First Order Definition of Rings Using Group of Units

By

Michael Kardos

May, 2023

Director of Thesis: Alexandra Shlapentokh, Ph.D.

Major Department: Mathematics

Abstract

We discuss the technical background and relevant research regarding the undecidability of $O_{\mathbb{Q}^{\mathrm{ab}}}$. Given an algebraic extension $K/\mathbb{Q}$, we consider the subring defined by

$$R_K = \{x \in O_K \mid \forall \varepsilon \in U_K \setminus \{1\}\ \exists \delta \in U_K : \delta - 1 \equiv x(\varepsilon - 1) \bmod (\varepsilon - 1)^2\}.$$

We later consider a similar construction over subrings of $\mathbb{Q}$ of characteristic 0. In doing this, we hope to gain insight into the result of the construction of R_K when $K = \mathbb{Q}^{\mathrm{ab}}$.

First Order Definition of Rings Using Group of Units

A Thesis

Presented to the Faculty of the Department of Mathematics

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Master's of Art in Mathematics

By

Michael Kardos

May, 2023

Director of Thesis: Alexandra Shlapentokh, Ph.D.

Thesis Committee Members:

Alexandra Shlapentokh, Ph.D.

Jungmin Choi, Ph.D.

Salman Abdulali, Ph.D.

Acknowledgements

First and foremost, I would like to thank my significant other, Chelsea Wood, and my family for their love and support. Thank you to Dr. Jungmin Choi and Dr. Salman Abdulali for serving as committee members for this thesis. I would also like to thank Dr. Gail Ratcliff for convincing me to major in mathematics and for helping me grow as a mathematician during my years as an undergraduate student. Lastly, I would like to express my utmost gratitude to my thesis advisor, Dr. Alexandra Shlapentokh, for sharing her time, knowledge, and enthusiasm for mathematics with me over the past year. I have learned so much under her guidance.

Contents

Chapter 1

Introduction

One open problem at the forefront of modern algebraic number theory asks whether or not the largest abelian extension of the rationals, denoted $\mathbb{Q}^{\mathrm{ab}}$, has a decidable first-order theory. This is an old problem and one of the first people who studied problems of this type was Julia Robinson who discussed such problems in her 1949 dissertation titled "Definability and Decision Problems in Arithmetic."

In this paper we discuss various ways of approaching this problem. We will start with the minimal necessary background in Number Theory and Logic, more specifically Model Theory. We will then show that under some circumstances to show that the first-order theory of a given ring is undecidable, it is sufficient to prove that the first-order theory of a subring is undecidable. In our case we show how to reduce the problem of $\mathbb{Q}^{\mathrm{ab}}$ to the analogous problem of a subring of its ring of integers. This subring is defined using the unit group of the ring of integers of $\mathbb{Q}^{\mathrm{ab}}$ and contains totally real algebraic integers only (see Chapter 3 for more details).

The undecidability (of the first-order theory) of rings of totally real integers may be easier to prove due to some results of Julia Robinson [Rob62] who established the undecidability of many such rings and provided a general blueprint for proofs of this kind. She conjectured the undecidability of all rings of totally real integers and in view of the reduction we will present

below, this conjecture implies the undecidability of the ring of integers of $\mathbb{Q}^{\text{ab}}$. Unfortunately, to date this conjecture is unproven. Thus, our reduction leaves us with the problem of proving that the ring of totally real integers we obtain as a result of our construction is undecidable.

To understand this problem better, we study the definability technique used to produce the subring of $O_{\mathbb{Q}^{\text{ab}}}$ (the ring of integers of $\mathbb{Q}^{\text{ab}}$). In particular we try to understand the kinds of rings this technique produces when used over subrings of other fields. We start this investigation with subrings of $\mathbb{Q}$ and determine what sort of rings are produced using this definability method. The hope is that in studying the rings produced by our definability technique in a variety of settings we will have a better understanding of the subring of $\mathbb{Q}^{\text{ab}}$ that was constructed.

Chapter 2

First-Order Theory of Rings

This chapter contains the necessary technical background in Logic explaining the meaning of the terms "undecidability" and "first-order theory". We will assume that the reader is familiar with a notion of a ring and just note that in this text the ring is always assumed to be an integral domain of characteristic 0 with unity.

2.1 The language of rings

As a general matter "the first-order theory" of any mathematical object (in our case, a ring) refers to the collections of all sentences in a first-order language true over the chosen object. Thus, we start with explaining the nature of the language we are going use: the first-order language of rings. The first order language of unital rings has an **alphabet**, which is a set made up of the constants 0 and 1, the functions defined by addition and multiplication, an equivalence relation ($=$), logical symbols ($\neg$, $\wedge$, $\vee$, $\exists$, $\forall$), parentheses, variables, and predicate symbols. (Predicates are boolean functions, that is functions with the range equal to the set $\{0, 1\}$.) We frequently refer to constant and variables symbols as **terms** in the first order language, and we call functions and predicates n-ary if they take n terms as arguments. Using this alphabet we may define the set of well-defined **formulas**, which is constructed as follows:

1. Any n-ary predicate symbol P is a formula.

2. If φ and ψ are formulas then so are $\neg\varphi$, $(\varphi \wedge \psi)$, and $(\varphi \vee \psi)$.

3. If x is a variable and φ a formula, then $(\exists x)\varphi$ and $(\forall x)\varphi$ are formulas.

4. No other strings are formulas.

There are two types of variables occurring in the formulas of our language: free variables and bound variables. We say a variable x is **bound** whenever it is in the scope of some quantifier where the variable of quantification is x. If a variable is not bound, then we say it is **free**. The formulas with all variables bound are called **sentences**, and the set of all first-order sentences that are true of a ring is the **first-order theory** of rings in the first-order language of rings. Note that the term first-order refers to the fact that we are only allowed to quantify over elements of the ring in question and not, for example, sets like in a second-order theory.

2.2 Computable functions and computable sets

One of the notions which will be important to us in this paper is the notion of computable functions. Informally, a **computable function** is a function whose domain and range are the natural numbers and whose value on every input is determined by a uniform algorithm, an algorithm independent of the input.

There are rigorous definitions of computable functions using Turing machines or some basic functions like addition, projection, etc. For examples, see [RF19].

Using the notion of a computable function, one can define a computable subset of the natural numbers.

Definition 2.2.1. A subset S of $\mathbb{N}$ is **computable** if its characteristic function is computable. A set S is called **computably enumerable** if the set is either empty or isomorphic to the range of some computable function.

It is not hard to see that the following lemma holds.

Lemma 2.2.2. *A subset S of $\mathbb{N}$ is computable if and only if the set and its complement are both computable enumerable.*

Remark 2.2.3. *Computable sets are also called* ***decidable****.*

2.2.1 Computable subsets of countable structures

We can transfer the notion of computable and computably enumerable sets to any countable structure. We remind the reader that a set is countable if it can be injectively mapped into the natural numbers. One can use this injection to define computable and computably enumerable subsets of the structure. More specifically, let A be a countable structure and let $\phi : A \to \mathbb{N}$ be an injection. A subset B of A is called computable, if $\phi(B)$ is computable in $\mathbb{N}$ and similarly B is called computably enumerable if $\phi(B)$ is computably enumerable in $\mathbb{N}$. Unfortunately the computable status of a structure can depend on the nature of the coding into $\mathbb{N}$. Below we will specify the coding before discussing computable and computably enumerable subsets of structures.

We will apply these ideas to define computable and computably enumerable subsets of countable rings as well as computable and computably enumerable sets of sentences in the first-order language of rings. Note that the set of well-formed formulas in the language of rings is countable.

2.3 Well-defined formulas in the language of rings

One can show by induction that a well-formed formula without occurrences of quantifiers, negations, conjunctions, or disjunctions is a polynomial or a polynomial equation. If we restrict ourselves to formulas which can become sentences (with addition of quantifiers or substitutions of constants for variables), then we will be considering polynomial equations only. Furthermore, we may reduce any polynomial equation to the form $P(\bar{X}) = 0$, where

$P(\bar{X}) \in R[\bar{X}]$, by adding the additive inverse of the right-hand side to both sides of the equation.

If we now allow use of quantifiers, conjunctions, and disjunctions, using prenex normal form, we can rewrite our formula in the form

$$E_1 x_1 \cdots E_r x_r \psi(x_1, \ldots, x_r, y_1, \ldots, y_m),$$

where ψ is constructed by taking conjunctions and disjunctions of polynomial equations.

Observe that negation of a polynomial equation just means that the polynomial is not zero. To deal with this situation, we will use the following lemma (see the proof of Proposition 2.2.4 in [Shl06]) applying to all rings of interest in this paper.

Lemma 2.3.1. *Let K be an algebraic extension of $\mathbb{Q}$, let R be a subring of K, and let x be an element of R. Then the statement $x \neq 0$ is equivalent to $\exists y_1 \cdots \exists y_r P(x, y_1, \ldots, y_r) = 0$, for some $P(X, Y_1, \ldots, Y_r) \in R[X, Y_1, \ldots, Y_r]$.*

From [Shl06] we get the following instance of the lemma above for the case of $R = \mathbb{Z}$. The polynomial $P(x, y_1, y_2, y_3)$ in this case can be taken to be $xy_3 - (2y_1 - 1)(3y_2 - 1)$.

Suppose $xy_3 - (2y_1 - 1)(3y_2 - 1) = 0$. Then $xy_3 = (2y_1 - 1)(3y_2 - 1)$. Assume now $x = 0$. Then either $y_1 = \frac{1}{2}$ or $y_2 = \frac{1}{3}$. Since $\frac{1}{2}, \frac{1}{3} \notin \mathbb{Z}$, it follows that if this polynomial equation holds, then $x \neq 0$. Suppose now $x \neq 0$. Then write $x = x_1 x_2$, where $(x_1, 2) = 1$ and $(x_2, 3) = 1$. Let $y_1 \equiv \frac{1}{2} \bmod x_1$ and let $y_2 \equiv \frac{1}{3} \bmod x_2$. Now we have that $(2y_1 - 1) \equiv 0 \bmod x_1$ and $(3y_2 - 1) \equiv 0 \bmod x_2$. Therefore, the right-hand side of the equation above is equivalent to $0 \bmod x$. Hence, there exists $y_3 \in \mathbb{Z}$, $y_3 = \frac{(2y_1-1)(3y_2-1)}{x}$. Thus, $x \neq 0$ if and only if $\exists y_1, y_2, y_3 \in \mathbb{Z} : xy_3 = (2y_1 - 1)(3y_2 - 1)$.

This lemma allows us to avoid considering formulas of the form $P(\bar{X}) \neq 0$. One can now show by induction that $\neg E_1 x_1 \cdots E_r x_r \psi(x_1, \ldots, x_r, y_1, \ldots, y_m)$, where ψ is a well-formed formula without occurrence of any quantifiers, is equivalent to $\bar{E}_1 x_1 \cdots \bar{E}_r x_r \neg\psi(x_1, \ldots, x_r, r_1, \ldots, y_m)$. By assumption and the lemma above, ψ is a conjunction and disjunction of polynomial equa-

tions. Since this paper concerns integral domains, a disjunction of two polynomial equations can be converted to one equation by using multiplication. Using the distributive property of conjunction over disjunction

$$R \wedge (P \vee Q)) = (R \wedge P) \vee (R \wedge Q)$$

and DeMorgan's law if necessary, by induction on the number of operations used to construct the formula, we can conclude that both ψ and $\neg\psi$ are disjunctions of systems of polynomial equations.

2.4 Defining subsets of rings in the first-order language of rings

Let R be a ring and let $p(\overline{t}, \overline{x})$ be a well-formed formula in the first-order language of rings, where $\overline{t} = (t_1, \ldots, t_k)$ and $\overline{x} = (x_1, \ldots, x_m)$. Let E_i for $i = 1, \ldots, m$ denote m quantifiers each of which may be either universal or existential. Let $A \subset R^k$ be defined as follows

$$A = \left\{(t_1, \ldots, t_k) \in R^k \,|E_1 x_1 \in R \cdots E_m x_m \in R \; p(\overline{t}, \overline{x})\right\}.$$

Then we call $E_1 x_1 \cdots E_m x_m \; p(\overline{t}, \overline{x})$ a **first-order definition** of the set A over R.

It is possible to show that if $\mathrm{Frac}(R)$ is not algebraically closed, any finite system polynomial equations can be collapsed into a single polynomial equation in the appropriate variables such that the resulting polynomial equation holds if and only if the system of equations holds (see Lemma 1.2.3 in [Shl06]).

We now prove a result connecting the undecidability of the first-order theory of a subring to the undecidability of the first-order theory of the ring that contains it.

Proposition 2.4.1. *Let $R_1 \subset R_2$ be two integral domains and assume that R_1 has a first-*

order definition over R_2. In other words there exists a well-formed formula $P(t, x_1, \ldots, x_m)$ composed of disjunctions, conjunctions, and negations of polynomial equations in the variables $t, x_1, \ldots, x_m$ such that for some sequence of quantifiers $E_1, \ldots, E_m$, where each E_i is either an existential or a universal quantifier, for any $t \in R_2$ the sentence

$$E_1 x_1 \ldots E_m x_m P(t, x_1, \ldots, x_m)$$

is true if and only if $t \in R_1$. Let $Q(t_1, \ldots, t_k)$ be a well-formed formula in the first-order language of rings, and let $E_1, \ldots E_k$ be a sequence of quantifiers. Then there exists a first-order formula $R(\bar{t}, \bar{z})$ such that for some fixed sequence of quantifiers $\hat{E}_1, \ldots, \hat{E}_r$ the sentence

$$\hat{E}_1 t_1 \ldots \hat{E}_k t_k \hat{E}_{k+1} z_1 \ldots \hat{E}_r z_{r-k} R(\bar{t}, \bar{z}) \tag{2.1}$$

is true over R_2 if and only if $E_1 t_1 \ldots E_k t_k Q(\bar{t})$ is true over R_1. Further, the construction of (2.1) is algorithmic given the sentence $E_1 \ldots E_k Q(t_1, \ldots, t_k)$.

Proof. We first take care of the trivial case. If $R_1 = R_2$, then the result clearly holds because $E_1 t_1 \cdots E_k t_k Q(\bar{t})$is both a statement over R_1 and R_2. Now, for the remainder of the proof assume $R_1 \subsetneq R_2$.

Let $n_1, \ldots, n_j$ be the indexes such that E_{n_i} is a universal quantifier, then we claim the sentence

$$E_1 t_1 \cdots E_k t_k \left(Q(\bar{t}) \wedge \left(\bigwedge_{i=1}^{k} E_{i1} x_{i1} \cdots E_{im} x_{im} P(t_i, \bar{x}_i) \right) \right. \tag{2.2}$$
$$\left. \vee \left(\bigvee_{i=1}^{j} \neg (E_{n_i 1} x_{n_i 1} \cdots E_{n_i m} x_{n_i m} P(t_i, \bar{x}_i)) \right) \right)$$

or, equivalently,

$$E_1 t_1 \cdots E_k t_k \left(Q(\bar{t}) \wedge \left(\bigwedge_{i=1}^{k} E_{i1} x_{i1} \cdots E_{im} x_{im} P(t_i, \bar{x}_i) \right) \right.$$
$$\left. \vee \neg \bigwedge_{i=1}^{j} E_{n_i 1} x_{n_i 1} \cdots E_{n_i m} x_{n_i m} P(t_i, \bar{x}_i) \right)$$

is true over R_2 if and only if $E_1 t_1 \ldots E_k t_k Q(\bar{t})$ is true over R_1.

First suppose $E_1 t_1 \cdots E_k t_k Q(\bar{t})$ is true over R_1 and take $\bar{t} \in R_2^k$. Since $Q(\bar{t})$ holds over R_1, for each existential quantifier in $E_1, \ldots, E_k$, we may find a corresponding element of R_1 such that $Q(\bar{t})$ is true for every $(t_{n_1}, \ldots, t_{n_j}) \in R_1^j$. Therefore, (2.2) holds in this case. Furthermore, if $(t_{n_1}, \ldots, t_{n_j}) \notin R_1^j$, then some t_{n_i} is not in R_1. It follows that

$$\neg(E_{n_i} x_{n_i 1} \cdots E_{n_i m} x_{n_i m} P(t_i \bar{x}_i))$$

is true, so (2.2) is true still. Thus, we may find a corresponding $t_i \in R_1$ for each existential quantifier such that for any $(t_{n_1}, \ldots, t_{n_j}) \in R_2^j$, (2.2) holds.

Now suppose (2.2) is true over R_2. Then we may find elements to pair with the existential quantifiers such that for all $(t_{n_1}, \ldots, t_{n_j}) \in R_2^j$, the statement holds. Since $R_1^j \subset R_2^j$, this implies that we may find elements to pair with the existential quantifiers such that (2.2) holds for all $(t_{n_1}, \ldots, t_{n_j}) \in R_1^j$. Notice, however, that

$$\neg \bigwedge_{i=1}^{j} E_{n_i 1} x_{n_i 1} \cdots E_{n_i m} x_{n_i m} P(t_i, \bar{x}_i)$$

is false whenever $(t_{n_1}, \ldots, t_{n_j}) \in R_1^j$. Thus, for (2.2) to be true in this case,

$$Q(\bar{t}) \bigwedge_{i=1}^{k} E_{i1} x_{i1} \cdots E_{im} x_{im} P(t_i, \bar{x}_i)$$

must be true. It follows that the items paired with the existential quantifiers must be in R_1

and $Q(\bar{t})$ must hold for these paired elements and all $(t_{n_1}, \ldots, t_{n_j}) \in R_1^j$. In other words, we may find elements in R_1 to pair with the existential quantifiers such that $Q(\bar{t})$ is true for all $(t_{n_1}, \ldots, t_{n_j}) \in R_1^j$. This is that same as saying $E_1 t_1 \cdots E_k t_k Q(\bar{t})$ is true over R_1, completing the proof. $\square$

In short, the above result shows that the first-order language of a given ring R is undecidable if there exists a subring S of R such that the first-order language of S is undecidable.

Chapter 3

Technical Background

3.1 Elementary Number Theory

The background in elementary number theory needed for this thesis is minimal. Aside from the basic definitions, which we assume the reader is familiar with, we define the Euler phi-function and use it to state Euler's theorem.

Definition 3.1.1. Let $n \in \mathbb{Z}$ with $n > 0$. We define the **Euler phi-function**, denoted $\phi(n)$ and sometimes called **Euler's totient function**, as follows:

$$\phi(n) = |\{x \in \mathbb{Z} : 1 \leq x \leq n; \gcd(x, n) = 1\}|.$$

(See Definition 7 in Chapter 2 of [Str94].) Next, we state Euler's theorem concerning the totient function.

Theorem 3.1.2 (Euler's Theorem)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$. If $\gcd(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \mod m.$$

(See Theorem 2.17 in [Str94].) When m is prime, this result is referred to as Fermat's little theorem.

3.2 Groups and Rings

3.2.1 Groups

Definition 3.2.1. Let G be an abelian group. We define the **rank** of G to be the cardinality of the maximal linearly independent subset.

Here linear independence is defined in the usual way with G viewed as a $\mathbb{Z}$-module. The definition above is the usual definition of group rank and operates under the assumption that the operation on the abelian group G is addition, as is the standard practice in algebra. However, in the case of the unit group, the operation is multiplication. In this case, we replace the notion of linear independence with that of multiplicative independence.

Definition 3.2.2. Let G be an abelian multiplicative group. We say a subset H of G is **multiplicatively independent** if for any finite subset I of H

$$\prod_{h \in I} h^{a_h} = 1$$

implies $a_h = 0$ for all h.

Next, we define a short exact sequence of group homomorphisms.

Definition 3.2.3. A sequence of group homomorphisms of the form

$$1 \longrightarrow H \xrightarrow{\phi} G \xrightarrow{\psi} K \longrightarrow 1,$$

where ϕ is injective, ψ is surjective, and $\mathrm{im}(\phi) = \ker(\psi)$ is called a **short exact sequence**.

The following theorem will be used later in the paper.

Theorem 3.2.4 (Generalized Rank-Nullity)**.** *If*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is a short exact sequence of finitely generated abelian groups, then

$$\operatorname{rank}(B) = \operatorname{rank}(A) + \operatorname{rank}(C).$$

For a proof of the above theorem, see Proposition 9.16 in [Lee00].

3.2.2 Commutative rings with unity and no zero-divisors

Below all rings are assumed to be commutative integral domains with unity of characteristic 0. If an element r of a ring R has a multiplicative inverse, then we say r is a **unit**. We often denote the set of (multiplicative) units of R by U_R and call it the **unit group**.

Since we assume that the ring R is a commutative ring, the unit group is abelian.

We now define an integral closure of a ring.

Definition 3.2.5. Given a ring R and a subring S of R, any element $r \in R$ such that r is a root of a monic polynomial over S is said to be **integral** over S. The set of elements that are integral over S is called the **integral closure** of S in R.

Let S and R be defined as above. The following result (Theorem 2.3 in [Jan96]) tells us that the integral closure of S is a subring of R.

Theorem 3.2.6. *Let S be a subring of the ring R. The set of elements of R which are integral over S is a subring of R containing S.*

Next, we will introduce a notion of divisibility in a ring R.

Definition 3.2.7. We define the symbol $|_R$ to mean **divides** in the ring R. That is, if we have $a, b \in R$ with $a|_R b$, then there exists some $c \in R$ such that $b = ac$. Similarly, we define $a \equiv_R b \mod m$, read a is **congruent to** b **modulo** m, for $a, b, m \in R$ if and only if $m|_R(a - b)$.

Next we show that divisibility in a subring implies divisibility in the ring.

Proposition 3.2.8. *Let S be a subring of a ring R. Then for any $a, b, m \in S$,*

$$a \equiv_S b \mod m$$

implies

$$a \equiv_R b \mod m.$$

Proof. Suppose $a \equiv_S b \mod m$. Then $m|_S(a-b)$. That is, there exists some element $c \in S$ such that $mc = a - b$. However, since a, b, c, and m are also elements of R, we have $m|_R(a-b)$ and $a \equiv_R b \mod m$. □

3.3 Using groups of units to construct subrings

Some of the ideas in this section are taken from [MRS23].

We now construct a subring using units of an integral domain R of characteristic zero.

Definition 3.3.1. Let R be a ring (under assumptions at the beginning of this section). We define a subring $\hat{R}$ of R by the following: $x \in \hat{R}$ if and only if for every unit $\varepsilon \in R$ with $\varepsilon \neq 1$ there exist a unit $\delta \in R$ such that

$$x \equiv_R \frac{\delta - 1}{\varepsilon - 1} \mod (\varepsilon - 1).$$

That is, take U_R to be the unit group in R, then

$$\hat{R} = \left\{ x \in R \middle| (\forall \varepsilon \in U_R \setminus \{1\})(\exists \delta \in U_R) \left(x(\varepsilon - 1) \equiv_R (\delta - 1) \bmod (\varepsilon - 1)^2 \right) \right\}.$$

It turns out that $\hat{R}$ is a ring.

Lemma 3.3.2. *Let R be a ring. If $x \in R$ and for some $\delta, \varepsilon \in U_R$ with $\varepsilon \neq 1$ we have that*

$$x(\varepsilon - 1) \equiv_R (\delta - 1) \bmod (\varepsilon - 1)^2$$

then $\delta \equiv_R 1 \bmod (\varepsilon - 1)$.

Proof. By definition of equivalence there exists $y \in R$ such that

$$x(\varepsilon - 1) - y(\varepsilon - 1)^2 = (\delta - 1).$$

Thus, $(\varepsilon - 1)|_R(\delta - 1)$ and $\delta - 1 \equiv_R 0 \bmod (\varepsilon - 1)$. It follows that

$$\delta \equiv_R 1 \bmod (\varepsilon - 1).$$

□

Corollary 3.3.3. *In the notation of the lemma above* $\frac{\delta - 1}{\varepsilon - 1} \in R$.

We now prove $\hat{R}$ is a ring.

Proposition 3.3.4. *$\hat{R}$ as defined above is a subring of R.*

Proof. To show that $\hat{R}$ is a subring of R, we will use the subring test, which involves showing closure under subtraction, closure under multiplication, and that the subset in question contains 1. First note that $1 \in \hat{R}$ since for every unit $\varepsilon \neq 1$,

$$1 \equiv_R \frac{\varepsilon - 1}{\varepsilon - 1} \mod (\varepsilon - 1).$$

Further, for any $x, y \in \hat{R}$, for any unit $\varepsilon \neq 1$, there exists units δ_1, δ_2 such that

$$\begin{aligned} x - y &\equiv_R \frac{\delta_1 - 1}{\varepsilon - 1} - \frac{\delta_2 - 1}{\varepsilon - 1} \\ &= \frac{(\delta_1 - 1) - (\delta_2 - 1)}{\varepsilon - 1} \\ &= \frac{\delta_1 - \delta_2}{\varepsilon - 1} \\ &= \delta_2 \frac{\delta_2^{-1}\delta_1 - 1}{\varepsilon - 1} \\ &\equiv_R \frac{\delta_2^{-1}\delta_1 - 1}{\varepsilon - 1} \mod (\varepsilon - 1). \quad \text{[Lemma 3.3.2]} \end{aligned}$$

Thus, $\hat{R}$ is closed under subtraction.

All that is left to prove is closure under multiplication. Let $x, y \in \hat{R}$ and let $\varepsilon \in U_R \setminus \{1\}$. First assume $y \equiv_R 0 \bmod (\varepsilon - 1)$. Then

$$xy \equiv_R 0 \bmod (\varepsilon - 1)$$

and

$$xy \equiv_R \frac{1-1}{\varepsilon - 1} \bmod (\varepsilon - 1)$$

Now, without loss of generality we can assume that neither x nor y are divisible by $\varepsilon - 1$. Then there exists a unit $\delta_2 \neq 1$ in R such that

$$y \equiv_R \frac{\delta_2 - 1}{\varepsilon - 1} \mod (\varepsilon - 1).$$

We may then find some unit $\delta_1 \in R$ such that

$$x \equiv_R \frac{\delta_1 - 1}{\delta_2 - 1} \mod (\delta_2 - 1).$$

Since $(\varepsilon - 1)|_R(\delta_2 - 1)$ by the proof of Lemma 3.3.2, we have

$$x \equiv_R \frac{\delta_1 - 1}{\delta_2 - 1} \mod (\varepsilon - 1).$$

Thus,

$$xy \equiv_R \frac{\delta_1 - 1}{\delta_2 - 1}\frac{\delta_2 - 1}{\varepsilon - 1} = \frac{\delta_1 - 1}{\varepsilon - 1} \mod (\varepsilon - 1).$$

It follows that $\hat{R}$ is a subring of R. □

Remark 3.3.5. *What other elements of R are in $\hat{R}$? Observe that $\mathbb{Z} \subset \hat{R}$ because $\hat{R}$ is a ring of characteristic 0.*

Looking ahead, the result stated above will be of particular use to us because the ring

of integers for any extension of $\mathbb{Q}$ will be an integral domain of characteristic zero. Hence when we look at the hat subring of the ring of integers, the proposition above tells us that we will always have $\mathbb{Z}$ as a subring.

3.4 Field extensions

For the purpose of this section, we assume that the reader is familiar with the basics of field theory. A good reference for this material is [Art91].

We remind the reader about some definitions from number theory. A finite extension of $\mathbb{Q}$ is called a **number field**. Given an extension K of $\mathbb{Q}$, we define the **ring of integers** of K, denoted O_K, to be the integral closure of $\mathbb{Z}$ in K. We will let U_K denote the group of units of O_K

We now state some important properties of the ring of integers O_K.

Proposition 3.4.1. *Any nonzero prime ideal $\mathfrak{p}$ of O_K is maximal.*

The above proposition follows from the introduction in Section 9 of [Jan96].

Theorem 3.4.2. *Let $\mathfrak{A}$ be a nonzero ideal of O_K. Then $\mathfrak{A}$ is contained in only a finite number of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{A} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ for some positive integers a_i.*

(See Theorem 3.13 in [Jan96].)

Theorem 3.4.3. *Given any nonzero prime ideal $\mathfrak{p}$ in O_K and positive integer a, the quotient ring $O_K/\mathfrak{p}^a$ is finite.*

The above proposition follows from Theorem 6.6 (b) [Jan96] and the fact that the residue ring of any ideal of $\mathbb{Z}$ is finite.

Given the theorem above, we consider what happens when we take the quotient of O_K over a product of prime ideals.

Theorem 3.4.4. *Given distinct nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ in O_K and positive integers $a_1, \ldots, a_n$, the quotient ring $O_K/\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ is finite.*

Proof. Let $\mathfrak{A} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$. By the Chinese Remainder Theorem,

$$O_K/\mathfrak{A} \cong O_K/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus O_K/\mathfrak{p}_n^{a_n}.$$

Since each $O_K/\mathfrak{p}_i^{a_i}$ is finite by Theorem 3.4.3, $O_K/\mathfrak{A}$ must be finite. □

Next we give a few results regarding relatively prime elements in the ring of integers O_K of an extension K.

Definition 3.4.5. Let K be a number field and let $x, y \in O_K$. We say x and y are **relatively prime** if there exists some $a, b \in O_K$ such that $ax + by = 1$.

Proposition 3.4.6. *Let K be a number field with $x, y \in O_K$ such that x and y are relatively prime. Then $x^m \equiv_{O_K} 1 \bmod y$, where m is the order of the multiplicative subgroup of units in $O_K/(yO_K)$.*

Corollary 3.4.7. *Let K be a number field with $x, y \in O_K$ such that $x \in U_K$ and $y \neq 0$. Then $x^m \equiv_{O_K} 1 \bmod y$, where m is the order of the multiplicative subgroup of units in $O_K/(yO_K)$.*

The proof of the above proposition is similar to that of Euler's theorem. The corollary follows immediately from the fact that if x is a unit, then x and y are relatively prime. Further, any ideal of O_K has a finite residue ring by Theorem 3.4.4.

Remark 3.4.8. *One can show that there exists some $m \in \mathbb{Z}_{>0}$ such that $x^m \equiv_{O_K} 1 \bmod y$ in an infinite algebraic extension K of $\mathbb{Q}$ by taking the elements $x, y \in O_K$ and viewing them as elements in $O_{\mathbb{Q}(x,y)}$. Then we may apply the proposition and corollary above to the infinite case.*

If K is a number field, we call its embedding ϕ into a fixed algebraic closure of $\mathbb{Q}$, denoted $\bar{\mathbb{Q}}$, **real** if $\phi(K) \subset \overline{\mathbb{Q}} \cap \mathbb{R}$. Whenever an embedding of a number field is not real, we call it **complex**. If all embeddings of K into $\bar{\mathbb{Q}}$ are real then we say K is a **totally real** number field. Similarly, if K has no real embeddings, then we call K a **totally complex** number field.

The embeddings of a number field K have the additional property that they map rings of integers to rings of integers.

Proposition 3.4.9. *Let K be a number field and $\bar{\mathbb{Q}}$ a fixed algebraic closure of $\mathbb{Q}$. Then, for any embedding $\phi : K \longrightarrow \bar{\mathbb{Q}}$, we have $\phi(O_K)$ is the ring of algebraic integers of $\phi(K)$.*

Proof. Let $\alpha \in K$. Then $\alpha \in O_K$ if and only if there exists a monic polynomial with integer coefficients, call it $p(x)$, such that $p(\alpha) = 0$. Taking ϕ on both sides of this equation yields $p(\phi(\alpha)) = 0$, since ϕ is the identity over $\mathbb{Q}$ and p has integer coefficients. Hence $\phi(\alpha)$ is an algebraic integer in $\phi(K)$.

Now suppose $\phi(\alpha) \in O_{\phi(K)}$, then there would exists some polynomial $q(x) \in \mathbb{Z}[x]$ such that $q(\phi(\alpha)) = 0$. This implies $q(\alpha) \in \ker(\phi)$. Since ϕ is injective by the definition of an embedding, we must have $q(\alpha) = 0$. Thus, $\alpha \in O_K$. This concludes the proof that $\phi(O_K) = O_{\phi(K)}$. □

3.5 Units of rings of integers of number fields

The following theorem links the embeddings of a number field K to the rank of its unit group.

Theorem 3.5.1 (Dirichlet's Unit Theorem)**.** *Let K be a number field and $\bar{\mathbb{Q}}$ a fixed algebraic closure of $\mathbb{Q}$. If r denotes the number of real embeddings of K into $\bar{\mathbb{Q}}$ and s denotes the number of conjugate pairs of complex embeddings of K into $\bar{\mathbb{Q}}$, then U_K is finitely generated and*

$$\operatorname{rank}(U_K) = r + s - 1.$$

Furthermore, $[K : \mathbb{Q}] = r + 2s$.

For a proof of Dirichlet's unit theorem, see Theorem 13.12 in [Jan96]. We can use the unit theorem to compare the ranks of unit groups of field extensions.

Proposition 3.5.2. *Given an extension L/K with the map $N : U_L \longrightarrow U_K$ defined by $N(u_L) = N_{L/K}(u_L)$. The following holds:*

$$\text{rank}(\ker(N)) = \text{rank}(U_L) - \text{rank}(U_K).$$

Proof. Since the unit group is always finitely generated by the proof of Dirichlet's unit theorem (see Theorem 13.12 in [Jan96]), we may apply the generalized rank-nullity theorem to the short exact sequence

$$1 \longrightarrow \ker(N) \longrightarrow U_L \xrightarrow{N} U_K \longrightarrow 1.$$

This gives

$$\text{rank}(U_L) = \text{rank}(\ker(N)) + \text{rank}(U_K),$$

which proves our claim. □

We now look at a particular subcase that gives $\text{rank}(U_L) = \text{rank}(U_K)$. This case will be of interest because, by the proposition above, $\text{rank}(\ker(N)) = 0$ when this occurs.

Proposition 3.5.3. *Let K and L be number fields with $[K : \mathbb{Q}] = n$, $[L : K] = 2$, K totally real, and L totally complex. Since $K \subset L$, we have $U_K \subset U_L$. Let N be defined as above. Then*

$$\text{rank}(U_L) = \text{rank}(U_K),$$

so the kernel of N has rank 0.

Proof. By Dirichlet's unit theorem, $\text{rank}(U_K) = n - 1$ and $\text{rank}(U_L) = n - 1$. Hence, $\text{rank}(U_K) = \text{rank}(U_L)$, as claimed. □

3.6 Some results from Galois theory

We now remind the reader of a result from Galois theory.

Theorem 3.6.1. *Let L/F be a Galois extension, and let K be an intermediate field. Let $H = Gal(L/K)$ be the corresponding subgroup of $G = Gal(L/F)$. Then K is a Galois extension of F if and only if H is a normal subgroup of G. When this is so, $Gal(K/F)$ is isomorphic to the quotient group G/H.*

(See Theorem 5.6 (b) in Chapter 14 of [Art91].) Next, we give a description of the characteristic polynomial of an element in terms of the embeddings of K into L.

Lemma 3.6.2. *Let $F \subset K \subset L$ be a chain of field extensions with L Galois over F. Take $a \in K$ and let Σ be the set of embeddings of K into L leaving F fixed. Then the characteristic polynomial for a over F is*

$$f(x) = \prod_{\sigma \in \Sigma} (x - \sigma(a)).$$

(See 10.25 in [Axl15].) Using the lemma above we obtain the following relationship to the norm map of a over F.

Lemma 3.6.3. *Let K be a separable extension over a field F. Take $a \in K$ such that $f(x)$ is the characteristic polynomial of a over F and let $b \in F$. Then $N_{K/F}(b - a) = f(b)$.*

Proof. Let Σ be the set of all embeddings of K into some fixed Galois extension L over F. Then for $y \in K$, we have

$$N_{K/F}(y) = \prod_{\sigma \in \Sigma} \sigma(y) \text{ and } f(x) = \prod_{\sigma \in \Sigma} (x - \sigma(a)).$$

Therefore,

$$N_{K/F}(b - a) = \prod_{\sigma \in \Sigma} \sigma(b - a) = \prod_{\sigma \in \Sigma} (b - \sigma(a)) = f(b).$$

□

3.7 Abelian and cyclotomic extensions

A Galois extension L of a field F is called **abelian** whenever $\mathrm{Gal}(L/F)$ is an abelian group.

A theorem from class field theory tells us precisely when a number field is an abelian extension of $\mathbb{Q}$. The theorem is known as the Kronecker-Weber theorem.

Theorem 3.7.1 (Kronecker-Weber)**.** *A number field L is an abelian extension of $\mathbb{Q}$ if and only if $L \subseteq \mathbb{Q}(\theta_n)$ for some nth root of unity θ_n.*

(See Theorem 5.10 in [Jan96].) One can generalize Kronecker-Weber to infinite extensions of $\mathbb{Q}$ to get the following corollary.

Corollary 3.7.2. *The set $\mathbb{Q}(\theta_{p^r}, p \in \mathscr{P}, r \in \mathbb{Z}_{>0})$, where $\mathscr{P}$ is the set of all prime numbers, is the largest abelian extension of $\mathbb{Q}$.*

Proof. Any embedding σ of $\mathbb{Q}(\theta_{p^r}, r \in \mathbb{Z}_{>0})$ is determined by the choice of a p-adic number $\alpha_p = a_0 + a_1 p + \cdots + a_k p^k + \cdots$ where each a_i is a representative of a residue class modulo p. In other words,

$$\theta_p \mapsto \theta_p^{a_0},\ \theta_{p^2} \mapsto \theta_{p^2}^{a_0+a_1 p},\ \ldots,\ \theta_{p^k} \mapsto \theta_{p^k}^{a_0+a_1 p+\cdots+a_{k-1}p^{k-1}},\ \ldots$$

We can extend the map α_p to all of $\mathbb{Q}(\theta_{q^r}, q \in \mathscr{P}, r \in \mathbb{Z}_{>0})$ by setting $\alpha_p(\theta_{q^r}) = \theta_{q^r}$ for $p \neq q$. Thus, as elements of $\mathrm{Gal}(\mathbb{Q}(\theta_{p^r}, p \in \mathscr{P}, r \in \mathbb{Z}_{>0})$ the maps α_p and α_q commute. Hence the set $\{\alpha_{p_i}, p_i \in \mathscr{P}\}$ generates an abelian group. So the field containing all roots of unity is a subfield of $\mathbb{Q}^{\mathrm{ab}}$.

Now suppose we have an abelian extension F of $\mathbb{Q}$. Then every finite subfield of F is contained in a cyclotomic extension, so every element of F is contained in a cyclotomic extension. Hence, $F \subset \mathbb{Q}(\theta_{p^r}, p \in \mathscr{P}, r \in \mathbb{Z}_{>0})$. Therefore, $\mathbb{Q}^{\mathrm{ab}}$ must be a subfield of $\mathbb{Q}(\theta_{p^r}, p \in \mathscr{P}, r \in \mathbb{Z}_{>0})$. Consequently, $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\theta_{p^r}, p \in \mathscr{P}, r \in \mathbb{Z}_{>0})$. □

We take a closer look at roots of unity, cyclotomic polynomials, and cyclotomic extensions.

Proposition 3.7.3. *Let θ_p be a primitive p-th root of unity. Then the minimal polynomial for θ_p, denoted by Φ_p, is given by*

$$\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

Furthermore, $[\mathbb{Q}(\theta_p) : \mathbb{Q}] = p - 1$.

(See Theorem 10.1 and the preceding paragraph in [Jan96].) We now give another result regarding the evaluation of cyclotomic polynomials at $x = 1$.

Proposition 3.7.4. *Given* $n \in \mathbb{Z}_{>0}$*, we have*

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1, \\ 1 & \text{if } p|n \text{ and } q|n \text{ for distinct primes } p \text{ and } q, \\ p & \text{if } n = p^r \text{ some prime } p \text{ and } r \in \mathbb{Z}_{>0}. \end{cases}$$

Proof. The case where $n = 1$ is trivial.

Let $n = p^r$ for some prime number p and positive integer r. We will show via induction on r that $\Phi_n(1) = p$. We know from Proposition 3.7.3 that when $r = 1$, $\Phi_n(1) = p$. Now assume the result holds for all positive integers less than r. Then we have

$$\Phi_{p^r}(x) = \frac{x^{p^r-1}}{\prod_{d|p^r, d<p^r} \Phi_d(x)} = \frac{x^{p^r-1} + x^{p^r-2} + \cdots + x + 1}{\prod_{k=1}^{r-1} \Phi_{p^k}(x)}.$$

Evaluating at $x = 1$, we obtain

$$\Phi_n(1) = \frac{p^r}{\prod_{k=1}^{r-1} p} = \frac{p^r}{p^{r-1}} = p.$$

Now assume the prime factorization of n contains at least two distinct primes, call them p and q. Let $S = \{k_1, k_2, \ldots\}$ be the subset of all positive integers with more that two distinct primes in their prime factorization, where k_1 is the smallest positive integer in S, k_2 the second smallest positive integer in S, and so on. We will show that $\Phi_{k_i}(1) = 1$ via induction on i. One can quickly see that $k_1 = 6$. Since

$$\Phi_{k_1}(x) = \frac{x^5 + x^4 + x^3 + x^2 + x + 1}{(x^2 + x + 1)(x + 1)},$$

we have $\Phi_{k_1}(1) = 1$, as desired. Now suppose the result holds for all $j < i$ and let r be a positive integer. We obtain the following:

$$\Phi_{k_i}(x) = \frac{x^{k_i} - 1}{\prod_{d|k_i, d<k_i} \Phi_d(x)} = \frac{x^{k_i-1} + x^{k_i-2} + \cdots + x + 1}{\prod_{d|k_i, d=p^r} \Phi_d(x)},$$

where the second equality follows from the induction hypothesis and geometric series formula. If k_1 has a prime factorization $k_i = p_1^{a_1} \cdots p_n^{a_n}$, then there are a_ℓ cyclotomic polynomials of the form $\Phi_{p_\ell^r}(x)$ in the denominator. Hence,

$$\Phi_{k_i}(1) = \frac{k_i}{\prod_{d|k_i, d=p^r} \Phi_d(1)} = \frac{k_i}{p_1^{a_1} \cdots p_n^{a_n}} = 1.$$

□

The next result gives a relationship between abelian extensions of $\mathbb{Q}$ and totally real fields.

Proposition 3.7.5. *Any abelian extension of $\mathbb{Q}$ that is not totally real is a totally complex degree 2 extension of a totally real field.*

Proof. Let K be an abelian extension of $\mathbb{Q}$ that is not totally real and $\bar{\mathbb{Q}}$ a fixed algebraic closure of $\mathbb{Q}$. The map taking any complex number to its complex conjugate, denoted by τ, is in $\mathrm{Gal}(K/\mathbb{Q})$. Hence we may define a subgroup $H = \{\epsilon, \tau\}$ of $\mathrm{Gal}(K/\mathbb{Q})$, where ϵ denotes the identity map. We claim that the fixed field of H, call it K^H, is a totally real field. We know from Proposition 3.6.1 that K^H is a Galois extension of $\mathbb{Q}$ because H is a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$. Furthermore, $[K : K^H] = 2$ by Galois Theory (see Theorem 1.15 in Chapter 14 of [Art91]). Now, to show that K^τ is totally real we need to show that for any embedding $\sigma : K^\tau \longrightarrow \bar{\mathbb{Q}}$, we have $\sigma(K^\tau) \subset \mathbb{R} \cap \bar{\mathbb{Q}}$. Since K^τ is the fixed field of complex conjugation, we know $K^\tau \subset \mathbb{R}$. Furthermore, the fact that K^τ is Galois implies that for all embeddings σ of K^τ into $\bar{\mathbb{Q}}$, we have $\sigma(K^\tau) = K^\tau$. These two facts prove that any embedding of K^τ into $\bar{\mathbb{Q}}$ is a subset of the real numbers. Hence K^τ is totally real, as

claimed. □

By Proposition 3.5.3 and the definition of a root of unity, we have the following corollary:

Corollary 3.7.6. *Let K and L be number fields with $[K : \mathbb{Q}] = n$, $[L : K] = 2$, K totally real, and L totally complex. With N defined as in Proposition 3.5.2 we have that* $\ker(N)$ *consists of roots of unity only.*

Proof. Since $\text{rank}(U_L) = \text{rank}(U_K)$, we have that $\text{rank}(\ker(N)) = 0$. Therefore for every element of $u \in \ker(N) = 0$ there must exists some number $n \in \mathbb{Z}$ such that $u^n = 1$. Thus, u is a root of unity. □

Lemma 3.7.7. *Let L, K be algebraic extensions of $\mathbb{Q}$, possibly of infinite degree. Assume K is totally real and L is a totally complex extension of K of degree 2. Let $x \in L$. There exists a totally real number field K_0, such that $[K_0(x) : K_0] \leq 2$ and $K_0(x)$ is either totally real or totally complex. Further, $N_{L/K}(x) = N_{L_0/K_0}(x)$.*

Proof. If $x \in K$, then we can take $K_0 = \mathbb{Q}(x)$. Suppose $x \notin K$. Then there exists $a, b \in K$ such that $x^2 + ax + b = 0$. Hence $\mathbb{Q}(x, a, b)$ is of degree 2 over $\mathbb{Q}(a, b)$, where $\mathbb{Q}(a, b)$ is totally real. Since $\mathbb{Q}(x, a, b)$ is not totally real, by Proposition 3.7.5, it must be totally complex. Since x satisfies the same minimal polynomial over K as over K_0, then norms with respect to both fields must be the same. □

Corollary 3.7.8. *Let L, K be algebraic extensions of $\mathbb{Q}$, possibly of infinite degree. Assume K is totally real and L is a totally complex extension of K of degree 2. Let $N : U_L \longrightarrow U_K$ be the norm map. Then* $\ker(N)$ *is of rank 0.*

Proof. Suppose $x \in \ker(N)$. If $x \in K$ and $x \in \ker(N)$, then $N_{L/K}(x) = x^2 = 1$. So $x = \pm 1$. Suppose, $\xi \in \ker(N), \xi \notin K$. Then by Lemma 3.7.7, there exist number fields L_0, K_0 such that K_0 is totally real, L_0 is a complex extension of degree 2 of K_0, $\xi \in L_0$ and $N_{L_0/K_0}(x) = 1$. Hence, by Lemma 3.7.6, ξ is a root of unity. Thus $\ker(N)$ contains elements of finite order only. Therefore, $\text{rank}(\ker(N)) = 0$. □

With L and K as above the corollary we just proved can be used to tell us more about the units in U_K.

Proposition 3.7.9. *Let L and K be as above. Let p be a prime number and $\mu \in U_L$ be such that $\mu \equiv_{O_L} 1 \bmod p$. Then $\mu^2 \in U_K$.*

Proof. Let $\nu \in U_K$ be such that $N_{L/K}(\mu) = \nu$ and consider

$$N\left(\frac{\mu^2}{\nu}\right) = N_{L/K}\left(\frac{\mu^2}{\nu}\right) = \frac{N_{L/K}(\mu)^2}{N_{L/K}(\nu)} = \frac{\nu^2}{\nu^2} = 1.$$

The above equation implies $\frac{\mu^2}{\nu} \in \ker(N)$. Hence Corollary 3.7.8 tells us $\frac{\mu^2}{\nu} = \xi_r$, where ξ_r is an rth root of unity. Since $\mu \equiv_{O_L} 1 \bmod p$, the conjugate $\bar{\mu}$ of μ over K satisfies $\bar{\mu} \equiv_{O_L} 1 \bmod p$. Therefore, $\nu = \mu\bar{\mu} \equiv_{O_L} 1 \bmod p$ and

$$\xi_r = \frac{\mu^2}{\nu} \equiv_{O_L} 1 \bmod p.$$

Since $\xi_r, 1, p \in \mathbb{Q}(\xi_r)$, we have that

$$\xi_r \equiv_{O_{\mathbb{Q}(\xi_r)}} 1 \bmod p.$$

This implies $N_{\mathbb{Q}(\xi_r)/\mathbb{Q}}(p) | N_{\mathbb{Q}(\xi_r)/\mathbb{Q}}(1-\xi_r)$. Since $N_{\mathbb{Q}(\xi_r)/\mathbb{Q}}(1-\xi_r) = \Phi_r(1)$ by Lemma 3.6.3 and $N_{\mathbb{Q}(\xi_r)/\mathbb{Q}}(p) = p^{[\mathbb{Q}(\xi_r):\mathbb{Q}]}$, we must then have $p^{[\mathbb{Q}(\xi_r):\mathbb{Q}]} | \Phi_r(1)$. Since Φ_r is either equal to 0, 1, or some prime number q by Proposition 3.7.4, if $[\mathbb{Q}(\xi_r) : \mathbb{Q}] > 1$, we must have $\Phi_r(1) = 0$. This can only occur if $\xi_r = 1$. Further, if $[\mathbb{Q}(\xi_r) : \mathbb{Q}] = 1$, then $\xi_r = \pm 1$. Thus, $\mu^2 = \pm\nu \in U_K$. □

Next we apply Definition 3.3.1 to define subsets of the ring of integers.

Proposition 3.7.10. *Let K be a totally real extension of $\mathbb{Q}$, L a totally complex extension of degree 2 over K, and p any prime number. Define R_L using Definition 3.3.1 with $R = O_L$,*

$U_R = U_L$, *and* $\hat{R} = R_L$. *Lastly, take*

$$\hat{U}_L = \{\varepsilon \in U_L \,|\, (\exists \varepsilon_0 \in U_L)(\varepsilon_0 \equiv_{O_L} 1 \bmod p \text{ and } \varepsilon = \varepsilon_0^2)\}$$

and

$$\hat{R}_L = \left\{ x \in O_L \middle| (\forall \varepsilon \in \hat{U}_L \setminus \{1\})(\exists \delta \in \hat{U}_L) \left(x \equiv_{O_L} \frac{\delta - 1}{\varepsilon - 1} \bmod (\varepsilon - 1) \right) \right\}.$$

Then

1. $\hat{U}_L$ *is an abelian subgroup of* U_L,
2. $\hat{U}_L \subset U_K$,
3. $2R_L \subset \hat{R}_L$,
4. $\hat{R}_L$ *is a ring,*
5. *and* $\hat{R}_L \subset O_K$ *whenever* U_L *has an element of infinite order.*

Proof.

1. To show that $\hat{U}_L$ is a subgroup of U_L it is sufficient to show that it is closed under multiplication and inverses. Suppose $\varepsilon, \delta \in \hat{U}_L$. Then there exists some $\varepsilon_0, \delta_0 \in U_L$ such that $\varepsilon_0 \equiv_{O_L} \delta_0 \equiv_{O_L} 1 \bmod p$, $\varepsilon = \varepsilon_0^2$, and $\delta = \delta_0^2$. Thus, $\varepsilon_0 \delta_0 \equiv_{O_L} 1 \bmod p$ and $\varepsilon\delta = \varepsilon_0^2 \delta_0^2 = (\varepsilon_0 \delta_0)^2$ with $\varepsilon_0 \delta_0 \in U_L$. Note that the last equality holds because U_L is abelian. Thus, $\varepsilon\delta \in \hat{U}_L$.

   Furthermore, $\varepsilon_0^{-1} \equiv_{O_L} \varepsilon_0^{-1}\varepsilon \equiv_{O_L} 1 \bmod p$ and $\varepsilon^{-1} = (\varepsilon_0^2)^{-1} = (\varepsilon_0^{-1})^2$, so $\varepsilon^{-1} \in \hat{U}_L$. This concludes the proof that $\hat{U}_L$ is an abelian subgroup of U_L.

2. This is an immediate corollary of Proposition 3.7.9.

3. Let $x \in R_L$. Then for every $\varepsilon \in \hat{U}_L \setminus \{1\}$ there exists a $\delta_0 \in U_L$ such that

$$x \equiv_{O_L} \frac{\delta_0 - 1}{\varepsilon - 1} \bmod (\varepsilon - 1).$$

Observe that $\delta_0^2 - 1 \equiv_{O_L} 2(\delta_0 - 1) \bmod (\delta_0 - 1)$. Thus,

$$\delta_0^2 - 1 \equiv_{O_L} 2(\delta_0 - 1) \bmod (\varepsilon - 1)$$

by Proposition 3.3.2, so

$$2x \equiv_{O_L} 2\frac{\delta_0 - 1}{\varepsilon - 1} \equiv_{O_L} \frac{\delta_0^2 - 1}{\varepsilon - 1} \bmod (\varepsilon - 1).$$

Note that Proposition 3.3.2 and the fact that $\varepsilon \equiv_{O_L} 1 \bmod p$ tells us that $\delta_0 \equiv_{O_L} 1 \bmod p$. It follows that $2R_L \subset \hat{R}_L$, as desired.

4. The proof that $\hat{R}_L$ is a ring is nearly identical to the proof of Proposition 3.3.4.

5. We begin by showing that if U_L has an element of infinite order, then $\hat{U}_L$ does as well. Suppose $\delta_0 \in U_L$ has infinite order. Then by Corollary 3.4.7 and Remark 3.4.8 there exists some positive integer m such that $\delta_0^m \equiv_{O_L} 1 \bmod p$. Taking $\varepsilon_0 = \delta_0^m$ and $\varepsilon = \varepsilon_0^2$, we have $\varepsilon \in \hat{U}_L$ is an element of infinite order.

   Now let τ denote the map that takes an number in L to its complex conjugate. Then we know $\tau(x) \in O_L$ for any $x \in O_L$ by Proposition 3.4.9 and Remark 3.4.8. Given $x \in \hat{R}_L$, for any $\varepsilon \in \hat{U}_L \setminus \{1\}$ there exists a $\delta \in \hat{U}_L$ such that

$$x \equiv_{O_L} \frac{\delta - 1}{\varepsilon - 1} \bmod (\varepsilon - 1).$$

   Applying τ to the congruence, we obtain

$$\bar{x} \equiv_{O_L} \frac{\delta - 1}{\varepsilon - 1} \bmod (\varepsilon - 1),$$

   where $\bar{x}$ denotes the complex conjugate of x. Hence,

$$x - \bar{x} \equiv_{O_L} 0 \bmod (\varepsilon - 1).$$

By the assumption that U_L has an element of infinite order and the preceding paragraph, some $\varepsilon \in \hat{U}_L$ has infinite order and $\varepsilon^r \in \hat{U}_L \setminus \{1\}$ for all $r \in \mathbb{Z}_{>0}$. Further, the above equivalence holds when we replace $\varepsilon - 1$ with $\varepsilon^r - 1$ for any $r \in \mathbb{Z}_{>0}$, that is,

$$x - \bar{x} \equiv_{O_L} 0 \bmod (\varepsilon^r - 1)$$

for each $r \in \mathbb{Z}_{>0}$. This implies $x - \bar{x} \in \bigcap_{i=1}^{r}(\varepsilon^r - 1)$, so $x - \bar{x}$ is divisible by every nonzero element of O_L by Corollary 3.4.7 and Remark 3.4.8. It follows that $x - \bar{x} = 0$, so $x \in O_K$. This completes the proof that $\hat{R}_L \subset O_K$.

□

3.8 Results of Julia Robinson and the theory of $O_{\mathbb{Q}^{\mathbf{ab}}}$

Julia Robinson was the first person to investigate the undecidability of the ring of integers in infinite extensions of $\mathbb{Q}$ (see [Rob59] and [Rob62]). She developed a method of showing that $\mathbb{Z}$ is definable in the rings of integers of totally real extensions of $\mathbb{Q}$. She also speculated that the theory of the ring of integers of any totally real extension is undecidable. In the previous section, we defined a ring of totally real integers over $O_{\mathbb{Q}^{\mathrm{ab}}}$. Thus, to show that the first-order theory of $O_{\mathbb{Q}^{\mathrm{ab}}}$ is undecidable it is sufficient to show that the theory of the ring of integers of every totally real *abelian* extension is undecidable. Further, one can hope to apply Julia Robinson's method to the ring constructed in the preceding section.

Unfortunately, at the moment, it is not clear what ring has been constructed. In hopes of understanding the result of that construction, one could study the construction in a more general context. We carry out such a construction over subrings of $\mathbb{Q}$ in the final section of this paper.

Chapter 4

Defining a Subring Using the Group of Units

In Chapter 3, we showed that one can construct subrings from units using any commutative integral domain of characteristic 0. In this chapter, we investigate the results of this construction when the ring in question is not a ring of integers but a general subring of $\mathbb{Q}$.

4.1 Construction using units over subrings of $\mathbb{Q}$

Consider the set

$$Z^{(p)} = \left\{ x \in \mathbb{Q} \middle| x = \frac{m}{p^a}, m \in \mathbb{Z}, a \in \mathbb{Z}_{\geq 0} \right\}.$$

We begin by proving $Z^{(p)}$ is a ring.

Proposition 4.1.1. *$Z^{(p)}$, as defined above, is a ring.*

Proof. Since $Z^{(p)} \subset \mathbb{Q}$ by definition, we shorten the proof that $Z^{(p)}$ is a ring by showing it is a subring of the rational numbers. Firstly, setting $m = 1$ and $a = 0$ in the definition of $Z^{(p)}$ gives us $\frac{1}{p^0} = 1 \in Z^{(p)}$. Moreover, if $\frac{m}{p^a}, \frac{n}{p^b} \in Z^{(p)}$, then

$$\frac{m}{p^a} - \frac{n}{p^b} = \frac{p^b m - p^a n}{p^{a+b}} \in Z^{(p)}$$

and

$$\frac{m}{p^a}\frac{n}{p^b} = \frac{mn}{p^{a+b}} \in Z^{(p)}.$$

Hence $Z^{(p)}$ contains 1 and is closed under subtraction and multiplication, so it is a subring of $\mathbb{Q}$. □

Now for a note on notation. When working with $Z^{(p)}$ we streamline our notation by using $|_p$ in place of $|_{Z^{(p)}}$ and $\equiv_p$ in place of $\equiv_{Z^{(p)}}$. Defining $\hat{Z}^{(p)}$ as in Definition 3.3.1, we wish to determine which elements of $Z^{(p)}$ are contained in $\hat{Z}^{(p)}$. However, before we do so, we introduce a lemma to simplify future calculations.

Lemma 4.1.2. *Let $p, q, r, \alpha \in \mathbb{Z}$. Then*

$$p^{\alpha q+r} \equiv (\pm 1)^q p^r \bmod (\pm p^\alpha - 1).$$

Proof. We prove this lemma with a simple calculation:

$$p^{\alpha q+r} = p^{\alpha q} p^r = (p^\alpha)^q p^r \equiv (\pm 1)^q p^r \bmod (\pm p^\alpha - 1).$$

□

The equivalence above is taken over $\mathbb{Z}$ and not $Z^{(p)}$; however, the notion of equivalence may be easily extended to $Z^{(p)}$ given that $\mathbb{Z} \subset Z^{(p)}$ by Proposition 3.3.5.

Proposition 4.1.3. *For any prime number p,*

$$\hat{Z}^{(p)} = Z^{(p)}.$$

Proof. Proposition 3.3.4 tells us that $\hat{Z}^{(p)}$ is a ring and Proposition 3.3.5 tells us that $\mathbb{Z} \subset \hat{Z}^{(p)}$. Now, given any $\alpha \in \mathbb{Z} \setminus \{0\}$, we may find some $q \in \mathbb{Z}$ such that $\alpha q - 1 > 0$.

Lemma 4.1.2 then tells us

$$\frac{1}{p} \equiv_p (\pm 1)^q p^{\alpha q - 1} \mod (\pm p^\alpha - 1).$$

Since

$$(\pm 1)^q p^{\alpha q - 1} \in \mathbb{Z} \subset \hat{Z}^{(p)},$$

for every $a \in \mathbb{Z} \setminus \{0\}$ there exists some $b \in \mathbb{Z}$ such that

$$(\pm 1)^q p^{\alpha q - 1} \equiv_p \frac{\pm p^b - 1}{\pm p^a - 1} \mod (\pm p^a - 1).$$

Thus, given $\alpha \in \mathbb{Z} \setminus \{0\}$, we may find some $\beta \in \mathbb{Z}$ such that

$$\frac{1}{p} \equiv_p (\pm 1)^q p^{\alpha q - 1} \equiv_p \frac{\pm p^\beta - 1}{\pm p^\alpha - 1} \mod (\pm p^\alpha - 1).$$

It follows that $\frac{1}{p} \in \hat{Z}^{(p)}$. The fact that $\hat{Z}^{(p)}$ is closed under multiplication then implies $\hat{Z}^{(p)} = Z^{(p)}$, as desired. □

In the above example, we saw that $\hat{Z}^{(p)} = Z^{(p)}$ for any prime number p. We look to expand upon this to see what happens when we allow powers of multiple prime numbers in the denominator of elements in our ring. In order to do this, we let P be a set of prime numbers and consider the set

$$Z^{(P)} = \left\{ x \in \mathbb{Q} \,\middle|\, x = \frac{m}{\prod_{i=1}^n q_i^{\alpha_i}} : m \in \mathbb{Z},\, n, \alpha_i \in \mathbb{Z}_{\geq 0},\, q_i \in P \right\}.$$

It is not hard to see that $Z^{(P)}$ is a ring much like $Z^{(p)}$. The proof is similar to the proof of Proposition 4.1.1, with the exception that p is replaced by a product of primes.

For $Z^{(P)}$ we use notation analogous to that of $Z^{(p)}$. That is, we use $|_P$ in place of $|_{Z^{(P)}}$ and $\equiv_P$ in place of $\equiv_{Z^{(P)}}$.

Proposition 4.1.4. *Let P be any nonempty set of prime numbers. Then $\hat{Z}^{(P)} = Z^{(P)}$.*

Proof. Suppose P is nonempty and fix $q \in P$. We wish to show that $\frac{1}{q} \in \hat{Z}^{(P)}$. First, let U_P denote the set of units in $Z^{(P)}$ and take any $u \in U_P \cap \mathbb{Z}$ with $u \neq 1$. We may then write $u - 1 = q^\beta k$, where $\beta \in \mathbb{Z}_{\geq 0}$ and $k \in \mathbb{Z} \setminus \{0\}$ with q and k coprime. Let $m = |k|$ so that $m \in \mathbb{Z}_{>0}$ with q and m coprime. This implies $m|_P(u-1)$ and $(u-1)|_P m$. Since q and m are coprime, we know

$$q^{\phi(m)} \equiv_P 1 \mod m$$

by Euler's Theorem, where ϕ denotes the Euler phi-function. Multiplying both sides of the congruence by $\frac{1}{q}$, we obtain

$$\frac{1}{q} \equiv_P q^{\phi(m)-1} \mod m.$$

We then have

$$\frac{1}{q} \equiv_P q^{\phi(m)-1} \mod (u-1)$$

and

$$\frac{1}{q} \equiv_P q^{\phi(m)-1} \mod \left(\frac{1}{u} - 1\right)$$

by the discussion above and the fact that $u - 1 = -u(u^{-1} - 1)$ so $(u^{-1} - 1)|_P(u-1)$. Since $\phi(m) \geq 1$, we know $q^{\phi(m)-1}$ is an integer. Hence it is in $\hat{Z}^{(P)}$ by Proposition 3.3.5. The proof of the aforementioned proposition then implies

$$\frac{1}{q} \equiv_P \frac{u^{q^{\phi(m)-1}} - 1}{u - 1} \mod (u-1)$$

and

$$\frac{1}{q} \equiv_P \frac{\left(\frac{1}{u}\right)^{q^{\phi(m)-1}} - 1}{\frac{1}{u} - 1} \mod \left(\frac{1}{u} - 1\right).$$

Since u was an arbitrary unit in $U_P \cap \mathbb{Z}$, this argument holds for any unit in that set. It follows that $\frac{1}{q} \in \hat{Z}^{(P)}$. This result holds for any prime in P by the fact that q was arbitrarily chosen. Since $\hat{Z}^{(P)}$ is closed under multiplication we must have $\hat{Z}^{(P)} = Z^{(P)}$. □

References

[Art91] M. Artin. *Algebra*. Prentice-Hall, Inc., 1991.

[Axl15] S. Axler. *Linear Algebra Done Right*. 3rd. Undergraduate Texts in Mathematics. Springer International Publishing, 2015.

[Jan96] G. Janusz. *Algebraic Number Fields*. 2nd. Graduate Studies in Mathematics. American Mathematical Society, 1996.

[Lee00] J. M. Lee. *Introduction to Topological Manifolds*. 1st. Graduate Texts in Mathematics. Springer-Verlag, 2000.

[MRS23] B. Mazur, K. Rubin, and A. Shlapentokh. "Defining $\mathbb{Z}$ using unit groups". Version 1. In: (Mar. 4, 2023). arXiv: `http://arxiv.org/abs/2303.02521v1 [math.NT, math.LO, 11U05]`. URL: `http://arxiv.org/abs/2303.02521v1`.

[RF19] M. Ram Murty and B. Fodden. *Hilbert's Tenth Problem: An Introduction to Logic, Number Theory, and Computability*. Student Mathematical Library. American Mathematical Society, 2019.

[Rob59] J. Robinson. "Definability and Decision Problems in Arithmetic". In: *Proceedings of the American Mathematical Society* 10 (1959), pp. 950–957.

[Rob62] J. Robinson. "On the Decision Problem for Algebraic Rings". In: *Studies in Mathematical Analysis and Related Topics* (1962), pp. 297–304.

[Shl06] A. Shlapentokh. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. 1st. New Math Monographs. Cambridge University Press, 2006.

[Str94] J. Strayer. *Elementary Number Theory*. Waveland Press, Inc., 1994.