An Introduction to

Algebraic Number Theory

Alistair Pattison

Carleton College Math Department

November 2023

Abstract

This paper is a whirlwind introduction to the field of algebraic number theory with the goal of stating and unpacking two important theorems: Dirichlet's unit Theorem and the fact that the class number is finite. Along the way, we'll cover things like the number fields, algebraic integers, cyclotomic fields, Dedekind domains, and generalizations of primes.

Contents

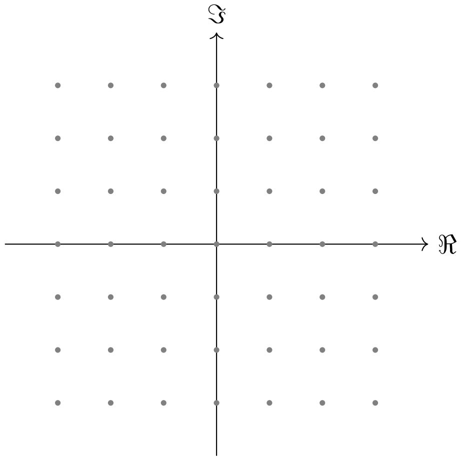

Figure 1: The lattice of Gaussian integers $\mathbb{Z}[i]$ in the complex plane.

a	b	
2	1	$3^2 + 4^2 = 5^2$
3	2	$5^2 + 12^2 = 13^2$
4	3	$7^2 + 24^2 = 25^2$
4	2	$12^2 + 16^2 = 20^2$
4	1	$15^2 + 8^2 = 17^2$

Table 1: The primative Pythagorean triples.

We started with a problem strictly about the integers, and

This paper will build towards proving that the ideal class group is finite, starting from Carleton's introductory algebra class. However, it will at times move very, very quickly and leave gaps in the exposition for the sake of brevity. To quote Richard Feynman:

> I am going to give what I will call an elementary demonstration. But elementary does not mean easy to understand. Elementary means that very little is required to know ahead of time in order to understand it, except to have an infinite amount of intelligence.

If this paper piques your interest, I encourage you to go read Marcus [1].

1 Preliminaries

Algebraic number theory (unsurprisingly) requires a lot of algebra.

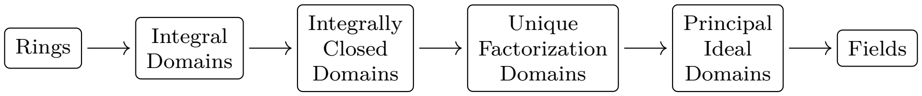

Figure 2: The hierarchy of rings.

1.1 Groups

We assume that the reader is familiar with the definition of a group and provide it here only for completeness.

Definition 1.1 (Group)**.** *A **group** is a set G along with an operation $\cdot : G \times G \to G$ such that for all $a, b \in G$,*

(i) $a \cdot b \in G$ *(closure),*

(ii) there exists an identity element e *such that* $a \cdot e = a$ *(identity),*

(iii) there exists some element a^{-1} *such that* $a \cdot a^{-1} = e$.

*If the $\cdot$ operation is commutative, we call G an **Abelian group**.*

1.2 Rings

Much of algebraic number theory is concerned with generalizations of integers int he complex plane, and how these generalizations are and are not similar to the integers. This is done through the lens of rings.

To do algebraic number theory, one unsupringly needs a bit of algebra.

Much of this (but not all!) is covered in Carleton's standard Algebra I course.

Definition 1.2 (Commutative ring)**.**

Definition 1.3 (Ideal)**.** *An (additive) subgroup, I, such that $ra \in I$ for all $r \in R$, $a \in I$.*

Definition 1.4 (Prime Ideal)**.** *An ideal, P, such that $ab \in P$ implies $a \in P$ or $b \in P$.*

Definition 1.5. *A commutative ring is an* integral domain *if $ab = 0$ implies $a = 0$ or $b = 0$. (No zero divisors.)*

Definition 1.6 (Fraction field)**.**

Definition 1.7 (Integral elements)**.**

The classic example is that $\operatorname{Frac}\mathbb{Z} = \mathbb{Q}$.

Definition 1.8 (Integrally Closed Domain)**.** *A ring R is integrally closed if for all $\alpha/\beta \in \operatorname{Frac} R$ that are integral over R, then $\beta \mid \alpha$, i.e., $\alpha/\beta \in R$.*

We say that the integral closure of $\operatorname{Frac} R$ *is R.*

This will come up later in the paper.

Any monic polynomials with integer coefficients must have integer roots.

Definition 1.9 (Unique factorization domain)**.** *A commutative ring R is a* unique factorization domain *if every element factors uniquely into irreducible elements.*

The integers are famously a UFD by the fundemental theorem of arithmatic.

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned} \tag{1}$$

The ring $\mathbb{Z}[i\sqrt{5}]$ will make many appearances throughout the rest of this paper.

Definition 1.10 (Principal Ideal Domain)**.** *A commutative ring R is a* principal ideal domain *if every ideal is generated by a single element.*

The rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x, y]$ are not because of the ideals $(2, x)$ and (x, y) respectively.

1.3 Fields

Definition 1.11 (Field)**.**

$$\begin{aligned} f(x) &= x^2 + 5 \\ &= (x + i\sqrt{5})(x - i\sqrt{5}) \end{aligned} \tag{2}$$

In some sense, f would be equally happy living in a much smaller field without these

Definition 1.12 (Finite field extensions)**.** *The* field extension $K(\alpha_1, \ldots, \alpha_n)$ *is the smallest field containing both K and each of $\alpha_1, \ldots, \alpha_n$.*

This is a number field.

2 Number Fields

Enough beating around the bush, here's the definition

Definition 2.1 (Number Field)**.** *A* number field $K \subset \mathbb{C}$ *is a finite extension of* $\mathbb{Q}$.

Definition 2.2 (Algebraic number)**.** *A complex number $\alpha \in \mathbb{C}$ is an* algebraic number *if it is the root of some monic polynomial $f \in \mathbb{Q}[x]$.*

Theorem 2.3. *Any number field can be written in the form*

$$K = \mathbb{Q}[\alpha] = \operatorname{span}_{\mathbb{Q}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

where n is the degree of the minimal polynomial of α.

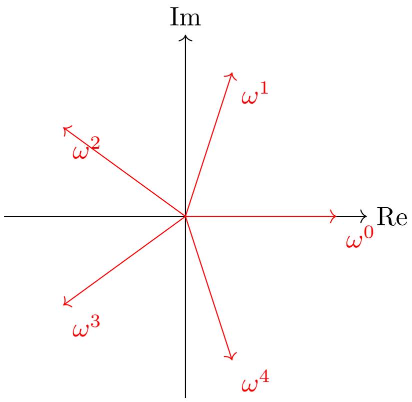

Figure 3: The fifth roots of unity.

Proof. □

Although we could use any algebraic number for , $for the purposes of this paper we'll focus on the two following$

Definition 2.4 (Cyclotomic field)**.**

Definition 2.5 (Quadratic field)**.**

It seems like positive m should be the simpler case, but itt turns out we know very little about these when $m > 0$ (more on this later).

2.1 Complex Embeddings

Definition 2.6 (Trace and norm)**.**

Definition 2.7 (Relative trace and norm)**.**

3 Number Rings

We have a generalization of the rationals to the complex plane, now we need an analogue to the integers.

Definition 3.1 (Algebraic Integer)**.** *An* algebraic integer *is a complex number α that is the root of some monic polynomial $f \in \mathbb{Z}[x]$.*

We use $\mathbb{A}$ to denote the set of all algebraic integers.

We would hope that the familiar integers $\mathbb{Z}$ remain integers under this more general definition, and that is indeed the case.

$f(x) = x - k$

- Any integer k is an algebraic integer because of $f(x) = x - k$
- $i\sqrt{5} \in \mathbb{A}$ because of $f(x) = x^2 + 5$

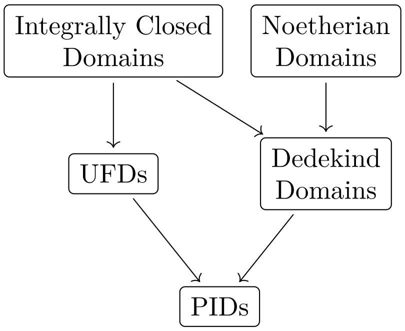

Figure 4: The two paths for an integrally closed domain with upward ambitions.

- $2 + \sqrt[3]{17} \in \mathbb{A}$ because of $f(x) = x^3 - 6x^2 + 12x - 25$
- $\mathbb{A}$ is a subring of $\mathbb{C}$ show that $\alpha - \beta, \alpha\beta \in \mathbb{A}$

Definition 3.2 (Number Ring)**.** *The* number ring *of a number field $K = \mathbb{Q}(\alpha)$ is the set of algebraic integers contained within K, denoted*

$$\mathcal{O}_K = \mathbb{A} \cap K.$$

We use $\mathcal{O}$ because it looks like a ring.
Sometimes you can just move α from next to the $\mathbb{Q}$ to next to the $\mathbb{Z}$.

3.1 Dedekind Domains

Number rings have some nice properties, so mathematicians have done what they love best and given those properties a definition.

Definition 3.3 (Noetherian domain)**.**

Definition 3.4 (Dedekind domain)**.** *A* Dedekind domain *is a ring R such that*

(i) R is integrally closed,

(ii) R is Noetherian, and

(iii) every nonzero prime ideal is maximal.

Theorem 3.5 (Number Rings are Dedekind Domains)**.**

Proof. □

This definition is pretty unhelpful. The reason we care about Dedekind domains at all is the following.

Theorem 3.6. *Ideals in Dedekind domains uniquely factor into prime ideals.*

Although we won't prove it, the converse of Theorem 3.6 is also true, and is sometimes taken as an alternative definition of Dedekind domains.

We use the one that we've chosen to use because its conditions are easier to show.

Theorem 3.7. *If a ring is a Dedekind domain and a unique factorization domain, then it's a principal ideal domain.*

Once you have prime factorization of both ring elements and ideals, you are guaranteed that all ideals are principal. Before we prove this theorem, we're going to work through an example.

The unique factorization of the ideal (6) completely captures the *failure* of unique factorization of the ring element 6. But this only happens because the prime ideals that 6 factors into are generated by two elements.

4 The Ideal Class Group

Definition 4.1 (Ideal Class Group)**.** *Let $K = \mathbb{Q}[\alpha]$ be a number field. The class group of K is the set of ideals of $\mathcal{O}_K$, modulo the equivilence relation*

$$I \sim J \text{ iff } \alpha I = \beta J \text{ for some nonzero } \alpha, \beta \in R.$$

This is the smallest relation that "kills the principal ideals", i.e., collapses them into a single equivilence class. You can also define the ideal class group as the quotent of fractional ideals by principal ideals.

Theorem 4.2. *The ideal class group is a group.*

Proof.

Lemma* 4.2.1** *(Ideal inverses exist).**

Have to show that there is an identity, inverses exists, and that ideal multiplication is well-defined. □

4.1 The Class Number

With so much machinery now built up, stating the goal of our paper is quite simple:

Definition 4.3 (Class Number)**.** *The class number of a number field $K = \mathbb{Q}[\alpha]$ is the size of its ideal class group.*

Theorem 4.4. *Class numbers are always finite.*

Never infinitely far from your dreams.

5 Conclusion

References

[1] D.A. Marcus. *Number Fields*. Universitext. Springer International Publishing, 2018. ISBN: 9783319902333. URL: https://link.springer.com/book/10.1007/978-3-319-90233-3.