Algebraic number theory

Alexandru Ghitza*
School of Mathematics and Statistics
University of Melbourne

Version of Tue 26th Apr, 2022 at 14:39

*(aghitza@alum.mit.edu)

Contents

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

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

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, $x \le y$, 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 Kevin Fergusson, Yuhan Gai, Miles Koumouris, Jonah Nelson, Liang Tee, and Abraham Zhang for corrections and suggestions on these notes.

2. Number fields and rings of integers

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 $\left\{\alpha^{n-1}, \ldots, \alpha, 1\right\}$ 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 $\left\{x_1, \ldots, x_n\right\}$ 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 $K = \mathrm{Frac}(R)$, 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 $K = \mathrm{Frac}(\mathcal{O}_K)$ and $\mathcal{O}_K$ is integrally closed.*

Proof. Clearly $\mathrm{Frac}(\mathcal{O}_K) \subseteq K$. 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

$$(c_n\alpha)^n + c_{n-1}(c_n\alpha)^{n-1} + \cdots + c_1c_n^{n-2}(c_n\alpha) + c_0c_n^{n-1} = 0,$$

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

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 $K = \mathbb{Q}(\theta)$.*

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

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

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 $\varphi: k^n \to V$ denote the k-linear map $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_iv_i$. 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

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

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

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

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 $[\Lambda : \Omega] \leq B^n$.

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 $\sigma_1, \ldots, \sigma_n$.

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 $K/\mathbb{Q}$:

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

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

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

$$\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha) = \frac{n}{d}\,\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) \quad \text{and} \quad \mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = \left(N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)\right)^{n/d}.$$

Conclude from this that $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Q}$ and $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Q}$.

Moreover, if $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Z}$ and $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Z}$.

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 $\{\beta_1, \ldots, \beta_n\}$ 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 $a_1, \ldots, a_n \in \mathbb{Q}$ 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

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

more precisely as a linear polynomial (function) with complex coefficients in the variables $a_1, \ldots, a_n$. From this viewpoint, $N(\lambda) = \prod_\sigma \sigma(\lambda)$ is a homogeneous polynomial of degree n

[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.

in $a_1, \ldots, a_n$. Therefore we can make $N(\lambda)$ arbitrarily small, say $|N(\lambda)| < 1$, by substituting sufficiently small rational values for $a_1, \ldots, a_n$.

But if $\mathcal{O}_K$ is not discrete in K, for any $\epsilon > 0$ there exist $a_1, \ldots, a_n \in \mathbb{Q}$ such that $|a_i| < \epsilon$ and $\lambda := \sum_i a_i \beta_i \in \mathcal{O}_K \setminus \{0\}$. In particular, we can get $|N(\lambda)| < 1$ while at the same time $N(\lambda) \in \mathbb{Z} \setminus \{0\}$, 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 $\{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Q}$-basis of K with $\beta_i \in \mathcal{O}_K$. Let $\gamma \in I \setminus \{0\}$, then $c := N(\gamma) \in I \cap \mathbb{Z}$ is a nonzero integer. Therefore $c\beta_i \in I$ for all I, and certainly $\{c\beta_1, \ldots, c\beta_n\}$ 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 $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ 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:

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

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.*

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

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

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.*

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. □

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

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.

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

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*

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

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

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

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 $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be a $\mathbb{Q}$-basis for K and let $M = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Then*

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

Proof. Fixing an integral basis $\omega_1, \ldots, \omega_n$ 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

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

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

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 $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_K$, then $\alpha\omega_1, \ldots, \alpha\omega_n$ is a $\mathbb{Z}$-module basis for $\alpha\mathcal{O}_K$. Expressing each $\alpha\omega_i$ as a $\mathbb{Z}$-linear combination of $\omega_1, \ldots, \omega_n$ 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

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

However, back to the definition of Δ, we have

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

□

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].

[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.

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

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

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] $\varphi\colon\mathcal{O}_K\to\mathfrak{p}^j/\mathfrak{p}^{j+1}$ 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 $N(IJ)=N(I)N(J)$.*

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 $p\mathcal{O}_K$:*

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

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:

$$\sum_{j=1}^{r}e_jf_j=n.$$

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

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

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

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 $I_1, \ldots, I_r$ 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 $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$ and let $\sigma_1, \ldots, \sigma_n$ 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:

$$\alpha\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_r$$
$$I = \mathfrak{q}_1 \dots \mathfrak{q}_s.$$

Since $\alpha\mathcal{O}_K \subseteq I$, we have $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \mathfrak{q}_1$, 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 $\sigma\colon K \to K$ 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

$$\sum_{j=1}^{g} e_j f_j = [K\colon\mathbb{Q}] = 2.$$

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.

□

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 $\bar{\cdot} : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ 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 $\bar{\cdot}$, $N(\mathfrak{p}_j) = p^{f_j}$ 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 $\omega_1, \ldots, \omega_n$ 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:

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

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 $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$:

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

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.

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

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

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 $\sigma_j : \mathbb{Q}(\zeta) \to \mathbb{C}$ 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

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

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 $1, 1-\zeta, \ldots, (1-\zeta)^{n-1} \in \mathcal{O}_K$ is a $\mathbb{Q}$-basis for K. By Proposition 2.34 any element $\alpha \in \mathcal{O}_K$ can be written in the form

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

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

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

where $\{j_1 < \cdots < j_s\} \subseteq \{0, \ldots, n-1\}$ 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 $\theta\,\frac{p}{(1-\zeta)^{j_1+1}} \in \mathcal{O}_K$:

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

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. □

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. □

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

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

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 $\sigma\colon \mathcal{O}_L \to \mathcal{O}_L$ inducing a ring isomorphism $\sigma\colon \mathcal{O}_L/\mathfrak{q}_i \to \mathcal{O}_L/\sigma(\mathfrak{q}_i)$. 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 $\varphi_\mathfrak{q}\colon D_\mathfrak{q} \to \mathrm{Gal}(\lambda/\kappa)$, $\sigma \mapsto \overline{\sigma}$, 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

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

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 $efg = [L:K]$. 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:*

		ramification degree	*inertial degree*
L	$\mathfrak{q}$		
e |	|	e	1
L^I	$\mathfrak{q}_I = \mathfrak{q} \cap \mathcal{O}_{L^I}$		
f |	|	1	f
L^D	$\mathfrak{q}_D = \mathfrak{q} \cap \mathcal{O}_{L^D}$		
g |	|	1	1
K	$\mathfrak{p}$		

Proof. We have a number of claims to verify:

(a) $[L^D:K] = g$.
By Galois theory $[L^D:K] = [G:D]$. 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 $(\mathcal{O}_{L^I}/(\mathfrak{q} \cap \mathcal{O}_{L^I}))[x] = \lambda_I[x]$. 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) $[L^I:L^D] = f$.
From the previous point we know that $f(\mathfrak{q}^I/\mathfrak{q}^D) = f$, so $[L^I:L^D] \geq f$. However, we know that $[D:I] \leq f$, 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 $\mathbb{Q}$).

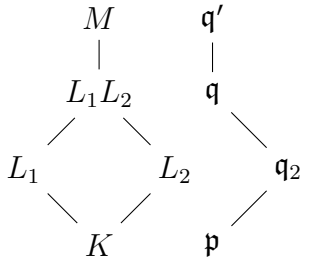
(b) $\mathfrak{p}$ splits completely in both L_1 and L_2 if and only if it splits completely in L_1L_2.

[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.

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.



(b) Similar to part (a).

□

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 $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ 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 $\omega_1, \ldots, \omega_n$ 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

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

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

In order to do this, let $\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ 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 $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$, $\sigma^{-1}(\mathfrak{q}_0)$ 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

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

($\Leftarrow$): 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

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

The assumption that $p \mid \Delta_K$ implies that the rows of the reduction modulo p of the matrix $[\mathrm{Tr}_{\mathbb{Q}}^K(\omega_i\omega_j)]$ 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

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

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

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

This says that $\mathrm{Tr}_{\mathbb{Q}}^K(\theta\mathcal{O}_K) \subseteq p\mathbb{Z}$, 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

$$\mathrm{Tr}_{\mathbb{Q}}^M(\theta\mathcal{O}_M) = \mathrm{Tr}_{\mathbb{Q}}^K\,\mathrm{Tr}_K^M(\theta\mathcal{O}_M) = \mathrm{Tr}_{\mathbb{Q}}^K\left(\theta\,\mathrm{Tr}_K^M(\mathcal{O}_M)\right) \subseteq \mathrm{Tr}_{\mathbb{Q}}^K(\theta\mathcal{O}_K) \subseteq p\mathbb{Z}.$$

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

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

Let $D = D(\mathfrak{q}/p) \subseteq G = \mathrm{Gal}(M/\mathbb{Q})$, 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 $x \in \mathcal{O}_M$

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

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

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

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

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

This says that

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

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 $\chi: G \to \mu^\times$. We say that characters $\chi_1, \dots, \chi_n$ 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 $\chi_1, \dots, \chi_n$ 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 $d \equiv 1 \pmod 4$.

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:

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

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 $\mathcal{O}_K = \mathbb{Z}[\sqrt{p^*}]$, we know that q splits completely in K if and only if the minimal polynomial $x^2 - p^*$ 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 $\left(\frac{q}{p}\right) = 1$. □

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