Cyclotomic Units

Dimitar P. Jetchev

May 6, 2024

Chapter 1

Introduction

This is my first experimental mini-project to formalize the theory of cyclotomic units in Lean.

Chapter 2

Regulators of Number Fields

This chapter presents basic definitions and results on regulators of number fields.

Let L be a number field with r_1 real and r_2 complex embeddings and let $r = r_1 + r_2 - 1$.

2.1 Definition of the regulator

Let $\epsilon_1, \dots, \epsilon_r$ be a set of independent units of L. Let $\sigma_1, \dots, \sigma_{r_1}$ be the set of real embeddings and let $(\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}), \dots, (\sigma_r, \overline{\sigma}_r)$ be the pairs of conjugate complex embeddings.

Definition 2.1.1. We define the regulator of the units $\epsilon_1, \dots, \epsilon_r$ of L as

$$R_L(\epsilon_1, \dots, \epsilon_r) := \sqrt{\det(\delta_i \log|\sigma_i(\epsilon_j)|)_{i,j}},$$

where

$$\delta_i = \begin{cases} 1 & \text{if } \sigma_i \text{ is real,} \\ 2 & \text{if } \sigma_i \text{ is complex.} \end{cases}$$

Chapter 3

The Index of Cyclotomic Units

3.1 Maximal real subfield

Definition 3.1.1. Let $K = \mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unit. Define the subfield $K^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ of K.

Lemma 3.1.2. *The subfield K^+ is the maximal real subfield of K.*

Proof. □

3.2 Cyclotomic units

Definition 3.2.1. Define the cyclotomic units of a cyclotomic field $K = \mathbb{Q}(\zeta_n)$ with ring of integers $O_K = \mathbb{Z}[\zeta_n]$ as the group

$$C_K := O_K^\times \cap \langle \zeta_n^a, 1 - \zeta_n^b : a, b \in \mathbb{Z}/n\mathbb{Z} \rangle.$$

3.3 Index theorem

Theorem 3.3.1. *Let $n := p^m \in \mathbb{N}$ for a prime p and a positive integer m, and let $K = \mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unit. Let O_K be the ring of integers of K. Let C_K be the group of cyclotomic units in K according to Definition 3.2.1. Then*

$$[O_{K^+}^\times : C_{K^+}] = h_{K^+},$$

where h_{K^+} is the class number of the maximal real subfield K^+ of K.

Proof.

- Show that the regulator of the units $\zeta(a)$ is non-zero, where

$$\zeta(a) := \zeta_{p^m}^{(1-a)/2} \frac{1 - \zeta_{p^m}^a}{1 - \zeta_{p^m}}, \qquad 1 < a < p^m/2, \ (a, p) = 1.$$

- We then compute the regulator $R(\{\zeta(a)\})$.

□

3.3.1 Computing the regulator for K^+

Lemma 3.3.2. *We have*

$$R(\{\zeta(a)\}) = h^+ R^+,$$

where R^+ is the regulator of K^+.

Proof. □

3.3.2 The index of cyclotomic units and the regulator

Lemma 3.3.3. *Let $\epsilon_1, \dots, \epsilon_r$ be independent units of a number field K that generate a subgroup A of the units of K modulo roots of unity and let $\eta_1, \dots, \eta_r$ generate a subgroup B. If $A \subseteq B$ is of finite index then*

$$[B : A] = \frac{R_K(\epsilon_1, \dots, \epsilon_r)}{R_K(\eta_1, \dots, \eta_r)}.$$

Proof. □