Algebraic Number Theory

Daniele Agostini

July 13, 2026

Preface

These notes are a work in progress. If you find any mistakes, please let me know.

The parts marked with ($\star$) are not part of the lectures, but we might discuss some of them in the exercise sessions.

Contents

1 Primes that are a sum of two squares **1**
- 1.1 Primes as difference of squares . . . 1
- 1.2 Primes as sum of squares . . . 2
- 1.3 Themes of the course . . . 6

2 Number fields and their rings of integers **7**
- 2.1 Integral extensions of rings . . . 7
- 2.2 Number fields . . . 10
  - 2.2.1 Definition and examples of number fields . . . 10
  - 2.2.2 Embeddings of number fields . . . 11
  - 2.2.3 Normal extensions and the Galois group . . . 13
  - 2.2.4 Trace, norm and the characteristic polynomial . . . 15
- 2.3 Rings of integers of number fields . . . 17
  - 2.3.1 The ring of integers as an abelian group . . . 20
  - 2.3.2 The discriminant . . . 24

3 Dedekind domains **29**
- 3.1 Definition and basic properties . . . 29
- 3.2 Fractional ideals and unique factorization . . . 30
  - 3.2.1 Unique factorization of ideals in a Dedekind domain . . . 34
  - 3.2.2 The class group of a Dedekind domain . . . 37
- 3.3 Prime splittings in rings of integers . . . 37
  - 3.3.1 Computing a factorization . . . 39
  - 3.3.2 Discriminant and ramification . . . 42

4 Geometry of numbers **44**
- 4.1 The absolute norm . . . 44
- 4.2 Minkowski's bound and finiteness of the class group . . . 46
  - 4.2.1 Lattices in $\mathbf{R}^n$ . . . 48
  - 4.2.2 The canonical embedding of a number field . . . 50
- 4.3 Dirichlet's unit theorem . . . 52
  - 4.3.1 The torsion part . . . 54
  - 4.3.2 The torsion-free part . . . 55

5 Prime splitting and Galois groups **58**
- 5.1 Ramification and inertia in Galois extensions . . . 58
  - 5.1.1 The Frobenius element . . . 61

5.2 Cyclotomic fields . . . 61
5.2.1 Quadratic reciprocity . . . 64
5.2.2 Proof of Quadratic Reciprocity . . . 66
5.3 Fermat's last theorem for regular primes . . . 68

A Commutative algebra **75**
A.1 Rings and ideals . . . 75
A.1.1 Homomorphisms . . . 76
A.2 Finitely generated ideals, principal ideals and Noetherian rings . . . 77
A.3 Divisibility . . . 77
A.4 Euclidean domains, principal ideal domains and unique factorization domains . . . 78
A.4.1 Euclidean domains . . . 78
A.4.2 Principal ideal domains . . . 79
A.4.3 Unique factorization domains . . . 80
A.4.4 Coprime elements and greatest common divisor . . . 81
A.4.5 Factorization in a PID . . . 84
A.5 Modules . . . 85
A.5.1 Finitely generated modules and Noetherian modules . . . 88
A.5.2 Free modules . . . 89
A.5.3 Finitely generated modules over a PID . . . 93
A.6 The Chinese remainder theorem . . . 98

B Field theory **100**
B.1 Characteristic and Frobenius . . . 100
B.2 Algebraic and finite extensions of fields . . . 101
B.2.1 The algebraic closure . . . 103
B.2.2 Separable extensions . . . 104
B.2.3 Field embeddings . . . 105
B.3 Galois Theory . . . 107
B.3.1 The fundamental theorem of Galois theory . . . 108

Chapter 1

Primes that are a sum of two squares

Algebraic Number Theory is essentially the study of integer (meaning in $\mathbf{Z}$) and rational (meaning in $\mathbf{Q}$) solutions to algebraic equations.

Example 1.0.1 (Fermat's Equation)**.** One of the most famous examples is Fermat's equation

$$X^n + Y^n = Z^n.$$

The integer solutions of this equation for $n = 2$ are called Pythagorean triples, and there's infinitely many of them. Pierre de Fermat wrote in the margin of a book in 1637 that this equation has no integer solutions for $n \geq 3$ and he stated to have a proof that was unfortunately too long to fit in the margin. The statement was ultimately proved by Andrew Wiles in 1994, after the development of a huge amount of new mathematics on the way.

1.1 Primes as difference of squares

We consider a simpler example. We want to solve the equation

$$p = x^2 - y^2 \quad p, x, y \in \mathbf{Z} \quad p \text{ prime number.} \tag{1.1.1}$$

Equivalently, we want to know which prime numbers are differences of two squares, and then possibly we would also like to find the squares.

We observe right away that we can factor the right-hand side as

$$p = (x - y)(x + y),$$

and since p is a prime number, it is irreducible in $\mathbf{Z}$ so one of $x - y$ or $x + y$ must be invertible in $\mathbf{Z}$, meaning equal to 1 or -1. We can furthermore assume that the invertible factor is $x - y$, otherwise we can just replace y with $-y$ (observe that the equation (1.1.1) does not change if we multiply either of x, y by -1). Hence we write

$$\begin{cases} x + y = p \\ x - y = 1 \end{cases}, \quad \begin{cases} x + y = -p \\ x - y = -1 \end{cases}.$$

We can solve both systems by linear algebra and we obtain

$$\begin{cases} x = \frac{p+1}{2} \\ y = \frac{p-1}{2} \end{cases}, \quad \begin{cases} x = -\frac{p+1}{2} \\ y = \frac{p-1}{2} \end{cases}.$$

These are almost all the solutions, the others can be found by changing sign to y. So all the possible solutions are:

$$\begin{cases} x = \frac{p+1}{2} \\ y = \frac{p-1}{2} \end{cases} , \quad \begin{cases} x = \frac{p+1}{2} \\ y = -\frac{p-1}{2} \end{cases} , \quad \begin{cases} x = -\frac{p+1}{2} \\ y = \frac{p-1}{2} \end{cases} , \quad \begin{cases} x = -\frac{p+1}{2} \\ y = -\frac{p-1}{2} \end{cases} .$$

Notice that we want x, y to be in $\mathbf{Z}$ so that both $p+1, p-1$ must be even, meaning that p must be an odd prime. We have proved:

Proposition 1.1.1. *A prime number $p \in \mathbf{Z}$ is a difference of two squares if and only if it is odd. In this case, we can write $p = x^2 - y^2$ with $x = \frac{p+1}{2}, y = \frac{p-1}{2}$ and all the other possibilities obtained changing signs to x or y.*

Observe that once we have explicit formulas for x, y the result is easy to check:

$$\left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 = \left(\frac{p+1}{2} - \frac{p-1}{2}\right)\left(\frac{p+1}{2} + \frac{p-1}{2}\right) = 1 \cdot p = p$$

and this does not even use that p is a prime number. However if we want both $\frac{p+1}{2}, \frac{p-1}{2}$ to be integers, we need p to be an odd number. Hence we proved

Proposition 1.1.2. *Any odd number $k \in \mathbf{Z}$ is the difference of two squares in $\mathbf{Z}$*

$$k = \left(\frac{k+1}{2}\right)^2 - \left(\frac{k-1}{2}\right)^2$$

At this point it is natural to ask about even numbers. Proposition 1.1.1 shows that 2 is not the difference of two squares, but of course there are even numbers with this property, for example $12 = 16 - 4 = 4^2 - 2^2$. Which even numbers are the difference of two squares? The answer is known and its proof is left as an exercise.

Exercise 1.1.3. *Show that an even number is the difference of two squares in $\mathbf{Z}$ if and only if it is divisible by 4.*

1.2 Primes as sum of squares

We consider the analogous question for the sum of squares. We want to solve the equation

$$p = x^2 + y^2 \quad p, x, y \in \mathbf{Z} \quad p \text{ prime number} .$$

Equivalently, we want to know which primes can be written as the sum of two squares, and if possible we want to find the squares. If we try to proceed as for the case (1.1.1) of the difference of two squares, we immediately get stuck because we cannot factorize $x^2 + y^2$. Let's then try to look at some examples:

p	2	3	5	7	11	13	17	19	...
s.o.s.	$1^2 + 1^2$	no	$1^2 + 2^2$	no	no	$2^2 + 3^2$	$1^2 + 4^2$	no	...

Is there a pattern? It turns out that there is indeed one

Theorem 1.2.1 (Fermat-1640 , Euler-1750, Lagrange-1770, Gauss-1800, Dirichlet-1870, Zagier-1990,...)**.** *An odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$. If this is the case, then p is a sum of squares in a unique way, meaning that if*

$$p = x^2 + y^2 \quad \text{for } x, y \in \mathbf{Z}$$

then x, y are uniquely determined, up to swapping them and changing sign.

One implication is fairly simple:

Lemma 1.2.2. *If an odd prime p is a sum of two squares, then $p \equiv 1 \pmod 4$.*

Proof. Modulo 4, the squares are:

n	0	1	2	3
$n^2 \pmod 4$	0	1	0	1

If $p = x^2 + y^2$, and p is odd, one of x, y must be even and the other odd. Hence, $p \equiv 0 + 1 \equiv 1 \pmod 4$. □

The converse is more difficult. Consider again the expression $p = x^2 + y^2$. One problem is that we could not factor the right hand side in $\mathbf{Z}$. However, we can factor the expression once we add in the imaginary unit $i \in \mathbf{C}$:

$$p = x^2 + y^2 = (x - iy)(x + iy) \tag{1.2.1}$$

This factorization takes place not in $\mathbf{Z}$ but in the ring of Gaussian integers $\mathbf{Z}[i]$.

Definition 1.2.3 (Gaussian integers)**.** The ring of Gaussian integers is the set

$$\mathbf{Z}[i] = \{a + ib \,|\, a, b \in \mathbf{Z}\}$$

This is a actually a subring of the field

$$\mathbf{Q}(i) = \{a + ib \,|\, a, b \in \mathbf{Q}\}$$

which is a Galois extension of $\mathbf{Q}$ of degree 2, with Galois group generated by the complex conjugation

$$\sigma \colon \mathbf{Q}(i) \longrightarrow \mathbf{Q}(i), \quad a + ib \mapsto a - ib, \qquad \sigma^2 = \mathrm{id}$$

Notice that this restricts to an isomorphism

$$\sigma \colon \mathbf{Z}[i] \to \mathbf{Z}[i]$$

Consider again the factorization (1.2.1). If we want to proceed as in the case of the difference of squares, we would need to consider the irreducibility of p in $\mathbf{Z}[i]$. To study this, it is useful to consider the norm:

Definition 1.2.4 (Norm of Gaussian integers)**.** The norm is the map $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$:

$$N(\alpha) = \alpha \cdot \sigma(\alpha) = \alpha \cdot \bar{\alpha} = |\alpha|^2, \quad N(a + ib) = a^2 + b^2.$$

Lemma 1.2.5. *The norm is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.for all $\alpha, \beta \in \mathbf{Z}[i]$.*

Proof. If $\alpha, \beta \in \mathbf{Z}[i]$ then using the properties of the complex absolute value we see that $N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha)N(\beta)$. Otherwise we can also use the fact that the complex conjugation is a homomorphism, so that $N(\alpha\beta) = \alpha\beta \cdot \sigma(\alpha\beta) = \alpha\beta \cdot \sigma(\alpha)\sigma(\beta) = N(\alpha)N(\beta)$. □

Corollary 1.2.6. *The units in* $\mathbf{Z}[i]$ *are the elements of norm 1:*

$$\mathbf{Z}[i]^\times = \{1, i, -1, -i\}$$

Proof. If $N(\alpha) = 1$ then $\alpha \cdot \sigma(\alpha) = 1$ so that $\sigma(\alpha)$ is the inverse of α in $\mathbf{Z}[i]$. Conversely, if $\alpha, \beta \in \mathbf{Z}[i]$ satisfy $\alpha\beta = 1$, then $N(\alpha)N(\beta) = N(1) = 1$ and since the norm is always non-negative it must be that $N(\alpha) = N(\beta) = 1$. Finally, the elements of norm one are precisely those listed above. □

Corollary 1.2.7. *If the norm of* $\alpha \in \mathbf{Z}[i]$ *is a prime number* $N(\alpha) \in \mathbf{Z}$*, then* α *is irreducible in* $\mathbf{Z}[i]$.

Proof. Assume that $\alpha = \beta \cdot \gamma$ for $\beta, \gamma \in \mathbf{Z}[i]$. Then $N(\alpha) = N(\beta) \cdot N(\gamma)$ and since $N(\alpha)$ is prime one of $N(\beta), N(\gamma)$ must be invertible in $\mathbf{Z}$, hence equal to 1. But then one of β, γ must be invertible in $\mathbf{Z}[i]$. □

Consider again the factorization in $\mathbf{Z}[i]$:

$$p = (x - iy)(x + iy)$$

If p is irreducible in $\mathbf{Z}[i]$, then one of $x - iy, x + iy$ must be an unit in $\mathbf{Z}[i]$ and up to changing sign to y we can assume that it is $x - iy$. Hence we get four cases

$$\begin{cases} x + iy = p \\ x - iy = 1 \end{cases}, \quad \begin{cases} x + iy = -p \\ x - iy = -1 \end{cases}, \quad \begin{cases} x + iy = -ip \\ x - iy = i \end{cases}, \quad \begin{cases} x + iy = ip \\ x - iy = -i \end{cases},$$

but all these cases are impossible: for example in the first one we can compare real and imaginary parts and we get $x = p = 1$, which is impossible since p is prime in $\mathbf{Z}$. So, we have proved that if p is the sum of two squares, then it is not irreducible in $\mathbf{Z}[i]$.

Assume now that p is not irreducible in $\mathbf{Z}[i]$. Then we can factor

$$p = \alpha \cdot \beta \qquad \text{in } \mathbf{Z}[i]$$

where $\alpha, \beta \in \mathbf{Z}[i]$ are not units, so that $N(\alpha), N(\beta) > 1$. Taking the norm we see that

$$p^2 = N(p) = N(\alpha)N(\beta)$$

so it must be that $N(\alpha) = N(\beta) = p$. If we write $\alpha = x + iy$ for certain $x, y \in \mathbf{Z}$, this means that

$$p = N(\alpha) = x^2 + y^2$$

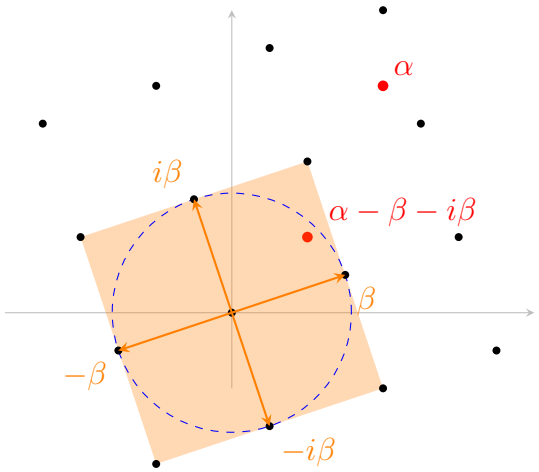
so that p is the sum of two squares in $\mathbf{Z}$. We have proved

Lemma 1.2.8. *A prime number* $p \in \mathbf{Z}$ *is the sum of two squares if and only if it is not irreducible in* $\mathbf{Z}[i]$.

What we need to show now is that an odd prime integer number $p \equiv 1 \pmod 4$ is not irreducible in $\mathbf{Z}[i]$. We will actually show that p is not a prime element in $\mathbf{Z}[i]$, but this is the same as being irreducible because it turns out that the Gaussian integers form an Euclidean Domain and hence a Unique Factorization Domain:

Proposition 1.2.9. *The Gaussian integers are an Euclidean Domain with respect to the norm. More precisely, given $\alpha, \beta \in \mathbf{Z}[i], \beta \neq 0$, there are $q, r \in \mathbf{Z}[i]$ with $N(r) < N(\beta)$ such that $\alpha = q\beta + r$. In particular, the Gaussian integers are a Principal Ideal Domain and an Unique Factorization Domain.*

Proof. This proof is geometric. Consider all the multiples $q\beta$ for $q \in \mathbf{Z}[i]$. These form the set $\Lambda = \{a\beta + ib\beta \,|\, a, b \in \mathbf{Z}\}$ which is a lattice in $\mathbf{C}$ generated by the two elements $\beta, i\beta$. As an exercise, prove that any $\alpha \in \mathbf{C}$ can be brought inside the disk $D = \{z \cdot \beta \,|\, z \in \mathbf{C}, |z| < 1\}$ via a translation with an element of the lattice Λ:



This means that we can write $\alpha = q\beta + r$ where $r = z\beta$ with $z \in \mathbf{C}, |z| < 1$. In particular $N(r) = |z|^2 \cdot |\beta|^2 = |z|^2 \cdot N(\beta) < N(\beta)$. □

Lemma 1.2.10. *Let $p \in \mathbf{Z}$ be an odd prime integer such that $p \equiv 1 \pmod 4$. Then -1 is a square in $\mathbf{F}_p$.*

Proof. The group of units $\mathbf{F}_p^\times = \mathbf{F}_p \setminus \{0\}$ is cyclic because a finite multiplicative subgroup of a field, so there is an element $a \in \mathbf{F}_p^\times$ of order $p-1$ such that $-1 = a^n$ in $\mathbf{F}_p^\times$. Then $a^{2n} = (-1)^2 = 1$ so that $p - 1 \mid 2n$, meaning that $\frac{p-1}{2} \mid n$, and we can write $-1 = a^{\frac{p-1}{2} \cdot k}$ for a certain $k \in \mathbf{Z}$. If $p \equiv 1 \pmod 4$, then $p - 1 = 4m$ for a certain $m \in \mathbf{Z}$ so that $\frac{p-1}{2} = 2m$ and $-1 = (a^{mk})^2$ is a square in $\mathbf{F}_p$. □

Corollary 1.2.11. *Let p be an odd prime such that $p \equiv 1 \pmod 4$. Then p is not irreducible in $\mathbf{Z}[i]$.*

Proof. We know that -1 is a square modulo p, meaning that there are $m, k \in \mathbf{Z}$ such that $-1 = m^2 - kp$. We can write this in $\mathbf{Z}[i]$ as

$$kp = m^2 + 1 = (m - i)(m + i)$$

Assume that p is irreducible in $\mathbf{Z}[i]$. Since this ring is an UFD, p is also prime, so that $p|m + i$ or $p|m - i$ in $\mathbf{Z}[i]$. But this is impossible: for example, in the first case we have $m + i = p(a + ib)$ for certain $a, b \in \mathbf{Z}$, so that $1 = pb$, which is absurd. Hence, p cannot be irreducible. □

Proof of Theorem 1.2.1. If an odd prime $p \in \mathbf{Z}$ is a sum of squares, we know from Lemma 1.2.2 that $p \equiv 1 \pmod 4$. If instead $p \equiv 1 \pmod 4$, then Corollary 1.2.11 shows that p is not irreducible in $\mathbf{Z}[i]$ and then Lemma 1.2.8 shows that p is a sum of squares.

Now we address the uniqueness of the squares: assume that $p = x^2 + y^2 = z^2 + w^2$ for $x, y, z, w \in \mathbf{Z}$. Then in $\mathbf{Z}[i]$ we have

$$(x + iy)(x - iy) = p = (z + iw)(z - iw)$$

and all $x + iy, x - iy, z + iw, z - iw$ have norm p, so that they are irreducible in $\mathbf{Z}[i]$ because of Corollary 1.2.7. Since $\mathbf{Z}[i]$ is an UFD, these two factorizations must coincide, up to multiplication by an unit. Up to replacing w with $-w$ we can assume that $x + iy = u \cdot (z + iw)$ for $u \in \mathbf{Z}[i]^\times$. If $u = 1$, this means $x = z, y = w$ if $u = -1$ this means $x = -z, y = -w$, if $u = i$ this means $x = -w, y = z$ and if $u = -i$ this means $x = w, y = -z$. □

The main step in the previous proof was proving that if p is an odd prime number such that $p \equiv 1 \pmod 4$, then p is not irreducible in $\mathbf{Z}[i]$. One can actually characterize completely the irreducible elements of $\mathbf{Z}[i]$ as in the following exercise:

Exercise 1.2.12. *Show that an element $\alpha \in \mathbf{Z}[i]$ is irreducible if and only if $N(\alpha)$ is prime in $\mathbf{Z}$ or if $\alpha = u \cdot p$ where $u \in \mathbf{Z}[i]^\times$ and $p \in \mathbf{Z}$ is a prime number such that $p \equiv 3 \pmod 4$.*

1.3 Themes of the course

Many ideas that appeared in the previous discussion will be central throughout the course. We saw that to solve a problem over $\mathbf{Z}$ it was useful to pass to a *larger ring* $\mathbf{Z}[i]$, which enjoys nice *factorization properties*. In order to study these factorization properties we used the *norm*, that was defined via the *isomorphism* of rings given by the *conjugation*. We also used some *geometric techniques* via *lattices*,...

These are (some of) the themes that we will explore in this course.

Chapter 2

Number fields and their rings of integers

2.1 Integral extensions of rings

Definition 2.1.1 (Integral Elements)**.** Let $A \subseteq B$ be rings. An element $\alpha \in B$ is called *integral* over A if there is a *monic polynomial* $f(x) \in A[x]$ that vanishes on α. Equivalently, there are $a_0, \dots, a_{n-1} \in A$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

The extension of rings $A \subseteq B$ is called *integral* if every element of B is integral over A.

Example 2.1.2. The square root $\sqrt{3} \in \mathbf{C}$ is integral over $\mathbf{Z}$, since it is a root of the polynomial $x^2 - 3$. The n-th primitive root of unity $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbf{C}$ is also integral over $\mathbf{Z}$ because it is a root of $x^n - 1$. Instead $\frac{1}{2} \in \mathbf{Q}$ is not integral over $\mathbf{Z}$ even if it is the root of the polynomial $2x - 1 \in \mathbf{Z}[x]$. The requirement that an integral element is a root of a *monic* polynomial is essential. Proving that $\frac{1}{2}$ is not integral is easy but we will see it as the consequence of a more general result later on.

Example 2.1.3. Let $d \in \mathbf{Z}$ be an integer such that $d \equiv 1 \pmod 4$, and let $\sqrt{d} \in \mathbf{C}$ be any square root. The complex number $\alpha = \frac{1+\sqrt{d}}{2} \in \mathbf{C}$ is integral over $\mathbf{Z}$. Indeed $2\alpha - 1 = \sqrt{d}$ so that $4\alpha^2 + 1 - 4\alpha = d$, meaning that $d - 1 = 4\alpha^2 - 4\alpha$. By hypothesis we can write $d - 1 = 4k$ for a $k \in \mathbf{Z}$, and then $\alpha^2 - \alpha - k = 0$.

If $A \subseteq B$ is a ring extension and if $\alpha \in B$ is an element, we have an evaluation map at α

$$\mathrm{ev}_\alpha : A[x] \longrightarrow B, \quad f(x) \mapsto f(\alpha)$$

which is a ring homomorphism. The image of this map is denoted by $A[\alpha] = \{a_n\alpha^n + \cdots + a_1\alpha + a_0 \,|\, a_i \in A\}$ and it is a subring of B with $A \subseteq A[\alpha] \subseteq B$. If $\alpha_1, \dots, \alpha_n \in B$ we can analogously define the subring $A[\alpha_1, \dots, \alpha_n] \subseteq B$ by evaluating all polynomials in $A[x_1, \dots, x_n]$ at the α_i.

Definition 2.1.4 (Finite extension)**.** An extension of rings $A \subseteq B$ is called finite if B is finitely generated as an A-module.

Lemma 2.1.5. *Being finite is transitive: let $A \subseteq B \subseteq C$ be ring extensions such that C is finite over B and B is finite over A. Then C is finite over A.*

Proof. Since C is finite over B, there are $x_1, \dots, x_r \in C$ such that every element in C has the form

$$b_1 x_1 + \cdots + b_r x_r \qquad b_i \in B.$$

Since B is finite over A, there are $y_1, \dots, y_s \in B$ such that any b is of the form $a_1 y_1 + \cdots + a_s y_s$ with $a_i \in A$. Plugging this into the previous expression shows that any element of C is a linear combination of the products $x_i y_j$ with coefficients in A. □

Proposition 2.1.6. *Let $A \subseteq B$ be a ring extension and let $\alpha \in B$. The following are equivalent*

1. *α is integral over A.*
2. *$A[\alpha]$ is finite over A.*
3. *there is an intermediate ring extension $A[\alpha] \subseteq C \subseteq B$, with C finite over A.*

In particular, any finite extension is integral.

Proof. (1) $\implies$ (2): Since α is integral, there are $a_{n-1}, \dots, a_0 \in A$ such that

$$\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_0$$

Let $M \subseteq A[\alpha]$ the A-module generated by $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. The previous relation shows that $\alpha^n \in (1, \alpha, \dots, \alpha^{n-1})$. If we multiply the relation by α we see that

$$\alpha^{n+1} = a_{n-1}\alpha^n + \cdots + a_0\alpha$$

so that $\alpha^{n+1} \in (1, \alpha, \dots, \alpha^{n-1}, \alpha^n) = M$. This way, we show that $\alpha^k \in M$ for any $k \in \mathbf{Z}_{\geq 0}$, and since these generate $A[\alpha]$ as an A-module, we are done.

(2) $\implies$ (3): just take $C = A[\alpha]$.

(3) $\implies$ (1): Consider the multiplication-by-α map

$$f = (\cdot\alpha)\colon C \longrightarrow C, \qquad x \mapsto \alpha x.$$

This is an endomorphis of a finitely generated A-module, so that Corollary A.5.24 shows that there is a monic polynomial $P(t) \in A[t]$ such that $P(f) = 0$. Hence $0 = P(f)(1) = P(\alpha)$. □

Corollary 2.1.7. *Let $A \subseteq B$ be a ring extension and let $\alpha_1, \dots, \alpha_n \in B$. The α_i are integral over A if and only if $A[\alpha_1, \dots, \alpha_n]$ is a finite extension of A.*

Proof. Since α_1 is integral over A, the extension $A[\alpha_1]$ is finite over A. Since α_2 is integral over A, it is also integral over $A[\alpha_1]$ because any polynomial with coefficients in A has also coefficients in $A[\alpha_1]$. Hence $A[\alpha_1, \alpha_2] = A[\alpha_1][\alpha_2]$ is finite over $A[\alpha_1]$. Since finiteness is transitive, we see that $A[\alpha_1, \alpha_2]$ is finite over A, and if we continue this way we see that $A[\alpha_1, \dots, \alpha_n]$ is finite over A. Conversely, if $A[\alpha_1, \dots, \alpha_n]$ is finite over A, then all the α_i are contained in a finite extension of A so they must be integral. □

Corollary 2.1.8. *Being integral is transitive: Let $A \subseteq B \subseteq C$ be ring extensions with B integral over A and C integral over B. Then C is integral over A.*

Proof. Let $\alpha \in C$. Since C is integral over B there are $b_0, \ldots, b_{n-1} \in B$ such that

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$$

Hence α is integral over $A[b_0, b_1, \ldots, b_{n-1}]$. This means that $A[b_0, \ldots, b_{n-1}, \alpha]$ is finite over $A[b_0, \ldots, b_{n-1}]$, which is finite over A because the b_i are integral over A. Hence $A[b_0, \ldots, b_{n-1}, \alpha]$ is finite over A, and α is integral over A. □

We now define the integral closure of a ring into an extension:

Corollary 2.1.9 (Integral Closure)**.** *Let $A \subseteq B$ be a ring extension. The set*

$$\bar{A} = \{\, \alpha \in B \mid \alpha \text{ is integral over } A \,\}$$

is a ring extension of A. It is called the integral closure *of A in B.*

Proof. We first prove that $\bar{A}$ is a ring. Let $\alpha, \beta \in B$ be integral over A. We need to show that $\alpha + \beta$ and $\alpha\beta$ are both integral over A. Corollary 2.1.7 shows that $A[\alpha, \beta]$ is a finite extension of A, and since any finite extension is integral, we see that $A[\alpha, \beta] \subseteq \bar{A}$. Now assume that $\alpha \in \overline{A}$ is invertible in B. Let $P(t) \in A[t]$ be a monic polynomial of the minimum possible degree such that $P(\alpha) = 0$ and write $P(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ □

Definition 2.1.10 (Integrally closed and normal rings)**.** Let $A \subseteq B$ be a ring extension. A is called *integrally closed in B* if the only elements in B that are integral over A are those of A itself

$$\bar{A} = A.$$

If A is a domain, A is called *integrally closed* or *normal* if it is integrally closed in $F = \operatorname{Frac} A$.

Example 2.1.11. The ring of integers $\mathbf{Z}$ is integrally closed. More generally, we have the following:

Proposition 2.1.12. *Any UFD is integrally closed.*

Proof. Let A be an UFD and let $\alpha \in F = \operatorname{Frac}(A)$ an element integral over A, that we can write as $\alpha = \frac{s}{t}$ with $s, t \in A$ coprime. Since α is integral,there are $a_0, \ldots, a_n \in A$ such that

$$\left(\frac{s}{t}\right)^n + a_{n-1}\left(\frac{s}{t}\right)^{n-1} + \cdots + a_1\frac{s}{t} + a_0 = 0$$

So that

$$s^n + a_{n-1}s^{n-1}t + \cdots + a_0 t^n = 0$$

This means in particular that $t \mid s^n$ so that any prime factor of t must be a prime factor of s as well. Since t, s are coprime, this means that t has no prime factor, so that $t \in A^\times$ and $\alpha = st^{-1} \in A$. □

Corollary 2.1.13. *Let $A \subseteq B$ be a ring extension and $\bar{A}$ the integral closure. Then $\bar{A}$ is integrally closed in B.*

Proof. Let $\alpha \in B$ be integral over $\bar{A}$, which is integral over A. Hence α is integral over A, which means $\alpha \in \bar{A}$. □

2.2 Number fields

2.2.1 Definition and examples of number fields

We now introduce the main objects of interest of the course:

Definition 2.2.1 (Number fields)**.** A number field is a finite field extension $\mathbf{Q} \subseteq K \subseteq \mathbf{C}$.

Example 2.2.2 (Quadratic extensions of $\mathbf{Q}$)**.** Let $d \in \mathbf{Z}$ be a square-free integer and let $\sqrt{d} \in \mathbf{C}$ be a square root. This is a root of the polynomial $x^2 - d$, hence it is integral over $\mathbf{Z}$ and algebraic over $\mathbf{Q}$. Furthermore, since this polynomial is irreducible over $\mathbf{Q}$, it is the minimal polynomial of $\sqrt{d}$. This shows that

$$\mathbf{Q}(\sqrt{d}) = \{a + b\sqrt{d} \,|\, a, b \in \mathbf{Q}\}$$

is a finite extension of $\mathbf{Q}$ of degree $[\mathbf{Q}(\sqrt{d}) : \mathbf{Q}] = 2$. Conversely, let $\mathbf{Q} \subseteq F \subseteq \mathbf{C}$ be a finite extension of $\mathbf{Q}$ of degree 2, and let $\alpha \in F, \alpha \notin \mathbf{Q}$. The degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ must divide $[F : \mathbf{Q}] = 2$ and it cannot be equal to 1, since $\alpha \notin \mathbf{Q}$, hence $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2$ so that $F = \mathbf{Q}(\alpha)$. The minimal polynomial $m_{\alpha,F}(x)$ has the form $m_{\alpha,F}(x) = x^2 + bx + c$ and since α is a root, it must have the form

$$\alpha = \frac{-b + \sqrt{b^2 - 4c}}{2}$$

where $\sqrt{b^2 - 4c} \in \mathbf{C}$ is one choice of a square root. We then see that $F = \mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{b^2 - 4c}) = \mathbf{Q}(\sqrt{\frac{s}{t}})$ where $s, t \in \mathbf{Z}, t \neq 0$ are integers. We can then write

$$F = \mathbf{Q}\left(\sqrt{\frac{s}{t}}\right) = \mathbf{Q}\left(\sqrt{\frac{st}{t^2}}\right) = \mathbf{Q}\left(\frac{1}{t}\sqrt{st}\right) = \mathbf{Q}(\sqrt{st})$$

and $st \in \mathbf{Z}$. Finally, we can write $st = e^2 \cdot d$ for two integers $e, d \in \mathbf{Z}$ with d square-free, hence

$$F = \mathbf{Q}(\sqrt{e^2 d}) = \mathbf{Q}(e\sqrt{d}) = \mathbf{Q}(\sqrt{d}).$$

This shows that all finite extension $\mathbf{Q} \subseteq F$ of degree $[F : \mathbf{Q}] = 2$ have the form $\mathbf{Q}(\sqrt{d})$, where $d \in \mathbf{Z}$ is a square-free integer. These are called *quadratic extensions* of $\mathbf{Q}$.

Example 2.2.3. Consider the primitive third root of unity given by $\zeta_3 = e^{\frac{2\pi i}{3}} \in \mathbf{C}$. This is a root of $x^3 - 1 = (x - 1)(x^2 + x + 1)$ so it must be a root of the polynomial $\Phi_3(x) = x^2 + x + 1$. This is irreducible over $\mathbf{Q}$ (otherwise $\zeta_3 \in \mathbf{Q}$) hence it is the minimal polynomial of ζ_3. In particular we see that

$$\zeta_3 = \frac{-1 + \sqrt{-3}}{2}$$

so that $\mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$.

The examples of number fields that we have seen up to now are principal. This is always the case:

Theorem 2.2.4 (Primitive element theorem)**.** *Let $F \subseteq K$ be a finite extension of number fields. Then $K = F(\alpha)$ for a certain $\alpha \in K$. In particular, any number field K is a principal extension of $\mathbf{Q}$, meaning that $K = \mathbf{Q}(\alpha)$ for an $\alpha \in K$.*

Remark 2.2.5. This theorem, as well as all the results that we are going to present in this section about extension of number fields are true more generally for any *finite and separable* field extension. If a field F has characteristic zero, any extension is separable, so that this is the case of number fields. The same is true also of other fields, for example all finite fields.

2.2.2 Embeddings of number fields

Recall that a field K is called *algebraically closed* if every algebraic extension of $K \subseteq F$ is equal to K itself: $K = F$. Equivalently, this means that every polynomial in $K[x]$ splits as a product of linear factors in $K[x]$ (why is this equivalent?).

Example 2.2.6 (The fundamental theorem of algebra)**.** The fundamental theorem of algebra asserts that field of complex numbers $\mathbf{C}$ is algebraically closed.

By definition, any number field is an extension $\mathbf{Q} \subseteq K \subseteq \mathbf{C}$. How many other subfields of $\mathbf{C}$ are there that are isomorphic to it? This is answered more generally by the following simple but fundamental result

Proposition 2.2.7. *Let $F \subseteq K$ be an extension of number fields, let $\alpha \in K$ be such that $K = F(\alpha)$ and let $m_{\alpha,F}(x)$ be its minimal polynomial over F. Let $\sigma\colon F \hookrightarrow \mathbf{C}$ be a field embedding and assume that the polynomial $\sigma(m_{\alpha,F}) \in \mathbf{C}[x]$ splits as*

$$\sigma(m_{\alpha,F})(x) = (x - \alpha_1) \dots (x - \alpha_n), \qquad \alpha_i \in \mathbf{C}.$$

Then the embeddings $\sigma'\colon K \hookrightarrow \mathbf{C}$ such that $\sigma'_{|F} = \sigma$ are all those of the form

$$\sigma'\colon K = F(\alpha) \hookrightarrow \mathbf{C}, \quad \sigma'_{|F} = \mathrm{id}_F, \quad \sigma'(\alpha) = \alpha_i.$$

In particular, there are $[F : K]$ such embeddings.

Proof. We know that $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$, so that an embedding $\sigma'\colon F(\alpha) \hookrightarrow \mathbf{C}$ corresponds to an homomorphism $\widetilde{\sigma'}\colon F[x] \to \mathbf{C}$ such that $\widetilde{\sigma'}(m_{\alpha,F}(x)) = 0$. If we ask that $\widetilde{\sigma'}_{|F} = \sigma'$, the homomorphism $\widetilde{\sigma}$ is completely determined by the image $\widetilde{\sigma'}(x) \in \mathbf{C}$ and this needs to be a root of $\sigma(m_{\alpha,F}(x))$ because we want that $\widetilde{\sigma'}(m_{\alpha,F}(x)) = 0$. Since we are in characteristic zero, the polynomial $\sigma(m_{\alpha,F}(x))$ has $n = \deg \sigma(m_{\alpha,F}(x)) = \deg m_{\alpha,F}(x) = [F(\alpha) : F]$ distinct roots in $\mathbf{C}$ and this proves the last statement. □

As an immediate consequence of Proposition B.2.20, we get:

Corollary 2.2.8. *1. If $F \subseteq K$ is an extension of number fields, there are $[K : F]$ distinct embeddings $\sigma\colon K \hookrightarrow \mathbf{C}$ such that $\sigma_{|F} = \mathrm{id}_F$.*

2. If $\mathbf{Q} \subseteq K$ is a number field, there are $[K : \mathbf{Q}]$ distinct embeddings $K \hookrightarrow \mathbf{C}$.

Proof. The first point follows from Proposition B.2.20 with the base embedding being $\mathrm{id}_K\colon K \to K$. For the second point, we observe that any embedding $\sigma\colon K \hookrightarrow \mathbf{C}$ satisfies the property $\sigma_{|\mathbf{Q}} = \mathrm{id}_{\mathbf{Q}}$ (why?). □

Example 2.2.9. Consider the number field $\mathbf{Q} \subseteq \mathbf{Q} \subseteq \mathbf{Q}(\sqrt{d})$, where $d \in \mathbf{Z}$ is a square-free integer. We know that the minimal polynomial of $\sqrt{d}$ is $m_{\alpha,\mathbf{Q}}(x) = x^2 - d$ and its roots are $\pm\sqrt{d}$. Hence there are two embeddings $\mathbf{Q}(\sqrt{d})$ that restrict to $\mathrm{id}_{\mathbf{Q}}$:

$$\mathrm{id}_{\mathbf{Q}(\sqrt{d})}\colon a + b\sqrt{d} \mapsto a + b\sqrt{d}, \qquad \sigma\colon a + b\sqrt{d} \mapsto a - b\sqrt{d},$$

Notice that the image of both these embeddings is again the same field $\mathbf{Q}(\sqrt{d})$ and these two embeddings give rise to two automorphisms $\mathbf{Q}(\sqrt{d}) \to \mathbf{Q}(\sqrt{d})$.

Example 2.2.10. Consider the number field $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2})$. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbf{Q}$ is $x^3 - 2$ and this splits over $\mathbf{C}$ as

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2}\zeta_3^2)$$

where $\zeta_3 = e^{\frac{2\pi i}{3}}$ is a primitive third root of unity. Hence, there are three embeddings $\mathbf{Q}(\sqrt[3]{2}) \hookrightarrow \mathbf{C}$, defined by

$$\mathrm{id}_{\mathbf{Q}(\sqrt[3]{2})} \colon \sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad \sigma_2 \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3, \quad \sigma_3 \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^2$$

Notice that the only one of these that sends $\mathbf{Q}(\sqrt[3]{2})$ to itself is the identity: indeed the image of the other two is not even contained in $\mathbf{R}$.

Example 2.2.11 (Cyclotomic fields)**.** For $n \in \mathbf{Z}_{>0}$ define $\zeta_n = e^{\frac{2\pi i}{n}}$. This is a primitive n-th root of unity, hence a root of

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i)$$

This shows that ζ_n integral over $\mathbf{Z}$. The number field $\mathbf{Q}(\zeta_n)$ is called the n-th cyclotomic field. The n-th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{1 \le i \le n-1 \\ \mathrm{GCD}(i,n)=1}} (x - \zeta_n^i)$$

which is a priori a polynomial with complex coefficients. We want to consider the minimal polynomial $m_{\zeta_n, \mathbf{Q}}(x)$: we know that

$$m_{\zeta_n, \mathbf{Q}}(x) = \prod_{\sigma \colon \mathbf{Q}(\zeta_n) \hookrightarrow \mathbf{C}} (x - \sigma(\zeta_n))$$

and since $m_{\zeta_n, \mathbf{Q}}(x) | x^n - 1$, we see that $\sigma(\zeta_n) = \zeta_n^i$ for some $0 \le i \le n-1$. Now we observe that ζ_n has order n as an element in the multiplicative group $\mathbf{C}^\times$ so that the same must be true of $\sigma(\zeta_n)$ for any embedding $\sigma \colon \mathbf{Q}(\zeta_n) \hookrightarrow \mathbf{C}$. This shows that $\sigma(\zeta_n) = \zeta_n^i$ for some $0 \le i \le n-1$ with $\mathrm{GCD}(n, i) = 1$. In other words

$$m_{\zeta_n, \alpha}(x) \mid \Phi_n(x) \qquad \text{in } \mathbf{C}[x]$$

It turns out that these two polynomials are actually equal

$$m_{\zeta_n, \mathbf{Q}}(x) = \Phi_n(x)$$

so that $\mathbf{Q}(\zeta_n)$ is a number field of degree

$$\mathbf{Q}(\zeta_n) = \#\{i \in \{0, \ldots, n-1\} \mid \mathrm{GCD}(i, n) = 1\} = \varphi(n)$$

where ϕ is Euler's totient function (or phi-function). The fact that $m_{\zeta_n, \mathbf{Q}}(x) = \Phi_n(x)$ or, equivalently, that the cyclotomic polynomial has integer coefficients and is irreducible in $\mathbf{Q}[x]$, is non-trivial and we will maybe see a proof later for the general case. However, the case of $n = p$ a prime number is easier: in this case

$$\Phi_p(x) = \prod_{i=1}^{n-1} (x - \zeta_n^i) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

and you are asked to prove in one exercise sheet that this is irreducible in $\mathbf{Q}[x]$ via Eisenstein's criterion.

2.2.3 Normal extensions and the Galois group

From the last two examples, we are naturally led to the following definition:

Definition 2.2.12 (Normal extension)**.** An extension of number fields $F \subseteq K$ is called *normal* if for every embedding $\sigma\colon K \hookrightarrow \mathbf{C}$ such that $\sigma_{|F} = \mathrm{id}_F$ it holds that $\sigma(K) = K$.

Example 2.2.13. Previous examples show the extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{d})$ with d square-free is normal, while the extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2})$ is not.

Lemma 2.2.14. *Let $F \subseteq K$ be an extension of number fields. Then the following are equivalent:*

1. *The extension $F \subseteq K$ is normal.*
2. *If $\alpha \in K$ is such that $K = F(\alpha)$, then minimal polynomial $m_{\alpha,F}(x)$ splits as a product of linear factors in $K[x]$.*
3. *$K = F(\alpha_1, \ldots, \alpha_n)$ where the $\alpha_i \in \mathbf{C}$ are the roots of a polynomial $P(x) \in F[x]$.*

Proof. (1) $\implies$ (2). If the extension is normal and if $\sigma_1, \ldots, \sigma_n\colon K \hookrightarrow \mathbf{C}$ are all the embeddings such that $\sigma_{i,|F} = \mathrm{id}_F$, then we know that $\sigma_i(\alpha) \in K$ and that the $\sigma_i(\alpha)$ are precisely the roots of $m_{\alpha,F}(x)$ over F.

(2) $\implies$ (3). Let $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$ be the roots of $m_\alpha(x)$ in $\mathbf{C}$ and assume that $\alpha = \alpha_1$. Then $\alpha_i \in K$ by assumption, and $K = F(\alpha) \subseteq F(\alpha_1, \ldots, \alpha_n) \subseteq K$, hence $K = F(\alpha_1, \ldots, \alpha_n)$.

(3) $\implies$ (1). Any embedding $\sigma\colon K \hookrightarrow \mathbf{C}$ such that $\sigma_{|F} = \mathrm{id}_F$ preserves the polynomial $P(t)$, meaning that $\sigma(P(t)) = P(t)$. We can assume that $P(t)$ is monic, so that

$$(t - \alpha_1) \ldots (t - \alpha_n) = P(t) = \sigma(P(t)) = (t - \sigma(\alpha_1)) \ldots (t - \sigma(\alpha_n))$$

Hence σ permutes the α_i and in particular $\sigma(K(\alpha_1, \ldots, \alpha_n)) \subseteq K(\alpha_1, \ldots, \alpha_n)$. □

In particular, if $K \subseteq K(\alpha)$ is an extension of number fields and if $m_\alpha(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ with $\alpha_i \in \mathbf{C}$, the smallest normal extension of K that contains $K(\alpha)$ is $K(\alpha_1, \ldots, \alpha_n)$. This is called *the normal closure* of the extension $K \subseteq K(\alpha)$.

Example 2.2.15. The normal closure of $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2})$ is $\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2) = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$.

The terminology of normal extension comes from group theory:

Definition 2.2.16 (Galois group)**.** The Galois group of an extension $K \subseteq F$ of number fields is

$$\mathrm{Aut}(F/K) = \{\sigma : F \longrightarrow F \mid \sigma \text{ isomorphism}, \sigma|_K = \mathrm{id}_K\}$$

Remark 2.2.17. By definition, an element of $\mathrm{Aut}(F/K)$ is a field embedding $\sigma\colon F \hookrightarrow \mathbf{C}$ such that $\sigma_{|K} = \mathrm{id}_K$ and $\sigma(F) = F$. In particular, we see that $|\mathrm{Aut}(F/K)| \leq [F : K]$ with equality if and only if $K \subseteq F$ is a normal extension.

If $K \subseteq F$ is an extension of number fields, for every subgroup $G < \mathrm{Aut}(F/K)$ we define its fixed field (you should check that this is indeed a field) as

$$\mathrm{Fix}(G) = \{\alpha \in F \mid \sigma(\alpha) = \alpha, \text{ for all } \sigma \in G\}$$

and this is an intermediate extension $K \subseteq \mathrm{Fix}(F/K) \subseteq F$. Conversely, if there is an intermediate extension $K \subseteq F' \subseteq F$, then there is a subgroup

$$\mathrm{Aut}(F/F') < \mathrm{Aut}(F/K)$$

The correspondence between subgroups and intermediate extension is particularly nice if $F \subseteq K$ is a normal extension, and it is described by the following:

Theorem 2.2.18 (Fundamental theorem of Galois theory)**.** *Let $K \subseteq F$ be a normal extension of number fields. Then there is a bijection*

$$\left\{ \begin{matrix} \textit{subgroups} \\ \textit{of } \mathrm{Gal}(F/K) \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \textit{subextensions} \\ K \subseteq F' \subseteq F \end{matrix} \right\}, \quad G \longmapsto \mathrm{Fix}(G), \quad \mathrm{Gal}(F/F') \hookleftarrow F'.$$

Furthermore, the extension $K \subseteq F'$ is normal if and only if $\mathrm{Aut}(F/F') < \mathrm{Aut}(F/K)$ is a normal subgroup, and in this case

$$\mathrm{Aut}(F'/K) \cong \mathrm{Aut}(F/K)/\mathrm{Aut}(F/F')$$

In particular, if we apply the bijection to the extension $K \subseteq K \subseteq F$ itself we get.

Corollary 2.2.19. *If $K \subseteq F$ is a normal extension of number fields, then $\mathrm{Fix}(\mathrm{Aut}(F/K)) = K$.*

Example 2.2.20. Let $d \in \mathbf{Z}$ be a square-free integer and let $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{d})$ be the corresponding number field. Then this is a normal extension and its Galois group is $\mathrm{Aut}(\mathbf{Q}(\sqrt{d})/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$, generated by $\sigma\colon \mathbf{Q}(\sqrt{d}) \mapsto \mathbf{Q}(\sqrt{d}), \sqrt{d} \mapsto -\sqrt{d}$. The only intermediate extensions $\mathbf{Q} \subseteq K \subseteq \mathbf{Q}(\sqrt{d})$ are $K = \mathbf{Q}$ and $K = \mathbf{Q}(\sqrt{d})$. This reflects the fact that $\mathbf{Z}/2\mathbf{Z}$ has no non-trivial subgroups.

Example 2.2.21. ($\star$) The Galois group of the extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2})$ is trivial $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{\mathrm{id}_{\mathbf{Q}(\sqrt[3]{2})}\}$. Consider now the normal closure $K = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$. We first claim that $[K : \mathbf{Q}] = 6$. Indeed, we have $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q} \subseteq \mathbf{Q}(\zeta_3)$ so that $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ and $[\mathbf{Q}(\zeta_3) : \mathbf{Q}] = 2$ must divide $[K : \mathbf{Q}]$, so that this is a multiple of 6. On the other hand, the minimal polynomial of $\sqrt[3]{2}$ over $\mathbf{Q}(\zeta_3)$ must divide the minimal polynomial $x^3 - 2$ of $\sqrt[3]{2}$ over $\mathbf{Q}$, so that $[K : \mathbf{Q}(\zeta_3)] \leq 3$. Since $[K : \mathbf{Q}] = [K : \mathbf{Q}(\zeta_3)] \cdot [\mathbf{Q}(\zeta_3) : \mathbf{Q}] \leq 6$, we see that $[K : \mathbf{Q}] = 6, [K : \mathbf{Q}(\zeta_3)] = 3$.

Now we want to determine the Galois group $\mathrm{Aut}(K/\mathbf{Q})$: the intermediate extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{\zeta_3})$ has two embeddings $\mathbf{Q}(\sqrt{\zeta_3}) \hookrightarrow \mathbf{C}, i = 1, 2$, given by

$$\mathrm{id}_{\mathbf{Q}(\sqrt{\zeta_3})}, \sigma\colon \mathbf{Q}(\zeta_3) \to \mathbf{Q}(\zeta_3), \quad \sigma(\zeta_3) = \zeta_3^{-1}.$$

Thanks to Proposition B.2.20, we see that $\mathrm{id}_{\mathbf{Q}(\sqrt{\zeta_3})}$ extends to three different embeddings $\tau_i\colon K \hookrightarrow \mathbf{C}, i = 1, 2, 3$, while σ extends to other three different embeddings $\sigma_j\colon K \hookrightarrow \mathbf{C}, j = 1, 2, 3$. These six must then be all the elements in $\mathrm{Aut}(K/\mathbf{Q})$ (think about it until it is clear). Proposition $B.2.20$ tells us also how to determine the τ_i and the σ_j explicitly: the minimal polynomial of $\sqrt[3]{2}$ over $\mathbf{Q}(\zeta_3)$ is $x^2 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2})$ and both $\mathrm{id}_{\mathbf{Q}(\zeta_3)}$ and σ leave it invariant. Then Proposition B.2.20 shows that

$$\tau_i\colon K \longrightarrow K, \begin{matrix} \zeta_3 \mapsto \zeta_3, \\ \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^i, \end{matrix} \qquad \sigma_i\colon K \longrightarrow K, \begin{matrix} \zeta_3 \mapsto \zeta_3^{-1}, \\ \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3^i \end{matrix} \qquad \text{for } i = 1, 2, 3.$$

As a group, one can show that $\mathrm{Aut}(K/\mathbf{Q}) \cong \mathfrak{S}_3$ the symmetric group of order three. The only non-trivial normal subgroup of $\mathfrak{S}_3$ is the alternating subgroup generated by the even permutations, which in this case are the elements of order three, given by τ_1, τ_2, τ_3. Hence the unique non-trivial normal intermediate extension is $\mathrm{Fix}(\tau_1, \tau_2, \tau_3) = \mathbf{Q}(\zeta_3)$. Each one of the σ_i has order two and it gives to an intermediate extension $F_i = \mathrm{Fix}(\sigma_i) = \mathbf{Q}(\sqrt[3]{2} \cdot \zeta_3^i)$. These are all the non-trivial intermediate extensions $\mathbf{Q} \subseteq K$.

Remark 2.2.22. ($\star$) Notice that in the previous example we have studied the field extension $K = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ without writing it as $K = \mathbf{Q}(\alpha)$ for a generator $\alpha \in K$. Indeed, even if it useful to know that a single generator exists, it is often non-trivial to find one, and it is often not necessary. In this case, you can check as an exercise that a a generator of K is given by $\alpha = \zeta_3 + \sqrt[3]{2}$.

2.2.4 Trace, norm and the characteristic polynomial

Let $F \subseteq K$ be an extension of number fields. Then K is a F-vector space of degree $n = [K : F]$ and for any $\alpha \in K$ the multiplication-by-α map

$$(\cdot\alpha)\colon K \longrightarrow K, \quad x \longmapsto \alpha x.$$

is an F-linear map.

Definition 2.2.23 (Trace, norm and characteristic polynomial)**.** In the above notation, the *trace and the norm of α with respect to the extension $F \subseteq K$* are the trace and the determinant of the F-linear map $(\cdot\alpha)\colon K \to K$:

$$\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}(\cdot\alpha), \quad \mathrm{N}_{K/F}(\alpha) = \det(\cdot\alpha).$$

The *characteristic polynomial of α with respect to the extension $F \subseteq K$* is the characteristic polynomial of the F-linear map $(\cdot\alpha)$. This is a monic polynomial of degree $n = [K : F]$ of the form

$$\chi_{\alpha,K/F}(x) = \det(x \cdot I_n - (\cdot\alpha)) = x^n - \mathrm{Tr}_{F/K}(\alpha)x^{n-1} + \cdots + (-1)^n \mathrm{N}_{F/K}(\alpha).$$

The coefficients of the characteristic polynomial $\chi_{\alpha,K/F}(x)$ are in the base field F and in particular this is true of norm and trace. So this defines two maps

$$\mathrm{Tr}_{K/F}\colon K \to F, \qquad \mathrm{N}_{K/F}\colon K \to F.$$

Example 2.2.24. Assume that $\alpha \in F$ so that the matrix representing $(\cdot\alpha)\colon K \to K$ as an F-linear map is simply $\alpha \cdot I_n$, where $n = [K : F]$. Then

$$\chi_{K/F,\alpha}(x) = (x - \alpha)^{[K:F]}, \quad \mathrm{Tr}_{K/F}(\alpha) = [K : F] \cdot \alpha, \quad \mathrm{N}_{K/F}(\alpha) = \alpha^{[K:F]}$$

Remark 2.2.25. Let $F \subseteq K$ be an extension of number fields and let $\alpha \in K$. The Cayley-Hamilton theorem A.5.20 shows that $\chi_{K/F,\alpha}(\alpha) = 0$ (think about this until it is clear), hence the characteristic polynomial is divided by the minimal polynomial:

$$m_{F,\alpha}(x) \mid \chi_{K/F,\alpha}(x) \quad \text{in } F[x].$$

Example 2.2.26. Assume that $K = F(\alpha)$ has degree $[F(\alpha) : F] = n$. In particular both the minimal polynomial $m_{F,\alpha}(x)$ and the characteristic polynomial $\chi_{F(\alpha)/F,\alpha}(x)$ are monic of degree n, and since the minimal polynomial always divides the characteristic polynomial we must have

$$m_{F,\alpha}(x) = \chi_{F(\alpha)/F,\alpha}(x)$$

So we can read off the trace $\mathrm{Tr}_{F(\alpha)/F}(\alpha)$ and norm $\mathrm{N}_{F(\alpha)/F}(\alpha)$ from the coefficients of the minimal polynomial:

$$m_{F,\alpha}(x) = x^n - \mathrm{Tr}_{F(\alpha)/F}(\alpha)x^{n-1} + \cdots + (-1)^n \mathrm{N}_{F(\alpha)/F}(\alpha)$$

This is actually the most important example, because of the following:

Lemma 2.2.27. *Let $F \subseteq K$ be an extension of number fields and let $\alpha \in K$. Then*

$$\chi_{K/F,\alpha}(x) = \chi_{F(\alpha)/F}(x)^{[K:F(\alpha)]},\ \mathrm{Tr}_{K/F}(\alpha) = [K : F(\alpha)]\cdot\mathrm{Tr}_{F(\alpha)/F}(x),\ \mathrm{N}_{K/F}(x) = \mathrm{N}_{F(\alpha)/F}(\alpha)^{[K:F(\alpha)]}.$$

Proof. The statement on the characteristic polynomial implies the other two (why?). To show the one about the characteristic polynomial, let $\beta_1, \ldots, \beta_m$ be a basis of K as an $F(\alpha)$-vector space. Then there is a decomposition of $F(\alpha)$-vector spaces $K = \bigoplus_{i=1}^m F(\alpha) \cdot \beta_i$ and these are invariant subspaces for the multiplication-by-α map $(\cdot\alpha)$. The restriction of $(\cdot\alpha)$ to each of these, seen as a F-linear map, has characteristic polynomial $\chi_{F(\alpha)/F}(x)$, hence the characteristic polynomial of $(\cdot\alpha)\colon K \to K$, seen as an F-linear map is $\chi_{K/F,\alpha}(x) = \chi_{F(\alpha)/F,\alpha}(x)^{[K:F(\alpha)]}$. □

Theorem 2.2.28 (Properties of trace and norm and characteristic polynomial)**.** *Let $F \subseteq K$ be an extension of number fields.*

1. *The trace is F-linear and the norm is multiplicative: for all $\alpha, \beta \in K, a, b \in F$ it holds that*

$$\mathrm{Tr}_{F/K}(a \cdot \alpha + b \cdot \beta) = a \cdot \mathrm{Tr}_{F/K}(\alpha) + b \cdot \mathrm{Tr}_{F/K}(\beta), \qquad \mathrm{N}_{F/K}(\alpha \cdot \beta) = \mathrm{N}_{F/K}(\alpha) \cdot \mathrm{N}_{F/K}(\beta)$$

2. *If $\sigma_1, \ldots, \sigma_n\colon K \hookrightarrow \mathbf{C}$ are all the embeddings of K such that $\sigma_{|F} = \mathrm{id}_F$, it holds that*

$$\chi_{K/F,\alpha}(x) = (x - \sigma_1(\alpha)) \ldots (x - \sigma_n(\alpha)),$$
$$\mathrm{Tr}_{K/F}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha), \quad \mathrm{N}_{K/F}(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha) \qquad \text{for all } \alpha \in K$$

Proof. 1. This follows from the fact that the trace is a linear function on matrices and the determinant a multiplicative one.

2. If we prove the statement on the characteristic polynomial, the other two follow because

$$(x-\sigma_1(\alpha)) \ldots (x-\sigma_n(\alpha)) = x^n - (\sigma_1(\alpha) + \ldots + \sigma_n(\alpha))x^{n-1} + \cdots + (-1)^n \cdot \sigma_1(\alpha) \ldots \sigma_n(\alpha).$$

For the characteristic polynomial, assume first that $K = F(\alpha)$. Then we know from Example 2.2.26 that the characteristic polynomial is equal to the minimal polynomial $\chi_{K/F,\alpha}(x) = m_{F,\alpha}(x)$, and we know from Proposition B.2.20, that $m_{F,\alpha}(x) = (x-\sigma_1(\alpha)) \ldots (x-\sigma_n(\alpha))$. In the general case, consider the tower of extensions $F \subseteq F(\alpha) \subseteq K$ and let $n = [F(\alpha) : F], m = [K : F(\alpha)]$. Lemma 2.2.27 shows that $\chi_{K/F,\alpha}(x) = \chi_{F(\alpha)/F,\alpha}(x)^m$. Let $\sigma_1, \ldots, \sigma_n\colon F(\alpha) \hookrightarrow \mathbf{C}$ be the embeddings such that $\sigma_{i,|F} = \mathrm{id}_F$. Proposition B.2.20 shows that each one of these extends to m distinct embeddings $\sigma_{i,j}\colon K \hookrightarrow \mathbf{C}$ for $j = 1, \ldots, m$ and these are all the embeddings $K \hookrightarrow \mathbf{C}$ that act as the identity on F. Hence we see that

$$\prod_{i=1}^n \prod_{j=1}^m (x - \sigma_{i,j}(\alpha)) = \prod_{i=1}^n (x - \sigma_i(\alpha))^m = \left(\prod_{i=1}^n (x - \sigma_i(\alpha))^m\right) = \chi_{F(\alpha)/F,\alpha}(x)^m. \qquad \square$$

The phenomenon that we have seen in the proof of Theorem 2.2.28 generalizes

Theorem 2.2.29 ($\star$)**.** *Trace and norm are transitive: if $F \subseteq L \subseteq K$ is a tower of number fields, it holds that*

$$\mathrm{Tr}_{L/F} = \mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{L/K}, \qquad \mathrm{N}_{L/F} = \mathrm{N}_{K/F} \circ \mathrm{N}_{L/K}\,.$$

($\star$) *Comments on the proof.* I will maybe write the proof of a more general fact in an appendix. In the meantime, if you are curious, observe that this result is related to the following natural question: if V is a finite-dimensional K-vector space, then it is also a finite-dimensional vector space ovee F, and if $f\colon V \to V$ is a K-linear map, then f is also an F-linear map. What is the relation between the trace (or the determinant, or the characteristic polynomial) of f seen as a K-linear map and the one of f seen as an F-linear map? □

The trace as a bilinear form

Let $F \subseteq K$ be an extension of number fields. The trace gives an F-bilinear map

$$\mathrm{Tr}_{K/F}\colon K \times K \longrightarrow F, \qquad (\alpha, \beta) \longmapsto \mathrm{Tr}_{K/F}(\alpha\beta),$$

of F-vector spaces. Equivalently, this gives an F-linear map

$$\mathrm{Tr}'_{K/F}\colon K \longrightarrow \mathrm{Hom}_F(K, F), \qquad \alpha \longmapsto \mathrm{Tr}_{K/F}(\alpha\,\cdot\,)$$

This is a non-degenerate bilinear form:

Theorem 2.2.30. *The bilinear form $\mathrm{Tr}_{K/F}$ is nondegenerate. This means, equivalently, that*

(a) there is no $\alpha \neq 0$ such that $\mathrm{Tr}_{K/F}(\alpha\beta) = 0$ for all $\beta \in K$,

(b) the map $\mathrm{Tr}'_{K/F}\colon K \to \mathrm{Hom}_F(K, F)$ is an isomorphism of F-vector spaces.

(c) for any basis $\alpha_1, \ldots, \alpha_n \in K$ of K as an F-vector space, there is a unique other basis $\beta_1, \ldots, \beta_n \in K$ of K as an F-vector space such that

$$\mathrm{Tr}_{K/F}(\alpha_i\beta_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

Proof. The equivalence of the three statements is a fact from linear algebra. We prove that (a) holds: if there is such an α, then for any $\gamma \in K$ it holds that

$$\mathrm{Tr}_{K/F}(\gamma) = \mathrm{Tr}_{K/F}(\alpha(\alpha^{-1}\gamma) = 0.$$

It is enough to prove that $\mathrm{Tr}_{K/F}$ is not identically zero: observe that, $\mathrm{Tr}_{K/F}(1) = [K : F] \neq 0$. □

2.3 Rings of integers of number fields

In the first chapter we considered the Gaussian integers $\mathbf{Z}[i]$ as a subring of the number field $\mathbf{Q}(i)$. We generalize this to a key definition:

Definition 2.3.1 (Ring of integers of a number field)**.** Let $\mathbf{Q} \subseteq K$ be a number field. Its ring of integers is the integral closure of $\mathbf{Z}$ inside K:

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

Remark 2.3.2. We know from Corollary 2.1.9 that this is indeed a subring of K.

Example 2.3.3. Let $d \in \mathbf{Z}$ be a square-free integer and consider the corresponding quadratic extension $\mathbf{Q}(\sqrt{d})$. We have of course that $\mathbf{Z}[\sqrt{d}] \subseteq \mathcal{O}_Q(\sqrt{d})$, but the ring $\mathcal{O}_K$ could be larger: for example, we have seen in Example 2.1.3 that if $d \equiv 1 \pmod 4$, then $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_Q(\sqrt{d})$.

We want to study number fields and their rings of integers in a systematic way.

Lemma 2.3.4. *Let K be a number field and let $\sigma\colon K \hookrightarrow \mathbf{C}$ be an embedding. If $\alpha \in K$ is integral over $\mathbf{Z}$, then $\sigma(\alpha)$ is also integral over $\mathbf{Z}$.*

Proof. By assumption, there are $a_{n-1}, \dots, a_0 \in \mathbf{Z}$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ Since any embedding $\sigma\colon K \hookrightarrow \mathbf{C}$ is the identity on $\mathbf{Q}$, we see that

$$\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0,$$

Then $\sigma(\alpha)$ is integral over $\mathbf{Z}$. □

We also observe that integral elements in a number field can be characterized by their minimal polynomial and characteristic polynomial.

Lemma 2.3.5. *Let K be a number field and $\alpha \in K$. The following are equivalent:*

1. *α is integral over $\mathbf{Z}$.*
2. *The characteristic polynomial $\chi_{K/\mathbf{Q},\alpha}(x)$ has coefficients in $\mathbf{Z}$.*
3. *The minimal polynomial $m_{\alpha,\mathbf{Q}}(x)$ has coefficients in $\mathbf{Z}$.*

In particular, if $\alpha \in \mathcal{O}_K$ the trace and the norm are integers: $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha), \mathrm{N}_{K/\mathbf{Q}}(\alpha) \in \mathbf{Z}$

Proof. If one of the two monic polynomials $m_{\alpha,\mathbf{Q}}(x)$ or $\chi_{K/\mathbf{Q},\alpha}(x)$ has integer coefficients, then α must be integral, since α is a root of both.

Assume instead that α is integral over $\mathbf{Z}$ and let $\sigma_1, \dots, \sigma_n\colon K \hookrightarrow \mathbf{C}$ be all the embeddings of K in $\mathbf{C}$. Then we know from Lemma 2.3.4 that $\sigma_i(\alpha)$ is integral over $\mathbf{Z}$ for each i, and then Theorem 2.2.28 shows that

$$\chi_{K/\mathbf{Q},\alpha}(x) = \Pi_{i=1}^n (x - \sigma_i(\alpha))$$

so that the coefficients of $\chi_{K/\mathbf{Q},\alpha}(x)$ are polynomial expressions of the $\sigma_i(\alpha)$. This means that $\chi_{K/\mathbf{Q}}(x)$ is a polynomial with rational coefficients that are integral over $\mathbf{Z}$. As $\mathbf{Z}$ is integrally closed in $\mathbf{Q}$, this means that these coefficients are in $\mathbf{Z}$. In particular, if we take $K = \mathbf{Q}(\alpha)$ we see that $m_{\alpha,\mathbf{Q}}(x) = \chi_{\mathbf{Q}(\alpha)/\mathbf{Q},\alpha}(x) \in \mathbf{Z}[x]$.

The last statement follows because $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha), \mathrm{N}_{K/\mathbf{Q}}(\alpha)$ are coefficients of $\chi_{K/\mathbf{Q},\alpha}(x)$. □

We can now determine the ring of integers of a quadratic extension:

Example 2.3.6 (Ring of integers of a quadratic extension)**.** Let $d \in \mathbf{Z}$ be a square-free integer and consider the quadratic extension $\mathbf{Q}(\sqrt{d})$ of $\mathbf{Q}$. The ring of integers of $\mathbf{Q}(\sqrt{d})$ is by definition the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{d})$:

$$\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \{\alpha \in \mathbf{Q}(\sqrt{d}) \,|\, \alpha \text{ integral over } \mathbf{Z}\}$$

We will show that

$$\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \begin{cases} \mathbf{Z}[\sqrt{d}] & d \equiv 2,3 \pmod 4, \\ \mathbf{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4. \end{cases}$$

(notice that if $d \equiv 0 \pmod 4$ then it is not square-free). Let $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ with $a, b \in \mathbf{Q}$. If $b = 0$, then $\alpha \in \mathbf{Q}$ so that $\alpha \in \mathbf{Z}$. Assume then that $b \neq 0$ so that $\alpha \notin \mathbf{Q}$. We observe that the polynomial

$$(x - a - b\sqrt{d})(x - a + b\sqrt{d}) = (x-a)^2 - db^2 = x^2 - 2ax + (a^2 - db^2)$$

is monic, with rational coefficients and vanishes at α. It must then be the minimal polynomial of α over $\mathbf{Q}$ (why?). Lemma 2.3.5 proves that $2a \in \mathbf{Z}, a^2 - db^2 \in \mathbf{Z}$. Write $a = \frac{A}{2}$ for $A \in \mathbf{Z}$ and $b = \frac{B}{C}$ for $B, C \in \mathbf{Z}$ coprime. Then

$$a^2 - db^2 = \frac{A^2}{4} - d\frac{B^2}{C^2} = K \in \mathbf{Z}$$

and then $A^2C^2 - 4KC^2 = 4d \cdot B^2$. We see that $C^2 \mid 4d$ and since d is square-free it must be that $C^2 \mid 4$, so we can write

$$4 = EC^2, \quad dEB^2 = A^2 - 4K \quad \text{for a certain } E \in \mathbf{Z}.$$

The first equation gives only the two possibilities $E = 4, C^2 = 1$ or $E = 1, C^2 = 4$. In the first case, we see that $b \in \mathbf{Z}$ and $A^2 \equiv 0 \pmod 4$ so that A is even and $a \in \mathbf{Z}$ as well, meaning $\alpha \in \mathbf{Z}[\sqrt{d}]$. In the second case, we can assume $C = 2$ so that we have

$$\alpha = \frac{A + B\sqrt{d}}{2}, \quad A^2 - dB^2 = 4K$$

We consider the three cases, recalling that A^2 is only $0, 1$ modulo 4, according to whether A is even or odd.

- $d \equiv 1 \pmod 4$: $A^2 \equiv B^2 \pmod 4$ so that A, B are either both even or both odd. In the first case $\alpha \in \mathbf{Z}[\sqrt{d}]$ and in the second case $\alpha \in \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.
- $d \equiv 2 \pmod 4$: $A^2 \equiv 2B^2 \pmod 4$, so that A, B must be both even, and then $\alpha \in \mathbf{Z}[\sqrt{d}]$.
- $d \equiv 3 \pmod 4$: $A^2 \equiv -B^2 \pmod 4$, so that A, B must be both even, and then $\alpha \in \mathbf{Z}[\sqrt{d}]$.

Example 2.3.7. The previous example shows that $\mathcal{O}_{\mathbf{Q}(i)} = \mathbf{Z}[i]$.

We now look at applications of the norm and the trace. The norm characterizes invertible elements as in the examples that we have seen:

Proposition 2.3.8. *Let K be a number field*

1. *If $\alpha \in K$, then $N_{K/\mathbf{Q}}(\alpha) = 0$ if and only if $\alpha = 0$.*
2. *If $\alpha \in \mathcal{O}_K$, there is $\beta \in \mathcal{O}_K$ such that $\alpha\beta = \mathrm{N}_{K/\mathbf{Q}}(\alpha)$.*
3. *If $\alpha \in \mathcal{O}_K$, then $\alpha \in \mathcal{O}_K^\times$ if and only if $\mathrm{N}_{K/\mathbf{Q}}(\alpha) \in \mathbf{Z}^\times$.*

Proof. 1. If we look at K as a $\mathbf{Q}$-vector space, the multiplication-by-α map $\cdot\alpha\colon K \to K$ fails to be an isomorphism if and only if it is zero. Hence, it has zero determinant if and only if it is itself zero.

2. The characteristic polynomial $\chi_{K/\mathbf{Q},\alpha}(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ has constant term $a_0 = (-1)^n \mathrm{N}_{K/\mathbf{Q}}(\alpha)$. The Cayley-Hamilton theorem shows that $\chi_{K/\mathbf{Q}}(\alpha) = 0$, hence

$$(-1)^n \mathrm{N}_{K/\mathbf{Q}}(\alpha) = -(\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha) = -(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1)\alpha$$

Since $\alpha \in \mathcal{O}_K$ we know that $a_i \in \mathbf{Z}$ for all $i = 1, \ldots, n-1$, so that $\beta = (-1)^{n+1}(\alpha^{n-1} + \ldots + a_1) \in \mathcal{O}_K$ satisfies $\alpha\beta = \mathrm{N}_{K/\mathbf{Q}}(\alpha)$.

3. Assume $\alpha \neq 0$ and let $\beta \in \mathcal{O}_K$ such that $\alpha\beta = \mathrm{N}_{K/\mathbf{Q}}(\alpha)$. If $\mathrm{N}_{K/\mathbf{Q}}(\alpha)^{-1} \in \mathbf{Z}$, then $\alpha^{-1} = \mathrm{N}_{K/\mathbf{Q}}(\alpha)^{-1} \cdot \beta \in \mathcal{O}_K$. Conversely, if $\alpha^{-1} \in \mathcal{O}_K$, then $\mathrm{N}_{K/\mathbf{Q}}(\alpha^{-1}) \in \mathbf{Z}$ and $N_{K/\mathbf{Q}}(\alpha) \cdot N_{K/\mathbf{Q}}(\alpha^{-1}) = N_{K/\mathbf{Q}}(\alpha\alpha^{-1}) = N_{K/\mathbf{Q}}(1) = 1$.

□

This was a result about the multiplicative structure of $\mathcal{O}_K$, which was obtained via the multiplicative norm. Instead the additive trace is going to give us a fundamental result about the additive structure of $\mathcal{O}_K$ as an abelian group.

2.3.1 The ring of integers as an abelian group

We start with a simple but useful lemma:

Lemma 2.3.9. *Let $\mathbf{Q} \subseteq K$ be a number field and $\mathcal{O}_K$ its ring of integers.*

1. *For any $\alpha \in K$, there is $b \in \mathbf{Z}$ such that $b \cdot \alpha \in \mathcal{O}_K$.*
2. *There is $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$.*
3. *There is a basis $\alpha_1, \ldots, \alpha_n$ of K as a $\mathbf{Q}$-vector space with $\alpha_i \in \mathcal{O}_K$ for all $i = 1, \ldots, n$.*

Proof. 1. We know that α is a root of a monic polynomial with coefficients in $\mathbf{Q}$, hence we can write

$$\alpha^n + \frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \cdots + \frac{a_1}{b_1}\alpha + \frac{a_0}{b_0} = 0$$

for some $a_i, b_i \in \mathbf{Z}, b_i \neq 0$. If we set $b = b_0b_1 \ldots b_{n-1}$ and we multiply this equation by b^n, we get

$$(b\alpha)^n + a_{n-1} \cdot \frac{b}{b_{n-1}}(b\alpha)^{n-1} + \cdots + a_1 \cdot \frac{b^{n-1}}{b_1}(b\alpha) + a_0 \cdot \frac{b^n}{b_0} = 0$$

which is a monic equation with coefficients in $\mathbf{Z}$. Hence $b\alpha \in \mathcal{O}_K$.

2. Let $\beta \in K$ be such that $K = \mathbf{Q}(\beta)$ and let $b \in \mathbf{Z}$ such that $b\beta \in \mathcal{O}_K$. Then $K = \mathbf{Q}(b\beta)$.

3. Take any basis $\alpha_1, \ldots, \alpha_n$ of K as a $\mathbf{Q}$-vector space and $b_1, \ldots, b_n \in \mathbf{Z}$ such that $b_i\alpha_i \in \mathcal{O}_K$. Then $b_1\alpha_1, \ldots, b_n\alpha_n$ is a $\mathbf{Q}$-basis of K made of integral elements. Alternatively, we can also take $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$ and notice that $1, \alpha, \ldots, \alpha^{n-1}$ is a $\mathbf{Q}$-basis of K made of integral elements. □

Let now K be a number field and let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be a basis of K as a $\mathbf{Q}$-vector space, which exists by the previous lemma. These elements are linearly independent over $\mathbf{Z}$ so that the $\mathbf{Z}$-submodule of $\mathcal{O}_K$ that they generate

$$\Lambda = (\alpha_1, \ldots, \alpha_n)_{\mathbf{Z}} \subseteq \mathcal{O}_K$$

is a free $\mathbf{Z}$-module of rank n. This brings us to the following definition:

Definition 2.3.10 (Lattice in a ring of integers)**.** Let K be a number field with and $\mathcal{O}_K$ be its ring of integers. A lattice in $\mathcal{O}_K$ is a free $\mathbf{Z}$-submodule $\Lambda \subseteq \mathcal{O}_K$ of rank $[K : \mathbf{Q}]$.

Remark 2.3.11. Equivalently, a lattice in $\mathcal{O}_K$ is a subgroup $\Lambda \subseteq \mathcal{O}_K$ generated by elements $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ that form a basis of K as a $\mathbf{Q}$-module. These exist because of Lemma 2.3.9.

If K is a number field and let $\Lambda \subseteq \mathcal{O}_K$ is a lattice in $\mathcal{O}_K$ the trace gives us a nondegenerate $\mathbf{Q}$-bilinear map

$$K \times K \longrightarrow \mathbf{Q}, \qquad (\alpha, \beta) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\beta)$$

The *dual of* Λ *with respect to the trace* is defined as

$$\Lambda^* := \{\beta \in K \mid \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\beta) \in \mathbf{Z} \text{ for all } \alpha \in \Lambda\}$$

Lemma 2.3.12. *Let K be a number field of degree and $\Lambda \subseteq \mathcal{O}_K$ a lattice in $\mathcal{O}_K$. The following hold:*

1. *Λ^* is a $\mathbf{Z}$-submodule of K and $\Lambda \subseteq \mathcal{O}_K \subseteq \Lambda^*$.*

2. *If $\Lambda \subseteq \Lambda' \subseteq \mathcal{O}_K$ is another lattice in $\mathcal{O}_K$, then $\Lambda \subseteq \Lambda' \subseteq \Lambda'^* \subseteq \Lambda^*$.*

3. *If $\alpha_1, \ldots, \alpha_n \in \Lambda$ is a basis of Λ as a free $\mathbf{Z}$-module, then there is a unique basis $\beta_1, \ldots, \beta_n \in \Lambda^*$ of Λ^* as a free $\mathbf{Z}$-module such that*

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i\beta_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

In particular, Λ^* is a free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$.

Proof. 1. If $\alpha, \beta \in \Lambda^*$ and $m, n \in \mathbf{Z}$ then for any $\gamma \in \Lambda$ we have that

$$\mathrm{Tr}_{K/\mathbf{Q}}((m\alpha + n\beta)\gamma) = m \cdot \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\gamma) + n \cdot \mathrm{Tr}_{K/\mathbf{Q}}(\beta\gamma)$$

which is in $\mathbf{Z}$ since $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha\gamma), \mathrm{Tr}_{K/\mathbf{Q}}(\beta\gamma) \in \mathbf{Z}$. Hence $m\alpha + n\beta \in \Lambda^*$ and this shows that Λ^* is a $\mathbf{Z}$-submodule. Furthermore, it holds that $\mathcal{O}_K \subseteq \Lambda^*$ because the trace of an element in $\mathcal{O}_K$ is in $\mathbf{Z}$.

2. All inclusions are straightforward (but check them yourself if this is not immediately clear).

3. Since the $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbf{Z}$, they are also linearly independent over $\mathbf{Q}$, hence they are a basis of K as a $\mathbf{Q}$-vector space. Since we know that the trace is non-degenerate by Theorem 2.2.30, there is another basis $\beta_1, \ldots, \beta_n$ of K as a $\mathbf{Q}$-vector space such that
$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i \beta_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$
We claim that these give a basis of Λ^* as well: any element in K can be written as
$$\beta = \sum_{i=1}^{n} b_i \cdot \beta_i, \qquad \text{for some } b_i \in \mathbf{Q}$$
and $\beta \in \Lambda^*$ if and only if $b_i = \mathrm{Tr}_{K/\mathbf{Q}}(\beta\alpha_i) \in \mathbf{Z}$ for all $i = 1, \ldots, n$ (why?). This shows that the $\beta_1, \ldots, \beta_n$ generate Λ^* as a $\mathbf{Z}$-module and since they are also linearly independent, they are a basis. □

As a corollary of this and of the classification of finitely generated $\mathbf{Z}$-modules, we get:

Theorem 2.3.13 (Finiteness of Integral Closure)**.** *let K be a number field. Then the ring of integers $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$.*

Proof. Let $\Lambda \subseteq \mathcal{O}_K$ be any lattice in $\mathcal{O}_K$. Then $\Lambda \subseteq \mathcal{O}_K \subseteq \Lambda^*$. We know that Λ^* is a finitely generated $\mathbf{Z}$-module, hence Noetherian because of Proposition A.5.15, so that $\mathcal{O}_K$ must also be finitely generated. It is also torsion-free because it is contained in K, hence by the classification theorem A.5.28 it must be free of finite rank. Finally as a consequence of Lemma 2.3.12 and of Corollary A.5.21 we have
$$[K : \mathbf{Q}] = \mathrm{rank}(\Lambda) \leq \mathrm{rank}(\mathcal{O}_K) \leq \mathrm{rank}(\Lambda^*) = [K : \mathbf{Q}]$$
so that $\mathrm{rank}(\mathcal{O}_K) = [K : \mathbf{Q}]$ as well. □

Remark 2.3.14. This can also be stated by saying that $\mathcal{O}_K$ is a lattice in $\mathcal{O}_K$ or that there is a basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$ as a $\mathbf{Z}$-module. This is called an *integral basis* of $\mathcal{O}_K$.

Example 2.3.15. Let $d \in \mathbf{Z}$ be square-free. We know that
$$\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \begin{cases} \mathbf{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4, \\ \mathbf{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4. \end{cases}$$
Then an integral basis of $\mathcal{O}_K$ is given by $1, \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and by $1, \sqrt{d}$ otherwise. In general, finding an integral basis of a ring of integer of a number field can be a hard problem.

The statement that the ring of integers $\mathcal{O}_K$ is a lattice in $\mathcal{O}_K$ can be generalized to ideals. We first start with an easy observation:

Lemma 2.3.16. *Let $A \subseteq B$ be an extension of rings and let $I \subseteq B$ be an ideal in B. Then $I \cap A$ is an ideal in A. Furthermore, if I is prime in B, then $A \cap I$ is prime in A.*

Proof. Straightforward exercise. □

Proposition 2.3.17. *Let K be a number field and $I \subseteq \mathcal{O}_K$ a non-zero ideal in its ring of integers. Then it holds that*

1. *$I \cap \mathbf{Z} \neq (0)$. In particular $\mathbf{Z}/I \cap \mathbf{Z}$ is a finite ring.*
2. *$\mathcal{O}_K/I$ is finitely generated as an $\mathbf{Z}/I \cap \mathbf{Z}$-module. In particular, $\mathcal{O}_K/I$ is a finite set.*
3. *I is a lattice in $\mathcal{O}_K$, meaning that it is a free abelian subgroup of rank $[K : \mathbf{Q}]$.*

Proof.
1. Let $\alpha \in I, \alpha \neq 0$. We know from Proposition 2.3.8 that there is $\beta \in \mathcal{O}_K$ such that $\alpha\beta = N_{K/\mathbf{Q}}(\alpha)$, so that $N_{K/\mathbf{Q}}(\alpha) \in I \cap \mathbf{Z}, N_{K/\mathbf{Q}}(\alpha) \neq 0$. This proves that $I \cap \mathbf{Z}$ is a non-zero ideal in $\mathbf{Z}$ so that $I \cap \mathbf{Z} = (m)$ for a certain $m \in \mathbf{Z}$, and $\mathbf{Z}/I \cap \mathbf{Z} \cong \mathbf{Z}/m\mathbf{Z}$ is finite.

2. The inclusion $\mathbf{Z} \subseteq \mathcal{O}_K$ induces an extension of rings $\mathbf{Z}/\mathbf{Z} \cap I \hookrightarrow \mathcal{O}_K/I$ that makes $\mathcal{O}_K/I$ into a $\mathbf{Z}/\mathbf{Z} \cap I$-module. It is easy to show that if $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ are generators of $\mathcal{O}_K$ as a $\mathbf{Z}$-module, then the classes $[\alpha_1], \ldots, [\alpha_n] \in \mathcal{O}_K/I$ are generators of $\mathcal{O}_K/I$ as a $\mathbf{Z}/I \cap \mathbf{Z}$-module. In particular, this means that there is a surjective homomorphism $(\mathbf{Z}/I \cap \mathbf{Z})^{\oplus n} \to \mathcal{O}_K/I$, and since $\mathbf{Z}/I \cap \mathbf{Z}$ is finite by point (1), it must be that $\mathcal{O}_K/I$ is finite as well.

3. Since I is a subgroup of a free abelian group, it is free. Furthermore, since the quotient $\mathcal{O}_K/I$ is finite, it follows from Lemma A.5.35 that the rank of I is the same as the rank of $\mathcal{O}_K$, which is precisely $[K : \mathbf{Q}]$.

□

Example 2.3.18. If $K = \mathbf{Q}(\alpha)$ is a number field of degree $[K : \mathbf{Q}(\alpha)]$ with $\alpha \in \mathcal{O}_K$ integral over $\mathbf{Z}$, then $\mathbf{Z}[\alpha] \subseteq \mathcal{O}_K$ is a subring and hence a subgroup. Notice that $\mathbf{Z}[\alpha] \supseteq (1, \alpha, \ldots, \alpha^{n-1})_{\mathbf{Z}}$ and moreover, since the minimal polynomial $m_{\alpha,\mathbf{Q}}(x) \in \mathbf{Z}[x]$ of α is monic, we can use it to express all $\alpha^n, \alpha^{n+1}, \ldots$, as elements in $(1, \alpha, \ldots, \alpha^{n-1})_{\mathbf{Z}}$. This shows that

$$\mathbf{Z}[\alpha] = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})_{\mathbf{Z}}$$

and in particular, it is a lattice in $\mathcal{O}_K$. Notice that the previous argument is equivalent to saying that the kernel of the evaluation map

$$\mathrm{ev}_\alpha \colon \mathbf{Z}[x] \mapsto K, \quad f(x) \mapsto f(\alpha)$$

Is the ideal generated by $(m_{\alpha,\mathbf{Q}}(x))$. Hence there is an isomorphism of rings

$$\mathbf{Z}[\alpha] \cong \mathbf{Z}[x]/(m_{\alpha,\mathbf{Q}}(x)).$$

2.3.2 The discriminant

Let K be a number field of degree $n = [K : \mathbf{Q}]$. The trace induces a non-degenerate bilinear form

$$\mathrm{Tr}^b_{K/\mathbf{Q}} \colon K \times K \longrightarrow \mathbf{Q}, \quad (\alpha, \beta) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\beta)$$

Let now $\alpha_1, \ldots, \alpha_n \in K$ be a basis of K as a $\mathbf{Q}$-vector space. With respect to this basis the bilinear map $\mathrm{Tr}^b_{K/\mathbf{Q}}$ is represented by the $n \times n$ matrix

$$T(\alpha_1, \ldots, \alpha_n) = (\mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i\alpha_j))_{1 \le i,j \le n} \in \mathbf{Q}^{n \times n}$$

This means that if we write $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n, \beta = b_1\alpha_1 + \ldots + b_n\alpha_n$ for certain $a_i, b_j \in \mathbf{Q}$, then

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha\beta) = \begin{pmatrix} a_1 & \ldots & a_n \end{pmatrix} \cdot T(\alpha_1, \ldots, \alpha_n) \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

For another interpretation of the matrix $T(\alpha_1, \ldots, \alpha_n)$, let $\beta_1, \ldots, \beta_n$ be the basis that is dual to $\alpha_1, \ldots, \alpha_n$ with respect to the trace, in the sense of Theorem 2.2.30. Then

$$\alpha_j = \sum_{i=1}^{n} \mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i\alpha_j) \cdot \beta_j \qquad \text{for all } j = 1, \ldots, n$$

(why is this true?). This means precisely that $T(\alpha_1, \ldots, \alpha_n)$ is the matrix representing the identity

$$\mathrm{id}_K \colon K \longrightarrow K$$

as a $\mathbf{Q}$-linear map with respect to the bases $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$.

Definition 2.3.19 (Discriminant of an n-tuple)**.** If K is a number field and if $\alpha_1, \ldots, \alpha_n \in K$ are a basis of K as a $\mathbf{Q}$-vector space, the *discriminant of* $(\alpha_1, \ldots, \alpha_n)$ is the determinant

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det T(\alpha_1, \ldots, \alpha_n) \in \mathbf{Q}$$

Lemma 2.3.20. *Let K be a number field and let $\alpha_1, \ldots, \alpha_n \in K$ be a basis of K as a $\mathbf{Q}$-vector space.*

1. $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$.
2. *If $\alpha'_1, \ldots, \alpha'_n \in K$ is another basis and if $M \in \mathrm{GL}_n(\mathbf{Q})$ is the change of basis matrix, so that $(\alpha_1, \ldots, \alpha_n) = (\alpha'_1, \ldots, \alpha'_n) \cdot M$, then* $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(M)^2 \cdot \mathrm{disc}(\alpha'_1, \ldots, \alpha'_n)$.
3. *If $\alpha'_1, \ldots, \alpha'_n \in K$ is another basis that generates the same $\mathbf{Z}$-submodule $(\alpha_1, \ldots, \alpha_n)_{\mathbf{Z}} = (\alpha'_1, \ldots, \alpha'_n)_{\mathbf{Z}}$, then* $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\alpha'_1, \ldots, \alpha'_n)$.
4. *If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, then* $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}$.

Proof. 1. Since $T(\alpha_1, \ldots, \alpha_n)$ is a matrix representation of the identity map $\mathrm{id}_K \colon K \to K$ with respect to the basis $\alpha_1, \ldots, \alpha_n$ and the dual basis $\beta_1, \ldots, \beta_n$, we know that $\det(T(\alpha_1, \ldots, \alpha_n)) \neq 0$ (Why can't we say that since this is a matrix representation of the identity map then its determinant must be 1?) .

2. One sees from linear algebra that $T(\alpha_1', \dots, \alpha_n') = M^t \cdot T(\alpha_1, \dots, \alpha_n) \cdot M$ and we conclude taking the determinant.

3. If the two bases generate the same $\mathbf{Z}$-module, then the matrix M of the previous point must be in $\mathrm{GL}_n(\mathbf{Z})$ so that $\det(M) \in \{-1, +1\}$ and $\det(M)^2 = 1$. We conclude using the previous point.

4. This follows because $T(\alpha_1, \dots, \alpha_n) \in \mathbf{Z}^{n \times n}$ has integer coefficients. □

Thanks to Lemma 2.3.20, the following definition makes sense:

Definition 2.3.21 (Discriminant of a lattice and of a number field)**.** Let K be a number field and let $\Lambda \subseteq \mathcal{O}_K$ be a lattice in $\mathcal{O}_K$. The discriminant of Λ is the discriminant of any basis $\alpha_1, \dots, \alpha_n \in \Lambda$ of Λ as a free $\mathbf{Z}$-module:

$$\mathrm{disc}(\Lambda) := \mathrm{disc}(\alpha_1, \dots, \alpha_n)$$

In particular, the discriminant of K is defined to be

$$\mathrm{disc}(K) := \mathrm{disc}(\mathcal{O}_K).$$

Example 2.3.22. Let $d \in \mathbf{Z}$ be a square-free integer. If $d \equiv 2, 3 \pmod 4$, we know that an integral basis of $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ is given by $1, \sqrt{d}$. Then

$$\mathrm{disc}(\mathbf{Q}(\sqrt{d})) = \mathrm{disc}(1, \sqrt{d}) = \det \begin{pmatrix} \mathrm{Tr}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(1) & \mathrm{Tr}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(\sqrt{d}) \\ \mathrm{Tr}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(\sqrt{d}) & \mathrm{Tr}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

If instead $d \equiv 1 \pmod 4$ then an integral basis of $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ is given by $1, \frac{1+\sqrt{d}}{2}$. We compute

$$\mathrm{disc}(\mathbf{Q}(\sqrt{d})) = \mathrm{disc}\left(1, \frac{1+\sqrt{d}}{2}\right) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d.$$

We can also interpret the discriminant in terms of cardinality:

Proposition 2.3.23. *Let K be a number field, let $\Lambda \subseteq \Lambda' \subseteq \mathcal{O}_K$ be two lattices in $\mathcal{O}_K$. The following statements hold*

1. *Λ/Λ' is finite and*
$$\mathrm{disc}(\Lambda) = |\Lambda'/\Lambda|^2 \cdot \mathrm{disc}(\Lambda')$$
2. *$\Lambda = \Lambda'$ if and only if $\mathrm{disc}(\Lambda) = \mathrm{disc}(\Lambda')$.*
3. *$\mathcal{O}_K \subseteq \frac{1}{\mathrm{disc}(\Lambda)}\Lambda$. Equivalently, $\mathrm{disc}(\Lambda) \cdot \alpha \in \Lambda$ for all $\alpha \in \mathcal{O}_K$.*

In particular, $\Lambda = \mathcal{O}_K$ if and only if $\mathrm{disc}(\Lambda) = \mathrm{disc}(K)$.

Proof. Since $\Lambda \subseteq \Lambda'$ is an inclusion of free $\mathbf{Z}$-modules of the same rank, we know that the quotient is finite because of Lemma A.5.35. Let now $\alpha_1, \dots, \alpha_n \in \Lambda$ and $\alpha_1', \dots, \alpha_n' \in \Lambda'$ be two bases as free $\mathbf{Z}$-modules of Λ and Λ' respectively. It we express the α_j as linear combinations of the α_i' we obtain a matrix $M \in \mathbf{Z}^{n \times n}$ such that $(\alpha_1, \dots, \alpha_n) = (\alpha_1', \dots, \alpha_n') \cdot M$ so that

$$\mathrm{disc}(\Lambda) = \mathrm{disc}(\alpha_1, \dots, \alpha_n) = \det(M)^2 \cdot \mathrm{disc}(\alpha_1', \dots, \alpha_n') = \det(M)^2 \,\mathrm{disc}(\Lambda')$$

Now we notice that the matrix M represents the inclusion $\Lambda \subseteq \Lambda'$ with respect to the two bases above, so that Lemma A.5.35 shows that $\det(M)^2 = |\det(M)|^2 = |\Lambda'/\Lambda|^2$.

The last statement follows by considering the inclusion of lattices $\Lambda \subseteq \mathcal{O}_K$. □

A sometimes useful corollary is:

Corollary 2.3.24. *Let K be a number field and $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ be a $\mathbf{Q}$-basis of K made up of integral elements such that $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbf{Z}$ is square-free. Then $\alpha_1, \dots, \alpha_n$ is an integral basis of $\mathcal{O}_K$.*

Proof. Let $\Lambda = (\alpha_1, \dots, \alpha_n)_{\mathbf{Z}}$ be the lattice generated by the $\alpha_1, \dots, \alpha_n$. We apply Proposition 2.3.23 to the inclusion of lattices $\Lambda \subseteq \mathcal{O}_K$ and we see that

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = |\mathcal{O}_K/\Lambda|^2 \cdot \operatorname{disc}(\mathcal{O}_K)$$

Since $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ is square-free, it must be that $|\mathcal{O}_K/\Lambda| = 1$, so that $\mathcal{O}_K = \Lambda$. □

We mention a couple of other ways to compute the discriminant:

Proposition 2.3.25. *Let K be a number field of degree $n = [K : \mathbf{Q}]$ and let $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbf{C}$ be all the embeddings of K in $\mathbf{C}$.*

1. *If $\alpha_1, \dots, \alpha_n \in K$ is a basis of K as a $\mathbf{Q}$-vector space, let $S(\alpha_1, \dots, \alpha_n) = (\sigma_i(\alpha_j))_{1 \le i,j \le n} \in \mathbf{Q}^{n \times n}$. Then*
$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = (\det S(\alpha_1, \dots, \alpha_n))^2.$$
2. *If $K = \mathbf{Q}(\alpha)$, let $m_{\mathbf{Q},\alpha}(x) \in \mathbf{Q}[x]$ be the minimal polynomial of α, and $m'_{\alpha,\mathbf{Q}}(x)$ be its derivative. Then*
$$\operatorname{disc}(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \prod_{1 \le i,j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{\frac{n(n-1)}{2}} \cdot \mathrm{N}_{K/\mathbf{Q}}(m'_{\mathbf{Q},\alpha}(\alpha)),$$

Proof. 1. Let $S = S(\alpha_1, \dots, \alpha_n) = (\sigma_i(\alpha_j))_{1 \le i,j \le n}$. Then for any $1 \le i, j \le n$ we have

$$(S^t \cdot S)_{ij} = \sum_{h=1}^{n} S^t_{ih} S_{hj} = \sum_{h=1}^{n} \sigma_h(\alpha_i)\sigma_h(\alpha_j) = \sum_{h=1}^{n} \sigma_h(\alpha_i\alpha_j) = \mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i\alpha_j)$$

This shows that $S^t \cdot S = T(\alpha_1, \dots, \alpha_n)$ so that taking determinants we have $\det(S)^2 = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$.

2. Let $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbf{C}$ be the embeddings of K inside $\mathbf{C}$ and consider the matrix $S = S(1, \alpha, \dots, \alpha^{n-1}) = (\sigma_i(\alpha^{j-1}))_{1 \le i,j \le n} = (\sigma_i(\alpha)^{j-1})_{1 \le i,j \le n}$. Using point (1), together with the Vandermonde formula for the determinant of S we see that

$$\begin{aligned}
\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = \det(S)^2 &= \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \\
&= \prod_{1 \le i < j \le n} (-1)(\sigma_i(\alpha) - \sigma_j(\alpha))(\sigma_j(\alpha) - \sigma_i(\alpha)) \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{\substack{1 \le i,j \le n \\ i \ne j}} (\sigma_i(\alpha) - \sigma_j(\alpha))
\end{aligned}$$

On the other hand, we know that , $m_{\alpha,\mathbf{Q}}(x) = (x - \sigma_1(\alpha)) \dots (x - \sigma_n(\alpha))$, so that

$$m'_{\alpha,\mathbf{Q}}(x) = \sum_{j=1}^{n} \frac{(x - \sigma_1(\alpha)) \dots (x - \sigma_n(\alpha))}{(x - \sigma_i(\alpha))}$$

In particular

$$m'_{\alpha,\mathbf{Q}}(\sigma_i(\alpha)) = \prod_{\substack{1\leq i\leq n\\ i\neq j}} (\sigma_i(\alpha) - \sigma_j(\alpha)).$$

Applying the norm, we see that

$$\mathrm{N}_{K/\mathbf{Q}}(m'_{\alpha,\mathbf{Q}}(\alpha)) = \prod_{j=1}^{n} \sigma_j(m'_{\alpha,\mathbf{Q}}(\alpha)) = \prod_{j=1}^{n} m'_{\alpha,\mathbf{Q}}(\sigma_j(\alpha)) = \prod_{\substack{1\leq i,j\leq n\\ i\neq j}} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

Which is what we wanted to prove. □

Remark 2.3.26. Observe that if $K = \mathbf{Q}(\alpha)$ is a number field of degree n and $\alpha \in \mathcal{O}_K$ is integral over $\mathbf{Z}$ then the abelian group generated by $1, \alpha, \ldots, \alpha^{n-1}$ is equal to $\mathbf{Z}[\alpha]$ because of Example 2.3.18. Hence Proposition 2.3.25 gives a way to compute

$$\operatorname{disc} \mathbf{Z}[\alpha] = \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}).$$

Example 2.3.27. Let $p \in \mathbf{Z}$ be an odd prime and consider the cyclotomic number field $\mathbf{Q}(\zeta_p)$, of degree $[\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1$. We want to compute the discriminant

$$\operatorname{disc} \mathbf{Z}[\zeta_p] = \operatorname{disc}(1, \zeta_p, \ldots, \zeta_p^{p-2})$$

using the previous formula. We know that the minimal polynomial of ζ_p over $\mathbf{Q}$ is the cyclotomic polynomial $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \ldots + x + 1$. We see that $\Phi'_p(x) = \frac{px^{p-1}(x-1)-(x^p-1)}{(x-1)^2}$, hence $\Phi'_p(\zeta_p) = \frac{p}{\zeta_p(\zeta_p-1)}$, and $\operatorname{disc}(1, \zeta_p, \ldots, \zeta_{p-1}) = (-1)^{\frac{(p-1)(p-2)}{2}} \cdot \frac{\mathrm{N}(p)}{\mathrm{N}(\zeta_p)\cdot\mathrm{N}(\zeta_p-1)}$, where we just denoted $\mathrm{N} = \mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}$ for simplicity. We know that $\mathrm{N}(p) = p^{p-1}$ and also that $\mathrm{N}(\zeta_p) = (-1)^{p-1}\Phi_p(0) = (-1)^{p-1}$. Finally, we see that the minimal polynomial of $\zeta_p - 1$ is $f(x) = \Phi_p(x+1)$ (why?), so that $\mathrm{N}(\zeta_p - 1) = (-1)^{p-1}f(0) = (-1)^{p-1}\Phi_p(1) = (-1)^{p-1}p$. In summary

$$\operatorname{disc} \mathbf{Z}[\zeta_p] = \operatorname{disc}(1, \zeta_p, \ldots, \zeta_p^{p-1}) = (-1)^{\frac{(p-1)(p-2)}{2}} \cdot p^{p-2} = (-1)^{\frac{(p-1)}{2}} \cdot p^{p-2}.$$

where the last equality follows from the fact that p is odd.

We can use this computation to find the ring of integers in $\mathbf{Q}(\zeta_p)$. Recall that a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$

is Eisenstein with respect to a prime number $p \in \mathbf{Z}$ if $p \mid a_i$ for all $i = 0, \ldots, n-1$ but $p^2 \nmid a_0$.

Proposition 2.3.28. *Let $K = \mathbf{Q}(\alpha)$ be a number field, with $\alpha \in \mathcal{O}_K$ and assume that the minimal polynomial $m_{\alpha,\mathbf{Q}}(x)$ is Eisenstein with respect to a prime p. Then $p\mathcal{O}_K \cap \mathbf{Z}[\alpha] = p\mathbf{Z}[\alpha]$ and $p \nmid |\mathcal{O}_K/\mathbf{Z}[\alpha]|$.*

Proof. Write

$$m_{\alpha,\mathbf{Q}}(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$

where $p \mid a_i$ for $i = 0, \ldots, n-1$ and $p^2 \nmid a_0$. First observe that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0 \in p\mathbf{Z}[\alpha]$$

hence $\alpha^n \mathbf{Z}[\alpha] \subseteq p\mathbf{Z}[\alpha]$. We show now that $p\mathcal{O}_K \cap \mathbf{Z}[\alpha] = p\mathbf{Z}[\alpha]$. This means that if $\beta \in \mathcal{O}_K$ and

$$p \cdot \beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

for certain $b_i \in \mathbf{Z}$, then $p \mid b_i$ for all $i = 0, \ldots, n-1$. To show this, multiply the above equality by α^{n-1} on both sides, so that $p\beta\alpha^{n-1} = b_0\alpha^{n-1} + p\gamma$ for a certain $\gamma \in \mathbf{Z}[\alpha]$. Then we can write $b_0\alpha^{n-1} = p\delta$ for a certain $\delta \in \mathcal{O}_K$. Taking the norm, we get

$$p^n N_{K/\mathbf{Q}}(\delta) = b_0^n \cdot N_{K/\mathbf{Q}}(\alpha)^{n-1} = (-1)^{n(n-1)} \cdot b_0^n a_0^{n-1}$$

Since $p \mid a_0$ but $p^2 \nmid a_0$, it must be that $p \mid b_0$. So we can write $b_0 = pb_0'$ for $b_0' \in \mathbf{Z}$ and then

$$p \cdot (\beta - b_0') = b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

Now we can multiply both sides by α^{n-2} and proceed as before. This shows that $p\mathcal{O}_K \cap \mathbf{Z}[\alpha] = p\mathbf{Z}[\alpha]$. Assume now that $p \mid |\mathcal{O}_K/\mathbf{Z}[\alpha]|$: then in the finite abelian group $\mathcal{O}_K/\mathbf{Z}[\alpha]$ there is an element of order p, meaning that there is $\beta \in \mathcal{O}_K$ such that $p\beta \in \mathbf{Z}[\alpha]$ but $\beta \notin \mathbf{Z}[\alpha]$. But this is impossible, since from what we have proved before we know that $p\beta = p\gamma$ for $\gamma \in \mathbf{Z}[\alpha]$ and then $\beta = \gamma \in \mathbf{Z}[\alpha]$. □

Corollary 2.3.29. *Let $p \in \mathbf{Z}$ be an odd prime number. Then $\mathcal{O}_{\mathbf{Q}(\zeta_p)} = \mathbf{Z}[\zeta_p]$.*

Proof. Let $\alpha = \zeta_p - 1$ so that $\mathbf{Q}(\zeta_p) = \mathbf{Q}(\alpha)$ and $\mathbf{Z}[\zeta_p] = \mathbf{Z}[\alpha]$. The minimal polynomial of α is $\Phi_p(x+1)$ which is Eisenstein. Then we know from Proposition 2.3.28 that $p \nmid |\mathcal{O}_{\mathbf{Q}(\alpha)}/\mathbf{Z}[\alpha]|$. On the other hand, we have seen in Example 2.3.27 that $\operatorname{disc} \mathbf{Z}[\alpha] = \operatorname{disc} \mathbf{Z}[\zeta_p] = (-1)^{\frac{p-1}{2}} p^{p-2}$, and we know from Proposition 2.3.23 that

$$(-1)^{\frac{p-1}{2}} p^{p-2} = \operatorname{disc} \mathbf{Z}[\alpha] = |\mathcal{O}_{\mathbf{Q}(\zeta_p)}/\operatorname{disc} \mathbf{Z}[\alpha]| \operatorname{disc} \mathcal{O}_{\mathbf{Q}(\zeta_p)}$$

Hence it must be $|\mathcal{O}_{\mathbf{Q}(\zeta_p)}/\mathbf{Z}[\alpha]| = 1$ and we are done. □

Chapter 3

Dedekind domains

3.1 Definition and basic properties

We are aiming to prove that every ideal in the ring of integers $\mathcal{O}_K$ of a number field K has a unique factorization as a product of prime ideals. There is a general class of rings for which this holds, named after the German mathematician Richard Dedekind (1831-1916).

Definition 3.1.1 (Dedekind domain)**.** A Dedekind domain is a domain A such that:

1. A is Noetherian.
2. A is integrally closed.
3. Every non-zero prime ideal in A is maximal, and there is at least one non-zero prime ideal.

Remark 3.1.2. Saying that A has a non-zero prime is equivalent to saying that A is not a field. Another way to phrase the third condition in the previous definition is to say that A has Krull dimension 1.

Example 3.1.3. If A is a PID which is not a field, then A is a Dedekind domain. Indeed, A is clearly Noetherian because every ideal is generated by a single element. Since A is a UFD it is also integrally closed because of Proposition 2.1.12. Finally, we know that every non-zero prime ideal in A is maximal from Lemma A.4.10.

More importantly, rings of integers in a number field are Dedekind domains. We start with an observation:

Lemma 3.1.4. *Let $F \subseteq A$ be a finite extension of rings where F is a field and A is a domain. Then A is a field as well.*

Proof. Take a non-zero element $\alpha \in A, \alpha \neq 0$ and consider the multiplication-by-α map $(\cdot\alpha)\colon A \to A$. This is injective because A is a domain, and since A is a finite-dimensional F-vector space, it is also surjective. Then there is $\beta \in A$ such that $\alpha\beta = 1$, meaning that $\alpha \in A^\times$. □

Theorem 3.1.5. *If K is a number field, the ring of integers $\mathcal{O}_K$ is a Dedekind domain.*

Proof. We first show that $\mathcal{O}_K$ is Noetherian: if $I \subseteq \mathcal{O}_K$ is a non-zero ideal, then we observed in Proposition 2.3.17 that it is finitely generated as an abelian group, so that it is also finitely generated as an ideal.

Next, Lemma2.3.9 shows that $\operatorname{Frac} \mathcal{O}_K = K$ and any element in α that is integral over $\mathcal{O}_K$ must also be integral over $\mathbf{Z}$ because of Lemma 2.1.8. Hence $\alpha \in \mathcal{O}_K$.

Finally, let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a non-zero prime ideal. Then we know from Proposition 2.3.17 that $\mathcal{O}_K/\mathfrak{p}$ is a finite exension of $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$. Observe that $\mathfrak{p} \cap \mathbf{Z}$ is a non-zero prime ideal, so that the quotient $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ is a finite field. Then $\mathcal{O}_K/\mathfrak{p}$ is a field because of Lemma 3.1.4, meaning that $\mathfrak{p}$ is maximal. Finally, $\mathcal{O}_K$ is not a field because otherwise $\mathcal{O}_K = \operatorname{Frac} \mathcal{O}_K = K$, so that any element $\mathbf{Q} \subseteq K$ is integral over $\mathbf{Z}$. This is a contradiction because $\mathbf{Z}$ is integrally closed in $\mathbf{Q}$. □

3.2 Fractional ideals and unique factorization

To prove the unique factorization in a Dedekind domain, it will be useful to work not only with ideals but with fractional ideals as well.

Definition 3.2.1 (Fractional ideal)**.** Let A be a Dedekind domain with fraction field $F = \operatorname{Frac} A$. A fractional ideal is a non-zero finitely-generated A-submodule $I \subseteq F$.

Remark 3.2.2. If A is a Dedekind domain, a non-zero ideal $I \subseteq A$ is the same as a fractional ideal contained in A. For this reason, we will also sometimes call it an integral ideal of A.

Example 3.2.3. A non-zero element $x \in F$, generates the A-submodule $Ax = \{ax \mid a \in A\}$, which is a fractional ideal. A fractional ideal generated by just one element is called *principal*.

Remark 3.2.4. If A is a Dedekind domain and if $I \subseteq F = \operatorname{Frac} A$ is a fractional ideal, then it is generated as an A-module by finitely many elements $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \in I$. In particular, if we take $b = b_1 \ldots b_n \in A, b \neq 0$, we see that $b \cdot I \subseteq A$, and it is easy to see that $b \cdot I$ is an ideal in A. Hence we can also write

$$I = \frac{1}{b} \cdot J, \quad \text{for an integral ideal } J \subseteq A$$

Conversely, if $J \subseteq A$ is an integral ideal and $b \in A, b \neq 0$, then $\frac{1}{b} J \subseteq F$ is a fractional ideal.

Definition 3.2.5 (Product of fractional ideals)**.** Let A be a Dedekind domain with fraction field $F = \operatorname{Frac} A$ and let $I, J \subseteq F$ be two fractional ideals. Their product $I \cdot J \subseteq F$ is the A-submodule generated by all the products xy for $x \in I, y \in J$. The product of no fractional ideals (empty product) is defined to be A.

Remark 3.2.6. Notice that the product IJ of two fractional ideals is indeed a fractional ideal: if I is generated as an A-module by $x_1, \ldots, x_r$ and J is generated as an A-module by $y_1, \ldots, y_s$, then $I \cdot J$ is generated as an A-module by $x_i y_j$ for $i = 1, \ldots, r$ and $j = 1, \ldots, s$.

Theorem 3.2.7 (Fractional ideals form a group)**.** *Let A be a Dedekind domain with fraction field $F = \operatorname{Frac} F$. The set of fractional ideals*

$$\operatorname{Div}(A) = \{I \subseteq F \mid I \text{ fractional ideal } \}$$

with the product is an abelian group. The neutral element is the ring A itself, and the inverse of a fractional ideal I is

$$I^{-1} := \{x \in F \mid xI \subseteq A\}$$

Remark 3.2.8. To get a sense of this theorem, consider first the set of principal fractional ideals:

$$\mathrm{Prin}(A) = \{I \subseteq F \,|\, I \text{ principal fractional ideal }\} = \{Ax \,|\, x \in F^\times\}$$

If Ax, Ay are two principal fractional ideals, then their product is

$$Ax \cdot Ay = Axy$$

which is again a principal fractional ideal. It is straightforward to see that $\mathrm{Prin}(A)$ with this operation is a group: the neutral element is $A = A \cdot 1$ and the inverse of Ax is Ax^{-1}. Notice that if $I = Ax$

$$Ax^{-1} = \{y \in F \,|\, y \cdot I \in A\}$$

Indeed, $y \cdot Ax \in A$ if and only if $xy = a$ for a certain $a \in A$, meaning that $y = ax^{-1} \in Ax^{-1}$.

We have just showed that $\mathrm{Prin}(A)$ is a group but also a bit more. Indeed, the previous reasoning shows that the map

$$F^\times \longrightarrow \mathrm{Prin}(A), \quad x \mapsto Ax$$

is a surjective homomorphism of groups. Notice that the kernel of this map is given by set of units $A^\times$ of A. Hence, as abelian groups, $\mathrm{Prin}(A) \cong F^\times / A^\times$.

To prove Theorem 3.2.7, we use a couple of general lemmas about (Noetherian) rings which are surprisingly useful:

Lemma 3.2.9. *Let A be a ring $\mathfrak{p} \subseteq A$ a prime ideal and $I_1, \ldots, I_n \subseteq A$ ideals such that*

$$I_1 \ldots I_n \subseteq \mathfrak{p}$$

Then one of the $I_1, \ldots, I_n$ is contained in $\mathfrak{p}$.

Proof. Assume otherwise so that there are $a_j \in I_j \setminus \mathfrak{p}$ for all $j = 1, \ldots, n$. Then $a_1 \ldots a_n \in I_1 \ldots I_n \subseteq \mathfrak{p}$ and since $\mathfrak{p}$ is prime it must be that one of the factors a_j belongs to I. □

Lemma 3.2.10. *Let A be a Noetherian ring and $I \subseteq A$ a non-zero ideal. Then I contains a product $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$ where each $\mathfrak{p}_i \subseteq A$ is a non-zero prime ideal.*

Proof. Consider the set of non-zero ideals that do not satisfy this property. Since A is Noetherian, if this set is non-empty, it has a maximal element I with respect to the inclusion. If we show that I is prime, we have reached a contradiction and we are done. Let $a, b \in A$ such that $ab \in I$ and assume that $a, b \notin I$. Then $I + (a), I + (b)$ are ideals that are strictly larger than I, and by construction of I, there are non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s \subseteq A$ such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq I + (a)$ and $\mathfrak{q}_1 \ldots \mathfrak{q}_s \subseteq I + (b)$. But then

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \cdot \mathfrak{q}_1 \ldots \mathfrak{q}_s \subseteq (I + (a)) \cdot (I + (b)) \subseteq I + (ab) \subseteq I$$

which is a contradiction by construction of I. □

Remark 3.2.11. If A is a Dedekind domain, Lemma 3.2.9 and Lemma 3.2.10 give a way to measure "how far" an ideal is from being prime. Let $I \subseteq A$ be an ideal $I \neq (0)$ and define

$$\Omega(I) = \min\{n \in \mathbf{Z}_{\geq 0} \,|\, \text{ there are prime non-zero ideals } \mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq A \text{ with } \mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq I\}$$

Notice that $\Omega(I) = 0$ if and only if I contains the empty product A, meaning $I = A$. If instead $\Omega(I) = n \geq 1$, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq A$ be non-zero prime ideals,such that

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subseteq I.$$

Since $I \neq A$, I is contained in a maximal ideal $\mathfrak{p}$, and by Lemma 3.2.9 we can assume, up to renumbering, that $\mathfrak{p}_n \subseteq \mathfrak{p}$. Since A is Dedekind, these are both maximal ideals, hence $\mathfrak{p}_n = \mathfrak{p}$. So that we can write

$$\mathfrak{p}_1 \ldots \mathfrak{p}_{n-1}\mathfrak{p} \subseteq I \subseteq \mathfrak{p}$$

In particular if $\Omega(I) = n = 1$, then $I = \mathfrak{p}$ is itself prime. So we can think of $\Omega(I)$ as a way that measures how far I is from being prime. We are going to make this more precise later, but let us consider for now the case of a PID.

Example 3.2.12. Let A be a PID, for example $A = \mathbf{Z}$ and take a non-zero ideal $I = (a)$ and assume that $a = q_1 \ldots q_n$ is a product of n prime elements (not necessarily pairwise coprime). In particular, we see that Aa is equal to a product of n prime ideals, so that

$$\Omega(Aa) \leq n$$

On the other hand, if $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \subseteq A$ are non-zero prime ideals, then $\mathfrak{p}_i = p_i A$ for some prime elements $p_i \in A$, and then

$$\mathfrak{p}_1 \ldots \mathfrak{p}_m \subseteq I \iff q_1 \ldots q_n \mid p_1 \ldots p_m$$

So that $p_1 \ldots p_m$ has at least n (not pairwise coprime) prime factors: this proves that $\Omega(Aa) \geq n$, so that $\Omega(Aa) = n$. If we write $a = p_1^{e_1} \ldots p_h^{e_h}$ where the p_i are pairwise coprime and the e_i are the respective multiplicities, then $\Omega(Aa) = n = e_1 + \ldots + e_h$, hence

$$\Omega(Aa) = \text{ number of prime factors of } a \text{ counted with multiplicity .}$$

If $A = \mathbf{Z}$ this coincides with the Omega function of `https://en.wikipedia.org/wiki/Prime_omega_function`.

Now we can prove that the set of fractional ideals in a Dedekind domain forms a group:

Proof of Theorem 3.2.7. It is straightforward to see that the product of fractional ideal is associative and commutative. Furthermore, if $I \subseteq F$ is a fractional ideal, then $A \cdot I \subseteq I$ because I is an A-submodule and $I \subseteq A \cdot I$ because $1 \in A$. Hence $A \cdot I = I$. To conclude, we need to show that if I is a fractional ideal, then the set $I^{-1} := \{x \in F \mid xI \subseteq A\}$ is a fractional ideal, and $I \cdot I^{-1} = A$. To show that I^{-1} is a fractional ideal, let $y_1, \ldots, y_n \in I$ be non-zero generators of I as an A-module. Then $x \in F$ belongs to I^{-1} if and only if $x \cdot y_i \in A$ for all $i = 1, \ldots, n$, meaning that $I^{-1} = \cap_{i=1}^n A y_i^{-1}$. Since I is the intersection of sub-A-modules of F it is itself a sub-A-module. Furthermore, since it is a sub-A-module of Ay_1^{-1} and A is Noetherian, it is finitely generated.

The actual work that we need to do is in proving that if I is a fractional ideal, $I \cdot I^{-1} = A$. This is where we use the fact that A is a Dedekind domain. By Remark 3.2.4, there is $b \in A$ such that $I = \frac{1}{b} \cdot J$ for an integral ideal $J \subseteq A$. It is then straightforward to see that $I^{-1} = b \cdot J^{-1}$ and that $I \cdot I^{-1} = J \cdot J^{-1}$. To conclude we need to prove the following:

Claim: If $J \subseteq A$ is a non-zero integral ideal, then $JJ^{-1} = A$.

We first consider the case when $J = \mathfrak{p}$ is a non-zero prime ideal. We notice that $A \subseteq \mathfrak{p}^{-1}$ so that

$$\mathfrak{p} = \mathfrak{p} \cdot A \subseteq \mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq A$$

and since $\mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq A$ is an ideal, and $\mathfrak{p}$ is maximal, we must have either $\mathfrak{p} \cdot \mathfrak{p}^{-1} = A$ or $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}$. We assume that $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}$ and we look for a contradiction. Take any $b \in \mathfrak{p}, b \neq 0$ and choose $m \in \mathbf{Z}_{\geq 1}$ minimal such that there is a product $\mathfrak{p}_1 \dots \mathfrak{p}_m \subseteq Ab$: we have

$$\mathfrak{p}_1 \dots \mathfrak{p}_m \subseteq Aa \subseteq \mathfrak{p} = \mathfrak{p} \cdot \mathfrak{p}^{-1}$$

Up to renumbering, Lemma 3.2.9 shows that $\mathfrak{p}_m \subseteq \mathfrak{p}$ and since both ideals are maximal, it must be $\mathfrak{p}_m = \mathfrak{p}$, so we can write

$$\mathfrak{p}_1 \dots \mathfrak{p}_{m-1} \cdot \mathfrak{p} \subseteq Ab \subseteq \mathfrak{p} = \mathfrak{p} \cdot \mathfrak{p}^{-1}$$

If $m = 1$, then $\mathfrak{p} = Ab$ is principal and we are done because of Remark 3.2.4. If $m > 1$ then $\mathfrak{p}_1 \dots \mathfrak{p}_{m-1} \nsubseteq Ab$ by minimality, so that there is $a \in \mathfrak{p}_1 \dots \mathfrak{p}_{m-1}$ such that $a \notin Ab$, meaning that $x = \frac{a}{b} \notin A$. On the other hand $x \cdot \mathfrak{p} = \frac{1}{b} a \cdot \mathfrak{p} \subseteq \frac{1}{b} Ab \subseteq A$, so that $x \in \mathfrak{p}^{-1}$, and $x\mathfrak{p} \subseteq \mathfrak{p}$. Now we use that A is integrally closed: consider the multiplication-by-x map

$$(\cdot x) \colon \mathfrak{p} \longrightarrow \mathfrak{p}$$

Since $\mathfrak{p}$ is a finitely generated A-module, the Cayley-Hamilton theorem in the version of Corollary A.5.24 shows that there are $a_0, \dots, a_{s-1} \in A$ such that

$$(x^s + a_{s-1}x^{s-1} + \dots + a_1 x + a_0)y = 0 \qquad \text{for all } y \in \mathfrak{p}$$

Taking any $y \in \mathfrak{p}, y \neq 0$ and using that A is a domain, we see that x is integral over A, hence $x \in A$. But this is a contradiction.

Now we prove the claim for an arbitrary non-zero integral ideal $J \subseteq A$. We proceed by induction on the minimum number $n = \Omega(J)$ such that there is a product $\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq J$ of non-zero prime ideals contained in J. Remark 3.2.11 shows that if $n = 0$ then $J = A$ and if $n = 1$ then J is prime and in both cases we know the result to be true. If $n \geq 2$ then Remark 3.2.11 shows that there is a prime ideal $\mathfrak{p}$ and prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_{n-1}$ so that

$$\mathfrak{p}_1 \dots \mathfrak{p}_{n-1}\mathfrak{p} \subseteq J \subseteq \mathfrak{p}$$

If we multipluy everything by $\mathfrak{p}^{-1}$ we get

$$\mathfrak{p}_1 \dots \mathfrak{p}_{n-1} = \mathfrak{p}_1 \dots \mathfrak{p}_{n-1}\mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq J\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$$

By induction, the result holds for the integral ideal $I = J\mathfrak{p}^{-1}$ and in particular there is a fractional ideal $H = \mathfrak{p}^{-1}I^{-1}$ such that $JH = A$. Then $H \subseteq J^{-1}$ by definition and

$$A = JH \subseteq J \cdot J^{-1} \subseteq A$$

This implies $JJ^{-1} = A$ and we are done. □

3.2.1 Unique factorization of ideals in a Dedekind domain

We can now prove the unique factorization of ideals in a Dedekind domain:

Theorem 3.2.13 (Unique factorization of ideals in a Dedekind domain)**.** *Let A be a Dedekind domain and let $I \subseteq A$ an ideal $I \neq (0)$. Then there are unique (up to reordering) mutually distinct non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_m \subseteq A$ and $e_1, \dots, e_m \in \mathbf{Z}_{>0}$ such that*

$$I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}.$$

Furthermore, the same results holds for a fractional ideal $I \neq (0), A$ if we allow $e_i \in \mathbf{Z}$.

Proof. Let us first consider the case of an integral ideal $I \subseteq A$. We prove the statement by induction on $n = \Omega(I)$ as in Remark 3.2.11. If $\Omega(I) = 0$ then $I = A$ and it can only be written as an empty product of primes. If instead $\Omega(I) = n \geq 1$, then as in Remark 3.2.11 we can write

$$\mathfrak{p}_1 \dots \mathfrak{p}_{n-1}\mathfrak{p}_n \subseteq I \subseteq \mathfrak{p}_n$$

for certain non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subseteq A$, and then

$$\mathfrak{p}_1 \dots \mathfrak{p}_{n-1} \subseteq I \cdot \mathfrak{p}_n^{-1} \subseteq \mathfrak{p}_n\mathfrak{p}_n^{-1} = A$$

By induction, the integral ideal $J = I\mathfrak{p}_n^{-1}$ has a factorization as a product of prime ideals, so the same is true of $I = J\mathfrak{p}_n$. Assume now that there is another factorization $J\mathfrak{p}_n = I = \mathfrak{q}_1 \dots \mathfrak{q}_m$, where the $\mathfrak{q}_i$ are non-zero primes. Then $\mathfrak{p}_n \supseteq \mathfrak{q}_1 \dots \mathfrak{q}_m$ so that via Lemma 3.2.9 we can assume that $\mathfrak{p}_n = \mathfrak{q}_m$. Then $\mathfrak{q}_1 \dots fq_{m-1} = I\mathfrak{p}_n^{-1} = J$ which is what we wanted to show.
Assume now that I is a fractional ideal. Recall that there is a $b \in A$ such that $J = bI \subseteq A$ is an integral ideal. Write then $J = \mathfrak{p}_1 \dots \mathfrak{p}_m, bA = \mathfrak{p}_{m+1} \dots \mathfrak{p}_s$ for certain non-zero prime ideals so that

$$I = (bA)^{-1} \cdot J = \mathfrak{p}_1 \dots \mathfrak{p}_m \cdot \mathfrak{p}_{m+1}^{-1} \dots \mathfrak{p}_s^{-1}$$

This shows that any fractional ideal has a factorization into prime ideals. Let us show now that this is unique. Assume that

$$\mathfrak{p}_1 \dots \mathfrak{p}_m \cdot \mathfrak{p}_{m+1}^{-1} \dots \mathfrak{p}_s^{-1} = I = \mathfrak{q}_1 \dots \mathfrak{q}_h \cdot \mathfrak{q}_{h+1}^{-1} \dots \mathfrak{q}_t^{-1}$$

for pairwise distinct non-zero prime ideals $\mathfrak{q}_j \subseteq A$. Then we can write

$$\mathfrak{p}_1 \dots \mathfrak{p}_m \cdot \mathfrak{q}_{h+1} \dots \mathfrak{q}_t = \mathfrak{q}_1 \dots \mathfrak{q}_h \cdot \mathfrak{p}_{m+1} \dots \mathfrak{p}_s$$

Since we already proved the uniqueness of the factorization for integral ideals, it is straightforward to conclude from here. □

Example 3.2.14. Consider the number field $K = \mathbf{Q}(\sqrt{-5})$ and its ring of integers $\mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$. In this ring the element 6 has two distinct factorizations into irreducible elements (see Exercise Sheet 1):

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

If we pass to the ideals, we get a factorization of the ideal (6) into two product of product of ideals

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = (6) = (2)(3)$$

Consider now the three ideals of $\mathbf{Z}[\sqrt{-5}]$ given by

$$\mathfrak{p}_1 = (3, 1+\sqrt{-5}),\ \mathfrak{p}_2 = (3, 1-\sqrt{-5}),\ \mathfrak{q} = (2, 1+\sqrt{-5}).$$

We claim that

$$(2) = \mathfrak{q}^2,\ (3) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$$

and we can check it with a computation:

$$\mathfrak{q}^2 = (4, 1-5+2\sqrt{-5}, 2+2\sqrt{-2}) = (4, -4+2\sqrt{-5}, 2+2\sqrt{-5}) = (4, 2\sqrt{-5}, 2+2\sqrt{-5}) = (2)$$
$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 = (9, 6, 3(1+\sqrt{-5}), 3(1-\sqrt{-5})) = (3)$$

We claim that $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}$ are all prime and mutually distinct. Observe that

$$\begin{aligned}
\mathbf{Z}[\sqrt{-5}]/\mathfrak{p}_1 &\cong \mathbf{Z}[x]/(x^2+5, 3, 1+x) \cong (\mathbf{Z}/3\mathbf{Z})[x]/(x^2+5, x+1) \cong \mathbf{F}_3[x]/(x^2-1, x+1) \\
&\cong \mathbf{F}_3[x]/(x+1) \cong \mathbf{F}_3 \\
\mathbf{Z}[\sqrt{-5}]/\mathfrak{p}_2 &\cong \mathbf{Z}[x]/(x^2+5, 3, 1-x) \cong (\mathbf{Z}/3\mathbf{Z})[x]/(x^2+5, x-1) \cong \mathbf{F}_3[x]/(x^2-1, x-1) \\
&\cong \mathbf{F}_3[x]/(x-1) \cong \mathbf{F}_3 \\
\mathbf{Z}[\sqrt{-5}]/\mathfrak{q} &\cong \mathbf{Z}[x]/(x^2+5, 2, 1+x) \cong (\mathbf{Z}/2\mathbf{Z})[x]/(x^2+5, x+1) \cong \mathbf{F}_2[x]/(x^2+1, x+1) \\
&\cong \mathbf{F}_2[x]/(x+1) \cong \mathbf{F}_2
\end{aligned}$$

This also shows that $\mathfrak{q}$ is not equal to $\mathfrak{p}_1, \mathfrak{p}_2$. To show that $\mathfrak{p}_1, \mathfrak{p}_2$ are not equal, observe that $2 = (1+\sqrt{-5}) + (1-\sqrt{-5}) \in \mathfrak{p}_1 + \mathfrak{p}_2$ and $3 \in \mathfrak{p}_1 + \mathfrak{p}_2$ so that $1 = 3 - 2 = \mathfrak{p}_1 + \mathfrak{p}_2$ and $\mathfrak{p}_1 + \mathfrak{p}_2 = (1)$. Hence the unique factorization of (6) as a product of prime ideals is

$$(6) = (2) \cdot (3) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{q}^2$$

By uniqueness, we should get the same result if we consider $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$ and indeed you should check as an exercise that

$$(1+\sqrt{-5}) = \mathfrak{p}_1 \cdot \mathfrak{q}, \quad (1-\sqrt{-5}) = \mathfrak{p}_2 \cdot \mathfrak{q}.$$

Remark 3.2.15. If A is a Dedekind domain and if $I \subseteq A$ is an integral ideal with factorization

$$I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$$

where the $\mathfrak{p}_i \subseteq A$ are non-zero prime ideals, we call the $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ the *prime factors* of I and the e_i are the multiplicities. Then, it is easy to prove, as in the case of a PID of Example 3.2.12, that the quantity $\Omega(I)$ of Remark 3.2.11 is the same as

$$\Omega(I) = e_1 + \dots + e_m = \text{ number of prime factors of } I \text{ counted with multiplicities.}$$

Remark 3.2.16. If A is a Dedekind domain and if $I, J \subseteq A$ are integral ideals, we say that I *divides* J and we write $I \mid J$ if one of the following equivalent conditions is satisfied (prove that they are equivalent as an exercise):

1. $I \supseteq J$.
2. $J = I \cdot H$ for another integral ideal $H \subseteq A$.

3. $I^{-1}J \subseteq A$ is an integral ideal.

4. All prime factors of I counted with multiplicity are also factors of J.

In particular, if $I \subseteq A$ is a non-zero ideal, the pairwise distinct prime ideals appearing in the factorization

$$I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$$

are precisely those prime ideals that contain I.

We also record the following useful fact, which is the Chinese Remainder Theorem for a Dedekind domain:

Proposition 3.2.17. *Let A be a Dedekind domain, $I \subseteq A$ a non-zero ideal with a factorization $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$ where the $\mathfrak{p}_i$ are pairwise distinct non-zero prime ideals and $e_i \in \mathbf{Z}_{\geq 0}$. Then $I = \mathfrak{p}_1^{e_1} \cap \dots \cap \mathfrak{p}_m^{e_m}$ and the map*

$$A/I \longrightarrow A/\mathfrak{p}_1^{e_1} \times \dots \times A/\mathfrak{p}_m^{e_m}, \quad a \mapsto ([a], [a], \dots, [a])$$

is an isomorphism of rings.

Proof. This follows from the Chinese Remainder Theorem A.6.3. □

To conclude, we study the ring structure of each factor appearing in Proposition 3.2.17.

Definition 3.2.18 (Residue field of a Dedekind domain)**.** If A is a Dedekind domain and $\mathfrak{p} \subseteq A$ is a non-zero prime ideal, hence maximal. The residue field of A at $\mathfrak{p}$ is the field

$$\mathbf{F}_\mathfrak{p} := A/\mathfrak{p}.$$

Proposition 3.2.19. *Let A be a Dedekind domain, $\mathfrak{p} \subseteq A$ a non-zero prime ideal and $e \in \mathbf{Z}_{\geq 0}$.*

1. *All the ideals of $A/\mathfrak{p}^e$ are*

$$(0) = \mathfrak{p}^e/\mathfrak{p}^e \subsetneq \mathfrak{p}^{e-1}/\mathfrak{p}^e \subsetneq \dots \subsetneq \mathfrak{p}^2/\mathfrak{p}^e \subsetneq \mathfrak{p}/\mathfrak{p}^e \subsetneq A/\mathfrak{p}^e$$

2. *All the ideals are principal: there is $t \in A$ such that $\mathfrak{p}^i/\mathfrak{p}^e = ([t^i])$ as ideals in $A/\mathfrak{p}^e$ for all $i = 0, \dots, e$.*

3. *There are isomorphisms of A-modules*

$$\mathbf{F}_\mathfrak{p} \xrightarrow{\sim} \frac{\mathfrak{p}^i/\mathfrak{p}^e}{\mathfrak{p}^{i+1}/\mathfrak{p}^e} \cong \mathfrak{p}^i/\mathfrak{p}^{i+1} \qquad \text{for } i = 0, \dots, e-1.$$

Proof. 1. We know that the ideals of the quotient $A/\mathfrak{p}^e$ are of the form $I/\mathfrak{p}^e$ where $\mathfrak{p}^e \subseteq I \subseteq A$ is an ideal. This means that $I \mid \mathfrak{p}^e$, so that $I = \mathfrak{p}^i$ for $i = 0, \dots, e$ and these are mutually distinct.

2. Take any $t \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $\mathfrak{p}^2 \subsetneq \mathfrak{p}^2 + (t) \subseteq \mathfrak{p}$ and the only possible prime factorization of the ideal in the middle is $\mathfrak{p}^2 + (t) = \mathfrak{p}$. Then we see

$$\mathfrak{p} \subseteq (t) + \mathfrak{p}^2 \subseteq (t) + ((t) + \mathfrak{p}^2)^2 \subseteq (t) + \mathfrak{p}^3 \subseteq \dots \subseteq (t) + \mathfrak{p}^e \subseteq \mathfrak{p}$$

Hence $\mathfrak{p} = (t) + \mathfrak{p}^e$. This shows that $\mathfrak{p}/\mathfrak{p}^e = ([t])$ in $A/\mathfrak{p}^e$ and the rest follows.

3. We have seen before that $\mathfrak{p} = (t) + \mathfrak{p}^2$, hence $\mathfrak{p}^i \subseteq (t^i) + \mathfrak{p}^{i+1} \subseteq \mathfrak{p}^i$ so that $\mathfrak{p}^i = (t^i) + \mathfrak{p}^{i+1}$. This means that the homomorphism of rings

$$\varphi \colon A \longrightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1}, \quad a \mapsto [at^i]$$

is surjective. Notice that $\mathfrak{p} \subseteq \operatorname{Ker}\varphi$ hence either $\mathfrak{p} = \operatorname{Ker}\varphi$ or $A = \operatorname{Ker}\varphi$. The second possibility cannot happen because $\varphi(1) = [t^i] \neq 0$ so it must be that $\mathfrak{p} = \operatorname{Ker}\varphi$ and we conclude. □

3.2.2 The class group of a Dedekind domain

Let A be a Dedekind domain and consider the group $\operatorname{Div}(A)$ of fractional ideal. Remark 3.2.8 shows that the subset $\operatorname{Prin}(A) \subseteq \operatorname{Div}(A)$ is actually a subgroup. Hence we can consider the quotient:

Definition 3.2.20 (The class group of a Dedekind domain)**.** The class group of a Dedekind domain A is

$$\operatorname{Cl}(A) = \operatorname{Div}(A)/\operatorname{Prin}(A).$$

This group detects whether a Dedekind domain has unique factorization of elements, not only of ideals:

Proposition 3.2.21. *Let A be a Dedekind domain. The following are equivalent*

1. $\operatorname{Cl}(A) = \{1\}$ *is the trivial group.*
2. *A is a PID.*
3. *A is a UFD.*

Proof. (1) $\implies$ (2) This means that any fractional ideal is principal, so that any integral ideal is principal as well.

(2) $\implies$ (3): we know that every PID is an UFD.

(3) $\implies$ (1): Assume that A is an UFD. We want to show that any fractional ideal is principal. Since any fractional ideal is a product of non-zero prime ideals (possibly with negative multiplicity), it is enough to show that any non-zero prime ideal $\mathfrak{p}$ is principal. Let $a \in \mathfrak{p}, a \neq 0$: since A is an UFD, this has a factorization $a = p_1 \dots p_n$ where the p_i are prime elements. By Lemma 3.2.9, we can assume that $Ap_1 \subseteq \mathfrak{p}$ but since they are both maximal ideal, it must be that $\mathfrak{p} = Ap_1$. □

3.3 Prime splittings in rings of integers

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers, which is a Dedekind domain and a finite extension $\mathbf{Z} \subseteq \mathcal{O}_K$. We have seen in Proposition 2.3.17 that if $\mathfrak{p} \subseteq \mathcal{O}_K$ is a non-zero prime ideal in $\mathcal{O}_K$ then $\mathfrak{p} \cap \mathbf{Z}$ is a non-zero prime ideal in $\mathbf{Z}$, hence it is of the form $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ for a prime number $p \in \mathbf{Z}$.

Definition 3.3.1 (Lying over)**.** We say that a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lies over a prime number $p \in \mathbf{Z}$ if

$$\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}.$$

Conversely, for any prime number $p \in \mathbf{Z}$, we can consider the ideal $p\mathcal{O}_K$ that it generates in $\mathcal{O}_K$.

Remark 3.3.2. The ideal $p\mathcal{O}_K$ is a proper ideal of $\mathcal{O}_K$. Equivalently, this means that p is not invertible in $\mathcal{O}_K$ which we know to be true since the norm $N_{K/\mathbf{Q}}(p) = p^{[K:\mathbf{Q}]}$ is not invertible in $\mathbf{Z}$ and because of Proposition 2.3.8.

Since $p\mathcal{O}_K$ is a proper ideal, we have a unique factorization

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}.$$

for certain mutually distinct non-zero prime ideals $\mathfrak{p}_i \subseteq \mathcal{O}_K$ with multiplicities $e_i \in \mathbf{Z}_{>0}$.

Remark 3.3.3. The prime ideals appearing in the previous factorization are precisely those prime ideals of $\mathcal{O}_K$ lying over p. Indeed, we know from Remark 3.2.16 that the prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ appearing in the factorization are precisely those such that $p\mathcal{O}_K \subseteq \mathfrak{p}$, meaning that $p\mathbf{Z} \subseteq \mathfrak{p} \cap \mathbf{Z}$. Since these are two non-zero prime ideals of $\mathbf{Z}$ it must be that $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$.

Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a non-zero prime ideal such that $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. Then we have seen in Proposition 2.3.17 that

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p} = \mathbf{F}_\mathfrak{p}$$

is a finite extension of fields.

Definition 3.3.4 (Ramification indexes and inertia degree)**.** Let $p \in \mathbf{Z}$ be a prime number with a factorization into pairwise distinct prime ideals

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}, \quad e_i \in \mathbf{Z}_{>0}$$

in the ring of integers $\mathcal{O}_K$.For any $\mathfrak{p}_i$ we define the:

- *Ramification index* of p at $\mathfrak{p}_i$ to be the multiplicity e_i.
- *Inertia degree* of p at $\mathfrak{p}_i$ to be $f_i = [\mathbf{F}_\mathfrak{p} : \mathbf{F}_p] = \dim_{\mathbf{F}_p} \mathbf{F}_\mathfrak{p}$.

We say that p *ramifies* in K if one of the ramification indexes is at least 2.

Example 3.3.5. Let $K = \mathbf{Q}(\sqrt{-5})$ so that $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$. We have seen in Example 3.2.14 that the prime factorizations of (2) and (3) in $\mathbf{Z}[\sqrt{-5}]$ are

$$(2) = \mathfrak{q}^2, (3) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$$

where $\mathfrak{q} = (2, 1 + \sqrt{-5}), \mathfrak{p}_1 = (3, 1 + \sqrt{-5}), \mathfrak{p}_2 = (3, 1 - \sqrt{-5})$. Hence 2 has ramification index 2 at $\mathfrak{q}$ while 3 has ramification index 1 at both $\mathfrak{p}_1, \mathfrak{p}_2$. Furthermore, we have also seen that $[\mathbf{F}_{\mathfrak{p}_i} : \mathbf{F}_3] = 1$ for $i = 1, 2$ and that $[\mathbf{F}_\mathfrak{q} : \mathbf{F}_2] = 1$ so all inertia degrees are equal to 1.

It turns out that the number of prime ideals of $\mathcal{O}_K$ appearing in the factorization of $p\mathcal{O}_K$ is always equal to the degree $[K : \mathbf{Q}]$, if we count the prime ideals with the ramification index and the inertia degree. Before stating and proving the precise result, we start with a lemma:

Lemma 3.3.6. *Let K be a number field and let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a non-zero prime ideal ying over a prime $p \in \mathbf{Z}$ with inertia degree $f = \dim_{\mathbf{F}_p} \mathbf{F}_\mathfrak{p}$. Assume that $p \in \mathfrak{p}^e$ for a certain $e \in \mathbf{Z}_{>0}$. Then the inclusion $\mathbf{Z}/p\mathbf{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}^e$ makes $\mathcal{O}_K/\mathfrak{p}^e$ into a $\mathbf{F}_p$-vector space of dimension*

$$\dim_{\mathbf{F}_p} \mathcal{O}_K/\mathfrak{p}^e = ef$$

Proof. We prove the statement by induction on e. For $e = 1$ the statement is clear. Assume now that $e > 1$ and consider the map

$$\pi\colon \mathcal{O}_K/\mathfrak{p}^e \longrightarrow \mathcal{O}_K/\mathfrak{p}^{e-1}$$

This is a surjective homomorphism of $\mathbf{F}_p$-vector spaces and the kernel is isomorphic to $\mathfrak{p}^{e-1}/\mathfrak{p}^e \cong \mathcal{O}_K/\mathfrak{p}$ because of Proposition 3.2.19. Then by induction we see that

$$\dim_{\mathbf{F}_p} = \dim_{\mathbf{F}_p} \mathcal{O}_K/\mathfrak{p}^{e-1} + \dim_{\mathbf{F}_p} \mathcal{O}_K/\mathfrak{p} = (e-1)f + f = ef.$$

□

Now we give the statement on the ramification indexes and inertia degrees:

Proposition 3.3.7. *Let K be a number field of degree $[K : \mathbf{Q}] = n$ and let $p \in \mathbf{Z}$ a prime number with prime factorization*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s} \qquad \text{in } \mathcal{O}_K$$

and let f_i be the inertia degree of p at $\mathfrak{p}_i$ for $i = 1, \dots, n$. Then $\mathcal{O}_K/p\mathcal{O}_K$ is an $\mathbf{F}_p$-vector space and

$$\dim_{\mathbf{F}_p} \mathcal{O}_K/p\mathcal{O}_K = e_1f_1 + \dots + e_sf_s = n.$$

Proof. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ form a basis of $\mathcal{O}_K$ as a $\mathbf{Z}$-module then it is straightforward to check that the classes $[\alpha_1], \dots, [\alpha_n] \in \mathcal{O}_K/p\mathcal{O}_K$ form a basis of $\mathcal{O}_K/p\mathcal{O}_K$ as a $\mathbf{F}_p$-vector space. Hence $\dim_{\mathbf{F}_p} \mathcal{O}_K/p\mathcal{O}_K = n$.

On the other hand, the Chinese Remainder Theorem 3.2.17 gives an isomorphism of $\mathbf{F}_p$-vector spaces

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \dots \times \mathcal{O}_K/\mathfrak{p}_s^{e_s}$$

and Lemma 3.3.6 shows that each $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ is a $\mathbf{F}_p$-vector space of dimension e_if_i. Hence $n = e_1f_1 + \dots + e_sf_s$. □

3.3.1 Computing a factorization

To compute the factorization of a prime in a ring of integers, a result of Dedekind and Kummer is often useful. Recall from Lemma 2.3.9 that if K is a number field, then we can always write $K = \mathbf{Q}(\alpha)$ for $\alpha \in \mathcal{O}_K$, but it is not necessarily true that $\mathcal{O}_K = \mathbf{Z}[\alpha]$. It is however true from Example 2.3.18 that $\mathbf{Z}[\alpha]$ is a lattice in $\mathcal{O}_K$ so that $\mathcal{O}_K/\mathbf{Z}[\alpha]$ is a finite abelian group.

Theorem 3.3.8 (Dedekind-Kummer)**.** *Let $K = \mathbf{Q}(\alpha)$ a number field with $\alpha \in \mathcal{O}_K$ and let $p \in \mathbf{Z}$ be a prime such that $p \nmid |\mathcal{O}_K/\mathbf{Z}[\alpha]|$. Let $m_{\mathbf{Q},\alpha}(x) \in \mathbf{Z}[x]$ be the minimal polynomial of α over $\mathbf{Q}$ and assume that the prime factorization of $\overline{m}_{\alpha,\mathbf{Q}}(x)$ in $\mathbf{F}_p[x]$ is*

$$\overline{m}_{\alpha,\mathbf{Q}}(x) = \overline{h}_1(x)^{e_1} \dots \overline{h}_s(x)^{e_s}$$

where $h_i(x) \in \mathbf{Z}[x]$ are monic with $\overline{h}_i(x) \in \mathbf{F}_p[x]$ irreducible, pairwise coprime in $\mathbf{F}_p[x]$ and $e_i \in \mathbf{Z}_{>0}$. Then the unique factorization of $p\mathcal{O}_K$ into prime ideals is

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$$

where $\mathfrak{p}_i = (p, h_i(\alpha))$. Furthermore, $\mathbf{F}_{\mathfrak{p}_i} \cong \mathbf{F}_p[x]/(\bar{h}_i(x))$ so that the inertia degree of p at $\mathfrak{p}_i$ is $f_i = \deg h_i$.

The key to this result is the following simple lemma:

Lemma 3.3.9. *Let $\Lambda \subseteq \Lambda'$ be two free abelian groups of rank n and let $p \in \mathbf{Z}$ be a prime such that $p \nmid |\Lambda/\Lambda'|$. Then $p\Lambda' \cap \Lambda = p\Lambda$ and the map*

$$\Lambda/p\Lambda \longrightarrow \Lambda'/p\Lambda', \quad [x] \mapsto [x]$$

is an isomorphism of $\mathbf{F}_p$-vector spaces.

Proof. Take any two bases $\beta_1, \dots, \beta_n$ of Λ and $\beta_1', \dots, \beta_n'$ of Λ' and let $A \in \mathbf{Z}^{n\times n}$ be the matrix representing the inclusion $\Lambda \hookrightarrow \Lambda'$ with respect to these bases. We know from Lemma A.5.35 that $|\Lambda'/\Lambda| = |\det A|$ so that $p \nmid \det(A)$. Now we see that the classes $[\beta_1], \dots, [\beta_n]$ are a basis of $\Lambda/p\Lambda$ and $[\beta_1'], \dots, [\beta_n']$ are a basis of $\Lambda'/p\Lambda'$ as $\mathbf{F}_p$-vector spaces, and the matrix representing the map in the statement of the proposition with respect to these bases is given by $\overline{A} \in \mathbf{F}_p^{n\times n}$. By hypothesis $\det(\overline{A}) \neq 0$ in $\mathbf{F}_p$ so that this is an isomorphism. In particular, the map is injective, meaning that $p\Lambda = p\Lambda' \cap \Lambda$. □

With this we can prove the Dedekind-Kummer theorem:

Proof of Theorem 3.3.8. The map $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K, [x] \mapsto [x]$ is an homomorphism of rings and Lemma 3.3.9 shows that it is an isomorphism. Consider the ideals $H_i = p\mathbf{Z}[\alpha] + h_i(\alpha)\mathbf{Z}[\alpha] \subseteq \mathbf{Z}[\alpha]$ for $i = 1, \dots, s$. We claim that these are all the prime ideals in $\mathbf{Z}[\alpha]$ that contain $p\mathbf{Z}[\alpha]$. This is equivalent to showing that the $H_i/p\mathbf{Z}[\alpha]$ are all the prime ideals in $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$: we see that

$$\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \cong \mathbf{Z}[x]/(p, m_{\alpha,\mathbf{Q}}(x)) \cong \mathbf{F}_p[x]/(\bar{m}_{\alpha,\mathbf{Q}}(x))$$

and since $\bar{m}_{\alpha,\mathbf{Q}}(x) = \bar{h}_1(x)^{e_1} \dots \bar{h}_s(x)^{e_s}$ is the prime factorization in the PID $\mathbf{F}_p[x]$, the prime ideals in $\mathbf{F}_p[x]/(\overline{m}_{\alpha,\mathbf{Q}}(x))$ are all those generated by the $\overline{h}_i(x)$. These ideals correspond precisely to the $H_i/p\mathcal{O}_K$ in $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$. This proves our claim, and the isomorphism $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \cong \mathcal{O}_K/p\mathcal{O}_K$ maps $H_i/p\mathcal{O}_K$ to $\mathfrak{p}_i/p\mathcal{O}_K$. Hence the $\mathfrak{p}_i$ are all the prime ideals in $\mathcal{O}_K$ that contain $p\mathcal{O}_K$. We also observe that

$$\mathbf{F}_{\mathfrak{p}_i} \cong \mathcal{O}_K/\mathfrak{p}_i \cong \frac{\mathcal{O}_K/p\mathcal{O}_K}{\mathfrak{p}_i/p\mathcal{O}_K} \cong \frac{\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]}{H_i/p\mathbf{Z}[\alpha]} \cong \mathbf{F}_p[x]/(\overline{h}_i(x)).$$

At this point, we know that the prime factorization of $p\mathcal{O}_K$ has the form $p\mathcal{O}_K = \mathfrak{p}_1^{e_1'} \dots \mathfrak{p}_s^{e_s'}$ for certain $e_i' \in \mathbf{Z}_{>0}$ and we want to prove that $e_i' = e_i$. To do so, it is enough to show that $p\mathcal{O}_K \mid \mathfrak{p}_1^{m_1} \dots \mathfrak{p}_s^{m_s}$ if and only if $m_i \geq e_i$ for each $i = 1, \dots, s$. Equivalently

$$(\mathfrak{p}_1/p\mathcal{O}_K)^{m_1} \cdot \ldots \cdot (\mathfrak{p}_s/p\mathcal{O}_K)^{m_s} = 0 \text{ in } \mathcal{O}_K/p\mathcal{O}_K \quad \text{if and only if} \quad m_i \geq e_i \text{ for all } i = 1, \dots, s.$$

and using the isomorphism $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$ this means that

$$(H_1/p\mathbf{Z}[\alpha])^{m_1} \cdot \ldots \cdot (H_s/p\mathbf{Z}[\alpha])^{m_s} = 0 \text{ in } \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \quad \text{if and only if} \quad m_i \geq e_i \text{ for all } i = 1, \dots, s.$$

Using the previous isomorphism $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \cong \mathbf{F}_p[x]/(\overline{m}_{\alpha,\mathbf{Q}}(x))$ and using the fact that the ideal $(H_i/p\mathbf{Z}[\alpha])^{m_i}$ corresponds to the ideal generated by $[\overline{h}_i(x)]$ in $\mathbf{F}_p[x]/(m_{\alpha,\mathbf{Q}}(x))$, we see that the statement can be rephrased as

$$m_{\alpha,\mathbf{Q}}(x) \mid \bar{h}_1(x)^{m_1} \dots \bar{h}_s(x)^{m_s} \quad \text{in } \mathbf{F}_p[x] \quad \text{if and only if} \quad m_i \geq e_i \text{ for all } i = 1, \dots, s.$$

and this is clearly true. □

Example 3.3.10. We have seen in Example 3.2.14 that if $K = \mathbf{Q}(\sqrt{-5})$ with $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$, then

$$2\mathcal{O}_K = (2, 1+\sqrt{-5})^2, \quad 3\mathcal{O}_K = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$

is the prime decomposition of the ideals generated by 2 and 3 in $\mathcal{O}_K$. This can also be seen from the Dedekind-Kummer Theorem 3.3.8: indeed the minimal polynomial of $\sqrt{-5}$ is $f(x) = x^2 + 5$ and its factorization into irreducible in $\mathbf{F}_2[x]$ and $\mathbf{F}_3[x]$ is

$$\begin{aligned} x^2 + 5 = x^2 + 1 = (x+1)^2 \quad & \text{in } \mathbf{F}_2[x], \\ x^2 + 5 = x^2 - 1 = (x+1)(x-1) \quad & \text{in } \mathbf{F}_3[x]. \end{aligned}$$

Example 3.3.11. Let now $d \in \mathbf{Z}$ be a square-free number and consider $K = \mathbf{Q}(\sqrt{d})$. We want to compute the factorization of $2\mathcal{O}_K$ into prime ideals. We consider various cases:

- $d \equiv 2 \pmod 4$: then $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$ and the minimal polynomial of $\sqrt{d}$ is $x^2 - d$. In $\mathbf{F}_2[x]$ this polynomial factors as $x^2 - d = x^2$, hence the Dedekind-Kummer theorem tells us that

  $$2\mathcal{O}_K = (2, \sqrt{d})^2$$

  is the prime factorization. In particular we see that the ramification index at the unique prime is 2 while the inertia degree is 1.

- $d \equiv 3 \pmod 4$: then $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$ and the minimal polynomial of $\sqrt{d}$ is $x^2 - d$. In $\mathbf{F}_2[x]$ we have that $x^2 - d = x^2 + 1 = (x+1)^2$, hence the Dedekind-Kummer theorem tells us that

  $$2\mathcal{O}_K = (2, \sqrt{d}+1)^2$$

  is the prime factorization. In particular we see that the ramification index at the unique prime is 2 while the inertia degree is 1.

- $d \equiv 1 \pmod 4$: then $\mathcal{O}_K = \mathbf{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{d}}{2}$. If we write $d = 4k+1$ for $k \in \mathbf{Z}$, the minimal polynomial of α is $x^2 - x - k$. Now we have two subcases

  - $k \equiv 1 \pmod 2$, meaning $d \equiv 5 \pmod 8$: then the minimal polynomial $x^2 - x - k$ is already irreducible in $\mathbf{F}_2[x]$ so that the ideal $2\mathcal{O}_K$ is prime in $\mathcal{O}_K$. The ramification degree is 1 and the inertia degree is 2.
  - $k \equiv 0 \pmod 2$, meaning that $d \equiv 1 \pmod 8$: then the minimal polynomial factors in $\mathbf{F}_2[x]$ as $x^2 - x - k = x(x-1)$ so that $2\mathcal{O}_K = (2, \alpha)(2, \alpha - 1)$ is the unique factorization. The ramification index and the inertia degree at both prime ideals are equal to 1.

Example 3.3.12. Let $K = \mathbf{Q}(\alpha)$ be a number field of degree $n = [K : \mathbf{Q}(\alpha)]$ with $\alpha \in \mathcal{O}_K$ and assume that the minimal polynomial $m_{\alpha,\mathbf{Q}}(x) \in \mathbf{Z}[x]$ is Eisenstein with respect to a prime number $p \in \mathbf{Z}$. Then Proposition 2.3.28 shows that $p \nmid |\mathcal{O}_K/\mathbf{Z}[\alpha]|$ so that we can apply the Dedekind-Kummer theorem. Observe that in $\mathbf{F}_p[x]$ the minimal polynomial factors as $\overline{m}_{\alpha,\mathbf{Q}}(x) = x^n$, so that

$$p\mathcal{O}_K = (p, \alpha)^n$$

is the prime factorization of the ideal $p\mathcal{O}_K$. The ramification index of p at the unique prime $\mathfrak{p} = (p, \alpha)$ is n and the inertia degree is 1: we say that p *completely ramifies* in K. An example of this is the cyclotomic field $\mathbf{Q}(\zeta_p) = \mathbf{Q}(1 - \zeta_p)$ for an odd prime number p.

3.3.2 Discriminant and ramification

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Consider a prime number $p \in \mathbf{Z}$ and the prime factorization

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r}$$

The prime number p ramifies if and only if at least one of the ramification indexes e_i is at least two.

Lemma 3.3.13. *The prime number $p \in \mathbf{Z}$ ramifies if and only if the ring $\mathcal{O}_K/p\mathcal{O}_K$ is not reduced: this means that there is an element $x \in \mathcal{O}_K/p\mathcal{O}_K$ such that $x \neq 0$ but $x^N = 0$ for a certain $N > 0$.*

Proof. Assume $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_r^{e_r}$ is the prime factorization of $p\mathcal{O}_K$. The Chinese remainder theorem shows that

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \dots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$$

If $e_i = 1$ for each i, then this ring is a product of fields, and it is easy to see that such a ring is reduced. Otherwise, we can assume that $e_1 \geq 2$. Take an element $\alpha \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^{e_1}$ and consider the element $x = ([\alpha], 0, 0, \dots, 0) \in \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \dots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$. Then $x^{e_1} = 0$ but $x \neq 0$. □

Theorem 3.3.14. *Let K be a number field. A prime number $p \in \mathbf{Z}$ ramifies in K if and only if p divides the discriminant* $\mathrm{disc}(K)$.

Proof. Fix an integral basis $\alpha_1, \dots, \alpha_n$ of $\mathcal{O}_K$ and consider the matrix $T = (\mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i\alpha_j))$. By definition $\mathrm{disc}(K) = \det(T)$ so that p divides the discriminant if and only if the matrix T is singular modulo p. This means that there are $m_1, \dots, m_n \in \mathbf{Z}$ not all divisible by p such that $\alpha = m_1\alpha_1 + \dots + m_n\alpha_n$ satisfies

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha \cdot \alpha_i) \in p\mathbf{Z} \quad \text{for all } i = 1, \dots, n\beta \in \mathcal{O}_K$$

In other words, there is $\alpha \in \mathcal{O}_K, \alpha \notin p\mathcal{O}_K$ such that

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha \cdot \beta) \in p\mathbf{Z} \quad \text{for all } \beta \in \mathcal{O}_K.$$

We can rephrase this again in terms of the ring $A = \mathcal{O}_K/p\mathcal{O}_K$, which is also a finite-dimensional $\mathbf{F}_p$-vector space. We can define the trace as the usual linear map

$$\mathrm{Tr}_{A/\mathbf{F}_p} \colon A \longrightarrow \mathbf{F}_p, \quad x \mapsto \mathrm{Tr}_{A/\mathbf{F}_p}(\cdot x \colon A \to A)$$

and this also gives a bilinear form over the $\mathbf{F}_p$ vector space A given by

$$\mathrm{Tr}_{A/\mathbf{F}_p} \colon A \times A \longrightarrow \mathbf{F}_p, \quad (x, y) \mapsto \mathrm{Tr}_{A/\mathbf{F}_p}(xy)$$

This bilinear form is represented by the matrix T, taken modulo p. Hence we can see that p divides the discriminant if and only if the bilinear form $\mathrm{Tr}_{A/\mathbf{F}_p}$ is degenerate.

Let now $p\mathcal{O}_K \cong \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_r^{e_r}$ be the irreducible factorization of $p\mathcal{O}_K$: then there is an isomorphism of rings and of $\mathbf{F}_p$ vector spaces given by the Chinese remainder theorem $A \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \dots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$. It is easy to see that the trace of A , taken as a bilinear form, splits into a direct sum of traces $\mathrm{Tr}_{A/\mathbf{F}_p} \cong \mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}_1^{e_1})/\mathbf{F}_p} \oplus \dots \oplus \mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}_r^{e_r})/\mathbf{F}_p}$, so what we need to prove is that the bilinear form given by $\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}_i^{e_i})/\mathbf{F}_p}$ is degenerate if and only if $e_i > 1$.

If $e_i = 1$, then $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field extension of $\mathbf{F}_p$ and it is a fact of field theory that any such extension has a non-degenerate trace (because every finite extension of a finite field is separable). If instead $e_i > 1$ we can take as in Lemma 3.3.13 an element $x \in \mathcal{O}_K/\mathfrak{p}_i^{e_i}, x \neq 0$ but $x^N = 0$ for a certain $N > 0$. Then for any other $y \in \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ we have that $(xy)^N = x^N y^N = 0$ so that the multiplication map $\cdot xy \colon \mathcal{O}_K/\mathfrak{p}_i^{e_i} \to \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ is nilpotent. Hence it trace must be zero by linear algebra. □

Chapter 4

Geometry of numbers

4.1 The absolute norm

Let K be a number field and $\mathcal{O}_K$ its ring of integers. If $I \subseteq \mathcal{O}_K$ is a non-zero ideal, we have seen in Proposition 2.3.17 that $\mathcal{O}_K/I$ is a finite set. Hence we can define:

Definition 4.1.1 (Ideal norm)**.** Let K be a number field with ring of integers $\mathcal{O}_K$. The *abosolute norm* of a non-zero ideal $I \subseteq \mathcal{O}_K$ is

$$\|I\| := |\mathcal{O}_K/I| \in \mathbf{Z}_{>0}$$

This is related to the norm of elements, as the name suggests:

Lemma 4.1.2. *Let K be a number field with ring of integers $\mathcal{O}_K$. If $I = (\alpha) \subseteq \mathcal{O}_K$ is a principal ideal, then*

$$\|(\alpha)\| = |N_{K/\mathbf{Q}}(\alpha)|.$$

Proof. Fix a basis $\beta_1, \ldots, \beta_n$ of $\mathcal{O}_K$ as a $\mathbf{Z}$ module so that $\alpha\beta_1, \ldots, \alpha\beta_m$ is a basis of $(\alpha) = \alpha \cdot \mathcal{O}_K$. Consider the inclusion $(\alpha) = \alpha \cdot \mathcal{O}_K \subseteq \mathcal{O}_K$ and let M be the matrix that represents the inclusion with respect to the bases above. Then M is also the matrix that represents the multiplication-by-α map $(\cdot\alpha)\colon K \longrightarrow K$ with respect to the basis $\alpha_1, \ldots, \alpha_m$ of K as a $\mathbf{Q}$-vector space. Then we know that

$$|\mathcal{O}_K/(\alpha)| = |\det(M)| = |\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)|. \qquad \square$$

Remark 4.1.3. A non-zero ideal $I \subseteq \mathcal{O}_K$ has norm $\|I\| = 1$ if and only if $I = \mathcal{O}_K$. Instead $I \subseteq \mathcal{O}_K$ is a non-zero prime ideal if and only if $\mathcal{O}_K/I$ is a field. In particular $\|I\|$ must be the power of a prime number. There is a partial converse: if $\|I\|$ is a prime number, then $\mathcal{O}_K/I$ must be a finite field, hence I is a non-zero prime ideal.

We can express the norm in terms of the prime factorization of the ideal

Proposition 4.1.4. *Let K be a number field.*

1. *If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a non-zero prime ideal with $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ and $f = [\mathbf{F}_\mathfrak{p} : \mathbf{F}_p]$, then*

$$\|\mathfrak{p}^e\| = \|\mathfrak{p}\|^e = p^{ef} \quad \text{for all } e \geq 0.$$

2. If $I \subseteq \mathcal{O}_K$ is a non-zero ideal with a prime factorization $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$, then

$$\|I\| = \|\mathfrak{p}_1\|^{e_1} \dots \|\mathfrak{p}_r\|^{e_r}.$$

3. If $I, J \subseteq \mathcal{O}_K$ are two ideals, then

$$\|I \cdot J\| = \|I\| \cdot \|J\|.$$

Proof. 1. We prove the statement by induction on e. If $e = 0$ then $I = A$ and $\|I\| = 1$. Assume now that $e > 0$. Then as in the proof of Lemma 3.3.6 we consider the natural map

$$\pi \colon \mathcal{O}_K/\mathfrak{p}^e \to \mathcal{O}_K/\mathfrak{p}^{e-1}$$

This is a surjective homomorphism of $\mathcal{O}_K$-modules whose kernel is isomorphic to $\mathfrak{p}^{e-1}/\mathfrak{p}^e \cong \mathcal{O}_K/\mathfrak{p}$ because of Proposition 3.2.19. By induction we get

$$|\mathcal{O}_K/\mathfrak{p}^e| = |\mathcal{O}_K/\mathfrak{p}^{e-1}| \cdot |\mathcal{O}_K/\mathfrak{p}| = p^{f(e-1)} \cdot p^f = p^{ef}.$$

2. By the Chinese Remainder Theorem of Proposition 3.2.17 and the previous point we have

$$\|I\| = |\mathcal{O}_K/I| = |\mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \dots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}| = \prod_{i=1}^{m} |\mathcal{O}_K/\mathfrak{p}_i^{e_i}| = \prod_{i=1}^{r} \|\mathfrak{p}_i\|^{e_i}$$

3. This follows from the previous point by taking the unique factorization of both ideals.

□

Remark 4.1.5. Let $I \subseteq \mathcal{O}_K$ be an ideal and let $\|I\| = p_1^{h_1} \dots p_r^{h_r}$ the factorization into prime numbers in $\mathbf{Z}$. Then Proposition 4.1.4 shows that $I \subseteq \mathcal{O}_K$ is a product of prime ideals lying over the $p_1, \dots, p_r$.

Remark 4.1.6. Using the unique factorization property for fractional ideals, we can extend the ideal norm to a homomorphism of multiplicative groups

$$\|\cdot\| \colon \operatorname{Div}(\mathcal{O}_K) \longrightarrow \mathbf{Q}^\times, \quad \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m} \mapsto \|\mathfrak{p}_1\|^{e_1} \dots \|\mathfrak{p}_m\|^{e_m}$$

where in the previous expression the $\mathfrak{p}_i$ are mutually distinct non-zero prime ideals in $\mathcal{O}_K$ and $e_i \in \mathbf{Z}$.

An important fact is that there are only finitely many ideals with norm bounded by a fixed number:

Lemma 4.1.7. *For any fixed $M \in \mathbf{Z}_{\geq 0}$ there are finitely many non-zero ideals $I \subseteq \mathcal{O}_K$ such that $\|I\| = M$.*

Proof. Assume that $\|I\| = M$ and write $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$ where the $\mathfrak{p}_i \subseteq \mathcal{O}_K$ are mutually distinct non-zero prime ideals, and $e_i \in \mathbf{Z}_{\geq 0}$. Write then $\mathfrak{p}_i \cap \mathbf{Z} = p_i\mathbf{Z}$ for certain prime numbers $p_i \in \mathbf{Z}$ for $i = 1, \dots, m$ and set $f_i := [\mathbf{F}_{\mathfrak{p}_i} : \mathbf{F}_{p_i}]$. Then

$$M = \|\mathfrak{p}_1\|^{e_1} \cdot \dots \cdot \|\mathfrak{p}_m\|^{e_m} = p_1^{e_1 f_1} \cdot \dots \cdot p_m^{e_m f_m}.$$

Hence there are finitely many possibilities for the p_i because they must be among the prime factors of M, so we only have finitely many possibilities for the $\mathfrak{p}_i$, because there are finitely many ideals lying over each prime. Since we must also have finitely many possibilities for the e_i, we conclude. □

Example 4.1.8. Fix $K = \mathbf{Q}(\sqrt{-5})$. We want to find all ideals $I \subseteq \mathcal{O}_K$ with norm $\|I\| = 2$. Notice that any such ideal must be prime and must lie over 2. The factorization of 2 in $\mathcal{O}_K$ is

$$2\mathcal{O}_K = (2, 1 + \sqrt{-5})^2$$

and $4 = \|2\mathcal{O}_K\| = \|(2, 1 + \sqrt{-5})\|^2$ so that $\|(2, 1 + \sqrt{-5})\| = 2$. Then $(2, 1 + \sqrt{-5})$ is the unique ideal in $\mathcal{O}_K$ of norm 2.

4.2 Minkowski's bound and finiteness of the class group

We now look at class groups in the context of number fields:

Definition 4.2.1 (Class group of a number field)**.** If K is a number field, its class group is

$$\mathrm{Cl}(K) := \mathrm{Cl}(\mathcal{O}_K) = \mathrm{Div}(\mathcal{O}_K)/\mathrm{Prin}(\mathcal{O}_K)$$

Remark 4.2.2. As for any Dedekind domain, the ring $\mathcal{O}_K$ is an UFD, and then also a PID, if and only if $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$.

The key result on this group is due to Hermann Minkowski (1864 - 1909). To state it, we start with a definition and a remark:

Remark 4.2.3. An embedding $\sigma\colon K \hookrightarrow \mathbf{C}$ is called *real* if $\sigma(K) \subseteq \mathbf{R}$, and it is called *complex* otherwise. Notice that if σ is a complex embedding and if $\iota\colon \mathbf{C} \to \mathbf{C}$ is the complex conjugation, then $\iota \circ \sigma$ is another complex embedding which is distinct from σ. Hence, the number of complex embeddings must be even. If r is the number of real embeddings, and $2s$ is the number of complex embeddings, then

$$r + 2s = [K : \mathbf{Q}].$$

Example 4.2.4. For example, let $d \in \mathbf{Z}$ be a square-free integers. The embeddings of $\mathbf{Q}(\sqrt{d})$ in $\mathbf{C}$ are given by the identity and by

$$\sigma\colon \mathbf{Q}(\sqrt{d}) \to \mathbf{C}, \sigma(\sqrt{d}) = -\sqrt{d}$$

These are both real if $d > 0$ and they are both complex if $d < 0$.

The surprising theorem of Minkowski is the following:

Theorem 4.2.5 (Minkowski's bound)**.** *Let K be a number field of degree n and let $2s$ be the number of its complex embeddings. Then each element in the class group $\mathrm{Cl}(K)$ can be represented by an ideal $I \subseteq \mathcal{O}_K$ such that*

$$\|I\| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\mathrm{disc}(K)|}$$

Before giving the proof, let us give a couple of important consequences:

Theorem 4.2.6. *If K is a number field, its class group $\mathrm{Cl}(K)$ is finite.*

Proof. By Minkowski's Theorem 4.2.5 there is $B_K > 0$ such that any element in the class group can be represented by an ideal $I \subseteq \mathcal{O}_K$ with $\|I\| < B_K$. By Lemma 4.1.7, there are finitely many such ideals. □

Definition 4.2.7 (Class number)**.** If K is a number field, its *class number* is

$$h_K = |\operatorname{Cl}(K)|.$$

Example 4.2.8. Let us consider the field $K = \mathbf{Q}(i)$. This has degree 2, two complex embeddings and $\operatorname{disc}(\mathbf{Q}(i)) = -4$. The bound appearing in Minkowski's Theorem 4.2.5 is

$$\frac{2!}{2^2}\left(\frac{4}{\pi}\right) \cdot \sqrt{|-4|} = \frac{4}{\pi} < 2.$$

Hence each element in $\operatorname{Cl}(\mathbf{Q}(i))$ can be represented by an ideal $I \subseteq \mathcal{O}_K$ of norm $\|I\| \leq 1$. The unique such ideal is $I = A$, hence

$$\operatorname{Cl}(\mathbf{Q}(i)) = \{1\}, \quad h_{\mathbf{Q}(i)} = 1.$$

and this gives another proof that $\mathcal{O}_{\mathbf{Q}(i)} = \mathbf{Z}[i]$ is a PID.

Example 4.2.9. If we consider the field $K = \mathbf{Q}(\sqrt{-5})$. Minkowski's bound shows that each element in the class group is represented by an ideal $I \subseteq \mathcal{O}_K$ of norm

$$\|I\| \leq \frac{2!}{2^2} \cdot \frac{4}{\pi} \cdot \sqrt{|-4 \cdot 5|} = \frac{4 \cdot \sqrt{5}}{\pi} < 3$$

Hence we can assume $\|I\| \leq 2$. On the other hand, we have already seen that there is precisely one ideal of norm 2, given by $(2, 1 + \sqrt{-5})$. This ideal is not principal otherwise it would be generated by an element $x + \sqrt{-5}y, x, y \in \mathbf{Z}$ of norm ± 2. But the equation

$$2 = |N_{K/\mathbf{Q}}(x + \sqrt{-5})| = x^2 + 5y^2$$

has no integer solutions. This shows that the class of $[(2, 1 + \sqrt{-5})]$ in the class group is not trivial, so that

$$\operatorname{Cl}(\mathbf{Q}(\sqrt{-5})) = \{1, [(2, 1 + \sqrt{-5})]\} \cong \mathbf{Z}/2\mathbf{Z}, \quad h_{\mathbf{Q}(\sqrt{-5})} = 2.$$

This shows in a different way that $\mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$ is not an UFD.

Another consequence of Minkowski's bound is the following

Theorem 4.2.10. *If K is a number field and there is no prime $p \in \mathbf{Z}$ that ramifies in K, then $K = \mathbf{Q}$.*

Proof. Since a prime ramifies if and only if it divides the discriminant, this is equivalent to showing that $|\operatorname{disc}(K)| > 1$ if $n = [K : \mathbf{Q}] > 1$. To do so, we can invert Minkowski's bound: we know that the non-empty class group is made of elements represented by ideals $I \subseteq \mathcal{O}_K$ such that

$$\sqrt{|\operatorname{disc}(K)|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \|I\|$$

Now notice that $\|I\| \geq 1$ and that $s \leq \frac{n}{2}$, hence

$$\sqrt{|\operatorname{disc}(K)|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}$$

Finally, one can check that the right hand side is strictly larger than 1 whenever $n > 1$, so we are done. □

4.2.1 Lattices in $\mathbf{R}^n$

Now we go towards the proof of Minkowski's bound. We consider the real vector space $\mathbf{R}^n$ with the metric given by the standard scalar product and norm

$$\langle x, y\rangle = x^t \cdot y, \quad |x| = \sqrt{x^t \cdot x}$$

Definition 4.2.11 (Lattices in $\mathbf{R}^n$)**.** A lattice in $\mathbf{R}^n$ is a free and finitely generated subgroup $\Lambda \subseteq \mathbf{R}^n$ of rank n that generates the whole of $\mathbf{R}^n$ as a real vector space.

Example 4.2.12. The most fundamental example of a lattice is $\mathbf{Z}^n$ inside $\mathbf{R}^n$.

If $\Lambda \subseteq \mathbf{R}^n$ is a lattice, an *integral basis* of Λ is a basis $\alpha_1, \ldots, \alpha_n$ of Λ as a free $\mathbf{Z}$-module.

Definition 4.2.13 (Discrete subgroup)**.** A subgroup $\Lambda \subseteq \mathbf{R}^n$ is discrete if the induced topology is the discrete one. Equivalently, each element $\lambda \in \Lambda$ has an open neighborhood $U \subseteq \mathbf{R}^n$ such that $U \cap \Lambda = \{\lambda\}$.

Lemma 4.2.14. *1. A lattice is a discrete subgroup of $\mathbf{R}^n$.*

2. A discrete subgroup of $\mathbf{R}^n$ is a closed subset of $\mathbf{R}^n$. It is furthermore a free and finitely generated abelian group of rank $s \leq n$ and it spans a vector space of dimension s. In particular, it is a lattice if and only if it has rank n.

3. A discrete subgroup $\Lambda \subseteq \mathbf{R}^n$ is a lattice if and only if there is a bounded subset B such that the map $B \to \mathbf{R}^n/\Lambda$ is surjective.

Proof. 1. Assume that Λ is a lattice and fix an integral basis $\alpha_1, \ldots, \alpha_n$. Since they generate $\mathbf{R}^n$ as a real vector space, they are also a basis of $\mathbf{R}^n$. Consider the linear map $f\colon \mathbf{R}^n \to \mathbf{R}^n$ that sends the canonical basis $e_1, \ldots, e_n$ to $\alpha_1, \ldots, \alpha_n$. This is a linear isomorphism and then also an homeomorphism of topological spaces. By construction $f(\mathbf{Z}^n) = \Lambda$ and since $\mathbf{Z}^n$ is clearly discrete in $\mathbf{R}^n$ it follows that Λ is also closed and discrete in $\mathbf{R}^n$.

2. We first show that a discrete subgroup $\Lambda \subseteq \mathbf{R}^n$ is closed. Choose a ball B centered in 0 such that $B \cap \Lambda = \{0\}$. Observe that if (x_i) is a sequence of elements in Λ such that $x_i \to x$ for $i \to \infty$, then there is $N > 0$ such that $x_i - x_j \in B$ for all $i, j \geq N$. Since $x_i - x_j \in \Lambda$, it must be that $x_i - x_j = 0$ for all $i, j \geq N$, meaning that the sequence is eventually constant, so that $x \in \Lambda$. For the rest of the statement, look at Proposition 4.15 in Milne, "Algebraic Number Theory".

3. If Λ is a lattice, then using the argument of point (1) we can reduce to the case $\Lambda = \mathbf{Z}^n$, where the statement is clear. Conversely, assume that $\Lambda \subseteq \mathbf{R}^n$ is a discrete subgroup and that there is a bounded set $B \subseteq \mathbf{R}^n$ such that $B \to \mathbf{R}^n/\Lambda$ is surjective. We want to use point (2) and prove that the subspace $H \subseteq \mathbf{R}^n$ spanned by Λ is the whole space. Assume that this is not true and let $v \in H^\perp, v \neq 0$. Then for any $M > 0$ and $h \in H$ we see that $|M \cdot v + h|^2 = |M \cdot v|^2 + |h|^2 \geq M^2|v|^2$. If we choose M large enough, this implies that $M \cdot v + h \notin B$ for any $h \in \Lambda$, which is impossible by hypothesis.

□

Corollary 4.2.15. *If $\Lambda \subseteq \mathbf{R}^n$ is a lattice and $B \subseteq \mathbf{R}^n$ a bounded subset, then $\Lambda \cap B$ is finite.*

Proof. It is enough to prove the statement for the closed ball $B = \{x \in \mathbf{R}^n \,|\, |x| \leq M\}$ where $M > 0$ is fixed. Observe that since Λ is closed and discrete, it follows that $\Lambda \cap B$ is compact and discrete, so that it must be finite. □

Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of a lattice $\Lambda \subseteq \mathbf{R}^n$. To any such basis we can associate the *fundamental domain*

$$P = \left\{ \sum_{i=1}^{n} \lambda_i \alpha_i \,|\, \lambda_i \in [0,1) \right\} \subseteq \mathbf{R}^n$$

which is a measurable subset of volume (or measure) given by the determinant of the matrix that has the α_i as column vectors.

$$\mathrm{vol}(P) = |\det(\alpha_1 | \ldots | \alpha_n)|$$

Lemma 4.2.16. *With the previous notation it holds that Two fundamental domains of Λ corresponding to different bases have the same volume.*

Proof. If $\alpha_1', \ldots, \alpha_n'$ is another integral basis of Λ then

$$(\alpha_1' | \ldots | \alpha_n') = A(\alpha_1 | \ldots | \alpha_n)$$

where $A \in \mathrm{GL}_n(\mathbf{Z})$. Since $|\det A| = 1$, this shows what we want. □

Then we can make the following definition:

Definition 4.2.17 (Volume of a lattice)**.** The *volume* of a lattice Λ is the volume of a fundamental domain. We denote it by $\mathrm{vol}(\Lambda)$.

The key observation, due to Minkowski, is the following:

Theorem 4.2.18 (Minkowski)**.** *Let $\Lambda \subseteq \mathbf{R}^n$ be a lattice and $S \subseteq \mathbf{R}^n$ a measurable subset with measure $\mathrm{vol}(S) > \mathrm{vol}(\Lambda)$. Then there are distinct $x, y \in S$ such that $x - y \in \Lambda$.*

Proof. Fix an integral basis of Λ and a corresponding fundamental domain P. Then

$$\mathbf{R}^n = \bigsqcup_{\lambda \in \Lambda} P + \lambda, \quad S = \bigsqcup_{\lambda \in \Lambda} S \cap (P + \lambda)$$

so that

$$\mathrm{vol}(S) = \sum_{\lambda \in \Lambda} \mathrm{vol}(S \cap (P + \lambda)) = \sum_{\lambda \in \Lambda} \mathrm{vol}((S - \lambda) \cap P)$$

Notice that the sets $(S - \lambda) \cap P$ cannot be mutually disjoint, otherwise the last sum would be less or equal than $\mathrm{vol}(P)$, which is impossible by hypothesis. Hence there are distinct $\lambda, \mu \in \Lambda$ such that $(S - \lambda) \cap (S - \mu) \cap P \neq \emptyset$. Then there are $x, y \in S$ so that $x - \lambda = y - \mu$ so that $x - y = \lambda - \mu \in \Lambda$. □

We recall another couple of definitions: a subset $S \subseteq \mathbf{R}^n$ is called *convex* if whenever $x, y \in S$ the whole segment between them is contained in S. It is called *symmetric* if whenever S contains x then it contains $-x$ as well. From analysis one knows that each convex subset is measurable, so its measure, or volume $\mathrm{vol}(S)$ is well-defined.

Theorem 4.2.19 (Minkowski's convex body theorem)**.** *Let $\Lambda \subseteq \mathbf{R}^n$ be a lattice and $S \subseteq \mathbf{R}^n$ a convex, symmetric subset such that one of the following conditions hold*

1. $2^n \operatorname{vol}(\Lambda) < \operatorname{vol}(S)$.
2. *S is compact and* $2^n \operatorname{vol}(\Lambda) \leq \operatorname{vol}(S)$.

Then S contains at least one non-zero element in Λ.

Proof. For the first case, consider the set $T = \frac{1}{2}S$, of volume $\operatorname{vol}(T) = \frac{1}{2^n}\operatorname{vol}(S) > \operatorname{vol}(\Lambda)$. We can apply Theorem 4.2.18 and we see that there are $x, y \in S$ such that $\frac{1}{2}x - \frac{1}{2}y = \lambda \in \Lambda$ with $\lambda \neq 0$. Hence λ lies in the segment between the point $x \in S$ and the point $-y \in S$ (since S is symmetric). Since S is convex, $\lambda \in S$.

For the second case, consider the subsets $S_\varepsilon = (1+\varepsilon)\cdot S = \{(1+\varepsilon)x \,|\, x \in S\}$ for each $\varepsilon > 0$. It is straightforward to show that each of these is symmetric and convex with $\operatorname{vol}(S_\varepsilon) > \operatorname{vol}(S) \geq \operatorname{vol}(\Lambda)$. Hence by what we have already proved $S_\varepsilon \cap (\Lambda - \{0\}) \neq \emptyset$. Since S_ε is compact, it is also bounded, and then the sets $S_\varepsilon \cap (\Lambda - \{0\})$ are non-empty and finite. Since $S_\varepsilon \subseteq S_{\varepsilon'}$ for $\varepsilon < \varepsilon'$ we have that

$$\bigcap_{\varepsilon>0} S_\varepsilon \cap (\Lambda - \{0\}) = \left(\bigcap_{\varepsilon>0} S_\varepsilon\right) \cap (\Lambda - \{0\}) = S \cap (\Lambda - \{0\})$$

must also be non-empty. □

4.2.2 The canonical embedding of a number field

We want to apply the previous theory to the case of number fields. Let K be a number field of degree n. Recall that we have n distinct field embeddings $\sigma\colon K \hookrightarrow \mathbf{C}$ and of these r are real and $2s$ are complex, for certain $r, s \in \mathbf{N}$. If $\sigma\colon K \hookrightarrow \mathbf{C}$ is an embedding, we denote by $\bar{\sigma}$ the composition of σ with the complex conjugation $\mathbf{C} \to \mathbf{C}$. Then we take all the real embeddings $\sigma_1, \ldots, \sigma_r\colon K \hookrightarrow \mathbf{C}$ and then choose complex embeddings $\sigma_{r+1}, \ldots, \sigma_{r+s}\colon K \hookrightarrow \mathbf{C}$ such that

$$(\sigma_1, \ldots, \sigma_r, \tau_1, \ldots, \sigma_s, \bar{\sigma}_1, \ldots, \bar{\sigma}_s) = (\sigma_1, \ldots, \sigma_n)$$

are all the embeddings of K in $\mathbf{C}$. The corresponding *canonical embedding* of K associated to this choice is

$$\Psi\colon K \longrightarrow \mathbf{R}^r \times \mathbf{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha)) \tag{4.2.1}$$

This is an injective ring homomorphism,as well as an homomorphism of $\mathbf{Q}$-vector spaces.

Observe now that if we take the usual basis $1, i$ of $\mathbf{C}$ over $\mathbf{R}$, we have isomorphisms of real vector spaces

$$\mathbf{R}^2 \to \mathbf{C}, \quad (x, y) \mapsto x + iy, \qquad \mathbf{C} \to \mathbf{R}^2, \quad z \mapsto (\Re z, \Im z)$$

Note that under this isomorphism, the usual scalar product on $\mathbf{R}^2$ becomes the scalar product on $\mathbf{C}$ given by

$$\langle z, w\rangle = \Re(z)\Re(w) + \Im(z)\Im(w) = \Re(z \cdot \bar{w}) = \frac{1}{2}(z \cdot \bar{w} + \bar{w} \cdot z)$$

and in particular we see that the norm in $\mathbf{R}^2$ corresponds to the usual norm on $\mathbf{C}$. With this identification $\mathbf{C} \cong \mathbf{R}^2$ in mind, we can also think of $\mathbf{R}^r \times \mathbf{C}^s$ as the real vector space $\mathbf{R}^{r+2s} = \mathbf{R}^n$, so we can also speak of lattices inside $\mathbf{R}^r \times \mathbf{C}^s$. Now we can relate our two definition of lattices

Proposition 4.2.20. *Let $\Lambda \subseteq \mathcal{O}_K$ be a lattice of discriminant* $\operatorname{disc}(\Lambda)$*. Under the canonical embedding $\Psi\colon K \to \mathbf{R}^r \times \mathbf{C}^s$, the image $\Psi(\Lambda)$ is a lattice in $\mathbf{R}^r \times \mathbf{C}^s$ of volume*

$$\operatorname{vol}(\Psi(\Lambda)) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(\Lambda)|}.$$

Proof. Since Ψ is also an injective homomorphism of groups, we know that $\Psi(\Lambda)$ is a free abelian group of rank n. We will now prove that this spans the whole space as a real vector space and we will also compute the volume at the same time. Let $\alpha_1, \dots, \alpha_n$ be an integral basis of Λ as a free abelian group. With the identification $\mathbf{R}^r \times \mathbf{C}^s = \mathbf{R}^{r+2s}$ we see that

$$\begin{aligned}\Psi(\alpha) &= (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \Re\sigma_{r+1}(\alpha), \Im\sigma_{r+1}(\alpha), \dots, \Re\sigma_{r+s}(\alpha), \Im\sigma_{r+s}(\alpha)) \\ &= (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \bar{\sigma}_{r+1}(\alpha), \dots, \sigma_{r+s}(\alpha), \bar{\sigma}_{r+s}(\alpha)) \cdot A \\ &= (\sigma_1(\alpha), \dots, \sigma_n(\alpha)) \cdot A\end{aligned}$$

where A is the $n \times n$ matrix

$$A = \begin{pmatrix} I_r & 0 & \dots & 0 \\ 0 & J & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & J \end{pmatrix}, \quad J = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

in particular $\det J = \frac{1}{2}$ and $\det A = \frac{1}{2^s}$. Then, the matrix that has the $\Psi(\alpha_i)$ as columns has determinant we get

$$|\det(\Psi(\alpha_1)|\dots|\Psi(\alpha_n))| = |\det(\sigma_i(\alpha_j))| \cdot \det(A) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(\Lambda)|}.$$

Where the second equality comes from Proposition 2.3.25. In particular, this shows that the $\Psi(\alpha_i)$ are linearly independent over $\mathbf{R}$, so that the group $\Psi(\Lambda)$ that they span is indeed a lattice of volume given by the previous expression. □

Since any non-zero ideal in $\mathcal{O}_K$ is also a lattice, we get

Corollary 4.2.21. *let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Then $\Psi(I) \subseteq \mathbf{R}^r \times \mathbf{C}^s$ is a lattice with volume*

$$\operatorname{vol}(\Psi(I)) = \frac{1}{2^s} \cdot \sqrt{|\operatorname{disc}(K)|} \cdot \|I\|$$

Proof. Using Proposition 4.2.20, we need to show that $|\operatorname{disc}(I)| = \|I\|^2 \cdot |\operatorname{disc}(K)|$, but this follows immediately from Proposition 2.3.23. □

Now we can give the key proposition for the proof of Minkowski's bound:

Proposition 4.2.22. *Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Then I contains a non-zero element $\alpha \in I$ with*

$$|N_{K/\mathbf{Q}}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\operatorname{disc}(K)|} \cdot \|I\|$$

Proof. For any fixed $M > 0$ consider the set

$$B_M = \left\{ (x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbf{R}^r \times \mathbf{C}^s \mid \sum_{i=1}^{r} |x_i| + 2 \sum_{j=1}^{s} |z_j| \leq M \right\}$$

One can show (see for example Lemma 4.22 in Milne, "Algebraic Number Theory") that this is a symmetric, convex and compact subset of volume :

$$\mathrm{vol}(B_M) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \frac{M^n}{n!}$$

This is a strictly increasing function of M that goes to 0 to infinity, so there is exactly one M such that $\mathrm{vol}(B_M) = 2^n \cdot \mathrm{vol}(\Psi(I))$, meaning that

$$M^n = n! \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\operatorname{disc}(K)|} \cdot \|I\|$$

By Theorem 4.2.19 there is $\alpha \in I, \alpha \neq 0$ such that $\Psi(\alpha) \in B_M$. By definition, this means that $\sum_{i=1}^{n} |\sigma_i(\alpha)| \leq M$ and using the inequality between the arithmetic and the geometric mean we see that

$$|N_{K/\mathbf{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \left(\frac{1}{n} \sum_{i=1}^{n} |\sigma_i(\alpha)| \right) \leq \frac{M^n}{n^n}$$

which is what we wanted to prove. □

As a consequence, we can prove Minkowski's bound for the representatives of the class group:

Proof of Theorem 4.2.5. Let K be a number field of degree n. Take any fractional ideal $H \subseteq F$. We want to show that the class of H in the class group is the same as the class of an integral ideal $I \subseteq \mathcal{O}_K$ with

$$\|I\| \leq B_K := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}.$$

Choose a principal fractional ideal $\mathcal{O}_K \cdot \beta$ such that $\mathcal{O}_K \beta \cdot H^{-1} = J \subseteq \mathcal{O}_K$ is an integral ideal. By Proposition 4.2.22, there is an element $\alpha \in J, \alpha \neq 0$ such that $|N_{K/\mathbf{Q}}(\alpha)| \leq B_K \cdot \|J\|$. Now notice that since $\alpha \in J$, it must be that $\alpha \mathcal{O}_K = I \cdot J$ for another ideal $I \subseteq \mathcal{O}_K$ and since the norm is multiplicative, we see that $\|I\| \leq B_K$. Finally, we see that

$$I = (\mathcal{O}_K \alpha) \cdot J^{-1} = (\mathcal{O}_K \alpha)(\mathcal{O}_K \beta^{-1}) H$$

so that I and H have the same class in the class group. □

4.3 Dirichlet's unit theorem

Let K be a number field. We consider the set $\mathcal{O}_K^\times$ of invertible elements in the ring $\mathcal{O}_K$. This is an abelian group with respect to the multiplication. A very deep result is that it is finitely generated and that its torsion-free part has a rank that can be computed precisely:

Theorem 4.3.1 (Dirichlet's Unit Theorem)**.** *Let K be a number field with r real embeddings and $2s$ complex embeddings. Then $\mathcal{O}_K^\times$ is finitely generated and there is an isomorphism of abelian groups*

$$\mathcal{O}_K^\times \cong \mathbf{Z}^{r+s-1} \times \mu_K.$$

where μ_K is the torsion part of $\mathcal{O}_K^\times$. Furthermore, μ_K is a finite cyclic group.

Example 4.3.2 (Quadratic extensions)**.** Let $d \in \mathbf{Z}$ be a square-free integer. Recall that

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

So an element in $\mathcal{O}_K$ is of the form $x + y\sqrt{d}$ or $x + y\left(\frac{1+\sqrt{d}}{2}\right)$, $x, y \in \mathbf{Z}$, and these are units if and only if their norm is ± 1. Computing the norm we get:

$$N_{K/\mathbf{Q}}(x + y\sqrt{d}) = x^2 - y^2 d = \pm 1 \quad (d \equiv 2,3 \pmod 4),$$
$$N_{K/\mathbf{Q}}\left(x + y\tfrac{1+\sqrt{d}}{2}\right) = \left(x + \tfrac{y}{2}\right)^2 - \tfrac{y^2}{4} d = \pm 1 \quad (d \equiv 1 \pmod 4).$$

The torsion part μ_K. Observe that $\alpha \in \mathcal{O}_K^\times$ is torsion of order m if and only if $\alpha^m = 1$ for a certain $m > 0$ and $\alpha^k \neq 1$ for all $0 \leq n < m$. This means precisely that $\alpha = \zeta_m$ is a primitive m-th root of unity. Observe that if $\zeta_m \in K$ is a primitive root of unity of order $m \geq 3$ (otherwise $\zeta_m = \pm 1$) then $\mathbf{Q}(\zeta_m) \subseteq K$, so that

$$\varphi(m) = [\mathbf{Q}(\zeta_m) : \mathbf{Q}] \mid [K : \mathbf{Q}] = 2,$$

hence $\varphi(m) = 1, 2$. Since we are assuming $m \geq 3$, it must be that $\varphi(m) = 2$ and then $K = \mathbf{Q}(\zeta_m)$. Moreover $\varphi(m) = 2$ if and only if $m = 3, 4, 6$, and in those cases we get the fields

$$\mathbf{Q}(\zeta_4) = \mathbf{Q}(i), \qquad \mathbf{Q}(\zeta_6) = \mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3}).$$

Hence we get

$$\mu_{\mathbf{Q}(\sqrt{d})} = \begin{cases} \langle i \rangle & \text{if } d = -1, \\ \langle \zeta_6 \rangle & \text{if } d = -3, \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

The torsion-free part. We divide into two sub-cases:

- $d < 0$: In this case the field $K = \mathbf{Q}(\sqrt{d})$ has two complex embeddings and no real embeddings. Hence, Dirichlet's theorem tells us that

  $$\mathcal{O}_K^\times = \mu_K,$$

  so that the group of units is finite cyclic and we have already given the full classification before. Notice that the characterization of the invertible elements via the norm shows that this group is indeed finite, but it is not clear at all that it is cyclic.

- $d > 0$: In this case the field $K = \mathbf{Q}(\sqrt{d})$ has two real embeddings and no complex embeddings. Furthermore,we have already seen that $\mu_K = \{\pm 1\}$ (which is also clear from the fact that these are the unique roots of unity contained in $\mathbf{R}$). Hence

$$\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbf{Z},$$

In concrete terms, this means that there is a unit $u \in \mathcal{O}_K^*$ such that

$$\mathcal{O}_K^\times = \{\pm u^n \mid n \in \mathbf{Z}\}.$$

This is called a *fundamental unit*. In particular, this tells us that the equations given by the norm have infinitely many integer solutions, which is a priori not clear.

We now start the proof of Dirichlet's theorem, considering the torsion part first:

4.3.1 The torsion part

We start by considering the torsion part

$$\mu_K = (\mathcal{O}_K^\times)_{\text{tor}}$$

Lemma 4.3.3. *The elements in μ_K coincide with the roots of unity that are contained in K. Furthermore, μ_K is a finite set.*

Proof. An element $\alpha \in \mathcal{O}_K^\times$ has order m if and only if it is a primitive m-th root of unity. Conversely if a root of unity is contained in K, then it is also contained in $\mathcal{O}_K$ since it is integral over $\mathbf{Z}$, and then it is invertible in $\mathcal{O}_K$.

For the finiteness: let $\zeta_m \in \mu_K$ be a primitive m-th root of unity. Then $\mathbf{Q}(\zeta_n) \subseteq K$, so that $\varphi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}] \mid [K : \mathbf{Q}]$. Hence K can contain only those primitive m-th roots of unity such that $\varphi(m) \mid [K : \mathbf{Q}]$, and these are finitely many. □

Once we know that this group is finite, it is not hard to show that it is cyclic, because of the following general fact:

Lemma 4.3.4. *Let K be any field and $G \subseteq K^\times$ a finite subgroup. Then G is cyclic.*

Proof. Let $n = |G|$. For any $d \mid n$, let $G_d = \{x \in G \mid x \text{ has order } d\}$. We claim that $|G_d| = 0$ or $|G_d| = \varphi(d)$. Suppose that $G_d \neq \emptyset$, so there is $\alpha \in G_d$. Now we see that

$$G_d \subseteq \{x \in G \mid x^d - 1 = 0\}, \quad (\alpha) \subseteq \{x \in G \mid x^d - 1 = 0\}$$

We observe that the polynomial $x^d - 1$ can have at most d roots in a field. On the other hand (α) has exactly d elements because α has order d, so that

$$(\alpha = \{x \in G \mid x^d - 1 = 0\}.$$

and G_d consists precisely of the elements in $(\alpha) \cong \mathbf{Z}/d\mathbf{Z}$ of order d, and there are $\varphi(d)$ of them. Observe that $G = \bigsqcup_{d|n} G_d$, hence

$$n = |G| = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n.$$

Hence it must be that $|G_d| = \varphi(d)$ for all $d \mid n$. In particular $|G_n| = \varphi(n) \neq 0$, so there is an element of order n, meaning that G is cyclic. □

Corollary 4.3.5. *The group μ_K is finite and cyclic.*

Proof. Follows from Lemma 4.3.3 and Lemma 4.3.4. □

4.3.2 The torsion-free part

To prove Dirichlet's theorem, we use again the canonical embedding (4.2.1):

$$\Psi\colon K \hookrightarrow \mathbf{R}^r \times \mathbf{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \dots, \sigma_{r+s}(\alpha)).$$

Recall that $\sigma_1, \dots, \sigma_r$ are all the real embeddings of K while $\sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma}_{r+1}, \dots, \overline{\sigma}_{r+s}$ are all the complex embeddings of K. Since we care about the units of $\mathcal{O}_K$, we care about the multiplicative structure, but we still want to study it with linear methods. The standard way to transform multiplicative problems into linear problems is to take a logarithm. Thus, we consider the map

$$L\colon \mathcal{O}_K^\times \hookrightarrow \mathbf{R}^r \times \mathbf{R}^s, \qquad \alpha \mapsto \big(\log|\sigma_1(\alpha)|, \dots, \log|\sigma_r(\alpha)|, \log|\sigma_{r+1}(\alpha)|, \dots, \log|\sigma_{r+s}(\alpha)|\big).$$

We make some observations:

Lemma 4.3.6. *If $B \subseteq \mathbf{R}^r \times \mathbf{R}^s$ is a bounded subset, then $L^{-1}(B)$ is finite.*

Proof. It is enough to show that for any $M > 0$ the set

$$S = \{\alpha \in \mathcal{O}_K^\times \mid \log|\sigma_i(\alpha)| \leq M \text{ for all } i\} = \{\alpha \in \mathcal{O}_K^\times \mid |\sigma_i(\alpha)| \leq e^M \text{ for all } i\}$$

is finite. However, if we define the subset

$$C = \{(x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}) \in \mathbf{R}^r \times \mathbf{C}^s \mid |x_i| \leq e^M \text{ for all } i\}$$

we see that this is a bounded subset of $\mathbf{R}^r \times \mathbf{C}^s$ so that $\Psi(\mathcal{O}_K) \cap C$ is finite because $\Psi(\mathcal{O}_K)$ is a lattice. Since Ψ is injective, it follows that $\Psi^{-1}(C)$ is finite, and $S \subseteq \Psi^{-1}(C)$ by definition. □

Lemma 4.3.7. *The map L is a well-defined homomorphism of groups, whose kernel is equal to μ_K. Moreover, the image is a discrete subgroup of the hyperplane*

$$H = \left\{(x_1, \dots, x_r, y_1, \dots, y_s) \in \mathbf{R}^r \times \mathbf{R}^s \;\middle|\; \sum x_i + 2\sum y_j = 0\right\} \cong \mathbf{R}^{r+s-1}.$$

Proof. If $\alpha \in K^\times$ then $\sigma_i(\alpha) \neq 0$ for all i so that $|\sigma_i(\alpha)| > 0$ for all i and the logarithm is well-defined. The fact that the map is an homomorphism of groups means simply that

$$\log|\sigma_i(\alpha\beta)| = \log|\sigma_i(\alpha)\sigma_i(\beta)| = \log|\sigma_i(\alpha)| + \log|\sigma_i(\beta)| \quad \text{for all } i.$$

Finally, the kernel of L is by definition the set of elements of $\mathcal{O}_K^\times$ such that $\log|\sigma_i(\alpha)| = 0$ for all i, meaning that $|\sigma_i(\alpha)| = 1$ for all i. This is of course satisfied by the elements of μ_K, since the σ_i send roots of unity to roots of unity and each root of unity has norm one. For the converse, observe that $\operatorname{Ker} L = L^{-1}(0)$ is finite because of Lemma 4.3.6, hence any element in it must have finite order, so that it must be a root of unity. This shows that $\operatorname{Ker} L \subseteq \mu_K$, hence $\operatorname{Ker} L = \mu_K$.

We see that the image of L is contained in H because if $\alpha \in \mathcal{O}_K^\times$ then

$$1 = |N_{K/\mathbf{Q}}(\alpha)| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \cdot \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)| \cdot |\overline{\sigma}_i(\alpha)| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \cdot \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)|^2$$

and taking the logarithms we see that $L(\alpha) \in H$. Finally, we show that $L(\mathcal{O}_K^\times)$ is a discrete subgroup in H. Take any ball $B \subseteq H$ centered at 0, then $L(\mathcal{O}_K^\times) \cap B$ is a finite subset by Lemma 4.3.6, so that shrinking the ball if necessary we can assume that $L(\mathcal{O}_K^\times) \cap B = \{0\}$. Then if $h \in L(\mathcal{O}_K^\times)$ we see that $B + h$ is a ball centered at h and $L(\mathcal{O}_K^\times) \cap (B + h) = \{h\}$. This shows that $L(\mathcal{O}_K^\times)$ is indeed a discrete subgroup of H. □

Corollary 4.3.8. *$\mathcal{O}_K^\times$ is finitely generated, and $\mathcal{O}_K^\times \cong \mu_K \times L(\mathcal{O}_K^\times)$.*

Proof. Since $L(\mathcal{O}_K^\times)$ is a discrete subgroup of $H \cong \mathbf{R}^{r+s-1}$, it is finitely generated by Lemma 4.2.14. The isomorphism follows from the fact that μ_K is the torsion part of $\mathcal{O}_K^\times$ so that

$$\mathcal{O}_K^\times \cong \mu_K \times (\mathcal{O}_K^\times/\mu_K) \cong \mu_K \times L(\mathcal{O}_K^\times)$$

where the last isomorphism follows from the fact proved in Lemma 4.3.7 that $\mu_K = \operatorname{Ker} L$. □

To conclude, we need to show that $L(\mathcal{O}_K^\times) \subseteq H$ is a discrete subgroup of rank $r+s-1$:

Proof of Dirichlet's Theorem. After Lemma 4.3.7 and Corollary 4.3.8, what we need to show is that $L(\mathcal{O}_K^\times)$ is a lattice in H. We already know that it is discrete, so we can use Lemma 4.2.14 and prove that there is a compact subset $B \subseteq H$ such that $B \to H/L(\mathcal{O}_K^\times)$ is surjective. Consider again the canonical embedding

$$\Psi\colon K \hookrightarrow \mathbf{R}^r \times \mathbf{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \dots, \sigma_{r+s}(\alpha))$$

The space $\mathbf{R}^r \times \mathbf{C}^s$ is a ring with the coordinate-wise multiplication and Ψ is a ring homomorphism. If $\mathbf{x} \in \mathbf{R}^r \times \mathbf{C}^s$ and $S \subseteq \mathbf{R}^r \times \mathbf{C}^s$ we denote

$$\mathbf{x} \cdot S = \{\mathbf{x} \cdot s \,|\, s \in S\}$$

where the multiplication is the coordinate-wise one given by the ring structure. Consider now the norm map

$$N\colon (\mathbf{R}^\times)^r \times (\mathbf{C}^\times)^s \to \mathbf{R}^\times, \quad (x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}) \mapsto \prod_{i=1}^{n} x_i \cdot \prod_{i=r+1}^{r+s} x_i \cdot \bar{x}_i$$

This is a group homomorphism and moreover $N(\Psi(\alpha)) = N_{K/\mathbf{Q}}(\alpha)$ for any $\alpha \in K^\times$. Consider also the subgroups

$$\Psi(\mathcal{O}_K^\times) \subseteq G := \{\mathbf{x} \in \mathbf{R}^r \times \mathbf{C}^s \,|\, |N(\mathbf{x})| = 1\} \subseteq (\mathbf{R}^\times)^r \times (\mathbf{C}^\times)^s$$

Taking coordinate-wise absolute value and logarithm, we get a surjective and continuous map $\Psi\colon G \to H$ that induces a surjective map $G/\Psi(\mathcal{O}_K^\times) \to H/L(\mathcal{O}_K^\times)$. Hence, it is enough to show that there is a compact subset $C \subseteq G$ such that $C \to G/\Psi(\mathcal{O}_K^\times)$ is surjective, because then $B = \Psi(C)$ is a compact subset such that $B \to H/L(\mathcal{O}_K^\times)$ is surjective. We will actually prove that there is a compact subset $T \subseteq \mathbf{R}^r \times \mathbf{C}^s$ such that

$$G \subseteq T \cdot \Psi(\mathcal{O}_K^\times) = \{\mathbf{y} \cdot \Psi(\alpha) \,|\, \alpha \in \mathcal{O}_K^\times\} \tag{4.3.1}$$

and then we can conclude by taking $C = T \cap G$.

To construct a set as in (4.3.1), a relatively straightforward computation shows that that if $\Lambda \subseteq \mathbf{R}^r \times \mathbf{C}^s$ is a lattice, then for any $\mathbf{x} \in (\mathbf{R}^\times)^r \times (\mathbf{C}^\times)^r$ the set $\mathbf{x} \cdot \Lambda$ is again a lattice with volume

$$\operatorname{vol}(\mathbf{x} \cdot \Lambda) = |N(\mathbf{x})| \cdot \operatorname{vol}(\Lambda).$$

We also know that $\Psi(\mathcal{O}_K)$ is a lattice in $\mathbf{R}^r \times \mathbf{C}^s$. Fix now a convex and symmetric compact subset $S \subseteq \mathbf{R}^r \times \mathbf{C}^s$ such that $\operatorname{vol}(S) \geq 2^n \cdot \operatorname{vol}(\Psi(\mathcal{O}_K))$. By Minkowski's Theorem 4.2.19 for

any $\mathbf{x} \in G$ with it holds that $S \cap \mathbf{x} \cdot \Psi(\mathcal{O}_K \setminus \{0\}) \neq \emptyset$. Hence there is an $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $\mathbf{x} \cdot \Psi(\alpha) \in S$,or, equivalently, $\mathbf{x} \in \Psi(\alpha^{-1}) \cdot S$

Claim: There are finitely many $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K \setminus \{0\}$ such that

$$G \subseteq \bigcup_{i=1}^{N} \Psi(\alpha_i^{-1} \cdot \mathcal{O}_K^{\times}) \cdot S = \left(\bigcup_{i=1}^{N} \Psi(\alpha_i^{-1}) \cdot S \right) \cdot \Psi(\mathcal{O}_K^{\times})$$

If we prove the claim, we are done, because the set $T = \cup_{i=1}^{N} \Psi(\alpha_i^{-1}) \cdot S$ is compact and it satisfies the condition in (4.3.1). We prove the claim: consider all possible ideals in $\mathcal{O}_K$ of the form $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ is such that $\mathbf{x} \cdot \Psi(\alpha) \in S$ for a certain $\mathbf{x}$ with $|N(\mathbf{x})| = 1$. For any such ideal, we see that

$$\|\alpha\mathcal{O}_K\| = |N_{K/\mathbf{Q}}(\alpha)| = |N(\Psi(\alpha))| = |N(\mathbf{x} \cdot \Psi(\alpha))| \leq M := \max\{N(\mathbf{y}) \,|\, \mathbf{y} \in S\}$$

and the set of ideals with norm bounded by M is finite by Lemma 4.1.7. Let $\alpha_1\mathcal{O}_K, \ldots, \alpha_N\mathcal{O}_K$ be all these ideals and take any $\mathbf{x} \in \mathbf{R}^r \times \mathbf{C}^s$ with $|N(\mathbf{x})| = 1$. We have seen before that there is $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $\mathbf{x} \cdot \Psi(\alpha) \in S$ and then $\alpha\mathcal{O}_K = \alpha_i\mathcal{O}_K$ for a certain i. This means that $\alpha = \alpha_i \cdot u$ for a certain $u \in \mathcal{O}_K^{\times}$,and then $\mathbf{x} \in \Psi(\alpha_i^{-1} \cdot u^{-1}) \cdot S$. □

Chapter 5

Prime splitting and Galois groups

5.1 Ramification and inertia in Galois extensions

Let K be a number field and assume that $\mathbf{Q} \subseteq K$ is a normal extension of $\mathbf{Q}$. Let also $G = \mathrm{Aut}(K/\mathbf{Q})$ be the Galois group. Observe that if we take $\alpha \in K$ and if

$$m_{\alpha,\mathbf{Q}}(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbf{Q}[x]$$

is the minimal polynomial of α over $\mathbf{Q}$, then $m_{\alpha,\mathbf{Q}}(x)$ is also the minimal polynomial of $\sigma(\alpha)$ for every $\sigma \in G$. In particular, $\alpha \in \mathcal{O}_K$ if and only if $m_{\alpha,\mathbf{Q}}(x)$ has integer coefficients, so that $\sigma(\alpha) \in \mathcal{O}_K$ for all $\sigma \in G$. This shows that every element $\sigma \in G$ induces an automorphism

$$\sigma \colon \mathcal{O}_K \longrightarrow \mathcal{O}_K$$

We want to study how this acts on the prime splitting of an ideal in $\mathcal{O}_K$. We start with a general lemma:

Lemma 5.1.1. *let R be a ring, $I \subseteq R$ an ideal and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq R$ prime ideals such that $I \subsetneq \mathfrak{p}_i$ for all i. Then $I \subsetneq \bigcup_{i=1}^n \mathfrak{p}_i$.*

Proof. We prove the statement by induction on n, the base case $n = 1$ being obvious. Take now $n > 1$. By induction $I \subsetneq \bigcup_{i \neq j} \mathfrak{p}_i$ for any $j = 1, \ldots, n$. Hence for any $j = 1, \ldots, n$ there is $x_j \in I$ such that $x_j \notin \mathfrak{p}_i$ for any $i \neq j$. If $x_j \notin \mathfrak{p}_j$, then $x_j \notin \bigcup_{i=1}^n \mathfrak{p}_j$, and we are done. Asusme that $x_j \in \mathfrak{p}_j$ for $j = 1, \ldots, n$. Take now the element

$$x = \sum_{i=1}^{n} x_1 \ldots \hat{x_i} \ldots x_n \in I$$

. Assume that $x \in \mathfrak{p}_j$. Then it must be that $x_1 \ldots \hat{x_j} \ldots x_n \in \mathfrak{p}_j$ as well, and since $\mathfrak{p}_j$ is prime, we have that $x_i \in \mathfrak{p}_j$ for one $i \neq j$. This is impossible by construction. This proves that $x \notin \bigcup_{i=1}^n \mathfrak{p}_j$ and we are done. □

Now we can prove

Proposition 5.1.2. *Assume that the number field K is a normal extension of $\mathbf{Q}$ and let $p \in \mathbf{Z}$ be a prime,with decomposition*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$$

for pairwise distinct non-zero prime ideals $\mathfrak{p}_i \subseteq \mathcal{O}_K$. Then G acts transitively on the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ and furthermore for the ramification degree and inertia degree it holds that

$$e(\mathfrak{p}_i) = e, \quad f(\mathfrak{p}_i) = f \qquad \text{for all } i$$

for certain e, f such that

$$efr = [K : \mathbf{Q}].$$

Proof. The key part of the statement is the transitivity. Assume by contradiction that the action is not transitive, then $r > 1$ and we can assume that $\mathfrak{p}_1 \neq \sigma(\mathfrak{p}_2)$ for all $\sigma \in G$. Since both ideals $\mathfrak{p}_1, \mathfrak{p}_2$ are maximal, this is the same as $\mathfrak{p}_1 \nsubseteq \sigma(\mathfrak{p}_2)$ for all $\sigma \in G$, and by the prime avoidance lemma 5.1.1, there is $x \in \mathfrak{p}_1$ such that $x \notin \sigma(\mathfrak{p}_2)$ for all $\sigma \in G$ or, equivalently, $\tau(x) \notin \mathfrak{p}_2$ for all $\tau \in G$ (why are the statements equivalent?). Consider now the norm, which we can write as

$$N_{K/\mathbf{Q}}(x) = \prod_{\tau \in G} \tau(x)$$

because the K is a normal extension of $\mathbf{Q}$. Then $N_{K/\mathbf{Q}}(x) \notin \mathfrak{p}_2$ because $\mathfrak{p}_2$ is prime, but $N_{K/\mathbf{Q}}(x) \in \mathfrak{p}_1 \cap \mathbf{Z} = p\mathbf{Z} \subseteq \mathfrak{p}_2$, a contradiction.

Once we know the transitivity, the other statements are easy: if $\sigma \in G$ then $\sigma(p\mathcal{O}_K) = \sigma(p)\mathcal{O}_K = p\mathcal{O}_K$ so that

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} = p\mathcal{O}_K = \sigma(\mathfrak{p}_1)^{e_1} \dots \sigma(\mathfrak{p}_r)^{e_r}$$

So if $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$ we must have that $e_1 = e_i$. Furthermore, in this case we also have an isomorphism of fields

$$\mathbf{F}_{\mathfrak{p}_1} = \mathcal{O}_K/\mathfrak{p}_1 \xrightarrow{\sigma} \mathcal{O}_K/\sigma(\mathfrak{p}_1) = \mathbf{F}_{\mathfrak{p}_i}$$

which fixes $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, so that

$$f_1 = [\mathbf{F}_{\mathfrak{p}_1} : \mathbf{F}_p] = [\mathbf{F}_{\mathfrak{p}_i} : \mathbf{F}_p] f_i$$

By the transitivity it follows that $e_i = e_1 = e, f_1 = f_1 = f$ for all i and then

$$[K : \mathbf{Q}] = \sum_{i=1}^{r} e_1 f_1 = efr$$

□

In the following, we fix a normal finite extension $\mathbf{Q} \subseteq K$ with Galois group $G = \mathrm{Aut}(K/\mathbf{Q})$. We also fix a prime $p \in \mathbf{Z}$ and we let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ be the set of primes in $\mathcal{O}_K$ lying over it and we let e, f be the common ramification and inertia degree, so that $[K : \mathbf{Q}] = efr$.

Definition 5.1.3. In this setting let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime lying over p. The associated *decomposition group* is

$$D_{\mathfrak{p}} = \{\sigma \in G \,|\, \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

Remark 5.1.4. It is easy to show that the decomposition group is indeed a subgroup of G. More precisely it is the stabilizer of the action of G on the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ of primes lying over p. Since the action of G on this set is transitive, we see that

$$|D_{\mathfrak{p}}| = \frac{|G|}{r} = \frac{[K : \mathbf{Q}]}{r} = ef$$

Furthermore, if $\mathfrak{p}'$ is another prime lying over p then we have shown before that there is $\sigma \in G$ such that $\mathfrak{p}' = \sigma(\mathfrak{p})$, and then $D_{\mathfrak{p}} = \sigma D_{\mathfrak{p}'} \sigma^{-1}$. Hence the subgroup $D_{\mathfrak{p}}$ is independent of $\mathfrak{p}$, up to conjugation inside G.

Remark 5.1.5. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime lying over p. Then there is a finite field extension $\mathbf{F}_p \subseteq \mathbf{F}_\mathfrak{p}$ of degree f. We know that this is a normal extension with Galois group cyclic of order f and generated by the Frobenius automorphism Frob. Now notice that if $\sigma \in D_\mathfrak{p}$, then σ induces an isomorphism

$$\overline{\sigma}\colon \mathbf{F}_\mathfrak{p} \longrightarrow \mathbf{F}_\mathfrak{p}, \quad \sigma_{|\mathbf{F}_p} = \mathrm{id}_{\mathbf{F}_p}$$

It is easy to see that the induced map

$$D_\mathfrak{p} \longrightarrow \mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p), \quad \sigma \mapsto \overline{\sigma}$$

is a group homomorphism.

Definition 5.1.6. In the notation of the last remark, the *inertia group* $I_\mathfrak{p}$ at $\mathfrak{p}$ is the kernel of the map

$$D_\mathfrak{p} \longrightarrow \mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p), \quad \sigma \mapsto \overline{\sigma}$$

Proposition 5.1.7. *With the previous notation, the map*

$$D_\mathfrak{p} \longrightarrow \mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p), \quad \sigma \mapsto \overline{\sigma}$$

is surjective and $|I_\mathfrak{p}| = e$.

Proof. Assume that $p\mathcal{O}_K = \mathfrak{p}_1^e \dots \mathfrak{p}_r^e$ and that $\mathfrak{p} = \mathfrak{p}_1$. Since $\mathbf{F}_p \subseteq \mathbf{F}_{\mathfrak{p}_1}$ is a finite extension of a finite field, we know from the Primitive Element Theorem B.2.18 that there is an element $\bar{\alpha} \in \mathbf{F}_{\mathfrak{p}_1}$ such that $\mathbf{F}_{\mathfrak{p}_1} = \mathbf{F}_p(\bar{\alpha})$. By the Chinese Remainder Theorem, we can find $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv \bar{\alpha} \mod \mathfrak{p}_1$ and $\alpha \equiv 0 \mod \mathfrak{p}_i$ for $i \geq 2$. We consider the polynomial:

$$f(x) = \prod_{\sigma \in G} (x - \sigma(\alpha))$$

The coefficients of this polynomial are in $\mathcal{O}_K$ and they are furthermore invariant under G, so that they are in $\mathcal{O}_K \cap \mathbf{Q} = \mathbf{Z}$. Then if we look at the polynomial $f(x)$ modulo $\mathfrak{p}_1$ we see that $f(\bar{x}) \in \mathbf{F}_p[x]$. Since the action of G on the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ is transitive, we can find $\sigma_1, \dots, \sigma_r$ such that $\sigma_i(\mathfrak{p}_i) \subseteq \mathfrak{p}_1$ for all $i = 1, \dots, r$ and moreover $G = \sqcup_{i=1}^r D_{\mathfrak{p}_1} \cdot \sigma_i$. We can assume that $\sigma_1 = \mathrm{id}$. For every $\tau \in D_{\mathfrak{p}_1}$ we see that if $i \geq 2$ then $\tau\sigma_i(\alpha) \in \tau(\sigma_i(\mathfrak{p}_i)) = \tau(\mathfrak{p}_1) = \mathfrak{p}_1$. Hence if we look at $f(x)$ modulo $\mathfrak{p}_1$ we get

$$\overline{f(x)} = \prod_{\tau \in D_\mathfrak{p}} (x - \overline{\tau(\alpha)}) \cdot \prod_{i=2}^{r} \prod_{\tau \in D_{\mathfrak{p}_1}} (x - \overline{\tau\sigma_i(\alpha)}) = \prod_{\tau \in D_\mathfrak{p}} (x - \overline{\tau(\alpha)}) \cdot x^{|G| - |D_{\mathfrak{p}_1}|}$$

Since $\overline{f}(\overline{\alpha}) = 0$, the minimal polynomial of $\overline{\alpha}$ must divide $\overline{f}(x)$ so that the minimal polynomial must divide the polynomial

$$\bar{g}(x) = \prod_{\tau \in D_\mathfrak{p}} (x - \overline{\tau(\alpha)})$$

Let now $\eta \in \mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$: this is defined by sending $\overline{\alpha}$ to one of the roots of its minimal polynomial over $\mathbf{F}_p$.This root must be of the form $\overline{\tau(\alpha)}$ for a certain $\tau \in D_{\mathfrak{p}_1}$ and this means that η is the image of τ according to our map. □

5.1.1 The Frobenius element

Assume now that we have a Galois extension $\mathbf{Q} \subseteq K$ and and that a prime $p \in \mathbf{Z}$ *does not ramify* in K so that

$$p\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

for pairwise distinct non-zero prime ideals in $\mathcal{O}_K$, and the common ramification degree is $e = 1$. Then Proposition 5.1.7 shows that for every prime $\mathfrak{p} \subseteq \mathcal{O}_K$ lying over p, the restriction map

$$D_\mathfrak{p} \longrightarrow \mathrm{Aut}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$$

is an isomorphism. We know that the group on the right is cyclic generated by the Frobenius automorphism. Hence there is a unique *Frobenius element* $\mathrm{Frob}_\mathfrak{p} \in D_\mathfrak{p} \subseteq \mathrm{Aut}(K/\mathbf{Q})$ which is a generator of $D_\mathfrak{p}$, it has order f and is the unique element in $\mathrm{Aut}(K/\mathbf{Q})$ with the properties that:

$$\mathrm{Frob}_\mathfrak{p}(\mathfrak{p}) = \mathfrak{p}, \quad \mathrm{Frob}_\mathfrak{p}(x) \equiv x^p \mod \mathfrak{p} \qquad \text{for all } x \in \mathcal{O}_K$$

Let now $\mathbf{Q} \subseteq K' \subseteq K$ be an intermediate field extension and assume that the extension $\mathbf{Q} \subseteq K'$ is also Galois. Let $\mathfrak{p}' = \mathfrak{p} \cap \mathcal{O}_{K'}$. This is a prime in $\mathcal{O}_{K'}$ lying over p and moreover p is not ramified in $\mathcal{O}_{K'}$, otherwise it would also be ramified in $\mathcal{O}_K$ (why?). Hence we can also define the Frobenius element $\mathrm{Frob}_{\mathfrak{p}'} \in \mathrm{Aut}(K/\mathbf{Q})$. Notice that since the extension $\mathbf{Q} \subseteq K'$ is normal, we have a restriction map

$$\mathrm{Aut}(K/\mathbf{Q}) \longrightarrow \mathrm{Aut}(K'/\mathbf{Q}), \quad \sigma \mapsto \sigma_{|K'}.$$

Recall also that p *completely ramifies* in K' if

$$p\mathcal{O}_{K'} = \mathfrak{p}'_1 \dots \mathfrak{p}'_{n'}$$

where $\mathfrak{p}'_i \subseteq \mathcal{O}_{K'}$ are pairwise distinct prime ideals and $n' = [K' : \mathbf{Q}]$. Equivalently, this means that the common ramification and inertia degree of the $\mathfrak{p}'_i$ are $e' = f' = 1$.

Lemma 5.1.8. *In the previous setting it holds that*

$$\mathrm{Frob}_{\mathfrak{p}_{|K'}} = \mathrm{Frob}_{\mathfrak{p}'}\,.$$

In particular, the prime p splits completely in K' if and only if $\mathrm{Frob}_{\mathfrak{p}_{|K'}} = \mathrm{id}_{K'}$.

Proof. We know that $\mathrm{Frob}_\mathfrak{p}(\mathfrak{p} \cap \mathcal{O}_K) = \mathfrak{p} \cap \mathcal{O}_K$ since $\mathrm{Frob}_\mathfrak{p}(\mathfrak{p}) = \mathfrak{p}$. It is now straightforward to check that $\mathrm{Frob}_\mathfrak{p}(x) \equiv x^p \pmod{\mathfrak{p}'}$ for all $x \in \mathcal{O}_{K'}$ and this shows that $\mathrm{Frob}_{\mathfrak{p}_{|K'}} = \mathrm{Frob}_{\mathfrak{p}'}$. For the last statement, observe that $\mathrm{Frob}_{\mathfrak{p}'}$ is a generator of $D_{\mathfrak{p}'}$, that has order $e'f'$, hence p is completely split in K' if and only if $\mathrm{Frob}_{\mathfrak{p}'} = \mathrm{id}_{K'}$. □

In particular, recall that a prime

5.2 Cyclotomic fields

We now want to discuss again cyclotomic fields: let $n \in \mathbf{N}$ and $\zeta_n = e^{\frac{2\pi i}{n}}$ be a primitive root of unity. The corresponding cyclotomic field is $\mathbf{Q}(\zeta_n)$. We have already defined the cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{1 \le i \le n-1 \\ \mathrm{GCD}(i,n)=1}} (x - \zeta_n^i)$$

so that this is a polynomial of degree $\phi(n)$ and

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

We have also already seen that any embedding $\sigma\colon \mathbf{Q}(\zeta_n) \hookrightarrow \mathbf{C}$ must send $\zeta_n \mapsto \zeta_n^i$ for i coprime to n. Hence $m_{\zeta_n,\mathbf{Q}}(x)$ divides $\Phi_n(x)$ in $\mathbf{C}[x]$, the extension $\mathbf{Q} \subseteq \mathbf{Q}(\zeta_n)$ is normal, and we have an injective map

$$\mathrm{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^\times, (\zeta_n \mapsto \zeta_n^i) \mapsto [i]$$

In $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] \leq \phi(n)$.

Lemma 5.2.1. *Let $p \in \mathbf{Z}$ be a prime number that does not divide n. Then p does not ramify in $\mathbf{Q}(\zeta_n)$.*

Proof. We compute $\operatorname{disc} \mathbf{Z}[\zeta_n]$. Let us write $x^n - 1 = m_{\zeta_n,\mathbf{Q}}(x) \cdot f(x)$ for $f(x) \in \mathbf{Z}[x]$. Then if we derive and we evaluate in ζ_n we get

$$n\zeta_n^{-1} = n\zeta_n^{n-1} = m'_{\zeta_n,\mathbf{Q}}(\zeta_n) f(\zeta_n)$$

and taking the norm we get

$$n^{[\mathbf{Q}(\zeta_n):\mathbf{Q}]} \cdot N_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}(\zeta_n^{-1}) = N_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}(m'_{\zeta_n,\mathbf{Q}}(\zeta_n)) \cdot N_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}(f(\zeta_n))$$

and since ζ_n is invertible in $\mathcal{O}_{\mathbf{Q}(\zeta_n)}$ we see that if p does not divide n, then it does not divide$N_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}(m'_{\zeta_n,\mathbf{Q}}(\zeta_n))$ either, and then this means that p does not divide $\operatorname{disc} \mathbf{Z}[\zeta_n]$. Now we know that

$$\operatorname{disc} \mathbf{Z}[\zeta_n] = |\mathcal{O}_{\mathbf{Q}(\zeta_n)}/\mathbf{Z}[\zeta_n]|^2 \cdot \operatorname{disc} \mathcal{O}_{\mathbf{Q}(\zeta_n)}$$

hence p does not divide $\operatorname{disc} \mathcal{O}_{\mathbf{Q}(\zeta_n)}$ meaning that it does not ramify. □

As a consequence we get:

Theorem 5.2.2. *The extension $\mathbf{Q} \subseteq \mathbf{Q}(\zeta_n)$ is normal of degree $\phi(n)$ and Galois group $(\mathbf{Z}/n\mathbf{Z})^\times$. The cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbf{Q}$: in particular it has integer coefficients and it is irreducible.*

Proof. If we show that the map

$$\mathrm{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^\times, (\zeta_n \mapsto \zeta_n^i) \mapsto [i]$$

is surjective, then it is also an isomorphism and we are done (why?). Notice that it is enough to show that the image contains all classes of primes $1 \leq p \leq n-1$ coprime to n, because they generate $(\mathbf{Z}/n\mathbf{Z})^\times$ as a group. Let p be such a prime: then it does not ramify in $\mathbf{Q}(\zeta_n)$ and if we denote by $\mathfrak{p}$ a prime lying over it in $\mathcal{O}_{\mathbf{Q}(\zeta_n)}$ we have a well-defined Frobenius element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ such that $\mathrm{Frob}_\mathfrak{p}(\mathfrak{p}) = \mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{p}(x) \equiv x^p \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_{\mathbf{Q}(\zeta_n)}$. This Frobenius element must have the form $\mathrm{Frob}_\mathfrak{p}(\zeta_n) = \zeta_n^i$ for a certain $1 \leq i \leq n-1$ coprime with n, so that $\zeta_n^i - \zeta_n^p \in \mathfrak{p}$. If we show that $\zeta_n^i - \zeta_n^p \notin \mathfrak{p}$ for all $0 \leq i \leq n-1, i \neq p$, we are done. If we take the derivative of the polynomial $x^n - 1$ and we evaluate it at ζ_n^p we get

$$n\zeta_n^{p(n-1)} = \prod_{0 \leq i \leq n-1 // i \neq p} (\zeta_n^p - \zeta_n^i)$$

so it is enough to show that $n\zeta_n^{p(n-1)} \notin \mathfrak{p}$, and since ζ_n is invertible, this is equivalent to $n \notin \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, which is true by hypothesis on p. □

In the previous proof, we computed explicitly the Frobenius element for a prime number p:

Proposition 5.2.3. *Let $n \in \mathbf{N}$, let $p \in \mathbf{Z}$ be a prime $p \nmid n$ and let $\mathfrak{p} \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_n)}$ be a prime lying over p. Then* $\mathrm{Frob}_{\mathfrak{p}}(\zeta_n) = \zeta_n^p$.

One can also compute explicitly the ring of integers of the cyclotomic field, but we will first need a preliminary result. If K and L are two number fields, then the field LK is the smallest field that contains both of them: for example if $K = \mathbf{Q}(\alpha), L = \mathbf{Q}(\beta)$, then $LK = \mathbf{Q}(\alpha, \beta)$. In this case we define

$$\mathcal{O}_K\mathcal{O}_L := \left\{ \sum_{i=1}^{n} \alpha_i\beta_i \,|\, \alpha_i \in \mathcal{O}_K, \beta_i \in \mathcal{O}_L, n \in \mathbf{N} \right\}$$

For example, if $\mathcal{O}_K = \mathbf{Z}[\alpha], \mathcal{O}_L = \mathbf{Z}[\beta]$ then $\mathcal{O}_K\mathcal{O}_L = \mathbf{Z}[\alpha, \beta]$.

Proposition 5.2.4. *Let K and L be two number fields such that*

$$[KL : \mathbf{Q}] = [K : \mathbf{Q}] \cdot [L : \mathbf{Q}]$$

If $d = \mathrm{GCD}(\mathrm{disc}(K), \mathrm{disc}(L))$, then it holds that $d\mathcal{O}_{KL} \subseteq \mathcal{O}_K\mathcal{O}_L$.

Proof. In the exercises. □

With this we can prove:

Theorem 5.2.5. *It holds that $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$.*

Proof. First we assume that $n = p^k$ is the power of a prime p. The minimal polynomial of ζ_{p^k} is

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{\prod_{d|p^k, d\neq p^k} \Phi_d(x)} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \sum_{i=0}^{p-1} x^{ip^{k-1}}.$$

Observe that if we look at this modulo p we get, using the Frobenius that

$$\Phi_{p^k}(x) \equiv \frac{(x-1)^{p^k}}{(x-1)^{p^{k-1}}} \equiv (x-1)^{p^{k-1}(p-1)} \pmod{p}$$

Consider then the element $\omega_{p^k} = 1 - \zeta_{p^k}$. The minimal polynomial of ω_{p^k} is $\Phi_{p^k}(1-x)$ and then the previous computation shows that

$$\Phi_{p^k}(1-x) \equiv x^{p^{k-1}(p-1)} \pmod{p}$$

However, the constant term of $\Phi_{p^k}(1-x)$ is $\Phi_{p^k}(1) = p$, so it is not divisible by p^2. This shows that the minimal polynomial of ω_{p^k} is Eisenstein with respect to p. On the other hand, we know that $|\operatorname{disc} \mathbf{Z}[\omega_p]| = |\operatorname{disc} \mathbf{Z}[\zeta p^k]|$ is a power of p, hence $|\mathcal{O}_{\mathbf{Q}(\zeta_{p^k})}/\mathbf{Z}[\omega_{p^k}]|$ is also a power of p, and then it follows from Proposition 2.3.28 that it must be $|\mathcal{O}_{\mathbf{Q}(\zeta_{p^k})}/\mathbf{Z}[\omega_{p^k}]| = 1$. This shows that $\mathcal{O}_{\mathbf{Q}(\zeta_{p^k})} = \mathbf{Z}[\zeta_{p^k}]$.

For the general case, let $n, m \in \mathbf{N}$ be coprime integers and assume that $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n], \mathcal{O}_{\mathbf{Q}(\zeta_m)} = \mathbf{Z}[\zeta_m]$: then we observe that

$$\mathbf{Q}(\zeta_n, \zeta_m) = \mathbf{Q}(\zeta_{nm}), \quad \mathbf{Z}[\zeta_n, \zeta_m] = \mathbf{Z}[\zeta_{nm}]$$

Indeed $\zeta_n = \zeta_{nm}^m, \zeta_m = \zeta_{nm}^m$ and if we choose $h, k \in \mathbf{Z}$ such that $hn + km = 1$, then

$$\zeta_n^k \zeta_m^h = \zeta_{nm}^{mk+hn} = \zeta_{nm}$$

We also know that $[\mathbf{Q}(\zeta_{nm}) : \mathbf{Q}] = \phi(nm) = \phi(n)\phi(m) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}][\mathbf{Q}(\zeta_m) : \mathbf{Q}]$. And a previous Lemma shows that any prime dividing both discriminants of $\mathbf{Q}(\zeta_n)$ and $\mathbf{Q}(\zeta_m)$ must divide both n and m, so the two discriminants are coprime. Then we can use the previous and get that $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathcal{O}_{\mathbf{Q}(\zeta_n)}\mathcal{O}_{\mathbf{Q}(\zeta_m)} = \mathbf{Z}[\zeta_{nm}]$ by what we have done before. Since we can factor any number as a product of pairwise coprime prime power, we are done. □

5.2.1 Quadratic reciprocity

As an application, we want to prove the classical quadratic reciprocity law. If $p \in \mathbf{Z}$ is a prime number and if $d \in \mathbf{Z}$ is any number, we say that *d is a square modulo p* if the equation

$$x^2 \equiv d \pmod{p} \quad \text{has a solution}$$

Equivalently, this means that the polynomial $x^2 - d$ has a root in $\mathbf{F}_p$. We also say that d is a non-zero square modulo p if d is a square modulo p and $p \not\equiv 0 \pmod{p}$. Being a square modulo p is encoded by the Legendre symbol:

Definition 5.2.6 (Legendre symbol)**.** If $p \in \mathbf{Z}$ is a prime number and $d \in \mathbf{Z}$ is any number, we define the *Legendre symbol*

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

Note that that the "L" at the bottom is not standard, but we use this notation in order to not get confused with fractions.

Example 5.2.7. Any number is a square modulo 2, hence

$$\left(\frac{d}{2}\right)_L = \begin{cases} 1 & \text{if } d \text{ odd} \\ 0 & \text{if } d \text{ even} \end{cases},$$

Instead we see that

$$\left(\frac{d}{5}\right)_L = \begin{cases} 1 & \text{if } d \equiv 1, 4 \pmod{5} \\ 0 & \text{if } d \equiv 0 \pmod{5} \\ -1 & \text{if } d \equiv 2, 3 \pmod{5} \end{cases}$$

Of course 0 is always a square modulo p, hence the question is only interesting for numbers that are non-zero modulo p. Furthermore, we have seen that all numbers are squares modulo 2, so the interesting case is when p is an odd prime.

Lemma 5.2.8. *Let p be an odd prime number. Then $\left(\frac{d}{p}\right)_L$ is the unique element in $\{-1, 0, 1\}$ such that*

$$\left(\frac{d}{p}\right)_L \equiv d^{\frac{p-1}{2}} \pmod{p}.$$

Furthermore, the map

$$\left(\frac{\cdot}{p}\right)_L : \mathbf{F}_p^\times \longrightarrow \{\pm 1\}, \quad d \mapsto \left(\frac{d}{p}\right)_L$$

is a homomorphism of multiplicative groups.

Proof. If $d \equiv 0 \pmod{p}$, then $\left(\frac{d}{p}\right)_L \equiv 0 \equiv d^{\frac{p-1}{2}}$ modulo p and 0 is the only element in $\{-1, 0, 1\}$ with this property. Let us now consider the case $d \not\equiv 0 \pmod{p}$. We know that the multiplicative group $\mathbf{F}_p^\times$ is cyclic generated by an element α of order $p-1$, so that the set of squares in $\mathbf{F}_p^\times$ is the subgroup generated by α^2, of order $\frac{p-1}{2}$. This shows that

$$\left(\frac{\alpha^m}{p}\right)_L = (-1)^m = \begin{cases} 1, & \text{if } m \text{ is even} \\ -1, & \text{if } m \text{ is odd} \end{cases} \tag{5.2.1}$$

On the other hand, we know that the element $\alpha^{\frac{p-1}{2}}$ has order 2, so it must be $\alpha^{\frac{p-1}{2}} \equiv -1$ modulo p (why?). Hence

$$(\alpha^m)^{\frac{p-1}{2}} = (\alpha^{\frac{p-1}{2}})^m = (-1)^m \pmod{p}$$

and moreover, $(-1)^m = (-1)^n$ modulo p if and only if $n \cong m$ modulo 2. This shows the first statement. The second statement follows from the formula (5.2.1), because it tells us that the map that we are looking at is the composition

$$\mathbf{F}_p^\times \longrightarrow \mathbf{Z}/(p-1)\mathbf{Z} \longrightarrow \{\pm 1\}$$

where the first one is the isomorphism that sends α to $[1]$ and the second one is the homomorphism that sends $[m]$ to $(-1)^m$. Since a composition of homomorphisms is an homomorphism, we are done. □

Let now $d \in \mathbf{Z}$ be an arbitrary integer, that we can write as a product

$$d = p_1^{e_1} \dots p_r^{e_r}$$

where the p_i are pairwise coprime prime numbers. Then Lemma 5.2.8 shows that

$$\left(\frac{d}{p}\right)_L = \left(\frac{p_1}{p}\right)_L^{e_1} \cdot \dots \cdot \left(\frac{p_r}{p}\right)_L^{e_r}$$

so if we can compute the Legendre symbol for prime numbers, we can compute it in general. Furthermore, any number is a square modulo 2 so we can restrict to the case where the prime at the bottom of the Legendre symbol is an odd prime. The most important result about the Legendre symbol is a famous classical result in number theory

Theorem 5.2.9 (Quadratic reciprocity)**.** *For any two odd and coprime prime numbers p, q it holds that*

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

Furthermore, if p is an odd prime number it holds that

$$\left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}}, \ \left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}}.$$

Example 5.2.10. Let us try to determine whether 105 is a square modulo 1009 (this is a prime number). We compute

$$\left(\frac{105}{1009}\right)_L = \left(\frac{3 \cdot 5 \cdot 7}{1009}\right)_L = \left(\frac{3}{1009}\right)_L \left(\frac{5}{1009}\right)_L \left(\frac{7}{1009}\right)_L = \left(\frac{1009}{3}\right)_L \left(\frac{1009}{5}\right)_L \left(\frac{1009}{7}\right)_L = \left(\frac{1}{3}\right)_L \left(\frac{4}{5}\right)_L \left(\frac{1}{7}\right)_L$$

5.2.2 Proof of Quadratic Reciprocity

We need some preparation:

Remark 5.2.11. Let $p \in \mathbf{Z}$ be an odd prime and $d \in \mathbf{Z}$ a square-free integer. Consider $\mathbf{Q}(\sqrt{d})$: we say that the prime p splits completely in $\mathbf{Q}(\sqrt{d})$ if $p\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq \mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ distinct prime ideals. We say instead that p is completely ramified in $\mathbf{Q}(\sqrt{d})$ if $p\mathcal{O}_K = \mathfrak{p}^2$ for a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{\mathbf{Q}(\sqrt{d})}$. Finally, we say that p is prime in $\mathbf{Q}(\sqrt{d})$ if $p\mathcal{O}_K$ is a prime ideal. With this notation, it holds that

$$\left(\frac{d}{p}\right)_L = \begin{cases} 1, & \text{if } p \text{ splits completely in } \mathbf{Q}(\sqrt{d}), \\ 0, & \text{if } p \text{ is completely ramified in } \mathbf{Q}(\sqrt{d}), \\ -1, & \text{if } p \text{ is prime in } \mathbf{Q}(\sqrt{d}). \end{cases}$$

In particular, p is unramified in $\mathbf{Q}(\sqrt{d})$ if and only if $p \nmid d$.

Proof. Indeed, we know that $|\mathcal{O}_{\mathbf{Q}(\sqrt{d})}/\mathbf{Z}[\sqrt{d}]| = 1$ if $d \equiv 2, 3 \pmod 4$ and $|\mathcal{O}_{\mathbf{Q}(\sqrt{d})}/\mathbf{Z}[\sqrt{d}]| = 2$ if $d \equiv 1 \pmod 4$ and in both cases $p \nmid |\mathcal{O}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}|$ because p is odd. Then we can use the Dedekind-Kummer theorem and observe that

$$\begin{aligned} p \text{ splits completely in } \mathbf{Q}(\sqrt{d}) &\iff x^2 - d \text{ has a non-zero root in } \mathbf{F}_p \\ p \text{ is completely ramified in } \mathbf{Q}(\sqrt{d}) &\iff x^2 - d \text{ has a zero root in } \mathbf{F}_p \\ p \text{ is prime in } \mathbf{Q}(\sqrt{d}) &\iff x^2 - d \text{ does not have a root in } \mathbf{F}_p \end{aligned}$$

This proves the statement about the Legendre symbol. The statement about the ramification follows from this or from the fact that $\operatorname{disc} \mathbf{Q}(\sqrt{d}) \mid 4d$. □

Lemma 5.2.12. *Let $p \in \mathbf{Z}$ be an odd prime number and define $p^* = (-1)^{\frac{p-1}{2}} \cdot p$. Then $\mathbf{Q}(\sqrt{p^*}) \subseteq \mathbf{Q}(\zeta_p)$ is the unique quadratic extension of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta_p)$. Furthermore, if $d \in \mathbf{F}_p^\times$, then*

$$\left(\frac{d}{p}\right)_L = 1 \iff \sigma_d \in \operatorname{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{p^*}))$$

Proof. We know that $\mathbf{Q}(\zeta_p)$ is a normal extension of $\mathbf{Q}$ with Galois group

$$\operatorname{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = \{\sigma_d \mid d \in \mathbf{F}_p^\times\}, \quad \sigma_d(\zeta_p) = \zeta_p^d$$

This group is isomorphic to $\mathbf{F}_p^\times \cong \mathbf{Z}/(p-1)\mathbf{Z}$. So it has a unique subgroup of index 2, which is precisely the set $\{\sigma^2 \mid \sigma \in \operatorname{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$. Hence $\mathbf{Q}(\zeta_p)$ contains a unique quadratic extension and if we show that $\sqrt{p^*} \in \mathbf{Q}(\zeta_p)$,then this must be the extension. Observe that if we consider the matrix $S = (\sigma_i(\zeta_p^{j-1}))$ for $1 \leq i, j \leq p-1$, we have

$$\operatorname{disc} \mathbf{Q}(\zeta_p) = \operatorname{disc} \mathbf{Z}[\zeta_p] = \det(S)^2$$

and since all entries of S are still in $\mathbf{Q}(\zeta_p)$ we get that $\det(S) = \sqrt{\operatorname{disc} \mathbf{Q}(\zeta_p)} \in \mathbf{Q}(\zeta_p)$. On the other hand, we know that

$$\operatorname{disc} \mathbf{Q}(\zeta_p) = (-1)^{\frac{p-1}{2}} p^{p-2} = p^{p-3} \cdot (-1)^{\frac{p-1}{2}} p = p^{p-3} \cdot p^*$$

and since $p-3$ is even we conclude that $\sqrt{p^*} \in \mathbf{Q}(\zeta_p)$. For the final statement , observe that by construction $\mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{p^*})) = \{\sigma^2 \,|\, \sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q})\}$, hence

$$\left(\frac{d}{p}\right)_L = 1 \iff \sigma_d = \sigma^2 \text{ for one } \sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \iff \sigma_d \in \mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{p^*})) \qquad \square$$

Lemma 5.2.13. *It holds that $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$, so that $\mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\zeta_8)$ and moreover*

$$\mathrm{Aut}(\mathbf{Q}(\sqrt{\zeta_8})/\mathbf{Q}(\sqrt{2})) = \{\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta_8)/\mathbf{Q}) \,|\, \sigma(\zeta_8) = \zeta_8^{\pm 1}\}$$

Proof. We see that $\zeta_8^2 = \zeta_4 = i$ so that

$$(\zeta_8 + \zeta_8^{-1})^2 = \zeta_8^2 + \zeta_8^{-2} + 2 = i - i + 2 = 2.$$

We know that $\mathbf{Q}(\zeta_8)$ is a normal extension of $\mathbf{Q}$ with Galois group

$$\mathrm{Aut}(\mathbf{Q}(\zeta_8)/\mathbf{Q}) = \{\sigma_d \,|\, d \in (\mathbf{Z}/8\mathbf{Z})^\times\} = \{\sigma_{\pm 1}, \sigma_{\pm 3}\}, \quad \sigma_d(\zeta_p) = \zeta_p^d$$

We know that $\mathrm{Aut}(\mathbf{Q}(\sqrt{\zeta_8})/\mathbf{Q}(\sqrt{2}))$ has index 2 and it clearly contains $\{\sigma_{\pm 1}\}$, so it must be equal to it. $\square$

Now we can give the proof

Proof of quadratic reciprocity. Let us consider the two latter statements first. Lemma 5.2.8 shows immediately that

$$\left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}}$$

Now let's consider the first equality (which is the main statement of quadratic reciprocity): let $p^* = (-1)^{\frac{p-1}{2}} p$. Then

$$\left(\frac{p^*}{q}\right)_L = \left(\frac{-1}{q}\right)_L^{\frac{p-1}{2}} \left(\frac{p}{q}\right)_L = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)_L$$

so what we need to prove is that

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

Consider the number fields $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{p^*}) \subseteq \mathbf{Q}(\zeta_p)$. We know that q does not ramify in $\mathbf{Q}(\zeta_p)$, so let $\mathfrak{q} \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ be a prime ideal lying over q. Proposition 5.2.3 shows that $\mathrm{Frob}_\mathfrak{q}(\zeta_p) = \zeta_p^q$, hence

$$\begin{aligned}
\left(\frac{p^*}{q}\right)_L = 1 &\iff q \text{ splits completely in } \mathbf{Q}(\sqrt{p^*}) && \text{because of Remark 5.2.11} \\
&\iff \mathrm{Frob}_\mathfrak{q} \in \mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{p^*})) && \text{because of Lemma 5.1.8} \\
&\iff \sigma_q \in \mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{p^*})) && \text{because } \mathrm{Frob}_\mathfrak{p}(\zeta_p) = \zeta_p^q \\
&\iff \left(\frac{q}{p}\right)_L = 1 && \text{because of Lemma 5.2.12}
\end{aligned}$$

For the last remaining equality we do a similar reasoning but we consider the extension of fields $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\zeta_8)$. If q is an odd prime, we know that q does not ramify in $\mathbf{Q}(\zeta_8)$, and if $\mathfrak{q} \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_8)}$ is a prime lying over q we know that $\mathrm{Frob}_{\mathfrak{q}}(\zeta_8) = \zeta_8^q$. Then we have

$$\begin{aligned}
\left(\frac{2}{q}\right)_L = 1 &\iff q \text{ splits completely in } \mathbf{Q}(\sqrt{2}) && \text{because of Remark 5.2.11}\\
&\iff \mathrm{Frob}_{\mathfrak{q}} \in \mathrm{Aut}(\mathbf{Q}(\zeta_8)/\mathbf{Q}(2)) && \text{because of Lemma 5.1.8}\\
&\iff \sigma_q \in \mathrm{Aut}(\mathbf{Q}(\zeta_8)/\mathbf{Q}(\sqrt{2})) && \text{because } \mathrm{Frob}_{\mathfrak{q}}(\zeta_8) = \zeta_8^q\\
&\iff q \equiv \pm 1 \pmod 8 && \text{because of Lemma 5.2.13}\\
&\iff (-1)^{\frac{q^2-1}{8}} = 1. &&
\end{aligned}$$

□

5.3 Fermat's last theorem for regular primes

The Fermat equation is

$$x^n + y^n = z^n$$

It was famously claimed by Fermat that this equation has no integer solutions for $n \geq 3$. This was only proven by Wiles hundreds of years later. Here we want to discuss a proof of this theorem, due to Kummer, for the so-called *regular primes*.

First observe that if x, y, z is an integer solution to Fermat's equation, and if p is a common prime factor of two of them, then p is also a factor of the third one. By factoring out such common factors repeatedly, we can assume that x, y, z are pairwise coprime. Let's first discuss the case $n = 2$, when the Fermat equation actually admits a solution.

Proposition 5.3.1. *All integer solutions to Fermat's quadratic equation*

$$x^2 + y^2 = z^2$$

with x, y, z pairwise coprime have (up to exchanging x, y) the form

$$x = \pm(a^2 - b^2), \quad y = \pm 2ab, \quad z = \pm(a^2 + b^2)$$

for certain $a, b \in \mathbf{Z}$ pairwise coprime.

Proof. It is straightforward to check that the x, y, z above give a solution to Fermat's quadratic equation. Conversely assume that x, y, z are pairwise coprime and give a solution. Looking at the equation modulo 4 we see that z must be odd. Now we write the equation as

$$z^2 = (x + iy)(x - iy) \quad \text{in } \mathbf{Z}[i]$$

Recall that the ring $\mathbf{Z}[i]$ is a PID (even Euclidean). We show that $x + iy, x - iy$ are coprime. An prime factor $\alpha \in \mathbf{Z}[i]$ of both $x + iy, x - iy$ would also be a prime factor of z and of a $2x$. However, since we know that z is an odd integer, we know that $2x$ and z are coprime in $\mathbf{Z}$, so that the ideal that they generate is the whole ring, and then they are also coprime in $\mathbf{Z}[i]$. This shows that $x + iy, x - iy, z$ are pairwise coprime in $\mathbf{Z}[i]$, and writing them as a product of prime factors, we see that we can assume that there are $u \in \mathbf{Z}[i]^\times$ and $\alpha \in \mathbf{Z}[i]$ such that

$$x + iy = u \cdot \alpha^2, \quad x - iy = \sigma(u) \cdot \sigma(\alpha)^2, \quad z = \pm N(\alpha)$$

where $\sigma\colon \mathbf{Q}(i) \to \mathbf{Q}(i)$ is the automorphism given by the complex conjugation. If we write $\alpha = a + ib$ for some$a, b \in \mathbf{Z}$, this means

$$x + iy = u \cdot (a^2 - b^2 + 2ab \cdot i), z = \pm(a^2 + b^2)$$

and since $u \in \{\pm 1, \pm i\}$ this gives exactly the result that we were looking for the form of x, y, z. Notice also that if a, b have a common factor, then x, y, z would also have one. □

Now we turn to the not-existence of solutions. Notice that if the Fermat's equation has a solution for a certain n, then it also has a solution for all divisors $d \mid n$: indeed, we can write $n = dh$ for $h \in \mathbf{N}$ and then

$$(x^h)^d + (y^h)^d = x^{hd} + y^{hd} = z^{hd} = (z^h)^d$$

Hence, proving that Fermat's equation does not have an integer solution for $n \geq 3$ is equivalent to proving it for for $n = 4$ and for $n = p$ an odd prime number.

Proposition 5.3.2. *The Fermat equation for $n = 4$ has no integer solutions.*

Proof. We will actually show that the equation

$$x^4 + y^4 = w^2$$

has no solution where x, y, w are positive integers. We will use the technique of Fermat's descent: assuming that there is such a solution, we will find another such solution x', y', w' with $w' < w$. We could then keep going and find an infinite strictly decreasing sequence of positive integers, which is impossible.

Let us construct the solution x', y', z'. Assume we have such a solution x^2, y^2, w to Fermat's quartic equation with pairwise coprime elements. In particular one of x, y must be odd and the other one even. We can assume that x is odd and we can write thanks to Proposition 5.3.1

$$x^2 = \pm(a^2 - b^2), \quad y^2 = \pm 2ab, \quad w = \pm(a^2 + b^2)$$

for $a, b \in \mathbf{Z}$ pairwise coprime. Since $x^2 > 0, y^2 > 0$ we can assume that a, b are both positive. Furthermore, since x is odd, one a, b must be odd and the other even. We can assume that a is odd and b is even. Then

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad w = a^2 + b^2$$

Now we apply again Proposition 5.3.1 to $a^2 = x^2 + b^2$ and reasoning as before we see that there must be $c, d \in \mathbf{Z}$ pairwise coprime, positive and not both odd such that such that

$$x = c^2 - d^2, \quad b = 2cd, \quad a = c^2 + d^2$$

If we write $y^2 = 2ab = 4acd$,since a, c, d are pairwise coprime, we see that they must all be squares $a = (w')^2, c = (x')^2, d = (y')^2$ for positive integers x', y', z'. Then

$$(x')^4 + (y')^4 = (w')^2$$

Hence we have found another solution of our equation into positive integers and since $w = a^2 + b^2 = (w')^4 + b^2$ we see that

$$w' < w.$$

□

Let us fix from now on an odd prime number p and an integer solution to the Fermat equation

$$x^p + y^p = z^p$$

where x, y, z are pairwise coprime. There are two cases to consider now

$$\textbf{Case 1} : p \nmid xyz, \quad \textbf{Case 2} : p \mid xyz$$

We will give a complete proof in Case 1, but we start with some general remarks.

The first one is an observation by Lamé.

Lemma 5.3.3. *There is a factorization*

$$z^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y) \qquad \text{in } \mathbf{Z}[\zeta_p]$$

Proof. We know that

$$t^p - 1 = \prod_{i=0}^{p-1}(t - \zeta_p^i)$$

and the identity follows if we replace $t = -\frac{x}{y}$ (we know that $y \neq 0$) because of the pairwise coprime assumption). □

Lamé then assumed that $\mathbf{Z}[\zeta_p]$ would be a UFD and showed that in Case 1, all elements $x + \zeta_p^i y$ would be pairwise coprime. Then he deduced that these elements all have the form $x + \zeta_p^i y = u_i \alpha_i^p$ for certain $u_i \in \mathbf{Z}[\zeta_p]^\times$ and $\alpha_i \in \mathbf{Z}[\zeta_p]$ and he could derive a contradiction. The problem is that $\mathbf{Z}[\zeta_p]$ is not an UFD in general.

Example 5.3.4. In the exercises, you are asked to show that $\mathbf{Z}[\zeta_{23}]$ is not an UFD. It actually holds that $\mathbf{Z}[\zeta_p]$ is an UFD for all $p < 23$.

However, Kummer noticed that the argument of Lamé could be repaired using unique factoriztion of ideals, but under the assumption that the prime p is a *regular prime*.

Definition 5.3.5 (Regular prime)**.** A prime p is regular if

$$p \nmid h_{\mathbf{Q}(\zeta_p)} = |\operatorname{Cl}(\mathbf{Q}(\zeta_p))|$$

Not all primes are regular, for example $p = 37$ is not. However it was conjectured by Siegel that there are infinitely many regular primes and that they make up around 60% of all primes (in a precise sense). However both parts of the conjecture are still wide open.

Here we want to present Kummer's argument.

Lemma 5.3.6. *The prime p is the unique prime that ramifies in $\mathbf{Q}(\zeta_p)$. Furthermore, there is a unique prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ lying over p and*

$$p\mathcal{O}_{\mathbf{Q}(\zeta_p)} = \mathfrak{p}^{p-1}, \quad \mathfrak{p} = (1 - \zeta_p^i) \text{ for any } i = 1, \ldots, p-1$$

Proof. We know that the discriminant of $\mathbf{Q}(\zeta_p)$ is, up to a sign, a power of p so that p is the unique prime that ramifies in $\mathbf{Q}(\zeta_p)$ Fix the element

$$\omega_p = 1 - \zeta_p \in \mathbf{Z}[\zeta_p]$$

We have seen in the exercises that the minimal polynomial of ω_p is $\Phi_p(1-x)$, which is Eisenstien with respect to the prime p. Hence the Dedekind-Kummer criterion shows that the prime splitting of p inside $\mathbf{Q}(\zeta_p)$ is given by

$$p\mathcal{O}_{\mathbf{Q}(\zeta_p)} = p\mathbf{Z}[\zeta_p] = (p, \omega_p)^{p-1} = \mathfrak{p}^{p-1}$$

and then $\mathfrak{p}$ is the unique prime lying over p. We also know that

$$|N_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\omega_p)| = |\Phi_p(1)| = p$$

hence (ω_p) must be prime and then $\mathfrak{p} = (\omega_p) = (1-\zeta_p^i)$. Finally, we know that $\mathbf{Q}(\zeta_p)$ is a normal extension of $\mathbf{Q}$ with $\mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = \{\sigma_i \,|\, i = 1, \dots, p-1\}$ and $\sigma_i(\zeta_p) = \zeta_p^i$. Since $\mathfrak{p}$ is the unique prime lying over p, it is stabilized by the whole group, meaning that $\mathfrak{p} = \sigma_i(\mathfrak{p}) = (1-\zeta_p^i)$ for all $i = 1, \dots, p-1$. □

Lemma 5.3.7. *The set of roots of unity in ζ_p is*

$$\mu_{\mathbf{Q}(\zeta_p)} = \{2p\text{-th roots of unity }\} = \{\pm\zeta_p^h \,|\, h = 0, \dots, p-1\}$$

Proof. Observe that $(-\zeta_p)^{2p} = 1$ and if $(-\zeta_p)$ does not have order $2p$ in $\mathbf{Q}(\zeta_p)^\times$ then it must have order $1, 2$ or p. All these possibilities are easily ruled out, so we see that $-\zeta_p$ is a primitive $2p$-th root of unity, and that all $2p$-th root of unity have the form $(-\zeta_p)^k$ for some $k = 0, \dots, 2p-1$. Each one of these can be written in the form $\pm\zeta_p^h$ for one $h = 0, \dots, p-1$ and since these are also $2p$ elements, we have proved that

$$\{\pm\zeta_p^h \,|\, h = 0, \dots, p-1\} = \{2p\text{-th roots of unity }\} \subseteq \mu_{\mathbf{Q}(\zeta_p)}$$

Assume now that $\zeta_m \in \mathbf{Q}(\zeta_p)$. Then we can write the prime factorization $m = q_1^{e_1} \dots q_r^{e_r}$ and it follows that $\zeta_{q_i^{e_i}} \in \mathbf{Q}(\zeta_p)$ and in particular $\zeta_{q_i} \in \mathbf{Q}(\zeta_p)$ for all i. If q_i is an odd prime coprime with p, we know that $\mathrm{disc}\,\mathbf{Q}(\zeta_p), \mathrm{disc}\,\mathbf{Q}(\zeta_{q_i})$ are coprime and then from the exercises it follows that $\mathbf{Q}(\zeta_p) \cap \mathbf{Q}(\zeta_{p_i}) = \mathbf{Q}$. Hence we can assume that the q_i are either equal to 2 or to p: $m = 2^e p^f$. Observe that if $f \geq 1$, then $[\mathbf{Q}(\zeta_{p^f}) : \mathbf{Q}] = \phi(p^f) = p^f - p^{f-1} \leq p - 1 = [\mathbf{Q}(\zeta_p) : \mathbf{Q}]$ if and only if $f = 1$. Hence we can assume $m = 2^e \cdot p^f, f \leq 1$. To conclude, we need to show that if $\mathbf{Q}(\zeta_{2^e}) \subseteq \mathbf{Q}(\zeta_p)$ then $e \leq 1$. Assume that $e \geq 2$, then $\mathbf{Q}(\zeta_{2^e p}) = \mathbf{Q}(\zeta_{2^e}, \zeta_p) \subseteq \mathbf{Q}(\zeta_p)$. We can again compare degrees:

$$(2^e - 2^{e-1}) \cdot (p-1) = \phi(2^e)\phi(p) = \phi(2^e p) = [\mathbf{Q}(\zeta_{2^e p}) : \mathbf{Q}] \text{ divides } [\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1$$

and then we see that $e \leq 1$. □

Lemma 5.3.8. *Let $\alpha, \beta \in \mathcal{O}_{\mathbf{Q}(\zeta_p)}$. For any $i = 0, \dots, p-1$ there are ideals $J_i \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ such that*

$$(\alpha + \zeta_p^i \beta) = (\alpha, \beta) \cdot J_i$$

Furthermore either the J_i are pairwise coprime, or $J_i = \mathfrak{p}J_i'$ for pairwise coprime ideals $J_i' \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$.

Proof. The first statement is clear since $\alpha + \zeta_p^i\beta \in (x, y)$. Take now $0 \leq i < j \leq p-1$ and assume that there is a non-zero prime ideal $\mathfrak{q} \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ such that $J_i = \mathfrak{q}J_i'$, $J_j = \mathfrak{q}J_j'$ for some ideals $J_i', J_j' \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$. Then

$$(\alpha + \zeta_p^i\beta, \alpha + \zeta_p^j\beta) = (\alpha, \beta) \cdot \mathfrak{q} \cdot (J_i' + J_j')$$

Observe now that

$$(\alpha + i\zeta_p^i\beta) - (\alpha + \zeta_p^j\beta) = \zeta_p^i(1 - \zeta_p^{j-i})\beta$$
$$(\alpha + i\zeta_p^i\beta) - \zeta_p^{i-j}(\alpha + \zeta_p^j\beta) = (1 - \zeta_p^{i-j})\alpha$$

hence using the fact that ζ_p is invertible in $\mathcal{O}_{\mathbf{Q}(\zeta_p)}$ and that $\mathfrak{p} = (1 - \zeta_p^{i-j}) = (1 - \zeta_p^{j-i})$ we get

$$\mathfrak{p} \cdot (\alpha, \beta) \subseteq ((1 - \zeta_p^{i-j})\alpha, \zeta_p^i(1 - \zeta_p^{j-i})\beta) \subseteq (\alpha + \zeta_p^i\beta, \alpha + \zeta_p^j\beta) = (\alpha, \beta) \cdot \mathfrak{q} \cdot (J_i' + J_j')$$

Looking at the unique factorization of the ideals we see that $\mathfrak{p} \subseteq \mathfrak{q}(J_i' + J_j')$ and since $\mathfrak{p}$ is maximal it must be that $\mathfrak{p} = \mathfrak{q}(J_i' + J_j')$, hence

$$\mathfrak{p} = \mathfrak{q}, \quad J_i' + J_j' = (1)$$

In particular $(\alpha + \zeta_p^i\beta) = (\alpha, \beta)\mathfrak{p}J_i'$. Now let any $h \in \{0, 1, \ldots, p-1\}$: we see that

$$\zeta_p^{i-h}(\alpha + \zeta_p^h\beta) = \zeta_p^{i-h}\alpha + \zeta_p^i\beta = \alpha(\zeta_p^{i-h} - 1) + (\alpha + \zeta_p^i\beta) \in (\alpha, \beta)\mathfrak{p}$$

so that we can write $(\alpha + \zeta_p^h\beta) = (\alpha, \beta) \cdot \mathfrak{p} \cdot J_h'$ for certain ideals J_h'. The previous reasoning shows that the ideals J_h' are pairwise coprime. □

Corollary 5.3.9. *Let x, y, z be a solution to $x^p + y^p = z^p$ with x, y, z pairwise coprime, and p a regular prime such that $p \nmid xyz$. Then there are $u_i \in \mathcal{O}_{\mathbf{Q}(\zeta_p)^\times}$ and $\alpha_i \in \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ such that*

$$x + \zeta_p^i y = u_i \cdot \alpha_i^p$$

Proof. We know that

$$z^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y)$$

Since the x, y, z are pairwise coprime, we know that $(x, y) = (1)$. Then the previous Lemma shows that if the ideals $(x + \zeta_p^i y) \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ are not pairwise coprime, it must be that they are all divisible by $\mathfrak{p}$. In particular then $z \in \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, which is impossible because $p \nmid z$. Hence the ideals $(x + \zeta_p^i y)$ are pairwise coprime, and since their product is $(z)^p$ there must be ideals $H_i \subseteq \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ such that $(x + \zeta_p^i y) = H_i^p$. Then $[H_i]^p = [1]$ in $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$ and since p does not divide the order of the class group, it must be that $[H_i] = [1]$, meaning that $H_i = (\alpha_i)$ for some $\alpha_i \in \mathcal{O}_{\mathbf{Q}(\zeta_p)}$. Since $(x + \zeta_p^i y) = (\alpha_i^p)$ it must be that $x + \zeta_p^i y = u_i\alpha_i^p$ for a unit $u_i \in \mathcal{O}_{\mathbf{Q}(\zeta_p)}^\times$. □

Now we can conclude the proof:

Proof of Case 1 of Fermat's Last Theorem for regular primes. : let p be a regular odd prime and let $x, y, z \in \mathbf{Z}$ be pairwise coprime such that

$$x^p + y^p = z^p, \qquad p \nmid xyz$$

Now we observe that if $p = 3$, then $x^3, y^3, z^3 \equiv \pm 1 \pmod 9$ and then $x^3 + y^3 \equiv z^3 \pmod 9$ has no solutions. So we can assume that $p \geq 5$. If we look at the Fermat equation modulo p we see that

$$z \equiv z^p \equiv x^p + y^p \equiv (x+y)^p \equiv x + y \pmod{p\mathbf{Z}}$$

Since $z \not\equiv 0 \pmod{p\mathbf{Z}}$ it must be that $x + y \not\equiv 0 \pmod{p\mathbf{Z}}$. Assume now that $x - y \equiv 0 \pmod{p\mathbf{Z}}$. Then $x \not\equiv -z \pmod{p\mathbf{Z}}$ otherwise $2x^p \equiv x^p + y^p \equiv z^p \equiv -x^p \pmod{p\mathbf{Z}}$ and then $3x^p \pmod{p\mathbf{Z}}$, that implies $x^p \equiv 0 \pmod{p\mathbf{Z}}$, which is a contradiction. Hence, up to exchanging y and $-z$ we can assume that

$$x^p + y^p = z^p, \qquad p \nmid xy(x+y)(x-y), \quad p \geq 5$$

The previous Corollary shows that there are $u \in \mathcal{O}^\times_{\mathbf{Q}(\zeta_p)}, \alpha \in \mathcal{O}_{\mathbf{Q}(\zeta_p)}$ such that

$$x + \zeta_p y = u \cdot \alpha$$

If we look at the automorphism $\tau \colon \mathbf{Q}(\zeta_p) \longrightarrow \mathbf{Q}(\zeta_p)$ given by $\tau(\zeta_p) = \zeta_p^{-1} = \overline{\zeta_p}$ we see that this is induced by the complex conjugation. If we apply τ we see that

$$x + \zeta_p^{-1} y = \tau(u) \cdot \tau(\alpha)$$

Now write $\alpha = c_0 + c_1\zeta_p + \ldots + c_{p-2}\zeta_p^{p-2}$ for certain $c_i \in \mathbf{Z}$. Then modulo $p\mathcal{O}_{\mathbf{Q}(\zeta_p)}$ we have

$$\alpha^p \equiv (c_0 + c_1\zeta_p + \ldots + c_{p-2}\zeta_p^{p-2})^p \equiv c_0^p + c_1^p\zeta_p^p + \ldots + c_{p-2}^p\zeta_p^{p(p-2)} \equiv c_0^p + \ldots + c_{p-2}^p$$
$$\tau(\alpha)^p \equiv (c_0 + c_1\zeta_p^{-1} + \ldots + c_{p-2}\zeta_p^{-(p-2)})^p \equiv c_0^p + c_1^p\zeta_p^{-p} + \ldots + c_{p-2}^p\zeta_p^{-p(p-2)} \equiv c_0^p + \ldots + c_{p-2}^p$$

Hence we also get that

$$x + \zeta_p y \equiv \frac{u}{\tau(u)}(x + \zeta_p^{-1} y) \pmod{p\mathcal{O}_{\mathbf{Q}(\zeta_p)}}$$

Now we observe that for any $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ we have that $\sigma\tau = \tau\sigma$ because the Galois group is abelian, hence

$$\sigma\left(\frac{u}{\tau(u)}\right) = \frac{\sigma(u)}{\sigma(\tau(u))} = \frac{\sigma(u)}{\tau(\sigma(u))} = \frac{\sigma(u)}{\overline{\sigma(u)}}$$

and this has absolute value 1 for all $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, hence $\frac{u}{\tau(u)}$ must be a root of unity contained in $\mathbf{Q}(\zeta_p)$. Lemma 5.3.7 shows that

$$x + \zeta_p y \equiv (\pm\zeta_p^h) \cdot (x + \zeta_p^{-1} y) \pmod{p\mathcal{O}_{\mathbf{Q}(\zeta_p)}}$$

for a certain $h = 0, \ldots, p-1$.If we look at this equivalence modulo $(1 - \zeta_p)$ (why can we do that?), then we get that

$$x + y \equiv (\pm 1)(x + y) \pmod{p\mathbf{Z}}$$

and since $p \nmid x + y$ it must be that $\pm 1 \equiv 1 \pmod{p\mathbf{Z}}$ and since p is odd it must be that $\pm 1 = 1$ in $\mathbf{Z}$. In conclusion, we have proved that

$$x\zeta_p^0 + \zeta_p y - x\zeta_p^h - y\zeta_p^{h-1} \equiv 0 \pmod{p\mathcal{O}_{\mathbf{Q}(\zeta_p)}}$$

Now notice that any $p-1$ distinct elements among the elements $\zeta_p^0, \zeta_p, \ldots, \zeta_p^{p-2}, \zeta_p^{p-1}$ are a $\mathbf{Z}$-basis of $\mathcal{O}_{\mathbf{Q}(\zeta_p)}$ (why?) so that the same holds of their equivalence classes in $\mathcal{O}_{\mathbf{Q}(\zeta_p)}/p\mathcal{O}_{\mathbf{Q}(\zeta_p)}$ if we consider it as a $\mathbf{F}_p$-vector space. Since $p \nmid xy$ the previous relation shows that two of $0, 1, h, h-1$ must coincide modulo p. This means $h \in \{0, 1, 2\}$ and then we get one of the following three cases

$$(\zeta_p - \zeta_p^{-1})y \equiv 0, \text{ or } (1-\zeta_p)(x-y) \equiv 0, \text{ or } (1-\zeta_p)^2 x \equiv 0 \qquad (\text{mod } p\mathcal{O}_{\mathbf{Q}(\zeta_p)})$$

and since $p \nmid xy(x-y)$ we see that

$$\zeta_p^{-1}(\zeta_p^2 - 1) \equiv 0, \text{ or } (1-\zeta_p) \equiv 0, \text{ or } (1-\zeta_p^2) \equiv 0 \qquad (\text{mod } (1-\zeta_p)^{p-1})$$

which we can also rewrite as

$$(\zeta_p + 1) \equiv 0, \text{ or } 1 \equiv 0, \text{ or } (1+\zeta_p) \equiv 0 \qquad (\text{mod } (1-\zeta_p)^{p-2})$$

We just have to rule out $\zeta_p + 1 \equiv 0 \pmod{(1-\zeta_p)^{p-2}}$, but since $p \geq 5$ this would imply $1+\zeta_p \equiv 0 \pmod{1-\zeta_p}$ and hence $2 \equiv 0 \pmod{1-\zeta_p}$. This is impossible because $\mathcal{O}_{\mathbf{Q}(\zeta_p)}/(1-\zeta_p) \cong \mathbf{F}_p$. $\square$

Appendix A

Commutative algebra

A.1 Rings and ideals

All the rings in this course will be commutative rings with unity 1. Let R be a ring. An element $u \in R$ is called *invertible* or an *unit* if there is another element $v \in R$ such that

$$uv = 1$$

The set of invertible elements in R is denoted by $R^\times$. Two elements $a, b \in R$ are called *associated* if they are the same up to multiplication by a unit, meaning that there is $u \in R^\times$ such that

$$a = ub$$

An element $a \in R$ is a *zero-divisor* if it is non zero, $a \neq 0$ and if there is another non zero element $b \in R, b \neq 0$ such that

$$ab = 0$$

A ring without zero-divisors is called a *domain*. Equivalently, a ring R is a domain if for any $a, b \in R$ it holds that

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

Remark A.1.1. Another way to see this is in terms of a cancellation property for equations in R. If R is a domain and $a \in R, a \neq 0$ then

$$ab = ac \implies b = c \qquad \text{for all } b, c \in R$$

Indeed, we can write the first equation as $a(b - c) = 0$ and since $a \neq 0$ it must be $b = c$.

A ring R is a *field* if any non-zero element is invertible: $R^\times = R \setminus \{0\}$. If R is a domain, its *field of fractions* or *fraction field* is

$$\operatorname{Frac} R = \left\{ \frac{a}{b} \,|\, a \in R, b \in R, b \neq 0 \right\}$$

where $\frac{a}{b} = \frac{a'}{b'}$ if and only if $ab' = a'b$ and the addition and the multiplication is the usual one between fractions. There is an inclusion $R \subseteq \operatorname{Frac} R, a \mapsto \frac{a}{1}$ and this the smallest field containing R, meaning that if $R \subseteq K$ and K is a field, then $\operatorname{Frac} R \subseteq K$ as well. The inclusion of a domain into its fraction field shows that a ring R is a domain if and only if it is a subring of a field.

An *ideal* of R is an additive subgroup $I \subseteq R$ which is "sticky" with respect to the multiplication:

$$a \in I, b \in R \implies ab \in I$$

If $I, J \subseteq R$ are two ideals, then the sum $I + J = \{a + b \,|\, a \in I, b \in J\}$ is an ideal and it is the smallest ideal containing both I, J. The intersection $I \cap J$ is also an ideal and it is the largest ideal contained in both I, J. The product ideal IJ is the ideal generated by the products $ab, a \in I, b \in J$, and $IJ \subseteq I \cap J$.

An ideal $\mathfrak{p} \subseteq R$ is called *prime* if it is a proper ideal $\mathfrak{p} \subsetneq R$ and if for any $a, b \in R$ it holds that

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}$$

An ideal $\mathfrak{m} \subseteq R$ is called *maximal* if it is a proper ideal $\mathfrak{m} \subsetneq R$ which is not contained in any strictly larger proper ideal. It holds that

$$\mathfrak{m} \text{ maximal} \implies \mathfrak{m} \text{ prime}$$

Remark A.1.2. Via the axiom of choice in the form of Zorn's lemma, we can assume that any ring has a non-zero maximal ideal.

If $I \subseteq R$ is an ideal, then the quotient R/I is a ring, and it holds that

$$\begin{aligned} I \text{ is prime} &\iff R/I \text{ is a domain,} \\ I \text{ is maximal} &\iff R/I \text{ is a field.} \end{aligned}$$

Furthermore, any ideal in R/I has the form J/I for a unique ideal $I \subseteq J \subseteq R$ and J/I is prime (resp. maximal) in R/I if and only if J is prime (resp. maximal) in R. Finally, if S is another ring, there is a correspondence between homomorphisms $f\colon R/I \to S$ and homomorphisms $f\colon R \to S$ such that $f(I) = 0$.

A.1.1 Homomorphisms

If R, S are two rings, a *ring homomorphism* from R to S is a map $f\colon R \to S$ such that

$$f(1) = 1, \quad f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b) \qquad \text{for all } a, b \in R$$

An invertible ring homomorphism is called an isomorphism, and in this case the inverse map is also a homomorphism. If $f\colon R \to S$ is a ring homomorphism, its *kernel* is the ideal

$$\operatorname{Ker} f = \{a \in R \,|\, f(a) = 0\}$$

while the image $\operatorname{Im} f \subseteq S$ is a subring of S. The map

$$R/\operatorname{Ker} f \longrightarrow \operatorname{Im} f, \qquad [a] \mapsto f(a)$$

is a ring isomorphism.

A.2 Finitely generated ideals, principal ideals and Noetherian rings

Let R be a ring. Elements $a_1, \ldots, a_n \in R$ generate the ideal

$$(a_1, \ldots, a_n) = \{a_1 b_1 + \cdots + a_n b_n \,|\, b_i \in R\}\,.$$

An ideal $I \subseteq R$ is called finitely generated if $I = (a_1, \ldots, a_n)$ for a finite number of elements a_i. The ideal I is called *principal* if it is generated by one element: $I = (a)$.

Rings where all ideals are finitely generated are particularly nice and deserve a name:

Definition A.2.1 (Noetherian rings)**.** A ring R is called Noetherian if one of the following equivalent conditions is satisfied

1. Any ideal in R is finitely generated.
2. There is no infinite strictly increasing chain of ideals in R:

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$$

Proof. We proof that the two conditions above are equivalent: assume that any ideal in R is finitely generated and let $I_1 \subseteq I_2 \subseteq I_3$ be an infinite increasing chain of ideals. It is easy to check that the union $I = \bigcup_{j=1}^{n} I_j$ is an ideal, so that $I = (a_1, \ldots, a_n)$ for finitely many $a_i \in I$. Since these are finitely many, there is one m such that $a_i \in I_m$ for all $i = 1, \ldots, n$ and then $I = I_m$ so that the chain is not strictly increasing. Conversely, assume that there is no strictly increasing chain of ideals in R and let I be any ideal. If I is not finitely generated, then there are $a_1, a_2, a_3, \cdots \in I$ such that

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \ldots$$

but this is impossible. □

Example A.2.2. A field K contains only two ideals: the zero ideal (0) and the whole field $K = (1)$. Since these two ideals are principal, a field is Noetherian.

Example A.2.3. All ideals in $\mathbf{Z}$ are principal, hence $\mathbf{Z}$ is Noetherian.

We get many more examples of Noetherian rings from the following fundamental theorem:

Theorem A.2.4 (Hilbert's basis theorem)**.** *If R is a Noetherian ring then the polynomial ring $R[x]$ is Noetherian as well.*

A.3 Divisibility

Let R be a ring. If $a, b \in R$ we say that a *divides* b in R if there is $c \in R$ such that $b = ac$, and we write $a \mid b$. Equivalently, this means that b belongs to the ideal generated by a:

$$a \mid b \iff b \in (a) \iff (b) \subseteq (a).$$

Exercise A.3.1. *Let R be a domain and let $a, b \in R$. Prove that the following are equivalent:*

1. *a, b are associated.*
2. *$a|b$ and $b|a$.*
3. *$(a) = (b)$.*

An element $a \in R$ is called *prime* if it is non-zero and if the ideal (a) that it generates is prime. Equivalently, this means that a is non-zero, is not invertible and when a divides a product, then it divides also one of the factors: for any $b, c \in R$

$$a \mid bc \implies a \mid b \text{ or } a \mid c, \qquad \text{for any } b, c \in R.$$

An element $a \in R$ is called *irreducible* if it is non-zero, if a is not invertible and if whenever a is factored as a product, one of the factors is invertible: for any $b, c \in R$

$$a = bc \implies b \in R^\times \text{ or } c \in R^\times \qquad \text{for any } b, c \in R.$$

Lemma A.3.2. *If R is a domain, then any prime element is irreducible.*

Proof. Let $a \in R$ be prime, so that a is nonzero and and assume that $a = bc$ for $b, c \in R$. Then a must divide one of b, c. We can assume that $b = a \cdot u$ for $u \in R$, so that $a = auc$. Since $a \neq 0$ and R is a domain, this means that $uc = 1$, so that c is invertible. □

Lemma A.3.3. *If R is a Noetherian domain then any element $a \in R$ which is non-zero and not invertible has a factorization as a product of irreducible elements*

$$a = p_1 \dots p_n \qquad \text{with } p_i \in R \text{ irreducible.}$$

Proof. If a itself is irreducible, we are done. Otherwise there is a factorization $a = a_1 b_1$ where a_1, b_1 are both non-zero and not invertible. This implies that $(a) \subset (a_1)$ and the inclusion is actually strict, otherwise $a_1 = ac_1$ so that $1 = b_1 c_1$ and b_1 would be invertible. Hence $(a) \subsetneq (a_1)$.

Now observe that if both a_1, b_1 are irreducible, we are done. Otherwise, we can assume that a_1 is not irreducible so we can write $a_1 = a_2 b_2$ for $a_2, b_2 \in R$ non-zero and not invertible. Then we see as before that $(a) \subsetneq (a_1) \subsetneq (a_2)$. Hence if the factorization does not stop, we will find an infinite strictly increasing sequence of ideals

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

and this is impossible since R is Noetherian. □

A.4 Euclidean domains, principal ideal domains and unique factorization domains

A.4.1 Euclidean domains

Definition A.4.1 (Euclidean domain)**.** An Euclidean domain is a domain R that admits an Euclidean function $D\colon R \setminus \{0\} \to \mathbf{Z}_{\geq 0}$ such that R has the Euclidean division property with respect to D. This means that for any $a, b \in R$ with $b \neq 0$ there are $q, r \in R$ such that

$$a = q \cdot b + rv \qquad \text{and} \qquad r = 0 \text{ or } D(r) < D(b)$$

Example A.4.2. The integers $\mathbf{Z}$ are an Euclidean domain with respect to the usual Euclidean norm $|\cdot|\colon \mathbf{Z} \to \mathbf{Z}_{\geq 0}$.

Example A.4.3. If K is a field, the polynomial ring $K[x]$ is an Euclidean domain with respect to the degree $\deg\colon K[x] \setminus \{0\} \to \mathbf{Z}_{\geq 0}$.

Example A.4.4. The Gaussian integers $\mathbf{Z}[i]$ are an Euclidean domain with respect to the norm $N\colon \mathbf{Z}[i] \to \mathbf{Z}, a + ib \mapsto a^2 + b^2$.

A.4.2 Principal ideal domains

Definition A.4.5 (Principal ideal domain)**.** A principal ideal domain (PID) is a domain R such that any ideal in R is principal.

Proposition A.4.6. *Any Euclidean domain is a PID.*

Proof. Let R be an Euclidean domain with respect to a function $D\colon R \setminus \{0\} \to \mathbf{Z}_{\geq 0}$ and let $I \subseteq R$ be an ideal. If $I = 0$, it is principal. If $I \neq 0$, let $a \in I$ be an element such that $D(a) = \min\{D(b) \,|\, b \in I, b \neq 0\}$. We want to show that I is generated by a. To do so, let b be any nonzero element in I, then by the Euclidean division with respect to D there are elements $q, r \in R$ such that $b = aq + r$. In particular $r = b - aq \in I$. If $r = 0$, then $b \in (a)$ and we are done. If $r \neq 0$ then we know that $D(r) < D(a)$ and this is impossible by construction. □

Remark A.4.7. The above proof tells us also how to find a generator of a nonzero ideal in an Euclidean domain. We need to take one nonzero element with the minimum possible value with respect to the Euclidean function.

Example A.4.8. The integers $\mathbf{Z}$, the Gaussian integers $\mathbf{Z}[i]$ and the polynomial ring $K[x]$ over a field K are Euclidean domains, hence they are also PID.

Remark A.4.9. The converse of Proposition A.4.6 is not true. It can be shown that the rings $\mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ and $\mathbf{R}[x, y]/(x^2 + y^2 + 1)$ are PID but not Euclidean [1]

Lemma A.4.10. *Let R be a principal ideal domain and let $p \in R, p \neq 0$. Then the following are equivalent:*

1. *(p) is maximal.*
2. *p is prime.*
3. *p is irreducible.*

Proof. If the ideal (p) is maximal, then it is prime, so that p is a prime element in R. Since R is a domain, if p is prime it is also irreducible. To conclude, we need to show that if p is irreducible then (p) is maximal: assume that there is a proper ideal $I \subsetneq R$ such that $(p) \subseteq I$. We want to show that $(p) = I$. Since R is a PID, it must be that $I = (q)$ for a certain $q \in I$ so that $p = uq$ for an $u \in R$. Since p is irreducible, one of u or q must be invertible, and it cannot be q otherwise $I = (q) = R$. Hence u is invertible and then $(p) = (q) = I$. □

[1] See K. Conrad, "Remarks about Euclidean domains", Theorems 5.22 and 5.23. The notes are available at `https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf`

A.4.3 Unique factorization domains

Definition A.4.11 (Unique factorization domain)**.** An unique factorization domain (UFD) is a domain R such that any non-zero and non invertible $a \in R$ can be written as a product of irreducible factors

$$a = p_1 \dots p_r \qquad \text{with } p_1, \dots, p_r \in R \text{ irreducible}$$

Furthermore such a factorization is unique up to invertible elements: this means that if $q_1, \dots, q_s \in R$ are irreducible and

$$a = p_1 \dots p_r = q_1 \dots q_s$$

then $r = s$ and, up to reordering, p_i is associated to q_i for all $i = 1, \dots, r$.

Lemma A.4.12. *A domain R is an UFD if and only if both the following conditions are satisfied*

1. *Any non-zero and not invertible element $a \in R$ has a factorization $a = p_1 \cdot p_r$ with the p_i irreducible.*

2. *Irreducible elements are the same as prime elements*

Proof. We know that prime elements in a domain are always irreducible. Assume that R is an UFD and let $p \in R$ be irreducible. We need to prove that p is prime. Let $a, b \in R$ such that $p \mid ab$, so that there is $q \in R$ such that

$$ab = pq$$

If a is invertible then $p \mid b$ and if a is zero then $p \mid a$, so that we can assume that a, b are both non-zero and not invertible. Write $a = a_1 \dots a_r$ and $b = b_1 \dots b_s$ as a product of irreducible factors so that

$$a_1 \dots a_r \cdot b_1 \dots b_s = pq$$

We can also write the right-hand-side of the previous equation as a product of irreducible factors where one of these factors is p. By uniqueness of the factorization, p must be associated to one of the a_i, and then $p \mid a$, or to one of the b_j, and then $p \mid b$.

Conversely, assume that R is a domain where both the above conditions are satisfied. Since we are assuming that any non-zero and not invertible element has a factorization, we need to prove that this is unique. let $p_1, \dots, p_r, q_1, \dots, q_s \in R$ be irreducible elements such that

$$p_1 \dots p_r = q_1 \dots q_s$$

Assume that $r \leq s$. By assumption, the p_i are prime, hence p_1 must divide one of $q_1, \dots, q_s$. Up to reordering,we can assume that $p_1 \mid q_1$ so that $q_1 = u_1 p_1$ for a certain $u_1 \in R$. Plugging this in in the previous equation we get

$$p_2 \dots p_r = u_1 \cdot q_2 \dots q_s$$

and if we keep going we see that for any $i = 1, \dots, r$ we can find $u_i \in R$ such that $q_i = u_i p_i$ and moreover

$$1 = u_1 \dots u_r \cdot q_{r+1} \dots q_s$$

This shows that $r = s$ and that all the u_i are invertible, which is what we wanted to prove. □

Corollary A.4.13. *A PID is an UFD.*

Proof. Since a PID is a Noetherian domain, we know that any non-zero and not invertible element has a factorization into irreducible. Moreover we also know from Lemma A.4.10 that all irreducible elements are prime. We conclude thanks to Lemma A.4.12. □

Example A.4.14. This shows that the integers $\mathbf{Z}$, the Gaussian integers $\mathbf{Z}[i]$ and the polynomial ring $K[x]$ with K a field are UFD. Other sources of UFD are given by the following result

Theorem A.4.15 (Gauss)**.** *If R is an UFD, the polynomial ring $R[x]$ is an UFD as well.*

Example A.4.16. In particular the polynomial rings $K[x_1, \ldots, x_n]$ with K a field and $\mathbf{Z}[x_1, \ldots, x_n]$ are UFD.

It is not true in general that any UFD is a PID.

Exercise A.4.17. *Show that the ideal (x, y) in the ring $\mathbf{Q}[x, y]$ is not principal, so that $\mathbf{Q}[x, y]$ is an UFD which is not a PID.*

Remark A.4.18. We have seen that

$$R \text{ Euclidean domain} \implies R \text{ PID} \implies R \text{ UFD}$$

and we have also seen that none of these implication is reversible.

A.4.4 Coprime elements and greatest common divisor

Let R be a ring and let $a, b \in R$. A *common divisor* of a, b is an element $c \in R$ such that $c \mid a, c \mid b$. The elements are called *coprime* if the only common divisors are invertible.

Lemma A.4.19. *If R is a domain and if $p, q \in R$ are two irreducible elements, then they are either coprime or associated.*

Proof. Assume that they are not coprime, so that there is a not invertible element $r \in R$ such that $p = ar, q = br$ for some $a, b \in R$. Since p, q are irreducible, a, b must be invertible so that p, q are associated. □

Definition A.4.20 (Greatest common divisor)**.** Let R be a domain and let $a, b \in R$. A *greatest common divisor* is an element $c \in R$ such that:

1. c divides both a, b: $c \mid a, c \mid b$.
2. if $c' \in R$ divides both a, b then c' divides c: $c' \mid a, c' \mid b \implies c' \mid c$.

If c is such a greatest common divisor we write $c = \mathrm{GCD}(a, b)$. This is an abuse of notation, since a greatest common divisor is not uniquely determined, see the remarks below.

Remark A.4.21. Two elements $a, b \in R$ in a domain R are coprime if and only if $1 = \mathrm{GCD}(a, b)$.

Remark A.4.22. A greatest common divisor is not unique: if c is a greatest common divisor of a, b and if c' is associated to c then c' is a greatest common divisor of a, b as well. The converse is also true: if c, c' are two greatest common divisors of a, b, then $c \mid c'$ and $c' \mid c$ and since R is a domain c, c' must be associated.

Remark A.4.23. More importantly, a greatest common divisor does not always exist. For an example, [2] consider the domain $R = \mathbf{Z}[\sqrt{-3}]$ and prove that the two elements $a = 4, b = 2+2\sqrt{-3}$ have no greatest common divisor.

If our ring is an UFD, everything is fine:

Lemma A.4.24. *Let R be an UFD. Then any $a \in R$ which is non-zero has a factorization of the form*

$$a = u \cdot p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

where $u \in R^\times$ is invertible, the $p_i \in R$ are irreducible and pairwise coprime and $e_i \in \mathbf{Z}_{>0}$. Furthermore, if

$$a = v \cdot q_1^{f_1} q_2^{f_2} \dots q_r^{f_s}$$

is another such factorization, then $r = s$ and, up to reordering, p_i is associated to q_i, and $e_i = f_i$ for all $i = 1, \dots, r$.

Proof. If a is invertible the result is straightforward. Assume a is not invertible. Then there is a factorization $a = p'_1 \dots p'_n$ into irreducible elements. If we collect the associated elements together, we get a factorization of the form that we want. The second statement follows from the uniqueness of the factorization in R. □

Corollary A.4.25. *Two non-zero elements a, b in an UFD R always have a greatest common divisor. It can be computed by the common associated irreducible factors in a factorization of a, b with the minimum common exponent.*

($\star$) Gauss' Lemma

If R is a UFD, then a polynomial $f(x) \in R[x]$ of positive degree is called *primitive* if the coefficients of f are coprime, meaning that the only common divisors are the invertible elements.

Remark A.4.26. Let $f(x) \in K[x]$ be a polynomial of positive degree. Then we can find $b \in K[x], b \neq 0$ (for example, the product of all denominators appearing in the coefficients of $f(x)$) such that $b \cdot f(x) = F(x) \in R[x]$. Let now $a = \text{GCD}(\text{ coefficients of } F)$, so that $F(x) = a \cdot F'(x)$ where $F'(x)$ is a primitive polynomial. This shows that there are $a, b \in R, b \neq 0$ such that

$$f(x) = \frac{a}{b} F'(x)$$

with $F'(x) \in R[x]$ primitive, and we can also assume a, b to be coprime.

Lemma A.4.27 (Gauss' Lemma)**.** *Let R be a UFD and let $K = \text{Frac}(R)$ be its field of fractions.*

1. *The product of two primitive polynomials in $R[x]$ is primitive.*
2. *If $f(x), g(x), h(x) \in K[x]$ are monic polynomials such that $f(x) = g(x)h(x)$, then $f \in R[x]$ if and only if $g(x), h(x) \in R[x]$.*
3. *A non-constant polynomial $f(x) \in R[x]$ is irreducible in $R[x]$ if and only if it is primitive and irreducible in $K[x]$.*

[2] Due to Arturo Magidin on Mathoverflow `https://math.stackexchange.com/q/4864187`

Proof. 1. Assume that $G(x), H(x) \in R[x]$ are two primitive polynomials and assume that there is a prime $p \in R[x]$ that divides all factors of $G(x)H(x)$. Then $G(x)H(x) = 0$ in $(R/(p))[x]$ and since (p) is prime, $R/(p)$ is a domain and $R/(p)[x]$ is a domain as well, meaning that $G(x) = 0$ or $H(x) = 0$ in $R/(p)[x]$. But this is impossible, because it would mean that p divides all coefficients of $G(x)$ or of $H(x)$.

2. Thanks to Remark A.4.26, we can write

$$g(x) = \frac{a}{b}G'(x), \quad h(x) = \frac{c}{d}H'(x)$$

for $G'(x), H'(x) \in R[x]$ primitive and a, b coprime and c, d coprime. In particular, $b \cdot g(x) \in R[x]$ and a divides all coefficients of this polynomial. Since $g(x)$ is monic, a must divide b and since a, b are coprime, we can assume, up to multiplying by an invertible element, that $a = 1$. Hence

$$g(x) = \frac{1}{b}G(x), \quad h(x) = \frac{1}{d}H(x)$$

Then we have

$$bc \cdot f(x) = G(x)H(x)$$

Assume now that $f(x) \in R[x]$: since $G(x), H(x)$ are primitive, the product $bc \cdot f(x)$ must be primitive. In particular, bc must be invertible in R and then $g(x), h(x)$ have coefficients in R.

3. Assume that $f(x)$ is primitive and irreducible in $K[x]$ and write $f(x) = g(x)h(x)$ in $R[x]$. Since $f(x)$ is irreducible in $K[x]$, we can assume that $g(x)$ is constant, so that $g(x) = b \in R$. Since $f(x)$ is primitive, b must be invertible in R.

   Conversely, assume that $f(x)$ is irreducible in $R[x]$. First we prove that it is primitive: write $f(x) = d \cdot F(x)$ where $d \in R$ is a common divisor of the coefficients of $f(x)$ and $F(x) \in R[x]$. Since $f(x)$ is of positive degree, $F(x)$ must be of positive degree as well, and since $f(x)$ is irreducible, d must be invertible. We now show that $f(x)$ is irreducible in $K[x]$: assume that $f(x) = g(x)h(x)$ with $g(x), h(x) \in K[x]$. If one of $f(x), g(x)$ has degree zero, we are done, otherwise there are elements $b, c, d, e \in R$ such that $b \cdot g(x) = d \cdot G(x), c \cdot h(x) = e \cdot H(x)$ with $G(x), H(x) \in R[x]$ primitive, and then

$$bc \cdot f(x) = de \cdot G(x)H(x)$$

   Since both $f(x)$ is primitive, we see that a greatest common divisors of the coefficients on the left-hand-side is bc and since $G(x)H(x)$ is primitive, we see that the greatest common divisor of the coefficients of the right hand side is de. Hence, we can write $f(x) = uG(x) \cdot H(x)$ for a $u \in R^\times$. Since $f(x)$ is irreducible in $R[x]$, one of $uG(x), H(x)$ must be of degree zero, and then one of $g(x), h(x)$ is of degree zero as well. □

As a consequence, we can prove

Proof of Theorem A.4.15. We want to use Lemma A.4.12 and show that any non-zero and not invertible element $f(x) \in R[x]$ is a product of irreducible factors and that any irreducible element is also prime.

For the existence of a factorization, consider $f(x) \in R[x]$ of positive degree (the case of degree zero is covered by R itself). We can write $f(x) = d \cdot F(x)$ for $d \in R$ and $F(x)$ primitive,

so it is enough to show that $F(x)$ has a factorization in irreducible. This factors into irreducible polynomials in $K[x]$: $F(x) = p_1(x)\dots p_r(x)$ with the $p_i(x) \in K[x]$, and we can write $p_i(x) = \frac{a_i}{b_i}P(x)$ for $a_i, b_i \in R$ and $P_i(x) \in R[x]$ primitive. Then $b_1 \dots b_r \cdot F(x) = a_1 \dots a_r P_1(x) \dots P_r(x)$. Notice that since $P_1(x) \dots P_r(x)$ is primitive, the greatest common divisor of all coefficients on the right-hand-side must be $a_1 \dots a_r$, and the same reasoning shows that the greatest common divisor of all coefficients on the left-hand-side must be $b_1 \dots b_r$. Then these two must be associated so that $F(x) = uP_1(x) \cdot \dots P_r(x)$ where $u \in R^\times$ and each $P_i(x) \in R[x]$ is primitive and irreducible in $K[x]$, hence irreducible in $R[x]$.

Let now $f(x) \in R[x]$ be irreducible We want to prove that it is prime. Let us consider only the case where f has positive degree, so that $f(x)$ is primitive in $R[x]$ and irreducible in $K[x]$. Assume that $f(x) \mid g(x)h(x)$ for $g(x), h(x) \in R[x]$. Since $f(x)$ is irreducible in $K[x]$ and this is an UFD, it is also prime in $K[x]$, so that we can assume that $f(x) \mid g(x)$ in $R[x]$. Then $g(x) = f(x) \cdot k(x)$ for $k(x) \in K[x]$. We can write $k(x) = \frac{a}{b}K(x)$ for $a, b \in R$ coprime, so that

$$bg(x) = af(x)K(x)$$

Since $f(x)K(x)$ is primitive, the greatest common divisor of all coefficients on the right-hand-side must be a which must then divide all the coefficients on the left-hand-side, and then b must divide a. This means that $\frac{a}{b} \in R$ so that $f(x) \mid g(x)$ in $R[x]$. □

A.4.5 Factorization in a PID

The unique factorization property in a PID can be rephrased in terms of ideals rather than in terms of elements. First we state Bezout's lemma for PIDs:

Lemma A.4.28 (Bezout)**.** *If R is a PID and $a, b \in R$ then an element $c \in R$ is a greatest common divisor of a, b if and only if it is a generator of the ideal generated by a, b:*

$$(a) + (b) = (\mathrm{GCD}(a, b)).$$

In particular there are $h, k \in R$ such that

$$\mathrm{GCD}(a, b) = ha + kb$$

Proof. Let c be a generator of $(a) + (b)$: this means in particular that $c \mid a, c \mid b$, because $a, b \in (a) + (b)$. Furthermore, since $c \in (a) + (b)$ it must be that $c = ah + bk$ for certain $h, k \in R$ so that any common divisor of a, b is also a divisor of c. □

Definition A.4.29 (Coprime ideals)**.** Two ideals $I, J \subseteq R$ in a ring R are called coprime if the only ideal containing both of them is the whole ring: $I + J = R$. Equivalently, this means that there are $a \in I, b \in J$ such that

$$a + b = 1.$$

Lemma A.4.30. *Let R be a ring and $(a), (b)$ two principal ideals generated by $a, b \in R$.*

1. *If $(a), (b)$ are coprime ideals then a, b are coprime elements.*
2. *If R is a PID and a, b are coprime elements then $(a), (b)$ are coprime ideals.*
3. *If R is a PID and $(a), (b)$ are prime ideals, then they are either equal or coprime.*

Proof. 1. Let $c \in R$ such that $c \mid a, c \mid b$. Since the ideals are coprime there are $h, k \in R$ such that $1 = ah + bk$ so that $c \mid 1$. This means that c is invertible.

2. Since R is a PID and a, b are coprime we know from Bezout's Lemma A.4.28 that $(a) + (b) = (1)$ meaning that the ideals are coprime.

3. If $(a), (b)$ are prime ideals, then a, b are prime elements, hence irreducible. Then Lemma A.4.19 shows that they are either associated (and then $(a) = (b)$) or coprime (and then $(a), (b)$ are coprime).

□

With this in mind, we can translate the statement about unique factorization of elements into unique factorization of ideals:

Proposition A.4.31 (Unique factorization of ideals in a PID)**.** *Let R be a PID and let $I \subseteq R$ be an ideal which is not zero and not R. Then there are mutually distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq R$ and $e_1, \ldots, e_r \in \mathbf{Z}_{>0}$ such that*

$$I = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$$

Furthermore the prime ideals $\mathfrak{p}_i$ and the exponents e_i are uniquely determined by I.

Proof. Since R is a PID, $I = (a)$ for one $a \in I$ which is not zero and not invertible. Then we can write a in the form $a = u \cdot p_1^{e_1} \ldots p_r^{e_r}$ where $u \in R^\times$ and the $p_i \in R$ are prime elements, pairwise coprime, and $e_i \in \mathbf{Z}_{>0}$. The ideals $\mathfrak{p}_i = (p_i)$ are prime and pairwise coprime as well, and we can write

$$I = (a) = (up_1^{e_1} \ldots p_r^{e_r}) = (p_1^{e_1}) \ldots (p_r^{e_r}) = (p_1)^{e_1} \ldots (p_r)^{e_r} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}.$$

For the uniqueness, assume that $I = \mathfrak{q}_1^{f_1} \ldots \mathfrak{q}_s^{f_s}$ where the $\mathfrak{q}_i$ are prime ideals, mutually distinct and $f_i \in \mathbf{Z}_{>0}$. Since R is a PID there are $q_i \in R$ mutually coprime such that $\mathfrak{q}_i = (q_i)$ and then $(a) = (q_1^{f_1} \ldots q_s^{f_s})$. This means that $a = vq_1^{f_1} \ldots q_s^{f_s}$ for $v \in R^\times$, and by the properties of unique factorization in R, it must be that $r = s$, and up to reordering, that $e_i = f_i$ and that p_i is associated to q_i, meaning precisely that $\mathfrak{p}_i = \mathfrak{q}_i$. □

Remark A.4.32. It is not hard to show that the statement of unique factorization for ideals in a PID as in Proposition A.4.31 implies the unique factorization for elements in a PID.

A.5 Modules

A module over a ring is the generalization of a vector space over a field.

Definition A.5.1 (Module)**.** A module over a ring R is an abelian group M together with a scalar multiplication by elements of R:

$$R \times M \longrightarrow M, \qquad (a, m) \mapsto a \cdot m$$

such that for all $a, a' \in R, m, m' \in M$ it holds that

1. $a \cdot (m + m') = a \cdot m + a \cdot m'$
2. $(a + a') \cdot m = a \cdot m + a' \cdot m$

3. $(aa') \cdot m = a \cdot (a' \cdot m)$

4. $1 \cdot m = m$.

Example A.5.2. Modules over a field are the same as vector spaces.

Example A.5.3. Modules over $\mathbf{Z}$ are the same as abelian groups (Why? Think about it until it is clear to you).

Example A.5.4. If $R \subseteq S$ is an extension of rings, then S is naturally an R-module where the scalar multiplication is given by the multiplication in S: ab for $a \in R, b \in S$. In particular, R is a module over itself.

Example A.5.5. If R is a ring and $n \in \mathbf{Z}_{>0}$, the set $R^{\oplus r}$ of column vectors with entries in R is an R module with the usual operations of entry-wise addition and scalar multiplication

$$\begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_r + b_r \end{pmatrix}, \quad c \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} ca_1 \\ \vdots \\ ca_n \end{pmatrix} \text{ for } a_i, b_i, c \in R$$

In general, if M, N are two R-modules, their *direct sum*

$$M \oplus N = \{(m, n) \,|\, m \in M, n \in N\}$$

is an R-module with the operations

$$(m, n)+(m', n') = (m+m', n+n'), \quad a \cdot (m, n) = (am, an) \quad \text{for all } a \in R, m, m' \in M, n, n' \in N$$

If M is an R-module, a *submodule* of M is an additive subgroup $N \subseteq M$ which is closed with respect to the multiplication by scalars:

$$a \in R, m \in N \implies am \in N \qquad \text{for all } a \in R, m \in M$$

Example A.5.6. A module M has always two submodules: the zero submodule $M = (0) = \{0\}$ and the full module M.

Example A.5.7. A submodule of the ring R itself is the same as an ideal $I \subseteq R$.

If M is an R-module and $N, N' \subseteq M$ are two submodules, then the intersection $N \cap N'$ and the sum $N + N' \subseteq M$ are also submodules of M. In particular, the sum $N + N'$ is the smallest submodule that contains both N, N', i.e. the submodule generated by N, N'.

If M is an R-module and $N \subseteq M$ a submodule, then the *quotient* M/N is an R-module with the operations

$$[m] + [m'] = [m + m'], \quad a \cdot [m] = [a \cdot m] \qquad \text{for all } a \in R, m, m' \in M$$

Example A.5.8. If R is a ring and $I \subseteq R$ is an ideal, the quotient ring R/I has a natural structure of R-module.

If M, N are R-modules a *homomorphism of R-modules* or an *R-linear* map from M to N is a map $f\colon M \longrightarrow N$ such that

$$f(m+m') = f(m) + f(m') \qquad f(a \cdot m) = a \cdot f(m) \qquad \text{for all } a \in R, m, m' \in M$$

An invertible homomorphism is called an *isomorphism* and in this case the inverse map is also an homomorphism. If $f\colon M \to N$ is a homomorphism of R-modules then its *kernel*

$$\operatorname{Ker} f = \{m \in M \mid f(m) = 0\}$$

is a submodule of M and the image $\operatorname{Im} f$ is a submodule of N. There is an isomorphism of R-modules given by the map:

$$M/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f \qquad [m] \mapsto f(m)$$

Furthermore, if $N \subseteq M$ is a submodule, any submodule of M/N has the form N'/N for a unique submodle $N \subseteq N' \subseteq M$, and the map

$$(M/N)/(N'/N) \xrightarrow{\sim} M/N', \quad [m] \mapsto [m]$$

is an isomorphism.

Example A.5.9. Consider the free modules $R^{\oplus r}, R^{\oplus s}$ and let $A \in R^{r\times s}$ be a $r \times s$ matrix with coefficients in R. The matrix induces a R-linear map via the usual matrix multiplication that we know from linear algebra

$$L_A\colon R^{\oplus s} \longrightarrow R^{\oplus r}, \qquad v \mapsto Av$$

Furthermore, if $f\colon R^{\oplus s} \longrightarrow R^{\oplus r}$ is an arbitrary R-linear map, consider the vectors $e_1, \dots, e_s \in R^{\oplus s}$ such that e_i is zero everywhere apart from the i-th position, where it is equal to 1, and take the $r \times s$ matrix $A = (f(e_1)|\dots|f(e_s))$ that has the images $f(e_i)$ as column vectors. Then it is easy to see that

$$f = L_A$$

This shows that any R-linear map $f\colon R^{\oplus s} \longrightarrow R^{\oplus r}$ is of the form L_A for a unique matrix $A \in R^{r\times s}$. Furthermore, the usual composition rules from linear algebra work so that, if $A \in R^{s\times r}, B \in R^{r\times t}$ then $AB \in R^{s\times t}$ and $L_A \circ L_B = L_{AB}$. Assume now that a linear map $L_A\colon R^{\oplus s} \longrightarrow R^{\oplus r}$ corresponding to $A \in R^{r\times s}$ is an isomorphism. Then there is an inverse map $L_B\colon R^{\oplus r} \to R^{\oplus s}$ corresponding to a matrix $B \in R^{s\times r}$ such that

$$AB = I_r, \qquad BA = I_s$$

Choose any maximal ideal $\mathfrak{m} \subseteq R$, and let $\overline{A} \in (R/\mathfrak{m})^{r\times s}, \overline{B} \in (R/\mathfrak{m})^{s\times r}$ the matrices obtained looking at all coefficients of A, B modulo $\mathfrak{m}$. Then it holds that

$$\overline{A} \cdot \overline{B} = \overline{I}_r, \qquad \overline{B} \cdot \overline{A} = \overline{I}_s$$

and since $(R/\mathfrak{m})$ is a field, we know from linear algebra that $r = s$. We now see that L_A is an isomorphism if and only if the matrix A is *invertible* in $R^{r\times r}$, meaning that there is another matrix $B \in R^{r\times r}$ with coefficients in R such that

$$AB = BA = I_n$$

The set of invertible matrices forms a subgroup of $R^{r\times r}$ denoted by $\mathrm{GL}_n(R)$. A matrix $A \in R^{r\times r}$ is invertible in $R^{r\times r}$ if and only if its determinant is invertible in R:

$$\mathrm{GL}_r(R) = \{A \in R^{r\times r} \mid A \text{ invertible } \} = \{A \in R^{r\times r} \mid \det(A) \in R^\times\}$$

Indeed, if there is $B \in R^{r\times r}$ such that $AB = I_1$, then $\det(A)\det(B) = \det(AB) = \det(I_r) = 1$ so that $\det(A) \in R^\times$. Conversely, if $A \in R^{r\times r}$ is an arbitrary matrix, then its *adjoint matrix* $B = \mathrm{adj}(A)$ is an $r \times r$ matrix whose coefficients are the $(r-1)\times(r-1)$ minors of A, up to a sign, and it holds that

$$A\,\mathrm{adj}(A) = \mathrm{adj}(A)A = \det(A)\cdot I_r$$

Hence, if $\det(A) \in R^\times$, then $B = \det(A)^{-1}\cdot \mathrm{adj}(A)$ is the inverse matrix for A.

In the previous example, we proved the following

Lemma A.5.10. *The two R-modules $R^{\oplus r}, R^{\oplus s}$ are isomorphic if and only if $r = s$.*

A.5.1 Finitely generated modules and Noetherian modules

If M is an R-module the submodule generated by $m_1, \ldots, m_n \in M$ is the smallest submodule $(m_1, \ldots, m_n) \subseteq M$ containing these elements, and it is the set of all possible linear combinations of these elements with coefficients in R:

$$(m_1, \ldots, m_n) = \{a_1m_1 + \cdots + a_nm_n \mid a_i \in R\}$$

The module M is called finitely generated if there are $m_1, \ldots, m_n \in M$ such that $M = (m_1, \ldots, m_n)$. A *cyclic module* is a module that is generated by a single element: $M = (m)$.

Remark A.5.11. If M is generated by one element m, then the map

$$R \to M, \quad a \mapsto a \cdot m$$

is a surjective homomorphism of R-modules, so that $M \cong R/\operatorname{Ker} f$. Conversely, if $I \subseteq R$ is an ideal, then R/I is generated by the class $[1]$ as an R-module. Hence, an R-module is cyclic if and only if it is isomorphic to a quotient R/I, where $I \subseteq R$ is an ideal. More generally, a module M is generated by r elements $m_1, \ldots, m_r$ if and only if the R-linear map

$$f\colon R^{\oplus r} \longrightarrow M, \quad \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} \mapsto a_1m_1 + \cdots + a_rm_r$$

is surjective. This means precisely that $M \cong R^{\oplus r}/N$ for the submodule $N = \operatorname{Ker} f$.

Definition A.5.12 (Noetherian module)**.** An R-module M is called Noetherian if one of the following equivalent conditions is satisfied:

1. Any submodule of R is finitely generated.
2. There is no infinite strictly increasing chain of submodules in M:

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \ldots$$

Proof. The proof is analogous to the case of rings in Definition A.2.1. Do it for modules as an exercise. □

Lemma A.5.13. *Let M be an R-module and $N \subseteq M$ be a submodule. Then M is Noetherian if and only if both N and M/N are Noetherian.*

Proof. If M is Noetherian then any submodule of N is also a submodule of M, hence it is finitely generated. Furthermore, any submodule of M/N is of the form N'/N for $N \subseteq N' \subseteq M$, where N' is a submodule of M. Since N' is finitely generated, N'/N is finitely generated as well.

Conversely assume that M/N and N are both Noetherian and let $N' \subseteq M$ be a submodule. Consider the map $\pi\colon M \to M/N$: the set $\pi(N') \subseteq M/N$ is a submodule, and it is finitely generated by classes $[m_1], \dots, [m_r]$ for certain $m_i \in N'$. This means that if $n' \in N'$ then $[n'] = [a_1 m_1 + \cdots + a_r m_r]$ in M/N for certain $a_i \in R$. In turn this means that $n' = a_1 m_1 + \cdots + a_r m_r + n$ for a certain $n \in N \cap N'$. Since N is Noetherian, any element in $N \cap N'$ is finitely generated by elements $n_1, \dots, n_s \in N \cap N'$. This shows that N' is finitely generated by the elements $m_1, \dots, m_r, n_1, \dots, n_s$. □

Corollary A.5.14. *If M, N are two Noetherian R-modules, the direct sum $M \oplus N$ is also Noetherian.*

Proof. Consider the submodule $M \oplus (0) \subseteq M \oplus N$. We have that $M \oplus (0) \cong M$ is Noetherian and $M \oplus N/(M \oplus (0))$ is Noetherian, so that the conclusion follows from Lemma A.5.13. □

Proposition A.5.15. *If R is a Noetherian ring and M is a finitely generated R-module then it is Noetherian.*

Proof. First we observe that R is Noetherian as a module over itself because it is Noetherian as a ring, hence $R^{\oplus r}$ is Noetherian as an R-module because of Corollary A.5.14. Assume now that M is finitely generated by elements $m_1, \dots, m_r \in M$. Remark A.5.11 shows M is isomorphic to a quotient $R^{\oplus n}/N$ of the Noetherian module $R^{\oplus n}$ so that it is itself Noetherian. □

A.5.2 Free modules

Let M be an R-module. Elements $m_1, \dots, m_r \in M$ are called *linearly independent* if whenever we have a linear combination of them that sums to zero, all coefficients must be zero:

$$a_1 m_1 + \cdots + a_r m_r = 0 \implies a_1 = \cdots = a_r = 0 \qquad \text{for all } a_1, \dots, a_r \in R$$

A *finite basis* of M is a *finite set of linearly independent generators* $m_1, \dots, m_r \in M$. A finitely module with a basis is called *free*.

Example A.5.16. The module $R^{\oplus r}$ has a canonical basis given by the column vectors e_i from $i = 1, \dots, r$ which are zero everywhere apart from the i-th coordinate, where they are equal to 1.

Remark A.5.17. An R-module M has a basis of r elements if and only if it is isomorphic to $R^{\oplus r}$. Indeed, if $m_1, \dots, m_r$ is a basis, then the R-linear map

$$f\colon R^{\oplus n} \longrightarrow M, \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto a_1 m_1 + \cdots + a_n m_n$$

is surjective because the m_i are generators and it is injective because the m_i are linearly independent. Conversely, if $f\colon R^{\oplus r} \to M$ is an isomorphism, then the images $m_i = f(e_i)$ of the canonical basis element form a basis of M.

Lemma A.5.18. *Any two finite bases of an R-module M have the same number of elements.*

Proof. If M has a basis with r element it is isomorphic to $R^{\oplus r}$ and if it has a basis with s elements then it is isomorphic to $R^{\oplus s}$ so that the conclusion follows from Lemma A.5.10. □

Definition A.5.19 (Rank of a finitely generated free module)**.** If M is a finitely generated free R-module, the cardinality of any basis is called the *rank* of M. A module M is free or rank r if and only if it is isomorphic to $R^{\oplus r}$.

The characteristic polynomial

Let R be a ring and $A \in R^{r\times r}$ a matrix. The *characteristic polynomial* of A is the monic polynomial with coefficients in R given by

$$\chi_A(t) = \det(tI_r - A) = t^r - \operatorname{tr}(A)t^{r-1} + \cdots + (-1)^r \det(A) \in R[t]$$

The most important fact about the characteristic polynomial is:

Theorem A.5.20 (Cayley-Hamilton)**.** *Let $A \in R^{r\times r}$ be a square matrix and let $\chi_A(t) = t^r + c_{r-1}t^{r-1} + \cdots + c_0 \in R[t]$ be its characteristic polynomial, then*

$$\chi_A(A) = A^r + c_{r-1}A^{r-1} + \cdots + c_1 A + c_0 I_r = 0.$$

Proof. Define an $R[t]$-module structure on $M = R^{\oplus r}$ via the multiplication

$$P(t) \star v = P(A)v \qquad \text{for all } P(t) \in R[t], v \in M \tag{A.5.1}$$

Let $e_1, \ldots, e_r \in M$ be the canonical basis vectors. Then

$$t \star e_j = Ae_j = a_{1j}e_1 + \cdots + a_{rj}e_r \quad \text{for all } j = 1, \ldots, r$$

We can write this in matrix form as

$$\begin{pmatrix} t & & \\ & \ddots & \\ & & t \end{pmatrix} \star \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{pmatrix} \star \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix},$$

where the $\star$ denotes that the multiplication in the matrix product should be carried out with respect to (A.5.1). We can rewrite this expression as

$$(t \cdot I_r - A) \star \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = 0,$$

and multiplying on the left by the adjoint matrix $\operatorname{adj}(tI_r - A)$ we get

$$\chi_A(t)I_r \star \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} \chi_A(t) \star e_1 \\ \vdots \\ \chi_A(t) \star e_r \end{pmatrix} = 0$$

This means that $\chi_A(t) \star e_i = \chi_A(A)e_i = 0$ for all $i = 1, \ldots, r$ and this means precisely that $\chi_A(A) = 0$. □

If M is a free module of rank r and if $f\colon M \to M$ is a R-linear map, then we can associate to f a matrix $A \in R^{r\times r}$ by choosing a basis of M as in linear algebra, and then the *characteristic polynomial* of f is the polynomial

$$\chi_f(t) = \chi_A(t).$$

As in linear algebra, it can be shown that this is independent of the chosen basis of M and hence of the matrix A associated to f. This gives in particular a way to define the *trace* and the *determinant* of the endomorphism of a free module of finite rank, by taking the trace and the determinant of A. The Cayley-Hamilton theorem implies that $\chi_f(f) = 0$, i.e. if $\chi_f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$, then

$$\chi_f(f) = f^n + a_{n-1}f^{n-1} + \cdots + a_1 f + a_0 \operatorname{id}_M = 0.$$

Corollary A.5.21. *Let M, N be free R-modules of finite rank.*

1. *If there is a surjective homomorphism $f\colon M \twoheadrightarrow N$, then* $\operatorname{rank}(M) \geq \operatorname{rank}(N)$.
2. *If there is an injective homomorphism $f\colon M \hookrightarrow N$ then* $\operatorname{rank}(M) \leq \operatorname{rank}(N)$.
3. *If there is an isomorphism $f\colon M \xrightarrow{\sim} N$ then* $\operatorname{rank}(M) = \operatorname{rank}(N)$.

Proof. ($\star$) Via choosing bases of M, N, we can suppose that $M \cong R^{\oplus m}, N \cong R^{\oplus n}$.

1. The map is given by a matrix multiplication $L_A\colon R^{\oplus m} \to R^{\oplus n}$ for $A \in R^{n\times m}$. Let $\mathfrak{m} \subseteq R$ be any maximal ideal and consider the matrix $\overline{A} \in (R/\mathfrak{m})^{n\times m}$. One can check (as an easy but important exercise) that the $R/\mathfrak{m}$-linear map $L_{\overline{A}}\colon (R/\mathfrak{m})^{\oplus m} \to (R/\mathfrak{m})^n$ is surjective, and since $R/\mathfrak{m}$ is a field, we know from linear algebra that $m \geq n$.
2. ($\star$) Assume that $m > n$ and let $g\colon R^{\oplus n} \hookrightarrow R^{\oplus m}$ be the following injective but not surjective homomorphism:

$$g\colon R^{\oplus n} \hookrightarrow R^{\oplus m}, \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

The composition $h = g \circ f\colon R^{\oplus m} \to R^{\oplus m}$ is injective. Let $P(t) = t^k + c_{k-1}t^{k-1} + \cdots + c_1 t + c_0 \in R[t]$ be a monic polynomial of the minimal possible degree such that $P(h) = 0$ (the

Cayley-Hamilton theorem shows that the characteristic polynomial is one such polynomial). Observe that $a_0 \neq 0$, otherwise

$$h((h^{k-1} + c_{k-1}t^{k-2} + \cdots + c_1 \operatorname{id}_M)(v)) = 0 \qquad \text{for all } v \in R^{\oplus m}$$

and since h is injective, this means $(h^{k-1} + c_{k-1}t^{k-2} + \cdots + c_1 \operatorname{id}_M) = 0$ which is impossible by the fact that k is the minimal degree of a monic polynomial vanishing on h. Choose now the element $e_{n+1} \in R^{\oplus m}$. Since $P(h) = 0$ we know that

$$-a_0 \cdot e_{n+1} = (h^{k-1} + c_{k-1}t^{k-2} + \cdots + c_1 h)(e_{n+1}) \in \operatorname{Im}(h) \subseteq \operatorname{Im}(g)$$

but the $n+1$-th coordinate of any vector in $\operatorname{Im}(g)$ is zero by construction, so that $a_0 = 0$, a contradiction.

3. This follows from the previous points but we proved this already in Lemma A.5.10.

□

Remark A.5.22. ($\star$) The proof for surjective maps is a straightforward reduction to linear algebra, but the same ideal does not work for injective maps: indeed if $L_A \colon R^{\oplus m} \to R^{\oplus n}$ is an injective R-linear map, and $\mathfrak{m} \subseteq R$ is a maximal ideal, then there is no guarantee that the map $L_{\overline{A}} \colon (R/\mathfrak{m})^{\oplus m} \to (R/\mathfrak{m})^{\oplus n}$ is injective as well. Consider for example the multiplication-by-2 map of $\mathbf{Z}$ (represented by the 1×1 matrix 2):

$$(\cdot 2) \colon \mathbf{Z} \to \mathbf{Z}, \quad n \mapsto 2n$$

On the quotient $\mathbf{Z}/2\mathbf{Z}$ this map is actually zero:

$$(\cdot \overline{2}) \colon \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}, \quad [n] \mapsto [2n] = 0.$$

The underlying issue here is that passing to the quotient $R/\mathfrak{m}R$ means tensoring by $\otimes_R R/\mathfrak{m}R$ and the tensor product is a right-exact functor (preserves surjectivity) but not a left-exact one (does not preserve injectivity). Ask me if you want to know more.

Remark A.5.23. If R is a domain, then we can give an easier proof of Corollary A.5.21 via linear algebra over the field $K = \operatorname{Frac} R$. Indeed, suppose that $L_A \colon R^{\oplus m} \hookrightarrow R^{\oplus n}$ is an injective map. We can also see A as a matrix with coefficients in K so that we have a map $L_A^{(K)} \colon K^{\oplus m} \hookrightarrow K^{\oplus n}$. Now notice that for any $v \in K^{\oplus m}$ there is an $a \in R, a \neq 0$ such that $a \cdot v \in R^{\oplus m}$, just take the product of all denominators appearing in the coordinates of v. Now we prove Corollary A.5.21:

1. We want to show that if L_A is surjective, then $L_A^{(K)}$ is surjective as well, so that the conclusion follows from linear algebra: let $w \in K^{\oplus n}$ and $a \in R$ such that $a \cdot w \in R^{\oplus n}$. Then there is $v \in R^{\oplus m}$ such that $a \cdot w = A \cdot v$ and then $w = A \cdot \frac{1}{a} v$.

2. We want to show that if L_A is injective, then $L_A^{(K)}$ is surjective as well, so that the conclusion follows from linear algebra: let $v \in K^{\oplus m}$ such that $A \cdot v = 0$ and let $a \in R, a \neq 0$ such that $a \cdot v \in R^{\oplus n}$. Then $A \cdot (av) = aAv = 0$ so that $a \cdot v = 0$ and then it must be that $v = 0$.

Notice that we defined the characteristic polynomial, trace and determinant for a R-linear map $f\colon M \to M$ of a free module M of finite rank. Can we do it for just a finitely generated R-module M? Assume that M is an R-module, finitely generated by $m_1, \dots, m_r$ and let $f\colon M \to M$ be an R-linear map. Then there are $a_{ij} \in R$ such that

$$f(m_j) = a_{1j}m_1 + \cdots + a_{rj}m_r \qquad \text{for all } j = 1, \dots, n$$

and this defines a matrix $A = (a_{ij}) \in R^{r\times r}$. The matrix A has a characteristic polynomial $\chi_A(t) \in R[t]$ so we could call this the characteristic polynomial of f. The problem with this definition is that the polynomial $\chi_A(t)$ is not independent of the chosen generating system: for a simple example $\mathbf{Z}$ is generated by 1 but also by $2, 3$ as a $\mathbf{Z}$-module, so if we use these two different systems of generators, we get a characteristic polynomial of degree 1 and another one of degree 2.

However, we still get something from this construction: if $\chi_A(t)$ is the characteristic polynomial of the matrix A defined before, then the Cayley-Hamilton Theorem A.5.20 shows that $\chi_A(A) = 0$ and then it is straightforward to show that we also have $\chi_A(f) = 0$. This proves the following version of the Cayley-Hamilton theorem for finitely generated modules.

Corollary A.5.24. *Let M be a finitely generated R-module and let $f\colon M \to M$ be an R-linear map. Then there is a monic polynomial $G \in R[x]$ such that $G(f) = 0$. In other words, there are $a_0, \dots, a_{r-1} \in R$ such that*

$$f^r + a_{r-1}f^{r-1} + \cdots + a_1 f + a_0 \operatorname{id}_M = 0$$

A.5.3 Finitely generated modules over a PID

Over a field, every vector space has a basis, so that every finitely generated module is free. This is very much not true over an arbitrary ring, but we can get something analogous over a principal ideal domain. We start with a general definition:

Definition A.5.25 (Torsion)**.** Let R be a ring and M an R-module. An element $m \in M$ is a *torsion element* if there is a non-zerodivisor $a \in R$ such that $am = 0$.In particular, if R is a domain, an element $m \in M$ is a *torsion element* if there is $a \neq 0$ such that $am = 0$. A *torsion module* is a module where every element is a torsion element, and a *torsion-free module* is a module where the only torsion element is zero.

Example A.5.26. A free module $R^{\oplus r}, r \geq 1$ is always torsion-free. In particular, over a field, all finitely generated modules are torsion-free. Instead, the $\mathbf{Z}$-module $\mathbf{Z}/6\mathbf{Z}$ is torsion, since $6 \cdot m = 0$ for all $m \in \mathbf{Z}/6\mathbf{Z}$.

Remark A.5.27. If M is an R-module, the set $M_{tor} = \{m \in M \mid m \text{ torsion element }\}$ is a submodule of M and it is itself a torsion module. The quotient M/M_{tor} is a torsion-free module.

Proof. To show that M_{tor} is a submodule, we need to show that if $m, m' \in M$ are torsion elements, then $m + m'$ and am are torsion for all $a \in A$. Since m, m' are torsion, there are two non-zerodivisors $b, b' \in R$ such that $bm = b'm' = 0$. Since b, b' are two non-zerodivisors, the product bb' is a non-zerodivisor as well. We see that

$$bb' \cdot (m + m') = 0, \quad b \cdot am = 0$$

The fact that M_{tor} is a torsion module is clear from the definition. To prove that the quotient M/M_{tor} is torsion-free, let $[m] \in M/M_{tor}$ be an element with $m \in M$ and assume that $a \cdot [m] = [am] = 0$ for a non-zerodivisor $a \in R$. This means that $am \in M_{tor}$ so that there is a non-zerodivisor b such that $abm = 0$. But then $ab \in R$ is a non-zerodivisor, and $m \in M_{tor}$ so that $[m] = 0$ in M/M_{tor}. □

The fundamental result about principal ideal domains is the following:

Theorem A.5.28 (Classification of finitely generated modules over a PID)**.** *Let R be a PID and M be a finitely generated module. The following holds:*

1. *if M is torsion-free, then it is free of finite rank.*
2. *if M is torsion, then there are unique ideals $(d_1), \ldots, (d_s) \subseteq R$ with $d_1 | d_2 | \ldots | d_s$ such that*

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \ldots R/(d_s)$$

3. *if M is arbitrary finitely generated, then $M \cong M_{tor} \oplus M/M_{tor}$. Hence, there is a unique $r \in \mathbf{Z}_{\geq 0}$ and ideals $(d_1), \ldots, (d_s) \subseteq R$ with $d_1 | \ldots | d_s$ such that*

$$M \cong R^{\oplus r} \oplus R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_s).$$

In particular, if M is a finitely generated module over a PID, this result tells us that M/M_{tor} is free. Then we define the *rank of* M as the rank of this free module

$$\operatorname{rank}(M) = \operatorname{rank}(M/M_{tor}).$$

We see that M is torsion if and only if it has rank zero.

Remark A.5.29. Up to now, we have defined the rank of a free finitely generated module over an arbitrary ring and the rank of a finitely generated module over a PID. There is not a notion of rank for an arbitrary finitely generated module over an arbitrary ring.

Remark A.5.30. The theorem tells us that any finitely generated R-module over a PID R is isomorphic to a direct sum of cyclic modules. Indeed, any cyclic R-module is isomorphic to $R/(d)$ for a certain $d \in R$, and if $d = 0$, then $R/(d) = R$.

Example A.5.31. In the case $R = \mathbf{Z}$, this is telling us that any finitely generated abelian group A is isomorphic to a direct sum $A \cong \mathbf{Z}^{\oplus r} \oplus \mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_s\mathbf{Z}$ for a certain $r \in \mathbf{Z}_{\geq 0}$ and $d_1 | d_2 | \ldots | d_s$. This statement is known as the classification of the finitely generated abelian groups.

The Smith normal form and the proof of the classification theorem

Here we discuss the proof of the classification theorem of finitely generated modules over a principal ideal domain R. It will follow from a special normal form for matrices with coefficients in R. If $A \in R^{r \times s}$ is a matrix with entries in R, the *elementary operations* that we can perform on the rows of A are the following:

1. Switch two rows.

2. Add to a row a multiple of another row by an element $a \in R$.

3. Multiply a row by an invertible element $u \in R^\times$

We can of course perform the analogous operations on the columns of A. As in linear algebra, the row operations can be interpreted as multiplying the matrix A on the left by a certain invertible matrix and the column operations correspond to multiplying A on the right by a certain invertible matrix.

Remark A.5.32. If K is a field, the last elementary operation can be rephrased as saying that we multiply a row (or a column) by a non-zero element. If R is an arbitrary ring, however, we must ask the element to be invertible.

Theorem A.5.33 (Smith normal form for matrices over a PID)**.** *If R is PID then any matrix $A \in R^{r\times s}$ can be brought via left and right multiplication by invertible matrices into Smith normal form*

$$\begin{pmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & d_s & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

for $d_1, \dots, d_s \in R$ with $d_i \neq 0$ and $d_1|d_2|\dots|d_s$. The d_i are uniquely determined by A up to associated elements by the formula

$$d_1 \cdot \ldots \cdot d_h = \mathrm{GCD}(\text{ all } h \times h \text{ minors of } A) \quad \text{for all } h = 1, 2, \dots$$

where we interpret the right hand side as 0 if all the $h \times h$ minors are equal to zero. Furthermore, if R is an Euclidean domain, A can be brought into Smith normal form by elementary row and column operations.

Example A.5.34. Let us give an example for an integer matrix:

$$A = \begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 2 & 2 & 3 \end{pmatrix}$$

We see that a greatest common divisor of all elements in the matrix is 1, and we can make it appear in the matrix via elementary operations

$$\begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 2 & 2 & 3 \end{pmatrix} \xrightarrow{(C3)\to(C3)-(C2)} \begin{pmatrix} 7 & 8 & 1 \\ 4 & 5 & 1 \\ 2 & 2 & 1 \end{pmatrix}$$

Via elementary operations we can put this greatest common divisor in the upper left corner

$$\begin{pmatrix} 7 & 8 & 1 \\ 4 & 5 & 1 \\ 2 & 2 & 1 \end{pmatrix} \xrightarrow{(C1)\leftrightarrow(C3)} \begin{pmatrix} 1 & 8 & 7 \\ 1 & 5 & 4 \\ 1 & 2 & 2 \end{pmatrix}$$

Since this greatest common divisor divides all other entries of the matrix, we can use elementary operations to reduce all other entries to the right of it and below it to zero

$$\begin{pmatrix} 1 & 8 & 7 \\ 1 & 5 & 4 \\ 1 & 2 & 2 \end{pmatrix} \xrightarrow[(R3)\to(R3)-(R1)]{(R2)\to(R2)-(R1)} \begin{pmatrix} 1 & 8 & 7 \\ 0 & -3 & -3 \\ 0 & -6 & -5 \end{pmatrix} \xrightarrow[(C3)\to(C3)-7(C3)]{(C2)\to(C2)-8(C1)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -3 \\ 0 & -6 & -5 \end{pmatrix}$$

Now we repeat the procedure with the smaller 2×2 matrix: a GCD of all elements is -1, and we can make it appear in the upper left corner of the submatrix with a series of elementary operations

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -3 \\ 0 & -6 & -5 \end{pmatrix} \xrightarrow{(C2)\to(C2)-(C3)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -3 \\ 0 & -1 & -5 \end{pmatrix} \xrightarrow{(R2)\leftrightarrow(R3)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -5 \\ 0 & 0 & -3 \end{pmatrix}$$

We can now use elementary operations to reduce all elements below and to the left of -1 to zero:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -5 \\ 0 & 0 & -3 \end{pmatrix} \xrightarrow{(C3)\to(C3)-5(C1)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -3 \end{pmatrix}$$

We end up with a matrix in Smith normal form. If we want, we can also use elementary operations so that all elements in the diagonal are non-negative

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -3 \end{pmatrix} \xrightarrow[(R3)\to-(R3)]{(R2)\to-(R2)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Sketch of proof over an Euclidean domain. We prove that any matrix A over an Euclidean domain R can be brought into Smith normal form. The idea is to use row and column operations to put $d_1 = \mathrm{GCD}(a_{ij})$ into the upper left corner of A. Since d_1 divides all othe entries, we can use elementary row and column operations to reduce all elements below d_1 and to the right of d_1 to zero, so that our matrix has the block form

$$\begin{pmatrix} d_1 & 0 \\ 0 & A' \end{pmatrix}$$

for a smaller matrix A'. Then we repeat the procedure A'. To make this work, we need to prove that the first step works:

Claim: If $A \neq 0$ then we can use row and column operations to put $d_1 = \mathrm{GCD}(a_{ij})$ in the upper left corner of the matrix.

Consider the function $D\colon R \setminus \{0\} \to \mathbf{Z}_{\geq 0}$ that makes R into an Euclidean domain. We prove the claim by induction on $m = \min\{D(a_{ij}) \,|\, a_{ij} \neq 0\}$. If $m = 0$, then there is an element $a_{ij} \neq 0$ with $D(a_{ij}) = 0$. Then a_{ij} must be invertible (why?) so that it is a greatest common divisors of all elements. We can switch rows and columns until this element goes in the upper left corner. For the induction step, let again $a_{ij} \neq 0$ be an element such that $D(a_{ij}) = m$. Via row and column operations we can assume that $a_{ij} = a_{11}$. Assume now that there is an entry in the first column which is not divisible by a_{11}, for example a_{21}. Then there are $q, r \in R, r \neq 0$ such that

$$a_{21} = qa_{11} + r, \quad D(r) < D(a_{11}) = m$$

Using an elementary row operation, we can replace a_{21} by $a_{21} - qa_{11} = r$ and then we prove the claim by induction. This way, we can assume that a_{11} divides all entries in the first row and column of A, so that we can use row and column operations to bring the matrix in the block form

$$\begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix}$$

Observe now that if a_{11} divides all elements in A', then it is the greatest common divisor and we are done. Otherwise, there is an element which is not divided, and, via row and column operations we can assume that it is the entry a'_{22} in row 2 and column 2. Then there are $q', r' \in R, r' \neq 0$ such that $a'_{22} = q'a_{11} + r', D(r') < D(a_{11}) = m$. Consider the sequence of elementary operations (that we represent only on the upper left 2×2 block

$$\begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} \to \begin{pmatrix} a_{11} & a_{11} \\ 0 & a_{22} \end{pmatrix} \to \begin{pmatrix} a_{11} & 0 \\ -q'a_{11} & a_{22} - q'a_{11} \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ -q'a_{11} & r' \end{pmatrix}$$

Since $D(r') < D(a_{11}) = m$ by construction, we conclude by induction.

We proved that a matrix can always be brought into Smith normal form. To check that the d_i are uniquely determined by A, up to associated elements, we check the formula

$$d_1 \dots d_h = \text{GCD}(\text{ all } s \times s \text{ minors of } A)$$

It is easy to see that the formhttps://www.kununu.com/ula holds if the matrix is in Smith normal form so we just need to show that the right hand side does not change if we perform elementary operations on A. However, this follows from the fact that the elementary operations on a square matrix change the determinant only up to multiplication by an invertible element. □

With the result about the Smith normal form, we prove the structure theorem for modules over PID (without the uniqueness of the d_i):

Sketch of proof of Theorem A.5.28. Let M be a finitely generated module over a PID R and let $m_1, \dots, m_r \in M$ be generators. This defines a surjective map $f\colon R^{\oplus r} \to M, f(e_i) = m_i$ for $i = 1, \dots, r$ and

$$M \cong R^{\oplus r} / \operatorname{Ker} f.$$

Note that $\operatorname{Ker} f$ is also finitely generated because $R^{\oplus r}$ is Noetherian thanks to Proposition A.5.15 so there is a surjection $R^{\oplus s} \to \operatorname{Ker} f$. This surjection gives an R-linear map $R^{\oplus s} \to R^{\oplus r}$ whose image is $\operatorname{Ker} f$, and such a map is the multiplication $L_A\colon R^{\oplus s} \to R^{\oplus r}$ by a matrix $A \in R^{r \times s}$:

$$M \cong R^{\oplus r} / \operatorname{Ker} f = R^{\oplus r} / \operatorname{Im} L_A$$

Theorem A.5.28 shows that, up to multiplying A to the left and the right by invertible matrices, we can assume that A is in Smith normal form. Since these left and right multiplication correspond to composing L_A with isomorphisms of $R^{\oplus r}, R^{\oplus s}$, we can assume directly that A is in Smith normal form

$$A = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \operatorname{diag}(d_1, \dots, d_h)$$

Then it follows that

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \dots \oplus R/(d_h) \oplus R^{r-h}$$

In particular $M_{tor} = R/(d_1) \oplus \cdots \oplus R/(d_h)$, $M/M_{tor} \cong R^{r-h}$ is free and $M \cong M_{tor} \oplus M/M_{tor}$. All the statements of the theorem follow, apart from the uniqueness of the d_i up to associated elements, which we do not discuss here. We just mention that it is related to the uniqueness up to associates of the d_i in the Smith normal form. □

We will also need another application of the Smith normal form in the case of free abelian groups of the same rank.

Lemma A.5.35. *Let $\Lambda \subseteq \Lambda'$ be two free abelian groups of ranks $n = \operatorname{rank}(\Lambda)$ and $n' = \operatorname{rank}(\Lambda') \geq n$.*

1. *There are bases $\alpha_1, \ldots, \alpha_n$ of Λ and $\alpha'_1, \ldots, \alpha'_{n'}$ of Λ' such that $\alpha_i = d_i \cdot \alpha'_i$ for $i = 1, \ldots, n$ and certain $d_1 | d_2 | \ldots | d_n$ all non-zero. Furthermore*

$$\Lambda/\Lambda' \cong (\mathbf{Z})^{\oplus(n'-n)} \oplus \mathbf{Z}/d_1\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/d_n\mathbf{Z}$$

2. *The quotient Λ'/Λ is finite if and only if $n = n'$. In this case, if $A \in \mathbf{Z}^{n \times n}$ is a matrix representing the inclusion $\Lambda \hookrightarrow \Lambda'$ with respect to an arbitrary basis $\beta_1, \ldots, \beta_n$ of Λ and $\beta'_1, \ldots, \beta'_n$ of Λ', then*

$$|\Lambda'/\Lambda| = |\det(A)|$$

Proof. Let $\beta_1, \ldots, \beta_n$ be an arbitrary basis of Λ and $\beta'_1, \ldots, \beta'_{n'}$ be an arbitrary basis of Λ' and let $A \in \mathbf{Z}^{n' \times n}$ be the matrix representing the inclusion $\Lambda \hookrightarrow \Lambda'$ with respect to these maps. Then the matrix A can be put in Smith normal form: meaning that there are matrices $B \in \mathrm{GL}_{n'}(\mathbf{Z}))$ and $C \in \mathrm{GL}_n(\mathbf{Z})$ such that $BAC = \begin{pmatrix} D \\ O \end{pmatrix}$ where $D = \operatorname{diag}(d_1, \ldots, d_n)$ with $d_1 | \ldots | d_n$. Since the inclusion is injective, the d_i must all be non-zero. This proves the first point and also that Λ'/Λ is finite if and only if $n = n'$. In this case, observe that B, C are then square matrices with $\det B, \det C \in \{\pm 1\}$ so that

$$|\Lambda'/\Lambda| = |\mathbf{Z}/d_1\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/d_n\mathbf{Z}| = d_1 \ldots d_n = |\det(D)| = |\det(B)\det(A)\det(C)| = |\det(A)|.$$

□

A.6 The Chinese remainder theorem

Let A be a ring. Two ideals $I, J \subseteq A$ are called *coprime* if $I + J = A$. Equivalently, this means that there are $a \in I, b \in J$ such that $a + b = 1$ or that $I + J$ is contained in a maximal ideal $I + J \subseteq \mathfrak{m} \subseteq A$.

Example A.6.1. If A is a PID, for example $A = \mathbf{Z}$ then two ideals $I = Aa$ and $J = Ab$ are coprime if and only if their generators a, b have no common prime factors. This is not true if A is an UFD, can you find a counterexample?

Lemma A.6.2. *let A be a ring and $I_1, \ldots, I_n, I, J \subseteq A$ ideals.*

1. *If $I_1, \ldots, I_n$ are all coprime with J, then $I_1 \ldots I_n$ and is also coprime with J.*
2. *IF I, J are coprime, then I^a, J^b are coprime for all $a, b \in \mathbf{Z}_{\geq 0}$.*

Proof. 1. By assumption, there are $a_h \in I_h, b_h \in J$ for all $h = 1, \dots, n$ such that $a_h + b_h = 1$. Then

$$1 = \prod_{h=1}^{n}(a_h + b_h) = a_1 \dots a_n + b_1 c_1 + \dots + b_n c_n$$

for certain $c_h \in A$. Hence $1 \in I_1 \dots I_n + J$.

2. By point (i), I^a is coprime with J and if we apply point (ii) again we see that I^a is coprime with J^b.

□

Theorem A.6.3 (Chinese Remainder Theorem)**.** *Let A be a ring and $I_1, \dots, I_n \subseteq A$ pairwise coprime ideals. Then $I_1 \cap \dots \cap I_n = I_1 \cdot \dots \cdot I_n$ and the map*

$$A/I_1 \dots I_n \longrightarrow A/I_1 \times \dots \times A/I_n, \quad [a] \mapsto ([a], [a], \dots, [a])$$

is an isomorphism of rings.

Proof. We proceed by induction on n. If $n = 1$ there is nothing to prove. If $n = 2$, let $a_h \in I_h$ for $h = 1, 2$ such that $a_1 + a_2 = 1$. If $x \in I_1 \cap I_2$ then

$$x = x \cdot 1 = x \cdot (a_1 + a_2) = xa_1 + xa_2 \in I_1 I_2$$

Hence $I_1 \cap I_2 \subseteq I_1 I_2 \subseteq I_1 \cap I_2$ so that $I_1 I_2 = I_1 \cap I_2$. Consider now the map

$$\pi \colon A \longrightarrow A/I_1 \times A/I_2, \quad a \mapsto ([a], [a])$$

This is a homomorphism of rings whose kernel is equal to $I_1 \cap I_2 = I_1 I_2$ so we need to prove that it is surjective. Observe that $a_1 = 1 - a_2$ so that $a_1 \in I_1$ and $a_1 \in 1 + I_2$. This means $\pi(a_1) = ([0], [1])$ and an analogous reasoning shows that $\pi(a_2) = ([1], [0])$. Then for any $b_1, b_2 \in A$ we see that $\pi(b_2 a_1 + b_1 a_2) = ([b_1], [b_2])$ so that π is surjective.

For the induction step, assume the result holds for $n-1$. The ideals $I = I_1 \cap \dots \cap I_{n-1}$ and I_n are coprime because of Lemma A.6.2 and using the induction we have then $I \cap I_n = I I_n = I_1 \dots I_n$. Furthermore, we also have isomorphisms

$$A/I_1 \dots I_n = A/I \cdot I_n \longrightarrow A/I \times A/I_n \longrightarrow A/I_1 \times \dots \times A/I_{n-1} \times A/I_n.$$

and the composition is precisely the maps that we are looking for. □

Example A.6.4. Take pairwise coprime numbers $m_1, \dots, m_s \in \mathbf{Z}$. Then the Chinese Remainder Theorem tells us that the map

$$\mathbf{Z}/m_1 \dots m_s \mathbf{Z} \longrightarrow \mathbf{Z}/m_1\mathbf{Z} \times \dots \times \mathbf{Z}/m_s\mathbf{Z}, \quad [a] \mapsto ([a], \dots, [a])$$

is an isomorphism. This means that if we choose arbitrary numbers $a_1, \dots, a_s \in \mathbf{Z}$ then there is another number $a \in \mathbf{Z}$ such that

$$a \equiv a_i \pmod{m_i}$$

and furthermore a is unique modulo $m_1 \dots m_s$.

Appendix B

Field theory

B.1 Characteristic and Frobenius

If R is a ring, there is always a unique ring homomorphism

$$\mathbf{Z} \longrightarrow R, \quad 1 \mapsto 1$$

If $n \in \mathbf{Z}$, we say that $n = 0$ in R if it belongs to the kernel of this homomorphism, meaning that $n \cdot 1 = 0$ in R.

Assume now that $R = F$ is a field: then the image of the previous homomorphism is a domain, so that the kernel must be a prime ideal. If the kernel is zero, we say that F has *characteristic zero*. Otherwise, the kernel is generated by a positive prime number $p \in \mathbf{Z}, p > 0$, and we then say that F has *characteristic* p.

Remark B.1.1. If F has characteristic 0, then the previous map is injective and we can consider $\mathbf{Z} \subseteq F$. Taking the field of fractions of $\mathbf{Z}$ we see that $\mathbf{Q} \subseteq F$. If instead F has characteristic p, then the image of the previous map is isomorphic to $\mathbf{Z}/p\mathbf{Z} \cong \mathbf{F}_p \subseteq F$. Hence F has characteristic zero if and only if it contains $\mathbf{Q}$ and it has characteristic p if and only if it contains $\mathbf{F}_p$.

One key difference between the two characteristics is the following:

Lemma B.1.2. *Let R be a ring and let $p \in \mathbf{Z}, p > 0$ be a prime number such that $p = 0$ in R. Then the Frobenius map defined by*

$$\mathrm{Frob}\colon R \longrightarrow R, \quad x \mapsto x^p$$

is a ring homomorphism, which is furthermore injective if R is a domain.

Proof. The only thing that is not obvious is that $\mathrm{Frob}(x+y) = \mathrm{Frob}(x) + \mathrm{Frob}(y)$ for all $x, y \in R$. We compute

$$\mathrm{Frob}(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = \mathrm{Frob}(x) + \mathrm{Frob}(y)$$

where the third equality follows from the fact that $p \mid \binom{p}{k}$ in $\mathbf{Z}$ for all $k = 1, \ldots, p-1$. The fact that if R is a domain then Frob is injective follows immediately by considering the kernel. □

Definition B.1.3. Let F be a field of positive characteristic p. The Frobenius homomorphism of F is the field homomorphism

$$\mathrm{Frob}\colon F \longrightarrow F, \quad x \mapsto x^p$$

Lemma B.1.4. *If F has positive characteristic p, then*

$$\mathrm{Frob}(x) = x \quad \text{if and only if} \quad x \in \mathbf{F}_p \subseteq F$$

Proof. The set of fixed points of the Frobenius coincide with the roots in F of the polynomial $t^p - t$. This polynomial has at most p roots, so if we prove that every element in $\mathbf{F}_p$ is a fixed point, these must be all the fixed points. So we can reduce to the case $F = \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, and what we actually have to prove is that $x^{p-1} = 1$ for all $x \in \mathbf{F}_p^\times$, and this follows from the fact that $\mathbf{F}_p^\times$ is a finite group of order $p - 1$. □

Remark B.1.5. If F is a finite field of characteristic p, the Frobenius homomorphism is actually an isomorphism, since it is an injective map between two sets of the same cardinality.

B.2 Algebraic and finite extensions of fields

If $F \subseteq K$ is an extension of fields, then an element $\alpha \in K$ integral over F is also called *algebraic*. If $F \subseteq K$ is an integral field extension, it is also called *algebraic*. This terminology is only used for field extensions, not for general ring extensions.

Remark B.2.1. If $F \subseteq K$ is a field extension, an element $\alpha \in K$ is algebraic over F if and only if it is a root of a *non-zero polynomial* (not necessarily monic) $P(x)$ with coefficients in F. Indeed, since F is a field, we can multiply $P(x)$ by the inverse of its leading coefficient to obtain a monic polynomial in $F[x]$ that vanishes at α.

If a field extension $F \subseteq K$ is finite, then K is a finitely generated F-vector space. The *degree* of the field extension is the dimension of K as a F-vector space and it is denoted by

$$[K : F] \stackrel{\text{def}}{=} \dim_F K$$

We know from Proposition 2.1.6 that any finite field extension is algebraic.

Lemma B.2.2. *If $F \subseteq K \subseteq L$ is a tower of field extensions, with K finite over F and L finite over K, then L is finite over F and*

$$[L : F] = [L : K] \cdot [K : F]$$

Proof. If $x_1, \ldots, x_n$ is a basis of L over K and $y_1, \ldots, y_m$ is a basis of K over F, the same proof of Lemma 2.1.5 shows that $x_i y_j$ is a basis of L over F. □

If $F \subseteq K$ is a field extension and $\alpha_1, \ldots, \alpha_n \in K$, we denote by $F(\alpha_1, \ldots, \alpha_n)$ the smallest subfield of K containing F and $\alpha_1, \ldots, \alpha_n$. This can be described explicitly in terms of the ring $F[\alpha_1, \ldots, \alpha_n] \subseteq K$: this is a domain, since it is a subring of a field, and then

$$F(\alpha_1, \ldots, \alpha_n) = \mathrm{Frac}\, F[\alpha_1, \ldots, \alpha_n] = \left\{ \frac{P(\alpha_1, \ldots, \alpha_n)}{Q(\alpha_1, \ldots, \alpha_n)} \mid P, Q \in F[x_1, \ldots, x_n], Q(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

A *principal field extension* of F is one of the form $F(\alpha)$. Let now $F \subseteq K$ be a field extension and let $\alpha \in K$. We have the the ring homomorphism

$$\mathrm{ev}_\alpha \colon F[x] \longrightarrow K, \quad P(x) \mapsto P(\alpha)$$

whose image is $F[\alpha]$. By definition, α is algebraic over F if and only if $\operatorname{Ker} \mathrm{ev}_\alpha \neq 0$. Since $F[x]$ is a Euclidean domain with respect to the degree, we know that $\operatorname{Ker} \mathrm{ev}_\alpha = (m_{\alpha,F}(x))$ where $m_{\alpha,F}(x) \in F[x]$ is the unique monic polynomial of smallest degree vanishing on α.

Definition B.2.3 (Minimal polynomial)**.** If $F \subseteq K$ is a field extension and $\alpha \in K$ is algebraic over F, the polynomial $m_{\alpha,F}(x)$ is called the *minimal polynomial* of α over F

Proposition B.2.4. *Let $\alpha \in K$ be algebraic over F and let $m_{\alpha,F}(x)$ be its minimal polynomial. The following properties hold:*

1. *If $P(x) \in F[x]$, then $P(\alpha) = 0$ if and only if $m_{\alpha,F}(x) \mid P(x)$ in $F[x]$.*
2. *The minimal polynomial $m_{\alpha,F}(x)$ is the unique monic irreducible polynomial in $F[x]$ vanishing on α.*
3. *$F(\alpha) = F[\alpha]$ and $F \subseteq F(\alpha)$ is a finite extension.*
4. *If $\deg m_\alpha(x) = n$, then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis of $F(\alpha)$ as a F-vector space, in particular*
$$[F(\alpha) : F] = \deg m_{\alpha,F}(x).$$

Proof. All the properties are fairly straightforward to prove:

1. This means precisely that $m_\alpha(x)$ generates $\operatorname{Ker} \mathrm{ev}_\alpha$.
2. We know that $F[x]/(m_{\alpha,F}(x)) \cong F[\alpha]$ and $F[\alpha]$ is a domain, since it is a subring of a field. Hence $(m_\alpha(x))$ is a prime ideal and $m_\alpha(x)$ is irreducible. Conversely, if $P(x) \in F[x]$ is irreducible and $P(\alpha) = 0$, then $m_\alpha(x) \mid P(x)$ so that $m_\alpha(x)$ and $P(x)$ must be associated. If $P(x)$ is monic, this means $P(x) = m_{\alpha,F}(x)$ by looking at the leading coefficient.
3. Since $F[x]$ is a PID, the ideal $(m_{\alpha,F}(x))$ is actually maximal, so that $F[\alpha] = F[x]/(m_{\alpha,F}(x))$ is a field, and then $F[\alpha] = \operatorname{Frac} F[\alpha] = F(\alpha)$. We also know from Proposition 2.1.6, that $F[\alpha] = F(\alpha)$ is finitely generated over F.
4. The proof of Proposition 2.1.6 shows that the $1, \alpha, \ldots, \alpha^{n-1}$ are generators of $F[\alpha]$ over F. If they are linearly dependent, then there is a non-zero polynomial in $F[x]$ of degree smaller than $m_{\alpha,F}(x)$ vanishing on α, but this is impossible.

□

Sometimes the minimal polynomial can also be useful to compute the inverse of an element:

Lemma B.2.5. *Let $F \subseteq K$ be a field extension and let $\alpha \in K^\times$ be algebraic over F. Write the minimal polynomial $m_{\alpha,F}(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in F[x]$. Then $a_0 \neq 0$ and*

$$\alpha^{-1} = -a_0^{-1}(\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1)$$

Proof. Observe that $a_0 = m_{\alpha,F}(0) \neq 0$ otherwise $m_{\alpha,F}(x)$ would be divisible by x and then it would be equal to x, meaning that $\alpha = 0$. The last formula follows from the property $m_{\alpha,F}(\alpha) = 0$, which we can also write as

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1 = -a_0.$$

□

B.2.1 The algebraic closure

Definition B.2.6. A field F is called algebraically closed if it has no non-trivial algebraic extensions: if $F \subseteq K$ is an algebraic field extension, then $F = K$.

Lemma B.2.7. *A field F is algebraically closed if and only if any polynomial in $F[x]$ factors completely as a product of linear factors in $F[x]$.*

Proof. Assume that F is algebraically closed and let $f(x) \in F[x]$ be an irreducible polynomial. We want to show that $f(x)$ is linear. The ideal $(f(x))$ is prime, hence maximal because $F[x]$ is a PID, so that the quotient $K = F[x]/(f(x))$ is a field. The natural map $K \to F$ is an embedding that realizes K as a finite extension of F of degree $\deg(f(x))$. Since K is algebraically closed, this must be the trivial extension, meaning that $\deg(f(x)) = 1$.

Conversely, assume that any irreducible polynomial $f(x)$ in $F[x]$ is linear and consider an algebraic extension $F \subseteq K$. The minimal polynomial $m_\alpha(x) \in K[x]$ is irreducible, hence of degree 1. This means that $\alpha \in K$. □

Theorem B.2.8 (Fundamental theorem of algebra)**.** *The field of complex numbers* $\mathbf{C}$ *is algebraically closed.*

Definition B.2.9 (Algebraic closure of a field)**.** Let F be a field. If F has an embedding $F \hookrightarrow \overline{F}$ into an algebraically closed field, which is algebraic over $\overline{F}$, then $\overline{F}$ is called the algebraic closure of F.

Remark B.2.10. Let $\overline{F}$ be the algebraic closure of F. Then it can be shown that if $F \subseteq K$ is an algebraic extension of F, there is an embedding $\sigma\colon K \hookrightarrow \overline{F}$ such that $\sigma_{|F} = \mathrm{id}_F$. Hence any algebraic extension can be considered a subfield of the algebraic closure.

In particular, if $\overline{F}'$ is another algebraic closure, then there are embeddings $\overline{F} \to \overline{F}'$ and $\overline{F}' \to \overline{F}$. That restrict to the identity on F. This way one can actually prove that there is an isomorphism $\overline{F} \cong \overline{F}'$ that restricts to the identity on F. In particular the algebraic closure is unique up to isomorphism and that's why we speak of *the* algebraic closure instead of *one* algebraic closure.

Example B.2.11. Consider the set

$$\overline{\mathbf{Q}} = \{\alpha \in \mathbf{C} \,|\, \alpha \text{ algebraic over } \mathbf{Q}\}$$

This is the integral closure of $\mathbf{Q}$ in $\mathbf{C}$, hence a subring. To show that it is a subfield as well, we need to show that if $\alpha \in \mathbf{C}^\times$ is algebraic over $\mathbf{Q}$, then the same is true of α^{-1}. Observe that $\alpha^{-1} \in \mathbf{Q}(\alpha)$, and since α is algebraic, $\mathbf{Q}(\alpha)$ is a finite extension of $\mathbf{Q}$. Hence α^{-1} is algebraic over $\mathbf{Q}$.

Example B.2.12. Recall that if F is a finite field then it must have cardinality p^n for a certain $p \in \mathbf{Z}_{>0}$ prime and a $n \in \mathbf{Z}_{>0}$. Furthermore, if two finite fields have the same cardinality, then they are isomorphic, so that there is up to isomorphism a unique field with p^n elements, that is denoted by $\mathbf{F}_{p^n}$. This field has characteristic p. Furthermore, we have a chain of finite extensions

$$\mathbf{F}_p \subseteq \mathbf{F}_{p^2} \subseteq \mathbf{F}_{p^3} \subseteq \dots$$

and it can be shown that $\overline{\mathbf{F}}_p = \bigcup_{n>0} \mathbf{F}_{p^n}$ is the algebraic closure of each of the $\mathbf{F}_{p^n}$.

In general, it follows from the axiom of choice that the algebraic closure exists for any field. So in the future we will consider any field F to be a subfield of its algebraic closure $\overline{F}$. Furthermore via Remark B.2.10 we will also consider any algebraic extension $F \subseteq K$ to be a sub-extension $F \subseteq K \subseteq \overline{F}$.

B.2.2 Separable extensions

Definition B.2.13. Let $F \subseteq K$ be an algebraic extension of fields. An element $\alpha \in K$ is called *separable* over F if the minimal polynomial $m_{\alpha,F}(x)$ has all distinct roots in $\bar{F}$:

$$m_{\alpha,F}(x) = (x-\alpha_1)\dots(x-\alpha_n) \text{ in } \overline{F}[x] \qquad \text{with } \alpha_i \neq \alpha_j \text{ if } i \neq j$$

The extension is called separable if every element is.

Lemma B.2.14. *Let $F \subseteq K$ be an algebraic field extension and let $\alpha \in K$ with minimal polynomial $m_{\alpha,F}(x) \in F[x]$. Consider also the formal derivative $m'_{F,\alpha}(x) \in F[x]$. Then the following are equivalent:*

1. *α is not separable over K.*
2. *$m_{F,\alpha}(x), m'_{F,\alpha}(x)$ have a common factor in $F[x]$.*
3. *$m'_{F,\alpha}(x) = 0$.*
4. *F has characteristic $p > 0$ and $m_{F,\alpha}(x) = g(x^p)$ for a certain polynomial $g(x) \in F[x]$.*

Proof. Write the factorization of $m_{\alpha,F}(x)$ in $\overline{F}[x]$ as $m_{\alpha,F}(x) = (x-\alpha_1)\dots(x-\alpha_n)$ so that

$$m'_{\alpha,F}(x) = \sum_{i=1}^{n} (x-\alpha_1)\dots\widehat{(x-\alpha_i)}\dots(x-\alpha_n), \quad m'_{\alpha,F}(\alpha_i) = \prod_{i\neq j}(\alpha_i-\alpha_j) \qquad \text{for all } i = 1,\dots,n$$

Now we prove the equivalence of the various statements:

(1) $\implies$ (2) If α is not separable, then we can assume that $\alpha_1 = \alpha_2$ and then $m'_{F,\alpha}(\alpha_1) = m_{F,\alpha}(\alpha_1) = 0$. This shows that both $m_{\alpha,F}(x), m'_{\alpha,F}(x)$ are divided by the minimal polynomial $m_{F,\alpha_1}(x)$ so they have a common factor.

(2) $\implies$ (3) Since $m_{F,\alpha}(x)$ is irreducible in $F[x]$, if it has a common factor with $m'_{F,\alpha}(x)$ it must be that $m_{F,\alpha}(x) \mid m'_{\alpha,F}(x)$. In particular, if $m'_{\alpha,F}(x) \neq 0$, then it has degree at least equal to the degree of $m_{F,\alpha}(x)$, which is impossible.

(3) $\implies$ (1) If $m'_{\alpha,F}(x) = 0$ then $m'_{\alpha,F}(\alpha_1) = 0$ so that $\alpha_i = \alpha_1$ for some $i \neq 1$.

(3) $\iff$ (4). Write $m_{F,\alpha}(x) = \sum_{k=0}^{n} a_k x^k$ so that $m'_{F,\alpha}(x) = \sum_{k=1}^{n} k a_k x^{k-1}$. Then the derivative is equal to zero if and only if $ka_k = 0$ for all $k = 1,\dots,n$. If $a_k \neq 0$, this means that $k = 0$ which is possible only if $\mathrm{char}(F) = p$ and $p \mid k$. $\square$

Corollary B.2.15. *If F is a field which is either of characteristic zero or finite, then any algebraic extension of F is separable.*

Proof. Let $F \subseteq K$ be an algebraic extension and let $\alpha \in K$ be an element. Denote by $m_{F,\alpha}(x)$ the characteristic polynomial. If α is not separable, Lemma B.2.14 shows that F has positive characteristic p and that there is a polynomial $g(x) = \sum_{i=0}^{m} b_i x^i$ such that $m_{F,\alpha}(x) = g(x^p)$. In particular this rules out the case of characteristic zero. If F is a finite field, then we know that the Frobenius homomorphism of F is surjective, hence there are $c_i \in F$ with $b_i = c_i^p$. Then we can write

$$m_{F,\alpha}(x) = g(x^p) = \sum_{i=0}^{m} c_i^p x^{pi} = \left(\sum_{i=0}^{m} c_i x^i \right)^p$$

but this is impossible since $m_{F,\alpha}(x)$ is irreducible. □

Remark B.2.16. ($\star$) A field F whose all algebraic extensions are separable is called *perfect*. One can actually show that a field F is perfect if and only if it has either characteristic zero or if it has positive characteristic p and if the Frobenius homomorphism is an isomorphism: indeed, in these two cases the proof of Corollary B.2.15 goes through unchanged. Conversely, assume that a field F has positive characteristic p and the Frobenius is not surjective, so that there is $x \in F$ such that $f(t) = t^p - x$ has no roots in F. Notice that $f'(t) = pt^{p-1} = 0$. Let $g(t)$ be a monic irreducible factor of $f(t)$, consider the field extension $K = F[t]/(g(t))$ of F and let α be the class $[t] \in K$ so that $g(t)$ is the minimal polynomial of α over F. We claim that α is not separable over F. Indeed, observe that in $K[t]$ we have $f(t) = t^p - x = t^p - \alpha^p = (t - \alpha)^p$, and since $g(t) \mid f(t)$ we see that $g(t)$ cannot have distinct roots in $\overline{F}[t]$.

Example B.2.17. ($\star$) For a concrete example of a non-separable extension let F be any field of characteristic p, take the polynomial ring $F[x]$ and consider the field $K = \operatorname{Frac} F[x] = F(x)$. The element $x \in K$ has no p-th root in K or equivalently it is not in the image of the Frobenius of K. Then the reasoning in Remark B.2.16 shows that the field extension $L = K(\sqrt[p]{x})$ is a not separable extension of K.

A nice property of separable extensions is the following

Theorem B.2.18 (Primitive element theorem)**.** *Let $F \subseteq K$ be a finite and separable extension, of fields. Then K is principal: $K = F(\alpha)$ for a certain $\alpha \in K$. In particular this applies to any finite extension of a field of characteristic zero or of a finite field.*

B.2.3 Field embeddings

One simple but useful fact about field homomorphism is that they are automatically embeddings, i.e. injective:

Lemma B.2.19. *If $f\colon F \to K$ is a field homomorphism, then it is injective.*

Proof. We know that $\operatorname{Ker} f \subseteq F$ is an ideal and it is not everything because $f(1) = 1$. Since F is a field, it must be $\operatorname{Ker} f = 0$. For another proof: let $\alpha \in F^\times$. Then α is invertible and $f(\alpha^{-1}) = f(\alpha)^{-1}$ so that $f(\alpha)$ is also invertible. Hence $f(\alpha) \neq 0$. □

A basic question in field theory is the following: let F be a field that we consider to be included in the algebraic closure $F \subseteq \overline{F}$. Let $F \subseteq K$ be a finite extension of fields: what are all the possible embeddings

$$\sigma\colon K \hookrightarrow \overline{F}, \quad \text{such that } \sigma_{|F} = \mathrm{id}_F$$

This is answered more generally by the following simple but fundamental result

Proposition B.2.20. *Let $F \subseteq F(\alpha)$ be a principal extension of fields, and let $m_{\alpha,F}(x)$ be its minimal polynomial over F. Let $\tau\colon F \hookrightarrow \overline{F}$ be a field embedding and assume that the polynomial $\sigma(m_{\alpha,F}) \in \overline{F}[x]$ splits as*

$$\sigma(m_{\alpha,F})(x) = (x-\alpha_1)\dots(x-\alpha_n), \qquad \alpha_i \in \overline{F}.$$

Then the embeddings $\sigma\colon F(\alpha) \hookrightarrow \overline{F}$ such that $\sigma_{|F} = \tau$ are all those of the form

$$\sigma_i\colon K = F(\alpha) \hookrightarrow \overline{F}, \quad \sigma_{|F} = \tau, \quad \sigma(\alpha) = \alpha_i.$$

In particular, the number of such embeddings $\sigma\colon K \hookrightarrow \overline{F}$ is equal to the number of distinct roots of $m_{F,\alpha}(x)$ in $\overline{F}[x]$.

Proof. We know that $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$, so that an embedding $\sigma\colon F(\alpha) \hookrightarrow \overline{F}$ corresponds to an homomorphism $\widetilde{\sigma}\colon F[x] \to \mathbf{C}$ such that $\widetilde{\sigma}(m_{\alpha,F}(x)) = 0$. If we ask that $\widetilde{\sigma}_{|F} = \tau$, the homomorphism $\widetilde{\sigma}$ is completely determined by the image $\widetilde{\sigma}(x) \in \mathbf{C}$ and this needs to be a root of $\sigma(m_{\alpha,F}(x))$ because we want that $\widetilde{\sigma}(m_{\alpha,F}(x)) = 0$. □

As an immediate consequence of Proposition B.2.20, we get:

Corollary B.2.21. *Let F be a field that is either of characteristic zero or finite and let $F \subseteq K$ be a finite extension of fields. Fix any field embedding $\tau\colon F \hookrightarrow \overline{F}$. Then there are $[K : F]$ distinct embeddings $\sigma\colon K \hookrightarrow \overline{F}$ such that $\sigma_{|F} = \tau$.*

Proof. By Corollary B.2.15 the extension $F \subseteq K$ is separable and then the primitive element theorem 2.2.4 shows that $K = F(\alpha)$ for a certain $\alpha \in K$. Since α is separable over F, the minimal polynomial $m_{\alpha,F}(x)$ has $\deg(m_{F,\alpha}(x)) = [K : F]$ distinct roots in $\overline{F}$. Then the statement follows immediately from Proposition B.2.20. □

Remark B.2.22 (Embeddings of number fields)**.** Consider a number field K, meaning that it is a finite extension $\mathbf{Q} \subseteq K$. First of all we notice that any field embedding $\sigma\colon K \hookrightarrow \mathbf{C}$ must satisfy $\sigma_{|\mathbf{Q}} = \mathrm{id}_{\mathbf{Q}}$ (why?) and that the image of σ must be contained in $\overline{\mathbf{Q}}$ (why?). Hence there is no difference in considering field embeddings $\mathbf{Q} \hookrightarrow \mathbf{C}$ and $\mathbf{Q} \hookrightarrow \overline{\mathbf{Q}}$, and Corollary B.2.21 shows that there are precisely $[K : \mathbf{Q}]$ embeddings $K \hookrightarrow \mathbf{C}$ and these can be determined explicitly as in Proposition B.2.20.

Example B.2.23. Consider the extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{d})$, where $d \in \mathbf{Z}$ is a square-free integer. The minimal polynomial of $\sqrt{d}$ is $m_{\alpha,\mathbf{Q}}(x) = x^2 - d$ and its roots are $\pm\sqrt{d}$. Hence there are two field embeddings $\mathbf{Q}(\sqrt{d}) \hookrightarrow \mathbf{C}$.

$$\mathrm{id}_{\mathbf{Q}(\sqrt{d})}\colon a + b\sqrt{d} \mapsto a + b\sqrt{d}, \qquad \sigma\colon a + b\sqrt{d} \mapsto a - b\sqrt{d},$$

Notice that the image of both these embeddings is again the same field $\mathbf{Q}(\sqrt{d})$ and these two embeddings give rise to two automorphisms $\mathbf{Q}(\sqrt{d}) \to \mathbf{Q}(\sqrt{d})$.

Example B.2.24. Let's look at the extension $\mathbf{Q}(\sqrt[3]{2})$ of $\mathbf{Q}$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ respectively, and

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$$

where $\zeta_3 = e^{2\pi i/3}$. The embeddings $\sigma\colon \mathbf{Q}(\sqrt[3]{2}) \hookrightarrow \mathbf{C}$ are

$$\sigma_i : \mathbf{Q}(\sqrt[3]{2}) \hookrightarrow \overline{\mathbf{Q}}, \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}, \omega^{i-1}\sqrt[3]{2}, \quad \text{for } i = 1, 2, 3$$

In particular, we see the only embedding that has still image inside $\mathbf{Q}(\sqrt[3]{2})$ is the identity

B.3 Galois Theory

We observe that to any field extension we can associate a group: we consider only the case where the base field is either finite or of characteristic zero for simplicity, but the general case is not much different.

Definition B.3.1 (Galois group)**.** Let F be a field that is either of characteristic zero or finite and let $F \subseteq K$ be a finite field extension. The Galois group of this extension is

$$\mathrm{Aut}(K/F) = \{\sigma\colon K \to \overline{F} \text{ embedding } \mid \sigma_{|F} = \mathrm{id}_F, \sigma(K) \subseteq K\}$$

This set is actually a group:

Lemma B.3.2. *With the previous notation any $\sigma \in \mathrm{Aut}(K/F)$ is an isomorphism $\sigma\colon K \to K$. In particular $\mathrm{Aut}(K/F)$ is a group with respect to the composition.*

Proof. If $\sigma\colon K \to K$ is a field embedding such that $\sigma_{|F} = \mathrm{id}_K$ then we can also see σ as an F-linear map of the vector space K, which is of finite dimension over K. Since σ is injective, it must be surjective as well. □

This group is related to an important propery of field extensions:

Definition B.3.3 (Normal extension)**.** Let F be a field that is either finite or of characteristic zero. A finite extension $F \subseteq K$ is called *normal* if for every embedding $\sigma : K \hookrightarrow \overline{F}$ s.t. $\sigma_{|F} = \mathrm{id}_F$, it holds that $\sigma(K) \subseteq K$.

Remark B.3.4. ($\star$) The previous definition makes sense for all finite extensions. In general, a finite extension $F \subseteq K$ is called *Galois* if it is normal and separable. If the base field F is either finite or of characteristic zero, then all finite extensions are automatically separable so that being normal is the same as being Galois.

Proposition B.3.5. *Let F be a field that is either of characteristic zero or finite and let $F \subseteq K$ be a finite extension. Then the following statements are equivalent.*

1. *$F \subseteq K$ is normal.*
2. *If $K = F(\alpha)$, the minimal polynomial $m_\alpha(x)$ splits as a product of linear factors in $K[x]$:*

$$m_{\alpha,F}(x) = (x - \alpha_1)\dots(x - \alpha_n), \quad \alpha_i \in K$$

3. $K = F(\alpha_1, \ldots, \alpha_n)$ *where* $P(x) = (x - \alpha_1) \ldots (x - \alpha_n) \in F[x]$.

Proof. (1) $\implies$ (2): Consider the splitting $m_{\alpha,F}(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ in $\overline{F}[x]$. Then all the embeddings $\sigma\colon F(\alpha) \hookrightarrow \overline{F}$ such that $\sigma_{|F} = \mathrm{id}_F$ satisfy $\sigma(\alpha) = \alpha_i$ for some i. Since all these embeddings have image in $F(\alpha)$ by definition, it must be that $\alpha_i \in F(\alpha)$ for all i. This shows that K is a normal extension, and since it is separable it is also Galois.

(2) $\implies$ (3): Take $P(x) = m_{F,\alpha}(x)$ where $\alpha \in K$ is any element such that $K = F(\alpha)$ (it exists because of the primitive element theorem).

(3) $\implies$ (1): If $\sigma\colon K \hookrightarrow \overline{F}$ is such that $\sigma_F = \mathrm{id}_F$ then σ must send the roots of $P(x)$ into other roots of $P(x)$. Hence it must send K to K. □

Example B.3.6. The extension $\mathbf{Q}(\sqrt[3]{2})$ is not Galois over $\mathbf{Q}$, but the larger extension $\mathbf{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ is.

Remark B.3.7. Let F be a field that is either finite or of characteristic zero and consider a finite field extension $F \subseteq K$. By the Primitive Element Theorem, there is $\alpha \in K$ such that $K = F(\alpha)$ and then the embeddings $\sigma\colon F(\alpha) \hookrightarrow \overline{F}$ such that $\sigma_F = \mathrm{id}_F$ correspond to the roots of the minimal polynomial $m_{F,\alpha}(x)$ in $\overline{F}$. The embeddings that lie in $\mathrm{Aut}(K/F)$ correspond to the roots that lie in K. Hence we

$$|\operatorname{Aut}(K/F)| \leq |\{\sigma\colon K \hookrightarrow \overline{F} \mid \sigma_{|F} = \mathrm{id}_F\}| = [K : F]$$

and the extension is normal if and only if this is an equality.

Example B.3.8. Let $F = \mathbf{F}_{p^n}$ be a finite field with p^n elements, where $p > 0$ is a positive prime number. Then this is a separable extension $\mathbf{F}_p \subseteq \mathbf{F}_{p^n}$ of degree n. We claim that this is a normal extension and that the Galois group is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ and generated by the Frobenius

$$\mathrm{Frob}\colon \mathbf{F}_{p^n} \longrightarrow \mathbf{F}_{p^n}$$

Indeed, the Frobenius lies in $\mathrm{Aut}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ because of Lemma B.1.4 so we just need to show that this has order n, because then

$$n = |(\mathrm{Frob})| \leq |\operatorname{Aut}(\mathbf{F}_{p^n}/\mathbf{F}_p)| \leq [\mathbf{F}_p^n : \mathbf{F}_p] = n$$

Assume that $k \in \mathbf{N}$ is such that $\mathrm{Frob}^k = \mathrm{id}$. This means that $x^{p^k} - x = 0$ for all $x \in \mathbf{F}_{p^n}$. Since this polynomial can have at most p^k roots in the field $\mathbf{F}_{p^n}$ it must be that $p^n \leq p^k$ so that $n \leq k$.

Remark B.3.9. If $F \subseteq F' \subseteq K$ is a tower of finite field extensions, and if $F \subseteq K$ is normal, then the extension $F' \subseteq K$ is normal as well: indeed, any field embedding $\sigma\colon K \hookrightarrow \overline{F} = \overline{F'}$ that is the identity on F' is also the identity on F,so that $\sigma(K) \subseteq K$. However, it is not true in general that $F \subseteq F'$ is a normal extension.

B.3.1 The fundamental theorem of Galois theory

Let F be a field that is either of characteristic zero or finite and let $F \subseteq K$ be a finite extension. For every subgroup $G < \mathrm{Aut}(K/F)$ we define its *fixed field* as the subset

$$\mathrm{Fix}(G) = K^G = \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \text{ for all } \sigma \in G\}$$

It is easy to check that this is an intermediate field extension $F \subseteq \mathrm{Fix}(G) \subseteq K$. Conversely, for an intermediate extension $K \subseteq F' \subseteq F$ we obtain a subgroup

$$\mathrm{Aut}(K/F') < \mathrm{Aut}(K/F).$$

Proposition B.3.10. *Let F be a field that is either of characteristic zero or finite and let $F \subseteq K$ be a finite extension. Then this extension is normal if and only if*

$$\mathrm{Fix}(\mathrm{Aut}(K/F)) = F.$$

Proof. ($\star$) Consider the fixed field $F' = \mathrm{Fix}(\mathrm{Aut}(K/F))$ and let $[F' : F] = m$. Let also $\sigma'_1, \dots, \sigma'_m$, be all the embeddings $\sigma' \colon F' \hookrightarrow \overline{F}$ such that $\sigma'_{|F} = \mathrm{id}_F$. We can assume $\sigma'_1 = \mathrm{id}_{F'}$. We can lift each one of these to embeddings $\sigma_1, \dots, \sigma_m \colon K \hookrightarrow \overline{F}$ such that $\sigma_{|F'} = \sigma'_F$ and we can also assume that $\sigma_1 = \mathrm{id}_F$. If K/F is normal, then $\sigma_i \in \mathrm{Aut}(K/F)$ by construction so that $(\sigma_i)_{|F'} = \mathrm{id}_{F'} = \sigma'_1$ for all i. Hence $m = 1$, meaning that $F' = F$.

Conversely, assume that $F' = F$ and let $\alpha \in K$ be an element such that $K = F(\alpha)$. Consider the polynomial

$$P(x) = \prod_{\sigma \in \mathrm{Aut}(K/F)} (x - \sigma(\alpha))$$

by construction, this polynomial is invariant by the action of $\mathrm{Aut}(K/F)$ hence its coefficients must be in $F' = F$. Furthermore, $P(\alpha) = 0$ (why?) so that $m_{F,\alpha}(x) \mid P(x)$. Hence

$$[K : F] = \deg m_{F,\alpha}(x) \leq \deg P(x) = |\,\mathrm{Aut}(K/F)| \leq [K : F]$$

so that it must be $|\,\mathrm{Aut}(K/F)| = [K : F]$ so that the extension is normal. □

A vast generalization of this statement is:

Theorem B.3.11 (Fundamental theorem of Galois theory)**.** *Let F be a field that is either of characteristic zero or finite and let $F \subseteq K$ be a finite and normal extension. Then*

(i) There is a bijection

$$\left\{ \begin{array}{c} \textit{subgroups} \\ \textit{of } \mathrm{Aut}(K/F) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{intermediate extensions} \\ F \subseteq F' \subseteq K \end{array} \right\}, \quad G \longmapsto \mathrm{Fix}(G), \mathrm{Aut}(K/F') \longleftarrow F'.$$

such that the index of the subgroup corresponds to the degree of the intermediate extension:

$$[\mathrm{Aut}(K/F) : \mathrm{Aut}(K/F')] = [F' : F]$$

(ii) The extension $F \subseteq F'$ is normal if and only if $\mathrm{Aut}(K/F') \subseteq \mathrm{Aut}(K/F)$ is normal. In this case there is an isomorphism

$$\mathrm{Aut}(K/F)/\,\mathrm{Aut}(K/F') \cong \mathrm{Aut}(F'/F).$$

Proof. ($\star$) We prove point (i) first. We first show that if $F \subseteq F' \subseteq K$ is an intermediate extension,then $F' = \mathrm{Fix}(\mathrm{Aut}(K/F'))$. Notice that the extension $F' \subseteq K$ is normal because Remark B.3.9 and then the statement follows from Proposition B.3.10. Now we show that if $G \subseteq \mathrm{Aut}(K/F)$ is a finite subgroup, then $G = \mathrm{Aut}(K/\,\mathrm{Fix}(G))$. It is clear that $G \subseteq \mathrm{Aut}(K/\,\mathrm{Fix}(G))$ so what we need to show is that $|G| = |\,\mathrm{Aut}(K/\,\mathrm{Fix}(G))|$. Set $F' = \mathrm{Fix}(G)$ and let $\alpha \in K$ such that $K = F'(\alpha)$. As in the proof of Proposition B.3.10, consider the polynomial

$$P(x) = \prod_{\sigma \in G} (x - \sigma(\alpha))$$

By construction, this has coefficients in $F' = \mathrm{Fix}(G)$ and $P(\alpha) = 0$ so that $m_{F',\alpha}(x) | P(x)$. This shows that

$$|\operatorname{Aut}(K/F')| \leq [K : F'] = \deg(m_{F',\alpha}(x)) \leq \deg P(x) = |G| \leq |\operatorname{Aut}(K/F')|$$

so that $|G| = |\operatorname{Aut}(K/\operatorname{Fix}(G))|$. This concludes the proof that the map is a bijection. For the statement about the degree, let $G \subseteq \operatorname{Aut}(K/F)$ be any subgroup and let $F' = \mathrm{Fix}(G)$. Then

$$[\operatorname{Aut}(K/F) : G] = \frac{|\operatorname{Aut}(K/F)|}{|G|} = \frac{|\operatorname{Aut}(K/F)|}{|\operatorname{Aut}(K/F')|} = \frac{[K : F]}{[K : F']} = [F' : F].$$

Now we consider point (ii). Fix an intermediate extension $F \subseteq F' \subseteq K$ and observe that any embedding $\sigma' \colon F' \to \overline{F}$ with $\sigma'_{|F'} = \mathrm{id}_{F'}$ can be extended to an embedding $\sigma \colon K \hookrightarrow \overline{F}$, which is an element of $\operatorname{Aut}(K/F)$ since $F \subseteq K$ is normal. This shows that there is a surjective restriction map

$$r \colon \operatorname{Aut}(K/F) \longrightarrow \{\sigma' \colon F' \hookrightarrow \overline{F} \,|\, \sigma'_{F'} = \mathrm{id}_{F'}\}, \quad \sigma \mapsto \sigma_{|F'}$$

If we define the set

$$N = r^{-1}(\operatorname{Aut}(F'/F)) = \{\sigma \in \operatorname{Aut}(K/F) \,|\, \sigma(F') \subseteq F'\}$$

this gives another surjective restriction map

$$r \colon N \longrightarrow \operatorname{Aut}(F'/F)$$

Furthermore, it is easy to see that N is a subgroup of $\operatorname{Aut}(K/F)$ and that the restriction map is a group homomorphism with kernel equal to $\operatorname{Aut}(K/F')$. This shows that $\operatorname{Aut}(K/F')$ is a normal subgroup in N and that $N/\operatorname{Aut}(K/F') \cong \operatorname{Aut}(F'/F)$. To conclude we are going to show the equivalences

$$F \subseteq F' \text{ is normal} \iff \operatorname{Aut}(K/F) = N \iff \operatorname{Aut}(F'/F) \subseteq \operatorname{Aut}(K/F') \text{ is normal}$$

For the first equivalence, observe that $F \subseteq F'$ is a normal extension if and only if any embedding $\sigma \colon F' \hookrightarrow \overline{F}$ with $\sigma_{|F} = \mathrm{id}_F$ is actually in $\operatorname{Aut}(F'/F)$. By construction, this means that $N = \operatorname{Aut}(K/F)$ (why?).

On the other hand, observe that $\operatorname{Aut}(K/F')$ is a normal subgroup in $\operatorname{Aut}(K/F)$ if and only if for all $\sigma \in \operatorname{Aut}(K/F'), \tau \in \operatorname{Aut}(K/F)$ we have $\tau^{-1}\sigma\tau \in \operatorname{Aut}(K/F')$, meaning $\sigma(\tau(x)) = \tau(x)$ for all $x \in F'$. This means that for all $\tau \in \operatorname{Aut}(K/F)$ we have $\tau(F') \subseteq \mathrm{Fix}(\operatorname{Aut}(K/F')) = F'$, where the last equality follows from (i). In other words $\operatorname{Aut}(K/F')$ is a normal subgroup in $\operatorname{Aut}(K/F)$ if and only if $N = \operatorname{Aut}(K/F)$. □