University of Antananarivo
Department of Mathematics and Computer Sciences

Academic Year 2022-2023

Algebra (4th year)

Lecturer in charge: Gérard Razafimanantsoa

The main objective of this course is to provide a solid foundation in algebra for those interested in coding theory and cryptography

1 Finite Field

1. Structure of Finite Fields
2. Polynomials over Finite Fields
3. Exponential Sums
4. Equations over Finite Fields

2 Function Fields

1. Function Fields of One Variable
2. Extensions of Valuations
3. Constant Field Extensions

3 Algebraic Varieties

1. Affine and Projective Spaces
2. Algebraic Sets
3. Varieties
4. Function Fields of Varieties
5. Morphisms and Rational Maps

4 Algebraic Curves

1. Nonsingular Curves
2. Maps Between Curves
3. Divisors
4. Riemann-Roch Spaces
5. Riemann's Theorem and Genus
6. The Riemann-Roch Theorem

References

[FJ08] Michael Fried and Moshe Jarden. *Field Arithmetic*. 3rd ed. Ergebnisse der Mathematik und ihrer Grenzgebiete 11. Springer, 2008.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite Field*. 2nd ed. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1997.

[LWX13] Sam Ling, Huaxiong Wang, and Chaoping Xing. *Algebraic Curves in Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 2013.

[NX09] Harald Niederreiter and Chaoping Xing. *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press, 2009.

[Pel+18] Ruud Pellikaan et al. *Codes, Cryptology and Curves with Computer Algebra*. Cambridge University Press, 2018.

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes*. 2nd ed. Graduate Texts in Mathematics. Springer, 2009.