Seminar on Iwasawa Theory of Elliptic Curves

Gabor Wiese

Sommersemester 2008

Abstract

Iwasawa theory studies arithmetic objects in certain p-adic towers of number fields. In this seminar we will focus on the classical case of $\mathbb{Z}_p$-extensions. We will discuss and prove the structure theory of finitely generated modules over the Iwasawa algebra. This will then allow us to derive Iwasawa's theorem on the behaviour of the p-part of the class number in a $\mathbb{Z}_p$-extension of a number field.

Then we will move on to elliptic curves, treating the contents of Greenberg's *Introduction to Iwasawa Theory for Elliptic Curves*. The principal result that we will obtain will be a theorem of Mazur's stating that the rank of an elliptic curve in a $\mathbb{Z}_p$-extension of a number field F is bounded if the Mordell-Weil group and the p-part of the Tate-Shafarevich-group at F are finite.

If time allows, we will make first steps on towards p-adic L-functions and Iwasawa's main conjecture.

- Date: Wednesday, 10-12 a.m.
- Place: ES 09.
- First session: 9 April 2008
- The language of the seminar is English.
- The webpage of the seminar is: http://maths.pratum.net/teaching/Iwasawa.html

Lectures

1 Introduction, Gabor Wiese

2 $\mathbb{Z}_p$-extensions, Adam Mohamed

Define the notion of a $\mathbb{Z}_p$-extension. Define the cyclotomic $\mathbb{Z}_p$-extension for any number field. Define the anti-cyclotomic $\mathbb{Z}_p$-extension for imaginary quadratic fields ([2], p. 5). Treat the $\mathbb{Z}_p$-extension arising from an elliptic curve with complex multiplication (see e.g. [4], Remark III.7.10). Now treat [5], Section 13.1.

3 The completed group algebra and class groups in $\mathbb{Z}_p$-extensions, Eduardo Ocampo

Write Γ for the additive group of $\mathbb{Z}_p$, but with multiplicative notation. Let Γ_n be Γ/Γ^{p^n}, which is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$, but with multiplicative notation. Then Γ is the projective limit of the Γ_n. Define Λ as the projective limit of the group rings $\mathbb{Z}_p[\Gamma_n]$ (as in [2], p. 37, line 3 up to "are the subject of Exercise 3.12"). It is a compact topological ring. Treat Exercise 3.12 of [2].

Recall facts on modules for profinite groups, including Pontryagin duality (see e.g. [3], 1.1.5–1.1.8) and introduce the terminology at the bottom of p. 21 of [2].

Let K_∞/K be a $\mathbb{Z}_p$-extension. For each n let L_n be the maximal unramified abelian p-extension of K_n. Let $X_n := \mathrm{Gal}(L_n/K_n)$. By class field theory this is the p-Sylow subgroup of the class group of K_n. Define X as the projective limit of the X_n. Show that X is isomorphic to $\mathrm{Gal}(L/K_\infty)$, where L is the union of the L_n. Show that X is a topological Λ-module. Some details for this talk can be found on p. 276–277 of [5].

4 The Iwasawa algebra, Marcel Mohyla

The aim of this talk is to establish the isomorphism

$$\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$$

(see [2], Theorem 3.10). More precisely, treat the first paragraph on p. 31 of [2] (not Theorem 3.1). Then prove Weierstraß' preparation theorem, i.e. [2], Theorem 3.5, Corollary 3.6, Corollary 3.7, Theorem 3.8.

5 Modules of the Iwasawa algebra, Ralf Butenuth

Treat [5], Section 13.2, and prove [2], Theorem 3.9. You may also find it helpful to look at the relevant parts of [2], Section 3.

6 Iwasawa's theorem, Marios Magioladitis

Prove Iwasawa's theorem ([5], Theorem 13.13), which describes the behaviour of the p-part of the class number in a $\mathbb{Z}_p$-extension. Please note that we have already provided many of the ingredients in earlier talks. These should not be proved again.

7 Some Galois cohomology, Eduardo Ocampo

Prove [2], Theorem 3.11, and establish that it is a special case of the Corank Lemma ([2], p. 22).

8 Elliptic curves and Galois cohomology I and II, Gabor Wiese (I) and Björn Buth (II)

Recall important properties of elliptic curves defined over number fields (see e.g. [4]) which are needed for this talk, in particular the Mordell-Weil theorem should be stated and the different reductions (e.g. good reduction) should be discussed. Prove [2], Theorem 2.4, Theorem 2.6 (using [2], Theorem 3.11, established in the previous talk rather than duality theory and Euler characteristics), Theorem 2.8 and Theorem 2.9.

9 Mazur's control theorem, Oscar Ledesma

Prove [2], Theorem 4.1.

10 Corollaries of Mazur's control theorem, Lassina Dembélé

Treat [2], Corollaries 4.9, 4.10, 4.11 and 4.12.

11 Further talks

If time allows, we will continue in the direction of p-adic L-functions and Iwasawa's main conjecture. An overview over the construction of the p-adic L-function attached to elliptic curves with complex multiplication ([1]) could be envisaged.

References

[1] Ehud de Shalit: *Iwasawa Theory of Elliptic Curves With Complex Multiplication*

[2] Ralph Greenberg: *Introduction to Iwasawa Theory for Elliptic Curves*, http://www.math.washington.edu/∼greenber/Park.ps

[3] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg: *Cohomology of Number Fields*

[4] Joseph H. Silverman: *The Arithmetic of Elliptic Curves*

[5] Lawrence Washington: *Introduction to Cyclotomic Fields*