}}$ diversa dal polinomio nullo.

Osservazione 10.1. Siano $n,m\in\mathbb{N}$ con $m\leq n$ e sia R un anello commutativo con identità $1\neq 0$. Allora $R[X_1,\dots,X_m]$ è isomorfo a un sottoanello di $R[X_1,\dots,X_n]$ contenente l'identità.

Dimostrazione. Si consideri il seguente sottoinsieme di $R[X_1,\dots,X_n]$:

$$S:=\left\{\sum_{I\in\mathbb{N}^n} s_I X^I \;\middle|\; s_I=0 \text{ per ogni } I\in\mathbb{N}^n,\ I=(i_1,\dots,i_n) \text{ con } i_h\neq 0 \text{ per un qualche } m+1\leq h\leq n\right\}$$

Dimostro che $S<R[X_1,\dots,X_n]$ è un sottoanello. Siano $\sum_{I\in\mathbb{N}^n} r_I X^I, \sum_{I\in\mathbb{N}^n} s_I X^I\in S$ elementi fissati. Per come si è definita l'operazione binaria di somma $+$ sull'anello $R[X_1,\dots,X_n]$ e per definizione di S, la somma degli elementi considerati appartiene ancora a S. Infatti, se valgono le condizioni $r_I=0$ e $s_I=0$ per ogni vettore di indici $I\in\mathbb{N}^n$ che verifichi le proprietà desiderate, allora per tali vettori $I\in\mathbb{N}^n$ anche $r_I+s_I=0$. Si osservi poi che l'appartenenza dell'elemento neutro additivo a S è banale poiché in tal caso vale che $s_I=0$ per qualsiasi vettore $I\in\mathbb{N}^n$ quindi, in particolare, per quelli che soddisfano le condizioni volute. Infine, l'opposto di un elemento $\sum_{I\in\mathbb{N}^n} r_I X^I\in S$ appartiene banalmente a S perché l'opposto di 0 in R è 0. Si può dunque affermare, data l'arbitrarietà nella scelta di $\sum_{I\in\mathbb{N}^n} r_I X^I, \sum_{I\in\mathbb{N}^n} s_I X^I\in S$, che $(S,+,0)$ è un sottogruppo di $(R[X_1,\dots,X_n],+,0)$. È immediato verificare che $1\cdot X^{\mathbf{0}}\in S$ perché l'unico coefficiente diverso da 0 che vi compare è associato al vettore $\mathbf{0}=(0,\dots,0)$. Si consideri ora il prodotto:

$$\sum_{K\in\mathbb{N}^n}\left(\sum_{\substack{I,J\in\mathbb{N}^n\\ I+J=K}} r_I\cdot s_J\right)X^K$$

Sarà sufficiente mostrare che, comunque fissato un vettore di indici $K\in\mathbb{N}^n$, $K=(k_1,\dots,k_n)$ con $k_h\neq 0$ per un qualche $m+1\leq h\leq n$, vale che $\sum_{I+J=K}^{I,J\in\mathbb{N}^n} r_I\cdot s_J=0$. Per farlo basta semplicemente osservare che, se $I=(i_1,\dots,i_n)$, $J=(j_1,\dots,j_n)$ sono tali che $I+J=K$, allora si dovrà avere che $i_h+j_h\neq 0$ in quanto $i_h+j_h=k_h$. Tenendo a mente che $i_h,j_h\in\mathbb{N}$, deve valere necessariamente che $i_h\neq 0$ oppure $j_h\neq 0$ e si può dunque assumere, senza perdita di generalità, che valga $i_h\neq 0$. Essendo $m+1\leq h\leq n$ ed essendo $\sum_{I\in\mathbb{N}^n} r_I X^I\in S$, per definizione di S vale che $r_I=0$ per ogni $I,J\in\mathbb{N}^n$ tali che $I+J=K$ ma allora, per tali vettori $I,J\in\mathbb{N}^n$, si ha che $r_I\cdot s_J=0$ in virtù della proposizione 6.1-(i). Non dipendendo il risultato ottenuto da una particolare scelta dei vettori $I,J\in\mathbb{N}^n$ tali che $I+J=K$, si può concludere che anche $\sum_{I+J=K}^{I,J\in\mathbb{N}^n} r_I\cdot s_J=0$. Non dipendendo il risultato ottenuto dalla scelta di $\sum_{I\in\mathbb{N}^n} r_I X^I, \sum_{I\in\mathbb{N}^n} s_I X^I\in S$, posso affermare che $S<R[X_1,\dots,X_n]$ è un sottoanello. Si consideri ora la mappa $\eta\colon R[X_1,\dots,X_m]\to S$ definita dalla condizione $\eta(\sum_{I\in\mathbb{N}^m} r_I X^I):=\sum_{J\in\mathbb{N}^n} s_J X^J$, dove si ha che $s_J:=r_I$ con $I=(i_1,\dots,i_m)$ se $J=(i_1,\dots,i_m,0,\dots,0)$, $s_J:=0$ altrimenti. È immediato verificare che η è un'applicazione ben definita e altrettanto facilmente si dimostra che è un isomorfismo unitario di anelli, dunque si ha la tesi. □

Osservazione 10.2. Sia $n \in \mathbb{N}$ fissato e sia R un anello commutativo con identità $1 \neq 0$. Prendendo $m := 0$ nell'osservazione 10.1 si ricava immediatamente, come caso particolare, che R è isomorfo a un sottoanello di $R[X_1, \dots, X_n]$ contenente l'identità.

Osservazione 10.3. Siano $n, m \in \mathbb{N}$ con $m \leq n$ e sia R un anello commutativo con identità $1 \neq 0$. Si vede con molta facilità che $(R[X_1, \dots, X_m])[X_{m+1}, \dots, X_n] \simeq R[X_1, \dots, X_n]$ in modo naturale. In particolare, l'anello $R[X_1, \dots, X_n]$ può essere ottenuto, a meno di isomorfismo, iterando per n volte la costruzione di un anello di polinomi su R in una variabile.

In vista dell'osservazione 10.3, posso restringermi al caso dei polinomi in una variabile. Per semplicità, un polinomio in una variabile può essere indicato con $a_0 + a_1X + \cdots + a_nX^n$ anziché con $\sum_{i \in \mathbb{N}} a_iX^i$ in quanto, per definizione di $R[X]$, si ha che $a_i = 0$ per ogni $i \in \mathbb{N}$ tranne che per un numero finito di indici, dunque esiste sicuramente un indice $n \in \mathbb{N}$ tale che $a_i = 0$ per ogni $i > n$.

Definizione 10.1. Sia R un anello commutativo con identità $1 \neq 0$ e sia $-\infty$ un simbolo formale. Prende il nome di *grado* l'applicazione $\deg\colon R[X] \to \mathbb{N} \cup \{-\infty\}$ definita dalla condizione seguente:

$$\deg(a_0 + a_1X + \cdots + a_nX^n) := \begin{cases} \max\{\, 0 \leq i \leq n \mid a_i \neq 0 \,\} & \text{se esiste } 0 \leq i \leq n \text{ tale che } a_i \neq 0 \\ -\infty & \text{se } a_i = 0 \text{ per ogni } 0 \leq i \leq n \end{cases}$$

Sia inoltre $f \in R[X]$, $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomio non nullo e sia $k := \deg(f)$. Il termine a_k viene detto il *coefficiente direttore di* f e si denota $\mathrm{lt}(f)$. Infine, per ogni $n \in \mathbb{N}$ si hanno le convenzioni:

$$-\infty < n\,, \quad -\infty + n := -\infty\,, \quad n + (-\infty) := -\infty\,, \quad -\infty + (-\infty) := -\infty$$

Proposizione 10.1. *Sia R un anello commutativo con identità $1 \neq 0$ e siano $f, g \in R[X]$ due polinomi.*

(i) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ *e si ha l'uguaglianza se $f = g = 0$ oppure se* $\deg(f) \neq \deg(g)$.

(ii) $\deg(f \cdot g) \leq \deg(f) + \deg(g)$ *e l'uguaglianza sussiste se $f = 0$, se $g = 0$ oppure se* $\mathrm{lt}(f) \cdot \mathrm{lt}(g) \neq 0$.

Dimostrazione. Innanzitutto, essendo $f, g \in R[X]$ polinomi, esistono $a_0, \dots, a_n, b_0, \dots, b_m \in R$ per i quali valgano le condizioni $f(X) = a_0 + a_1X + \cdots + a_nX^n$, $g(X) = b_0 + b_1X + \cdots + b_mX^m$. Se f e g sono non nulli si può supporre, senza perdita di generalità, che $n = \deg(f)$, $m = \deg(g)$. Infatti, se fosse $\deg(f) = k$ con $0 \leq k \leq n - 1$, allora nell'espressione di f potrei ignorare tutti i termini successivi al k-esimo perché essi sono nulli, cioè potrei riscrivere $f(X) = a_0 + a_1X + \cdots + a_kX^k$. Chiaramente, lo stesso argomento è applicabile per il polinomio g. Inoltre, a meno di ridefinire i polinomi f e g scambiandoli di ruolo, si può assumere che valga $n \geq m$.

(i) Si consideri innanzitutto il caso in cui f e g sono polinomi nulli. Naturalmente, per come è stata definita l'operazione binaria $+$ su $R[X]$ nell'esempio 6.12, anche $f + g$ è il polinomio nullo e quindi vale banalmente la formula $\deg(f + g) = \max\{\deg(f), \deg(g)\}$. Si assuma ora che f e g siano non entrambi nulli. Distinguo due possibilità, a seconda che $n > m$ oppure $n = m$. Se $n > m$, allora:

$$(f + g)(X) = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_m + b_m)X^m + a_{m+1}X^{m+1} + \cdots + a_nX^n$$

Poiché si assume che $n = \deg(f)$, si ha che $a_n \neq 0$ e di conseguenza $\deg(f + g) = n$. Chiaramente, se fosse stato $n < m$, allora $\deg(f + g) = m$ e posso dunque affermare, nel caso generale, che vale la formula $\deg(f + g) = \max\{n, m\}$. Se invece $n = m$, allora si ha la seguente condizione:

$$(f + g)(X) = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_m + b_m)X^m$$

In questo caso, pur essendo $a_m, b_m \neq 0$ in quanto coefficienti direttori di f e g, non è vero a priori che $a_m + b_m \neq 0$ e di conseguenza $\deg(f + g) \leq m$. Posso quindi concludere che, in generale, vale la formula $\deg(f + g) \leq \max\{n, m\}$.

(ii) Per come si è definita l'operazione binaria moltiplicativa $\cdot$ su $R[X]$ nell'esempio 6.12, il prodotto dei polinomi f e g assume la seguente forma:

$$(f \cdot g)(X) = \sum_{k=0}^{n+m} \Bigg(\sum_{\substack{i=1,\dots,n \\ j=1,\dots,m \\ i+j=k}} a_i \cdot b_j \Bigg) X^k$$

È parecchio evidente che, se f oppure g è il polinomio nullo, allora lo è anche il prodotto $f \cdot g$ e vale dunque in maniera ovvia la formula $\deg(f \cdot g) = \deg(f) + \deg(g)$. Mi restringo quindi al caso non banale in cui f e g sono entrambi non nulli e osservo che il termine di $f \cdot g$ associato a X^{n+m} è dato semplicemente da $a_n \cdot b_m$. Se si assume per ipotesi che $a_n \cdot b_m \neq 0$, allora posso concludere che $\deg(f \cdot g) = n + m$, ma in generale non è detto che tale condizione sia soddisfatta e quindi, a priori, varrà soltanto la disuguaglianza $\deg(f \cdot g) \leq n + m$. □

Osservazione 10.4. Sia R un dominio integrale e siano $f, g \in R[X]$ polinomi. Dalla proposizione 10.1-(ii) segue banalmente che $\deg(f \cdot g) = \deg(f) + \deg(g)$ in quanto, se $f, g \neq 0$ allora, per la definizione 10.1, si ha che $\mathrm{lt}(f), \mathrm{lt}(g) \neq 0$ e dunque, essendo per ipotesi R un dominio integrale, la condizione $\mathrm{lt}(f) \cdot \mathrm{lt}(g) \neq 0$ è automaticamente soddisfatta.

Corollario 10.1. *Sia R un dominio integrale. Valgono le seguenti affermazioni.*

(i) *$R[X]$ è un dominio integrale.*

(ii) *$U(R[X]) \simeq U(R)$.*

Dimostrazione.

(i) Siano $f, g \in R[X]$ due polinomi non nulli. Da questa assunzione segue, per la definizione 10.1, che $\deg(f) \geq 0$ e che $\deg(g) \geq 0$. Poiché per ipotesi R è un dominio integrale, per l'osservazione 10.4 vale la formula $\deg(f \cdot g) = \deg(f) + \deg(g)$ e in particolare $\deg(f \cdot g) \geq 0$. Nuovamente in virtù della definizione 10.1, si può concludere che $f \cdot g$ è un polinomio non nullo e questo dimostra, per arbitrarietà nella scelta dei polinomi non nulli $f, g \in R[X]$, che $R[X]$ non ammette divisori dello zero non banali, cioè che $R[X]$ è un dominio integrale.

(ii) Dalla dimostrazione dell'osservazione 10.1 segue che R è isomorfo al seguente sottoanello di $R[X]$:

$$S := \left\{ \sum_{i \in \mathbb{N}} s_i X^i \in R[X] \;\middle|\; s_i = 0 \text{ per ogni } i \in \mathbb{N}^* \right\}$$

In questo caso particolare l'isomorfismo, che è unitario (definizione 8.2), è fornito dall'applicazione $\eta \colon R \to S$ definita dalla condizione $\eta(r) := r$, dove l'elemento r a secondo membro va inteso come polinomio, cioè $r = r \cdot X^0$. Si ricordi inoltre che, essendo η un omomorfismo unitario di anelli, la condizione $u \in U(R)$ implica, in virtù dell'osservazione 8.2, che $\eta(u) \in U(R[X])$ e si può dunque affermare, per arbitrarietà nella scelta di $u \in U(R)$, che $\eta(U(R)) \subseteq U(R[X])$. Ripetendo lo stesso ragionamento con l'applicazione inversa η^{-1} si ottiene anche l'altro contenimento e posso dunque affermare che $\eta(U(R)) = U(R[X])$. Restringendo η su $U(R)$ si trova quindi una mappa biiettiva la cui immagine è il gruppo $U(R[X])$. Tale applicazione è anche un omomorfismo di gruppi in virtù del fatto che η è un isomorfismo unitario di anelli. Questa semplice osservazione mi dà la tesi. □

Si enuncia adesso il seguente risultato fondamentale, la cui dimostrazione[31] non verrà trattata.

Teorema 10.1 (Algoritmo della divisione euclidea)**.** *Sia R un dominio integrale e siano $f, g \in R[X]$ due polinomi tali che $g \neq 0$ e $\mathrm{lt}(g) \in U(R)$. Allora esistono unici polinomi $q, r \in R[X]$, con $\deg(r) < \deg(g)$, tali che sia soddisfatta la condizione $f(X) = g(X) \cdot q(X) + r(X)$.*

Osservazione 10.5. Sia R un campo e siano $f, g \in R[X]$ polinomi tali che $g \neq 0$. Si noti che la condizione $\mathrm{lt}(g) \in U(R)$ è automaticamente verificata in quanto $\mathrm{lt}(g) \neq 0$ per la definizione 10.1 e ogni elemento non banale di un campo è invertibile (definizione 6.6). Posso dunque usare l'algoritmo della divisione euclidea.

Corollario 10.2. *Sia R un campo. Allora l'anello $R[X]$ è un dominio euclideo con funzione euclidea la restrizione del grado su $R[X] \setminus \{0\}$, vale a dire la funzione $\delta \colon R[X] \setminus \{0\} \to \mathbb{N}$ definita da $\delta(f) := \deg(f)$.*

Dimostrazione. Innanzitutto, dal momento che per ipotesi R è un campo, in virtù dell'osservazione 6.5 e del corollario 10.1-(i) si ha che $R[X]$ è un dominio integrale. Fatta questa considerazione, l'asserto deriva immediatamente dalla definizione 9.7 e dall'osservazione 10.5. □

[31] Una dimostrazione è reperibile negli appunti del corso AL110.

Esempio 10.1. Nell'enunciato del corollario 10.2 l'ipotesi che R sia un campo non può essere indebolita, come mostra il seguente controesempio. Si consideri un dominio integrale R che non è un campo. Esiste dunque un elemento $p \in R$ tale che $p \neq 0$ e $p \notin U(R)$. Mostro che l'ideale $(p, X) \lhd R[X]$ non è un ideale principale. Suppongo per assurdo che esista un polinomio $f \in R[X]$ tale che $(p, X) = (f(X))$. Da questa assunzione segue innanzitutto che $X \in (f(X))$ cioè, ricordando l'osservazione 7.7, che esiste un polinomio $a \in R[X]$ tale che $X = a(X) \cdot f(X)$. Passando al grado nella relazione precedente si ottiene la condizione $\deg(X) = \deg(a \cdot f)$ e quindi, poiché si assume che R sia un dominio integrale, per l'osservazione 10.4 si ha che $\deg(a) + \deg(f) = 1$. Da questo si può dedurre che $a(X) = a_0 + a_1 X$, $f(X) = b_0$ oppure $a(X) = b_0$, $f(X) = a_0 + a_1 X$ per certi $a_0, a_1, b_0 \in R$ con $a_1, b_0 \neq 0$. In ambo i casi, per come si è definita l'operazione binaria $\cdot$ su $R[X]$ nell'esempio 6.12, il polinomio ottenuto dal prodotto di a e f assume la forma seguente:

$$(a \cdot f)(X) = (a_0 \cdot b_0) + (a_1 \cdot b_0)X \tag{13}$$

Utilizzando quindi il fatto che $a(X) \cdot f(X) = X$, si dovrà avere che $a_1 \cdot b_0 = 1$, cioè che $a_1, b_0 \in U(R)$. Di conseguenza, se fosse $f(X) = b_0$ allora, per il corollario 10.1-(ii) con la relativa dimostrazione, si avrebbe che $f \in U(R[X])$. In particolare, per l'osservazione 7.3 varrebbe che $(f(X)) = R[X]$ e quindi $1 \in (f(X))$, cioè $1 \in (p, X)$. Questo significa che esistono elementi $c_0, \ldots, c_n, d_0, \ldots, d_m \in R$ tali che valga la relazione:

$$1 = p \cdot (c_0 + c_1 X + \cdots + c_n X^n) + X \cdot (d_0 + d_1 X + \cdots + d_m X^m)$$

Si deduce quindi che $p \cdot c_0 = 1$ e in particolare si ottiene che $p \in U(R)$, ma questo è assurdo. Si supponga invece che $f(X) = a_0 + a_1 X$ e si osservi che, per la relazione (13), vale la condizione $a_0 \cdot b_0 = 0$. Poiché si assume che R sia un dominio integrale e che $b_0 \neq 0$, deve necessariamente valere che $a_0 = 0$ e dunque si ha che $f(X) = a_1 X$. Ma allora, usando il fatto che $p \in (f(X))$, deduco che esistono elementi $e_0, \ldots, e_p \in R$ tali che la seguente condizione sia verificata:

$$p = a_1 X \cdot (e_0 + e_1 X + \cdots + e_p X^p) = (a_1 \cdot e_0)X + (a_1 \cdot e_1)X^2 + \cdots + (a_1 \cdot e_p)X^{p+1}$$

Dovrebbe dunque valere che $p = 0$, ma questo è assurdo e posso quindi concludere che $(p, X) \lhd R[X]$ non è un ideale principale. Ricordando la definizione 9.7, questo dimostra che $R[X]$ non è un dominio a ideali principali e dunque, per contrapposizione logica dal teorema 9.2-(i), non è nemmeno un dominio euclideo.

Per trattare l'esempio che segue occorre una generalizzazione per polinomi in più variabili del concetto di grado. Per ogni $n \in \mathbb{N}$ con $n \geq 2$ introduco quindi la mappa $\deg\colon R[X_1, \ldots, X_n] \to \mathbb{N} \cup \{-\infty\}$ data da:

$$\deg\left(\sum_{I \in \mathbb{N}^n} r_I X^I\right) := \begin{cases} \max\{\, i_1 + \cdots + i_n \mid r_I \neq 0\,,\, I = (i_1, \ldots, i_n)\,\} & \text{se esiste } I \in \mathbb{N}^n \text{ tale che } r_I \neq 0 \\ -\infty & \text{se } r_I = 0 \text{ per ogni } I \in \mathbb{N}^n \end{cases}$$

Si tratta di un'applicazione ben definita in quanto $r_I = 0$ per ogni $I \in \mathbb{N}^n$ tranne che per un numero finito di indici e il massimo fra gli elementi di un sottoinsieme finito di $\mathbb{N}$ esiste.

Esempio 10.2. Il corollario 10.2 non vale, in generale, per anelli di polinomi in più variabili, come mostra il seguente controesempio. Sia infatti $n \in \mathbb{N}$ con $n \geq 2$ fissato e sia R un campo. Come nell'esempio 10.1, sarà sufficiente mostrare che l'ideale $(X_1, X_2) \lhd R[X_1, \ldots, X_n]$ non è un ideale principale. Suppongo per assurdo che esista un polinomio $f \in R[X_1, \ldots, X_n]$ tale che $(X_1, X_2) = (f(X_1, \ldots, X_n))$. In particolare, si ha che $X_1 \in (f(X_1, \ldots, X_n))$ e dunque esiste un polinomio $a \in R[X_1, \ldots, X_n]$ tale che valga la condizione $X_1 = a(X_1, \ldots, X_n) \cdot f(X_1, \ldots, X_n)$. Passando poi al grado, si ottiene che $\deg(X_1) = \deg(a \cdot f)$ e quindi, ricordando che per ipotesi R è un campo e in particolare un dominio integrale (osservazione 6.5), si può applicare l'analogo dell'osservazione 10.4, per cui vale che $\deg(a) + \deg(f) = 1$. A questo punto si possono distinguere due casi, a seconda che $\deg(f) = 0$ oppure $\deg(f) = 1$. Se fosse $\deg(f) = 0$, allora si avrebbe che $f(X_1, \ldots, X_n) = c_0$ per un qualche $c_0 \in R$ con $c_0 \neq 0$. In tal caso, siccome $f(X_1, \ldots, X_n) \in (X_1, X_2)$ essendo $(X_1, X_2) = (f(X_1, \ldots, X_n))$, devono esistere collezioni $\{r_I\}_{I \in \mathbb{N}^n}, \{s_I\}_{I \in \mathbb{N}^n} \subseteq R$ tali che si abbia:

$$c_0 = X_1 \cdot \left(\sum_{I \in \mathbb{N}^n} r_I X^I\right) + X_2 \cdot \left(\sum_{I \in \mathbb{N}^n} s_I X^I\right)$$

Dalla relazione precedente si deduce che $c_0 = 0$, ma questo è assurdo e di conseguenza la possibilità in cui $\deg(f) = 0$ va scartata. Si assuma quindi che $\deg(f) = 1$ e si osservi che $\deg(a) = 0$ in virtù della relazione

$\deg(a) + \deg(f) = 1$. Esistono quindi elementi $a_0, c_0, \dots, c_n \in R$ con $a_0 \neq 0$, $c_1, \dots, c_n$ non tutti nulli tali che $a(X_1, \dots, X_n) = a_0$, $f(X_1, \dots, X_n) = c_0 + c_1X_1 + \cdots + c_nX_n$. Scrivendo esplicitamente il polinomio ottenuto dal prodotto $a \cdot f$ e ricordando che $X_1 = a(X_1, \dots, X_n) \cdot f(X_1, \dots, X_n)$, si ricava la condizione:

$$X_1 = (a_0 \cdot c_0) + (a_0 \cdot c_1)X_1 + \cdots + (a_0 \cdot c_n)X_n$$

Ne segue che $a_0 \cdot c_1 = 1$ e che $a_0 \cdot c_i = 0$ per ogni $0 \leq i \leq n$ con $i \neq 1$. Essendo $a_0 \neq 0$ e ricordando che R è un dominio integrale, per tali indici si deve avere la condizione $c_i = 0$ e dunque $f(X_1, \dots, X_n) = c_1X_1$. Utilizzando ora il fatto che anche $X_2 \in (f(X_1, \dots, X_n))$ essendo $(X_1, X_2) = (f(X_1, \dots, X_n))$, deduco che esiste un qualche $b \in R[X]$ tale che $X_2 = b(X_1, \dots, X_n) \cdot f(X_1, \dots, X_n)$. Usando come prima la formula per determinare il grado del prodotto di due polinomi si deduce che $\deg(b) = 0$ e di conseguenza esiste un elemento $b_0 \in R$ con $b_0 \neq 0$ tale che $b(X_1, \dots, X_n) = b_0$. Scrivendo in maniera esplicita il polinomio dato dal prodotto $b \cdot f$ e utilizzando il fatto che $f(X_1, \dots, X_n) = c_1X_1$, si ottiene quindi la seguente condizione:

$$X_2 = (b_0 \cdot c_1)X_1$$

Da tale relazione segue tuttavia che $1 = 0$ e questo contraddice l'ipotesi che R sia un campo. Posso quindi affermare che $(X_1, X_2) \lhd R[X_1, \dots, X_n]$ non è un ideale principale. La discussione precedente mi consente di concludere, in virtù della definizione 9.7, che $R[X_1, \dots, X_n]$ non è un dominio a ideali principali e dal teorema 9.2-(i) segue dunque, per contrapposizione logica, che $R[X]$ non è nemmeno un dominio euclideo.

10.1 Fattorialità in anelli di polinomi

Definizione 10.2. Sia R un dominio a fattorizzazione unica e si consideri un dato polinomio non costante $f \in R[X]$, $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Il massimo comune divisore dei termini $a_0, \dots, a_n$ viene detto il *contenuto di* f e si denota $C(f)$. Per convenzione, si definisce inoltre $C(r) := r$ per ogni $r \in R$. Infine, un polinomio $f \in R[X]$ prende il nome di *polinomio primitivo* se $C(f) \sim 1$.

La definizione 10.2 è ben posta per il lemma 9.1-(i).

Osservazione 10.6. Siano R un anello commutativo con identità $1 \neq 0$, $a_1, \dots, a_n, c \in R$ elementi fissati tali che $c \mid a_i$ per ogni $1 \leq i \leq n$. Allora $c \mid a_1 + \cdots + a_n$.

Dimostrazione. Sia $1 \leq i \leq n$ un indice fissato. Poiché si assume che $c \mid a_i$, per la definizione 9.1-(i) esiste un elemento $x_i \in R$ tale che $a_i = c \cdot x_i$ ma allora, sommando sull'indice $1 \leq i \leq n$, si ottiene la relazione:

$$a_1 + \cdots + a_n = (c \cdot x_1) + \cdots + (c \cdot x_n) = c \cdot (x_1 + \cdots + x_n)$$

Di nuovo in virtù della definizione 9.1-(i), si ha la tesi. □

Lemma 10.1 (di Gauss)**.** *Sia R un dominio a fattorizzazione unica e siano $f, g \in R[X]$ due polinomi non nulli. Allora vale la condizione $C(f \cdot g) \sim C(f) \cdot C(g)$. In particolare, se f e g sono polinomi primitivi, allora lo è anche il prodotto $f \cdot g$.*

Dimostrazione. Dato che per ipotesi $f \in R[X]$ è un polinomio non nullo, esistono elementi $a_0, \dots, a_n \in R$ con $a_n \neq 0$ tali che $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Sia $d := C(f)$ e si osservi che, per ogni $0 \leq i \leq n$, in virtù del lemma 9.1-(i) vale che $d \mid a_i$ cioè, ricordando la definizione 9.1-(i), esiste un elemento $a_i' \in R$ tale che $a_i = d \cdot a_i'$. Sia adesso $f_1 \in R[X]$ il polinomio definito da $f_1(X) := a_0' + a_1'X + \cdots + a_n'X^n$, cosicché si abbia per costruzione che $f(X) = C(f) \cdot f_1(X)$. Noto che, per il lemma 9.1-(iii) e in virtù della definizione iterativa del massimo comune divisore di più elementi fornita nella dimostrazione del lemma 9.1-(i), si ha che il massimo comune divisore degli elementi $d \cdot a_0', \dots, d \cdot a_n'$ è associato al prodotto di d con il massimo comune divisore di $a_0', \dots, a_n'$, cioè che $d \sim d \cdot C(f_1)$. Per la proposizione 9.1-(iv) è equivalente richiedere che valga $d \cdot C(f_1) \sim d$, mentre in virtù della proposizione 9.1-(vi) esiste un certo elemento $u \in U(R)$ tale che $d \cdot C(f_1) = d \cdot u$. Utilizzando l'ipotesi che R sia un dominio a fattorizzazione unica e in particolare un dominio integrale assieme al fatto che $d \neq 0$ per la definizione 9.1-(i), posso usare la legge di cancellazione sinistra (osservazione 6.6-(ii)), ottenendo che $C(f_1) = u$. In particolare, vale che $C(f_1) \in U(R)$ e dunque, in virtù dell'osservazione 9.1, si ha che $C(f_1) \sim 1$, vale a dire che f_1 è un polinomio primitivo. Ripetendo lo stesso argomento nel caso di g, si ottiene che $g(X) = C(g) \cdot g_1(X)$ per un certo polinomio primitivo g_1 e dunque $(f \cdot g)(X) = C(f) \cdot C(g) \cdot (f_1 \cdot g_1)(X)$. Si noti che, in virtù dell'ipotesi che f e g siano polinomi

non nulli, anche $f \cdot g$ è un polinomio non nullo e dunque lo è anche $f_1 \cdot g_1$. Passando quindi ai contenuti e applicando nuovamente il lemma 9.1-(iii), si ottiene che $C(f \cdot g) \sim C(f) \cdot C(g) \cdot C(f_1 \cdot g_1)$. Sarà dunque sufficiente mostrare che $C(f_1 \cdot g_1) \sim 1$, cioè che $f_1 \cdot g_1$ è un polinomio primitivo.

Suppongo per assurdo che $C(f_1 \cdot g_1) \not\sim 1$ cioè, per l'osservazione 9.1, che $C(f_1 \cdot g_1) \notin U(R)$. Essendo $f_1 \cdot g_1$ un polinomio non nullo, per la definizione 10.2 anche $C(f_1 \cdot g_1) \neq 0$ ma allora, dato che per ipotesi R è un dominio a fattorizzazione unica, esiste una fattorizzazione in irriducibili $C(f_1 \cdot g_1) = c_1 \cdots c_p$. Ora, se $g_1(X) = b'_0 + b'_1 X + \cdots + b'_m X^m$ con $b'_0, \ldots, b'_m \in R$, $b'_m \neq 0$, allora il prodotto $f_1 \cdot g_1$ assume la forma:

$$(f_1 \cdot g_1)(X) = \sum_{k=0}^{n+m} \left(\sum_{\substack{i=0,\ldots,n \\ j=0,\ldots,m \\ i+j=k}} a'_i \cdot b'_j \right) X^k$$

Dalla decomposizione di $C(f_1 \cdot g_1)$ in irriducibili e dal fatto che $c_1 \neq 0$ in quanto elemento irriducibile di R segue che $c_1 \mid C(f_1 \cdot g_1)$, ma allora $c_1 \mid \sum_{i+j=k} a'_i \cdot b'_j$ per ogni $0 \leq k \leq n+m$ in virtù del lemma 9.1-(i). Adesso suppongo per assurdo che $c_1 \mid C(f_1)$. Siccome $C(f_1) \sim 1$, in virtù della definizione 9.1-(ii) si ha in particolare che $C(f_1) \mid 1$ e quindi, per transitività della relazione di divisibilità (osservazione 9.2), vale che $c_1 \mid 1$. Per la definizione 9.1-(i) esiste dunque un elemento $x \in R$ tale che $1 = c_1 \cdot x$ ma allora, tenendo a mente che R è un anello commutativo, si può affermare che $c_1 \in U(R)$, contraddicendo il fatto che $c_1 \in R$ sia un elemento irriducibile. Deve dunque valere che $c_1 \nmid C(f_1)$ e inoltre, riapplicando lo stesso argomento con g_1 al posto di f_1, si ottiene anche che $c_1 \nmid C(g_1)$. Si osservi adesso che, siccome $c_1 \nmid C(f_1)$, in virtù del lemma 9.1-(i) deve esistere almeno un indice $0 \leq i \leq n$ tale che $c_1 \nmid a'_i$ e di conseguenza l'intero positivo $s := \min\{\, 0 \leq i \leq n \mid c_1 \nmid a'_i \,\}$ è ben definito. Per ragioni analoghe, anche $t := \min\{\, 0 \leq j \leq m \mid c_1 \nmid b'_j \,\}$ è un intero positivo ben definito. Si scelga ora $k := s + t$ e si osservi che:

$$\sum_{\substack{i=0,\ldots,n \\ j=0,\ldots,m \\ i+j=k}} a'_i \cdot b'_j = a'_{s+t} \cdot b'_0 + \cdots + a'_{s+1} \cdot b'_{t-1} + a'_s \cdot b'_t + a'_{s-1} \cdot b'_{t+1} + \cdots + a'_0 \cdot b'_{s+t}$$

Per costruzione, per ogni $0 \leq i \leq s-1$ si ha che $c_1 \mid a'_i$ cioè, per la definizione 9.1-(i), esiste un elemento $x_i \in R$ tale che $a'_i = c_1 \cdot x_i$. Moltiplicando a destra per b'_{s+t-i} ambedue i membri della relazione ottenuta, si ottiene che $a'_i \cdot b'_{s+t-i} = c_1 \cdot (x_i \cdot b'_{s+t-i})$ e dunque $c_1 \mid a'_i \cdot b'_{s+t-i}$. Analogamente, per ogni $0 \leq j \leq t-1$ vale che $c_1 \mid b'_j$ e ripetendo lo stesso argomento di prima posso affermare che $c_1 \mid a'_{s+t-j} \cdot b'_j$. Si ricordi ora che $c_1 \mid \sum_{i+j=k} a'_i \cdot b'_j$ per ogni $0 \leq k \leq n+m$ e in particolare per $k := s+t$, ma allora $c_1 \mid a'_s \cdot b'_t$ in virtù dell'osservazione 10.6. Infine, siccome R è un dominio a fattorizzazione unica, per la proposizione 9.3-(iii) l'elemento irriducibile c_1 è anche un elemento primo. La condizione $c_1 \mid a'_s \cdot b'_t$ implica dunque che $c_1 \mid a'_s$ oppure $c_1 \mid b'_t$, ma in entrambi i casi si ha una contraddizione o con la definizione di s, o con la definizione di t e posso quindi concludere che $C(f_1 \cdot g_1) \sim 1$. Non dipendendo il risultato ottenuto da una particolare scelta dei polinomi primitivi f_1 e g_1, la seconda parte dell'enunciato è dimostrata.

A questo punto si verifica facilmente che vale la condizione $C(f) \cdot C(g) \cdot C(f_1 \cdot g_1) \sim C(f) \cdot C(g)$ e dal fatto già noto che l'essere elementi associati è una relazione di equivalenza, quindi una relazione transitiva (proposizione 9.1-(iv)), segue che $C(f \cdot g) \sim C(f) \cdot C(g)$. Con questo è dimostrata anche la prima parte dell'enunciato e dunque si ha la tesi. □

Allo scopo di semplificare la notazione, da qui in avanti un dominio integrale D verrà trattato, con un piccolo abuso di linguaggio, come un sottoinsieme del proprio campo dei quozienti. Se infatti $f \in D[X]$ è un polinomio, allora esistono $a_0, \ldots, a_n \in D$ tali che $f(X) = a_0 + a_1 X + \cdots + a_n X^n$. Applicando ora ai singoli coefficienti il monomorfismo unitario di anelli $i\colon D \to Q(D)$ introdotto nella proposizione 8.3-(i), si ottiene il polinomio $i(f) \in Q(D)[X]$ definito da $i(f)(X) := i(a_0) + i(a_1)X + \cdots + i(a_n)X^n$. L'abuso di notazione permette dunque di identificare i polinomi f e $i(f)$.

Lemma 10.2. *Siano D un dominio a fattorizzazione unica, $F := Q(D)$ e siano $f, g \in D[X]$ due polinomi primitivi. Allora f e g sono associati in $D[X]$ se e solo se sono associati in $F[X]$.*

Dimostrazione. Si osservi innanzitutto che, se f e g sono associati in $D[X]$, allora sono associati anche in $F[X]$ banalmente. Suppongo dunque che f e g siano associati in $F[X]$. Poiché si assume che $F = Q(D)$, per la proposizione 8.2 si ha che F è un campo e in particolare un dominio integrale per l'osservazione 6.5. Dal corollario 10.1-(i) segue quindi che $F[X]$ è un dominio integrale ma allora, per la proposizione 9.1-(vi),

esiste un elemento $u \in U(F[X])$ tale che $f(X) = g(X) \cdot u(X)$. Tenendo a mente il corollario 10.1-(ii) con la relativa dimostrazione, posso affermare che $u \in U(F)$ e di conseguenza $f(X) = u \cdot g(X)$. Inoltre, poiché si assume che $F = Q(D)$, esistono due elementi $a, b \in D$ con $b \neq 0$ tali che $u = \frac{a}{b}$ ma allora, moltiplicando a sinistra per b ambo i membri della relazione precedente, si ottiene che $b \cdot f(X) = a \cdot g(X)$. Si osservi ora che f e g sono polinomi non nulli perché per ipotesi essi sono polinomi primitivi e quindi $C(f), C(g) \neq 0$. Inoltre, se fosse $a = 0$, allora $b \cdot f(X)$ sarebbe il polinomio nullo e di conseguenza, notando che $D[X]$ è un dominio integrale in virtù del corollario 10.1-(i), dovrebbe valere che $b = 0$ oppure f è il polinomio nullo. Entrambe le possibilità contraddicono le assunzioni fatte in precedenza e dunque $a \neq 0$. A questo punto, passando ai contenuti, applicando il lemma di Gauss (lemma 10.1), tenendo a mente la definizione 10.2 e utilizzando infine l'ipotesi che $f, g \in D[X]$ siano due polinomi primitivi, si ottiene la condizione che segue:

$$b \sim b \cdot C(f) = C(b) \cdot C(f) \sim C(b \cdot f) \sim C(a \cdot g) \sim C(a) \cdot C(g) = a \cdot C(g) \sim a$$

Ricordando che l'essere elementi associati è una relazione di equivalenza per la proposizione 9.1-(iv), posso affermare che $a \sim b$ cioè, in virtù della proposizione 9.1-(vi), che esiste un qualche elemento $v \in U(D)$ tale che $a = b \cdot v$. In particolare, da una condizione precedente si deduce che $b \cdot f(X) = b \cdot v \cdot g(X)$ ma allora, ricordando che $D[X]$ è un dominio integrale e che $b \neq 0$, si può applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)) e si ottiene che $f(X) = v \cdot g(X)$. Dalla proposizione 9.1-(v) segue infine che f e g sono associati in $D[X]$ e dunque si ha la tesi. □

Lemma 10.3. *Sia D un dominio a fattorizzazione unica, sia $F := Q(D)$ e sia $f \in D[X]$ un polinomio primitivo e non costante. Allora f è un elemento irriducibile in $D[X]$ se e solo se f è irriducibile in $F[X]$.*

Dimostrazione. Innanzitutto, mi occupo di mostrare il viceversa procedendo per contrapposizione logica. In altre parole dimostro che, se f non è irriducibile in $D[X]$, allora non lo è neanche in $F[X]$. Ovviamente, se $f \in U(D[X])$, allora $f \in U(F[X])$ e di conseguenza f non è irriducibile in $F[X]$. Posso quindi supporre che $f \notin U(D[X])$ e in tal caso, siccome f non è irriducibile in $D[X]$, per la definizione 9.2-(ii) esistono due polinomi $p, q \in D[X]$ con $p, q \notin U(D[X])$ tali che $f(X) = p(X) \cdot q(X)$. Passando al grado nella relazione precedente, si ricava che $\deg(f) = \deg(p \cdot q)$. Ricordando che per ipotesi D è un dominio a fattorizzazione unica e in particolare un dominio integrale, posso applicare l'osservazione 10.4, in virtù della quale vale la formula $\deg(f) = \deg(p) + \deg(q)$, ma per ipotesi f è un polinomio non costante, cioè tale che $\deg(f) \geq 1$ e di conseguenza vi sono due possibilità, a seconda che p e q siano o meno polinomi di grado strettamente positivo. Se $\deg(p) \geq 1$ e $\deg(q) \geq 1$, allora $p, q \notin U(F[X])$ in virtù del corollario 10.1-(ii) con la relativa dimostrazione ed essendo $f(X) = p(X) \cdot q(X)$ posso affermare che f non è irriducibile in $F[X]$. Si assuma ora che p oppure q sia un polinomio di grado 0, cioè costante e non nullo. Naturalmente posso assumere, senza perdita di generalità, che p sia un polinomio costante e non nullo, cioè che esista un qualche $p_0 \in D$ con $p_0 \neq 0$ tale che $p(X) = p_0$. Si noti ora che, se q fosse il polinomio nullo, allora lo sarebbe anche f per la proposizione 6.1-(i), ma questo contraddice l'ipotesi che f sia un polinomio non costante e di conseguenza $q \neq 0$. Passando ora ai contenuti nella relazione $f(X) = p_0 \cdot q(X)$, si ricava che $C(f) \sim C(p_0 \cdot q)$ e quindi, ricordando che per ipotesi f è un polinomio primitivo vale a dire, per la definizione 10.2, che $C(f) \sim 1$ e applicando il lemma di Gauss, cioè il lemma 10.1, si ottiene la condizione seguente:

$$1 \sim C(f) \sim C(p_0 \cdot q) \sim C(p_0) \cdot C(q) = p_0 \cdot C(q)$$

Tenendo a mente che l'essere elementi associati è una relazione di equivalenza per la proposizione 9.1-(iv), dalla relazione precedente si deduce che $p_0 \cdot C(q) \sim 1$ e in particolare, in virtù della definizione 9.1-(ii), si ha che $p_0 \cdot C(q) \mid 1$ cioè, per la definizione 9.1-(i), esiste un elemento $x \in D$ tale che $1 = (p_0 \cdot C(q)) \cdot x$. In particolare, posso affermare che $p_0 \in U(D)$ quindi, in vista del corollario 10.1-(ii), si ha che $p \in U(D[X])$ e questo è assurdo. Dovendo scartare la possibilità in cui p oppure q è un polinomio costante e non nullo, posso concludere che f non è un elemento irriducibile in $F[X]$.

Si assuma adesso che f sia irriducibile in $D[X]$ e si considerino due polinomi fissati $g, h \in F[X]$ tali che $f(X) = g(X) \cdot h(X)$. Anche qui posso distinguere il caso in cui g e h sono polinomi di grado strettamente positivo da quello in cui uno dei due polinomi ha grado 0. In quest'ultimo caso è possibile assumere, senza perdita di generalità, che $\deg(g) = 0$, cioè che g sia un polinomio costante e non nullo. Equivalentemente, esiste un elemento $g_0 \in F$ con $g_0 \neq 0$ tale che $g(X) = g_0$ ma, essendo F un campo per la proposizione 8.2, ogni suo elemento non banale è invertibile e in particolare $g_0 \in U(F)$. Dal corollario 10.1-(ii) segue quindi che anche $g \in U(F[X])$ e questo implica che f è un elemento irriducibile in $F[X]$. Adesso suppongo per

assurdo che $\deg(g) \geq 1$ e $\deg(h) \geq 1$. In tal caso, esistono $a_0, \dots, a_n, b_0, \dots, b_n, c_0, \dots, c_m, d_0, \dots, d_m \in D$ con $a_n, b_0, \dots, b_n, c_m, d_0, \dots, d_m \neq 0$ tali che valgano le due condizioni seguenti:

$$g(X) = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \cdots + \frac{a_n}{b_n}X^n\,, \quad h(X) = \frac{c_0}{d_0} + \frac{c_1}{d_1}X + \cdots + \frac{c_m}{d_m}X^m$$

Si ponga per semplicità $b := b_0 \cdots b_n$ e si consideri il polinomio $g_1 \in D[X]$ definito dalla relazione seguente:

$$g_1(X) := (a_0 \cdot b_1 \cdot b_2 \cdots b_n) + (b_0 \cdot a_1 \cdot b_2 \cdots b_n)X + \cdots + (b_0 \cdots b_{n-1} \cdot a_n)X^n$$

Ripetendo lo stesso argomento utilizzato nella prima parte della dimostrazione del lemma di Gauss, si può affermare che $g_1(X) = C(g_1) \cdot g_2(X)$ per un certo polinomio primitivo $g_2 \in D[X]$. A questo punto, posto $a := C(g_1)$, osservando che $b \neq 0$ per costruzione, tenendo a mente le definizioni di g e g_1 e utilizzando la relazione precedente, si ha che:

$$g(X) = \frac{1}{b} \cdot g_1(X) = \frac{a}{b} \cdot g_2(X)$$

Passando al grado nella relazione precedente e utilizzando l'osservazione 10.4, ricavo che $\deg(g) = \deg(g_2)$ e di conseguenza anche $\deg(g_2) \geq 1$. Naturalmente, ripetendo lo stesso procedimento con h al posto di g, si deduce che esistono $c, d \in D$ con $d \neq 0$ e un polinomio primitivo $h_2 \in D[X]$ tali che $h(X) = \frac{c}{d} \cdot h_2(X)$ e $\deg(h_2) \geq 1$. Ricordando adesso che per ipotesi $f(X) = g(X) \cdot h(X)$, dalla discussione precedente deduco che $f(X) = \frac{a}{b} \cdot \frac{c}{d} \cdot g_2(X) \cdot h_2(X)$ e in particolare, moltiplicando a sinistra per $b \cdot d$ entrambi i membri della relazione ottenuta, posso affermare che $b \cdot d \cdot f(X) = a \cdot c \cdot g_2(X) \cdot h_2(X)$. Adesso, utilizzando il fatto che $f, g_2, h_2 \in D[X]$ sono tre polinomi primitivi e applicando il lemma di Gauss, si ha la seguente condizione:

$$b \cdot d \sim b \cdot d \cdot C(f) \sim C(b \cdot d \cdot f) \sim C(a \cdot c \cdot g_2 \cdot h_2) \sim a \cdot c \cdot C(g_2 \cdot h_2) \sim a \cdot c$$

Come al solito, si può utilizzare il fatto che l'essere elementi associati è una relazione di equivalenza e in particolare una relazione simmetrica e transitiva (proposizione 9.1-(iv)) per ottenere che $a \cdot c \sim b \cdot d$ e di conseguenza, in virtù della proposizione 9.1-(vi), esiste un elemento $u \in U(D)$ tale che $a \cdot c = (b \cdot d) \cdot u$. In particolare, da una relazione precedente segue che $b \cdot d \cdot f(X) = b \cdot d \cdot u \cdot g_2(X) \cdot h_2(X)$ e quindi, notando che $D[X]$ è un dominio integrale per il corollario 10.1-(i) e utilizzando il fatto che $b \cdot d \neq 0$, posso applicare la legge di cancellazione sinistra (osservazione 6.6-(ii)) per ottenere che $f(X) = u \cdot g_2(X) \cdot h_2(X)$. Adesso basta notare che $\deg(u \cdot g_2) = \deg(u) + \deg(g_2)$ di nuovo in virtù dell'osservazione 10.4 e di conseguenza $\deg(u \cdot g_2) \geq 1$. Dal momento che anche $\deg(h_2) \geq 1$ si può affermare, in vista del corollario 10.1-(ii) con la relativa dimostrazione, che $u \cdot g_2, h_2 \notin U(D[X])$ e dunque f non può essere un elemento irriducibile in $D[X]$, contraddicendo le ipotesi. Dalla discussione precedente si deduce che la possibilità in cui $\deg(g) \geq 1$ e $\deg(h) \geq 1$ non è ammessa e posso quindi concludere che f è un elemento irriducibile in $F[X]$. □

Teorema 10.2. *Se D è un dominio a fattorizzazione unica, allora lo è anche $D[X]$.*

Dimostrazione. Sia $f \in D[X]$ un qualunque polinomio non nullo e non invertibile. Distinguo innanzitutto due possibilità, a seconda che f sia o meno un polinomio di grado strettamente positivo. Se $\deg(f) = 0$, cioè se f è un polinomio costante e non nullo, allora esiste un elemento $f_0 \in D$, $f_0 \neq 0$ tale che $f(X) = f_0$ e inoltre, dato che per ipotesi $f \notin U(D[X])$, per il corollario 10.1-(ii) con la relativa dimostrazione si può affermare che $f_0 \notin U(D)$. Posso quindi utilizzare l'ipotesi che D sia un dominio a fattorizzazione unica per affermare che esiste una decomposizione in irriducibili $f_0 = c_1 \cdots c_n$. Detto questo, basterà mostrare che, fissato un indice $1 \leq i \leq n$, l'elemento c_i è irriducibile anche in $D[X]$. Si considerino quindi due polinomi $g, h \in D[X]$ tali che $c_i = g(X) \cdot h(X)$. Passando al grado e usando l'ipotesi che D sia un dominio integrale per poter applicare l'osservazione 10.4, ottengo che $\deg(g) + \deg(h) = 0$, quindi $\deg(g) = 0$ e $\deg(h) = 0$. Esistono dunque $g_0, h_0 \in D$, $g_0, h_0 \neq 0$ tali che $g(X) = g_0$, $h(X) = h_0$, ma allora $c_i = g_0 \cdot h_0$ ed essendo c_i un elemento irriducibile in D vale che $g_0 \in U(D)$ oppure $h_0 \in U(D)$. In virtù del corollario 10.1-(ii), ciò equivale a richiedere che valga $g \in U(D[X])$ oppure $h \in U(D[X])$ e dunque, siccome il risultato ottenuto non dipende dalla scelta dei due polinomi $g, h \in D[X]$ tali che $c_i = g(X) \cdot h(X)$, posso affermare che c_i è anche un elemento irriducibile in $D[X]$. Questo dimostra che $f(X) = c_1 \cdots c_n$ è una decomposizione di f in irriducibili. Suppongo adesso che $\deg(f) \geq 1$. Come si è già osservato nella dimostrazione del lemma di Gauss, vale a dire il lemma 10.1, esiste un polinomio primitivo $f_1 \in D[X]$ tale che $f(X) = C(f) \cdot f_1(X)$. Sia ora $F := Q(D)$ e si noti che F è un campo per la proposizione 8.2. Dal corollario 10.2 segue dunque che $F[X]$ è un dominio euclideo e in particolare, per il teorema 9.2, è anche un dominio a fattorizzazione

unica. Poiché si assume $\deg(f) \geq 1$ posso affermare, in virtù dell'osservazione 10.4, che anche $\deg(f_1) \geq 1$ e quindi $f_1 \notin U(F[X])$ per il corollario 10.1-(ii). Inoltre, vale che $f_1 \neq 0$ perché, se così non fosse, allora si avrebbe che $f = 0$ per la proposizione 6.1-(i), ma questo contraddice le ipotesi. Il polinomio $f_1 \in D[X]$ possiede quindi una decomposizione in irriducibili $f_1(X) = p_1^*(X) \cdots p_n^*(X)$ in $F[X]$. Da un fatto provato nella dimostrazione del lemma 10.3 segue che, comunque fissato $1 \leq i \leq n$, esistono $a_i, b_i \in D$ con $b_i \neq 0$ e un polinomio primitivo $p_i \in D[X]$ tali che $p_i^*(X) = \frac{a_i}{b_i} \cdot p_i(X)$. Si noti adesso che, se fosse $\frac{a_i}{b_i} = 0$ per un certo $1 \leq i \leq n$, allora p_i^* sarebbe il polinomio nullo e questo contraddice l'assunzione che $p_i^* \in F[X]$ sia un elemento irriducibile. Deve dunque valere, per ogni $1 \leq i \leq n$, che $\frac{a_i}{b_i} \neq 0$, quindi $\frac{a_i}{b_i} \in U(F)$ perché F è un campo. Dal corollario 10.1-(ii) segue poi che $\frac{a_i}{b_i} \in U(F[X])$ per ogni $1 \leq i \leq n$, ma allora p_i^* e p_i sono associati in $F[X]$ per la proposizione 9.1-(v) e in virtù del fatto che $p_i^*(X) = \frac{a_i}{b_i} \cdot p_i(X)$. Di conseguenza, in virtù dell'osservazione 9.3-(ii), anche p_i è un polinomio irriducibile per ogni $1 \leq i \leq n$. Ricordando ora la definizione 9.2-(ii), per ogni $1 \leq i \leq n$ si hanno in particolare le due condizioni $p_i \neq 0$ e $p_i \notin U(F[X])$ dalle quali si ricava, in vista del corollario 10.1-(ii), che p_i è un polinomio non costante. Fissato adesso un indice $1 \leq i \leq n$, tenendo a mente che p_i è anche un polinomio primitivo, si può applicare il lemma 10.3, in virtù del quale si ha che p_i è un polinomio irriducibile in $D[X]$. A questo punto, ponendo per semplicità $a := a_1 \cdots a_n$ e $b := b_1 \cdots b_n$, si ottiene che $f_1(X) = \frac{a}{b} \cdot p_1(X) \cdots p_n(X)$. Equivalentemente, se moltiplico a sinistra per b entrambi i membri di tale relazione, ottengo che $b \cdot f_1(X) = a \cdot p_1(X) \cdots p_n(X)$. Adesso, notando che $p_1 \cdots p_n \in D[X]$ è un polinomio primitivo per il lemma di Gauss (lemma 10.1), posso ripetere passo dopo passo l'argomento usato nel corso del lemma 10.2 per ottenere un elemento $u \in U(D)$ tale che $f_1(X) = u \cdot p_1(X) \cdots p_n(X)$. Naturalmente, per il corollario 10.1-(ii) con la relativa dimostrazione si ha che $u \in U(D[X])$ e dunque, in virtù della proposizione 9.1-(v), si ottiene che $u \cdot p_1 \sim p_1$. In particolare, per l'osservazione 9.3-(ii), vale che $u \cdot p_1$ è un polinomio irriducibile in $D[X]$. Ora bisogna distinguere due possibilità. Se $C(f) \in U(D)$ allora, ponendo $v := C(f) \cdot u$ e ripetendo l'argomento appena concluso con v al posto di u, si ottiene che $v \cdot p_1$ è un elemento irriducibile in $D[X]$ e di conseguenza una fattorizzazione di f in irriducibili è data da $f(X) = v \cdot p_1(X) \cdots p_n(X)$. Se invece $C(f) \notin U(D)$, noto che $C(f) \neq 0$ perché si assume che f sia un polinomio non nullo ma allora, dato che per ipotesi D è un dominio a fattorizzazione unica, esiste una decomposizione in irriducibili $C(f) = c_1 \cdots c_m$. Procedendo esattamente come nel caso in cui $\deg(f) = 0$, si mostra che $c_1, \ldots, c_m$ sono anche elementi irriducibili in $D[X]$ e di conseguenza una decomposizione di f in irriducibili è data da $f(X) = c_1 \cdots c_m \cdot u \cdot p_1(X) \cdots p_n(X)$. Dato che il risultato ottenuto non dipende da una particolare scelta del polinomio non nullo e non invertibile $f \in D[X]$, posso concludere che $D[X]$ è un dominio a fattorizzazione.

Ora mi occupo di mostrare che in $D[X]$ vale l'unicità della fattorizzazione. Sia $f \in D[X]$ un polinomio non nullo e non invertibile. Purché si utilizzi la convenzione del prodotto vuoto, cioè purché si definisca $a_1 \cdots a_0 := 1$, due fattorizzazioni qualsiasi di f in irriducibili si possono esprimere nella maniera seguente, con $c_1, \ldots, c_m, d_1, \ldots, d_r \in D$ elementi irriducibili, $p_1, \ldots, p_n, q_1, \ldots, q_s \in D[X]$ polinomi irriducibili non costanti, cioè tali che $\deg(p_i) \geq 1$, $\deg(q_j) \geq 1$ comunque vengano assegnati indici $1 \leq i \leq n$, $1 \leq j \leq s$:

$$\begin{aligned} f(X) &= c_1 \cdots c_m \cdot p_1(X) \cdots p_n(X) \\ f(X) &= d_1 \cdots d_r \cdot q_1(X) \cdots q_s(X) \end{aligned} \tag{14}$$

Sia adesso $1 \leq i \leq n$ un indice fissato e si osservi che, per un fatto già giustificato nella dimostrazione del lemma di Gauss (lemma 10.1), esiste un polinomio primitivo $p_i' \in D[X]$ tale che $p_i(X) = C(p_i) \cdot p_i'(X)$, ma p_i è un polinomio irriducibile in $D[X]$ e dunque si ha $C(p_i) \in U(D[X])$ oppure $p_i' \in U(D[X])$. La seconda possibilità va scartata in quanto contraddice la formula $\deg(p_i) = \deg(p_i')$ data dall'osservazione 10.4 con l'assunzione che $\deg(p_i) \geq 1$. Dovrà dunque valere che $C(p_i) \in U(D[X])$ e quindi, per il corollario 10.1-(ii) con la relativa dimostrazione e in virtù dell'osservazione 9.1, si ha che $C(p_i) \sim 1$. Questo dimostra, data l'arbitrarietà nella scelta dell'indice $1 \leq i \leq n$, che i polinomi $p_1, \ldots, p_n \in D[X]$ sono primitivi. Usando un procedimento del tutto analogo, si vede che anche $q_1, \ldots, q_s \in D[X]$ sono polinomi primitivi. Passando ora ai contenuti nelle relazioni (14), si distinguono due possibilità. Se $m = 0$ allora, per il lemma di Gauss, si avrebbe che $C(f) \sim 1$ e dunque, siccome l'essere elementi associati è una relazione di equivalenza per la proposizione 9.1-(iv), si ottiene che $d_1 \cdots d_r \sim 1$. Se fosse $r \neq 0$ allora, per l'osservazione 9.1, varrebbe che $d_1 \cdots d_r \in U(D)$, cioè esisterebbe un elemento $x \in D$ tale che $(d_1 \cdots d_r) \cdot x = 1$. In particolare, l'elemento irriducibile $d_1 \in D$ sarebbe invertibile e questo è assurdo. Di conseguenza, se $m = 0$, allora anche $r = 0$ e ovviamente, per simmetria, vale anche il viceversa. Suppongo dunque che $m, r \neq 0$ e osservo che, in tal caso, tenendo sempre a mente la definizione 10.2 e applicando nuovamente il lemma di Gauss, si ottiene che $c_1 \cdots c_m \sim d_1 \cdots d_r$. In virtù della proposizione 9.1-(vi), esiste un elemento $u \in U(D)$ tale che si abbia

la relazione $c_1 \cdots c_m = u \cdot d_1 \cdots d_r$, ma $u \cdot d_1 \in D$ è un elemento irriducibile poiché $u \cdot d_1 \sim d_1$ banalmente e vale l'osservazione 9.3-(ii). Di conseguenza, dato che per ipotesi D è un dominio a fattorizzazione unica, in D vale l'unicità della fattorizzazione, quindi $m = r$ e vale, a meno di permutare gli indici e utilizzando la transitività della relazione di associazione, la condizione $c_i \sim d_i$ per ogni $1 \leq i \leq m$. Adesso, ricordando che F è un campo per la proposizione 8.2 e che $c_1, \ldots, c_m, d_1, \ldots, d_r \in D$ sono elementi irriducibili, quindi non nulli, posso affermare che $c_1, \ldots, c_m, d_1, \ldots, d_r \in U(F)$. Quindi, in virtù delle relazioni (14), vale che:

$$p_1(X) \cdots p_n(X) = v \cdot q_1(X) \cdots q_s(X)\,, \quad \text{dove} \quad v := d_1 \cdots d_r \cdot c_1^{-1} \cdots c_m^{-1}$$

Assumo che $n = 0$ e suppongo per assurdo che $s \neq 0$. In tal caso, varrebbe che $v \cdot q_1(X) \cdots q_s(X) = 1$ e in particolare, passando al grado e applicando l'osservazione 10.4, si dovrebbe avere che $\deg(q_j) = 0$ per ogni $1 \leq j \leq s$, ma questo è assurdo. Questo dimostra quindi che, se $n = 0$, allora anche $s = 0$ e naturalmente, per simmetria e in virtù del fatto che $v \in U(F)$, vale anche il viceversa. Suppongo dunque che $n, s \neq 0$ e osservo che $v \cdot q_1 \sim q_1$ banalmente. Dal momento che $q_1 \in D[X]$ è un polinomio irriducibile e ricordando che q_1 è un polinomio primitivo e non costante, in virtù del lemma 10.3 si ha che $q_1 \in F[X]$ è un polinomio irriducibile ma allora, per l'osservazione 9.3-(ii), posso affermare che lo è anche $v \cdot q_1$. Ora, usando il fatto che $F[X]$ è un dominio a fattorizzazione unica in quanto dominio euclideo (teorema 9.2 e corollario 10.2), per l'unicità della fattorizzazione $n = s$ e vale, a meno di reindicizzare gli elementi q_i e per la transitività della relazione di associazione (proposizione 9.1-(iv)), che p_i e q_i sono associati in $F[X]$ comunque fissato un indice $1 \leq i \leq n$. Tenendo infine a mente che $p_1, \ldots, p_n, q_1, \ldots, q_s \in D[X]$ sono polinomi primitivi si può concludere, in virtù del lemma 10.2, che p_i e q_i sono associati in $D[X]$ per ogni $1 \leq i \leq n$. L'unicità delle fattorizzazioni in $D[X]$ è così dimostrata e posso affermare che $D[X]$ è un dominio a fattorizzazione unica. □

Esempio 10.3. In virtù del teorema 10.2 si ha che, in generale, non vale il viceversa del teorema 9.2-(ii). Si consideri infatti un dominio a fattorizzazione unica R che non è un campo. Un tale R esiste perché, in vista degli esempi 6.1 e 9.3, posso scegliere $R := \mathbb{Z}$. Per il teorema 10.2 già menzionato, anche $R[X]$ è un dominio a fattorizzazione unica però, come si è già osservato nell'esempio 10.1, non è un dominio a ideali principali in quanto $(p, X) \lhd R[X]$ non è un ideale principale per ogni $p \in R$ con $p \neq 0$ e con $p \notin U(R)$. Si ha dunque un controesempio al viceversa del teorema 9.2-(ii).

Infine, combinando il teorema 10.2 e l'osservazione 10.3, si ricava immediatamente il seguente fatto.

Corollario 10.3. *Sia $n \in \mathbb{N}$ fissato e sia D un dominio a fattorizzazione unica. Allora $D[X_1, \ldots, X_n]$ è anch'esso un dominio a fattorizzazione unica.*