Seminar Summer 2016:

Elliptic curves and the Weil conjectures

Wednesday 16–18, M 102
Prof. Dr. Moritz Kerz

Summary:

In this seminar we learn the basic theory of elliptic curves and we prove the Weil conjectures for elliptic curves. Elliptic curves are among the simplest objects in algebraic geometry for which we have a fairly complete understanding geometrically, but which have extremely deep arithemetic aspects. An elliptic curve E is by definition a certain projective algebraic curve which has a group law. In affine coordinates x, y it can (over most fields) be described concretely by a Weierstrass equation of the form

$$y^2 = x^3 + Ax + B \tag{1}$$

with A and B constants.

In talks 1–3 we will summarize with few proofs some background material from algebraic geometry. Details are presented in the parallel lecture *Algebraic geometry II*, but it is not necessary to attend that lecture as we only use these results as a black box. In talks 4–11 we learn the basic theory of elliptic curves over arbitrary perfect field.

Our final goal (talks 12–13) is to understand the number of solutions of equation (1) defining an elliptic curve over finite fields. Hasse proved the important theorem that

$$N = \text{number of solutions of (1) over } \mathbb{F}_q$$

satisfies $|N - q| \leq 2\sqrt{q}$. We will prove this deep inequality and see that it is equivalent to the famous Riemann hypothesis (which is part of the Weil conjectures) for the elliptic curve E, which says that any zero of the Zeta-function $\zeta_E(x) = 0$ satisfies $\mathrm{Re}(x) = 1/2$.

Required knowledge:
Commutative Algebra, Algebraic Geometry I

Modules:
BSem, MV, MSem

Registration:
If you like to participate you have to come to our preliminary discussion on Thursday 4.2.16, 2:15 pm in M 201 or write me an email.

Talks:

1) 13.4. Algebraic varieties: [S] Sec. I.1-I.3 (K. Blomenhofer)

2) 27.4. Discrete valuation rings and algebraic curves: [AM] Sec. 9 and [S] Sec. II.1-II.2, (K. Blomenhofer)

3) 4.5. Divisors, differentials and the Riemann-Roch theorem: [S] Sec. II.3-II.5 (S. Feil)

4) 11.5. Weierstrass equations: [S] Sec. III.1, restrict to $ch(K) \neq 2, 3$ for simplicity, do not discuss the Legendre form (L. Bauer)

5+6) 18.5. The group law: [S] Sec. III.2 and III.3, do not discuss the singular case $\Delta = 0$ (M. Blüml)

7) 25.6. Isogenies: [S] Sec. III.4 (G. Schwalbe)

8) 1.6. The invariant differential: [S] Sec. III.5 (A. Pangerl)

9) 8.6. The dual isogeny: [S] Sec. III.6 (J. Loher)

10) 15.6. The Tate module: [S] Sec. III.7 up to Thm. 7.7 (Y. Mousa)

11) 22.6. The Weil pairing: [S] Sec. III.8 (J. Sotakova)

12) 29.6. Number of rational points: [S] Sec. V.1 (M. Moreschi)

13) 6.7. The Weil conjectures: [S] Sec. V.2 (H.-U. Kufner)

References

[AM] Atiyah, M. F., Macdonald, I. G. *Introduction to commutative algebra*, Addison-Wesley Publishing.

[S] Silverman , J. *The arithmetic theory of elliptic curves*, Graduate Texts in Mathematics **106** Springer-Verlag, New York, 1986.

Email: moritz.kerz@mathematik.uni-r.de