Algebraic number theory

Alexandru Ghitza[*]
School of Mathematics and Statistics
University of Melbourne

Version of Mon 13th Jun, 2022 at 09:26

[*] (aghitza@alum.mit.edu)

Contents

1. Introduction 5

2. Number fields and rings of integers 7

2.1. Algebraicity and integrality 7

2.2. Rings of integers are Dedekind domains 10

2.3. Unique factorisation into prime ideals 13

2.4. Discriminant 16

2.5. Ideal norm and finiteness of the ideal class group 18

3. Decomposition of primes in ring extensions 23

3.1. From polynomial factorisation to prime ideal decomposition 25

3.2. Cyclotomic fields 29

3.3. Quadratic Reciprocity, take one 33

3.4. Extensions of number fields, and the Galois advantage 36

3.5. Cyclotomic fields redux, and more Quadratic Reciprocity 44

4. Some finiteness results 47

4.1. The Convex Body Theorem 48

4.2. Dirichlet's Unit Theorem 51

4.3. Continued fractions and units in real quadratic fields 55

5. Local rings and fields 59

5.1. Local rings 59

5.2. Discrete valuation rings 60

5.3. Completions 63

5.4. p-adic numbers 65

5.5. Some weirdness of the p-adic topology 66

5.6. Hensel's Lemma 67

5.7. Non-archimedean completions via algebra 69

5.8. Arithmetic of p-adic fields 70

5.8.1. Prime ideal decomposition in p-adic fields 71

A. Revision: Algebra 73

A.1. Rings 73

A.2. Fields 73

1. Introduction

Number theory is a very old subject, dating back thousands of years. This gave it plenty of time to develop in many different directions; its branches are classified according to their aims and methods. The particular branch we are exploring is characterised by the use of abstract algebra, or more generally by the emphasis on the understanding of the algebraic structures that occur in problems with an arithmetic focus.

In this section we will attempt to make these vague opening remarks more concrete with the use of a couple of particular questions. We will take an impressionistic approach and focus on the storyline rather than the technical details (whose time will come soon enough).

Here's the start of a well-trodden path: find all integer solutions (x, y, z) to the equation $x^2 + y^2 = z^2$ such that the three integers x, y, z have no nontrivial common divisors[1]. There is a very beautiful and simple geometric construction that gives a complete answer to this question, but here I want to set aside geometric intuition and use algebra instead[2].

Let's start by ruling out the possibility that z may be even. That can only happen in two ways:

- x and y are both even—but then z^2 is even, hence z is even and (x, y, z) is not primitive;
- x and y are both odd—in this case we observe that $x^2 \equiv y^2 \equiv 1 \pmod 4$, hence $z^2 \equiv 2 \pmod 4$, which is impossible.

So z is odd, which implies that $\gcd(z, 2x) = 1$.

We can rewrite the defining equation as

$$(x + iy)(x - iy) = z^2. \tag{1.1}$$

Where is this happening though? Well, we could be hasty and place ourselves over $\mathbb{C}$, but we're about to say words like "prime element" and "divides" and so on, and these don't make much sense over $\mathbb{C}$. Luckily, we don't need to go all the way to $\mathbb{C}$, when the following is enough:

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

Suppose we could convince ourselves that Equation (1.1) forces $x + iy$ to be of the form $u\alpha^2$, where u is a unit in the ring $\mathbb{Z}[i]$ and α is some element of $\mathbb{Z}[i]$. One fact we will see later is that the set of units of $\mathbb{Z}[i]$ is

$$\left(\mathbb{Z}[i]\right)^\times = \{1, -1, i, -i\}.$$

Writing $\alpha = m + in$ with $m, n \in \mathbb{Z}$, we see easily that x and y are of the form $\pm(m^2 - n^2)$ and $\pm 2mn$, while z is of the form $\pm(m^2 + n^2)$.

It remains then to prove the claim that $x + iy = u\alpha^2$. It is the case that the ring $\mathbb{Z}[i]$ is a unique factorisation domain, so that every nonzero, non-unit element has an essentially unique[3] factorisation into a finite product of irreducible elements.

[1] Of course, such solutions (x, y, z) are called primitive Pythagorean triples.

[2] This argument is borrowed from the introduction to [4].

[3] Spelling out the precise meaning of *essentially unique* is a bit more cumbersome than in the case of $\mathbb{Z}$, but not very hard, see [5, Definition 6.9].

It suffices to prove that any irreducible element π of $\mathbb{Z}[i]$ that divides $x + iy$ must divide it an even number of times. Since any π dividing $x + iy$ also divides z, and clearly must divide z^2 an even number of times, it suffices to prove that π does not divide $x - iy$.

So let's assume that an irreducible element π of $\mathbb{Z}[i]$ divides both $x + iy$ and $x - iy$. As we have already seen, π divides z. It also divides $2x = (x+iy)+(x-iy)$, so it divides $\gcd(z, 2x) = 1$, contradiction.

Let's go back and look at some of the features we exploited in this argument. We considered the smallest field extension $\mathbb{Q}(i)$ over which $x^2 + y^2$ splits into linear factors. In order to use divisibility arguments, we imposed an integrality condition leading us to the ring $\mathbb{Z}[i]$. We used the fact that this ring is a UFD, and that we know the complete list of units.

We will spend most of the semester working out how to properly generalise these objects and studying their properties. This will involve number fields ($\mathbb{Q}(i)$ above), their rings of integers ($\mathbb{Z}[i]$), the groups of units of these rings of integers, the passage from divisibility arguments involving elements to splitting arguments involving ideals, and more.

Instead of taking the purely utilitarian view of abstract algebra as a means to the end of studying arithmetic, we will use this as an excuse to learn the basics of commutative algebra, which is a very powerful tool that's best understood in conjunction with one of its main areas of application (algebraic number theory, algebraic geometry, representation theory).

As a final remark, it would be weird to pretend we're not in the 21st century. While this will not be a central theme of the subject, we will on occasion discuss the use of computational methods.

Exercise 1.1. As mentioned in the discussion above, there is a geometric argument leading to the parametrisation of the integral points on the curve $x^2 + y^2 = z^2$. See if you can piece this argument together.

Here are some hints to get you started, if you need them:

(a) The integral points on $x^2 + y^2 = z^2$ are in bijective correspondence with the rational points on $X^2 + Y^2 = 1$, so it's enough to parametrise the latter.

(b) Find one rational point P on $X^2 + Y^2 = 1$. (This should not require thought; there are 4 obvious candidates.)

(c) Consider the set of all lines passing through P. Can you characterise those lines that intersect $X^2 + Y^2 = 1$ in a second rational point?

(d) Put it all together to get formulas for the set of rational points on $X^2 + Y^2 = 1$.

Exercise 1.2 (Project Euler Problem 9)**.** There is a unique Pythagorean triple (x, y, z) with positive entries, $x \leq y$, and the property that $x + y + z = 1000$. Find it.

Acknowledgements

The lectures notes [2] by Matt Baker and the textbook [4] by Daniel Marcus have been major sources of inspiration.

Thanks go to Brian Chan, Kevin Fergusson, Yuhan Gai, Miles Koumouris, Jonah Nelson, Lachlan Potter, Liang Tee, and Abraham Zhang for corrections and suggestions on these notes.

2. Number fields and rings of integers

2.1. Algebraicity and integrality

A *number field* K is a finite extension of the rational numbers $\mathbb{Q}$. Elements of number fields are called *algebraic numbers*.

By the Primitive Element Theorem, any number field K contains an element β such that $K = \mathbb{Q}(\beta)$.

You may well have seen another definition of algebraic numbers, which is fine because of the following

> **Exercise 2.1.** Let K be a number field and let $\alpha \in K$ be an algebraic number. Prove that there exists some nonzero polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.
>
> Conversely, suppose that $\alpha \in \mathbb{C}$ satisfies $f(\alpha) = 0$ for some nonzero polynomial $f \in \mathbb{Q}[x]$. Show that there exists a number field K such that $\alpha \in K$.

In particular, we see that the set of all algebraic numbers is a field, none other than $\overline{\mathbb{Q}}$.

> **Example 2.2.** The field $\mathbb{Q}(i)$ of Gaussian numbers is a number field. Therefore $\alpha := 3 - \frac{i}{2}$ is an algebraic number. What rational polynomial equation does it solve?

Number fields generalise the field of rational numbers $\mathbb{Q}$. A natural question is: what is the right generalisation of the ring of integers $\mathbb{Z}$?

This is more subtle than expected:

> **Example 2.3.** The element $\beta_1 = \sqrt{-3}$ is clearly a primitive element for $K = \mathbb{Q}(\sqrt{-3})$. So is
>
> $$\beta_2 = \frac{1 + \sqrt{-3}}{2},$$
>
> in other words $\mathbb{Q}(\beta_1) = \mathbb{Q}(\beta_2)$.
>
> But $\mathbb{Z}[\beta_1] \subsetneq \mathbb{Z}[\beta_2]$.
>
> The moral being that we cannot use primitive elements to generalise $\mathbb{Z}$.

Given a ring extension $R \subseteq S$, we say that $\alpha \in S$ is an *integral element* (over R) if there exists a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$. We say that S is an *integral extension* of R if every $\alpha \in S$ is integral over R.

> **Exercise 2.4.** To make some sense of the terminology: show that for the ring extension $\mathbb{Z} \subsetneq \mathbb{Q}$, $\alpha \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $\alpha \in \mathbb{Z}$.

Let K be a number field. We define the *ring of integers* $\mathcal{O}_K$ of K to be

$$\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ is integral over } \mathbb{Z}\}.$$

Elements of rings of integers are called *algebraic integers*.

But... is $\mathcal{O}_K$ really a ring? In other words, given $\alpha, \beta \in \mathcal{O}_K$, can we conclude that $\alpha + \beta$ and $\alpha\beta$ are also in $\mathcal{O}_K$?

We'll answer this (in the affirmative) more generally.[1] Given a ring extension $R \subseteq S$, the set of elements of S that are integral over R is called the *integral closure* of R in S.

Theorem 2.5. *The integral closure of R in S is a ring.*

To prove this, the following equivalent formulation of integrality is useful (this is pretty close to the treatment in [1, Proposition 5.1]):

Proposition 2.6. *Let $R \subseteq S$ be rings and $\alpha \in S$. The following are equivalent:*

(a) α is integral over R;

(b) $R[\alpha]$ is a finitely-generated R-module *(that is, there exists a finite subset Σ of $R[\alpha]$ such that $R[\alpha] = \mathrm{Span}_R(\Sigma)$);*

(c) there exists a ring R' such that $R[\alpha] \subseteq R' \subseteq S$ and R' is a finitely-generated R-module.

Proof. **(a) ⇒ (b):** The integrality of α gives the existence of an R-linear relation

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0, \qquad c_i \in R.$$

We can then isolate

$$\alpha^n = -c_{n-1}\alpha^{n-1} - \cdots - c_1\alpha - c_0,$$

and continue iteratively to show that α^j is in the R-span of $\{\alpha^{n-1}, \ldots, \alpha, 1\}$ for all $j \geq n$. Therefore this finite set generates $R[\alpha]$ as an R-module.

(b) ⇒ (c): Obvious, taking $R' = R[\alpha]$.

(c) ⇒ (a): Let $\{x_1, \ldots, x_n\}$ be an R-spanning set for R'. At least one of the x_i must be nonzero, as $1 \in R'$.

Fixing $i \in \{1, \ldots, n\}$, since $\alpha \in R'$ and $x_i \in R'$, we have $\alpha x_i \in R'$, so we may express this in terms of the spanning set:

$$\alpha x_i = c_{i1}x_1 + c_{i2}x_2 + \cdots + c_{in}x_n.$$

This defines a matrix $C \in M_n(R)$ with the property that

$$\alpha \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = C \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \qquad \Rightarrow \qquad (\alpha I - C) \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = 0.$$

This implies[2] that $\det(\alpha I - C) = 0$.

Expanding out $\det(\alpha I - C)$ gives us a monic polynomial with coefficients in R having α as a root, so α is integral over R. □

The other ingredient is the transitivity[3] of the property of being finitely-generated:

[1] For a more direct proof, involving more or less the same arguments, see [4, Theorem 2 in Chapter 2].

[2] Seeing this is very easy over a field and a bit more involved over a ring; but you can involve the adjugate matrix of $(\alpha I - C)$ to deduce that $\det(\alpha I - C)\mathbf{x} = \mathbf{0}$, and then conclude that $\det(\alpha I - C)$ acts as zero on the whole R-module R'.

[3] Transitivity is not quite the right term for this, as the three objects involved are not of the same type, but it's the best we can do.

Exercise 2.7 ([2, Lemma 1.7] or [1, Proposition 2.16])**.** Suppose $R \subseteq S$ are rings and M is an S-module. If M is finitely-generated as an S-module and S is finitely-generated as an R-module, then M is finitely-generated as an R-module.

We're finally ready for the

Proof of Theorem 2.5. We have to show that the integral closure A of R in S is a subring of S.

The only interesting part is showing that if $\alpha, \beta \in A$ then $\alpha + \beta, \alpha\beta \in A$.

If $\alpha, \beta \in A$ then they are both integral over R. In particular, $R[\alpha]$ is a finitely-generated R-module. Since β is integral over R, it certainly is integral over $R[\alpha]$, so $\big(R[\alpha]\big)[\beta]$ is a finitely-generated $R[\alpha]$-module, so by "transitivity" we get that $R[\alpha, \beta]$ is a finitely-generated R-module.

This means that every element of $R[\alpha, \beta]$ (for instance $\alpha + \beta$ and $\alpha\beta$) is integral over R. □

Here is a useful integrality criterion:

Exercise 2.8 ([2, Lemma 1.12])**.** An algebraic number $\alpha \in \overline{\mathbb{Q}}$ is an algebraic integer if and only if its minimal polynomial has integer coefficients.

Example 2.9. Suppose d is a squarefree integer and let $K = \mathbb{Q}(\sqrt{d})$. (This is called a *quadratic field.*) Show that the ring of integers of K is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

We have seen that finite generation is "transitive" in Exercise 2.7. So is integrality:

Exercise 2.10. If $R \subseteq S \subseteq T$ with S integral over R and T integral over S, then T is integral over R.

Let R be an integral domain and let $K = \operatorname{Frac}(R)$, the fraction field of R. We say that R is *integrally closed* if any $\alpha \in K$ that is integral over R automatically lies in R.

Example 2.11. The ring $\mathbb{Z}$ is integrally closed. (This is a simple reformulation of Exercise 2.4.)

Proposition 2.12. *If K is a number field with ring of integers $\mathcal{O}_K$ then $K = \operatorname{Frac}(\mathcal{O}_K)$ and $\mathcal{O}_K$ is integrally closed.*

Proof. Clearly $\operatorname{Frac}(\mathcal{O}_K) \subseteq K$. If $\alpha \in K$ then there is some polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. By clearing the denominators in the coefficients of f, we may arrange for f to have integral coefficients:

$$f(\alpha) = c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0, \qquad c_i \in \mathbb{Z}.$$

We can multiply this relation by c_n^{n-1} and rewrite it as

$$(c_n\alpha)^n + c_{n-1}(c_n\alpha)^{n-1} + \cdots + c_1 c_n^{n-2}(c_n\alpha) + c_0 c_n^{n-1} = 0,$$

which means that $\beta \coloneqq c_n\alpha$ satisfies $\beta \in \mathcal{O}_K$. Therefore $\alpha = \frac{\beta}{c_n} \in \operatorname{Frac}(\mathcal{O}_K)$.

To show that $\mathcal{O}_K$ is integrally closed, suppose $\alpha \in K$ is integral over $\mathcal{O}_K$. Since $\mathcal{O}_K$ is an integral extension of $\mathbb{Z}$, Exercise 2.10 implies that α is integral over $\mathbb{Z}$, but then $\alpha \in \mathcal{O}_K$. □

We record here a side effect of the above proof, for future reference:

Corollary 2.13. *For any $\alpha \in K$ there exists $d \in \mathbb{Z}$ such that $d\alpha \in \mathcal{O}_K$. In particular, there exists $\theta \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\theta)$.*

2.2. Rings of integers are Dedekind domains

The next property we investigate is how $\mathcal{O}_K$ sits (geometrically) inside the number field K, viewed as a finite-dimensional $\mathbb{Q}$-vector space.

Proposition 2.14. *Let $k \in \{\mathbb{Q}, \mathbb{R}\}$ and let V be an n-dimensional k-vector space. Suppose $\Lambda \subseteq V$ is a $\mathbb{Z}$-module spanning V. The following are equivalent:*

(a) Λ is a discrete $\mathbb{Z}$-submodule *of V (that is, there exists an open neighbourhood of $0 \in V$ that only intersects Λ in $\{0\}$).*

(b) Λ is finitely generated as a $\mathbb{Z}$-module.

(c) Λ has rank n as a $\mathbb{Z}$-module.

(d) $\Lambda \cong \mathbb{Z}^n$ as a $\mathbb{Z}$-module.

Proof. Since $\Lambda \subseteq V$, it is torsion-free as a $\mathbb{Z}$-module.

(b) ⇒ (a): Let $\{\lambda_1, \ldots, \lambda_m\}$ be a $\mathbb{Z}$-basis for Λ. Consider

$$U = \left\{ \sum_{i=1}^{m} a_i\lambda_i \in V \,\middle|\, |a_i| < 1, a_i \in k \right\}.$$

This is an open neighbourhood of $0 \in V$, and $U \cap \Lambda = \{0\}$, so Λ is discrete.

(a) ⇒ (b): Let $\{v_1, \ldots, v_n\}$ be a k-basis for V, with $v_i \in \Lambda$. Define

$$\Omega = \operatorname{Span}_{\mathbb{Z}}\{v_1, \ldots, v_n\} \subseteq \Lambda.$$

Evidently Ω is a finitely-generated $\mathbb{Z}$-module, so if we can show that the index $[\Lambda : \Omega]$ is finite, we can conclude that Λ is finitely-generated as a $\mathbb{Z}$-module.

Let $X = \Lambda/\Omega$. Let $\varphi\colon k^n \to V$ denote the k-linear map $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i v_i$. We may choose the coset representatives in X to lie in the image under φ of the half-open n-cube $C = [0,1)^n$.

Now we use the assumption that Λ is discrete, so that there exists $B \in \mathbb{Z}_{>0}$ such that

$$\left\{ \sum_{i=1}^{n} c_i v_i \,\middle|\, |c_i| < \frac{1}{B}, c_i \in k \right\} \cap \Lambda = \{0\}.$$

Divide each side $[0,1)$ of the n-cube C into B equal segments of length $\frac{1}{B}$: $[0, \frac{1}{B}), \ldots [\frac{B-1}{B}, 1)$. This partitions C into B^n cubes of side length $\frac{1}{B}$.

If x_1, x_2 are representatives of cosets in $X = \Lambda/\Omega$ that lie in the same small cube, then $x_1 - x_2 \in \Lambda$ and

$$x_1 - x_2 = \sum_{i=1}^{n} c_i v_i \qquad \text{with each } |c_i| < \frac{1}{B},$$

implying that $x_1 = x_2$ by the choice of B. So each of the small B^n cubes contains at most one coset representative, therefore $[\Lambda : \Omega] \le B^n$.

Finally, the **equivalence of (b), (c), and (d)** comes from the fact that a finitely generated torsion free $\mathbb{Z}$-module is free of finite rank, but this rank must equal the k-dimension n of V, since V is spanned by Λ. □

A subset Λ of V satisfying the conditions in Proposition 2.14 is called[4] a *lattice* in V. If Λ is a lattice in V, then $\Omega \subseteq \Lambda$ is a *sublattice* of Λ if Ω is itself a lattice in V.

Theorem 2.15. *If K is a number field then $\mathcal{O}_K$ is a lattice in K and any nonzero ideal I of $\mathcal{O}_K$ is a sublattice of $\mathcal{O}_K$.*

In order to prove this result, we need to take a short detour and discuss embeddings (injective homomorphisms) of number fields into $\mathbb{C}$.

Suppose K is a number field of degree n, then the Primitive Element Theorem gives us some β such that $K = \mathbb{Q}(\beta)$, where the minimal polynomial f of β over $\mathbb{Q}$ has degree n. The complex roots of f are called the *conjugates* of β. Defining an embedding $\sigma\colon K = \mathbb{Q}(\beta) \to \mathbb{C}$ is equivalent to specifying an element $\sigma(\beta) \in \mathbb{C}$ with the property that $f(\sigma(\beta)) = 0$, in other words a conjugate of β. So there are precisely n embeddings $K \hookrightarrow \mathbb{C}$, often denoted $\sigma_1, \dots, \sigma_n$.

If $K \subseteq L$ are two number fields, then each embedding of K into $\mathbb{C}$ can be extended to $[L\colon K]$ distinct embeddings of L into $\mathbb{C}$.

We can now define the *trace* and the *norm* functions of the extension $K/\mathbb{Q}$:

$$\mathrm{Tr}^K_{\mathbb{Q}}\colon K \to \mathbb{Q} \qquad\qquad \mathrm{Tr}^K_{\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad \text{for all } \alpha \in K$$

$$\mathrm{N}^K_{\mathbb{Q}}\colon K \to \mathbb{Q} \qquad\qquad \mathrm{N}^K_{\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{for all } \alpha \in K.$$

> **Exercise 2.16.** Let K be a number field of degree n over $\mathbb{Q}$. Given $\alpha \in K$, let $f \in \mathbb{Q}[x]$ be its minimal polynomial and let $d = \deg(f)$. Show that
>
> $$\mathrm{Tr}^K_{\mathbb{Q}}(\alpha) = \frac{n}{d}\, \mathrm{Tr}^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha) \quad \text{and} \quad \mathrm{N}^K_{\mathbb{Q}}(\alpha) = \left(N^{\mathbb{Q}(\alpha)}_{\mathbb{Q}}(\alpha)\right)^{n/d}.$$
>
> Conclude from this that $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha) \in \mathbb{Q}$ and $\mathrm{N}^K_{\mathbb{Q}}(\alpha) \in \mathbb{Q}$.
>
> Moreover, if $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $\mathrm{N}^K_{\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

We are ready for the

Proof of Theorem 2.15. In the proof of Proposition 2.12 we saw that for any $\alpha \in K$ we have $c\alpha \in \mathcal{O}_K$ for some positive integer c. Therefore we can find a $\mathbb{Q}$-basis $\{\beta_1, \dots, \beta_n\}$ of K with $\beta_i \in \mathcal{O}_K$. In other words, $\mathcal{O}_K$ spans K over $\mathbb{Q}$.

It remains to show that $\mathcal{O}_K$ is discrete in K. Given $\lambda \in \mathcal{O}_K \setminus \{0\}$, there exist $a_1, \dots, a_n \in \mathbb{Q}$ such that $\lambda = \sum_{i=1}^{n} a_i \beta_i$. For any embedding σ of K into $\mathbb{C}$, we think of $\sigma(\lambda)$ as

$$\sigma(\lambda) = \sum_{i=1}^{n} \sigma(\beta_i) a_i,$$

[4] This is fairly standard terminology in number theory, but beware that in other disciplines it would be called a *complete lattice*, and a lattice would only be required to span some subspace of V.

more precisely as a linear polynomial (function) with complex coefficients in the variables $a_1, \dots, a_n$. From this viewpoint, $N(\lambda) = \prod_\sigma \sigma(\lambda)$ is a homogeneous polynomial of degree n in $a_1, \dots, a_n$. Therefore we can make $N(\lambda)$ arbitrarily small, say $|N(\lambda)| < 1$, by substituting sufficiently small rational values for $a_1, \dots, a_n$.

But if $\mathcal{O}_K$ is not discrete in K, for any $\epsilon > 0$ there exist $a_1, \dots, a_n \in \mathbb{Q}$ such that $|a_i| < \epsilon$ and $\lambda := \sum_i a_i \beta_i \in \mathcal{O}_K \smallsetminus \{0\}$. In particular, we can get $|N(\lambda)| < 1$ while at the same time $N(\lambda) \in \mathbb{Z} \smallsetminus \{0\}$, contradiction.

Finally, we consider a nonzero ideal I of $\mathcal{O}_K$. It is discrete since it's a submodule of $\mathcal{O}_K$.

Let $\{\beta_1, \dots, \beta_n\}$ be a $\mathbb{Q}$-basis of K with $\beta_i \in \mathcal{O}_K$. Let $\gamma \in I \smallsetminus \{0\}$, then $c := N(\gamma) \in I \cap \mathbb{Z}$ is a nonzero integer. Therefore $c\beta_i \in I$ for all I, and certainly $\{c\beta_1, \dots, c\beta_n\}$ is a $\mathbb{Q}$-basis of K. □

Corollary 2.17. *If K is a number field and I is a nonzero ideal of $\mathcal{O}_K$, then the quotient $\mathcal{O}_K/I$ is a finite ring.*

Proof. We have just seen that I is a rank n free $\mathbb{Z}$-submodule of the rank n free $\mathbb{Z}$-module $\mathcal{O}_K$. Therefore $\mathcal{O}_K/I$ is a finitely generated torsion $\mathbb{Z}$-module, hence finite. □

Recall that a ring R is *Noetherian* if every ideal of R is finitely generated, or equivalently if every ascending chain of ideals of R stabilises (see [5, Exercise 63] or [1, Chapter 7]). (Or equivalently, if every nonempty set of ideals of R has a maximal element.)

Corollary 2.18. *If K is a number field then $\mathcal{O}_K$ is a Noetherian ring.*

Proof. Let $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals of $\mathcal{O}_K$. If all $I_j = 0$ then the chain stabilises.

Otherwise there is a smallest j such that $I := I_j \neq 0$. There is a bijection

$$\{\text{ideals of } \mathcal{O}_K/I\} \quad \leftrightarrow \quad \{\text{ideals of } \mathcal{O}_K \text{ containing } I\}$$

so both sets are finite since Corollary 2.17 says that $\mathcal{O}_K/I$ is finite. This forces the ascending chain to stabilise since its elements lie in a finite set of ideals. □

The *Krull dimension* of a ring R is the maximum length of any strict chain of prime ideals in R:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n.$$

Exercise 2.19. Suppose R is an integral domain.

(a) The Krull dimension of R is 0 if and only if R is a field.

(b) The Krull dimension of R is ≤ 1 if and only if every nonzero prime ideal of R is maximal.

Corollary 2.20. *If K is a number field then $\mathcal{O}_K$ has Krull dimension* 1.

Proof. We first rule out the possibility that $\dim \mathcal{O}_K = 0$: since $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, which is not a field, we know that $\mathcal{O}_K$ is not a field.

Now we show that every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is maximal (and use Exercise 2.19). But Corollary 2.17 says that $\mathcal{O}_K/\mathfrak{p}$ is a finite ring, in fact a finite integral domain since $\mathfrak{p}$ is a prime ideal. However, any finite integral domain is automatically a field, so $\mathfrak{p}$ is maximal. □

Exercise 2.21. Recall (or work out) why a finite integral domain is a field.

A Noetherian integral domain R that is integrally closed of Krull dimension 1 is called a *Dedekind domain*. Therefore we have proved that

Theorem 2.22. *If K is a number field then $\mathcal{O}_K$ is a Dedekind domain.*

2.3. Unique factorisation into prime ideals

Our next objective is to prove a property of Dedekind domains that is crucial for arithmetic applications: unique factorisation of ideals into prime ideals. This will be Theorem 2.28, for which we need a number of intermediate results.

Recall that the sum of two ideals I and J is defined as

$$I + J = \{i + j \mid i \in I, j \in J\}.$$

It is the smallest ideal of R containing both I and J.

On the other hand, the product of I and J is defined as

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k \,\middle|\, n \in \mathbb{N}, i_k \in I, j_k \in J \right\}.$$

In other words, IJ is the smallest ideal of R containing the products ij for all $i \in I$, $j \in J$.

In addition to the concept of ideal, we also make use of the more general concept of fractional ideal: Let $K = \mathrm{Frac}(R)$ with R an integral domain; a *fractional ideal* of R is an R-submodule $I \subseteq K$ with the property that there exists $d \in R$, $d \neq 0$, such that $dI \subseteq R$. The sum and product operations for fractional ideals are defined in the same way as for ideals.

Example 2.23. Let I be the $\mathbb{Z}$-submodule of $\mathbb{Q}$ generated by $\frac{1}{2}$, $\frac{1}{3}$, and $\frac{1}{5}$. Then taking $d = 2 \cdot 3 \cdot 5 = 30$ we have $di \in \mathbb{Z}$ for all $i \in I$, so I is a fractional ideal of $\mathbb{Z}$ that is not an actual ideal of $\mathbb{Z}$.

Example 2.24. Let $K = \mathrm{Frac}(R)$, R an integral domain, J a nonzero ideal of R. Then

$$J^{-1} := \{\alpha \in K \mid \alpha J \subseteq R\}$$

is a fractional ideal of R that contains R.

(Take d to be any nonzero element of J.)

Here is an ideal version of the defining property of prime ideals:

Exercise 2.25. Let R be a ring, $I_1, \ldots, I_n$ ideals of R, and $\mathfrak{p}$ a prime ideal of R such that $I_1 \ldots I_n \subseteq \mathfrak{p}$. Then there exists $j \in \{1, \ldots, n\}$ such that $I_j \subseteq \mathfrak{p}$.

Lemma 2.26. *Let R be a Noetherian ring and I a nonzero ideal of R. There exist nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of R such that $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq I$.*

Proof. Suppose the statement is false and let S be the set of all nonzero ideals I of R for which the statement fails.

Since S is a nonempty set of ideals of R and R is Noetherian, S has a maximal element $I_{\max} \in S$. This is not a prime ideal, so there exist elements $x_1, x_2 \in R$ such that $x_1, x_2 \notin I_{\max}$ but $x_1 x_2 \in I_{\max}$. Let $J_1 = I_{\max} + x_1 R$, then J_1 properly contains $I_{\max}$ so $J_1 \notin S$. Similarly for $J_2 = I_{\max} + x_2 R$.

So the statement of the Lemma holds for both J_1 and J_2, and we have a nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ such that

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq J_1, \qquad \mathfrak{q}_1 \ldots \mathfrak{q}_m \subseteq J_2 \qquad \Rightarrow \qquad \mathfrak{p}_1 \ldots \mathfrak{p}_n \mathfrak{q}_1 \ldots \mathfrak{q}_m \subseteq J_1 J_2.$$

However,

$$J_1 J_2 = (I_{\max} + x_1 R)(I_{\max} + x_2 R) = I_{\max}(I_{\max} + x_1 R + x_2 R) + x_1 x_2 R \subseteq I_{\max},$$

implying that $I_{\max} \notin S$, contradiction. □

Proposition 2.27. *Let $\mathfrak{p}$ be a nonzero prime ideal of a Dedekind domain R.*

(a) $\mathfrak{p}^{-1} \neq R$.

(b) If J is a nonzero ideal of R, then $\mathfrak{p}^{-1} J \neq J$.

(c) $\mathfrak{p}^{-1}\mathfrak{p} = R$.

Proof.

(a) We want to exhibit an element of $\mathfrak{p}^{-1}$ that is not in R. Since $\mathfrak{p}$ is nonzero, it contains some nonzero element $i \in \mathfrak{p}$, and $I := iR$ is a nonzero ideal of R. By Lemma 2.26 there exist nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq I$. Choose these prime ideals in such a way that n is as small as possible. Now $\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq I \subseteq \mathfrak{p}$, so at least one $\mathfrak{p}_k \subseteq \mathfrak{p}$, say (for the sake of notation) $\mathfrak{p}_1 \subseteq \mathfrak{p}$. However R is Dedekind hence of Krull dimension 1, so $\mathfrak{p}_1 = \mathfrak{p}$.

If $n = 1$, we conclude that $\mathfrak{p} = iR$, so that $\mathfrak{p}^{-1} = i^{-1}R$. Suppose $i^{-1}R = R$, then $\mathfrak{p} = iR = R$, contradicting the fact that $\mathfrak{p}$ is prime.

If $n > 1$, the minimality of n implies that $\mathfrak{p}_2 \ldots \mathfrak{p}_n \nsubseteq iR$, so there exists $j \in \mathfrak{p}_2 \ldots \mathfrak{p}_n$ with $j \notin iR$. However $j\mathfrak{p} = \mathfrak{p}_1 j \subseteq \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n \subseteq iR$. Now consider the element $x = \frac{j}{i} \in K$. By construction $x\mathfrak{p} \subseteq R$ but $x \notin R$.

(b) Suppose $\mathfrak{p}^{-1} J = J$ and let $\alpha_1, \ldots, \alpha_m$ be a set of generators of J. Given $x \in \mathfrak{p}^{-1}$ and $i \in \{1, \ldots, m\}$ we can write

$$x\alpha_i = \sum_{j=1}^{m} c_{ij} \alpha_j \qquad c_{ij} \in R.$$

Note that this equality takes place in the fraction field K of R.

Let $C = (c_{ij})$ be the matrix formed by these coefficients, and let $A = xI_m - C \in M_m(K)$; then

$$A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} = 0,$$

hence $\det(A) = 0$. But as a polynomial expression in x, $\det(A)$ is monic with coefficients in R, so we conclude that x is integral over R.

Since R is Dedekind, it is integrally closed, so $x \in R$. This implies that $\mathfrak{p}^{-1} = R$, contradicting the result of part (a).

(c) Since $R \subseteq \mathfrak{p}^{-1}$ we have $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R$. But $\mathfrak{p}$ is a nonzero prime ideal in a ring of Krull dimension 1, so it is a maximal ideal, hence one of the two inclusions must be an equality (and the other one strict). By part (b), we know that the first inclusion is strict: $\mathfrak{p} \neq \mathfrak{p}^{-1}\mathfrak{p}$. Therefore $\mathfrak{p}^{-1}\mathfrak{p} = R$.

□

Theorem 2.28. *Any Dedekind domain R has unique factorisation of ideals, that is every proper ideal I of R can be written uniquely (up to permuting the factors) as a product of finitely many prime ideals of R.*

Proof. We prove the existence claim by contradiction. Let S denote the set of proper ideals of R that **do not** have a prime factorisation, and suppose $S \neq \varnothing$. Since R is Noetherian, S has a maximal element J. In turn, J is contained in some maximal ideal[5] $\mathfrak{p}$. Starting with $R \subseteq \mathfrak{p}^{-1}$ we get $J \subseteq J\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$.

But we know that $J \neq J\mathfrak{p}^{-1}$, so by the maximality of J we must have $J\mathfrak{p}^{-1} \notin S$:

$$J\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_n.$$

Multiply both sides by $\mathfrak{p}$ to get that $J \notin S$, contradiction.

For uniqueness, suppose we have

$$I = \mathfrak{p}_1 \dots \mathfrak{p}_n = \mathfrak{q}_1 \dots \mathfrak{q}_m.$$

In particular, $\mathfrak{q}_1 \dots \mathfrak{q}_m \subseteq \mathfrak{p}_1$, which is a prime ideal, so there exists j such that $\mathfrak{q}_j \subseteq \mathfrak{p}_1$. Without loss of generality $j = 1$, so $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$, but in fact we have equality since R is 1-dimensional. So we can multiply both sides of the equality by $\mathfrak{p}^{-1}$ and reduce it to

$$\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{q}_2 \dots \mathfrak{q}_m.$$

Continue until you conclude that $m = n$ and (after permutation) $\mathfrak{p}_j = \mathfrak{q}_j$ for all j. □

We often group together the prime ideals that appear more than once in the factorisation and write, for a proper ideal I of R:

$$I = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}, \qquad \mathfrak{p}_j \text{ distinct, } e_j \in \mathbb{Z}_{>0}.$$

We also write $\mathrm{ord}_{\mathfrak{p}_j}(I) = e_j$ or $v_{\mathfrak{p}_j}(I) = e_j$ and extend this notation to elements $\alpha \in R$ via $\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\alpha R)$. This has the property that

$$\mathrm{ord}_{\mathfrak{p}}(IJ) = \mathrm{ord}_{\mathfrak{p}}(I) + \mathrm{ord}_{\mathfrak{p}}(J).$$

The following result is part of the first assignment:

Proposition 2.29. *Let R be a Dedekind domain and let $I \neq 0$ be an ideal of R.*

(a) If $I = \mathfrak{p}_1 \dots \mathfrak{p}_n$ is the factorisation of I into prime ideals, then $I^{-1} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1}$.

(b) Show that $II^{-1} = R$.

Given a Dedekind domain R, let $I(R)$ denote the set of nonzero fractional ideals of R.

Lemma 2.30. *$I(R)$ is an abelian group under multiplication, with identity element R.*

[5] We perversely denote this $\mathfrak{p}$ instead of $\mathfrak{m}$, but it's okay because we're in a Dedekind domain.

Proof. If J_1, J_2 are fractional ideals, then $d_1 J_1 \subseteq R$ and $d_2 J_2 \subseteq R$ for some $d_1, d_2 \in R \setminus \{0\}$. Letting $d = d_1 d_2$, we have $d(J_1 J_2) = (d_1 J_1)(d_2 J_2) \subseteq R$, so $J_1 J_2$ is a fractional ideal.

It's clear that R is the identity element.

If J is a nonzero fractional ideal, with $I := dJ \subseteq R$, then I is a nonzero ideal of R. Consider the fractional ideal dI^{-1}:

$$J\,dI^{-1} = (dJ)I^{-1} = II^{-1} = R,$$

so dI^{-1} is the inverse of J. □

Borrowing from the terminology for ideals, we define a *principal fractional ideal* of R to be a fractional ideal of the form xR for some $x \in K$. Letting $P(R)$ denote the set of all nonzero principal fractional ideals of R, we have that $P(R)$ is a subgroup of $I(R)$. This leads us to an essential element in the study of number fields and their rings of integers: the *ideal class group* of a Dedekind domain R is defined to be

$$\mathrm{Cl}(R) = I(R)/P(R).$$

One of our next milestones will be to prove that, for $R = \mathcal{O}_K$ the ring of integers in a number field, the class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite. Its cardinality is called the *class number* of $\mathcal{O}_K$ (or by abuse of language, of K). It is an arithmetically important quantity as it measures how far a ring is from having unique factorisation into irreducibles.

It is also closely related to the notion of Picard group of a ring, or more generally of a scheme, which plays an important role in algebraic geometry.

2.4. Discriminant

Given a separable field extension L/K, fix an algebraic closure $\overline{K}$ of K and let $\sigma_1, \dots, \sigma_n \colon L \hookrightarrow \overline{K}$ be the distinct embeddings. For elements $\alpha_1, \dots, \alpha_n \in L$, consider the matrix $\Sigma = (\sigma_i(\alpha_j))$ and let $\Delta = \Delta(\alpha_1, \dots, \alpha_n) := (\det \Sigma)^2$.

Lemma 2.31. *Suppose $\beta \in L$ is a primitive element for L/K, so that $L = K(\beta)$. Then $\Delta(1, \beta, \dots, \beta^{n-1}) \in K \setminus \{0\}$.*

Proof. We have

$$\Sigma = \Sigma(1, \beta, \beta^2, \dots, \beta^{n-1}) = \begin{bmatrix} 1 & (\sigma_1(\beta)) & (\sigma_1(\beta))^2 & \dots & (\sigma_1(\beta))^{n-1} \\ 1 & (\sigma_2(\beta)) & (\sigma_2(\beta))^2 & \dots & (\sigma_2(\beta))^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\sigma_n(\beta)) & (\sigma_n(\beta))^2 & \dots & (\sigma_n(\beta))^{n-1} \end{bmatrix},$$

a Vandermonde matrix in the variables $\sigma_1(\beta), \dots, \sigma_n(\beta)$. Therefore

$$\Delta = (\det \Sigma)^2 = \prod_{1 \le i < j \le n} (\sigma_i(\beta) - \sigma_j(\beta)) = (-1)^{\binom{n}{2}} \prod_{1 \le i \ne j \le n} (\sigma_i(\beta) - \sigma_j(\beta)).$$

Since $\sigma_i \neq \sigma_j$ and β is a generator of the field extension L/K, we get that $\sigma_i(\beta) \neq \sigma_j(\beta)$, so $\Delta \neq 0$.

Letting G denote the Galois group of the minimal polynomial of β over K, we have that G is a subgroup of the symmetric group S_n, and Δ is invariant under the permutation action of S_n on $\{\sigma_1, \dots, \sigma_n\}$. Therefore Δ is invariant under G, hence it takes values in the base field K. □

Proposition 2.32. *Let $\alpha_1, \dots, \alpha_n \in L$. Then $\Delta = \Delta(\alpha_1, \dots, \alpha_n) \in K$ and $\Delta = 0$ if and only if $\alpha_1, \dots, \alpha_n \in L$ are linearly dependent over K.*

Proof. Suppose $\alpha_1, \dots, \alpha_n$ satisfy a K-linear relation, say there is an K-linear form ϕ in n variables such that $\phi(\alpha_1, \dots, \alpha_n) = 0$.

Since the embeddings σ_i are themselves K-linear, for all i we have

$$\phi(\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)) = \sigma_i(\phi(\alpha_1, \dots, \alpha_n)) = 0,$$

which implies that the vectors

$$v_1 = \begin{bmatrix} \sigma_1(\alpha_1) \\ \vdots \\ \sigma_n(\alpha_1) \end{bmatrix}, \dots, v_n = \begin{bmatrix} \sigma_1(\alpha_n) \\ \vdots \\ \sigma_n(\alpha_n) \end{bmatrix}$$

themselves satisfy the relation $\phi(v_1, \dots, v_n) = 0$. But these are precisely the columns of the matrix Σ, hence the determinant of Σ is zero.

If $\alpha_1, \dots, \alpha_n$ are linearly independent, hence a basis of L over K, consider the change of basis matrix $P \in \mathrm{GL}_n(K)$ satisfying

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = P \begin{bmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{bmatrix}.$$

As M has coefficients in the base field K fixed by all the embeddings σ_i, the above equation holds after applying these embeddings, and we can package all this into

$$\Sigma(\alpha_1, \alpha_2, \dots, \alpha_n) = P\Sigma(1, \theta, \dots, \theta^{n-1}).$$

Take determinants on both sides and square to conclude. □

The following consequence is immediate:

Corollary 2.33. *If $K \subset L$ are number fields and $\omega_1, \dots, \omega_n \in \mathcal{O}_L$, then $\Delta(\omega_1, \dots, \omega_n) \in \mathcal{O}_K$.*

In particular, if $K = \mathbb{Q}$ and $\omega_1, \dots, \omega_n \in \mathcal{O}_L$ are a $\mathbb{Q}$-basis, then $\Delta(\omega_1, \dots, \omega_n)$ is a (strictly) positive integer.

Proposition 2.34. *Let K be a number field and $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ a $\mathbb{Q}$-basis for K. Let $\Delta = \Delta(\alpha_1, \dots, \alpha_n)$. Then*

$$\mathcal{O}_K \subseteq \mathbb{Z}\frac{\alpha_1}{\Delta} + \dots + \mathbb{Z}\frac{\alpha_n}{\Delta}.$$

Proof. For a given $\alpha \in \mathcal{O}_K$, write

$$\alpha = c_1\alpha_1 + \dots + c_n\alpha_n \qquad c_j \in \mathbb{Q}.$$

We want to show that $\Delta c_j \in \mathbb{Z}$ for all j.

Let $\Sigma = \Sigma(\alpha_1, \dots, \alpha_n)$ so that $\Delta = (\det \Sigma)^2$. We apply the embeddings $\sigma_1, \dots, \sigma_n$ to the expression for α to get

$$\begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix} = \Sigma \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

Let $\delta = \det \Sigma$ and let Σ' be the adjugate matrix of Σ, so that $\Sigma\Sigma' = \delta I$. Multiply both sides of the last equality by $\delta\Sigma'$ to get

$$\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \Delta \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

Each m_j is an algebraic integer, but also $m_j = \Delta c_j \in \mathbb{Q}$, so $m_j \in \mathbb{Z}$ hence $\Delta c_j \in \mathbb{Z}$, as needed. □

Proposition 2.35. *Let $\mathcal{O}_K$ be the ring of integers in a number field K. If $\omega_1, \dots, \omega_n$ and $\omega'_1, \dots, \omega'_n$ are $\mathbb{Z}$-module bases for $\mathcal{O}_K$, then*

$$\Delta(\omega_1, \dots, \omega_n) = \Delta(\omega'_1, \dots, \omega'_n).$$

Proof. Letting P denote the change of basis matrix, we have $P \in \mathrm{GL}_n(\mathbb{Z})$ and $\Delta = (\det P)^2 \Delta'$, but $\det P \in \{-1, 1\}$. □

So the value of $\Delta(\omega_1, \dots, \omega_n) \in \mathbb{Z}$ is independent of the choice of integral basis. We call it the *discriminant* of $\mathcal{O}_K$ (or, by abuse of language, of K) and denote it Δ_K.

Proposition 2.36. *Let $\mathcal{O}_K$ be the ring of integers in a number field K. Let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ be a $\mathbb{Q}$-basis for K and let $M = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$. Then*

$$\Delta(\alpha_1, \dots, \alpha_n) = [\mathcal{O}_K : M]^2 \, \Delta_K.$$

Proof. Fixing an integral basis $\omega_1, \dots, \omega_n$ of $\mathcal{O}_K$, we let P be the change of basis matrix so that

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = P \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}.$$

As before, apply the embeddings σ_i to conclude that

$$\Delta(\alpha_1, \dots, \alpha_n) = (\det P)^2 \Delta_K.$$

Finally, note that $\det P = [\mathcal{O}_K : M]$. □

2.5. Ideal norm and finiteness of the ideal class group

Let $\mathcal{O}_K$ be the ring of integers in a number field K. Recall that we want to show that the class group of $\mathcal{O}_K$ is finite. In order to do this we will define the *norm of an ideal I* of $\mathcal{O}_K$ as $N(I) = [\mathcal{O}_K : I]$.

The relation between the norm of an element and the norm of the principal ideal it generates is what we would hope for:

Proposition 2.37. *For any $\alpha \in \mathcal{O}_K$ we have $N(\alpha\mathcal{O}_K) = |N(\alpha)|$.*

Proof. Take an integral basis $\omega_1, \dots, \omega_n$ of $\mathcal{O}_K$, then $\alpha\omega_1, \dots, \alpha\omega_n$ is a $\mathbb{Z}$-module basis for $\alpha\mathcal{O}_K$. Expressing each $\alpha\omega_i$ as a $\mathbb{Z}$-linear combination of $\omega_1, \dots, \omega_n$ gives us

$$\begin{bmatrix} \alpha\omega_1 \\ \vdots \\ \alpha\omega_n \end{bmatrix} = A \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}$$

with $A \in M_n(\mathbb{Z})$ and $|\det A| = [\mathcal{O}_K : \alpha\mathcal{O}_K] = N(\alpha\mathcal{O}_K)$. Getting the embeddings involved leads us to

$$\Delta(\alpha\omega_1, \dots, \alpha\omega_n) = N(\alpha\mathcal{O}_K)^2 \Delta_K.$$

However, back to the definition of Δ, we have

$$\Delta(\alpha\omega_1, \dots, \alpha\omega_n) = (\det \Sigma(\alpha\omega_1, \dots, \alpha\omega_n))^2 = (\sigma_1(\alpha) \dots \sigma_n(\alpha))^2 (\det \Sigma(\omega_1, \dots, \omega_n))^2 = N(\alpha)^2 \Delta_K.$$

□

Next we show that the ideal norm function is multiplicative: $N(IJ) = N(I)N(J)$.

You already know this to be true in the case where I and J are relatively prime ideals, by the ring version of the Chinese Remainder Theorem[6].

Lemma 2.38. *Let R be a ring of Krull dimension 1, $\mathfrak{p}$ and $\mathfrak{q}$ distinct nonzero prime ideals of R, and $s, t \in \mathbb{Z}_{>0}$. Then the ideals $\mathfrak{p}^s$ and $\mathfrak{q}^t$ are relatively prime.*

Proof. In the special case $s = t = 1$, we have $\mathfrak{p} \subsetneq \mathfrak{p} + \mathfrak{q} \subseteq R$ (since the ideals are distinct), but $\mathfrak{p}$ is maximal (because of Krull dimension 1) so $\mathfrak{p} + \mathfrak{q} = R$, done.

For general s and t, we want to show that $1 \in \mathfrak{p}^s + \mathfrak{q}^t$. I claim that $(\mathfrak{p} + \mathfrak{q})^{s+t} \subseteq \mathfrak{p}^s + \mathfrak{q}^t$, which will finish the proof by the special case $s = t = 1$ settled above[7].

We need to prove that any product of the form $(p_1 + q_1)(p_2 + q_2)\dots(p_{s+t} + q_{s+t})$ is in fact in $\mathfrak{p}^s + \mathfrak{q}^t$. But such product is the sum of products of $s + t$ factors, each of which is either a p_i or a q_j. Since the number of p_i's and the number of q_j's adds up to $s + t$, each of these products contains $\geq s$ p_i's or $\geq t$ q_j's, which puts it in $\mathfrak{p}^s$ or in $\mathfrak{q}^t$. □

Lemma 2.39. *Let $\mathcal{O}_K$ be the ring of integers in a number field K, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $N(\mathfrak{p}^m) = N(\mathfrak{p})^m$ for all $m \in \mathbb{Z}_{\geq 0}$.*

Proof. There is a chain of ideals

$$\mathfrak{p}^m \subsetneq \mathfrak{p}^{m-1} \subsetneq \dots \subsetneq \mathfrak{p} \subsetneq \mathcal{O}_K,$$

from which we know that

$$N(\mathfrak{p}^m) = [\mathcal{O}_K : \mathfrak{p}^m] = \prod_{j=0}^{m-1} [\mathfrak{p}^j : \mathfrak{p}^{j+1}].$$

We claim that, for all j, $\mathfrak{p}^j/\mathfrak{p}^{j+1} \cong \mathcal{O}_K/\mathfrak{p}$, which certainly will imply the desired result.

Pick an element $\beta \in \mathcal{O}_K$ with $\mathrm{ord}_{\mathfrak{p}}(\beta) = j$ and define a group homomorphism[8] $\varphi: \mathcal{O}_K \to \mathfrak{p}^j/\mathfrak{p}^{j+1}$ by $\varphi(x) = \beta x$. It remains to sort out two details:

- $\ker\varphi = \mathfrak{p}$. This follows from the equality of ideals $\beta\mathcal{O}_K \cap \mathfrak{p}^{j+1} = \beta\mathfrak{p}$: it is clear that $\beta\mathfrak{p} \subseteq \beta\mathcal{O}_K \cap \mathfrak{p}^{j+1}$. In the other direction, let $\beta x \in \beta\mathcal{O}_K \cap \mathfrak{p}^{j+1}$. Therefore

  $$j + \mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(\beta) + \mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(\beta x) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{p}^{j+1}) = j + 1,$$

  so $\mathrm{ord}_{\mathfrak{p}}(x) \geq 1$ and $x \in \mathfrak{p}$.

- φ is surjective. This follows from the equality of ideals $\beta\mathcal{O}_K + \mathfrak{p}^{j+1} = \mathfrak{p}^j$: we have

  $$\mathfrak{p}^{j+1} \subsetneq \beta\mathcal{O}_K + \mathfrak{p}^{j+1} \subseteq \mathfrak{p}^j,$$

  from which we can conclude by considering the unique factorisation of the ideal $\beta\mathcal{O}_K + \mathfrak{p}^{j+1}$.

□

Theorem 2.40. *Let $\mathcal{O}_K$ be the ring of integers in a number field K, and let I and J be ideals of $\mathcal{O}_K$. Then $N(IJ) = N(I)N(J)$.*

[6] Recall that two ideals I and J of a ring R are *relatively prime* if $I + J = R$, and that in this situation, the Chinese Remainder Theorem gives a ring isomorphism $R/(IJ) \cong (R/I) \times (R/J)$.

[7] I believe that we can lower this a bit more to $(\mathfrak{p} + \mathfrak{q})^{s+t-1} \subseteq \mathfrak{p}^s + \mathfrak{q}^t$, but such level of optimisation is not actually needed in the proof.

[8] Here we are working with the additive structure of $\mathcal{O}_K$.

Proof. Combine the factorisation of ideals of $\mathcal{O}_K$ into prime ideals with the two previous lemmas. □

Theorem 2.41. *Let $\mathcal{O}_K$ be the ring of integers in a number field K of degree n, and let $p \in \mathbb{Z}$ be a prime number. Consider the unique factorisation of the ideal $p\mathcal{O}_K$:*

$$p\mathcal{O}_K = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j},$$

where the $\mathfrak{p}_j$'s are distinct prime ideals and $e_j \in \mathbb{Z}_{>0}$. Then for each j we have $N(\mathfrak{p}_j) = p^{f_j}$ for some $f_j \in \mathbb{Z}_{>0}$, and the following relation holds:

$$\sum_{j=1}^{g} e_j f_j = n.$$

Proof. This follows from the multiplicativity of the ideal norm and the relation between the element norm and the ideal norm:

$$p^n = N(p) = N(p\mathcal{O}_K) = \prod_{j=1}^{g} N(\mathfrak{p}_j)^{e_j}.$$

This equation forces $N(\mathfrak{p}_j)$ to be a power of p, and gives the desired relation between the e_j's, the f_j's, and the degree n. □

The positive integer e_j is called the *ramification index* of $\mathfrak{p}_j$ over p, while the positive integer f_j is called the *residue degree* or *inertial degree* of $\mathfrak{p}_j$ over p.

Our proof of finiteness of the ideal class group follows the strategy described in the following

Proposition 2.42. *Let $\mathcal{O}_K$ be the ring of integers in a number field K.*

(a) Given any $B > 0$, the number of ideals of $\mathcal{O}_K$ whose norm is less than B is finite.

(b) The ideal class group of $\mathcal{O}_K$ is finite if and only if there exists a constant $B > 0$ (depending only on K) such that every ideal class contains an ideal of norm less than B.

Proof.

(a) Luckily for us, ideal norms are non-negative integers. Therefore it suffices to show, for every $n \geq 0$, that the number of ideals of norm n is finite.

Suppose I is an ideal with norm n, that is $\#(\mathcal{O}_K/I) = n$. Then $n\alpha = 0$ for all $\alpha \in \mathcal{O}_K/I$, which implies that $n\mathcal{O}_K \subseteq I$. But $\mathcal{O}_K/n\mathcal{O}_K$ is finite, so there are only finitely many ideals containing $n\mathcal{O}_K$, hence finitely many ideals I of norm n.

(b) Suppose there exists a constant $B > 0$ such that every ideal class contains an ideal of norm less than B. By part (a), the number of such ideals is finite, and each ideal belongs to at most one ideal class, therefore there are finitely many ideal classes.

Conversely, suppose the ideal class group is finite and pick representatives $I_1, \dots, I_r$ for the ideal classes. Let $B = \max\{N(I_j)\} + 1$, then B satisfies the desired condition.

□

Theorem 2.43. *Let $\mathcal{O}_K$ be the ring of integers in a number field K. Let $\omega_1, \dots, \omega_n$ be an integral basis for $\mathcal{O}_K$ and let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings of K into $\mathbb{C}$. Set*

$$B_K := \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\omega_j)|.$$

(a) Every nonzero ideal I of $\mathcal{O}_K$ contains a nonzero element α such that

$$|N(\alpha)| \leq B_K\, N(I).$$

(b) Every ideal class of $\mathcal{O}_K$ contains a nonzero ideal of norm less than B_K.

Proof.

(a) Let $m \in \mathbb{Z}_{>0}$ be maximal with the property that $m^n \leq N(I)$, so that $N(I) < (m+1)^n$. We define a subset S of $\mathcal{O}_K$ by

$$S = \left\{ \sum_{j=1}^{n} m_j \omega_j \mid m_j \in \{0, 1, \ldots, m\} \right\}.$$

Clearly $\#S = (m+1)^n > N(I)$, so the elements of S cannot all be in distinct cosets modulo I. Let $x \neq y \in S$ be such that $\alpha := x - y \in I$, then

$$\alpha = \sum_{j=1}^{n} c_j \omega_j \qquad \text{with } |c_j| \leq m.$$

What can we say about the norm of α?

$$|N(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| = \prod_{i=1}^{n} \left| \sum_{j=1}^{n} c_j \sigma_i(\omega_j) \right| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |c_j|\, |\sigma_i(\omega_j)| \leq m^n \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\omega_j)| = m^n B_K \leq B_K\, N(I).$$

(b) Take an arbitrary ideal class c of $\mathcal{O}_K$ and let I be some (non-fractional) ideal representing the **inverse** of c under the group operation of $\mathrm{Cl}(\mathcal{O}_K)$: $[I] = c^{-1}$. By part (a), there exists a nonzero element $\alpha \in I$ such that $|N(\alpha)| \leq B_K\, N(I)$.

Let's consider the unique factorisation into prime ideals of $\alpha\mathcal{O}_K$ and of I:

$$\begin{aligned} \alpha\mathcal{O}_K &= \mathfrak{p}_1 \ldots \mathfrak{p}_r \\ I &= \mathfrak{q}_1 \ldots \mathfrak{q}_s. \end{aligned}$$

Since $\alpha\mathcal{O}_K \subseteq I$, we have $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{q}_1$, and the latter is a prime ideal so there exists j such that $\mathfrak{p}_j \subseteq \mathfrak{q}_1$, from which we get $\mathfrak{p}_j = \mathfrak{q}_1$ from Krull dimension 1. This implies that the prime ideal factorisation of I is a subset of the prime ideal factorisation of $\alpha\mathcal{O}_K$; letting J denote the ideal defined by the complement (the remaining part of the factorisation), we have $\alpha\mathcal{O}_K = IJ$.

We note that the class $[J]$ of J in $\mathrm{Cl}(\mathcal{O}_K)$ is precisely c, and that

$$N(J) = |N(\alpha)|/N(I) \leq B_K,$$

as wanted.

□

Putting all the pieces together, we arrive at our goal:

Theorem 2.44. *The ideal class group of the ring of integers in a number field is finite.*

A side effect of the proof also gives us

Corollary 2.45. *Let $\mathcal{O}_K$ be the ring of integers of a number field K. If every ideal I such that*

$$N(I) \leq B_K := \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\omega_j)|$$

is principal, then $\mathcal{O}_K$ is a principal ideal domain.

3. Decomposition of primes in ring extensions

Let $\mathcal{O}_K$ be the ring of integers in a number field K of degree n over $\mathbb{Q}$. We have seen that, given any prime number $p \in \mathbb{Z}$, there exists a decomposition

$$p\mathcal{O}_K = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j},$$

where the $\mathfrak{p}_j$'s are distinct prime ideals of $\mathcal{O}_K$, $e_j \in \mathbb{Z}_{>0}$, $N(\mathfrak{p}_j) = p^{f_j}$ with $f_j \in \mathbb{Z}_{>0}$ and $\sum_{j=1}^{g} e_j f_j = n$.

We say that $\mathfrak{p}_j$ *lies over* p (or that $\mathfrak{p}_j$ divides p). Several different situations may arise:

- p is *ramified* in $\mathcal{O}_K$ if there exists j such that $e_j > 1$;
- p is *totally ramified* in $\mathcal{O}_K$ if $p\mathcal{O}_K = \mathfrak{p}^n$ for a prime ideal $\mathfrak{p}$;
- p is *inert* in $\mathcal{O}_K$ if $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$;
- p *splits completely* in $\mathcal{O}_K$ if $g = n$.

Example 3.1. Let $K = \mathbb{Q}(i)$. Then

- $2\mathcal{O}_K = (1+i)^2$ so 2 is totally ramified;
- if $p \equiv 1 \pmod 4$ then $p\mathcal{O}_K = (a+bi)(a-bi)$ with a, b such that $a^2 + b^2 = p$, so p splits completely;
- if $p \equiv 3 \pmod 4$ then p is inert.

These claims can be proved using properties of norms, but we'll get most of them as a special case of the next result.

Recall that for any prime number p, we have the *quadratic residue symbol* modulo p, defined by

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{if } p \mid d \\ 1 & \text{if } d \text{ is a square modulo } p \\ -1 & \text{if } d \text{ is not a square modulo } p. \end{cases}$$

Proposition 3.2. *Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree.*[1] *Let p be a prime with $\gcd(p, 2d) = 1$.*

(a) If $\left(\frac{d}{p}\right) = 1$ then p splits completely in $\mathcal{O}_K$. More precisely

$$p\mathcal{O}_K = \left(p, a + \sqrt{d}\right)\left(p, a - \sqrt{d}\right)$$

where $a^2 \equiv d \pmod p$, the two ideals on the right are prime and distinct.

[1] Just to be clear, an integer d is called *squarefree* if $d \neq 1$ and d is not divisible by m^2 for any $m \in \mathbb{Z}_{>1}$. In particular, -1 is considered squarefree but 1 is not.

(b) If $\left(\frac{d}{p}\right) = -1$ then p is inert in $\mathcal{O}_K$.

Proof.

(a) We have
$$(p, a + \sqrt{d})(p, a - \sqrt{d}) = (p^2, p(a + \sqrt{d}), p(a - \sqrt{d}), a^2 - d).$$
Since $a^2 \equiv d \pmod{p}$, all four generators of the ideal on the right are divisible by p, so $(p, a + \sqrt{d})(p, a - \sqrt{d}) \subseteq p\mathcal{O}_K$.

Conversely, $p^2 \in (p, a + \sqrt{d})(p, a - \sqrt{d})$, but also
$$p(2a) = p(a + \sqrt{d}) + p(a - \sqrt{d}) \in (p, a + \sqrt{d})(p, a - \sqrt{d}).$$
Therefore $p = p \gcd(p, 2a) = \gcd(p^2, p(2a)) \in (p, a + \sqrt{d})(p, a - \sqrt{d})$.

We now prove that $(p, a + \sqrt{d}) \neq (p, a - \sqrt{d})$. Suppose not, then $a - \sqrt{d} \in (p, a + \sqrt{d})$, hence
$$2a = (a - \sqrt{d}) + (a + \sqrt{d}) \in (p, a + \sqrt{d}),$$
But then $1 = \gcd(p, 2a) \in (p, a + \sqrt{d})$, forcing $(p, a + \sqrt{d}) = \mathcal{O}_K$ and therefore $p\mathcal{O}_K = (p, a + \sqrt{d})(p, a - \sqrt{d}) = (p, a + \sqrt{d})^2 = \mathcal{O}_K^2 = \mathcal{O}_K$, contradiction.

Note also that $(p, a + \sqrt{d}) = \mathcal{O}_K$ if and only if $(p, a - \sqrt{d}) = \mathcal{O}_K$ (and therefore both these claims are falsified as above): letting $\sigma : K \to K$ denote the Galois automorphism $\sigma(\sqrt{d}) = -\sqrt{d}$, we have that
$$1 = \alpha p + \beta(a + \sqrt{d}) \qquad \text{for some } \alpha, \beta \in \mathcal{O}_K$$
if and only if
$$1 = \sigma(1) = \sigma(\alpha)p + \sigma(\beta)(a - \sqrt{d}).$$
At this point we can check that $(p, a + \sqrt{d})$ and $(p, a - \sqrt{d})$ are in fact prime ideals. For this we use the fact that, whatever prime factorisation $p\mathcal{O}_K$ has, it satisfies
$$\sum_{j=1}^{g} e_j f_j = [K : \mathbb{Q}] = 2.$$
There's not much wriggle room here, we must be in one of the following cases:

- $g = 1$, $e_1 = 2$, $f_1 = 1$; the juxtaposition of this and $p\mathcal{O}_K = (p, a + \sqrt{d})(p, a - \sqrt{d})$ would force $(p, a + \sqrt{d}) = (p, a - \sqrt{d})$, ruled out above;
- $g = 1$, $e_1 = 1$, $f_1 = 2$; dismissed in the same way as the previous point;
- $g = 2$, $e_1 = e_2 = f_1 = f_2 = 1$, implying that both $(p, a + \sqrt{d})$ and $(p, a - \sqrt{d})$ are prime ideals (of norm p, in fact).

(b) Suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.

I claim that if $\left(\frac{d}{p}\right) = -1$, then $N(\mathfrak{p}) \neq p$. To see this, note that $x^2 - d$ has a root ($\sqrt{d}$) in $\mathcal{O}_K$, hence it has a root in $\mathcal{O}_K/\mathfrak{p}$. If it were the case that $N(\mathfrak{p}) = p$, then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$, so that $x^2 - d$ would have a root in $\mathbb{Z}/p\mathbb{Z}$, which contradicts the quadratic residue symbol assumption.

Now consider the ideal $p\mathcal{O}_K$. We have $N(p\mathcal{O}_K) = p^2$. If p is not inert in $\mathcal{O}_K$, then the factorisation of $p\mathcal{O}_K$ would contain at least one prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with norm dividing p^2 properly, in other words $N(\mathfrak{p}) = p$, contradicting the property we proved above.

□

3.1. From polynomial factorisation to prime ideal decomposition

The following result, attributed to Kummer and Dedekind, gives very detailed information about prime decompositions under some favourable conditions.

Theorem 3.3. *Let $\mathcal{O}_K$ be the ring of integers in a number field K, and let $\theta \in \mathcal{O}_K$ be such that $K = \mathbb{Q}(\theta)$. Let $h \in \mathbb{Z}[x]$ be the minimal polynomial of θ. Let p be a prime number such that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ and let $\overline{\cdot}\colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ be reduction modulo p. Factor the polynomial $\overline{h}$ into irreducible polynomials:*

$$\overline{h} = \overline{h}_1^{e_1} \dots \overline{h}_g^{e_g}, \qquad \overline{h}_j \in \mathbb{F}_p[x] \text{ distinct.}$$

Then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

where $\mathfrak{p}_j = \big(p, h_j(\theta)\big)$ is a prime ideal, $h_j \in \mathbb{Z}[x]$ is any preimage of h_j under $\overline{\cdot}$, $N(\mathfrak{p}_j) = p^{f_j}$ with $f_j = \deg(\overline{h}_j)$, and the $\mathfrak{p}_j$'s are distinct.

We'll get to the proof soon, after a few examples and some preparatory results.

Example 3.4. Consider $K = \mathbb{Q}(\sqrt{10})$. We know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$, so we may apply Theorem 3.3 with $\theta = \sqrt{10}$ and any prime p. The minimal polynomial is of course $x^2 - 10$.

Taking $p = 3$, we have

$$x^2 - 10 \equiv (x-1)(x+1) \pmod 3,$$

so we conclude that

$$3\mathcal{O}_K = (3, \sqrt{10} - 1)(3, \sqrt{10} + 1).$$

For $p = 5$ we have

$$x^2 - 10 \equiv x^2 \pmod 5,$$

so

$$5\mathcal{O}_K = (5, \sqrt{10})^2.$$

Exercise 3.5. Show that the ideals $(3, \sqrt{10}-1)$, $(3, \sqrt{10}+1)$, and $(5, \sqrt{10})$ are not principal in $\mathbb{Z}[\sqrt{10}]$.

Lemma 3.6. *Let $\mathcal{O}_K$ be the ring of integers in a number field K. Let $\theta \in \mathcal{O}_K$ with minimal polynomial $h \in \mathbb{Z}[x]$. Let p be a prime number and $\overline{h}_0$ a factor of $\overline{h}$ in $\mathbb{F}_p[x]$. Let $h_0 \in \mathbb{Z}[x]$ be any preimage of $\overline{h}_0$. Then*

$$\mathbb{Z}[x]/\big(p, h_0(x)\big) \cong \mathbb{Z}[\theta]/\big(p, h_0(\theta)\big).$$

Proof. Let φ be the composition of the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[\theta]$ (given by $x \mapsto \theta$) with the quotient morphism $\mathbb{Z}[\theta] \to \mathbb{Z}[\theta]/(p, h_0(\theta))$. Since it's the composition of two surjective maps, φ is surjective.

Any $f \in (p, h_0(x))$ maps to $(p, h_0(\theta))$ and hence so zero under φ. So it remains to show that $\ker \varphi \subseteq (p, h_0(x))$.

Let $f \in \ker\varphi$, then $f(\theta) \in (p, h_0(\theta))$, in other words there exist $a, b \in \mathbb{Z}[x]$ such that

$$f(\theta) = a(\theta)p + b(\theta)h_0(\theta).$$

With this in mind, define $F \in \mathbb{Z}[x]$ by

$$F(x) := f(x) - a(x)p - b(x)h_0(x).$$

We know that $F(\theta) = 0$, so $h \mid F$ as h is the minimal polynomial of θ. So $F(x) = h(x)c(x)$ for some $c \in \mathbb{Z}[x]$.

However, $\overline{h}_0 \mid \overline{h}$, implying that $h(x) \in (p, h_0(x))$, hence that $F(x) \in (p, h_0(x))$, and finally that $f(x) \in (p, h_0(x))$. □

The following result allows us to move certain questions about $\mathcal{O}_K$ (which may be cumbersome to compute explicitly) to the much more explicit subring $\mathbb{Z}[\theta]$.

Lemma 3.7. *Let $\mathcal{O}_K$ be the ring of integers in a number field K and let $\theta \in \mathcal{O}_K$ be such that $K = \mathbb{Q}(\theta)$. If a prime number p does not divide $[\mathcal{O}_K{:}\mathbb{Z}[\theta]]$ then*

$$\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathcal{O}_K/p\mathcal{O}_K.$$

Proof. Let φ be the composition of the inclusion $\mathbb{Z}[\theta] \to \mathcal{O}_K$ and the quotient morphism $\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$.

We claim that φ is surjective. By the assumption $p \nmid [\mathcal{O}_K{:}\mathbb{Z}[\theta]]$, we know that $\mathcal{O}_K/\mathbb{Z}[\theta]$ is a finite abelian group of order not divisible by p. Note that multiplication by p is bijective as a map from such a group to itself. So given $\alpha \in \mathcal{O}_K$, there exists $\alpha' \in \mathcal{O}_K$ such that $\alpha\mathbb{Z}[\theta] = p\alpha'\mathbb{Z}[\theta]$. Therefore $\alpha - p\alpha' \in \mathbb{Z}[\theta]$, and $\varphi(\alpha - p\alpha') = \alpha p\mathcal{O}_K$.

Now we determine $\ker\varphi$. It is clear that $p\mathbb{Z}[\theta] \subseteq \ker\varphi$. Conversely, let $\alpha \in \ker\varphi$, so $\alpha \in \mathbb{Z}[\theta] \cap p\mathcal{O}_K$. Write $\alpha = p\beta$ with $\beta \in \mathcal{O}_K$. We have $p\beta = \alpha \in \mathbb{Z}[\theta]$ so $p\beta\mathbb{Z}[\theta] = 0 \in \mathcal{O}_K/\mathbb{Z}[\theta]$. But we've seen that multiplication by p is bijective on $\mathcal{O}_K/\mathbb{Z}[\theta]$, so we must have $\beta\mathbb{Z}[\theta] = 0$, in other words $\beta \in \mathbb{Z}[\theta]$ and $\alpha = p\beta \in p\mathbb{Z}[\theta]$. □

Proof of Theorem 3.3. We break the conclusion into several parts:

(a) "$\mathfrak{p}_j$ is a prime ideal with norm p^{f_j}, where $f_j = \deg(\overline{h}_j)$."

Using Lemma 3.7 then Lemma 3.6 we have

$$\mathcal{O}_K/\mathfrak{p}_j = \mathcal{O}_K/(p, h_j(\theta)) \cong \mathbb{Z}[\theta]/(p, h_j(\theta)) \cong \mathbb{Z}[x]/(p, h_j(x)) \cong \mathbb{F}_p[x]/(\overline{h}_j(x)).$$

But we know that $\overline{h}_j \in \mathbb{F}_p[x]$ is an irreducible polynomial, so it generates a maximal ideal, therefore the quotient is a field of degree $f_j = \deg(\overline{h}_j)$, and $\mathfrak{p}_j$ is prime with the desired norm.

As a side effect we note something we'll use later in the proof:

$$[K{:}\mathbb{Q}] = n = \deg(h) = \deg(\overline{h}) = \sum_{j=1}^{g} e_j \deg(\overline{h}_j) = \sum_{j=1}^{g} e_j f_j.$$

(b) "$\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$."

We know that $\overline{h}_i$ and $\overline{h}_j$ have no common factors in $\mathbb{F}_p[x]$, therefore $1 \in (\overline{h}_i, \overline{h}_j)$ in $\mathbb{F}_p[x]$, hence $1 \in (p, h_i, h_j)$ in $\mathbb{Z}[x]$, so $1 \in (p, h_i(\theta), h_j(\theta))$ in $\mathcal{O}_K$. But

$$(p, h_i(\theta), h_j(\theta)) \subseteq (p, h_i(\theta)) + (p, h_j(\theta)) = \mathfrak{p}_i + \mathfrak{p}_j,$$

so $1 \in \mathfrak{p}_i + \mathfrak{p}_j$, therefore $\mathfrak{p}_i \neq \mathfrak{p}_j$.

(c) "$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_g^{e_g}$."

Note that in any commutative ring $(a,b)(a,c) = (a^2, ab, ac, bc) \subseteq (a, bc)$. So

$$\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_g^{e_g} = (p, h_1(\theta))^{e_1}\dots(p, h_g(\theta))^{e_g} \subseteq (p, h_1(\theta)^{e_1}\dots h_g(\theta)^{e_g}) = (p, h(\theta)) = p\mathcal{O}_K.$$

Therefore $\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_g^{e_g} = (p\mathcal{O}_K)J$ for some ideal J. This forces

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1'}\dots\mathfrak{p}_g^{e_g'}$$

for some e_j' with $0 \le e_j' \le e_j$ for all j and $\sum e_j' f_j = n = \sum e_j f_j$. We conclude that $e_j' = e_j$ for all j.

□

The condition $p \nmid [\mathcal{O}_K{:}\mathbb{Z}[\theta]]$ in Theorem 3.3 invites some comments:

(a) This holds for any prime p in the case where $\mathcal{O}_K = \mathbb{Z}[\theta]$.

(b) This holds for any prime p such that $p^2 \nmid \Delta(1, \theta, \dots, \theta^{n-1})$, since as we have seen

$$\Delta(1, \theta, \dots, \theta^{n-1}) = [\mathcal{O}_K{:}\mathbb{Z}[\theta]]^2 \Delta_K.$$

(c) The condition also holds in case the minimal polynomial h of θ is *Eisenstein* at p, that is p divides all the coefficients of h except for the leading one, and p^2 does not divide the constant coefficient.

(d) It is sometimes possible, given p, to tweak the initial choice of θ so that p does not divide the index. For instance, consider $K = \mathbb{Q}(\alpha)$, where α has minimal polynomial $x^3 + 2x + 22$. Using the formula you are proving in Assignment 1, we see that

$$\Delta(1, \alpha, \alpha^2) = -2^2 \cdot 5^2 \cdot 131.$$

The only primes p such that $p^2 \mid \Delta(1, \alpha, \alpha^2)$ are 2 and 5. The polynomial $x^3 + 2x + 22$ is Eisenstein at 2, so that's sorted.

For $p = 5$ we need to do something else. Let $\theta = \frac{1}{5}(\alpha^2 + \alpha - 2)$. Clearly $\theta \notin \mathbb{Q}$ (otherwise α would satisfy a polynomial equation of degree 2 over $\mathbb{Q}$), so $\mathbb{Q} \subsetneq \mathbb{Q}(\theta) \subseteq K$. Since $[K{:}\mathbb{Q}] = 3$, we must have $[K{:}\mathbb{Q}(\theta)] = 1$ so $K = \mathbb{Q}(\theta)$. You may have doubts that θ is an algebraic integer, but we can compute its minimal polynomial: $x^3 + 2x^2 + 4x - 2$, so that $\theta \in \mathcal{O}_K$. Finally, $\Delta(1, \theta, \theta^2) = -2^2 \cdot 131$, so we can use Theorem 3.3 with θ to deal with $p = 5$:

$$5\mathcal{O}_K = (5, \theta - 1)(5, \theta - 3)(5, \theta - 4).$$

Incidentally, had we tried to apply Theorem 3.3 with α for $p = 5$ we would have gotten an incorrect answer:

$$5\mathcal{O}_K = (5, \alpha - 1)^2(5, \alpha - 3).$$

(e) Unfortunately, the method used in the previous part is not always successful: there exist primes p and rings of integers $\mathcal{O}_K$ such that $p \mid [\mathcal{O}_K{:}\mathbb{Z}[\theta]]$ for all $\theta \in \mathcal{O}_K$.

Corollary 3.8. *Suppose the minimal polynomial h of θ is Eisenstein at p. Then p is totally ramified in $\mathcal{O}_K$.*

Theorem 3.3 and, more generally, the explicit factorisation into prime ideals, can be applied to the computation of the ideal class group, which in turn can be used for solving equations in integers. This is based on the Minkowski method and the fact that every ideal class contains an ideal of norm less than

$$B_K = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\omega_j)|,$$

where $\omega_1, \dots, \omega_n$ is an integral basis of $\mathcal{O}_K$. (Note that B_K depends on this choice of basis.)

The idea is that the list of all nonzero ideals of $\mathcal{O}_K$ of norm less than B_K contains a set of representatives of the ideal classes, and smaller norm translates into something easier to compute with. More precisely, suppose I is an ideal of norm less than B_K. This ideal has a factorisation into prime ideals:

$$I = \mathfrak{p}_1 \dots \mathfrak{p}_r, \qquad \mathfrak{p}_j \text{ prime ideal of } \mathcal{O}_K.$$

Given $\mathfrak{p}_j$ in the above factorisation, there exists a unique prime number p such that $p \in \mathfrak{p}_j$, which implies that we can find $\mathfrak{p}_j$ in the factorisation of $p\mathcal{O}_K$ into prime ideals. In particular, $N(\mathfrak{p}_j)$ is a power of p.

On the other hand, $N(\mathfrak{p}_j)$ divides $N(I)$, which is less than B_K. It follows that $N(\mathfrak{p}_j)$ is less than B_K, and therefore p is less than B_K.

The conclusion is that we can discover all the possible candidates for prime ideals appearing in the factorisation of the ideal I by looking at the factorisation of the principal ideals $p\mathcal{O}_K$ for all primes p up to the bound B_K. Once all possible prime ideal factors are found, we find all ideals I by taking products that remain under the norm bound B_K.

Let's observe this strategy in action in two simple examples.

Example 3.9. Consider $K = \mathbb{Q}(\sqrt{2})$. The integral basis $\{1, \sqrt{2}\}$ gives the bound

$$B_K = (1+\sqrt{2})^2 \cong 5.8,$$

so we are looking at the prime numbers less than 5.8. We can apply Theorem 3.3 with $\theta = \sqrt{2}$ and any p, and it tells us that 3 and 5 are inert in $\mathcal{O}_K$; they have norms 9 and 25, both bigger than 5.8, so we may safely ignore them.

As for $p = 2$, we have $2\mathcal{O}_K = (\sqrt{2}\mathcal{O}_K)^2$. We conclude that the only nonzero ideals of norm less than 5.8 are $\mathcal{O}_K$, $\sqrt{2}\mathcal{O}_K$, and $2\mathcal{O}_K$. They are all principal, so we conclude that every ideal class contains a principal ideal, therefore every ideal class is trivial in the ideal class group. In other words, $\mathrm{Cl}(\mathcal{O}_K) = 1$ and $\mathcal{O}_K$ is a PID.

Example 3.10. Consider $K = \mathbb{Q}(\sqrt{-5})$. The integral basis $\{1, \sqrt{-5}\}$ gives the bound

$$B_K = (1+\sqrt{5})^2 \approx 10.5,$$

so we are looking at the prime numbers less than 10.5.

We summarise the results of the application of Theorem 3.3 with $\theta = \sqrt{-5}$ and $p = 2, 3, 5, 7$:

p	$p\mathcal{O}_K$	short names
2	$(2, 1+\sqrt{-5})^2$	$\mathfrak{p}_2^2$
3	$(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	$(\sqrt{-5}\mathcal{O}_K)^2$	$\mathfrak{p}_5^2$
7	$(7, 1+\sqrt{-5})(7, 1-\sqrt{-5})$	$\mathfrak{p}_7\mathfrak{p}_7'$

I leave it as an exercise to check that there are no elements of norm ±2, ±3, or ±7 in $\mathcal{O}_K$, and therefore that the prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_7$, and $\mathfrak{p}_7'$ are not principal.

It is then clear that $[\mathfrak{p}_2]$ has order 2 as an element of the ideal class group. We can relate the classes of the other prime ideals listed above to $[\mathfrak{p}_2]$ in the following way: $N(1+\sqrt{-5}) = 6$ so we conclude that $(1+\sqrt{-5})\mathcal{O}_K$ is either $\mathfrak{p}_2\mathfrak{p}_3$ or $\mathfrak{p}_2\mathfrak{p}_3'$. It turns out to be the former. Therefore $[\mathfrak{p}_2][\mathfrak{p}_3] = 1$, but $[\mathfrak{p}_2]$ has order 2 so $[\mathfrak{p}_3] = [\mathfrak{p}_2]$. Similar endeavours yield $[\mathfrak{p}_3'] = [\mathfrak{p}_7] = [\mathfrak{p}_7'] = [\mathfrak{p}_2]$.

The conclusion is that every ideal class of $\mathcal{O}_K$ has a representative whose class is some power of $[\mathfrak{p}_2]$, so that $\mathrm{Cl}(\mathcal{O}_K)$ is a group of order 2.

Example 3.11. Let's solve the equation $y^2 = x^3 - 5$ in integers.

We start with two elementary observations:

- x is odd; otherwise y is odd and $y^2 \equiv -1 \pmod 4$, impossible.
- $\gcd(x,y) = 1$; since $5 = x^3 - y^2$ the only other possible divisor would be 5, but then y^2 is divisible by 25 and $x^3 - 5$ is divisible by 5, impossible.

With this out of the way, it is time to factor over $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$:

$$\big(y+\sqrt{-5}\big)\big(y-\sqrt{-5}\big) = x^3.$$

Suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ that divides both $(y+\sqrt{-5})\mathcal{O}_K$ and $(y-\sqrt{-5})\mathcal{O}_K$. Then $\mathfrak{p}$ divides $x^3\mathcal{O}_K$, hence divides $x\mathcal{O}_K$, and since x is odd, does not divide $2\mathcal{O}_K$. Also $2y \in (y+\sqrt{-5})\mathcal{O}_K + (y-\sqrt{-5})\mathcal{O}_K$, so $\mathfrak{p}$ divides $2y\mathcal{O}_K$, hence divides $y\mathcal{O}_K$. However, $\gcd(x,y) = 1$, so we have reached a contradiction.

Therefore the ideals $(y+\sqrt{-5})\mathcal{O}_K$ and $(y-\sqrt{-5})\mathcal{O}_K$ have no common prime ideal factors. Taking the prime ideal factorisation of $x^3\mathcal{O}_K = (x\mathcal{O}_K)^3$ into account, we must have that

$$(y+\sqrt{-5})\mathcal{O}_K = I^3, \qquad (y-\sqrt{-5})\mathcal{O}_K = J^3,$$

for some ideals I and J of $\mathcal{O}_K$.

Changing perspective to the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ now, we have $[I]^3 = [J]^3 = 1$, but the group has order 2 by Example 3.10, forcing $[I] = [J] = 1$. Moreover, a quick norm computation tells us that the only units in $\mathcal{O}_K$ are ±1, both cubes in $\mathcal{O}_K$, therefore

$$y+\sqrt{-5} = (a+b\sqrt{-5})^3$$

for some $a, b \in \mathbb{Z}$. Expanding the cube and comparing multiples of $\sqrt{-5}$ on both sides we conclude that $1 = b(3a^2 - 5b^2)$, which is impossible to solve in integers.

Therefore the equation $y^2 = x^3 - 5$ has no integer solutions.

3.2. Cyclotomic fields

It's high time we met our second explicit family of number fields (the first being the quadratic fields).

Fix $m \geq 3$ and let $\zeta = e^{2\pi i/m}$. We call any root of $x^m - 1$ an m-th root of unity; clearly ζ is an m-root of unity. We call $\mathbb{Q}(\zeta)$ a *cyclotomic field*.

Let $\Phi \in \mathbb{Z}[x]$ denote the minimal polynomial of ζ over $\mathbb{Q}$. It is a divisor of $x^m - 1$. So if ξ is a conjugate of ζ (that is, another root of Φ), then ξ is also an m-th root of unity. Moreover, ξ is not an n-th root of unity for any $n < m$. (If that were the case then Φ would divide $x^n - 1$, contradicting the fact that $\zeta^n = e^{2\pi i n/m} \neq 1$.) Therefore we have an inclusion

$$\{\text{conjugates of } \zeta\} \subseteq \{\zeta^k \mid k \in S\}.$$

where we define

$$S = \{k \in \mathbb{Z} \mid 1 \leq k \leq m, \gcd(k, m) = 1\}.$$

We prove that this is actually an equality:

Proposition 3.12. *For any $k \in S$, we have that ζ^k is a conjugate of ζ.*

> **Exercise 3.13.** Suppose $h \in \mathbb{Z}[x]$ is monic and $h = fg$ with $f, g \in \mathbb{Q}[x]$ monic. Then $f, g \in \mathbb{Z}[x]$.

Proof of Proposition 3.12. We will prove that if $\xi = \zeta^k$ with $k \in S$ and p is a prime not dividing m, then ξ^p is a conjugate of ξ. The claim in the Proposition will then follow by repeated application of this principle with p running through the prime decomposition of k.

Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of ξ over $\mathbb{Q}$. Since $\xi^m - 1 = 0$, we have $x^m - 1 = f(x)g(x)$ for some $g \in \mathbb{Q}[x]$. But Exercise 3.13 tells us that $g \in \mathbb{Z}[x]$.

We move on to considering ξ^p now. It also is a root of $x^m - 1 = f(x)g(x)$; we are trying to show that it is a root of f, so let's assume it's a root of g, that is $g(\xi^p) = 0$. We interpret this as saying that ξ is a root of the polynomial $g(x^p)$, therefore the minimal polynomial f of ξ divides $g(x^p)$ in $\mathbb{Q}[x]$, therefore in $\mathbb{Z}[x]$ by another application of Exercise 3.13. Reducing modulo p, $\overline{g}(x)^p = \overline{g}(x^p)$ is divisible by $\overline{f}(x)$ in $\mathbb{F}_p[x]$. Let $\overline{h} \in \mathbb{F}_p[x]$ be an irreducible polynomial such that $\overline{h}(x) \mid \overline{f}(x)$, then $\overline{h}^2 \mid f(x)g(x) = x^m - 1$. Therefore $\overline{h}$ divides the derivative of $x^m - 1$, which is $\overline{m}x^{m-1}$, forcing $\overline{h}(x)$ to be a scalar multiple of a power of x. However, this contradicts the fact that $\overline{h}(x)$ divides $x^m - 1$.

So the assumption that ξ^p is a root of g leads to a contradiction, which implies that ξ^p is a root of f, in other words it is a conjugate of ξ. □

Corollary 3.14. *The cyclotomic field $\mathbb{Q}(\zeta)$ has degree $\varphi(m)$ over $\mathbb{Q}$, and its Galois group is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. By Proposition 3.12 we know that ζ has $\varphi(m)$ conjugates, so that is the degree.

For the statement about the Galois group G of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, note that an element $\sigma \in G$ is uniquely determined by $\sigma(\zeta)$, which can be any ζ^k for $k \in S$, which gives us a bijection between G and $(\mathbb{Z}/m\mathbb{Z})^\times$.

If $\sigma, \tau \in G$ are given by $\sigma(\zeta) = \zeta^k$ and $\tau(\zeta) = \zeta^\ell$, then $\tau \circ \sigma$ is given by

$$(\tau \circ \sigma)(\zeta) = \tau(\sigma(\zeta)) = \tau(\zeta^k) = \tau(\zeta)^k = (\zeta^\ell)^k = \zeta^{\ell k},$$

in other words the map from G to $(\mathbb{Z}/m\mathbb{Z})^\times$ is a group homomorphism. □

Recall (?) that the *Euler phi function* φ is defined as

$$\varphi(m) = \#S = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

It is a multiplicative arithmetic function: $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m, n) = 1$, and

$$\varphi(p^r) = (p-1)p^{r-1}.$$

For any $m \in \mathbb{N}$, let

$$\mu_m = \langle \zeta_m \rangle = \{\omega \in \mathbb{C} \mid \omega^m = 1\}$$

be the group of m-th roots of unity, and let

$$\mu_\infty = \bigcup_{m=1}^{\infty} \mu_m$$

be the group of all roots of unity.

Proposition 3.15. *Given $m \geq 3$, let $\zeta = e^{2\pi i/m}$.*

(a) If m is even, $\mathbb{Q}(\zeta_m) \cap \mu_\infty = \mu_m$.

(b) If m is odd, $\mathbb{Q}(\zeta_m) \cap \mu_\infty = \mu_{2m}$.

Proof. We start by remarking that if m is odd, then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$, since

$$\big(- \zeta_{2m}\big)^m = -e^{2\pi i m/2m} = -(-1) = 1.$$

Therefore it suffices to prove part (a) of the Corollary. Suppose m is even and let $\theta \in \mathbb{Q}(\zeta)$ be a primitive k-th root of unity for some k, so that $\mu_k = \langle \theta \rangle$. Then $\zeta\theta$ is a primitive ℓ-th root of unity with $\ell = \operatorname{lcm}(m,k)$, hence $\mathbb{Q}(\zeta\theta) \subseteq \mathbb{Q}(\zeta)$ and $\varphi(\ell) \leq \varphi(m)$. The latter forces $\ell = m$, in other words $k \mid m$ so $\theta \in \mu_m$. □

Corollary 3.16. *The m-th cyclotomic fields for m even are all pairwise non-isomorphic.*

For any algebraic number α of degree n, set

$$\Delta(\alpha) := \Delta(1, \alpha, \dots, \alpha^{n-1}).$$

Lemma 3.17. *Let $m \geq 3$ and let $\zeta = e^{2\pi i/m}$. Then*

$$\Delta(\zeta) = \Delta(1-\zeta).$$

Proof. For any embedding $\sigma_j\colon \mathbb{Q}(\zeta) \to \mathbb{C}$ we have $\sigma_j(1-\zeta) = 1 - \sigma_j(\zeta)$, so that

$$\Delta(\zeta) = \prod_{i<j} \big(\sigma_i(\zeta) - \sigma_j(\zeta)\big) = \prod_{i<j} \big((1-\sigma_i(\zeta)) - (1-\sigma_j(\zeta))\big) = \prod_{i<j} \big(\sigma_i(1-\zeta) - \sigma_j(1-\zeta)\big) = \Delta(1-\zeta).$$

□

Recall the notation

$$S = \{k \in \mathbb{Z} \mid 1 \leq k \leq m, \gcd(k,m) = 1\}.$$

Lemma 3.18. *Let $\zeta = e^{2\pi i/p^r}$ with p prime and $r \in \mathbb{N}$. Then*

$$\prod_{k \in S} \big(1 - \zeta^k\big) = p.$$

In particular,

$$\frac{p}{(1-\zeta)^{\#S}} \in \mathbb{Z}[\zeta].$$

Proof. For $k \in S$, ζ^k is a root of $x^{p^r} - 1$, but not of $x^{p^{r-1}} - 1$, therefore it is a root of

$$f(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \sum_{j=0}^{p-1} x^{jp^{r-1}}.$$

Note also that $\#S = \varphi(p^r) = (p-1)p^{r-1} = \deg(f)$, so in fact these are all the complex roots of f, so that

$$f(x) = \prod_{k \in S} \left(x - \zeta^k\right).$$

Now we use $f(1) = p$.

The last statement follows since we have in $\mathbb{Z}[\zeta]$:

$$1 - \zeta^k = (1-\zeta)(1 + \zeta + \zeta^2 + \cdots + \zeta^{k-1}).$$

□

Corollary 3.19. *The polynomial $f \in \mathbb{Z}[x]$ defined in the proof of Lemma 3.18 is the minimal polynomial of ζ over $\mathbb{Q}$ (and, in particular, irreducible).*

Proof. We know that ζ is a root of f (as $1 \in S$), so the minimal polynomial h of ζ divides f. But $\deg(h) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p^r) = \deg(f)$, so we conclude that $h = f$. □

Another way to see that f is irreducible is by looking at $f(x+1)$ modulo p:

$$f(x+1) = \frac{(x+1)^{p^r} - 1}{(x+1)^{p^{r-1}} - 1} \equiv \frac{\left(x^{p^r} + 1\right) - 1}{\left(x^{p^{r-1}} + 1\right) - 1} = x^{\varphi(p^r)} \pmod{p},$$

so $f(x+1)$ has all but the leading coefficient divisible by p. On the other hand, $f(0+1) = p$ so the constant coefficient of $f(x+1)$ is not divisible by p^2. Therefore $f(x+1)$ is Eisenstein at p, and so it is irreducible, hence f itself is irreducible.

Lemma 3.20. *Let $\zeta = e^{2\pi i/m}$ and let $K = \mathbb{Q}(\zeta)$. Then $\Delta(\zeta) \mid m^{\varphi(m)}$.*

Proof. Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of ζ over $\mathbb{Q}$. Write $x^m - 1 = f(x)g(x)$ with $g \in \mathbb{Z}[x]$. Differentiate:

$$mx^{m-1} = f'(x)g(x) + f(x)g'(x)$$

and set $x = \zeta$ to get

$$m\zeta^{m-1} = f'(\zeta)g(\zeta) \qquad \Rightarrow \qquad m = \zeta f'(\zeta)g(\zeta).$$

Now we take the norm from K to $\mathbb{Q}$:

$$m^{\varphi(m)} = N(m) = N(f'(\zeta))N(\zeta g(\zeta)) = \pm\Delta(\zeta)N(\zeta g(\zeta)).$$

Since ζ, and therefore also $\zeta g(\zeta)$, are algebraic integers, we conclude that $\Delta(\zeta) \mid m^{\varphi(m)}$. □

Exercise 3.21. Consider the case $m = p$ a prime number and show that $\Delta(\zeta) = \pm p^{p-2}$.

Theorem 3.22. *Let $\zeta = e^{2\pi i/p^r}$ with p prime and $r \in \mathbb{N}$. Let $K = \mathbb{Q}(\zeta)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Proof. Let $n = \varphi(p^r)$. We start by noting that $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$, so that it suffices to prove that $\mathcal{O}_K = \mathbb{Z}[1-\zeta]$. Also $1, 1-\zeta, \dots, (1-\zeta)^{n-1} \in \mathcal{O}_K$ is a $\mathbb{Q}$-basis for K. By Proposition 2.34 any element $\alpha \in \mathcal{O}_K$ can be written in the form

$$\alpha = \frac{c_0 + c_1(1-\zeta) + \dots + c_{n-1}(1-\zeta)^{n-1}}{\Delta(1-\zeta)}.$$

By Lemmas 3.17 and 3.20 we know that the denominator of this expression is a power of p.

Suppose that $\mathcal{O}_K \neq \mathbb{Z}[1-\zeta]$, then there exists $\theta \in \mathcal{O}_K$ of the form

$$\theta = \frac{c_{j_1}(1-\zeta)^{j_1} + \dots + c_{j_s}(1-\zeta)^{j_s}}{p}$$

where $\{j_1 < \dots < j_s\} \subseteq \{0, \dots, n-1\}$ and c_{j_i} is not divisible by p for all i.

By Lemma 3.18 we know that $\frac{p}{(1-\zeta)^n} \in \mathbb{Z}[\zeta]$, so $\frac{p}{(1-\zeta)^{j_1+1}} \in \mathbb{Z}[\zeta]$ and $\theta \frac{p}{(1-\zeta)^{j_1+1}} \in \mathcal{O}_K$:

$$\theta \frac{p}{(1-\zeta)^{j_1+1}} = \frac{c_{j_1}}{1-\zeta} + c_{j_2}(1-\zeta)^{j_2-j_1-1} + \dots + c_{j_s}(1-\zeta)^{j_s-j_1-1}.$$

Most of the right hand side is in $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$, and the left hand side is in $\mathcal{O}_K$, so we conclude that $\frac{c_{j_1}}{1-\zeta} \in \mathcal{O}_K$. This means that $p = N(1-\zeta) \mid N(c_{j_1}) = c_{j_1}^n$, so $p \mid c_{j_1}$, contradiction. □

3.3. Quadratic Reciprocity, take one

Let $\zeta = e^{2\pi i/p}$ with p an odd prime, and let $K = \mathbb{Q}(\zeta)$. We have seen that $K/\mathbb{Q}$ is a Galois extension with Galois group G isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Therefore G has a unique subgroup of every order dividing $p-1$. In particular, by the Galois correspondence there is a unique subfield L of K of degree 2 over $\mathbb{Q}$. We will determine this subfield explicitly via a very concrete method, which will also lead us to a proof of the Law of Quadratic Reciprocity.

Consider the following expression, an example of a *Gauss sum*:

$$g = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \zeta^t \in \mathbb{Z}[\zeta].$$

Theorem 3.23. *The cyclotomic integer g satisfies the relation*

$$g^2 = p^* := (-1)^{(p-1)/2} p.$$

Therefore the unique quadratic subfield of $\mathbb{Q}(\zeta)$ is $\mathbb{Q}(\sqrt{p^*})$.

Before jumping into this, let's look at some basic properties of the quadratic residue symbol.

Lemma 3.24. *Let p be an odd prime number and $a, b \in \mathbb{Z}$.*

*(a) (*Euler's criterion*) $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.*

(b) (multiplicativity) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. The claims are trivially true if a or b is zero modulo p.

Suppose now that $a, b \not\equiv 0 \pmod{p}$.

(a) Using Fermat's Little Theorem we see that

$$\left(a^{(p-1)/2}-1\right)\left(a^{(p-1)/2}+1\right)=a^{p-1}-1\equiv 0 \pmod{p}.$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field we conclude that $a^{(p-1)/2}\equiv \pm 1 \pmod{p}$.

I claim that $x^2\equiv a \pmod{p}$ is solvable if and only if $a^{(p-1)/2}\equiv 1 \pmod{p}$. For this we use the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic; let k be a generator (also known as a *primitive root* modulo p). Write $a\equiv k^b \pmod{p}$, $x\equiv k^y \pmod{p}$, then we are considering the solvability of $k^{2y}\equiv k^b \pmod{p}$, which is equivalent to the solvability of $2y\equiv b \pmod{p-1}$.

On one hand, if this congruence is solvable then $b=2c$ for some $c\in\mathbb{N}$ (since both $2y$ and $p-1$ are even), so that $a^{(p-1)/2}\equiv \left(k^c\right)^{p-1}\equiv 1 \pmod{p}$.

On the other hand, if $k^{b(p-1)/2}\equiv a^{(p-1)/2}\equiv 1 \pmod{p}$, then $p-1$ divides $b(p-1)/2$, so that $2|b$, in which case $2y\equiv b \pmod{p-1}$ is clearly solvable.

(b) We use the previous part:

$$\left(\frac{ab}{p}\right)\equiv (ab)^{(p-1)/2}=a^{(p-1)/2}b^{(p-1)/2}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Since both quantities are ±1 and $p>2$ we conclude that the quantities are equal.

□

Lemma 3.25. *Given $n\in\mathbb{Z}$, we have*

$$\sum_{t\in\mathbb{Z}/p\mathbb{Z}}\zeta^{nt}=\begin{cases}0 & \text{if } n\not\equiv 0 \pmod{p}\\ p & \text{if } n\equiv 0 \pmod{p}.\end{cases}$$

Proof. If $n\equiv 0 \pmod{p}$ then $\zeta^n=1$ and the claim follows.

Otherwise, $\zeta^n\neq 1$ and

$$\sum_{t\in\mathbb{Z}/p\mathbb{Z}}\zeta^{nt}=\frac{\zeta^{np}-1}{\zeta^n-1}=\frac{0}{\zeta^n-1}=0.$$

□

Proof of Theorem 3.23. We place the Gauss sum g into a family by setting, for any $a\in\mathbb{Z}/p\mathbb{Z}$:

$$g_a=\sum t\in(\mathbb{Z}/p\mathbb{Z})^\times\left(\frac{t}{p}\right)\zeta^{at}.$$

Clearly $g_1=g$. I claim that

$$g_a=\left(\frac{a}{p}\right)g.$$

To see that $g_0=0$, note that g_0 is the sum of the quadratic residue symbol over all nonzero elements mod p, but half of these contribute $+1$ and the other half contribute -1.

For the remaining case $a\neq 0$, multiplication by a is a bijective map from $(\mathbb{Z}/p\mathbb{Z})^\times$ to itself, which allows us to reindex the sum:

$$\left(\frac{a}{p}\right)g_a=\sum_{t\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{at}{p}\right)\zeta^{at}=\sum_{s\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{s}{p}\right)\zeta^{s}=g.$$

Consider the sum

$$S=\sum_{a\in\mathbb{Z}/p\mathbb{Z}}g_a g_{-a}.$$

We will compute this sum in two different ways.

First, we have

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \begin{cases} 0 & \text{if } a = 0 \\ \left(\frac{-1}{p}\right) g^2 & \text{if } a \neq 0. \end{cases}$$

Summing over a we get

$$S = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{-1}{p}\right) g^2 = (p-1)\left(\frac{-1}{p}\right) g^2.$$

The other evaluation goes via

$$g_a g_{-a} = \sum_{x,y \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{xy}{p}\right) \zeta^{a(x-y)},$$

and summing over a we get

$$S = \sum_{x,y \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{xy}{p}\right) \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \zeta^{a(x-y)} = p(p-1),$$

where we used Lemma 3.25 to see that only the summands with $x = y$ are nonzero.

We conclude that

$$p(p-1) = S = (p-1)\left(\frac{-1}{p}\right) g^2.$$

□

Theorem 3.26 (Law of Quadratic Reciprocity)**.** *Let $p \neq q$ be odd prime numbers. Then*

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Proof. Consider the family of Gauss sums with $a \in \mathbb{Z}/p\mathbb{Z}$:

$$g_a = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \zeta^{at} \in \mathbb{Z}[\zeta].$$

Raise $g = g_1$ to the q-th power:

$$g^q \equiv \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \zeta^{tq} = g_q = \left(\frac{q}{p}\right) g \pmod{q\mathbb{Z}[\zeta]}.$$

Multiply both sides by g:

$$g^{q+1} \equiv \left(\frac{q}{p}\right) g^2 \pmod{q\mathbb{Z}[\zeta]} \qquad \Rightarrow \qquad \left(p^*\right)^{(q-1)/2} p^* \equiv \left(\frac{q}{p}\right) p^* \pmod{q},$$

where we notice that the last congruence only involves integers. We can cancel out the common p^* factor as $p \neq q$:

$$\left(p^*\right)^{(q-1)/2} \equiv \left(\frac{q}{p}\right) \pmod{q}.$$

Finally, we use Euler's criterion. □

3.4. Extensions of number fields, and the Galois advantage

So far we have been studying properties of finite extensions $K/\mathbb{Q}$ where the base field is the rational numbers. It is useful to generalise this slightly to finite extensions L/K where both L and K are number fields. Much of what we have discovered to this point extends to this setting, albeit with more intricate proofs. In particular, we have the following

Theorem 3.27. *Let L/K be a finite extension of number fields and let $n = [L{:}K]$. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then there is a unique factorisation*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g},$$

where the $\mathfrak{q}_j$'s are the distinct prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$, $e_j \in \mathbb{Z}_{\geq 1}$, and the uniqueness is up to permutation of the factors. Moreover, letting $f_j = [\mathcal{O}_L/\mathfrak{q}_j{:}\mathcal{O}_K/\mathfrak{p}]$, we have

$$\sum_{j=1}^{g} e_j f_j = n.$$

We will not prove this (see [2, Theorem 4.27] for a proof), but parts of the statement could do with some clarification.

If $\mathfrak{p}$ is a nonzero prime ideal of a ring of integers $\mathcal{O}_K$, we call the quotient $\mathcal{O}_K/\mathfrak{p}$ the *residue field* of $\mathfrak{p}$. We know that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for a prime number p, and that $\mathcal{O}_K/\mathfrak{p}$ is a finite extension of $\mathbb{F}_p$. These facts generalise to our setting as follows: a nonzero prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ *lies over* $\mathfrak{p}$ if $\mathfrak{q}$ contains $\mathfrak{p}\mathcal{O}_L$, the ideal of $\mathcal{O}_L$ generated by $\mathfrak{p}$.

Proposition 3.28. *Suppose L/K is a finite extension of number fields and $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$.*

(a) A nonzero prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ lies over $\mathfrak{p}$ if and only if $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

(b) $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$.

(c) If $\mathfrak{q}$ lies over $\mathfrak{p}$ then the residue field $\mathcal{O}_L/\mathfrak{q}$ is a finite extension of the residue field $\mathcal{O}_K/\mathfrak{p}$.

Proof.

(a) One direction is clear: if $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$ then $\mathfrak{p} \subseteq \mathfrak{q}$ so $\mathfrak{q}$ lies over $\mathfrak{p}$.

Conversely, suppose $\mathfrak{p} \subseteq \mathfrak{q}$. Then $\mathfrak{q} \cap \mathcal{O}_K$ is a prime ideal containing $\mathfrak{p}$, but $\mathfrak{p}$ is maximal, so we must have $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

(b) Let $\alpha \in \mathcal{O}_K$ have $\mathfrak{p}$-valuation 1, that is $\alpha \in \mathfrak{p}$ but $\alpha \notin \mathfrak{p}^2$. Then $\alpha\mathcal{O}_K = \mathfrak{p}I$, where I is an ideal that does not contain $\mathfrak{p}$. By the maximality of $\mathfrak{p}$, this means that $\mathfrak{p}$ and I are coprime ideals in $\mathcal{O}_K$, so there exist $a \in \mathfrak{p}$ and $b \in I$ such that $a + b = 1$.

Suppose now that $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, then $b\mathcal{O}_L = b\mathfrak{p}\mathcal{O}_L \subseteq \alpha\mathcal{O}_L$, so that $b = \alpha c$ for some $c \in \mathcal{O}_L$. We have $c = \frac{b}{\alpha} \in K$, so $c \in \mathcal{O}_K$ and $b \in \alpha\mathcal{O}_K \subseteq \mathfrak{p}$, implying that $1 = a + b \in \mathfrak{p}$, contradiction.

(c) Consider the composition of the inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ and the quotient map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q}$. The kernel of this composition is $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$ (by part (a)), so we get an injective map $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q}$.

For the finite-dimensionality, let $p\mathbb{Z} = \mathfrak{q} \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, then we know that both $\#(\mathcal{O}_K/\mathfrak{p}) = N(\mathfrak{p})$ and $\#(\mathcal{O}_L/\mathfrak{q}) = N(\mathfrak{q})$ are powers of p.

□

Now we introduce the additional assumption that L is a Galois extension of K. This drastically simplifies the picture:

Proposition 3.29. *Let L/K be a finite Galois extension of number fields with Galois group G and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Let $n = [L{:}K]$.*

(a) G acts transitively on the set of prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$.

(b) In the context of the prime ideal decomposition of $\mathfrak{p}\mathcal{O}_L$, all the e_j's are equal to a common value e, all the f_j are equal to a common value f, and

$$efg = n.$$

Proof.

(a) By definition of the Galois group, G acts on elements of L: $\sigma \cdot \alpha = \sigma(\alpha)$. It is clear that any $\sigma \in G$, being a field automorphism of L that fixes K pointwise, restricts to a ring automorphism of $\mathcal{O}_L$ that fixes $\mathcal{O}_K$ pointwise. In particular, σ takes prime ideals of $\mathcal{O}_L$ to prime ideals of $\mathcal{O}_L$. Also, if $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{q}$, then $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) \subseteq \sigma(\mathfrak{q})$, so σ takes prime ideals lying over $\mathfrak{p}$ to prime ideals lying over $\mathfrak{p}$.

For the transitivity, suppose $\mathfrak{q}_1 \neq \mathfrak{q}_2$ are prime ideals lying over $\mathfrak{p}$ and $\sigma(\mathfrak{q}_1) \neq \mathfrak{q}_2$ for all $\sigma \in G$. Then $\mathfrak{q}_2 \subsetneq \sigma(\mathfrak{q}_1) + \mathfrak{q}_2$ and the latter is forces to be $\mathcal{O}_L$ by the maximality of $\mathfrak{q}_2$. In other words, $\sigma(\mathfrak{q}_1)$ and $\mathfrak{q}_2$ are coprime ideals for all $\sigma \in G$. Similarly, $\sigma(\mathfrak{q}_1)$ and $\tau(\mathfrak{q}_1)$ are either equal or coprime for any $\sigma, \tau \in G$. We can therefore apply the Chinese Remainder Theorem to find a solution $\alpha \in \mathcal{O}_L$ to the simultaneous congruences

$$\begin{aligned} \alpha &\equiv 0 \pmod{\mathfrak{q}_2} \\ \alpha &\equiv 1 \pmod{\sigma(\mathfrak{q}_1)} \qquad \text{for all } \sigma \in G. \end{aligned}$$

Consider the element

$$a := N_K^L(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

We have that $a \in \mathfrak{q}_2 \cap \mathcal{O}_K = \mathfrak{p}$. However $\alpha \notin \sigma^{-1}(\mathfrak{q}_1)$, hence $\sigma(\alpha) \notin \mathfrak{q}_1$ for all $\sigma \in G$. Since $\mathfrak{q}_1$ is a prime ideal, this implies that $a \notin \mathfrak{q}_1$, hence $a \notin \mathfrak{q}_1 \cap \mathcal{O}_K = \mathfrak{p}$, contradiction.

(b) Fix $i \neq j$. By the previous part, there exists $\sigma \in G$ such that $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$. Compare now the two factorisations

$$\begin{aligned} \mathfrak{p}\mathcal{O}_L &= \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g} \\ \mathfrak{p}\mathcal{O}_L &= \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{q}_1)^{e_1} \dots \sigma(\mathfrak{q}_g)^{e_g}. \end{aligned}$$

By uniqueness, the exponents e_i of $\sigma(\mathfrak{q}_i)$ and e_j of $\sigma(\mathfrak{q}_j)$ must be equal.

For the residue degrees, note that σ gives a ring isomorphism $\sigma{:}\,\mathcal{O}_L \to \mathcal{O}_L$ inducing a ring isomorphism $\sigma{:}\,\mathcal{O}_L/\mathfrak{q}_i \to \mathcal{O}_L/\sigma(\mathfrak{q}_i)$. In particular the cardinalities of these two residue fields are equal.

□

Given a prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$, we consider its *decomposition group*, defined as the stabiliser of $\mathfrak{q}$ with respect to the Galois action:

$$D_{\mathfrak{q}} = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

This is a subgroup of G of order $n/g = ef$.

We also consider the *inertia group*, defined by

$$I_{\mathfrak{q}} = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

We have $I_{\mathfrak{q}} \subseteq D_{\mathfrak{q}}$. In fact, $I_{\mathfrak{q}}$ is the kernel of a group homomorphism $\varphi_{\mathfrak{q}}$ that we will define shortly.

First some notation. Let $\kappa = \mathcal{O}_K/\mathfrak{p}$ and $\lambda = \mathcal{O}_L/\mathfrak{q}$ be the respective residue fields. We know that λ/κ is an extension of degree f of finite fields of characteristic p, where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

Here is all you need to know about finite extensions of finite fields:

Theorem 3.30. *Let λ/κ be a finite extension, with $\#\kappa = q$. The extension is Galois with cyclic Galois group generated by the Frobenius automorphism of λ, $\sigma_q\colon \lambda \to \lambda$ given by $\sigma_q(x) = x^q$.*

There is a canonical group homomorphism $\varphi_{\mathfrak{q}}\colon D_{\mathfrak{q}} \to \operatorname{Gal}(\lambda/\kappa)$, $\sigma \mapsto \overline{\sigma}$, defined as follows: let $\sigma \in D_{\mathfrak{q}}$ and $\overline{x} \in \lambda$. Let $x \in \mathcal{O}_L$ be any preimage of $\overline{x}$ under the quotient map, and let $\overline{\sigma}(\overline{x}) = \sigma(x) + \mathfrak{q}$. Is this well-defined? Suppose $x' \in \mathcal{O}_L$ also maps to $\overline{x}$, then $x - x' \in \mathfrak{q}$, so

$$\sigma(x) - \sigma(x') = \sigma(x - x') \in \sigma(\mathfrak{q}) = \mathfrak{q},$$

as wanted. Note also that if $\overline{x} \in \kappa \subseteq \lambda$ then we can certainly take $x \in \mathcal{O}_K \subseteq \mathcal{O}_L$, so that

$$\overline{\sigma}(\overline{x}) = \sigma(x) + \mathfrak{q} = x + \mathfrak{q} = \overline{x},$$

so $\overline{\sigma}$ fixes κ pointwise.

It is clear that $I_{\mathfrak{q}} = \ker \varphi_{\mathfrak{q}}$, so that we have an exact sequence of groups

$$1 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \xrightarrow{\varphi_{\mathfrak{q}}} \operatorname{Gal}(\lambda/\kappa).$$

To show that the map $\varphi_{\mathfrak{q}}$ is surjective, let's consider what Galois theory tells us about the situation. (For simplicity of notation we write simply I and D.)

> **Exercise 3.31** (Multiplicativity of ramification degree and inertial degree)**.** Let $K \subseteq L \subseteq M$ be number fields. Let $\mathfrak{m}$ be a nonzero prime ideal of $\mathcal{O}_M$, $\mathfrak{q} := \mathfrak{m} \cap \mathcal{O}_L$, $\mathfrak{p} := \mathfrak{m} \cap \mathcal{O}_K$. Then
>
> $$e(\mathfrak{m}/\mathfrak{p}) = e(\mathfrak{m}/\mathfrak{q})e(\mathfrak{q}/\mathfrak{p})$$
> $$f(\mathfrak{m}/\mathfrak{p}) = f(\mathfrak{m}/\mathfrak{q})f(\mathfrak{q}/\mathfrak{p}).$$

Theorem 3.32. *Let L/K be a finite Galois extension of number fields. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_L$ above $\mathfrak{p}$. Let $e = e(\mathfrak{q}/\mathfrak{p})$, $f = f(\mathfrak{q}/\mathfrak{p})$, and g the number of distinct prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}$, so that $efg = [L\colon K]$. Let $D = D_{\mathfrak{q}/\mathfrak{p}}$ be the decomposition group at $\mathfrak{q}$, $I = I_{\mathfrak{q}/\mathfrak{p}}$ be the inertia group at $\mathfrak{q}$, with respective fixed fields L^D and L^I. Then the degrees, ramification degrees, and inertial degrees of the various intermediate extensions are as in the following diagram:*

$$\begin{tikzcd}
 & & \textit{ramification degree} & \textit{inertial degree} \\
L \arrow[dd, dash, "e"'] & \mathfrak{q} \arrow[dd, dash] & & \\
 & & e & 1 \\
L^I \arrow[dd, dash, "f"'] & \mathfrak{q}_I = \mathfrak{q} \cap \mathcal{O}_{L^I} \arrow[dd, dash] & & \\
 & & 1 & f \\
L^D \arrow[dd, dash, "g"'] & \mathfrak{q}_D = \mathfrak{q} \cap \mathcal{O}_{L^D} \arrow[dd, dash] & & \\
 & & 1 & 1 \\
K & \mathfrak{p} & &
\end{tikzcd}$$

Proof. We have a number of claims to verify:

(a) $[L^D \colon K] = g$.
By Galois theory $[L^D \colon K] = [G \colon D]$. For each $\sigma \in G$, every element $\sigma\delta$ of the coset σD sends $\mathfrak{q}$ to $\sigma(\delta(\mathfrak{q})) = \sigma(\mathfrak{q})$, and $\sigma D = \tau D$ if and only if $\sigma(\mathfrak{q}) = \tau(\mathfrak{q})$. Therefore we have a bijection between $\{$cosets of D in $G\}$ and $\{$prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}\}$, hence the cardinality of G/D is g.

(b) $e(\mathfrak{q}_D/\mathfrak{p}) = 1$, $f(\mathfrak{q}_D/\mathfrak{p}) = 1$.
Start by noting that $g(\mathfrak{q}/\mathfrak{q}_D) = 1$, so $e(\mathfrak{q}/\mathfrak{q}_D)f(\mathfrak{q}/\mathfrak{q}_D) = ef$. However we also have $e(\mathfrak{q}/\mathfrak{q}_D) \mid e$ and $f(\mathfrak{q}/\mathfrak{q}_D) \mid f$, so we conclude that they are equal to e and f. This implies the claim.

(c) $f(\mathfrak{q}/\mathfrak{q}_I) = 1$.
It suffices to prove that the Galois group of the extension λ/λ_I is trivial. Let $\overline{\alpha} \in \lambda$. Let $\alpha \in \mathcal{O}_L$ be any preimage of $\overline{\alpha}$ and consider the polynomial

$$h(x) = \prod_{\sigma \in I} (x - \sigma(\alpha)) \in \mathcal{O}_L[x].$$

This actually has coefficients in $\mathcal{O}_{L^I}$, so its reduction $\overline{h}$ modulo $\mathfrak{q}$ has coefficients in $\overline{(\mathcal{O}_{L^I}/(\mathfrak{q} \cap \mathcal{O}_{L^I}))[x]} = \lambda_I[x]$. However, for $\sigma \in I$ we have $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$, so that $\overline{\sigma(\alpha)} = \overline{\alpha}$ and we have

$$\overline{h}(x) = (x - \overline{\alpha})^{\# I}.$$

This means that every element of the Galois group of λ/λ_I sends $\overline{\alpha}$ to $\overline{\alpha}$, as there are no other roots of $\overline{h}$. Since the Galois group acts trivially on every element of the extension, both the group and the extension must be trivial.

(d) $[L^I \colon L^D] = f$.
From the previous point we know that $f(\mathfrak{q}^I/\mathfrak{q}^D) = f$, so $[L^I \colon L^D] \geq f$. However, we know that $[D \colon I] \leq f$, so we get equality.

□

The field L^D fixed by the decomposition group is called the *decomposition field* of $\mathfrak{q}$, and the field L^I fixed by the inertia group is called the *inertia field* of $\mathfrak{q}$.

We have been working with the tower of number fields

$$K \subseteq L^D \subseteq L^I \subseteq L$$

associated with the choice of a prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ lying above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. If we have some intermediate extension K' with $K \subseteq K' \subseteq L$, we can take $\mathfrak{p}' = \mathfrak{q} \cap \mathcal{O}_{K'}$ and consider the inertia and decomposition groups $I' \subseteq D'$ associated with $\mathfrak{q}/\mathfrak{p}'$. If $H = \mathrm{Gal}(L/K') \subseteq G$, then it is clear that

$$D' = D \cap H, \qquad I' = I \cap H.$$

Also, if H and J are subgroups of G, then $L^{H \cap J} = L^H L^J$, the compositum[2] of the fields L^H and L^J.

Proposition 3.33.

(a) L^D *is the largest subextension* K' *of* L/K *such that* $e(\mathfrak{p}'/\mathfrak{p}) = 1$ *and* $f(\mathfrak{p}'/\mathfrak{p}) = 1$.

(b) L^I *is the largest subextension* K' *of* L/K *such that* $e(\mathfrak{p}'/\mathfrak{p}) = 1$.

Proof.

(a) We have seen in Theorem 3.32 that L^D satisfies the conditions. Suppose now that K' is a subextension satisfying the same conditions. We have $K' = L^H$ for some $H \subseteq G$. Then $L^{D'} = L^{D \cap H} = L^D K'$. The condition on the degrees gives

$$\#D' = e(\mathfrak{q}/\mathfrak{p}')f(\mathfrak{q}/\mathfrak{p}') = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p}) = \#D,$$

so $D' = D$ and $L^D K' = L^{D'} = L^D$, hence $K' \subseteq L^D$.

(b) The proof for this part is similar, using

$$\#I' = e(\mathfrak{q}/\mathfrak{p}') = e(\mathfrak{q}/\mathfrak{p}) = \#I.$$

□

Corollary 3.34. *Let* L_1, L_2 *be finite extensions of a number field* K *and let* $\mathfrak{p}$ *be a nonzero prime ideal of* $\mathcal{O}_K$.

(a) $\mathfrak{p}$ *is unramified in both* L_1 *and* L_2 *if and only if it is unramified in* L_1L_2 *(compositum taken inside a fixed algebraic closure of* $\mathbb{Q}$*).*

(b) $\mathfrak{p}$ *splits completely in both* L_1 *and* L_2 *if and only if it splits completely in* L_1L_2.

Proof.

(a) Suppose $\mathfrak{p}$ is unramified in L_1L_2. In the tower $K \subseteq L_1 \subseteq L_1L_2$, the total ramification degree is 1, so by multiplicativity both intermediate ramification degrees are also 1, hence $\mathfrak{p}$ is unramified in L_1. The same argument shows that it is also unramified in L_2.

Conversely, suppose $\mathfrak{p}$ is unramified in both L_1 and L_2. Let M be the Galois closure of L_1L_2, $\mathfrak{q}'$ a prime ideal of M lying over $\mathfrak{p}$, and $\mathfrak{q} = \mathfrak{q}' \cap \mathcal{O}_{L_1L_2}$. Let $I = I_{\mathfrak{q}'/\mathfrak{p}}$ and consider the inertia field M^I. Since $\mathfrak{q}_2 = \mathfrak{q}' \cap \mathcal{O}_{L_2}$ is unramified over $\mathfrak{p}$, we have $L_2 \subseteq M^I$. Similarly, $L_1 \subseteq M^I$, therefore $L_1L_2 \subseteq M^I$ and $\mathfrak{p}$ is unramified in L_1L_2.

$$\begin{tikzcd}
 & M \arrow[d, dash] & & \mathfrak{q}' \arrow[d, dash] & \\
 & L_1L_2 \arrow[dl, dash] \arrow[dr, dash] & & \mathfrak{q} \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] & & \mathfrak{q}_2 \arrow[dl, dash] \\
 & K & & \mathfrak{p} &
\end{tikzcd}$$

(b) Similar to part (a).

□

[2] If K_1 and K_2 are subfields of a field L, then their *compositum* K_1K_2 is the smallest subfield of L that contains both K_1 and K_2.

Corollary 3.35. *Let L be a finite extension of a number field K and let M be the Galois closure of L/K. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$.*

(a) $\mathfrak{p}$ is unramified in L if and only if it is unramified in M.

(b) $\mathfrak{p}$ splits completely in L if and only if it splits completely in M.

Proof.

(a) One direction is clear (if $\mathfrak{p}$ is unramified in M then it is unramified in L). For the other direction, assume $\mathfrak{p}$ is unramified in L. For any $\sigma\colon L \hookrightarrow \mathbb{C}$ fixing K, $\mathfrak{p} = \sigma(\mathfrak{p})$ is unramified in $\sigma(L)$. But M is the compositum of $\sigma(L)$ for all σ, hence $\mathfrak{p}$ is unramified in M.

(b) Similar to part (a).

□

Corollary 3.36. *The following is a short exact sequence:*

$$1 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \xrightarrow{\varphi_{\mathfrak{q}}} \mathrm{Gal}(\lambda/\kappa) \to 1.$$

Proof. Follows directly from Theorem 3.32. □

Corollary 3.37. *Let L/K be a finite Galois extension of number fields and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$.*

(a) The cardinality of the inertia group $I_{\mathfrak{q}}$ is equal to the ramification degree $e = e(\mathfrak{q}/\mathfrak{p})$. In particular, $\mathfrak{p}$ is unramified in $\mathcal{O}_L$ if and only if $I_{\mathfrak{q}}$ is the trivial group.

(b) The quotient $D_{\mathfrak{q}}/I_{\mathfrak{q}}$ is cyclic of order $f = f(\mathfrak{q}/\mathfrak{p})$ and there is a canonical element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in D_{\mathfrak{q}}/I_{\mathfrak{q}}$ that generates the quotient group and maps to the Frobenius automorphism $\sigma_p \in \mathrm{Gal}(\lambda/\kappa)$. In particular, if $\mathfrak{p}$ is unramified in $\mathcal{O}_L$, then the Frobenius is a well-defined element of the decomposition group $D_{\mathfrak{q}}$.

(c) If $\mathfrak{p}$ is unramified in $\mathcal{O}_L$, then the Frobenius element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in D_{\mathfrak{q}}$ is the unique element $\sigma \in G = \mathrm{Gal}(L/K)$ with the property that

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{q}} \qquad \text{for all } \alpha \in \mathcal{O}_L.$$

Proof. Everything follows directly from Theorem 3.32, except for part of (c): if $\sigma \in G$ satisfies the congruence, then $\sigma(\mathfrak{q}) = \mathfrak{q}$, so that $\sigma \in D_{\mathfrak{q}}$, where we know that the congruence determines $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ uniquely. □

How do the objects we have been working with depend on the choice of prime ideal $\mathfrak{q}$ above $\mathfrak{p}$?

Proposition 3.38. *Let L/K be a finite Galois extension of number fields and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Let $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$ and let $\sigma \in G = \mathrm{Gal}(L/K)$ be such that $\mathfrak{q}' = \sigma(\mathfrak{q})$. Then*

$$D_{\mathfrak{q}'/\mathfrak{p}} = \sigma D_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1}$$
$$I_{\mathfrak{q}'/\mathfrak{p}} = \sigma I_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1}.$$

If $\mathfrak{p}$ is unramified in L, then

$$\mathrm{Frob}_{\mathfrak{q}'/\mathfrak{p}} = \sigma\, \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\, \sigma^{-1}.$$

Proof. Here is the calculation for $D_{\mathfrak{q}'/\mathfrak{p}}$:

$$\begin{aligned} D_{\mathfrak{q}'/\mathfrak{p}} &= \{\tau \in G \mid \tau(\mathfrak{q}') = \mathfrak{q}'\} = \{\tau \in G \mid \tau(\sigma(\mathfrak{q})) = \sigma(\mathfrak{q})\} \\ &= \{\tau \in G \mid \sigma^{-1}\tau\sigma(\mathfrak{q}) = \mathfrak{q}\} = \{\sigma\eta\sigma^{-1} \in G \mid \eta(\mathfrak{q}) = \mathfrak{q}\} \\ &= \sigma\{\eta \in G \mid \eta(\mathfrak{q}) = \mathfrak{q}\}\sigma^{-1} = \sigma D_{\mathfrak{q}/\mathfrak{p}}\sigma^{-1}. \end{aligned}$$

□

We say that L/K is an *abelian extension* if it is Galois and its Galois group is abelian.

Corollary 3.39. *If L is a finite abelian extension of a number field K, then the groups $D_{\mathfrak{q}/\mathfrak{p}}$ and $I_{\mathfrak{q}/\mathfrak{p}}$ and the Frobenius element $\operatorname{Frob}_{\mathfrak{q}/\mathfrak{p}}$ depend only on $\mathfrak{p}$, not on the choice of prime ideal $\mathfrak{q}$ over it.*

We're a little overdue for the following result, but the proof benefits from the transitivity of the Galois action we have been exploiting lately:

Theorem 3.40. *Let K be a number field and $p \in \mathbb{Z}$ a prime number. Then p is ramified in $\mathcal{O}_K$ if and only if p divides the discriminant Δ_K of $\mathcal{O}_K$.*

Proof. Fix an integral basis $\omega_1, \dots, \omega_n$ of $\mathcal{O}_K$, and let M denote the Galois closure of K.

($\Rightarrow$): Since p is ramified, there exists a prime ideal $\mathfrak{p}_0$ of $\mathcal{O}_K$ such that $e(\mathfrak{p}_0/p) > 1$. Writing $p\mathcal{O}_K = \mathfrak{p}_0 J$, the ideal J is then contained in all the prime ideals of $\mathcal{O}_K$ above p, and $p\mathcal{O}_K \subsetneq J$.

Let $\theta \in J \setminus p\mathcal{O}_K$ and write

$$\theta = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n, \qquad a_j \in \mathbb{Z}.$$

Since $\theta \notin p\mathcal{O}_K$, there exists j such that $p \nmid a_j$. Without loss of generality $j = 1$. We have

$$\Delta(\theta, \omega_2, \dots, \omega_n) = a_1^2 \Delta_K.$$

Since $p \nmid a_1$, it suffices to prove that $p \mid \Delta(\theta, \omega_2, \dots, \omega_n)$.

In order to do this, let $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ be the embeddings of K into $\mathbb{C}$, extending each of them to an embedding $\sigma_j \colon M \hookrightarrow \mathbb{C}$ of the Galois closure M. Since $\theta \in J$, we know that $\theta \in \mathfrak{p}$ for all $\mathfrak{p}$ in $\mathcal{O}_K$ above p. Therefore $\theta \in \mathfrak{q}$ for all $\mathfrak{q}$ in $\mathcal{O}_M$ above p.

Fix one of the prime ideals $\mathfrak{q}_0$ of $\mathcal{O}_M$ above p. For any $\sigma \in \operatorname{Gal}(M/\mathbb{Q})$, $\sigma^{-1}(\mathfrak{q}_0)$ is another such prime ideal, so $\theta \in \sigma^{-1}(\mathfrak{q}_0)$, hence $\sigma(\theta) \in \mathfrak{q}_0$. In particular, $\sigma_j(\theta) \in \mathfrak{q}_0$ for all embeddings σ_j. Therefore

$$\Delta(\theta, \omega_2, \dots, \omega_n) \in \mathfrak{q}_0 \cap \mathbb{Z} = p\mathbb{Z}.$$

($\Leftarrow$): Suppose $p \mid \Delta_K$ but p is unramified in K.

Let $\Sigma = \Sigma(\omega_1, \dots, \omega_n)$ so that $\Delta_K = \det(\Sigma)^2$ and note that

$$\Delta_K = \det(\Sigma)^2 = \det(\Sigma^T)\det(\Sigma) = \det(\Sigma^T\Sigma) = \det([\operatorname{Tr}_{\mathbb{Q}}^K(\omega_i\omega_j)]).$$

The assumption that $p \mid \Delta_K$ implies that the rows of the reduction modulo p of the matrix $[\operatorname{Tr}_{\mathbb{Q}}^K(\omega_i\omega_j)]$ are linearly dependent over $\mathbb{F}_p$; in other words there are integers $a_1, \dots, a_n \in \mathbb{Z}$, not all divisible by p, such that

$$a_1 \begin{bmatrix} \operatorname{Tr}_{\mathbb{Q}}^K(\omega_1\omega_1) \\ \vdots \\ \operatorname{Tr}_{\mathbb{Q}}^K(\omega_n\omega_1) \end{bmatrix} + \cdots + a_n \begin{bmatrix} \operatorname{Tr}_{\mathbb{Q}}^K(\omega_1\omega_n) \\ \vdots \\ \operatorname{Tr}_{\mathbb{Q}}^K(\omega_n\omega_n) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \pmod{p}.$$

Let $\theta = a_1\omega_1 + \cdots + a_n\omega_n$, then we can rewrite the above as

$$\begin{bmatrix} \operatorname{Tr}^K_{\mathbb{Q}}(\omega_1\theta) \\ \vdots \\ \operatorname{Tr}^K_{\mathbb{Q}}(\omega_n\theta) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \pmod p.$$

This says that $\operatorname{Tr}^K_{\mathbb{Q}}(\theta\mathcal{O}_K) \subseteq p\mathbb{Z}$, but $\theta \notin p\mathcal{O}_K$ since not all a_j are divisible by p.

Let's get back to the other assumption, namely that p is unramified in K. Since $\theta \notin pR$, then there exists some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p such that $\theta \notin \mathfrak{p}$. By Corollary 3.35 we also know that p is unramified in the Galois closure M. Letting $\mathfrak{q}$ be any prime ideal of $\mathcal{O}_M$ above $\mathfrak{p}$, we have that $\theta \notin \mathfrak{q}$.

However

$$\operatorname{Tr}^M_{\mathbb{Q}}(\theta\mathcal{O}_M) = \operatorname{Tr}^K_{\mathbb{Q}}\operatorname{Tr}^M_K(\theta\mathcal{O}_M) = \operatorname{Tr}^K_{\mathbb{Q}}\left(\theta\operatorname{Tr}^M_K(\mathcal{O}_M)\right) \subseteq \operatorname{Tr}^K_{\mathbb{Q}}(\theta\mathcal{O}_K) \subseteq p\mathbb{Z}.$$

As p is unramified in M, we can use the Chinese Remainder Theorem to find an element $\alpha \in \mathcal{O}_M$ that is not contained in $\mathfrak{q}$ but is contained in all the other prime ideals of $\mathcal{O}_M$ above p.

For all $x \in \mathcal{O}_M$, we have

$$\operatorname{Tr}^M_{\mathbb{Q}}(\theta\alpha x) \in \operatorname{Tr}^M_{\mathbb{Q}}(\theta\mathcal{O}_M) \subseteq p\mathbb{Z} \subseteq \mathfrak{q}.$$

Let $D = D(\mathfrak{q}/p) \subseteq G = \operatorname{Gal}(M/\mathbb{Q})$, then for any $\sigma \in G \smallsetminus D$ we have that $\alpha \in \sigma^{-1}(\mathfrak{q}) \neq \mathfrak{q}$, so that $\sigma(\alpha) \in \mathfrak{q}$. This means that for all $x \in \mathcal{O}_M$ we have

$$\sigma(\theta\alpha x) \in \mathfrak{q}.$$

We conclude then that for all $x \in \mathcal{O}_M$

$$\sum_{\sigma\in D}\sigma(\theta\alpha x) = \operatorname{Tr}^M_{\mathbb{Q}}(\theta\alpha x) - \sum_{\sigma\in G\smallsetminus D}\sigma(\theta\alpha x) \in \mathfrak{q}.$$

At this point we invoke unramifiedness of p in M once more: this tells us that D is identified with $\operatorname{Gal}(\mu/\mathbb{F}_p)$, where $\mu = \mathcal{O}_M/\mathfrak{q}$ is the residue field of $\mathfrak{q}$. Using this identification, the last equation becomes

$$\sum_{\overline{\sigma}\in\operatorname{Gal}(\mu/\mathbb{F}_p)} \overline{\sigma}(\overline{\theta}\,\overline{\alpha}\,\overline{x}) = 0 \qquad \text{for all } \overline{x} \in \mu.$$

Since $\theta \notin \mathfrak{q}$ and $\alpha \notin \mathfrak{q}$, we see that $\overline{\theta}\,\overline{\alpha} \neq 0$, so we can set $\overline{y} = \overline{\theta}\,\overline{\alpha}\,\overline{x}$ to get

$$\sum_{\overline{\sigma}\in\operatorname{Gal}(\mu/\mathbb{F}_p)} \overline{\sigma}(\overline{y}) = 0 \qquad \text{for all } \overline{y} \in \mu.$$

This says that

$$\sum_{\overline{\sigma}\in\operatorname{Gal}(\mu/\mathbb{F}_p)} \overline{\sigma} = 0,$$

where the two sides of the equality are thought of as functions from μ to μ. However, this contradicts linear independence of characters (see below). □

Exercise 3.41 (Linear independence of characters).

(a) Let G be a group and μ a field. A *character* of G with values in μ is a group homomorphism $\chi\colon G \to \mu^\times$. We say that characters $\chi_1, \ldots, \chi_n$ are linearly independent if there are no nontrivial relations

$$a_1\chi_1 + \cdots + a_n\chi_n = 0,$$

where both sides are viewed as functions $G \to \mu$.

Prove that if $\chi_1, \ldots, \chi_n$ are distinct characters then they are linearly independent. (See [3, Theorem 7 in Section 14.2] if you get stuck.)

(b) Deduce that if $\sigma_1, \dots, \sigma_n$ are distinct embeddings of a field κ into a field μ, then they are linearly independent.

(c) Deduce that if $\sigma_1, \dots, \sigma_n$ are distinct automorphisms of a field μ, then they are linearly independent.

Corollary 3.42. *Let L/K be a finite extension of number fields. There are only finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that ramify in L.*

In particular, for any number field L, there are only finitely many primes $p \in \mathbb{Z}$ that ramify in L.

Example 3.43. The primes that ramify in the quadratic extension $\mathbb{Q}(\sqrt{d})$ with d squarefree are precisely

(a) the primes that divide $4d$, if $d \equiv 2, 3 \pmod 4$;

(b) the primes that divide d, if $d \equiv 1 \pmod 4$.

3.5. Cyclotomic fields redux, and more Quadratic Reciprocity

Now, as promised, let's have another look at cyclotomic fields. I will once again restrict to the case $m = p^r$, but a lot of what we will say holds for arbitrary m.

Theorem 3.44. *Let $m = p^r$ with $p \in \mathbb{Z}$ prime and $r \in \mathbb{Z}_{\geq 1}$. Let $\zeta = e^{2\pi i/m}$, $K = \mathbb{Q}(\zeta)$ so that $\mathcal{O}_K = \mathbb{Z}[\zeta]$. Let $\ell \in \mathbb{Z}$ be prime such that $\ell \neq p$ and let f denote the order of ℓ as an element of $(\mathbb{Z}/m\mathbb{Z})^\times$. Then the ideal $\ell\mathcal{O}_K$ has the decomposition*

$$\ell\mathcal{O}_K = \mathfrak{l}_1 \dots \mathfrak{l}_g,$$

where $\mathfrak{l}_1, \dots, \mathfrak{l}_g$ are distinct prime ideals of $\mathcal{O}_K$, $f(\mathfrak{l}_j/\ell) = f$ for all j, and $fg = \varphi(m)$.

Proof. We know from Lemma 3.20 that $|\Delta_K|$ is a power of p, so ℓ does not ramify in K. As $K/\mathbb{Q}$ is a Galois extension, we know that $f(\mathfrak{l}_j/\ell) = f'$ for some integer f' and that $f'g = \varphi(m)$. Moreover, if $\mathfrak{l}$ is any prime ideal of $\mathcal{O}_K$ above ℓ, we know that the decomposition group $D = D(\mathfrak{l}/\ell)$ is cyclic of order f', generated by the Frobenius element $\mathrm{Frob}_\ell \in G$.

I claim that $\mathrm{Frob}_\ell \in G$ is given explicitly by $\mathrm{Frob}_\ell(\zeta) = \zeta^\ell$. To see this, recall that Frob_ℓ is the unique element $\sigma \in G$ such that $\sigma(x) \equiv x^\ell \pmod \ell$ for all $x \in \mathcal{O}_K = \mathbb{Z}[\zeta]$. But the map $\zeta \mapsto \zeta^\ell$ has precisely this property:

$$\begin{aligned} a_0 + a_1\zeta + \dots + a_{n-1}\zeta^{n-1} &\mapsto a_0 + a_1\zeta^\ell + \dots + a_{n-1}\zeta^{\ell(n-1)} \\ &\equiv (a_0 + a_1\zeta + \dots + a_{n-1}\zeta^{n-1})^\ell \pmod \ell, \end{aligned}$$

where we made use of the binomial theorem modulo ℓ.

However, the order of $\zeta \mapsto \zeta^\ell$ inside $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$ is precisely the order of ℓ in $(\mathbb{Z}/m\mathbb{Z})^\times$, therefore $f' = f$. □

Corollary 3.45. *A prime $\ell \in \mathbb{Z}$ splits completely in $\mathbb{Z}[\zeta]$ if and only if $\ell \equiv 1 \pmod m$.*

Example 3.46. Let $m = 5^2$, so that $\varphi(m) = 20$. Here is a table of primes together with the factorisation of the cyclotomic polynomial $\Phi = x^{20} + x^{15} + x^{10} + x^5 + 1$ over $\mathbb{F}_\ell$:

ℓ	$\ell \pmod{5^2}$	order of ℓ in $(\mathbb{Z}/5^2\mathbb{Z})^\times$	factorisation of Φ over $\mathbb{F}_\ell$
101	1	1	$(x+4)(x+9)(x+13)(x+20)(x+21)$ $\times(x+22)(x+23)(x+30)(x+33)(x+43)$ $\times(x+45)(x+47)(x+49)(x+64)(x+70)$ $\times(x+76)(x+77)(x+82)(x+85)(x+96)$
149	24	2	$(x^2+39x+1)(x^2+49x+1)$ $\times(x^2+55x+1)(x^2+75x+1)$ $\times(x^2+90x+1)(x^2+97x+1)$ $\times(x^2+106x+1)(x^2+120x+1)$ $\times(x^2+129x+1)(x^2+134x+1)$
7	7	4	$(x^4+2x^3+4x^2+2x+1)$ $\times(x^4+4x^3+4x+1)$ $\times(x^4+4x^3+3x^2+4x+1)$ $\times(x^4+5x^3+5x^2+5x+1)$ $\times(x^4+6x^3+5x^2+6x+1)$
31	6	5	$(x^5+15)(x^5+23)(x^5+27)(x^5+29)$
29	4	10	$(x^{10}+6x^5+1)(x^{10}+24x^5+1)$
3	3	20	$x^{20}+x^{15}+x^{10}+x^5+1$

Let's revisit the law of quadratic reciprocity. Take an odd prime number p and let $L = \mathbb{Q}(\zeta)$. Recall that the Galois group $G = \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of even order, so L has a unique quadratic subfield K. Consider the tower of extensions $\mathbb{Q} \subseteq K \subseteq L$. We know that p is the unique prime that ramifies in L, therefore it is the unique prime that ramifies in K. This implies that $\Delta_K = \pm p$, and comparing this with the explicit discriminant formula for quadratic fields we conclude that $\Delta_K = (-1)^{(p-1)/2} p$, which we denote by p^*.

On the other hand, let $H \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ be the subset of the squares in $(\mathbb{Z}/p\mathbb{Z})^\times$. It is easy to see that this is a subgroup, and we know it has index 2 in G. Therefore its fixed field L^H has degree 2 over $\mathbb{Q}$, so it must be the same as the quadratic subfield K described above.

We can play these two descriptions against each other to obtain:

Theorem 3.47 (Law of Quadratic Reciprocity, Take Two)**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Proof. As above, let $\zeta = e^{2\pi i/p}$, $L = \mathbb{Q}(\zeta)$, K the unique quadratic subfield of L.

Since $K = \mathbb{Q}(\sqrt{p^*})$ and $p^* \equiv 1 \pmod 4$, we know that $[\mathcal{O}_K : \mathbb{Z}[\sqrt{p^*}]] = 2$. Letting $\theta = \sqrt{p^*}$ and recalling that q is odd, we have $q \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ so we may apply Theorem 3.3 to conclude that q splits completely in K if and only if the minimal polynomial $x^2 - p^*$ of θ factors into linear factors modulo q, in other words if and only if $\left(\frac{p^*}{q}\right) = 1$.

Now let $\mathfrak{q}$ be any prime ideal of $\mathcal{O}_L$ lying above q, and let $D = D_{\mathfrak{q}/q} \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ be the decomposition group at $\mathfrak{q}$. Since $q \neq p$, it is unramified in L, and we have seen in the proof of Theorem 3.44 that the Frobenius element at $\mathfrak{q}$ can be identified with $q \in (\mathbb{Z}/p\mathbb{Z})^\times$. So $D = \langle q \rangle$. Of course, the decomposition field L^D is the largest subextension of L in which q splits completely. So q splits completely in K if and only if $K \subseteq L^D$. But $K = L^H$, so q splits completely in K if and only if $D \subseteq H$. But $D = \langle q \rangle$, so q splits completely in K if and only if $q \in H$, which is the subgroup of squares in $(\mathbb{Z}/p\mathbb{Z})^{\times}$.

Therefore q splits completely in K if and only if $\left(\frac{q}{p}\right) = 1$. □

4. Some finiteness results

In an earlier chapter, we looked at $\mathcal{O}_K$ sitting as a lattice inside $\mathbb{Q}^n$ via

$$\mathcal{O}_K \subseteq K \cong \mathbb{Q}^n$$

Recall that in our terminology, a lattice in $\mathbb{Q}^n$ or in $\mathbb{R}^n$ is a discrete $\mathbb{Z}$-submodule of rank n.

We are going to construct a canonical embedding

$$\iota\colon \mathcal{O}_K \hookrightarrow \mathbb{R}^n$$

and show that $\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$.

Split the list of n distinct embeddings $K \hookrightarrow \mathbb{C}$ into the *real embeddings* $\sigma_1, \dots, \sigma_{r_1}\colon K \hookrightarrow \mathbb{R}$ and the pairs of conjugate *complex embeddings* $\tau_1, \overline{\tau}_1, \dots, \tau_{r_2}, \overline{\tau}_{r_2}\colon K \hookrightarrow \mathbb{C}$ with $\tau_j(K) \notin \mathbb{R}$. We have $n = r_1 + 2r_2$. The pair (r_1, r_2) is called the *signature* of K.

We combine these embeddings into $\iota\colon K \hookrightarrow \mathbb{R}^n$ as the composition of

$$K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^{r_1+2r_2} = \mathbb{R}^n$$

by

$$\begin{aligned} \alpha &\mapsto \big(\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \tau_1(\alpha), \dots, \tau_{r_2}(\alpha)\big) \\ &\mapsto \big(\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \operatorname{Re}(\tau_1(\alpha)), \operatorname{im}(\tau_1(\alpha)), \dots, \operatorname{Re}(\tau_{r_2}(\alpha)), \operatorname{im}(\tau_{r_2}(\alpha))\big). \end{aligned}$$

Proposition 4.1. *$\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$.*

Proof. We know that $\mathcal{O}_K$, and hence $\iota(\mathcal{O}_K)$, are finitely generated over $\mathbb{Z}$. We need to show that given a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ of $\mathcal{O}_K$, the vectors $\iota(\alpha_1), \dots, \iota(\alpha_n)$ are linearly independent over $\mathbb{R}$.

TODO: huge matrix!

The determinant D of this matrix is $(-2i)^{r_2}$ times the determinant of the original matrix; on the other hand, $D^2 = \Delta_K \neq 0$. We conclude that the determinant of the original matrix is nonzero, so the vectors are linearly independent. □

We will quantify how big a lattice $\Lambda \subseteq \mathbb{R}^n$ is by considering the quotient $\mathbb{R}^n/\Lambda$.

A *fundamental domain* for (the action on $\mathbb{R}^n$ by translations by) Λ is a set $\mathcal{F} \subset \mathbb{R}^n$ of the form

$$\mathcal{F} = \left\{ \sum_{i=1}^n a_i v_i \colon a_i \in [0,1) \right\},$$

where $v_1, \dots, v_n$ is a $\mathbb{Z}$-basis for Λ.

There is a bijection of sets

$$\mathcal{F} \xrightarrow{\sim} \mathbb{R}^n/\Lambda.$$

TODO: picture of fundamental domain for a $\Lambda \subseteq \mathbb{R}^2$.

We define the *covolume* of Λ and the volume of $\mathbb{R}^n/\Lambda$ to be the volume of the fundamental domain $\mathcal{F}$:

$$\operatorname{covol}(\Lambda) = \operatorname{vol}(\mathcal{F}) = |\det([v_1\, v_2\, \dots\, v_n])|.$$

Corollary 4.2. $\operatorname{covol}(\iota(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|\Delta_K|}$.

If $\Omega \subseteq \Lambda \subseteq \mathbb{R}^n$ is a sublattice, then

$$\operatorname{covol}(\Omega) = [\Lambda\colon\Omega]\operatorname{covol}(\Lambda).$$

Corollary 4.3. *For any non-zero ideal I of $\mathcal{O}_K$,*

$$\operatorname{covol}(\iota(I)) = 2^{-r_2}\sqrt{|\Delta_K|}N(I).$$

Given a signature (r_1, r_2), we define a function $N\colon\mathbb{R}^{r_1+2r_2} \to \mathbb{R}$ by

$$N(a_1, \dots, a_r, x_1, y_1, \dots, x_{r_2}, y_{r_2}) = a_1 \dots a_r(x_1^2 + y_1^2)\dots(x_{r_2}^2 + y_{r_2}^2).$$

If $\alpha \in K$, then

$$N(\iota(\alpha)) = N_{\mathbb{Q}}^K(\alpha).$$

4.1. The Convex Body Theorem

A subset $S \subseteq \mathbb{R}^n$ is *convex* if

$$x, y \in S \text{ and } \lambda \in [0,1] \quad\Rightarrow\quad \lambda x + (1-\lambda)y \in S.$$

We say $S \subseteq \mathbb{R}^n$ is *symmetric* if whenever $x \in S$, $-x \in S$.

Convex sets are (Lebesgue) measurable.

Let $S \subseteq \mathbb{R}^n$ be bounded and measurable. A function $T\colon S \to \mathbb{R}^n$ is:

- *volume-preserving* if $\operatorname{vol}(T(S)) = \operatorname{vol}(S)$;
- *piecewise volume-preserving* if we can write $S = \coprod_{j=1}^{\infty} S_j$ such that $T\mid_{S_j}$ is volume-preserving for all j.

Lemma 4.4. *Let $S \subseteq \mathbb{R}^n$ be bounded and measurable, and let $T\colon S \to \mathbb{R}^n$ be piecewise volume-preserving. If $\operatorname{vol}(S) > \operatorname{vol}(T(S))$, then T is not injective.*

Proof. Write $S = \coprod_{j=1}^{\infty} S_j$ so that $T|_{S_j}$ is volume-preserving. If T is injective, then $T(S) = \coprod_{j=1}^{\infty} T(S_j)$. Then

$$\operatorname{vol}(S) > \operatorname{vol}(T(S)) = \sum_{j=1}^{\infty}\operatorname{vol}(T(S_j)) = \sum_{j=1}^{\infty}\operatorname{vol}(S_j) = \operatorname{vol}(S),$$

contradiction. □

Lemma 4.5. *Let Λ be a lattice in $\mathbb{R}^n$ and let $\mathcal{F} \subseteq \mathbb{R}^n$ be a fundamental domain. Define $T\colon\mathbb{R}^n \to \mathcal{F}$ as follows: for any $x \in \mathbb{R}^n$, let $T(x) \in \mathcal{F}$ be the unique representative of $x + \Lambda$ in $\mathcal{F} = \mathbb{R}^n/\Lambda$. (So that $x - T(x) \in \Lambda$.)*

Then T is a piecewise translation, in particular it is piecewise volume-preserving.

Proof. Fix a $\mathbb{Z}$-basis $v_1, \dots, v_n$ of Λ and let $\mathcal{F}$ be the fundamental domain defined by $v_1, \dots, v_n$.

For $m = (m_1, \dots, m_n) \in \mathbb{Z}^n$, let

$$w_m = \sum_{j=1}^{n} m_j v_j \in \Lambda.$$

Then

$$\mathbb{R}^n = \coprod_{m\in\mathbb{Z}^n}\left(\mathcal{F} + w_m\right)$$

and $T|_{\mathcal{F}+w_m}\colon\mathcal{F} + w_m \to \mathcal{F}$ is translation by $-w_m$. □

Theorem 4.6 (Minkowski). *Let Λ be a lattice in $\mathbb{R}^n$ and let $S \subseteq \mathbb{R}^n$ be a bounded, convex, symmetric set. If* $\mathrm{vol}(S) > 2^n \mathrm{covol}(\Lambda)$*, then S contains a nonzero element of Λ.*

If, in addition, S is compact, then: if $\mathrm{vol}(S) \geq 2^n \mathrm{covol}(\Lambda)$*, then S contains a nonzero element of Λ.*

Proof. Consider the sublattice $2\Lambda \subseteq \Lambda$. We know that $\mathrm{covol}(2\Lambda) = 2^n \mathrm{covol}(\Lambda)$. Let $\mathcal{F}$ be a fundamental domain for 2Λ. Let $T\colon \mathbb{R}^n \to \mathcal{F}$ be the piecewise volume-preserving map from Lemma 4.5.

By hypothesis

$$\mathrm{vol}(S) > \mathrm{vol}(\mathcal{F}) \geq \mathrm{vol}(T(S))$$

(the second inequality due to $T(S) \subseteq \mathcal{F}$), so by Lemma 4.4, T is not injective. Therefore there exist elements $x \neq y$ of S such that $T(x) = T(y)$. Let

$$z = x - y = \big(x - T(x)\big) - \big(y - T(x)\big) = \big(x - T(x)\big) - \big(y - T(y)\big) \in 2\Lambda,$$

with $z \neq 0$. So $z = 2w$ for $w \in \Lambda$, $w \neq 0$.

Since S is symmetric, we know that $-y \in S$, therefore

$$w = \frac{1}{2} z = \frac{1}{2} x - \frac{1}{2} y = \frac{1}{2} x + \left(1 - \frac{1}{2}\right)(-y),$$

and the latter is in S because S is convex.

Assume now that S is also compact, and suppose that $\mathrm{vol}(S) = 2^n \mathrm{covol}(\Lambda)$. For each $n \in \mathbb{N}$, consider $\left(1 + \frac{1}{n}\right) S$. We get a sequence of elements $\lambda_1, \lambda_2, \cdots \in \Lambda \cap 2S$. Since $2S$ is compact, there exists a subsequence that converges to some $\lambda \in \Lambda \cap 2S$. But

$$\lambda \in \bigcap_{n \in \mathbb{N}} \left(1 + \frac{1}{n}\right) S = \overline{S} = S,$$

since S is compact, hence closed. □

Define

$$\mathbb{B}_1 = \{x \in \mathbb{R}^n \mid |N(x)| \leq 1\}.$$

Proposition 4.7. *Let $S \subseteq \mathbb{B}_1$ be a symmetric, convex, compact set. For any nonzero ideal I in $\mathcal{O}_K$, there exists $\alpha \in I$, $\alpha \neq 0$, such that*

$$|N_{\mathbb{Q}}^K(\alpha)| \leq \frac{2^n 2^{-r_2} \sqrt{|\Delta_K|}}{\mathrm{vol}(S)} N(I).$$

Proof. For any $t > 0$, consider the set tS: it is bounded, symmetric, convex, with volume $\mathrm{vol}(tS) = t^n \mathrm{vol}(S)$, and

$$tS \subseteq \{x \in \mathbb{R}^n \mid |N(x)| \leq t^n\}.$$

Fixing now

$$t = 2\left(\frac{\mathrm{covol}(\iota(I))}{\mathrm{vol}(S)}\right)^{1/n},$$

then tS $= 2^n \mathrm{covol}(\iota(I))$, so by Minkowski's Convex Body Theorem, tS contains a nonzero element of $\iota(I)$. So there exists $\alpha \neq 0$, $\alpha \in I$ such that $|N_{\mathbb{Q}}^K(\alpha)| \leq t^n$, then use

$$\mathrm{covol}(\iota(I)) = 2^{-r_2} \sqrt{|\Delta_K|} N(I).$$

□

How good the resulting bound is depends on how large we can make the volume of S. It would be great to take $S = \mathbb{B}_1$ itself, but what does the latter really look like?

Example 4.8. Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field (so $d > 0$ is squarefree). The signature of K is $(r_1, r_2) = (2, 0)$. We have

$$\mathbb{B}_1 = \{(a, b) \in \mathbb{R}^2 \mid |ab| \leq 1\}.$$

Consider the hyperbolas with equations $ab = 1$ and $ab = -1$; altogether there are 4 curves that divide the plane into 5 connected regions. The set $\mathbb{B}_1$ is the connected region that contains the origin $(0, 0)$. It is symmetric, but clearly neither convex nor compact.

A “large” subset S of $\mathbb{B}_1$ that is symmetric, convex, compact, is the filled square defined by

$$S = \{(a, b) \in \mathbb{R}^2 \mid |a| + |b| \leq 2\}.$$

We can see that $S \subseteq \mathbb{B}_1$ on the graph, or symbolically by noting that

$$\sqrt{|a|\,|b|} \leq \frac{|a| + |b|}{2},$$

and therefore

$$|ab| \leq \frac{(|a| + |b|)^2}{4} \leq \frac{4}{4} = 1.$$

In the general case, we define $S \subseteq \mathbb{R}^n$ by

$$S = \left\{x \in \mathbb{R}^{r_1+2r_2} \mid |a_1| + \cdots + |a_{r_1}| + 2\left(\sqrt{x_1^2 + y_1^2} + \cdots + \sqrt{x_{r_2}^2 + y_{r_2}^2}\right) \leq n\right\}.$$

S is clearly symmetric, bounded, and closed (hence compact). One can show that it is also convex, and a subset of $\mathbb{B}_1$. Moreover, some super fun multivariable calculus shows that

$$\mathrm{vol}(S) = \frac{n^n}{n!} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2}.$$

Given all this, we define the *Minkowski constant* of the number field K:

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

Theorem 4.9. *Every ideal class in $\mathcal{O}_K$ contains a nonzero ideal of norm at most M_K.*

Proof. Follows from Proposition 4.7 since

$$\frac{2^n 2^{-r_2} \sqrt{|\Delta_K|}}{\mathrm{vol}(S)} = M_K.$$

□

Example 4.10. Was this worth the effort?

Take $K = \mathbb{Q}(\sqrt{-5})$, then

$$M_K = \frac{2!}{2^2} \frac{4}{\pi} \sqrt{|20|} = \frac{4\sqrt{5}}{\pi} \approx 2.85,$$

so every ideal class has a representative of norm ≤ 2. We just need to check that the ideal above 2 is not principal to conclude that K has class number 2. (With the methods of the previous chapters, the norm bound was 10.5, so we had to consider $p = 2, 3, 5, 7$.)

Corollary 4.11. *For any number field we have*

$$\sqrt{|\Delta_K|} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}.$$

Proof. The smallest possible norm of a nonzero ideal of $\mathcal{O}_K$ is 1, so $M_K \geq 1$, hence the bound. □

Corollary 4.12. *If $K \neq \mathbb{Q}$ then $|\Delta_K| \geq 2$.*

Proof. Clearly $r_2 \leq (n/2)$, so $(\pi/4)^{r_2} \geq (\pi/4)^{n/2}$. One can show by induction that

$$\frac{n^n}{n!} \geq 2^{n-1} \qquad \text{for all } n \geq 2.$$

So if $n \geq 2$ then

$$\sqrt{|\Delta_K|} \geq \pi^{n/2} 2^{-1} \geq \frac{\pi}{2} > 1.$$

□

Corollary 4.13. *If $K \neq \mathbb{Q}$, then the set of prime numbers that ramify in K is nonempty.*

4.2. Dirichlet's Unit Theorem

Theorem 4.14. *Let K be a number field of signature (r_1, r_2), let $\mathcal{O}_K^\times$ denote the multiplicative group of $\mathcal{O}_K$, and let W_K be the torsion subgroup of $\mathcal{O}_K^\times$, that is*

$$W_K = K \cap \mu_\infty.$$

Then W_K is a finite cyclic group and

$$\mathcal{O}_K^\times \cong W_K \times \mathbb{Z}^r,$$

where $r = r_1 + r_2 - 1$.

Before giving the proof of Dirichlet's Theorem, we look at some examples.

Example 4.15. Let $K = \mathbb{Q}$, then $(r_1, r_2) = (1, 0)$ so $r = 0$.
We have $W_\mathbb{Q} = \{\pm 1\}$ and $\mathbb{Z}^\times = W_\mathbb{Q} = \{\pm 1\}$.

Example 4.16. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field, then $(r_1, r_2) = (0, 1)$ so once again $r = 0$.
We have

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1\} & \text{if } d \leq -5 \text{ or } d = -2 \\ \{\pm 1, \pm i\} & \text{if } d = -1 \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } d = -3, \text{ where } \omega^2 + \omega + 1 = 0. \end{cases}$$

Example 4.17. Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field, then $(r_1, r_2) = (2, 0)$ so $r = 1$.
We have $K \subseteq \mathbb{R}$ so $W_K = \{\pm 1\}$ since $\mathbb{R} \cap \mu_\infty = \{\pm 1\}$. So $\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$, in other words

$$\mathcal{O}_K^\times = \{\pm u^m \mid m \in \mathbb{Z}\}$$

for some $u \in \mathcal{O}_K^\times$.
For instance, letting $u = 1 + \sqrt{2}$, we have $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}^\times = \{\pm 1\} \times \langle u \rangle$.

Example 4.18. Let $K = \mathbb{Q}(\zeta_m)$ with $m = p^r > 2$. This has signature $(r_1, r_2) = (0, \varphi(m)/2)$. We have seen that

$$W_K = \begin{cases} \mu_m & \text{if } m \text{ is even} \\ \mu_{2m} & \text{if } m \text{ is odd.} \end{cases}$$

It is easy to see that for any k with $\gcd(k, m) = 1$ the element

$$\frac{1-\zeta^k}{1-\zeta}$$

is a unit (its norm is 1), but in general the group of units contain other elements that are more difficult to describe.

In order to prove the Unit Theorem, we need a multiplicative analogue of the embedding

$$\iota \colon \mathcal{O}_K \hookrightarrow \mathbb{R}^{r_1+2r_2}$$

that we used to study the class group.

Define $L \colon K^\times \to \mathbb{R}^{r_1+r_2}$ by

$$L(\alpha) = \big(\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1}(\alpha)|, \log|\tau_1(\alpha)|^2, \ldots, \log|\tau_{r_2}(\alpha)|^2\big).$$

This is a group homomorphism (multiplication on $K^\times$ and addition on $\mathbb{R}^{r_1+r_2}$) and it is related to the norm map via

$$\log|N^K_{\mathbb{Q}}(\alpha)| = S(L(\alpha)),$$

where $S \colon \mathbb{R}^{r_1+r_2} \to \mathbb{R}$ is the sum function $S(x_1, \ldots, x_{r_1+r_2}) = x_1 + \cdots + x_{r_1+r_2}$.

The following result, attributed to Kronecker, will allow us to deduce some properties of the map L.

Proposition 4.19. *(a) For $M > 0$ and $n \geq 1$, let $S_{\leq M}(n) \subseteq \mathbb{C}$ consist of all algebraic integers α whose minimal polynomial f has degree n and such that all the roots α_j of f satisfy $|\alpha_j| \leq M$. Then $S_{\leq M}(n)$ is a finite set.*

(b) $\coprod_{n\geq 1} S_{\leq 1}(n) = \mu_\infty$.

Proof. (a) Write

$$f(z) = \prod_{j=1}^{n}(z - \alpha_j) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathbb{Z}[z].$$

As we expand the product, the coefficient a_j is a sum of $\binom{n}{j}$ monomials of total degree $n-j$ in the variables $\alpha_1, \ldots, \alpha_n$, so

$$|a_j| \leq \binom{n}{j} M^{n-j} \qquad \text{for } j = 0, \ldots, n-1.$$

As the degree is fixed and the coefficients are restricted to a finite set, the set of possible polynomials f is finite, hence the set $S_{\leq M}(n)$ of possible α's is finite.

(b) In one direction, if $\zeta \in \mu_\infty$ has order n, then clearly $\zeta \in S_{\leq 1}(n)$ (as all the conjugates of a root of unity are roots of unity, and we have an explicit description of these as complex numbers of absolute value 1).

In the other direction, let $\alpha \in S_{\leq 1}(n)$ and let $K = \mathbb{Q}(\alpha)$. Then $\{\alpha, \alpha^2, \alpha^3, \ldots\} \subseteq K$ so $\{\alpha, \alpha^2, \ldots\} \subseteq \coprod_{d|n} S_{\leq 1}(d)$, a finite set. Hence there exist $k_1 \neq k_2$ such that $\alpha^{k_1} = \alpha^{k_2}$, and we are done.

□

Corollary 4.20. $\ker(L|_{\mathcal{O}_K^\times}) = W_K$ *and* $\#W_K < \infty$.

Proof. Let $\alpha \in \mathcal{O}_K^\times$, then α is in $\ker(L)$ if and only if $|\sigma(\alpha)| = 1$ for all embeddings $K \hookrightarrow \mathbb{C}$. In other words, $\alpha \in S_{\le 1}(n)$ for $n \le \deg(K)$, hence by part (a) of Proposition 4.19, $\ker(L|_{\mathcal{O}_K^\times})$ is finite, and by part (b) of Proposition 4.19, $\alpha \in \mu_\infty \cap K = W_K$. □

Corollary 4.21. *Let* $\Lambda = L(\mathcal{O}_K^\times)$*, then* Λ *is a discrete subset of the hyperplane*

$$H = \{x \in \mathbb{R}^{r_1+r_2} \mid x_1 + \cdots + x_{r_1+r_2} = 0\}.$$

Proof. That $\Lambda \subseteq H$ follows directly from $\log|N_{\mathbb{Q}}^K(\alpha)| = S(L(\alpha))$ where S is the sum function. Now fix some $M > 1$ and consider

$$T = \{x \in H \mid x \in \Lambda \text{ and } |x| \le \log(M)\}.$$

We want to prove that T is finite. Consider

$$\begin{aligned} L^{-1}(T) &= \{\alpha \in \mathcal{O}_K^\times \mid L(\alpha) \in T\} \\ &\subseteq \{\alpha \in \mathcal{O}_K^\times \mid |\sigma(\alpha)| \le M \text{ for all } \sigma\colon K \hookrightarrow \mathbb{C}\} \\ &= \coprod_{1 \le n \le \deg(K)} S_{\le M}(n), \end{aligned}$$

which is finite by Proposition 4.19. Hence T is finite, and Λ is discrete in H. □

Lemma 4.22. *Let* $A \in M_n(\mathbb{R})$ *be such that*

- *each row sums to* 0*;*
- *all the diagonal entries are strictly positive;*
- *all the non-diagonal entries are strictly negative.*

Then A *has rank* $n - 1$.

Proof. Since each row sums to 0, the vector consisting of all 1's is in the kernel of A, hence the rank of A is strictly less than n.

Let $v_1, \dots, v_n$ denote the columns of A. I claim that $v_1, \dots, v_{n-1}$ are linearly independent. Suppose that is not the case and consider a nontrivial linear relation

$$c_1 v_1 + \cdots + c_{n-1} v_{n-1} = 0, \qquad \text{not all } c_j = 0.$$

Let k be the index of the largest c_j in absolute value. Divide the relation by c_k so that the new $c_k = 1$ and $c_j \le 1$ for all $j \ne k$. Therefore $c_j a_{jk} \ge a_{jk}$ for all $j \ne k$.

Also

$$\sum_{j=1}^{n-1} a_{kj} > \sum_{j=1} a_{kj} + a_{k,n-1} = k\text{-th row sum} = 0.$$

But then in the k-th row we have

$$0 = \sum_{j=1}^{n-1} c_j a_{kj} \ge \sum_{j=1}^{n-1} a_{kj} > 0,$$

contradiction. □

Recall the embedding $\iota\colon \mathcal{O}_K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ given by

$$\iota(\alpha) = \big(\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \tau_1(\alpha), \dots, \tau_{r_2}(\alpha)\big).$$

We can restrict it to $\mathcal{O}_K^\times$ and relate it to L via the function $\pi\colon (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \to \mathbb{R}^{r_1+r_2}$ given by

$$\pi(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) = \big(\log|x_1|, \dots, \log|x_{r_1}|, \log|z_1|^2, \dots, \log|z_{r_2}|^2\big),$$

so that $L = \pi \circ \iota$.

Lemma 4.23. *Let K be a number field with signature (r_1, r_2). Fix k with $1 \le k \le r_1 + r_2$. There exists a constant C such that for any $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, there exists $\beta \in \mathcal{O}_K$, $\beta \neq 0$ with $|N_{\mathbb{Q}}^K(\beta)| \le C$ and if*

$$L(\alpha) = (a_1, \dots, a_{r_1+r_2}), \qquad L(\beta) = (b_1, \dots, b_{r_1+r_2}),$$

then $b_i < a_i$ for all $i \neq k$.

Proof. Let

$$C = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

Let $a_i' \in \mathbb{R}$ be such that $a_i' < a_i$ for all $i = 1, \dots, r_1 + r_2$. Define a subset $S \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by

$$|x_i|^{\epsilon_i} \le C_i,$$

where

$$\epsilon_i = \begin{cases} 1 & \text{if } 1 \le i \le r_1 \\ 2 & \text{if } r_1 + 1 \le i \le r_1 + r_2, \end{cases}$$
$$C_i = e^{a_i'} \text{ for } i \neq k,$$
$$C_k = \frac{C}{\prod_{i \neq k} C_i}.$$

Then S is symmetric, compact, and convex. We have

$$\operatorname{vol}(S) = 2^{r_1}\pi^{r_2} C = 2^n \operatorname{covol}(\iota(\mathcal{O}_K)).$$

By the Convex Body Theorem, S contains a nonzero element of $\iota(\mathcal{O}_K)$. Let β be the corresponding element of $\mathcal{O}_K$. □

Proof of Dirichlet's Unit Theorem. It remains to show that $\Lambda = L(\mathcal{O}_K^\times)$ is a lattice in H. This requires $r_1 + r_2 - 1$ linearly independent vectors in Λ, which we get from Lemma 4.22, by producing units $u_1, \dots, u_{r_1+r_2} \in \mathcal{O}_K^\times$ such that

$$A = \begin{bmatrix} L(u_1) \\ \vdots \\ L(u_{r_1+r_2}) \end{bmatrix}$$

satisfies the conditions of Lemma 4.22.

In other words, let $1 \le k \le r_1 + r_2$. We want $u \in \mathcal{O}_K^\times$ such that $L(u) = (a_1, \dots, a_{r_1+r_2})$ with $a_k > 0$ and $a_i < 0$ for all $i \neq k$. For this we use Lemma 4.23. Start with any nonzero $\alpha_0 \in \mathcal{O}_K$. Apply Lemma 4.23 iteratively to get elements $\alpha_j \in \mathcal{O}_K$, $\alpha_j \neq 0$, $L(\alpha_j) = (a_1(j), \dots, a_{r_1+r_2}(j))$, with $|N(\alpha_j)| \le C$ and $a_i(j) < a_i(j-1)$ for all $i \neq k$. Consider the principal ideals $\alpha_j\mathcal{O}_K$. They all have norm bounded by C, so there are only finitely many such ideals, hence $\alpha_{j_1}\mathcal{O}_K = \alpha_{j_2}\mathcal{O}_K$ for some $j_2 > j_1$. Then $u := \alpha_{j_1}/\alpha_{j_2} \in \mathcal{O}_K^\times$ satisfies the desired properties. □

4.3. Continued fractions and units in real quadratic fields

We give a quick overview of continued fractions and describe how they relate to fundamental units of real quadratic fields.

A *continued fraction* is a limiting process summarised in the form

$$a_1 + \cfrac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots}}} =: [a_1, a_2, a_3, a_4, \dots],$$

where $a_j \in \mathbb{Z}_{>0}$. The truncation $[a_1, a_2, \dots, a_n]$ is called the n-th *convergent* and the value of the continued fraction is by definition

$$\lim_{n\to\infty} [a_1, a_2, \dots, a_n] \in \mathbb{R}.$$

This limit always exists.

Every irrational $\alpha \in \mathbb{R}_{>1}$ has a unique continued fraction expansion. This expansion is periodic if and only if $[\mathbb{Q}(\alpha) \colon \mathbb{Q}] = 2$.

Example 4.24. Let $\alpha = [1, 1, 1, 1, \dots]$. We have

$$\alpha = 1 + \frac{1}{\alpha},$$

so $\alpha^2 - \alpha - 1 = 0$, hence

$$\alpha = \frac{1+\sqrt{5}}{2} \approx 1.618033\dots,$$

also known as the golden ratio.

Given $\alpha \in \mathbb{R}_{>1}$, the continued fraction expansion is obtained as follows: let $\alpha_1 := \alpha$ and $a_1 := \lfloor \alpha_1 \rfloor$, then for each $n \in \mathbb{Z}_{>0}$:

$$\alpha_{n+1} := \frac{1}{\alpha_n - a_n}, \qquad a_{n+1} := \lfloor \alpha_{n+1} \rfloor.$$

This gives rise to the expansion

$$\alpha = [a_1, a_2, a_3, \dots].$$

Given a continued fraction $[a_1, a_2, \dots]$, define matrices

$$A_n := \begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{bmatrix} := P_0 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} := P_n := A_1 A_2 \dots A_n.$$

Then for all $n \geq 0$ we have

$$\begin{aligned} p_{n+1} &= a_{n+1} p_n + p_{n-1} \\ q_{n+1} &= a_{n+1} q_n + q_{n-1} \\ \frac{p_n}{q_n} &= [a_1, \dots, a_n]. \end{aligned}$$

In fact,

$$p_n q_{n-1} - p_{n-1} q_n = \det(P_n) = (-1)^n,$$

from which we conclude that $\gcd(p_n, q_n) = 1$ for all $n \geq 1$.

If $\alpha \in \mathbb{R}_{>1}$ is irrational then

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2},$$

which starts to explain why continued fractions play a crucial role in diophantine approximation.

Our interest, however, lies with the role they play in the description of fundamental units for real quadratic fields.

Theorem 4.25. *Let $d \in \mathbb{Z}_{>0}$ be squarefree with $d \equiv 2, 3 \pmod 4$. Let k be the period of the continued fraction expansion for $\sqrt{d}$. Then the fundamental unit in the ring of integers of $\mathbb{Q}(\sqrt{d})$ is*

$$\varepsilon = p_k + q_k\sqrt{d}.$$

Example 4.26. Take $K = \mathbb{Q}(\sqrt{19})$. We have

$$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}] \approx 4.35889\ldots,$$

so $k = 6$. We compute

$$P_6 = \begin{bmatrix} 4 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 170 & 61 \\ 39 & 14 \end{bmatrix}$$

and conclude that the fundamental unit is

$$\varepsilon = 170 + 39\sqrt{19}.$$

There is another approach that does not require any congruence assumptions on d. Let $\theta > 1$ be a quadratic irrational, that is $[\mathbb{Q}(\theta) : \mathbb{Q}] = 2$. We say that θ is *reduced* if

$$-\frac{1}{\sigma(\theta)} > 1,$$

where σ is the non-identity Galois element.

Galois proved that θ is reduced if and only if its continued fraction expansion is *purely periodic*, that is of the form $\theta = [\overline{a_1, a_2, \ldots, a_k}]$.

Example 4.27. Consider $\alpha = [\overline{1}] = [1, 1, 1, \ldots]$. We have seen that

$$\alpha = \frac{1 + \sqrt{5}}{2} > 1.$$

We check

$$-\frac{1}{\sigma(\alpha)} = -\frac{2}{1 - \sqrt{5}} = \frac{2(\sqrt{5} + 1)}{4} = \alpha > 1,$$

so α is indeed reduced.

Theorem 4.28. *Let $K = \mathbb{Q}(\sqrt{d})$, $d > 0$ squarefree. Let $\theta \in K$ be a reduced element with the property that $\Delta(\theta) = \Delta_K$. Let $\theta = [\overline{a_1, \dots, a_k}]$ be the continued fraction expansion and let*

$$\varepsilon = q_{k-1} + q_k \theta.$$

Then ε is the fundamental unit of K.

Finding a reduced element as needed above can be done as follows:

Proposition 4.29. *Given $d > 0$ squarefree, set*

$$\omega := \begin{cases} \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

Then

$$\theta := \frac{1}{\omega - \lfloor \omega \rfloor}$$

is a reduced element.

Example 4.30. We reconsider the case $K = \mathbb{Q}(\sqrt{19})$ from this point of view. We have $\omega = \sqrt{19}$ and

$$\theta = \frac{1}{\sqrt{19} - 4} \approx 2.78629 \cdots = [\overline{2, 1, 3, 1, 2, 8}].$$

The period is $k = 6$, so we compute

$$P_6 = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 8 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 326 & 117 \\ 39 & 14 \end{bmatrix}$$

and conclude that the fundamental unit is

$$\varepsilon = 14 + 117\theta = 14 + \frac{117}{\sqrt{19} - 4} = 170 + 39\sqrt{19}.$$

5. Local rings and fields

Up to this point, we have been studying arithmetic from a global perspective. It turns out that certain questions become (sometimes much) easier when considered locally. We will spend some time exploring what this means. In the process we will introduce (or review) some more commutative algebra.

Let's start with a bit of notation: given a commutative[1] ring A, we let $\operatorname{Spec}(A)$ denote the set[2] of prime ideals of A.

5.1. Local rings

A ring A is a *local ring* if it has a unique maximal ideal $\mathfrak{m}$. It is easy to see that, in this case, $A^\times = A \smallsetminus \mathfrak{m}$. (If $u \notin \mathfrak{m}$, what ideal does $\mathfrak{m} \cup \{u\}$ generate?)

A handy result for local rings is

Lemma 5.1 (Nakayama)**.** *Let A be a local ring, M a finitely generated A-module, and $I \subsetneq A$ a proper ideal. Consider the A-module*

$$IM = \left\{ \sum a_i x_i \mid a_i \in I, x_i \in M \right\}.$$

(a) If $IM = M$ then $M = 0$.

(b) If $N \subseteq M$ and $N + IM = M$, then $N = M$.

Proof. □

How do we get a local ring? Any field is a local ring with unique maximal ideal 0, but that is boring. To get a local ring that is not a field, we can use *localisation*.

Let A be an integral domain and let $K = \operatorname{Frac}(A)$. We say that $S \subseteq A$ is a *multiplicative set* if $0 \notin S$, $1 \in S$, and S is closed under multiplication.

Given a multiplicative set S, define

$$S^{-1}A = \left\{ \frac{a}{b} \in K \mid b \in S \right\}.$$

There is a canonical injective ring homomorphism

$$A \hookrightarrow S^{-1}A \qquad \text{given by} \qquad a \mapsto \frac{a}{1}.$$

> **Example 5.2.** Let $\mathfrak{p}$ be a nonzero prime ideal of A and let $S = A \smallsetminus \mathfrak{p}$, then S is a multiplicative set and $S^{-1}A$ is denoted
>
> $$A_\mathfrak{p} = \left\{ \frac{a}{b} \in K \mid b \notin \mathfrak{p} \right\}$$

[1] All our rings are commutative unless explicitly declared otherwise, but the beginning of a new chapter is a good place to recall this convention.

[2] Yes, this has way more structure than just being a set. All in due time.

and called the *localisation of A at $\mathfrak{p}$*.

An instance of this is

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$

Proposition 5.3. *Let S be a multiplicative set in an integral domain A. There is a bijective correspondence*

$$\operatorname{Spec}(S^{-1}A) \xrightarrow{\cong} \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\}$$

given by $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ for any $\mathfrak{q} \in \operatorname{Spec}(S^{-1}A)$ and[3] *$\mathfrak{p} \mapsto \mathfrak{p}(S^{-1}A)$ for any $\mathfrak{p} \in \operatorname{Spec}(A)$ such that $\mathfrak{p} \cap S = \varnothing$.*

Now the name "localisation of A at $\mathfrak{p}$" is finally justified:

Corollary 5.4. *$A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.*

5.2. Discrete valuation rings

A *discrete valuation ring* (DVR) is a PID with exactly one nonzero prime ideal[4]. (Equivalently, it is a PID that is a local ring but not a field.)

Proposition 5.5. *An integral domain A is a DVR if and only if:*

(a) A is Noetherian.

(b) A is integrally closed.

(c) A has exactly one nonzero prime ideal.

This is quite close to the definition of Dedekind domains, modulo the gap between condition (c) and having Krull dimension 1. Indeed:

Proposition 5.6. *If A is a Dedekind domain and $\mathfrak{p}$ is a nonzero prime ideal, then $A_{\mathfrak{p}}$ is a DVR.*

An important special case is of course that where $A = \mathcal{O}_K$ is the ring of integers in a number field.

This may be a good moment to stop and take stock of what we have found: by "localising at $\mathfrak{p}$" in the manner we discussed, we end up with a ring where

- the units are determined in a straightforward way: $A_{\mathfrak{p}}^{\times} = A_{\mathfrak{p}} \smallsetminus \mathfrak{p}A_{\mathfrak{p}}$;
- the class number is 1.

Considering that the corresponding concepts for rings of integers are highly nontrivial gives some credence to the initial claim that arithmetic questions are easier locally.

It is weird for something to be called a *discrete valuation* ring without having defined discrete valuations. We remedy this now: Let K be a field. A *discrete valuation* is a nonzero group homomorphism $v\colon K^{\times} \to \mathbb{Z}$ such that

$$v(a+b) \geq \min\{v(a), v(b)\} \qquad \text{for all } a, b \in K^{\times}.$$

We call the valuation v *normalised* if $v(K^{\times}) = \mathbb{Z}$. Occasionally we may extend to $v\colon K \to \mathbb{Z} \cup \{\infty\}$ by setting $v(0) = \infty$.

[3] Here, as in previous chapters, $\mathfrak{p}(S^{-1}A)$ signifies the ideal generated by $\mathfrak{p} \subseteq S^{-1}A$, where we view $\mathfrak{p}$ as sitting inside $S^{-1}A$ via the canonical embedding $A \hookrightarrow S^{-1}A$.

[4] It is clear that a DVR has Krull dimension 1. The converse is of course not true: $\mathbb{Z}$ is a PID of Krull dimension 1, but not a DVR.

Example 5.7. Let A be a PID and $K = \operatorname{Frac}(A)$. Let π be an irreducible element of A. Define $v_\pi \colon K^\times \to \mathbb{Z}$ by

$$v_\pi(x) = m, \qquad \text{where } x = \pi^m \frac{a}{b}, m \in \mathbb{Z}, a, b \in A \text{ coprime to } \pi.$$

For a concrete example, take $A = \mathbb{Z}$ and $\pi = p$ a prime number, getting the *p-adic valuation* v_p.

Example 5.8. Let A be a Dedekind domain and $K = \operatorname{Frac}(A)$. Let $\mathfrak{p}$ be a prime ideal of A. For $x \in K^\times$, consider the fractional ideal xA and let $\mathfrak{p}^{v_\mathfrak{p}(x)}$ be the power of $\mathfrak{p}$ in the factorisation of xA into prime ideals of A. Then $v_\mathfrak{p}$ is called the *$\mathfrak{p}$-adic valuation* on K.

Lemma 5.9. *Let v be a discrete valuation. If $v(a) > v(b)$ then $v(a+b) = v(b)$.*

Proof. If $\omega \in K^\times$ has finite order, then $v(\omega) = 0$ because $\mathbb{Z}$ is a torsion-free group and v is a group homomorphism. In particular $v(-1) = 0$, so that $v(-a) = v(-1) + v(a) = v(a)$.

If $v(a) > v(b)$ then

$$v(b) = v\big((a+b) - a\big) \geq \min\{v(a+b), v(a)\} \geq \min\{v(a), v(b)\} = v(b),$$

so the inequalities are in fact equalities, and $v(a+b) = v(b)$. □

An *absolute value* on a field K is a function $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ such that

- $|x| = 0$ if and only if $x = 0$;
- $|xy| = |x|\,|y|$;
- $|x+y| \leq |x| + |y|$.

If, in addition, we have

$$|x+y| \leq \max\{|x|, |y|\}, \tag{5.1}$$

we say that the absolute value is *non-archimedean.* (Otherwise we say that it is *archimedean.*)

An argument very similar to that of Lemma 5.9 shows that equality in Equation (5.1) holds if $|x| \neq |y|$.

Example 5.10. (a) For any field K, take $|0| = 0$ and $|x| = 1$ for all $x \in K^\times$. This is called the *trivial absolute value* on K.

(b) On $K = \mathbb{C}$ we have, for $z = x + iy$:

$$|z|_\mathbb{C} = \sqrt{x^2 + y^2}.$$

This is an archimedean absolute value on $\mathbb{C}$; its restriction to $\mathbb{R}$ is an archimedean absolute value on $\mathbb{R}$.

(c) For any number field K and any embedding $\sigma \colon K \to \mathbb{C}$, we have an archimedean absolute value on K defined by

$$|x| = |\sigma(x)|_\mathbb{C}.$$

(d) Given a discrete valuation $v\colon K \to \mathbb{Z} \cup \{\infty\}$ on a field K, and a number $b \in \mathbb{R}_{>1}$, set

$$|x|_v = b^{-v(x)}.$$

This defines a non-archimedean absolute value on K.

Two special cases are particularly popular:

(i) $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ gives the *p-adic absolute value* on $\mathbb{Q}$:

$$|x|_p = p^{-v_p(x)}.$$

(ii) For any number field K and any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we get the $\mathfrak{p}$*-adic absolute value* on K:

$$|x|_\mathfrak{p} = \big(N(\mathfrak{p})\big)^{-v_\mathfrak{p}(x)}.$$

There is a converse of sorts for the passage from discrete valuation to non-archimedean absolute value discussed in (d) above: if $|\cdot|$ is a non-trivial non-archimedean absolute value on K, define $v\colon K^\times \to \mathbb{R}$ by

$$v(x) = -\log|x| \qquad \text{for all } x \in K^\times.$$

Then

$$\begin{aligned} v(xy) &= v(x) + v(y) \\ v(x+y) &\geq \min\{v(x), v(y)\}. \end{aligned}$$

If $v(K^\times)$ is discrete in $\mathbb{R}$, then v is a scalar multiple of a discrete valuation on K.

An absolute value on K defines a metric on K via $(a,b) \mapsto |a-b|$, hence a topology on K. For instance, $|\cdot|_p$ on $\mathbb{Q}$ defines the *p-adic topology*, with respect to which we have

$$\lim_{n\to\infty} p^n = 0.$$

Two absolute values that define the same topology are said to be *equivalent.*

Theorem 5.11 (Ostrowski). *Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$.*

(a) If $|\cdot|$ is archimedean, then it is equivalent to $|\cdot|_\infty$, the restriction of $|\cdot|_\mathbb{C}$ to $\mathbb{Q}$.

(b) If $|\cdot|$ is non-archimedean, then it is equivalent to $|\cdot|_p$ for exactly one prime number p.

An equivalence class of non-trivial absolute values on K is called[5] a *place* w of K. In this terminology, Ostrowski's Theorem says that the set of places of $\mathbb{Q}$ is indexed by

$$\{\text{prime numbers } p \in \mathbb{Z}\} \cup \{\infty\}.$$

This can be generalised to

Theorem 5.12. *Let K be a number field. The set of places of K is indexed by*

(a) the non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$;

[5] Confusingly, places are typically denoted by the letter v in the literature, despite the fact that they are absolute values, not valuations. Also confusing is the fact that places are often called primes. I will break with tradition and denote a place by w, and never call it a prime of K in this subject.

(b) the real embeddings of K;

(c) the conjugate pairs of complex embeddings of K.

Theorem 5.13 (The Product Formula for $\mathbb{Q}$)**.** *For any $x \in \mathbb{Q}^\times$ we have*

$$\prod_{w \text{ place of } \mathbb{Q}} |x|_w = 1.$$

Proof. Write $x = \frac{a}{b}$ with $a, b \in \mathbb{Z} \setminus \{0\}$. For any prime number p we have

$$|x|_p = 1 \qquad \text{unless} \qquad p \text{ divides } a \text{ or } b.$$

So the product is actually finite, despite appearances.

Set $\varphi(x) = \prod_w |x|_w$. This is a group homomorphism $\varphi\colon \mathbb{Q}^\times \to \mathbb{R}^\times$. By unique factorisation in $\mathbb{Z}$, a generating set for the group $\mathbb{Q}^\times$ is

$$\{-1\} \cup \{p \text{ prime number}\}.$$

So to prove that φ is identically 1, it suffices to show that $\varphi(-1) = 1$ and $\varphi(p) = 1$ for any prime number p.

We know that $|-1| = 1$ for any absolute value, so $\varphi(-1) = 1$.

If p is prime,

$$|p|_w = \begin{cases} p & \text{if } w = \infty \\ \frac{1}{p} & \text{if } w = p \\ 1 & \text{if } w \neq p \text{ is prime,} \end{cases}$$

so $\varphi(p) = 1$. □

The product formula also holds for arbitrary number fields K; to prove it, one needs to study how places of $\mathbb{Q}$ extend to places of K.

5.3. Completions

A *valued field* is a pair $(K, |\cdot|)$ where K is a field and $|\cdot|$ is an absolute value. We say that a valued field is complete if it is complete as a metric space with respect to the absolute value. A *compatible homomorphism*[6] between valued fields $(K, |\cdot|_K)$ and $(L, |\cdot|_L)$ is a ring homomorphism $f\colon K \to L$ such that

$$|f(x)|_L = |x|_K \qquad \text{for all } x \in K.$$

Since K and L are fields, such a map f is automatically injective.

Given a valued field $(K, |\cdot|)$, there exists a complete valued field[7] $(\hat{K}, \|\cdot\|)$ and a compatible homomorphism $i\colon K \to \hat{K}$ that are universal in the following sense: any compatible homomorphism $f : K \to L$ to a complete valued field $(L, |\cdot|_L)$ factors uniquely through i, that is, there exists a unique compatible homomorphism $g\colon \hat{K} \to L$ such that $f = g \circ i$.

Concretely, we take

$$\begin{aligned} \hat{K} &= \{\text{equivalence classes of } |\cdot|\text{-Cauchy sequences in } K\} \\ \|(x_n)\| &= \lim_{n\to\infty} |x_n| \\ i(x) &= (x, x, \dots). \end{aligned}$$

[6] The term “compatible homomorphism” is not standard in this setting.

[7] We write $\|\cdot\|$ for the absolute value on the completion $\hat{K}$ in the definition to prevent confusing it with $|\cdot|$, but in practice one uses the same symbol for the absolute value on K and its canonical extension to the completion.

Example 5.14. (a) Take $\mathbb{Q}$ and $|\cdot|_\infty$, then the completion is $\mathbb{R}$ with its customary absolute value.

(b) Take $\mathbb{Q}$ and $|\cdot|_p$, then the completion is denoted $\mathbb{Q}_p$ and is called the field of *p-adic numbers*.

Let us consider the non-archimedean case more carefully.

Let $v\colon K^\times \to \mathbb{Z}$ be a normalised discrete valuation and let $|\cdot|\colon K \to \mathbb{R}_{>0}$ be a corresponding absolute value on K. We have the valuation ring and valuation ideal:

$$\begin{aligned} A &= \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid |x| \leq 1\} \\ \mathfrak{m} &= \{x \in K \mid v(x) > 0\} = \{x \in K \mid |x| < 1\}. \end{aligned}$$

Consider $x \in K^\times$ and let (x_n) be a representing Cauchy sequence. Then $\|x\| = \lim_{n\to\infty} |x_n|$ is a limit point of the set $|K^\times|$, which is discrete hence closed in $\mathbb{R}$. Therefore $\|x\| \in |K^\times|$, from which we conclude $\|\hat{K}^\times\| = |K^\times|$, so that $\|\cdot\|$ is a discrete absolute value on $\hat{K}$.

Let $\hat{v}\colon \hat{K}^\times \to \mathbb{Z}$ denote the corresponding normalised discrete valuation; we have

$$\begin{aligned} \hat{A} &= \{x \in \hat{K} \mid \hat{v}(x) \geq 0\} = \{x \in \hat{K} \mid \|x\| \leq 1\} \\ \hat{\mathfrak{m}} &= \{x \in \hat{K} \mid \hat{v}(x) > 0\} = \{x \in \hat{K} \mid \|x\| < 1\}. \end{aligned}$$

Both A and $\hat{A}$ are DVRs hence PIDs, so the two ideals $\mathfrak{m}$ and $\hat{\mathfrak{m}}$ are principal. A generator of $\mathfrak{m}$ is called a *uniformiser*.

Exercise 5.15. If $\pi \in A$ satisfies $\mathfrak{m} = \pi A$, then $\hat{\mathfrak{m}} = \pi\hat{A}$.

Exercise 5.16. The composition $A \hookrightarrow \hat{A} \to \hat{A}/\hat{\mathfrak{m}}$ induces an injective ring homomorphism $A/\mathfrak{m} \to \hat{A}/\hat{\mathfrak{m}}$. Prove that this is surjective, hence an isomorphism. (The same holds for the similarly defined map $A/\mathfrak{m}^n \to \hat{A}/\hat{\mathfrak{m}}^n$ for any $n \in \mathbb{Z}_{\geq 1}$.)

Proposition 5.17. *Let K be a valued field with valuation ring A and valuation ideal $\mathfrak{m}$. Fix a uniformiser π of A and a set S of representatives for $A/\mathfrak{m} = \hat{A}/\hat{\mathfrak{m}}$. The sequence of partial sums of the series*

$$a_{-n}\pi^{-n} + \cdots + a_0 + a_1\pi + a_2\pi^2 + \cdots + a_k\pi^k + \ldots, \qquad a_i \in S,$$

is Cauchy, hence defines an element of the completion $\hat{K}$. Conversely, every element of $\hat{K}$ has a unique expression of the above form.

Proof. Let $x_M = \sum_{i=-n}^{M} a_i\pi^i$. Then for $M < N$ we have

$$|x_M - x_N| = \left|\sum_{i=M+1}^{N} a_i\pi^i\right| = |\pi|^{M+1}\left|a_{M+1} + a_{M+2}\pi + \cdots + a_N\pi^{N-M-1}\right| \leq |\pi|^{M+1},$$

and $|\pi|^{M+1} \to 0$ as $M \to \infty$ since $|\pi| < 1$. So (x_M) is Cauchy.

Conversely, let $x \in \hat{K}$. Write $x = \pi^n y$ with $y \in \hat{A}$, $n \in \mathbb{Z}$. There exists a unique $a_0 \in S$ such that $y - a_0 \in \hat{\mathfrak{m}} = \pi\hat{A}$ (this a_0 represents the coset $y + \mathfrak{m}$).

Therefore $(y - a_0)/\pi \in \hat{A}$, hence there exists a unique $a_1 \in S$ such that $(y - a_0)/\pi - a_1 = (y - a_0 - a_1\pi)/\pi \in \hat{\mathfrak{m}} = \pi\hat{A}$.

Continue in this manner. In the limit, we have

$$x = \pi^n y = \pi^n(a_0 + a_1\pi + a_2\pi^2 + \dots).$$

The process was uniquely determined by x, with no choices involved, so the resulting expression is uniquely determined. □

5.4. p-adic numbers

Restricting to the special case of the field $\mathbb{Q}_p$ (the completion of $\mathbb{Q}$ with respect to the p-adic absolute value), we get that every element of $\mathbb{Q}_p$ has a unique representative of the form

$$a_{-n}p^{-n} + \dots + a_0 + a_1 p + a_2 p^2 + \dots, \qquad 0 \le a_i < p.$$

The corresponding valuation ring is $\mathbb{Z}_p$, the elements of which have no negative powers on p in their representation. Its unique maximal ideal is $p\mathbb{Z}_p$.

Example 5.18. In $\mathbb{Q}_2$, we have

$$1 + 2 + 2^2 + \dots = -1.$$

To see this, note that

$$1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1,$$

which converges 2-adically to $0 - 1 = -1$ as $n \to \infty$.

Example 5.19. I claim that -1 is a square in $\mathbb{Q}_5$ (in fact, in $\mathbb{Z}_5$).

To show this, we construct $a_0 + a_1 5 + a_2 5^2 + \dots$ such that

$$\left(a_0 + a_1 5 + a_2 5^2 + \dots\right)^2 + 1 = 0.$$

Starting to expand the square, the first step is

$$a_0^2 + 1 \equiv 0 \pmod 5,$$

which has two solutions: 2 and 3. Let's pick $a_0 = 2$, plug it into our mystery 5-adic number and continue:

$$4 + 20a_1 + 1 \equiv 0 \pmod{5^2} \quad \Rightarrow \quad 1 + 4a_1 \equiv 0 \pmod 5,$$

which has the unique solution $a_1 = 1$.

We continue in this manner, one coefficient at the time. Why don't we get stuck with an equation that we cannot solve? Suppose we have

$$b_n = a_0 + a_1 5 + \dots + a_n 5^n$$

such that $b_n^2 + 1 \equiv 0 \pmod{5^{n+1}}$. Let $c = (b_n^2 + 1)/5^{n+1}$. We are looking for a_{n+1} such that

$$\left(b_n + a_{n+1}5^{n+1}\right)^2 + 1 \equiv 0 \pmod{5^{n+2}},$$

which can be worked into

$$5^{n+1}\left(c + 2b_n a_{n+1}\right) \equiv 0 \pmod{5^{n+2}} \quad \Rightarrow \quad c + 2b_n a_{n+1} \equiv 0 \pmod 5.$$

Since $b_n \equiv a_0 \equiv 2 \pmod 5$, there is a unique solution $a_{n+1} \equiv c \pmod 5$.

We will soon see that the iterative process used in this example gives a general method for solving polynomial equations in complete DVRs, courtesy of Hensel's Lemma.

5.5. Some weirdness of the p-adic topology

We give a few examples of counter-intuitive behaviour encountered in non-archimedean settings.

Example 5.20 (Every triangle is isosceles)**.** This is a geometric interpretation of the fact that the non-archimedean triangle inequality

$$|x \pm y|_p \leq \max\{|x|_p, |y|_p\}$$

is an equality if $|x|_p < |y|_p$:

$$|x \pm y|_p = |y|_p.$$

The triangle with vertices 0, x, and y has side lengths $|x|_p$, $|y|_p$, $|x-y|_p$.

Example 5.21 (Any point in a disc is a centre)**.** Let $a \in \mathbb{Q}_p$ and consider the open disc of radius $r > 0$:

$$B_r(a) = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\}.$$

Now take $b \in B_r(a)$. For any $x \in B_r(a)$ we have

$$|x-b|_p = |(x-a)+(a-b)|_p \leq \max\{|x-a|_p, |a-b|_p\} < r,$$

so that $x \in B_r(b)$.

The same argument shows that $B_r(b) \subseteq B_r(a)$, so that $B_r(b) = B_r(a)$ and b is a centre of the disc.

Moving on to more analytic matters, we have

Lemma 5.22. *A series $\sum_{n=0}^{\infty} a_n$ converges in $\mathbb{Q}_p$ if and only if*

$$\lim_{n\to\infty} |a_n|_p = 0.$$

Proof. The interesting direction is the one that fails in the archimedean setting: suppose the general term converges p-adically to 0.

Let $S_M = \sum_{n=0}^{M} a_n$, then for $M < N$ we have

$$|S_M - S_N|_p = |a_{M+1} + \cdots + a_N|_p \leq \max\{|a_{M+1}|_p, \ldots, |a_N|_p\} \to 0 \quad \text{as } M \to \infty.$$

Since the sequence of partial sums is Cauchy, it converges in $\mathbb{Q}_p$. □

Example 5.23. Consider the power series

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \ldots$$

Where does this converge?

It is not hard to see that for $n = a_0 + a_1 p + \cdots + a_r p^r$,

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^r} \right\rfloor = \frac{n - \sum a_i}{p-1}.$$

Therefore

$$v_p\left(\frac{x^n}{n!}\right) = n\left(v_p(x) - \frac{1}{p-1}\right) + \frac{\sum a_i}{p-1}.$$

As $n \to \infty$, the second term has growth proportional to $\log(n)$, so the behaviour is dictated by the first term. In particular, $|x^n/n!|_p \to 0$ if and only if $v_p(x) > 1/(p-1)$.

We conclude that the exponential series converges in the disc $|x|_p < p^{-1/(p-1)}$.

5.6. Hensel's Lemma

Lemma 5.24 (Not Hensel's Lemma). *Let A be a commutative ring, $f \in A[x]$ and $a, b \in A$. Then*

$$f(a+b) = f(a) + bf'(a) + b^2 y$$

for some $y \in A$.

Proof. We have

$$f(x) = c_n f_n(x) + \cdots + c_1 f_1(x) + c_0 f_0(x),$$

where $c_j \in A$ and $f_j(x) = x^j$.

Since the relation we are trying to prove is A-linear in f, it suffices to prove it for all the elements $f_j(x) = x^j$. By the binomial theorem we have

$$f_j(a+b) = (a+b)^j = a^j + ja^{j-1}b + b^2 y = f_j(a) + bf_j'(a) + b^2 y,$$

where

$$y = \sum_{i=2}^{j} \binom{j}{i} a^{j-i} b^{i-2} \in A.$$

□

Theorem 5.25 (Hensel's Lemma). *Let A be a complete DVR with maximal ideal $\mathfrak{m} = \pi A$. Let $f \in A[x]$ and suppose $\alpha_0 \in A$ is a simple root of f modulo π, that is*

$$f(\alpha_0) \equiv 0 \pmod{\pi}, \qquad f'(\alpha_0) \not\equiv 0 \pmod{\pi}.$$

Then there exists a unique $\alpha \in A$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{\pi}$. (We sometimes express this as: every simple root in $A/\mathfrak{m}$ lifts to a unique root in A.)

Proof. I claim that there exists a sequence of elements $\alpha_0, \alpha_1, \alpha_2, \ldots$ of A such that for all $n \geq 0$ we have

$$\begin{aligned} f(\alpha_n) &\equiv 0 \pmod{\pi^{n+1}} \\ f'(\alpha_n) &\not\equiv 0 \pmod{\pi} \\ \alpha_n &\equiv \alpha_{n-1} \pmod{\pi^n}, \end{aligned}$$

where we set $\alpha_{-1} \in A$ to an arbitrary value (say, $\alpha_{-1} = 1$), and the congruence $\alpha_0 \equiv \alpha_{-1} \pmod{\pi^0}$ is vacuously true.

Assuming that the claim is correct, we have for $M < N$:

$$\alpha_N \equiv \alpha_M \pmod{\pi^{M+1}},$$

so $|\alpha_N - \alpha_M| \le |\pi|^{M+1} \to 0$ as $M \to \infty$. Therefore the sequence (α_n) is Cauchy and converges to some $\alpha \in A$. Polynomial functions are continuous so $f(\alpha) = \lim_{n\to\infty} f(\alpha_n) = 0$.

It remains to prove the claim, which we do by induction on n.

The base case $n = 0$ is clear.

For the induction step, assume that the statement holds for an arbitrary, fixed $n \ge 0$. Let $\beta \in A$ be an as-of-yet-unspecified parameter, and let $\alpha_{n+1} = \alpha_n + \beta\pi^{n+1}$. Then $\alpha_{n+1} \equiv \alpha_n \pmod{\pi^{n+1}}$ and by Lemma 5.24

$$f(\alpha_{n+1}) = f(\alpha + \beta\pi^{n+1}) \equiv f(\alpha_n) + \beta\pi^{n+1} f'(\alpha_n) \pmod{\pi^{n+2}}.$$

Write $f(\alpha_n) = \gamma\pi^{n+1}$ with $\gamma \in A$, then

$$f(\alpha_{n+1}) \equiv 0 \pmod{\pi^{n+2}} \quad \Leftrightarrow \quad \beta \equiv -\frac{\gamma}{f'(\alpha_n)} \pmod{\pi}.$$

So we take any $\beta \in A$ satisfying the above congruence modulo π. The congruence class modulo π^{n+2} of α_{n+1} is uniquely determined. Since $\alpha_{n+1} \equiv \alpha_n \pmod{\pi}$ we have $f'(\alpha_{n+1}) \equiv f'(\alpha_n) \not\equiv 0 \pmod{\pi}$. □

There are numerous applications of this result. Here is one:

Proposition 5.26. *Let p be an odd prime number. Then*

$$\mu_\infty \cap \mathbb{Q}_p = \mu_{p-1}.$$

Proof. Fix $n \in \mathbb{N}$ and consider the polynomial $f(x) = x^n - 1$. We distinguish two cases:

(a) $\gcd(n,p) = 1$. Then $f'(x) = nx^{n-1}$ and for any $\alpha_0 \not\equiv 0 \pmod{p}$ we have $f'(\alpha_0) \not\equiv 0 \pmod{p}$. So by Hensel's Lemma, each root of f in $\mathbb{F}_p^\times$ gives rise to precisely one root of f in $\mathbb{Z}_p$. But by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \mathbb{F}_p^\times$, in other words each element of $\mathbb{F}_p^\times$ is a $(p-1)$-st root of 1.

(b) $\gcd(n,p) > 1$. I claim that $\mu_n \cap \mathbb{Q}_p = \{1\}$. It suffices to prove this in the case $n = p$.

Let $x \in \mathbb{Z}_p$ be a p-th root of 1. Writing $x = x_0 + py$ with $y \in \mathbb{Z}_p$ and $x_0 \in \{0, 1, \ldots, p-1\}$, we see that we must have $x_0 = 1$, since $x_0^p \equiv x_0 \pmod{p}$. By the binomial theorem

$$1 = x^p = (1+py)^p = 1 + p^2y + \sum_{k=2}^{p-1} \binom{p}{k} (py)^k + p^p y^p.$$

If $y \ne 0$ then

$$-p^2y = \sum_{k=2}^{p-1} \binom{p}{k} (py)^k + p^p y^p,$$

so by taking p-valuations we get

$$v_p(y)+2 = v_p(-p^2y) \ge \min_{2\le k\le p-1} \left\{ v_p\binom{p}{k} + k + kv_p(y), p + pv_p(y) \right\} \ge \min\{3+2v_p(y), p+pv_p(y)\},$$

which leads us to a contradiction since $p \ge 3$.

□

5.7. Non-archimedean completions via algebra

There is another construction of the completion of a field with respect to a non-archimedean valuation, which is based on the concept of inverse limit of rings.

An *inverse system* (also known as *projective system*) consists of a sequence $(A_n)_{n\in\mathbb{N}}$ of rings and homomorphisms

$$f_{n+1}\colon A_{n+1} \to A_n \qquad \text{for all } n \in \mathbb{N}.$$

Example 5.27. Take a prime p, let $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and consider the quotient maps $f_{n+1}\colon A_{n+1} \to A_n$ given by $f_{n+1}(a + p^{n+1}\mathbb{Z}) = a + p^n\mathbb{Z}$.

The *inverse limit* (or *projective limit*) is

$$A := \varprojlim_{n\in\mathbb{N}} A_n := \left\{(a_1, a_2, a_3, \dots) \in \prod_{n\in\mathbb{N}} A_n \mid a_n = f_{n+1}(a_{n+1}) \text{ for all } n \in \mathbb{N}\right\}.$$

This is a ring equipped with natural projections $\pi_n\colon A \to A_n$ given by $\pi_n((a_k)) = a_n$. The elements of A are called *coherent sequences*.

The data $(A, (\pi_n))$ satisfies a universal mapping property, which gives another way of defining the inverse limit (and shows that it is unique up to unique isomorphism).

Example 5.28. I claim that $\mathbb{Z}_p$ is the inverse limit of the inverse system from the previous example.

An element $x \in \mathbb{Z}_p$ can be written in the form

$$x_0 + px_1 + p^2x_2 + \dots, \qquad 0 \le x_i \le p-1.$$

This corresponds to the coherent sequence $(a_1, a_2, \dots)$ defined by the "partial sums":

$$\begin{aligned} a_1 &= x_0 \in \mathbb{Z}/p\mathbb{Z} \\ a_2 &= x_0 + px_1 \in \mathbb{Z}/p^2\mathbb{Z} \\ a_3 &= x_0 + px_1 + p^2x_2 \in \mathbb{Z}/p^3\mathbb{Z} \\ &\vdots \end{aligned}$$

A more general example is obtained by taking A to be a ring and I an ideal in A, then setting $A_n = A/I^n$ and $f_{n+1}\colon A/I^{n+1} \to A/I^n$, $f(x + I^{n+1}) = x + I^n$. The resulting inverse limit $\hat{A}$ is called the *I-adic completion* of A. There is a natural ring homomorphism $\varphi\colon A \to \hat{A}$ given by $\varphi(a) = (a + I^n)_n$.

Exercise 5.29. Show that

$$\ker\varphi = \bigcap_{n\in\mathbb{N}} I^n.$$

Example 5.30. If $A = k[x]$ and $I = (x)$, then $\hat{A} = k[[x]]$, the ring of formal power series with coefficients in k.

Given an A-module M, set $M_n = M/I^nM$ and $f_{n+1}: M/I^{n+1}M \to M/I^nM$ given by $f_{n+1}(m + I^{n+1}M) = m + I^nM$. The inverse limit $\hat{M}$ is the I-adic completion of M and is an $\hat{A}$-module. This applies, in particular, to ideals J of A, giving rise to ideals $\hat{J}$ of $\hat{A}$.

Example 5.31. Take $A = \mathbb{Z}$, $I = p\mathbb{Z}$.

(a) Let $J = I$, we have:

$$\begin{aligned} J_1 &= (p\mathbb{Z})/(p^2\mathbb{Z}) = p(\mathbb{Z}/p\mathbb{Z}) = 0 \\ J_2 &= (p\mathbb{Z})/(p^3\mathbb{Z}) = p(\mathbb{Z}/p^2\mathbb{Z}) \\ &\vdots \\ J_n &= p(\mathbb{Z}/p^n\mathbb{Z}). \end{aligned}$$

So $\hat{J} = \hat{I} = p\mathbb{Z}_p$.

(b) Let $J = q\mathbb{Z}$, q prime not equal to p.

$$\begin{aligned} J_1 &= q\mathbb{Z}/pq\mathbb{Z} = q(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \\ J_2 &= q\mathbb{Z}/p^2q\mathbb{Z} = q(\mathbb{Z}/p^2\mathbb{Z}) = \mathbb{Z}/p^2\mathbb{Z} \\ &\vdots \end{aligned}$$

So $\hat{J} = q\mathbb{Z}_p = \mathbb{Z}_p$.

(c) Generally, if $J = m\mathbb{Z}$, let $v = v_p(m)$, then $\hat{J} = p^v\mathbb{Z}_p = \hat{I}^v$.

Proposition 5.32. *If A is a ring and $\mathfrak{m}$ is a maximal ideal then the $\mathfrak{m}$-adic completion $\hat{A}$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$.*

An important special case is that where $A = \mathcal{O}_K$ is the ring of integers in a number field and $\mathfrak{m}$ is any nonzero prime ideal of $\mathcal{O}_K$.

Completion has nice algebraic properties. For instance, if A is Noetherian, I is any ideal, then $\hat{A}$ is Noetherian, and if we restrict to finitely generated modules M, then $M \mapsto \hat{M}$ is an exact functor.

5.8. Arithmetic of p-adic fields

A *p-adic field* (not standard terminology) is a finite extension K of $\mathbb{Q}_p$. Letting $n = [K:\mathbb{Q}_p]$, we have the absolute value

$$|x|_K = |N^K_{\mathbb{Q}_p}(x)|_p^{1/n},$$

which has the property $|x|_K = |x|_p$ for $x \in \mathbb{Q}_p$. The field K is complete with respect to $|\cdot|_K$.

Here is one example of how p-adic fields are simpler than number fields:

Proposition 5.33. *If L/K is an extension of p-adic fields, then there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.*

If $K/\mathbb{Q}$ is a number field and $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$, then $K_\mathfrak{p}$ is a p-adic field, where $p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}$. Conversely, if $F/\mathbb{Q}_p$ is a p-adic field then there exists a number field $K/\mathbb{Q}$ and a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $K_\mathfrak{p} \cong F$.

Viewing both $\mathbb{Q}_p$ and K as subfields of $K_\mathfrak{p}$, we have $\mathbb{Q}_p \cap K = \mathbb{Q}$. There is an injective group homomorphism $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \to \mathrm{Gal}(K/\mathbb{Q})$ given by restriction to K. The image of this homomorphism is precisely the decomposition group $D_{\mathfrak{p}/p}$.

5.8.1. Prime ideal decomposition in p-adic fields

Let K be a p-adic field. Let A_K be its valuation ring and $\mathfrak{p}_K$ the unique maximal ideal of A_K.

$$\begin{tikzcd} K \arrow[d, dash] & A \arrow[d, dash] & \mathfrak{p}_K^e \arrow[d, dash] & \kappa = A_K/\mathfrak{p}_K \arrow[d, dash] \\ \mathbb{Q}_p & \mathbb{Z}_p & p\mathbb{Z}_p & \mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p \end{tikzcd}$$

If we let $f = [\kappa{:}\mathbb{F}_p]$, then $ef = n = [K{:}\mathbb{Q}_p]$.

We say that $K/\mathbb{Q}_p$ is

- unramified if $e = 1$ (so $f = n$);
- totally ramified if $e = n$ (so $f = 1$).

Unramified extensions

Fix an algebraic extension L of $\mathbb{Q}_p$, with valuation ring $A = A_L$ and residue field λ. There is a bijective correspondence

$$\{K/\mathbb{Q}_p \text{ finite unramified, } K \subseteq L\} \leftrightarrow \{\kappa/\mathbb{F}_p \text{ finite, } \kappa \subseteq \lambda\}.$$

To go from the left to the right, simply map K to $A_K/\mathfrak{p}_K$. To go from the right to the left, choose a primitive element α_0 so that $\kappa = \mathbb{F}_p[\alpha_0]$, and let $f_0 \in \mathbb{F}_p[x]$ be the minimal polynomial of α_0. Let $f \in A_L[x]$ be any lift of f_0. By Hensel's Lemma, there exists a unique $\alpha \in A_L$ such that $\alpha \equiv \alpha_0 \pmod{\mathfrak{p}}$ and $f(\alpha) = 0$. Finally let $K = \mathbb{Q}_p[\alpha]$.

This reduces the study of unramified extensions of $\mathbb{Q}_p$ to the study of finite extensions of $\mathbb{F}_p$. Recall that, for each $n \in \mathbb{N}$, there is a unique (up to $\mathbb{F}_p$-isomorphism) extension $\kappa_n = \mathbb{F}_{p^n}$ of $\mathbb{F}_p$ of degree n, namely the splitting field of the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$. The Galois group $\mathrm{Gal}(\kappa_n/\mathbb{F}_p)$ is cyclic of order n, generated by $a \mapsto a^p$.

So for each $n \in \mathbb{N}$ there is a unique unramified extension $K_n = \mathbb{Q}_{p^n}$ of $\mathbb{Q}_p$ of degree n, namely the splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$. The Galois group $\mathrm{Gal}(K_n/\mathbb{Q}_p)$ is cyclic of order n, generated by the Frobenius element characterised by

$$\mathrm{Frob}(\beta) \equiv \beta^p \pmod{\mathfrak{p}} \qquad \text{for all } \beta \in A_{K_n}.$$

Example 5.34. Let $p = 3$ and $n = 2$. In $\mathbb{F}_3[x]$ we have the decomposition into irreducible factors

$$x^9 - x = x(x-1)(x+1)(x^2+1)(x^4+1).$$

Then $\kappa_2 = \mathbb{F}_3[i]$, $i^2 = -1$. This splits $x^2 + 1$, but how about $x^4 + 1$? Over κ_2 we have

$$x^4 + 1 = (x^2 + i)(x^2 - i) = \big(x - (1+i)\big)\big(x + (1+i)\big)\big(x - (2+i)\big)\big(x + (2+i)\big).$$

So $K_2 = \mathbb{Q}_3[i]$, $i^2 = -1$, is the unique unramified quadratic extension of $\mathbb{Q}_3$.

Exercise 5.35. Describe the unique unramified quadratic extension of $\mathbb{Q}_5$.

Totally ramified extensions

Before we start:

Lemma 5.36. *Let A be a DVR, $n \geq 2$, and $y_1 \neq 0, y_2, \dots, y_n \in \operatorname{Frac}(A)$ be such that*

$$v(y_1) < v(y_j) \qquad \text{for all } j \geq 2.$$

Then

$$y_1 + y_2 + \cdots + y_n \neq 0.$$

Proof. Without loss of generality, $y_1 = 1$. (Otherwise, divide all y_j by y_1.)

So for all $j \geq 2$ we have $v(y_j) \geq 1$, that is $y_j \in \mathfrak{m}$, the unique maximal ideal of A. Therefore

$$y_2 + \cdots + y_n \in \mathfrak{m},$$

which, since $y_1 = 1 \notin \mathfrak{m}$, implies that

$$y_1 + y_2 + \cdots + y_n \notin \mathfrak{m}.$$

□

A monic polynomial $f \in \mathbb{Q}_p[x]$ is *Eisenstein* if

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in p\mathbb{Z}_p$ for $i = 0, \dots, n-1$ and $a_0 \notin p^2\mathbb{Z}_p$.

Proposition 5.37. *Let K be a p-adic field. Then $K/\mathbb{Q}_p$ is totally ramified if and only if $K = \mathbb{Q}_p[\alpha]$, where α is a root of an Eisenstein polynomial.*

Proof. Proof of the forward direction: Let $\pi \in A_K$ be a uniformiser. The minimal polynomial of π has coefficients in $\mathbb{Z}_p$:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

so

$$a_n\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_1\pi + a_0 \qquad \text{with } a_n = 1.$$

Let v denote the discrete valuation on K. We have $v(\pi) = 1$ and $v(a) \equiv 0 \pmod{n}$ for $a \in \mathbb{Z}_p$. So $v(a_j\pi^j) = v(a_j) + j$ for $j = 0, \dots, n$.

Let $m = \min_j\{v(a_j\pi^j)\}$. By Lemma 5.36 there exist $0 \leq i < j \leq n$ such that $m = v(a_i\pi^i) = v(a_j\pi^j)$. But $v(a_i\pi^i) = v(a_i) + i \equiv i \pmod{n}$, and similarly $v(a_j\pi^j) \equiv j \pmod{n}$, so we must have $i = 0$ and $j = n$.

We conclude that $v(a_0) = v(a_0\pi^0) = v(a_n\pi^n) = v(\pi^n) = n$, hence $v_p(a_0) = 1$.

Also, for all $k = 1, \dots, n-1$ we have $v(a_k) + k = v(a_k\pi^k) \geq n$, so $v(a_k) \geq n - k > 0$, so $v_p(a_k) > 0$. □

A. Revision: Algebra

Algebraic number theory is the application of algebraic methods to arithmetic questions. This requires the reader to live and breathe algebraic structures such as groups, rings, fields, vector spaces, modules, ideals. We also lean pretty heavily on the Galois theory of field extensions.

The purpose of this appendix is to give a summary of things you are expected to be familiar with. Use this as an opportunity to reconnect with your knowledge in algebra and/or to diagnose any gaps that need filling. Good places to go for help are your notes from MAST20022+MAST30005 and [3].

A.1. Rings

In this subject all rings are commutative and have 1.

If $R \subseteq S$ are two rings, we say that S is a *ring extension* of R. In this case S is an R-algebra.

Given a ring extension $R \subseteq S$ and an element $\alpha \in S$, we write $R[\alpha]$ for the smallest (under inclusion) subring of S that contains both R and α, and refer to $R \subseteq R[\alpha]$ as the *ring extension generated by α*.

> **Exercise A.1.** Show that the notation $R[\alpha]$ makes sense, in that $R[\alpha]$ can be identified with the set of all polynomial expressions in α with coefficients in R. More precisely, let $\mathrm{ev}\colon R[x] \to S$ denote the ring homomorphism "evaluation at α" uniquely determined by $\mathrm{ev}(x) = \alpha$. Show that $\mathrm{im}(\mathrm{ev}) = R[\alpha]$.

A.2. Fields

If $E \subseteq F$ are two fields, we say that F is a *field extension* of E, often (confusingly) denoted F/E. In this case F is a vector space over E, and we say that that F/E is a *finite field extension* if F is a finite-dimensional E-vector space.

Given a field extension F/E and an element $\alpha \in F$, we write $E(\alpha)$ for the smallest (under inclusion) subfield of F that contains both E and α, and refer to $E(\alpha)/E$ as the *field extension generated by α*.

> **Exercise A.2.** Suppose that α is algebraic over E, that is there exists $f \in E[x]$ such that $f(\alpha) = 0$. Show that $E(\alpha) = E[\alpha]$.

The Primitive Element Theorem (see [5, Proposition 27.12] or [3, Theorem 25 in Section 14.4]) says that for any finite separable field extension F/E there exists $\alpha \in F$ such that $F = E(\alpha)$.

Bibliography

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] M. Baker. Algebraic number theory course notes. Math 8803, Georgia Tech, Fall 2006.

[3] D. Dummit and R. Foote. *Abstract algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[4] D. Marcus. *Number fields.* Universitext. Springer, Cham, 2018. Second edition, With a foreword by Barry Mazur.

[5] L. Reeves. Lecture notes on rings, modules and fields. MAST30005, University of Melbourne, 2015.

Index

I-adic completion, 69
$\mathfrak{p}$-adic absolute value, 62
$\mathfrak{p}$-adic valuation, 61
p-adic absolute value, 62
p-adic field, 70
p-adic numbers, 64
p-adic topology, 62
p-adic valuation, 61

abelian extension, 42
absolute value, 61
algebraic integers, 8
algebraic numbers, 7

character, 43
class number, 16
coherent sequences, 69
compatible homomorphism, 63
complete lattice, 11
complex embeddings, 47
compositum, 40
conjugates, 11
continued fraction, 55
convergent, 55
convex, 48
covolume, 47
cyclotomic field, 29

decomposition field, 39
decomposition group, 37
Dedekind domain, 13
discrete $\mathbb{Z}$-submodule, 10
discrete valuation, 60
discrete valuation ring, 60
discriminant, 18

Eisenstein, 27, 72
Euler phi function, 30
Euler's criterion, 33

field extension, 73
field extension generated by α, 73
finite field extension, 73
finitely-generated R-module, 8
fractional ideal, 13
fundamental domain, 47

Gauss sum, 33

ideal class group, 16
inert, 23
inertia field, 39
inertia group, 38
inertial degree, 20
integral closure, 8
integral element, 7
integral extension, 7
integrally closed, 9
inverse limit, 69
inverse system, 69

Krull dimension, 12

lattice, 11
lies over, 23, 36
local ring, 59
localisation, 59

Minkowski constant, 50
multiplicative set, 59

Noetherian, 12
norm, 11
norm of an ideal, 18
normalised, 60
number field, 7

piecewise volume-preserving, 48
place, 62
primitive element, 73
primitive root, 34
principal fractional ideal, 16
projective limit, 69
projective system, 69
purely periodic, 56

quadratic field, 9
quadratic residue symbol, 23

ramification index, 20

ramified, 23
real embeddings, 47
reduced, 56
relatively prime, 19
residue degree, 20
residue field, 36
ring extension, 73
ring extension generated by α, 73
ring of integers, 8

signature, 47
splits completely, 23
squarefree, 23
sublattice, 11
symmetric, 48

Theorem
    Primitive Element, 73
totally ramified, 23
trace, 11
trivial absolute value, 61

uniformiser, 64

valued field, 63
volume-preserving, 48