Introduction to Algebraic Number Theory

Philippe Michel December 18, 2024

with some minor additions and changes by Manuel Luethi

Table des matieres

CHAPTER I

Fermat's equation

"J'ai trouvé une merveilleuse démonstration de cette proposition,
mais la marge est trop étroite pour la contenir."

I.1. Introduction

Diophantine equations are equations of the shape

$$P(x_1, \dots, x_r) = 0,$$

where $P(X_1, \dots, X_r)$ is a polynomial in a number of variables with integral coefficients and where one looks for solutions in integers $(x_1, \dots, x_r) \in \mathbb{Z}^r$. Fermat's equations are the diophantine equations in three unknowns given by

$$x^n + y^n = z^n,\ (x, y, z) \in \mathbb{Z}^3 \tag{I.1}$$

for $n \in \mathbb{N}_{\geqslant 1}$ an integer. Observe that, since the polynomial $X^n + Y^n - Z^n$ is homogeneous, whenever $(x_0, y_0, z_0) \in \mathbb{Z}^3$ is a solution, then for any $a \in \mathbb{Z}$ the triple (ax_0, ay_0, az_0) is also a solution. So it is natural to search for the *primitive* solutions (x, y, z), i.e., solutions for which x, y, z are coprime (i.e., $\gcd(x, y, z) = 1$).

The case $n = 2$,

$$x^2 + y^2 = z^2,\ (x, y, z) \in \mathbb{Z}^3,\ \gcd(x, y, z) = 1, \tag{I.2}$$

is known since antiquity and there is a simple procedure to find all its solutions.

THEOREM. *All primitive solution to the equation* (I.2) *are obtained as follows.*

(1) Take $t = u/v$ a rational number (written as an irreducible fraction, $\gcd(u, v) = 1$), and let D_t the line with slope t and passing through the point $(1, 0)$, i.e., the line given by the equation

$$V = t(U - 1).$$

(2) The line D_t intersect the unit circle

$$U^2 + V^2 = 1$$

in two distinct points: $(1, 0)$ and

$$P_t = \left(\frac{t^2 - 1}{t^2 + 1}, -\frac{2t}{t^2 + 1}\right) = \left(\frac{u^2 - v^2}{u^2 + v^2}, -\frac{2uv}{u^2 + v^2}\right)$$

and P_t has rational coordinates.

(3) The triple $(u^2 - v^2, -2uv, u^2 + v^2)$ is a primitive solution to (I.2).

In particular the equation (I.2) *admits infinitely many solutions.*

Fermat was the first to realize that for $n \geqslant 3$ the situation is very different and he claimed his famous *Fermat's Last Theorem (FLT)*.

– *"Un cube n'est jamais la somme de deux cubes,*
une puissance quatrième n'est jamais la somme de deux puissances quatrièmes
et plus généralement aucune puissance supérieure à 2 n'est la somme de deux puissances analogues."

He then established the FLT for $n = 4$ and for the other n's wrote his famous sentence.

In modern terms Fermat's claim is rewritten as follows.

THEOREM. *For $n \geqslant 3$ the only primitive solutions (x, y, z) to Fermat's equation (I.1) are contained in the set*

$$\{(\varepsilon_1, \varepsilon_2, 0),\ (\varepsilon_1, 0, \varepsilon_2),\ (0, \varepsilon_1, \varepsilon_2) \colon \varepsilon_1, \varepsilon_2 \in \{\pm 1\}\}.$$

Since their introduction Fermat's equations and the search for their solutions have captured the minds of many mathematicians and have indeed been largely responsible for the development of algebraic number theory. It is only in 1995 that Andrew Wiles proved Fermat's claim, the culmination of a serie of tremendous developments that have taken place during the 19th and 20th century.

In this chapter, as a warm-up, we will discuss the very first cases of Fermat's equation and will start with a variant of the case $n = 2$ due to Fermat.

I.2. Sums of two squares

THEOREM I.1 (Fermat). *An integer $n \in \mathbb{Z} - \{0\}$ is a sum of two squares, i.e.,*

$$n = a^2 + b^2,\ a, b \in \mathbb{Z},$$

if and only if the following are true.

- *$n > 0$.*
- *n is the product of a square and a (possibly empty) product of prime numbers $\equiv 1, 2 \pmod 4$.*

In particular a prime $p \geqslant 2$ is a sum of two squares if and only if $p \equiv 1, 2 \pmod 4$.

Given a complex number $z = a + ib$, then

$$z.\overline{z} = |z|^2 = a^2 + b^2,$$

Thus, given $n \in \mathbb{N}$, the question whether n is a sum of two squares is equivalent to the question whether there exists $z = a + ib \in \mathbb{Z} + i\mathbb{Z}$ such that

$$z.\overline{z} = n.$$

I.2.1. The ring of Gaussian integers.

PROPOSITION I.2.1. *The additive subgroup of $\mathbb{C}$*

$$\mathbb{Z} + i\mathbb{Z} = \{a + ib \colon a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$, called the ring of Gaussian integers. We also have the equality

$$\mathbb{Z} + i\mathbb{Z} = \mathbb{Z}[i] = \{P(i) \colon P(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 \in \mathbb{Z}[X]\}.$$

Moreover the field of fractions of $\mathbb{Z}[i]$ is

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \mathbb{Q} + i\mathbb{Q}.$$

This field is called the field of Gaussian numbers.

PROOF. Clearly $\mathbb{Z} + i\mathbb{Z}$ is an additive subgroup containing $\mathbb{Z}$, hence $0, 1$.

Given $a + ib, c + id \in \mathbb{Z} + i\mathbb{Z}$, we have

$$(a + ib).(c + id) = (ac - bd) + i(bc + ad) \in \mathbb{Z} + i\mathbb{Z},$$

hence $\mathbb{Z} + i\mathbb{Z}$ is a ring. Note that $\mathbb{Z} + i\mathbb{Z}$ is the image of the evaluation at i restricted to the subspace of polynomials of degree at most one inside $\mathbb{Z}[X]$. Therefore $\mathbb{Z} + i\mathbb{Z} \subset \mathbb{Z}[i]$.

We have in fact

$$\mathbb{Z} + i\mathbb{Z} = \mathbb{Z}[i]$$

as $\mathbb{Z}[i]$ is the smallest subring of $\mathbb{C}$ containing both $\mathbb{Z}$ and i. Alternatively, one uses that $i^2 = -1$ which implies that for any

$$P(X) = a_{2d}X^{2d} + a_{2d-1}X^{2d-1} + \cdots + a_0 \in \mathbb{Z}[X]$$

we have

$$P(i) = a_{2d}(-1)^d + a_{2d-1}(-1)^{d-1}.i + \cdots + a_0 \in \mathbb{Z} + i\mathbb{Z}.$$

Clearly

$$\mathbb{Q} + i\mathbb{Q} \subset \mathbb{Q}[i] \subset \mathbb{Q}(i) = \mathrm{Frac}(\mathbb{Z}[i])$$

and the ring $\mathbb{Q} + i\mathbb{Q}$ is a a field since it is stable under addition and multiplication and for non-zero $a + ib \in \mathbb{Q} + i\mathbb{Q}$ we have

$$(a + ib)^{-1} = \frac{a - ib}{a^2 + b^2} \in \mathbb{Q} + i\mathbb{Q} - \{0\}.$$

Therefore, $\mathbb{Q}(i)$ being the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and i, we have $\mathbb{Q}(i) \subset \mathbb{Q} + i\mathbb{Q}$ and hence equality. □

Definition I.1. *The norm on $\mathbb{Q}(i)$ is the map*

$$\mathrm{Nr}(z) = z.\overline{z} = a^2 + b^2.$$

Proposition I.2.2. *The norm is $\mathbb{Q}$-valued, multiplicative, definite (i.e., $z = 0 \iff \mathrm{Nr}(z) = 0$), and $\mathrm{Nr}(\mathbb{Z}[i]) \subset \mathbb{Z}_{\geqslant 0}$.*

Proposition I.2.3. *We have*

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{z \in \mathbb{Z}[i],\ \mathrm{Nr}(z) = 1\}.$$

Proof. If $z \in \mathbb{Z}[i]^\times$ is a unit, by multiplicativity of the norm, we have $\mathrm{Nr}(z) \in \mathbb{Z}^\times = \{\pm 1\}$, hence $\mathrm{Nr}(z) = a^2 + b^2 = 1$ which implies that $z \in \{\pm 1, \pm i\}$ and these are obviously units. Alternatively if $\mathrm{Nr}(z) = 1$ then $z.\overline{z} = 1$ so $z^{-1} = \overline{z} \in \mathbb{Z}[i]^\times$. □

Another consequence of the multiplicativity of the norm is the following:

Corollary I.2.4. *If m, n are sums of two squares then so is $m.n$.*

The converse is not true: $9 = 3.3$ is a sum of two squares but 3 is not. Nevertheless there is a partial converse which we will prove later.

Proposition I.2.5. *If $(m, n) = 1$, then*

$$mn = \square + \square \iff m = \square + \square \text{ and } n = \square + \square.$$

To prove this we will need the following fundamental result.

Proposition I.2.6. *The ring $\mathbb{Z}[i]$ is a Principal Ideal Domain (PID): $\mathbb{Z}[i]$ is a domain (i.e., $z.w = 0 \implies z$ or $w = 0$) and every ideal $\mathfrak{q} \subset \mathbb{Z}[i]$ is generated by one element, i.e., there exists $q \in \mathbb{Z}[i]$ such that*

$$\mathfrak{q} = (q) = q\mathbb{Z}[i].$$

Proof. This follows from a stronger property, namely $\mathbb{Z}[i]$ is a euclidean ring:

$$\forall z, q \in \mathbb{Z}[i],\ q \neq 0,\ \exists k, r \in \mathbb{Z}[i] \text{ such that } \mathrm{Nr}(r) < \mathrm{Nr}(q),\ z = qk + r.$$

There exists $k \in \mathbb{Z}[i]$ such that

$$|z/q - k| < 1.$$

Indeed any point—and thus also z/q—in $\mathbb{C}$ is at distance $\leqslant \sqrt{2}/2 < 1$ from an element k of $\mathbb{Z}[i]$. We choose

$$r = z - kq \in \mathbb{Z}[i].$$

Then

$$|r| = |z - qk| < |q| \iff \mathrm{Nr}(z - qk) < \mathrm{Nr}(q).$$

This proves that $\mathbb{Z}[i]$ is euclidean.

Let $\mathfrak{q} \subset \mathbb{Z}[i]$ be a non-zero ideal. Let $0 \neq q \in \mathfrak{q}$ such that $\mathrm{Nr}(q)$ is minimal among the norms of elements in $\mathfrak{q}$ (such q exists since Nr takes values in $\mathbb{N}$). Let $0 \neq b \in \mathfrak{q}$, then there exists $r \in \mathbb{Z}[i]$ such that $b = qk + r$ with $\mathrm{Nr}(r) < \mathrm{Nr}(q)$ and $r = b - qk \in \mathfrak{q}$; therefore $r = 0$ and $b = qr \in q\mathbb{Z}[i]$. As b was arbitrary, we obtain that

$$q\mathbb{Z}[i] \subset \mathfrak{q} \subset q\mathbb{Z}[i].$$

□

PROPOSITION I.2.7. *Let $\mathfrak{q} = (q)$ be a non zero ideal generated by $q = a + ib \in \mathbb{Z}[i]$, then $\mathbb{Z}[i]/\mathfrak{q}$ is finite and*

$$|\mathbb{Z}[i]/\mathfrak{q}| = \mathrm{Nr}(q) = a^2 + b^2.$$

PROOF. One has

$$\mathfrak{q} = (a + ib)(\mathbb{Z} + i\mathbb{Z}) = \mathbb{Z}(a + ib) + \mathbb{Z}(-b + ia)$$

and the index of $\mathfrak{q}$ in $\mathbb{Z}[i]$ is the index of $\mathbb{Z}(a, b) + \mathbb{Z}(-b, a)$ in $\mathbb{Z}^2 = \mathbb{Z}(1, 0) + \mathbb{Z}(0, 1)$. As of the discussion in Section A.2.1, this index is equal to

$$\left|\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right| = a^2 + b^2.$$

□

I.2.2. Prime factorisation in a PID. Let us recall that for a general ring $\mathcal{O}$ we have the following basic operations/definitions regarding the set of ideals:

- Given two ideals $\mathfrak{m}, \mathfrak{n} \subset \mathcal{O}$, we say that $\mathfrak{m}$ *divides* $\mathfrak{n}$ if $\mathfrak{n} \subset \mathfrak{m}$. This relation is denoted by
$$\mathfrak{m}|\mathfrak{n}.$$
- Given a subset $M \subseteq \mathcal{O}$, we denote by (M) or $(m\colon m \in M)$ the ideal generated by M, i.e., the smallest ideal in $\mathcal{O}$ containing M.
- Given two ideals $\mathfrak{m}, \mathfrak{n} \subset \mathcal{O}$ we define the following ideals:
$$\mathfrak{m} + \mathfrak{n} := (m + n\colon m \in \mathfrak{m}, n \in \mathfrak{n}) = (\mathfrak{m}, \mathfrak{n}),$$
$$\mathfrak{m}.\mathfrak{n} := (m.n\colon m \in \mathfrak{m}, n \in \mathfrak{n}) \subset \mathfrak{m} \cap \mathfrak{n}.$$
- A proper ideal $\mathfrak{p} \subsetneq \mathcal{O}$ is prime if $\mathcal{O}/\mathfrak{p}$ is a domain, i.e., for any $a, b \in \mathcal{O}$, if $a.b \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. The set of prime ideals is denoted by
$$\mathrm{Spec}(\mathcal{O})$$
(for "spectrum") and a typical non-zero prime will be denoted $\mathfrak{p}$.
- A proper ideal $\mathfrak{m} \subsetneq \mathcal{O}$ is maximal if it is maximal, relative to inclusion, amongst all proper ideals (i.e., it is not contained in any distinct proper ideal). Equivalently, an ideal $\mathfrak{m}$ is maximal if $\mathcal{O}/\mathfrak{m}$ is a field (in particular a maximal ideal is a prime ideal). The set of maximal ideals is denoted by
$$\mathrm{Spec}_{\max}(\mathcal{O}).$$

We recall that the ring $\mathcal{O}$ is a *domain* if for all $a, b \in \mathcal{O}$ we have

$$a.b = 0_{\mathcal{O}} \implies a = 0_{\mathcal{O}} \text{ or } b = 0_{\mathcal{O}}.$$

DEFINITION I.2. *A Principal Ideal Domain (PID) $\mathcal{O}$ is a ring which is a domain and for which every ideal $\mathfrak{m} \subset \mathcal{O}$ is principal, i.e., of the form*

$$\mathfrak{m} = (m) = m.\mathcal{O} = \{m.a,\ a \in \mathcal{O}\}$$

for some $m \in \mathcal{O}$.

THEOREM I.2 (Factorisation in PIDs). *In a PID $\mathcal{O}$, every non-zero prime ideal is maximal.*

Moreover, for every ideal $\mathfrak{m}$, there exists a unique tuple of natural integers $(v_\mathfrak{p}(\mathfrak{m}))_{\mathfrak{p}\ prime}$ indexed by $\mathrm{Spec}(\mathcal{O})$ *such that $v_\mathfrak{p}(\mathfrak{m}) = 0$ for all but finitely many $\mathfrak{p}$ and such that $\mathfrak{m}$ can be written as the following (finite) product:*

$$\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})},$$

where $\mathfrak{p}^0 := \mathcal{O}$ and the product runs over the non-zero prime ideals.

Alternatively, call a non-zero element $p \in \mathcal{O}$ "prime" if it is the generator of a prime ideal $\mathfrak{p} = p\mathcal{O}$ and for every non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}$ choose an associated prime p (i.e., $\mathfrak{p} = (p) = p\mathcal{O}$). By considering the prime factorisation of the principal ideal $\mathfrak{p} = (m)$ generated by $m \in \mathcal{O}$, i.e.,

$$(m) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})} = \prod_\mathfrak{p} (p)^{v_{(p)}((m))},$$

we obtain that any $m \in \mathcal{O}$ can be written as a product of prime powers:

$$m = u.\prod_\mathfrak{p} p^{v_p(m)},$$

where $u \in \mathcal{O}^\times$ and $v_p(m) = v_\mathfrak{p}(\mathfrak{m})$. Moreover, for non-zero $m \in \mathcal{O}$, this factorisation is unique (given the choice of a generator p for each prime ideal $\mathfrak{p}$).

REMARK I.1. The integer $v_\mathfrak{p}(\mathfrak{m})$ is called the valuation of $\mathfrak{m}$ at the prime ideal $\mathfrak{p}$ (or the $\mathfrak{p}$-adic valuation of $\mathfrak{m}$) and likewise for $v_p(m)$.

Because of this the standard factorisation properties of $\mathbb{Z}$ extend to a general PID $\mathcal{O}$. Let $\mathfrak{m}, \mathfrak{n} \subset \mathcal{O}$ non-zero ideals. Then

$$\mathfrak{m}|\mathfrak{n} \iff \forall \mathfrak{p},\ v_\mathfrak{p}(\mathfrak{m}) \leqslant v_\mathfrak{p}(\mathfrak{n}),$$

$$\mathfrak{m}.\mathfrak{n} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m}) + v_\mathfrak{p}(\mathfrak{n})},$$

$$[\mathfrak{m}, \mathfrak{n}] := \text{largest ideal contained in } \mathfrak{m} \text{ and } \mathfrak{n} = \mathfrak{m} \cap \mathfrak{n} = \prod_\mathfrak{p} \mathfrak{p}^{\max(v_\mathfrak{p}(\mathfrak{m}), v_\mathfrak{p}(\mathfrak{n}))},$$

$$(\mathfrak{m}, \mathfrak{n}) := \text{smallest ideal containing both } \mathfrak{m} \text{ and } \mathfrak{n} = \mathfrak{m} + \mathfrak{n} = \prod_\mathfrak{p} \mathfrak{p}^{\min(v_\mathfrak{p}(\mathfrak{m}), v_\mathfrak{p}(\mathfrak{n}))}.$$

In particular, we obtain the following equivalent characterization of coprimality of ideals:

$$(\mathfrak{m}, \mathfrak{n}) = \mathcal{O} \iff \forall \mathfrak{p},\ v_\mathfrak{p}(\mathfrak{m}).v_\mathfrak{p}(\mathfrak{n}) = 0.$$

I.2.3. Proof of Proposition I.2.5. Consider two integers $m, n \in \mathbb{N}$ such that $(m, n) = 1$ (in the usual sense) and suppose that $m.n = \square + \square$ or in other terms

$$m.n = (a + ib)(a - ib),\ a + ib \in \mathbb{Z}[i].$$

Let

$$\mathfrak{a} = (a + ib)\mathbb{Z}[i].$$

Applying complex conjugation we have

$$\overline{\mathfrak{a}} = \overline{(a + ib)\mathbb{Z}[i]} = (a - ib)\overline{\mathbb{Z}[i]} = (a - ib)\mathbb{Z}[i].$$

Observe that the ideals (m) and (n) are coprime in $\mathbb{Z}[i]$:

$$1 \in m\mathbb{Z} + n\mathbb{Z} \Longrightarrow 1 \in m\mathbb{Z}[i] + n\mathbb{Z}[i] = (m) + (n).$$

In other terms their decompositions into prime factors are disjoint.

Since $\mathfrak{a}|(mn) = (m).(n)$ we have

$$\mathfrak{a} = (\mathfrak{a}, (m)).(\mathfrak{a}, (n))$$

and likewise

$$\overline{\mathfrak{a}} = (\overline{\mathfrak{a}}, (m)).(\overline{\mathfrak{a}}, (n))$$

and

$$(m).(n) = (\mathfrak{a}, (m))(\overline{\mathfrak{a}}, (m))(\mathfrak{a}, (n))(\overline{\mathfrak{a}}, (n)).$$

Again, since (m) and (n) are coprime we conclude that

$$(m) = (\mathfrak{a}, (m))(\overline{\mathfrak{a}}, (m)),\ (n) = (\mathfrak{a}, (n))(\overline{\mathfrak{a}}, (n)).$$

Since $\overline{m} = m$ we have

$$(\overline{\mathfrak{a}}, (m)) = (\overline{\mathfrak{a}}, \overline{(m)}) = \overline{(\mathfrak{a}, (m))}$$

so if we write

$$(\mathfrak{a}, (m)) = (a' + ib')\mathbb{Z}[i]$$

we have

$$(\overline{\mathfrak{a}}, (m)) = \overline{(\mathfrak{a}, (m))} = (a' - ib')\mathbb{Z}[i].$$

Since

$$(m) = (\mathfrak{a}, (m))(\overline{\mathfrak{a}}, (m)) = (a' + ib')(a' - ib')\mathbb{Z}[i] = (a'^2 + b'^2)\mathbb{Z}[i],$$

there is some $u' \in \mathbb{Z}[i]$ such that

$$m = u'.(a' + ib').(a' - ib') = u'(a'^2 + b'^2).$$

Since $m \geqslant 1$ we have $u' \geqslant 1$ so $u' = 1$ and $m = \square + \square$. Exchanging the roles of m and n we conclude. □

I.2.4. Gaussian primes. Proposition I.2.5 reduces the proof of Fermat's theorem to the case where $m = p$ is a prime and we have to show that

$$p = \square + \square \iff p \equiv 1, 2 \,(\mathrm{mod}\, 4).$$

Such prime are called Gaussian primes.

Observe that

$$2 = 1^2 + 1^2 = z_2\overline{z_2},\ z_2 = 1 + i.$$

It is therefore sufficient to show that

THEOREM I.3. *Let p be an odd prime. The following are equivalent.*

(1) $p = \square + \square$.
(2) $p \equiv 1 \,(\mathrm{mod}\, 4)$.
(3) -1 *is a square modulo* p.

PROOF. If $p = a^2 + b^2$, then $(p, ab) = 1$ (for example, if $p|a$, then $p = a^2 + b^2$ implies $p|b$ and it follows that $p^2|a^2 + b^2 = p$, which is absurd). Let $a^{(-1)} \in \mathbb{Z}$ be such that $a^{(-1)} \,(\mathrm{mod}\, p)$ is the multiplicative inverse of a mod p (i.e., $a.a^{(-1)} \equiv 1 \,(\mathrm{mod}\, p)$); we have

$$1 + (a^{(-1)})^2 b^2 = 1 + (a^{(-1)}b)^2 \equiv 0 \,(\mathrm{mod}\, p)$$

and hence -1 is a square in $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$.

Hence

$$\alpha := (a^{(-1)}b)^2 \,(\mathrm{mod}\, p) \in \mathbb{F}_p^\times$$

has exactly order 4 ($\alpha^2 = -1 \in \mathbb{F}_p^\times$) and therefore $4 || \mathbb{F}_p^\times | = p - 1$.

Alternatively (that was proposed by someone in the audience), for any $a \in \mathbb{Z}$ one has $a^2 \equiv 0 \,(\mathrm{mod}\, 4)$ if a is even and $a^2 \equiv 1 \,(\mathrm{mod}\, 4)$ if a is odd therefore if p is odd a and b must have distinct parities and

$$p = a^2 + b^2 \equiv 1 + 0 \,(\mathrm{mod}\, 4).$$

Now suppose that $4|p - 1$. Since $\mathbb{F}_p^\times$ is cyclic, it admits a cyclic subgroup of order 4. If $\alpha \in \mathbb{F}_p^\times$ is a generator of that subgroup, then α^2 has order 2 exactly so equals -1 and $-1 = \alpha^2$ is a square in $\mathbb{F}_p$.

Let us show now that if -1 is a square modulo p, then $p = \square + \square$.

Suppose again that $-1 = \alpha^2 \in \mathbb{F}_p$ and let $m \in \mathbb{Z}$ such that $m \equiv \alpha \,(\mathrm{mod}\, p)$. Then

$$m^2 + 1 = (m + i).(m - i) \in p\mathbb{Z}[i].$$

Let us consider the ideal

$$\mathfrak{p} := (m + i)\mathbb{Z}[i] + p\mathbb{Z}[i]$$

generated by $m + i$ and p. Write this ideal

$$\mathfrak{p} = (a + ib)\mathbb{Z}[i].$$

ince $p \in \mathbb{Z}[i]$ we have a surjective map

$$\mathbb{Z}[i]/p\mathbb{Z}[i] \mapsto \mathbb{Z}[i]/\mathfrak{p}$$

so

$$|\mathbb{Z}[i]/\mathfrak{p}| = a^2 + b^2 \text{ divides } |\mathbb{Z}[i]/(p)| = p^2$$

therefore we have either

$$a^2 + b^2 = (a + ib)(a - ib) = 1,\ p \text{ or } p^2.$$

The first case cannot occur: this would imply that $1 \in \mathfrak{p}$ but for any $z \in \mathfrak{p}$ we have

$$z = u(m + i) + v.p,\ u, v \in \mathbb{Z}[i]$$

and

$$\begin{aligned}\mathrm{Nr}(z) &= (u(m + i) + v.p)\overline{(u(m + i) + v.p)} \\ &= \mathrm{Nr}(u)(m^2 + 1) + \mathrm{Nr}(v)p^2 + p(u(m + i)\overline{v} + \overline{u(m + i)}v) \equiv 0 \,(\mathrm{mod}\, p).\end{aligned}$$

There third case cannot occur either since $m + i \notin p\mathbb{Z}[i]$ (the elements of $p\mathbb{Z}[i]$ are the Gaussian integers whose real and imaginary parts are divisible by p) so we have

$$|\mathbb{Z}[i]/\mathfrak{p}| = a^2 + b^2 = p.$$

□

Remark I.2. In addition we see that $\mathfrak{p} = (m+i)\mathbb{Z}[i]+p\mathbb{Z}[i]$ is a prime ideal: the quotient $\mathbb{Z}[i]/\pi$ is a ring of order p and since the map

$$x \in \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p \to x \,(\mathrm{mod}\, \mathfrak{p}) = \mathbb{Z}[i]/\mathfrak{p}$$

induced by the inclusion $\mathbb{Z} \subset \mathbb{Z}[i]$ is non-trivial it is injective and an isomorphism.

I.3. Fermat's equation for $n = 3$

As pointed out before, Fermat established his FLT when $n = 4$ (we leave it as a non-trivial exercise; cf. [1, §I.1.2]). This enabled him to make the following reduction.

Proposition I.3.1. *To prove FLT completely, it is sufficient to prove it when $n = p$ is an odd prime.*

Proof. Suppose we know FLT for all odd primes and for $n = 4$. Let $n \geqslant 6$ which is neither 4 or an odd prime, then n can be factored as $n = k.\ell$ where k is either 4 or an odd prime p. Suppose we have a primitive solution

$$x^n + y^n = z^n.$$

this can be written as

$$(x^\ell)^k + (y^\ell)^k = (z^\ell)^k$$

and (x^ℓ, y^ℓ, z^ℓ) is primitive and thus belongs to

$$\{(\varepsilon_1, \varepsilon_2, 0),\ (\varepsilon_1, 0, \varepsilon_2),\ (0, \varepsilon_1, \varepsilon_2) \colon \varepsilon_1, \varepsilon_2 \in \{\pm 1\}\}.$$

Therefore (x, y, z) belongs to that set. □

It "remains" to establish FLT for $n = p \geqslant 3$ an odd prime. Notice that since p is odd, Fermat's equation can be written

$$x^p + y^p + (-z^p) = x^p + y^p + (-z)^p = 0,$$

so that, replacing z by $-z$, it takes the more symmetric form

$$x^p + y^p + z^p = 0.$$

Historically, one considers two cases: Given a primitive solution (x, y, z) (such that $xyz \neq 0$ and $\gcd(x, y, z) = 1$), we consider the alternatives

Case 1: $p \nmid xyz$
Case 2: $p|xyz$.

The second case is the hard one.

In this section we discuss the case $n = p = 3$ which is due to Euler but we follow a method of Eisenstein.

I.3.1. The first case. Suppose that $3 \nmid xyz$ then

$$x \equiv \varepsilon_1 \,(\mathrm{mod}\, 3), y \equiv \varepsilon_2 \,(\mathrm{mod}\, 3), z \equiv \varepsilon_3 \,(\mathrm{mod}\, 3)$$

where $\varepsilon_i = \pm 1$.

Lemma I.3.2. *We have*

$$x^3 \equiv \varepsilon_1 \,(\mathrm{mod}\, 9).$$

Proof. Write $x = \varepsilon_1 + 3k$, then

$$x^3 = \varepsilon_1^3 + 3.\varepsilon_1^2.3k + 3\varepsilon_1.(3k)^2 + (3k)^3 \equiv \varepsilon_1^3 \,(\mathrm{mod}\, 9) = \varepsilon_1 \,(\mathrm{mod}\, 9).$$

□

This finishes the proof in this, since the equation

$$\varepsilon_1 + \varepsilon_2 = \varepsilon_3 \,(\mathrm{mod}\, 9)$$

has no solutions satisfying $\varepsilon_i = \pm 1$.

I.3.2. The second case. Suppose that $3|xyz$. We may assume without loss of generality that $3|z$ (and $3 \nmid xy$). Substituting z by $-3^v z'$ for $v \geqslant 1$ and such that $3 \nmid z'$, the equation can be rewritten as

$$x^3 + y^3 = 3^{3v} z^3,\ 3 \nmid xyz.$$

We will show that, if such a solution exists (with $xyz \neq 0$ and x, y, z pairwise coprime), the equation

$$(x')^3 + (y')^3 = 3^{3(v-1)}(z')^3,\ 3 \nmid x'y'z'$$

also has a solution. From there we obtain a contradiction on the existence of such (x, y, z) by induction on v (the case $v = 0$ is the first case and has been treated already).

This kind of argument (i.e., reducing an equation to another one which is "simpler", because the exponent v is reduced by 1) is called a *descent*.

I.3.3. The ring of Eisenstein integers. We will use a cubic analog of the ring of Gaussian integers.

Consider the usual cubic root of unity

$$j = \frac{-1 + i\sqrt{3}}{2} = e^{\frac{2\pi i}{3}}$$

so that

$$\mu_3 = \{z \in \mathbb{C},\ z^3 = 1\} = \{1, j, \overline{j}\}.$$

Fermat's equation becomes

$$(x + y)(x + jy)(x + j^2 y) = 3^{3v} z^3.$$

We are therefore studying a polynomial equation whose variables belong to the so called *ring of Eisenstein integers*

$$\mathbb{Z}[j] = \{P(j) \colon P \in \mathbb{Z}[X]\}.$$

THEOREM I.4. *The ring of Eisenstein integers enjoys the following properties.*

(1) One has

$$\mathbb{Z}[j] = \mathbb{Z} + j\mathbb{Z}. \tag{I.3}$$

(2) $\mathbb{Z}[j]$ is invariant under complex conjugation:

$$\mathbb{Z}[j] = \overline{\mathbb{Z}[j]}. \tag{I.4}$$

(3) The group of units is

$$\mathbb{Z}[j]^\times = \{z \in \mathbb{Z}[j] \colon z\overline{z} = 1\} = \pm\{1, j, j^2\}.$$

(4) For any $0 \neq z \in \mathbb{Z}[j]$, let $(z) = z.\mathbb{Z}[j]$ the corresponding principal ideal. Then

$$|\mathbb{Z}[j]/(z)| = z.\overline{z}. \tag{I.5}$$

(5) The ring $\mathbb{Z}[j]$ is a PID.

In what follows, as was the case for the Gaussian numbers, we define the norm Nr on $\mathbb{Q}(j)$ (and on $\mathbb{Z}[j]$) by

$$\mathrm{Nr}(z) = z.\overline{z}.$$

PROOF. We start with (I.3). We first note that

$$j^2 + j + 1 = 0 :$$

Indeed $j^3 - 1 = 0$ and $X^3 - 1 = (X - 1)(X^2 + X + 1)$. Therefore $j^2 = -j - 1$ and any polynomial $P(j)$ with integral coefficients evaluated at j can be written as an integral combination of 1 and j. Alternatively, one can do Euclidean division of $P(X)$ with respect to $X^2 + X + 1$: one has

$$P(X) = (X^2 + X + 1)S(X) + R(X), \ \deg R < 2$$

and writing $R(X) = a + bX, \ a, b \in \mathbb{Z}$ we see that

$$P(j) = (j^2 + j + 1)S(j) + R(j) = R(j) = a + bj \in \mathbb{Z} + j\mathbb{Z}.$$

Property (I.4) follows from the identity

$$\overline{j} = j^2 = -1 - j.$$

To compute the group of units, we first show that

$$z \in \mathbb{Z}[j]^\times \iff \mathrm{Nr}(z) = 1.$$

Note for $z = a + bj \in \mathbb{Z}[j]$ we have

$$\mathrm{Nr}(z) = z.\overline{z} = a^2 - ab + b^2 \in \mathbb{N}$$

since $\mathrm{Nr}(z) \geqslant 0$.

Given $z \in \mathbb{Z}[j]^\times$, we have $z^{-1} \in \mathbb{Z}[j]$. Therefore

$$\mathrm{Nr}(z)\,\mathrm{Nr}(z^{-1}) = \mathrm{Nr}(z.z^{-1}) = \mathrm{Nr}(1) = 1$$

and

$$\mathrm{Nr}(z), \mathrm{Nr}(z^{-1}) \in \mathbb{N}_{>0}.$$

Therefore $\mathrm{Nr}(z) = 1$. Conversely, if $\mathrm{Nr}(z) = z.\overline{z} = 1$, then $\overline{z} \in \mathbb{Z}[j]$ is the inverse of z in $\mathbb{Z}[j]$ and hence is a unit.

To compute $\mathbb{Z}[j]^\times$, we observe (by completing the square) that

$$\mathrm{Nr}(z) = a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2$$

and it remains to solve the equation

$$\left(a-\frac{b}{2}\right)^2+\frac{3}{4}b^2=1,\ a,b\in\mathbb{Z}$$

by inspection of the various cases.

For (I.5), we have for $z=a+jb$

$$(z)=z.\mathbb{Z}[j]=\mathbb{Z}(a+jb)+\mathbb{Z}(aj+bj^2)=\mathbb{Z}(a+jb)+\mathbb{Z}(-b+(a-b)j)$$

and thus

$$|\mathbb{Z}[j]/(z)|=\left|\det\begin{pmatrix}a & b\\ -b & (a-b)\end{pmatrix}\right|=|a^2-ab+b^2|=\mathrm{Nr}(z).$$

The proof that $\mathbb{Z}[j]$ is a PID is left as an exercise. It follows using the same argument as for the Gaussian integers: The complex plane $\mathbb{C}$ is tiled by the translates of parallelotope

$$\mathcal{P}_j=[0,1]+j[0,1]$$
$$\mathbb{C}=\bigcup_{a,b\in\mathbb{Z}}a+bj+\mathcal{P}_j$$

and the diameter of $\mathcal{P}_j$ is the length of the diagonal $[0,j-1]$ equals

$$|j-1|=(\frac{9}{4}+\frac{3}{4})^{1/2}=\sqrt{3}<2,$$

so any element of $\mathbb{C}$ is at distance <1 of an element of $\mathbb{Z}+\mathbb{Z}.j$. □

Already in the proof of Theorem I.3, we encountered the problem of "factoring primes" in $\mathbb{Z}$ when viewed as elements in $\mathbb{Z}[i]$. We encountered three classes, namely

(1) the odd primes for which $p\equiv 1\,(\mathrm{mod}\,4)$—i.e., the case where $\mathbb{Z}[i]/(p)$ was not a domain and therefore p factors as a product of two distinct primes—,
(2) the prime 2 which is associated to a square in $\mathbb{Z}[i]$—i.e., $2=(1+i)(1-i)=(-i)(1+i)^2$—,
(3) and the odd primes $p\equiv 3\,(\mathrm{mod}\,4)$, which can be shown to be prime in $\mathbb{Z}[i]$. Indeed, assume that $p\equiv 3\,(\mathrm{mod}\,4)$ is not prime in $\mathbb{Z}[i]$ and, in particular, (p) is not a prime ideal. Then $p=z_1.z_2$ for non-units $z_1,z_2\in\mathbb{Z}[i]$ and therefore $p=z_i.\overline{z_i}$, which contradicts the conclusion of Theorem I.3.

In this section, as mentioned already, we will rely on the factorization of the prime 3 inside $\mathbb{Z}[j]$, which happens to behave as for the prime 2 in $\mathbb{Z}[i]$.

PROPOSITION I.3.3. *Let $\pi_3=1-j$. The ideal $\mathfrak{p}_3=(\pi_3)$ is a prime ideal in $\mathbb{Z}[j]$ and*

$$\mathbb{Z}[j]/\mathfrak{p}_3\simeq\mathbb{F}_3.$$

Moreover, we have

$$\overline{\mathfrak{p}}_3=(\overline{\pi}_3)=(\pi_3)=\mathfrak{p}_3$$

and the decomposition

$$(3)=(\pi_3).(\overline{\pi_3})=\mathfrak{p}_3^2.$$

PROOF. We have

$$|\mathbb{Z}[j]/\mathfrak{p}_3|=\mathrm{Nr}(1-j)=(1-j)(1-\overline{j})=3$$

therefore $3\in\mathfrak{p}_3$ and $\mathbb{Z}[j]/\mathfrak{p}_3$ is a ring with three elements. Moreover the map induced by the inclusion $3\mathbb{Z}\subset\mathfrak{p}_3$

$$x\in\mathbb{Z}/3\mathbb{Z}\simeq\mathbb{F}_3\to x\,(\mathrm{mod}\,\pi_3)\in\mathbb{Z}[j]/\mathfrak{p}_3$$

is non trivial (hence injective) since $1\notin\mathfrak{p}_3$: for any $z\in\mathfrak{p}_3$ we have $z=(1-j)z',\ z'\in\mathbb{Z}[j]$ and

$$\mathrm{Nr}(z)=3\,\mathrm{Nr}(z')\in 3\mathbb{Z}.$$

We have therefore an isomorphism

$$\mathbb{F}_3\simeq\mathbb{Z}[j]/\mathfrak{p}_3$$

so $\mathfrak{p}_3$ is prime.

We have

$$1 - \overline{j} = 1 - j^2 = (1 + j)(1 - j) = -j^2(1 - j)$$

Since $-j^2$ is a unit in $\mathbb{Z}[j]$, we have

$$\overline{\mathfrak{p}}_3 = (1 - \overline{j}) = -j^2(1 - j)\mathbb{Z}[j] = (1 - j)\mathbb{Z}[j] = \mathfrak{p}_3$$

and

$$(3) = (1 - j).(1 - \overline{j}) = \mathfrak{p}_3^2.$$

□

I.3.4. Starting the descent. Recall that we are given a non-trivial solution (x, y, z) satisfying

$$x^3 + y^3 = 3^{3v}z^3,$$

where x, y, z are pairwise coprime and by the first case $v \in \mathbb{N}_{>0}$. Set

$$A = x + y,\ B = x + jy,\ C = x + j^2y = \overline{B}$$

We have therefore

$$A.B.C = 3^{3v}z^3,\ v \geqslant 1$$

LEMMA I.3.4. *We have*

$$A = 3^{3v-1}z_0,\ B = \pi_3 z_1,\ C = \overline{\pi_3}.\overline{z_1} = \pi_3 z_2$$

where $z_0, z_1, z_2 \in \mathbb{Z}[j]$ are pairwise coprime and coprime with $\mathfrak{p}_3$.

PROOF. By assumption we have $3|A.B.C$ and therefore $\pi_3|A.B.C$. By Gauss's lemma, π_3 divides at least one of A, B or C. Also observe that

$$A - B = (1 - j)y = \pi_3 y,\ A - C = (1 - j^2)y = \overline{\pi}_3 y = -j^2\pi_3 y.$$

It follows that $\pi_3|A,\ B$ and C: suppose for instance that $\pi_3|A$, then $\pi_3|B$ and $\pi_3|C$ and the other cases are similar.

In addition, since B and C are complex conjugates, the order of divisibility of B by π_3 is the same as the order of divisibility of C by $\overline{\pi}_3 = -j^2.\pi_3$; therefore π_3 divides B and C to the same order.

Note that none of x, y, z are divisible by π_3, otherwise either $x^2 = x\overline{x}$, $y^2 = y\overline{y}$, or $z^2 = z\overline{z}$ would be divisible by $\pi_3\overline{\pi}_3 = 3$, which is in contradiction to the assumption that $3 \nmid xyz$.

Now, since

$$B - C = j\pi_3 y$$

and since π_3 does not divide y, π_3 divides B and C at order exactly 1. Therefore

$$B = \pi_3 z_1,\ C = \overline{\pi}_3.\overline{z}_1 = -j^2\pi_3\overline{z}_1 = \pi_3 z_2$$

with $z_1, z_2 \in \mathbb{Z}[j]$ coprime with π_3. Since π_3 divides B and C at order 1 exactly and divides 3 at order 2 exactly, and as z is coprime to π_3, we see that π_3 divides $(3^v z)^3$ at order $6v$ exactly, and therefore divides A at order $6v - 2$ exactly. Moreover $3^{3v-1} = (-j^2)^{3v-1}\pi_3^{6v-2}$ and therefore

$$A = 3^{3v-1}z_0,\ z_0 \in \mathbb{Z}[j],\ \gcd(z_0, \pi_3) = 1.$$

Let us show that z_0, z_1 are coprime: let $\mathfrak{p} = (\pi)$ be a prime ideal dividing (z_0) (in particular $\mathfrak{p} \neq \mathfrak{p}_3$) and suppose that $\pi|z_1$. Then π divides A and B and, since

$$A - B = \pi_3 y,\ jA - B = -\pi_3 x,$$

it follows that π divides x and y. But then $\mathrm{Nr}(\pi) = \pi\overline{\pi}$ divides $\mathrm{Nr}(x) = x^2$ and $\mathrm{Nr}(y) = y^2$ which is excluded. One shows in the same way that z_0, z_1 and z_2 are pairwise coprime. □

LEMMA I.3.5. *There exists $u_0, u_1, u_2 \in \{1, j, j^2\}$ and $\rho_0, \rho_1, \rho_2 \in \mathbb{Z}[j]$ such that*

$$z_0 = u_0\rho_0^3,\ z_1 = u_1\rho_1^3,\ z_2 = u_2\rho_2^3$$

PROOF. We have the identity of ideals

$$(z^3) = (z_0).(z_1).(z_2).$$

Consider the prime decomposition of (z),

$$(z) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}},\ v_{\mathfrak{p}} = v_{\mathfrak{p}}(z);$$

we have

$$(z^3) = \prod_{\mathfrak{p}} \mathfrak{p}^{3v_{\mathfrak{p}}} = (z_0.z_1.z_2) = (z_0).(z_1).(z_2).$$

Therefore, if $\mathfrak{p}$ divides z at order $v_{\mathfrak{p}}$, it divides $z_0.z_1.z_2$ at order $3v_{\mathfrak{p}}$ and, since the z_i are pairwise coprime, $\mathfrak{p}$ divides exactly one of $z_i,\ i = 0, 1, 2$ at order $3v_{\mathfrak{p}}$. Therefore

$$(z_i) = \left(\prod_{\mathfrak{p}|z_i} \mathfrak{p}^{v_{\mathfrak{p}}} \right)^3.$$

Let $\rho_i \in \mathbb{Z}[j]$ be a generator of the ideal $\prod_{\mathfrak{p}|z_i} \mathfrak{p}^{v_{\mathfrak{p}}}$:

$$\prod_{\mathfrak{p}|z_i} \mathfrak{p}^{v_{\mathfrak{p}}} = \rho_i.\mathbb{Z}[j].$$

We have

$$(\rho_i^3) = (z_i),\ i = 0, 1, 2$$

and therefore there exist units $u_i \in \mathbb{Z}[j]^\times$, $i = 0, 1, 2$, such that

$$z_i = u_i \rho_i^3.$$

Observe that, since 3 is odd,

$$z_i = u_i \rho_i^3 = (-u_i)(-\rho_i^3) = -u_i(-\rho_i)^3$$

so we may assume without loss of generality that $u_i \in \{1, j, j^2\}$. □

LEMMA I.3.6. *Under the above assumptions we have $u_0 = 1$ and, moreover, we can choose $\rho_0 \in \mathbb{Z}$.*

PROOF. We have $z_0 = (x + y)/3^{3v-1} \in \mathbb{Q}$, so that $z_0/\overline{z}_0 = 1$, and therefore

$$\frac{u_0}{\overline{u}_0} = (\frac{\overline{\rho}_0}{\rho_0})^3$$

is a cube in the fraction field $\mathbb{Q}(j) = \mathrm{Frac}(\mathbb{Z}[j])$. The next lemma shows that in fact

$$\frac{\overline{\rho}_0}{\rho_0} \in \mathbb{Z}[j]^\times$$

and therefore

$$\frac{u_0}{\overline{u}_0} \in (\mathbb{Z}[j]^\times)^3.$$

For $u_0 \in \{1, j, j^2\}$, the only possibility is $u_0 = 1$, and we then have

$$\rho_0^3 = z_0 = A/3^{3v-1} \in \mathbb{Q}^\times.$$

The roots of the cubic polynomial $X^3 - z_0$ are $\{\rho_0, j\rho_0, j^2\rho_0\}$ and one of them is real. We may assume without loss of generality that ρ_0 is a real number; therefore, since

$$\rho_0 = a + jb,\ a, b \in \mathbb{Z}$$

is real, we have that $b = 0$ and $\rho_0 \in \mathbb{R} \cap \mathbb{Z}[j] = \mathbb{Z}$. □

Let us now prove the claim made above:

LEMMA I.3.7. *Let $u \in \mathbb{Z}[j]^\times$ be a unit and $\rho \in \mathbb{Q}(j)$ be such that $\rho^3 = u$ then $\rho \in \mathbb{Z}[j]^\times$.*

PROOF. Write $\rho = r/s$ with $r, s \in \mathbb{Z}[j]$ and coprime. We have

$$r^3 = us^3.$$

If $\mathfrak{p}$ is a prime dividing r, then $\mathfrak{p}|s^3$ and therefore $\mathfrak{p}|s$ (Gauss' lemma), which contradicts the coprimality of r, s. Therefore r is a unit. We show in the same way that s is a unit. □

LEMMA I.3.8. *Under the above assumption ($\rho_0 \in \mathbb{Z}$) we have $u_1 = 1$.*

PROOF. We have $A = x + y \equiv 0 \,(\mathrm{mod}\, 9)$ and since $(9) = \mathfrak{p}_3^4$ we have

$$\pi_3 y = A - B \equiv -B = -u_1\rho_1^3\pi_3 \,(\mathrm{mod}\, \mathfrak{p}_3^4).$$

Therefore

$$y \equiv -u_1\rho_1^3 \,(\mathrm{mod}\, \mathfrak{p}_3^3).$$

Since $3 \nmid y$, we have $y \equiv \pm 1 \,(\mathrm{mod}\, 3)$ which implies that

$$u_1^{-1} \equiv \pm\rho_1^3 \,(\mathrm{mod}\, 3).$$

Since $\mathbb{Z}[j]/\mathfrak{p}_3 = \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ one has (since $\rho_1 \not\equiv 0 \,(\mathrm{mod}\, \mathfrak{p}_3)$)

$$\rho_1 \equiv \pm 1 \,(\mathrm{mod}\, \mathfrak{p}_3).$$

hence

$$\rho_1 = \pm 1 + \pi_3 r,\ r \in \mathbb{Z}[j]$$

and

$$\rho_1^3 = (\pm 1)^3 + 3(\pm 1)^2\pi_3 r + 3(\pm 1)\pi_3^2 r^2 + (\pm 1)^2\pi_3^3 r^3 \equiv \pm 1 \,(\mathrm{mod}\, 3).$$

Therefore

$$u_1 \equiv \pm 1 \,(\mathrm{mod}\, 3).$$

This last congruence excludes $u_1 = j$ and $u_1 = j^2$ since $j \pm 1 \not\equiv 0 \,(\mathrm{mod}\, 3)$ ($j + 1 = -j^2$ is a unit $j - 1 = -\pi_3$ is divisible by π_3 to order 1 and not by $\pi_3^2 = -j^2.3$). Since $u_1 \in \{1, j, j^2\}$ we have necessarily $u_1 = 1$. □

I.3.5. Conclusion. We have proven that

$$x + y = 3^{3v-1}\rho_0^3,\ x + jy = (1 - j)\rho_1^3,\ x + j^2 y = \overline{x + jy} = (1 - j^2)\overline{\rho}_1^3$$

with

$$\rho_0 \in \mathbb{Z} - \{0\},\ \rho_1 = a + jb \in \mathbb{Z}[j].$$

Moreover we know that $3 \nmid \rho_0$

Expanding $(a + jb)^3$ and plugging into the second equation and identifying the real and j parts, we find that

$$x = a^3 + b^3 - 6ab^2 + 3a^2 b,\ y = -a^3 - b^3 + 6a^2 b - 3ab^2,\ x + y = 9ab(a - b).$$

Observe that $a, b, a - b$ are pairwise coprime (in $\mathbb{Z}$) since x and y are coprime: if $p|(a, b)$ then $p|x$ and $p|y$ since x and y are polynomials in a and b with no constant term. If $p|(a, a - b)$ or $p|(b, a - b)$, then also $p|(a, b)$. So these two cases reduce to the first case.

Moreover by the last equation we have

$$ab(a - b) = a^2 b - ab^2 = (3^{(v-1)}\rho_0)^3.$$

Since a, b and $a - b$ are pairwise coprime and $(3^{(v-1)}\rho_0)^3$ is the cube of an integer, a, b and $a - b$ are cubes of integers and therefore $a^2 b$ and $-ab^2$ are also cubes ($-1 = (-1)^3$ is a cube): write

$$a^2 b = (x_0')^3,\ -ab^2 = (y_0')^3,\ \rho_0 = z_0'.$$

We have therefore a solution of Fermat's equation

$$a^2 b - ab^2 = {x_0'}^3 + {y_0'}^3 = (3^{(v-1)}\rho_0)^3.$$

We have produced an integral solution $(x_0' = a^2 b, y_0' = -ab^2, z_0' = \rho_0)$ to the equation

$$X^3 + Y^3 = (3^{(v-1)}Z)^3. \tag{I.6}$$

In order to complete the descent step, we need a solution with x_0', y_0', ρ_0 pairwise coprime and the product $x_0'.y_0'.\rho_0$ not divisible by 3. We know already that $3 \not| z_0'$. If $3 \not| ab$ then $3 \not| x_0'y_0'\rho_0$. Given $p \neq 3$, if p divide two of (x_0', y_0', z_0') it will divide the third and we will obtain another smaller solution to the above equation, namely $(x_0'/p, y_0'/p, z_0'/p)$ those product is not divisible by 3. Continuing the process we may assume that x_0', y_0', ρ_0 are pairwise coprime.

Suppose now that $3|x_0' = a^2b$ and, for instance, that $3|a$. It follow that $3 \nmid (a-b)b$ by pairwise coprimality of $a, b, a-b$. Write $c = a-b$, we have $3 \nmid bc$ and the equation becomes

$$bc(b+c) = b^2c + bc^2 = (3^{(v-1)}\rho_0)^3.$$

with $b, c, b+c$ pairwise coprime. As above $b, c, b+c$ are also cubes of integers and so are

$$b^2c = x_0''^3, \ bc^2 = y_0''^3$$

and we eventually obtain a solution (x_0'', y_0'', ρ_0) to (I.6) where none of the entries are divisible by 3. By the same reduction as above we may also assume that x_0'', y_0'', ρ_0 are pairwise coprime and we conclude by induction on v that for $v \geqslant 0$ there exists no $(x, y, z) \in \mathbb{Z}^3$ such that

$$x^3 + y^3 = (3^v z)^3$$

with $3 \not| xyz$ and x, y, z pairwise coprime. □

Remark I.3. People have subsequently tried to solve Fermat's equation

$$x^p + y^p = z^p$$

for other values of the prime p by working with the (cyclotomic) ring $\mathbb{Z}[\zeta_p]$, where ζ_p is a p-th root of unity (for instance $\exp(\frac{2\pi i}{p})$).

In 1847, Gabriel Lamé announced the complete resolution of FLT for any n. Unfortunately (or fortunately) Lamé's proof was incorrect: it was based on the "fact" that $\mathbb{Z}[\zeta_p]$ was a UFD which is true for some primes p (for instance $p = 3$) but false in general.

In 1850, Kummer realized that some portions of that argument could be repaired by replacing factorisation of algebraic numbers by factorisation of "ideal numbers" (which are the now called *ideals*) recovered all previously known cases of the FLT (for an odd prime) and established new cases; however this approach did not extend to *all primes*.

As we will see, the fundamental obstruction is a finite commutative group, called the ideal class group of $\mathbb{Z}[\zeta_p]$, which is denoted $\mathrm{Cl}(\zeta_p)$. Its order is called the *class number* $h(\zeta_p)$. We have the following statement:

The ring $\mathbb{Z}[\zeta_p]$ is a PID if and only if the ideal class group is trivial.

One can show that as soon as p is sufficiently large $h(\zeta_p) > 1$ so there is really no possibility to completely mimick Lamé's proof. However, Kummer was able to prove FLT for primes p such that p does not divide the class number $h(\zeta_p)$. One calls such primes p *regular*.

Also Kummer provided an elementary criterion (not involving the class number) to determine whether a prime p is regular; this criterion is formulated in terms of the p-divisibility of numerators of Bernoulli numbers (depending on p).

It is conjectured, but not known, that there exist infinitely many regular primes.

One of the main objectives of this course will be to define the ideal class group (in greater generality) and to establish its basic properties.

Exercise I.1. (1) Prove that $\mathbb{Z}[j]$ is a PID.

(2) Prove that for a prime $p \neq 3$, the following are equivalent:
- p is of the shape $p = a^2 - ab + b^2$ $a, b \in \mathbb{Z}$.
- $p \equiv 1 \pmod 3$.
- -3 is a square modulo p.

CHAPTER II

Lattices in number fields

II.1. Archimidean/geometric embeddings

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the subfield of algebraic numbers $\mathbb{C}$. In the sequel, all the finite extensions of $\mathbb{Q}$ we will consider are included in $\overline{\mathbb{Q}}$ so are fields of complex numbers.

Let $K/\mathbb{Q}$ a finite extension of degree n. This is therefore a subfield of $\mathbb{C}$ and for any $\sigma \in \mathrm{Hom}(K, \overline{\mathbb{Q}})$, $\sigma(K)$ is another subfield isomorphic to K and contained in $\mathbb{C}$ and the set of all such subfields is precisely

$$\sigma(K),\ \sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}).$$

REMARK II.1. Since $K/\mathbb{Q}$ is separable, $|\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})| = n$.

DEFINITION II.1. *Given $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ an embedding of K in $\mathbb{C}$. If $\sigma(K) \subset \mathbb{R}$, σ is a real embedding and complex if $\sigma(K) \not\subset \mathbb{R}$.*

We denote the complex conjugation

$$\sigma_{\mathbb{C}}(\bullet) = \overline{\bullet} : z \in \mathbb{C} \to \overline{z} \in \mathbb{C}.$$

The group $\{\mathrm{Id}, \sigma_{\mathbb{C}}\}$ acts on $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$: the real embeddings are the fixed points for this action and the complex ones decompose into pairs of complex conjugate embeddings. In particular the number of complex embedding is even. The number of real embeddings is denoted $r_1 = r_1(K)$ and the number of complex ones is denoted $2r_2 = 2r_2(K)$ so that

$$r_1 + 2r_2 = n.$$

REMARK II.2. This can be considered as an archimedean version of the degree formula.

Set

$$r = r_1 + r_2$$

and

$$(\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots, \sigma_r) \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})^r$$

a choice of representatives of the various orbits of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ under the action of $\{\mathrm{Id}, \sigma_{\mathbb{C}}\}$: such a choice is called a *type* for K (there are 2^{r_2} possible types up to permutation). In other terms given a type as above

$$\{\sigma_1, \cdots, \sigma_{r_1}\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$$

is the set of real embeddings and

$$\{\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+1}, \cdots, \overline{\sigma}_{r_1+r_2}\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) - \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R}).$$

is the set of complex ones.

Let K_∞ be the $\mathbb{R}$-algebra

$$K_\infty := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \prod_{i=1}^{r_1+r_2} K_i$$

with

$$K_i = \begin{cases} \mathbb{R} & i \leqslant r_1 \\ \mathbb{C} & i = r_1 + 1, \cdots, r_2. \end{cases}$$

We have

$$K_\infty \simeq \mathbb{R}^n$$

where we have identified $\mathbb{C}$ with $\mathbb{R}^2$ via the usual $\mathbb{R}$-linear map

$$z = x + iy \in \mathbb{C} \to (x, y) \in \mathbb{R}^2.$$

Given a type, let

$$\sigma_\infty : \begin{array}{ccc} K & \mapsto & K_\infty \\ z & \mapsto & \sigma_\infty(z) = (\sigma_1(z), \cdots, \sigma_r(z)) \end{array}.$$

This is an injective morphism of $\mathbb{Q}$-algebra called the *archimedean* or *geometric* embedding associated to the type. In the sequel the type is fixed once and for all.

II.2. Lattices in number fields

We let $K \subseteq \overline{\mathbb{Q}}$ as above, i.e., K is a *number field* of degree n.

PROPOSITION II.2.1. *Let $\mathcal{B} = (\omega_1, \dots, \omega_n) \in K^n$. The following are equivalent.*

(1) $\mathcal{B}$ is a $\mathbb{Q}$-basis of K.

(2) $\sigma_\infty(\mathcal{B}) = \big(\sigma_\infty(\omega_1), \dots, \sigma_\infty(\omega_n)\big)$ is a basis of $\mathbb{R}^n$.

The following is an immediate corollary of Proposition II.2.1

COROLLARY II.2.1. *$\sigma_\infty(K)$ is dense in $\mathbb{R}^n$.*

The proof of Proposition II.2.1 relies on the following Lemma. For what follows, we enumerate the elements of $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ so that for all $1 \leqslant i \leqslant r_2$ we have $\sigma_{r+i} = \overline{\sigma_{r_1+i}}$.

LEMMA II.2.2. *Let $\mathcal{B} = (\omega_1, \dots, \omega_n) \in K^n$. Then $\mathcal{B}$ is a $\mathbb{Q}$-basis of K if and only if* $\det\big(\sigma_i(\omega_j)\big) \neq 0$.

PROOF. If $\mathcal{B}$ is not a basis, then $\mathcal{B}$ satisfies a non-trivial relation over $\mathbb{Q}$ and, since the embeddings are $\mathbb{Q}$-linear, therefore the columns of $\big(\sigma_i(\omega_j)\big)$ satisfy a linear relation, i.e., $\det\big(\sigma_i(\omega_j)\big) = 0$.

Now suppose that $\mathcal{B}$ is a basis and suppose that $(c_1, \dots, c_n) \in \mathbb{C}^n$ give rise to a linear relation among the rows, i.e.,

$$\forall 1 \leqslant j \leqslant n \quad \sum_{i=1}^{n} \sigma_i(\omega_j) = 0.$$

Since $\mathcal{B}$ is a basis, $\mathbb{Q}$-linearity of the embeddings implies that

$$\sum_{i=1}^{n} c_i \sigma_i = 0$$

and, by Lemma A.5.5, it follows that $c_1 = \cdots = c_n = 0$. In particular, the rows are linearly independent and, hence, $\det\big(\sigma_i(\omega_j)\big) \neq 0$. □

PROOF OF PROPOSITION II.2.1. Let $B = \big(\sigma_i(\omega_j)\big) \in M_n(\mathbb{C})$ and let $A = \big(\sigma_\infty(\omega_j)\big)$. If $1 \leqslant k \leqslant r_2$, then $B_{r+k,j} = \overline{B_{r_1+k,j}}$, hence

$$A_{r_1+2(k-1)+1,j} = \frac{1}{2}(B_{r_1+k,j} + B_{r+k,j}), \quad A_{r_1+2k,j} = \frac{1}{2\mathrm{i}}(B_{r_1+k,j} - B_{r+k,j}),$$

thus

$$\det(B) = (2\mathrm{i})^{r_2} \det(A)$$

and the equivalence follows from Lemma II.2.2. □

DEFINITION II.2. *A subgroup $\Lambda < K$ is a* lattice *if it is generated by a $\mathbb{Q}$-basis of K.*

DEFINITION II.3. *A subgroup $\Gamma < \mathbb{R}^n$ is a* (geometric) lattice *if it is generated by a basis of $\mathbb{R}^n$.*

The following is an immediate corollary of Proposition II.2.1.

COROLLARY II.2.2. *A subgroup $\Lambda < K$ is a lattice if and only if $\sigma_\infty(\Lambda)$ is a geometric lattice.*

Recall that a subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete and cocompact; cf. A.2.4.

LEMMA II.2.3. *Let $\Lambda < K$ be a subgroup. Then Λ is a lattice if and only if Λ is finitely generated and contains a $\mathbb{Q}$-basis of K.*

PROOF. If Λ is a lattice, then Λ is generated by a basis, in particular finitely generated and contains a basis.

Now suppose that Λ is generated by the finite set $S \subseteq \Lambda$ and suppose that $\mathcal{B} \in \Lambda^n$ is a $\mathbb{Q}$-basis of K. In what follows, we denote by $\Lambda_{\mathcal{B}} < K$ the lattice generated by $\mathcal{B}$. Note that $\Lambda_{\mathcal{B}} \subseteq \Lambda$.

Since $\mathcal{B}$ is a basis, every element in S is a $\mathbb{Q}$-linear combination in $\mathcal{B}$ and, clearing denominators, there exists $N \in \mathbb{N}$ such that $N\Lambda \subseteq \Lambda_{\mathcal{B}}$.

Since $\sigma_\infty(\Lambda_{\mathcal{B}}) \subseteq \sigma_\infty(\Lambda)$, Corollary II.2.2 and Lemma A.2.4 imply that $\sigma_\infty(\Lambda)$ is cocompact. On the other hand, $\sigma_\infty(\Lambda) \subseteq \frac{1}{N}\sigma_\infty(\Lambda_{\mathcal{B}})$ implies that $\sigma_\infty(\Lambda)$ is discrete. Hence $\sigma_\infty(\Lambda)$ is discrete and cocompact, therefore a lattice. In particular, Λ is a lattice by Corollary II.2.2. □

EXERCISE II.1. Let $\Lambda_1, \Lambda_2 < K$ be lattices and let $\Lambda_1.\Lambda_2$ be the subgroup generated by all products of elements in Λ_1 and Λ_2, i.e.,

$$\Lambda_1.\Lambda_2 = \left\{ \sum_{i=1}^{\ell} a_i b_i \colon \ell \in \mathbb{N} \cup \{0\}, a_i \in \Lambda_1, b_i \in \Lambda_2 \right\}.$$

Show that $\Lambda_1.\Lambda_2$ is a lattice.

Recycling the argument used in the proof, one obtains a proof of the following.

PROPOSITION II.2.4. *Let $\Lambda_1, \Lambda_2 < K$ lattices. There exists $N \in \mathbb{N}$ such that*

$$N\Lambda_1 \subseteq \Lambda_2 \subseteq \frac{1}{N}\Lambda_1.$$

The proof is left as an exercise.

II.3. The discriminant of a basis and the discriminant of a lattice

DEFINITION II.4. *Let $\mathcal{B} = (\omega_1, \dots, \omega_n) \in K^n$. We define the* discriminant *of $\mathcal{B}$ by*

$$\operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}) = \det\left(\sigma_i(\omega_j)\right)^2.$$

EXERCISE II.2. Let $\mathcal{B}_1, \mathcal{B}_2 \in K^n$ such that the subgroups of K generated by $\mathcal{B}_1$ and $\mathcal{B}_2$ respectively are equal. Then

$$\operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}_1) = \operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}_2).$$

DEFINITION II.5. *Let $\Lambda < K$ be a lattice. The* discriminant *of Λ is defined as*

$$\operatorname{disc}_{K/\mathbb{Q}}(\Lambda) = \operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}),$$

where $\mathcal{B} \in \Lambda^n$ is any $\mathbb{Z}$-basis of Λ.

EXERCISE II.3. Let $\mathcal{B} \in K^n$ be a $\mathbb{Q}$-basis of K. Then

$$\operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}) = (2\mathrm{i})^{2r_2} \operatorname{covol}\left(\sigma_\infty(\Lambda_{\mathcal{B}})\right)^2.$$

LEMMA II.3.1. *Let $\mathcal{B} = (\omega_1, \dots, \omega_n) \in K^n$ be a $\mathbb{Q}$-basis of K. Then*

$$\operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}) = \det\left(\operatorname{tr}_{K/\mathbb{Q}}(\omega_i\omega_j)\right).$$

In particular, $\operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}) \in \mathbb{Q} \setminus \{0\}$.

PROOF. Recall that for any $x \in K$, the expression $\mathrm{tr}_{K/\mathbb{Q}}(x)$ denotes the trace of the $\mathbb{Q}$-linear endomorphism $[\times x]_{K/\mathbb{Q}}$ of K given by multiplication by x.

Using the primitive element theorem, we can assume that $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ with minimal polynomial $f \in \mathbb{Q}[X]$. Let $A \in M_n(\mathbb{Q})$ denote the companion matrix corresponding to f. Using the basis $\mathcal{E} = (1, \alpha, \dots, \alpha^{n-1})$ of K, one checks that the extension of the map $\iota\colon \alpha \mapsto A$ to a homomorphism $\mathbb{Q}(\alpha) \to M_n(\mathbb{Q})$ of unital $\mathbb{Q}$-algebras gives a matrix representation of $[\times\bullet]_{K/\mathbb{Q}}$, i.e., for every $x \in K$, the matrix $\iota(x)$ is the representation matrix of $[\times x]_{K/\mathbb{Q}}$ with respect to $\mathcal{E}$.

Since f is separable, the matrix A is diagonalizable with eigenvalues $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$. Since ι is a homomorphism of $\mathbb{Q}$-algebras, it follows that for every $x \in K$ the matrix $\iota(x)$ is diagonalizable with eigenvalues $\sigma_1(x), \dots, \sigma_n(x)$ (which might not be pairwise distinct, e.g., consider $x = 0$). It follows that

$$\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j).$$

This proves the lemma. □

LEMMA II.3.2. *Let $\Lambda_1 \subseteq \Lambda_2 < K$ be lattices. Then*

$$[\Lambda_2 \colon \Lambda_1]^2 = \frac{\mathrm{disc}_{K/\mathbb{Q}}(\Lambda_1)}{\mathrm{disc}_{K/\mathbb{Q}}(\Lambda_2)}.$$

PROOF. Note that

$$[\Lambda_2 \colon \Lambda_1] = \frac{\mathrm{covol}\left(\sigma_\infty(\Lambda_1)\right)}{\mathrm{covol}\left(\sigma_\infty(\Lambda_2)\right)}.$$

Indeed, if $v_1, \dots, v_\ell \in \sigma_\infty(\Lambda_2)$ are representatives of $\sigma_\infty(\Lambda_2)/\sigma_\infty(\Lambda_1)$, and if $F_2 \subseteq \mathbb{R}^n$ is a fundamental domain for $\sigma_\infty(\Lambda_2) \curvearrowright \mathbb{R}^n$, one easily checks that

$$F_1 = \bigsqcup_{k=1}^{\ell} (v_k + F_2)$$

is a fundamental domain for Λ_2 and, by translation invariance of the Lebesgue measure, we have

$$\mathrm{covol}\left(\sigma_\infty(\Lambda_1)\right) = \mathrm{vol}(F_1) = \ell \mathrm{vol}(F_2) = [\Lambda_2 \colon \Lambda_1]\, \mathrm{covol}\left(\sigma_\infty(\Lambda_2)\right).$$

Hence, the Lemma follows from Exercise II.3. □

II.4. Orders in number fields and the ring of integers

DEFINITION II.6. *An* order $\mathcal{O} \subseteq K$ *is a lattice which is also a unital subring.*

LEMMA II.4.1. *There exists an order $\mathcal{O} \subseteq K$.*

PROOF. Let $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ and let $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ be the polynomial obtained by multiplying the minimal polynomial of f by a common denominator of the coefficients. Let $\beta = a_n\alpha$. Then $K = \mathbb{Q}(\beta)$ and, therefore, $(1, \dots, \beta^{n-1})$ is a $\mathbb{Q}$-basis of K. Moreover, letting

$$g = X + a_n a_{n-1} X^{n-1} + \cdots + a_n^{n-1} a_0 \in \mathbb{Z}[X],$$

we have

$$g(\beta) = a_n^{n-1} f(\alpha) = 0$$

and, hence,

$$\mathbb{Z}[\beta] = \mathbb{Z} + \cdots + \mathbb{Z}\beta^{n-1}.$$

Hence $\mathbb{Z}[\beta]$ is a lattice and, therefore, an order. □

LEMMA II.4.2. *Let $\mathcal{O} \subseteq K$ be an order. Then* $\mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}) \in \mathbb{Z} \setminus \{0\}$.

PROOF. Let $\mathcal{B} = (\omega_1, \dots, \omega_n) \in \mathcal{O}^n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Since $[\times\omega_i\omega_j]\omega_k \in \mathcal{O}$ for all $\omega_i, \omega_j, \omega_k$ and since $\mathcal{B}$ is a $\mathbb{Z}$-basis of $\mathcal{O}$, we have that $\mathrm{tr}_{K/\mathbb{Q}}(\omega_i\omega_j) \in \mathbb{Z}$ for all ω_i, ω_j. In particular, the discriminant of $\mathcal{O}$ is an integer by Lemma II.3.1. The discriminant of any lattice is non-zero, hence also of □

COROLLARY II.4.1. *Every increasing sequence of orders in K stabilizes. In particular, K has a maximal order.*

PROOF. Let $\mathcal{O}_1 \subseteq \mathcal{O}_2 \subseteq \cdots$ be an increasing sequence of orders. As of Lemma II.3.2, we know that

$$\forall i \in \mathbb{N} \quad \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_{i+1}) | \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_i).$$

Since any non-empty subset of $\mathbb{N}$ has a minimum, Lemma II.3.2 implies that there exists a maximal order in K. □

THEOREM II.1. *There exists a unique maximal order $\mathcal{O}_K \subseteq K$, called the* ring of integers *in K.*

PROOF. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ orders in K. Let $\mathcal{O} \subseteq K$ be the subgroup generated by products of elements of $\mathcal{O}_1$ and $\mathcal{O}_2$; cf. Exercise II.1. Then $\mathcal{O}$ is a lattice as of Exercise II.1. Moreover, since $\mathcal{O}_1$ and $\mathcal{O}_2$ are unital, we know that $\mathcal{O}_1$ and $\mathcal{O}_2$ are contained in $\mathcal{O}$. Since $\mathcal{O}_1$ and $\mathcal{O}_2$ are unital subrings, $\mathcal{O}$ is a unital subring. In particular, $\mathcal{O}$ is an order.

This shows that any two orders are contained in a common order. Therefore there exists a unique maximal order. □

CHAPTER III

Dedekind rings

III.1. Integral Extensions

For what follows, by a ring we generally mean a commutative unital ring.

THEOREM III.1. *Let R be a ring and $A \subset R$ a subring. Given $z \in R$, the following are equivalent.*

(1) z is the root of a monic polynomial with coefficients in A.

(2) The ring

$$A[z] = \{P(z) \colon P(X) \in A[X]\} \subset R$$

is a A-module of finite type (f.t).

(3) There exists a subring $B \subset R$ containing A and z which is an f.t A-module.

We then say that z is integral over A.

REMARK III.1. If A is a field, this is the definition of an algebraic element.

PROOF. (1) $\implies$ (2): Let $P \in A[X]$ a monic polynomial such that $P(z) = 0$. By euclidean division, for any $Q \in A[X]$ there exist $K, R \in A[X]$ such that

$$Q = KP + R, \qquad \text{with } \deg R < \deg P.$$

Writing $R(X) = a_d X^d + \cdots + a_0$ with $a_i \in A$, we find that

$$Q(z) = R(z) = a_d z^d + \cdots + a_0 \in A + \cdots + Az^d$$

with $d < \deg(P)$ and therefore $A[z] \subset R$ is f.t.

(2) $\implies$ (3): Choose $B = A[z]$.

(3) $\implies$ (1): Given B as in (3), let $z_1, \ldots, z_d$ be a finite set of generators:

$$B = A.z_1 + \cdots + A.z_d.$$

Let

$$[\times z] : \begin{array}{ccc} B & \mapsto & B \\ x & \mapsto & z.x \end{array}$$

be the A-module endomorphism of B given by multiplication by z. We have

$$\forall i \quad z.z_i = \sum_j a_{ij}.z_j.$$

Let

$$M_z = (a_{ij})_{i,j \leq d} \in M_d(A) \text{ and } \mathbf{z} = (z_i)_i \in B^d.$$

The above system of equalities can be writen

$$(z\mathrm{Id}_d - M_z)\mathbf{z} = C(z)\mathbf{z} = \mathbf{0}$$

where $\mathbf{0} \in B^d$ denotes the zero vector and $C(z)$ is the matrix

$$C(z) = z.\mathrm{Id} - M_z = (\delta_{ij}.z - a_{ij})_{1 \leqslant i,j \leqslant d} \in M_d(B).$$

Fix $i \leqslant d$ and define the vectors $\mathbf{v}_j \in B^d,\ j \leqslant d$ as follows: if $j \neq i$, we set

$$\mathbf{v}_j = C(z)^{(j)}$$

and if $j = i$ we set

$$\mathbf{v}_i = z_i.C(z)^{(i)}.$$

By multilinearity of the determinant, we have

$$\det(\mathbf{v}_1, \dots, \mathbf{v}_d) = z_i \det C(z).$$

Set

$$\mathbf{w}_i := \sum_{k=1}^{d} z_k.C(z)^{(k)} = \mathbf{v}_i + \sum_{\substack{k=1 \\ k\neq i}}^{d} z_k.\mathbf{v}_k,\ \mathbf{w}_j := \mathbf{v}_j,\ j \neq i.$$

Since the determinant is alternating we have

$$\det(\mathbf{w}_1, \dots, \mathbf{w}_d) = \det(\mathbf{v}_1, \dots, \mathbf{v}_d) = z_i \det C(z).$$

Since

$$\mathbf{w}_i = C(z).\mathbf{z} = \mathbf{0}$$

we have

$$\det(\mathbf{w}_1, \dots, \mathbf{w}_d) = 0 = z_i \det C(z).$$

We have shown that

$$\forall i \quad \det C(z).z_i = 0$$

and therefore

$$\det C(z).1_B = \det C(z) = 0.$$

Since $\det C(z)$ is a monic polynomial in z with coefficients in A, we are done.

□

LEMMA III.1.1. *Suppose $A \subset B \subset R$ and assume that B is an f.t. A-module and R an f.t. B-module. Then R is an f.t. A-module.*

PROOF. Let $y_1, \dots, y_d \in B$, $z_1, \dots, z_e \in R$ such that

$$B = Ay_1 + \cdots + Ay_d,$$
$$R = Bz_1 + \cdots + Bz_e.$$

Then

$$R = \sum_{i=1}^{d} \sum_{j=1}^{e} Ay_i z_j.$$

□

PROPOSITION III.1.2. *The set $\mathcal{O}_R(A) \subset R$ of A-integral elements in R is a subring of R containing A.*

PROOF. It is clear that $A \subset \mathcal{O}_R(A)$ (a is a root of $X - a$).

If $A[z]$ and $A[z']$ are f.t. then $A[z][z'] \cong A[z, z']$ is f.t and contains $z + z'$ and $z.z'$. Indeed z' is integral over A and, in particular, over $A[z]$. Therefore, Lemma III.1.1 implies that $A[z, z']$ is f.t. over A. This implies that $\mathcal{O}_R(A)$ is closed under multiplication and addition. □

DEFINITION III.1. *The ring $\mathcal{O}_R(A)$ is the integral closure of A in R. If $\mathcal{O}_R(A) = R$, i.e., if every element of R is integral over A, one saysthat R is integral over A or that the extension R/A is integral.*

PROPOSITION III.1.3. *If B/A is integral and C/B is integral, then C/A is integral.*

PROOF. Exercise. □

DEFINITION III.2. *If A is a domain and $Q = \mathrm{Frac}(A)$ is the field of fractions of A, then the* integral closure *of A is the integral closure of A in Q. The ring A is* integrally closed *if it is equal to its integral closure.*

We have the following consequence from the previous proposition:

COROLLARY III.1.4. *The integral closure of a domain A is itself integrally closed.*

REMARK III.2. If $A \subset B$ is a domain and B/A is integral, then A is a field if and only if B is a field. Indeed, let $z \in B - \{0\}$,

$$z^d + \cdots + a_1 z + a_0 = 0$$

and assume without loss of generality that $a_0 \neq 0$. If A is a field, then a_0 is inveritble in B and thus

$$1 = -a_0^{-1}(z^{d-1} + \cdots + a_1)z$$

implies that z is invertible in B.

On the other hand, if B is a field and $z \in A \setminus \{0\}$, then the assumption that $z^{-1} \in B$ is integral over A implies that we can find $a_{d-1}, \ldots, a_0 \in A$ such that

$$z^{-d} = -a_{d-1}z^{-(d-1)} - \cdots - a_0.$$

Multiplying both sides by z^{d-1} shows that $z^{-1} \in A$.

REMARK III.3. When A is a field, integrality is equivalent to algebraicity.

PROPOSITION III.1.5. *If A is a PID, then A is integrally closed.*

PROOF. Let $z \in \mathcal{O}_Q(A)$, i.e., suppose that there are $a_0, \ldots, a_{d-1} \in A$ such that:

$$z^d + \cdots + a_1 z + a_0 = 0.$$

We may assume without loss of generality that $a_0 \neq 0$. Write $z = a/b$ with $a, b \in A$ coprime. We have

$$a^d + \cdots + a_1 a b^{d-1} + a_0 b^d = 0.$$

Therefore

$$a^d = -b(a_{d-1}a^{d-1} + \cdots + a_1 a b^{d-1} + a_0 b^{d-1})$$

so that b divides a^d. As a and b are coprime, it follows that b is a unit and therefore $z = a/b \in A$. □

III.2. Dedekind rings

We will be interested mostly in the integral closure of $\mathbb{Z}$ in a number field $K|\mathbb{Q}$. As it will turn out, the integral closure $\mathcal{O}_K = \mathcal{O}_K(\mathbb{Z})$, called the *ring of integers in K*, will not be a PID and not even a UFD. However, an important property of $\mathbb{Z}$ is preserved when passing to the integral closure $\mathcal{O}_K$, namely the unique factorization of ideals into prime ideals; cf. §A.1.2 for a recollection of this in the case of PIDs. Because of the importance of this inheritence, we will discuss it in somewhat greater detail. More precisely, we introduce a more general class of rings for which unique prime factorisation of ideals is true.

DEFINITION III.3. *A ring A is Dedekind if*

(1) A is a domain,
(2) A is integrally closed,
(3) A is noetherian.
(4) every non-zero prime ideal is maximal.

REMARK III.4. We refer the reader to §A.1.1 for a recollection of the definition and basic properties of noetherian rings and modules.

EXAMPLE III.1. A PID A is a Dedekind ring: this is a domain by definition; any prime ideal is maximal; any ideal is generated by one element so A is noetherian and we have seen in the previous section that A is integrally closed.

The two key results about Dedekind rings in this course are the following.

III.2.1. Factorisation of ideals. The first property is a generalisation to the unique factorisation property of ideals in PIDs. In what follows, given a ring A, we denote by $\mathcal{I}_A$ the set of non-zero ideals in A.

THEOREM III.2. *Let A be a Dedekind ring. Every ideal $\mathfrak{a} \in \mathcal{I}_A$ factors uniquely as a product of non-zero prime ideals: there exists a unique function*

$$v_\bullet(\mathfrak{a})\colon \begin{array}{ccc} \mathrm{Spec}(A) & \mapsto & \mathbb{N} \\ \mathfrak{p} & \mapsto & v_\mathfrak{p}(\mathfrak{a}) \end{array}$$

such that

- $v_{\{0\}}(\mathfrak{a}) = 0$,
- *for a.e.* $\mathfrak{p}$, $v_\mathfrak{p}(\mathfrak{a}) = 0$, *and*
- *one has the following factorisation*

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})},$$

where $\mathfrak{p}^0 = A$ for any $\mathfrak{p} \in \mathrm{Spec}(A)$.

DEFINITION III.4. *Given an ideal $\mathfrak{a} \in \mathcal{I}_A$ and a non-zero prime $\mathfrak{p} \in \mathrm{Spec}(A)$, the integer*

$$v_\mathfrak{p}(\mathfrak{a})$$

is called the valuation of $\mathfrak{a}$ at the prime $\mathfrak{p}$ *or the* $\mathfrak{p}$-adic valuation of $\mathfrak{a}$. *This is the largest integer v such that $\mathfrak{p}^v | \mathfrak{a}$. For the zero ideal we set*

$$v_\mathfrak{p}(\{0\}) = +\infty.$$

REMARK III.5. Since A is a domain the zero ideal $\{0\} = 0.A$ is a prime but of course does not contain any non-zero ideal: this is why we have set $v_{\{0\}}(\mathfrak{a}) = 0$. Usually we will use $\mathfrak{p}$ is denote a *non-zero* prime ideal.

We deduce from the existence and unicity of the factorisation the following result regarding arithmetics of ideals in Dedekind rings.

COROLLARY III.2.1. *Let A a Dedekind ring and $\mathfrak{a}, \mathfrak{b} \subset A$ two ideals (possibly 0). Then*

$$\mathfrak{a} | \mathfrak{b} \iff \forall \mathfrak{p},\ v_\mathfrak{p}(\mathfrak{a}) \leqslant v_\mathfrak{p}(\mathfrak{b}).$$

$$\mathfrak{a}.\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b})}$$

$$\mathfrak{a} \cap \mathfrak{b} = \textit{largest ideal contained in } \mathfrak{a} \textit{ and } \mathfrak{b} =: [\mathfrak{a}, \mathfrak{b}] = \prod_\mathfrak{p} \mathfrak{p}^{\max(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))}$$

$$\mathfrak{a} + \mathfrak{b} = \textit{smallest ideal containing both } \mathfrak{a} \textit{ and } \mathfrak{b} =: (\mathfrak{a}, \mathfrak{b}) = \prod_\mathfrak{p} \mathfrak{p}^{\min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))}$$

and

$$(\mathfrak{a}, \mathfrak{b}).[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a}.\mathfrak{b}.$$

In other terms, for any prime ideal $\mathfrak{p}$ one has

$$v_\mathfrak{p}(\mathfrak{a}.\mathfrak{b}) = v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b}),$$
$$v_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = v_\mathfrak{p}\big([\mathfrak{a}, \mathfrak{b}]\big) = \max\big\{v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\big\},$$
$$v_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = v_\mathfrak{p}\big((\mathfrak{a}, \mathfrak{b})\big) = \min\big\{v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\big\}.$$

In particular, two ideals $\mathfrak{a}, \mathfrak{b}$ in a Dedekind ring are coprime (that is $\mathfrak{a} + \mathfrak{b} = A$) if and only if their valuation functions

$$v_\bullet(\mathfrak{a})\colon \mathfrak{p} \mapsto v_\mathfrak{p}(\mathfrak{a}),\ v_\bullet(\mathfrak{b})\colon \mathfrak{p} \mapsto v_\mathfrak{p}(\mathfrak{b})$$

have disjoint supports:

$$(\mathfrak{a}, \mathfrak{b}) = A \iff \forall \mathfrak{p} \quad v_\mathfrak{p}(\mathfrak{a}).v_\mathfrak{p}(\mathfrak{b}) = 0.$$

III.2.2. Stability. The second property is the stability of the class of Dedekind rings under integral closure in a separable extension.

THEOREM III.3. *Let A be a Dedekind ring with field of fractions Q and suppose that K/Q is a finite separable extension, then $\mathcal{O}_K(A)$ is an A-module of finite type and a Dedekind ring.*

III.2.3. The three key examples of Dedekind rings. The cases of main interest to us are the following.

- Suppose $A = \mathbb{Z}$, $Q = \mathbb{Q}$, and $K/\mathbb{Q}$ is a finite (therefore algebraic and necessarily separable) extension of $\mathbb{Q}$ (contained in $\mathbb{C}$). The integral closure of $\mathbb{Z}$ in K is called the *ring of integers* of K and is denoted
$$\mathcal{O}_K = \{z \in K : \exists P \in \mathbb{Z}[X] \text{ monic such that } P(z) = 0\}.$$
- Suppose $A = \mathbb{C}[X]$, $Q = \mathbb{C}(X)$, and $K/\mathbb{C}(X)$ is a finite (therefore algebraic and necessarily separable) extension of Q contained in some algebraic closure $\overline{\mathbb{C}(X)}$. For instance, suppose that $K = Q(Y)$ where Y is a solution in $\overline{\mathbb{C}(X)}$ of the polynomial equation
$$\mathrm{Eq}(X, Y) = 0$$
for a polynomial $\mathrm{Eq} \in \mathbb{C}[U, V]$ in two variables. Then the set of solutions of the equation
$$\mathcal{C} : \mathrm{Eq}(x, y) = 0, \quad (x, y) \in \mathbb{C}^2$$
defines a complex algebraic affine curve with an algebraic map to the affine line
$$(x, y) \in \mathcal{C}(\mathbb{C}) \mapsto x \in \mathbb{C}$$
and the field K is the field of (algebraic) functions on $\mathcal{C}$. To this curve corresponds a projective algebraic curve $\overline{\mathcal{C}(\mathbb{C})}$ with an algebraic map
$$x : \overline{\mathcal{C}(\mathbb{C})} \mapsto \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$$
and the integral closure
$$\mathcal{O}_K = \{F \in K : \exists P \in \mathbb{C}[X][Z] \text{ monic such that } P(F) = 0\}$$
corresponds to the algebraic functions on $\overline{\mathcal{C}(\mathbb{C})}$ which are regular outside the preimage $x^{-1}(\infty)$.

  Alternatively (and equivalently), to $\mathcal{C}$ is associated a Riemann surface $\overline{\mathcal{C}(\mathbb{C})}$ with a map x to the projective line (the Riemann sphere) and $\mathcal{O}_K$ corresponds to the meromorphic functions on $\overline{\mathcal{C}(\mathbb{C})}$ which are holomorphic outside the preimage $x^{-1}(\infty)$.
- Suppose $A = \mathbb{F}_p[X]$, $Q = \mathbb{F}_p(X)$, and $K/\mathbb{F}_p(X)$ is a finite (therefore algebraic) and separable (this is not always the case) extension of Q contained in some algebraic closure $\overline{\mathbb{F}_p(X)}$. We denote the integral closure by $\mathcal{O}_K$:
$$\mathcal{O}_K = \{F \in K : \exists P \in \mathbb{F}_q[X][Z] \text{ monic such that } P(F) = 0\}.$$
This situation corresponds to that of an algebraic curve $\mathcal{C}(\mathbb{F}_p)$ defined over the finite field $\mathbb{F}_p$ by some equation, for instance
$$\mathrm{Eq}(x, y) = 0, \quad \mathrm{Eq}(U, V) \in \mathbb{F}_p[U, V],$$
with a map to the projective line $\mathbb{P}^1(\mathbb{F}_p)$. The ring $\mathcal{O}_K$ corresponds to those algebraic functions on $\overline{\mathcal{C}(\mathbb{F}_p)}$ defined over $\mathbb{F}_p$ which are regular outside the preimage $x^{-1}(\infty)$.

REMARK III.6. The fact that in all three cases A is a PID provides additional structures on the rings $\mathcal{O}_K$ by comparison with the general theory.

III.3. Factorisation into primes

In this section we will prove Theorem III.2. We start with some preparations.

LEMMA III.3.1 (Gauss' Lemma for ideals). *Let A be a domain and $\mathfrak{p}$ be a prime ideal. Let $\mathfrak{a}, \mathfrak{b}$ be ideals such that $\mathfrak{p}|\mathfrak{a}.\mathfrak{b}$ then either $\mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$.*

PROOF. Suppose that $\mathfrak{a} \not\subset \mathfrak{p}$, we will prove that $\mathfrak{b} \subset \mathfrak{p}$. We fix an element $a \in \mathfrak{a} - \mathfrak{p}$, which exists by assumption. Let $b \in \mathfrak{b}$; since $\mathfrak{a}.\mathfrak{b} \subset \mathfrak{p}$ we have $a.b \in \mathfrak{p}$ and, as $A/\mathfrak{p}$ is a domain, we either have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Since $a \notin \mathfrak{p}$, we have $b \in \mathfrak{p}$. As $b \in \mathfrak{b}$ was arbitrary, it follows that $\mathfrak{p}|\mathfrak{b}$. □

LEMMA III.3.2. *Let A be a noetherian ring and $\mathfrak{a}$ be a non-zero ideal, then $\mathfrak{a}$ contains a product of non-zero prime ideals.*

PROOF. Consider the set of all non-zero ideals $\mathfrak{a} \subset A$ which do not contain any product of non-zero prime ideals. Since A is noetherian this set contains a maximal element $\mathfrak{a}$ which is not prime. Therefore there exist $x, y \notin \mathfrak{a}$ such that $x.y \in \mathfrak{a}$. Consider the ideals

$$Ax + \mathfrak{a},\ Ay + \mathfrak{a}.$$

As they are strictly greater than $\mathfrak{a}$, they contain products of non-zero prime ideals

$$\mathfrak{p}_1.\cdots\mathfrak{p}_r \subset Ax + \mathfrak{a},\ \mathfrak{q}_1.\cdots\mathfrak{q}_s \subset Ay + \mathfrak{a}$$

and then

$$\mathfrak{p}_1.\cdots\mathfrak{p}_r.\mathfrak{q}_1.\cdots\mathfrak{q}_s \subset (Ax + \mathfrak{a})(Ax + \mathfrak{a}) \subset Axy + \mathfrak{a} = \mathfrak{a}.$$

This is a contradiction. □

DEFINITION III.5. *Let A a domain and $Q = \mathrm{Frac}(A)$. A subset $\mathfrak{f} \subset Q$ is a* fractional (A-)ideal *if there is $b \in A$ such that $\mathfrak{a} = b.\mathfrak{f}$ is a non-zero ideal in A.*

REMARK III.7. Note that a fractional ideal in a Dedekind ring (more generally a noetherian domain) is of finite type: if $\mathfrak{f} \subset Q$ is a fractional ideal and $b \in A - \{0\}$ such that $\mathfrak{a} = b.\mathfrak{f} \subset A$ is an ideal, then $\mathfrak{a}$ is of finite type (because A is noetherian) and therefore $\mathfrak{f} = b^{-1}.\mathfrak{a}$ is of finite type.

The following lemma will prove useful later on.

LEMMA III.3.3. *Let A be a Dedekind ring, $\mathfrak{a}$ a non-zero ideal in A, and $x \in \mathrm{Frac}(A)$. If $x\mathfrak{a} \subset \mathfrak{a}$, then $x \in A$.*

PROOF. If $x\mathfrak{a} \subset \mathfrak{a}$, then also $P(x)\mathfrak{a} \subset \mathfrak{a}$ for all $P \in A[X]$. Thus for any $b \in \mathfrak{a} \setminus \{0\}$ we have

$$bA[x] \subset \mathfrak{a} \subset A.$$

Moreover, $bA[x]$ is an ideal in A and, in particular, $A[x]$ is a fractional ideal and therefore of finite type. Thus x is integral over A. As A is integrally closed, it follows that $x \in A$. □

PROPOSITION III.3.4. *Let A be a Dedekind ring and $\mathfrak{p} \subset A$ be a maximal/prime ideal. There exists a fractional ideal $\mathfrak{p}^{-1} \subset \mathrm{Frac}(A)$ such that*

$$\mathfrak{p}.\mathfrak{p}^{-1} = A.$$

Moreover, we have $A \subsetneq \mathfrak{p}^{-1}$.

PROOF. Let

$$\mathfrak{p}^{-1} = \{x \in Q \colon x.\mathfrak{p} \subset A\}.$$

We will show that $\mathfrak{p}.\mathfrak{p}^{-1} = A$.

By definition, $\mathfrak{p}^{-1}$ is an A-module containing A and $\mathfrak{p}.\mathfrak{p}^{-1} \subset A$. Moreover for any $b \in \mathfrak{p} - \{0\}$, we have $\mathfrak{p}^{-1}.b \subset A$ and therefore $\mathfrak{p}^{-1}$ is a fractional ideal.

We have $A \subset \mathfrak{p}^{-1}$ and hence

$$\mathfrak{p} \subset \mathfrak{p}.\mathfrak{p}^{-1} \subset A.$$

Since $\mathfrak{p}$ is maximal, this implies that either

$$\mathfrak{p}.\mathfrak{p}^{-1} = \mathfrak{p} \text{ or } \mathfrak{p}.\mathfrak{p}^{-1} = A.$$

Suppose $\mathfrak{p}.\mathfrak{p}^{-1} = \mathfrak{p}$. For $x \in \mathfrak{p}^{-1}$, we have $x.\mathfrak{p} \subset \mathfrak{p}$ and therefore $x \in A$ by Lemma III.3.3. As x was arbitrary, this implies that $\mathfrak{p}^{-1} \subset A$. Therefore $\mathfrak{p}^{-1} = A$. We will derive a contradiction.

Let $a \in \mathfrak{p} - \{0\}$. By Lemma III.3.2, there exists $r \geqslant 1$ and r prime ideals $\mathfrak{p}_i$, $i = 1, \cdots, r$, such that

$$\mathfrak{p}_1.\cdots.\mathfrak{p}_r \subset A.a \subset \mathfrak{p};$$

let us also assume that r is minimal with this property.

Since

$$\mathfrak{p}_1.\cdots.\mathfrak{p}_r \subset \mathfrak{p},$$

Gauss' lemma for ideals implies that there is i (say $i = 1$) such that

$$\mathfrak{p}_1 \subset \mathfrak{p}.$$

Since $\mathfrak{p}_1$ is maximal, we have $\mathfrak{p}_1 = \mathfrak{p}$. Setting $\mathfrak{b} = \mathfrak{p}_2.\cdots.\mathfrak{p}_r$, we therefore have

$$\mathfrak{p}.\mathfrak{b} \subset A.a.$$

By the minimality of r, $\mathfrak{b}$ is not contained in $A.a$. Thus we fix $b \in \mathfrak{b}$ such that $b \notin A.a$. We have

$$b.\mathfrak{p} \subset A.a$$

so that (multiply both sides by a^{-1})

$$b.a^{-1}\mathfrak{p} \subset A,$$

hence $b.a^{-1} \in \mathfrak{p}^{-1} = A$. Multiplying both sides by a, we obtain that $b \in A.a$, a contradiction. □

III.3.1. Proof of Theorem III.2. We can now prove Theorem III.2. Let $\mathfrak{a} \neq A$ be a non-zero proper ideal which is not a product of prime ideals and which is maximal for this property. Let $\mathfrak{p}$ be a maximal ideal containing $\mathfrak{a}$. We have a strict inclusion

$$\mathfrak{a} \subset \mathfrak{p}$$

and if we multiply both sides by the fractional ideal $\mathfrak{p}^{-1}$ we obtain

$$\mathfrak{p}^{-1}\mathfrak{a} \subset A$$

and since $A \subset \mathfrak{p}^{-1}$ we also have $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$. The inclusion

$$\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$$

is strict: suppose that

$$\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a},$$

then for any $x \in \mathfrak{p}^{-1}$ we have $x.\mathfrak{a} \subset \mathfrak{a}$ and thus $x \in A$ by Lemma III.3.3. In particular, we find that $\mathfrak{p}^{-1} \subset A$, which is in contradiction to Proposition III.3.4.

By the maximality of $\mathfrak{a}$, the ideal $\mathfrak{p}^{-1}\mathfrak{a}$ which is strictly bigger than $\mathfrak{a}$ is a product of prime ideals and $\mathfrak{a} = \mathfrak{p}.\mathfrak{p}^{-1}\mathfrak{a}$ is the product of $\mathfrak{p}$ and of this product of prime ideals, which is a contradiction.

Let us show that this decomposition is unique. Suppose that we have

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} = \prod_{\mathfrak{p}} \mathfrak{p}^{v'_{\mathfrak{p}}(\mathfrak{a})}.$$

Suppose that $\mathfrak{q} \in \mathrm{Spec}(A)$ is such that $v_{\mathfrak{q}}(\mathfrak{a}) > v'_{\mathfrak{q}}(\mathfrak{q})$. Multiplying both sides by $(\mathfrak{q}^{-1})^{v'_{\mathfrak{q}}(\mathfrak{a})}$, we obtain

$$\mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{a}) - v'_{\mathfrak{q}}(\mathfrak{a})} \prod_{\mathfrak{p} \neq \mathfrak{q}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} = \prod_{\mathfrak{p} \neq \mathfrak{q}} \mathfrak{p}^{v'_{\mathfrak{p}}(\mathfrak{a})}.$$

Therefore $\mathfrak{q} | \prod_{\mathfrak{p} \neq \mathfrak{q}} \mathfrak{p}^{v'_{\mathfrak{p}}(\mathfrak{a})}$ and by Gauss' Lemma $\mathfrak{q}$ contains one of the $\mathfrak{p} \neq \mathfrak{q}$, which is not possible since the $\mathfrak{p}$ are maximal and distinct from $\mathfrak{q}$. □

III.3.2. Extension to fractional ideals. Let us recall that a fractional ideal $\mathfrak{f} \subset Q$ is a subset of the shape $\mathfrak{f} = b^{-1}\mathfrak{a}$, where $\mathfrak{a}$ is a non-zero ideal in A and $b \in A - \{0\}$.

Let $\mathfrak{f}, \mathfrak{f}'$ be two fractional ideals. We define their sum to be the A-module generated by sums of elements from $\mathfrak{f}$ and $\mathfrak{f}'$,

$$\mathfrak{f} + \mathfrak{f}' = \{f + f' \colon f \in \mathfrak{f}, f' \in \mathfrak{f}'\}$$

and their product $\mathfrak{f}.\mathfrak{f}'$ to be the A-module generated by their products,

$$\mathfrak{f}.\mathfrak{f}' = \big(\{f.f' \colon f \in \mathfrak{f}, f' \in \mathfrak{f}'\}\big).$$

The A-modules $\mathfrak{f}+\mathfrak{f}', \mathfrak{f}.\mathfrak{f}'$ and $\mathfrak{f}\cap\mathfrak{f}'$ are all fractional ideals: if $\mathfrak{f} = b^{-1}.\mathfrak{a},\ \mathfrak{f}' = {b'}^{-1}.\mathfrak{a}'$ for $b, b' \in A-\{0\}$ and $\mathfrak{a}, \mathfrak{a}' \in \mathcal{I}_A$, then

$$bb'(\mathfrak{f} + \mathfrak{f}') = b'.\mathfrak{a} + b.\mathfrak{a}', \quad (bb').\mathfrak{f}.\mathfrak{f}' = \mathfrak{a}.\mathfrak{a}', \quad bb'.\mathfrak{f} \cap \mathfrak{f}' = b'.\mathfrak{a} \cap b.\mathfrak{a}'.$$

Let $\mathfrak{f} = b^{-1}.\mathfrak{a}$ a fractional ideal and consider the factorisations

$$(b) = b.A = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(b)},\ \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})};$$

we have therefore

$$b.\mathfrak{f} = (b).\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(b)}.\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

and multiplying by powers of the fractional ideals $\mathfrak{p}^{-1}$, we see that

$$\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a}) - v_{\mathfrak{p}}(b)}.$$

We can deduce the following

THEOREM III.4. *Let A be a Dedekind ring with field of fractions Q. Every fractional ideal $\mathfrak{f}$ factors as a product of primes ideals (possibly with negative exponents): there exists a unique function*

$$v_\bullet(\mathfrak{f})\colon \begin{array}{ccc} \mathrm{Spec}(A) & \mapsto & \mathbb{Z} \\ \mathfrak{p} & \mapsto & v_{\mathfrak{p}}(\mathfrak{f}) \end{array}$$

such that

- $v_{\{0\}}(\mathfrak{f}) = 0$
- *for a.e. $\mathfrak{p}$, $v_{\mathfrak{p}}(\mathfrak{f}) = 0$, and*
- *(setting $\mathfrak{p}^0 = A$) one has the following factorisation*

$$\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f})}.$$

- *For*

$$\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f})},\ \mathfrak{f}' = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f}')}$$

two fractional ideals, we have

$$\mathfrak{f}.\mathfrak{f}' = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f}) + v_{\mathfrak{p}}(\mathfrak{f}')}.$$

- *If we define the fractional ideal*

$$\mathfrak{f}^{-1} := \prod_{\mathfrak{p}} \mathfrak{p}^{-v_{\mathfrak{p}}(\mathfrak{f})}$$

we have

$$\mathfrak{f}.\mathfrak{f}^{-1} = A.$$

– *In addition we have*

$$\mathfrak{f}' \subset \mathfrak{f} \iff \mathfrak{f} | \mathfrak{f}' \iff \forall \mathfrak{p}\ v_{\mathfrak{p}}(\mathfrak{f}) \leqslant v_{\mathfrak{p}}(\mathfrak{f}').$$
$$\mathfrak{f} + \mathfrak{f}' =: (\mathfrak{f}, \mathfrak{f}') = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(v_{\mathfrak{p}}(\mathfrak{f}), v_{\mathfrak{p}}(\mathfrak{f}'))},$$
$$\mathfrak{f} \cap \mathfrak{f}' =: [\mathfrak{f}, \mathfrak{f}'] = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(v_{\mathfrak{p}}(\mathfrak{f}), v_{\mathfrak{p}}(\mathfrak{f}'))}$$
$$(\mathfrak{f}, \mathfrak{f}').[\mathfrak{f}, \mathfrak{f}'] = \mathfrak{f}.\mathfrak{f}'.$$

DEFINITION III.6. *Given $\mathfrak{f}$ a non-zero fractional ideal, the exponent $v_{\mathfrak{p}}(\mathfrak{f})$ is called the $\mathfrak{p}$-adic valuation of $\mathfrak{f}$. This is the largest integer v such that $\mathfrak{p}^v | \mathfrak{f}$ (i.e. $\mathfrak{f} \subset \mathfrak{p}^v$). For $\mathfrak{f} = (0)$ we set $v_{\mathfrak{p}}(\{0\}) = +\infty$.*

III.3.3. The ideal class group. From the above discussion we have the following

COROLLARY III.3.1. *Let A be a Dedekind domain with field of fractions Q. The set $\mathcal{F}_A$ of fractional ideals in Q equipped with the multiplication of fractional ideals forms a commutative group whose identity element is the ideal A. Moreover $(\mathcal{F}_A, .)$ is isomorphic to the free commutative group (of formal finite integral linear combinations) generated by the non-zero prime ideals*

$$(\mathcal{F}_A, .) \simeq \mathrm{Div}(\mathrm{Spec}(A)) = \left\{ \sum_{\mathfrak{p}} v_{\mathfrak{p}}.\mathfrak{p} \colon v_{\mathfrak{p}} \in \mathbb{Z},\ v_{\mathfrak{p}} = 0 \text{ for a.e. } \mathfrak{p} \right\}$$

via the map

$$\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f})} \mapsto \sum_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{f}).\mathfrak{p}.$$

DEFINITION III.7. *A fractional ideal is* principal *if it is of the form $(f) = f.A$ for $f \in Q^\times$. We denote by*

$$\mathcal{PF}_A \subset \mathcal{F}_A$$

the set of principal fractional ideals.

Observe that the product of two principal ideals is principal. One has

LEMMA III.3.5. *The set of principal fractional ideals $\mathcal{PF}_A$ forms a subgroup of $\mathcal{F}_A$ under multiplication and the map*

$$(\bullet) \colon \begin{array}{ccc} Q^\times & \mapsto & \mathcal{PF}_A \\ f & \mapsto & (f) = f.A \end{array}$$

is a group morphism whose kernel is the group of units

$$\ker((\bullet)) = A^\times.$$

DEFINITION III.8. *The ideal class group of A is the quotient*

$$\mathrm{Cl}(A) := \mathcal{F}_A / \mathcal{PF}_A.$$

Observe that $\mathrm{Cl}(A)$ is trivial if and only if A is a PID and that, in general, $\mathrm{Cl}(A)$ is generated by the classes of prime ideals in $\mathcal{F}_A$.

III.4. Stability of the Dedekind property

In this section we prove Theorem III.3 which we recall is the following.

THEOREM. *Let A be a Dedekind ring with field of fractions Q and suppose that K/Q is a finite separable extension, then $\mathcal{O}_K(A)$ is an A-module of finite type and a Dedekind ring.*

For what follows, we will assume that we are given a fixed algebraic closure $\overline{Q}$ of Q and an extension $Q \subset K \subset \overline{Q}$ as in Theorem III.3. It is clear that $\mathcal{O}_K(A)$ is a domain and integrally closed. We thus have to show that every ideal of $\mathcal{O}_K(A)$ is of finite type and that every prime ideal is maximal. For this we will need the separability hypothesis.

Let us recall the following characterization of separability for finite extensions.

THEOREM. *A finite field extension K/Q is separable if and only if one of the following equivalent conditions is satisfied.*

- *For any $z \in K$, the linear map $[\times z]\colon K \mapsto K$ is diagonalisable (over $\overline{Q}$).*
- *For any $z \in K$, its minimal polynomial $P_{Q,\min,z}(X)$ has simple roots.*
- *The trace bilinear form*

$$\langle \cdot, \cdot \rangle_{K/Q}\colon \begin{array}{ccc} K \times K & \mapsto & Q \\ (z, z') & \mapsto & \mathrm{tr}_{K/Q}(z.z') = \mathrm{tr}\big([\times z.z']_{K/Q}\big) \end{array}$$

  is non-degenerate.
- *Let $\overline{Q}$ be an algebraic closure of Q. Then $|\mathrm{Hom}_Q(K, \overline{Q})| = [K\colon Q]$.*

Let us also recall that if $[K\colon Q]$ is coprime to $\mathrm{car}(Q)$ or if Q is a finite field then K/Q is always separable.

Let $d = [K\colon Q]$ be the degree of the field extension.

LEMMA III.4.1. *One has*

$$\mathcal{O}_K(A) = \{z \in K\colon P_{K/Q,\mathrm{char},z}(X) \in A[X]\}.$$

PROOF. As $P_{K/Q,\mathrm{char},z}$ is monic, it suffices to show that $P_{K/Q,\mathrm{char},z} \in A[X]$ for any $z \in \mathcal{O}_K(A)$. As of Proposition A.3.3 and Theorem A.5, we have

$$P_{K/Q,\mathrm{char},z}(X) = P_{Q,\min,z}(X)^{[K\colon Q[z]]}.$$

Thus it suffices to show that for $z \in \mathcal{O}_K(A)$ we have $P_{Q,\min,z} \in A[Z]$. Let $z_i \in \overline{Q}$, $i = 1, \ldots, r$ denote the pairwise distinct roots of $P_{Q,\min,z}$. Suppose that $P \in A[X]$ is a monic polynomial such that $P(z) = 0$. Then $P_{Q,\min,z} | P$ and hence $P(z_i) = 0$ for all the roots z_i. In particular, all the z_i are integral over A. Moreover, the coefficients of

$$P_{Q,\min,z}(X) = \prod_i (X - z_i)$$

are sums of products of the z_i and therefore contained in $A[z_1, \ldots, z_r] \cap Q$. Note that $A[z_1, \ldots, z_r]$ is of finite type over A by integrality of the z_i and thus all the coefficients of $P_{Q,\min,z}$ are integral over A. As A is integrally closed, it follows that $P_{Q,\min,z} \in A[X]$. □

LEMMA III.4.2. *For any $z \in K$, there exists $b \in A$ such that $b.z \in \mathcal{O}_K(A)$.*

PROOF. Let

$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0,\ a_i \in K,\ a_0 \neq 0$$

be an annihilating polynomial of z and let $b \in A - \{0\}$ be such that $ba_i \in A$. We have

$$b^d P(z) = 0 = (bz)^d + a_{d-1}b(bz)^{d-1} + \cdots + b^d a_0$$

and therefore $bz \in \mathcal{O}_K(A)$. □

PROPOSITION III.4.3. *The ring $\mathcal{O}_K(A)$ is an A-module of finite type. If A is a PID, then B is free of rank $d = [K : Q]$.*

PROOF. Let $z_1, \cdots z_d$ be a Q-basis of K. There is $b \in A - \{0\}$ such that $bz_1, \cdots, bz_d \in \mathcal{O}_K(A)$. Then $bz_1, \cdots, bz_d$ is a Q-basis, so we may assume without loss of generality that $z_1, \cdots, z_d \in \mathcal{O}_K(A)$ to begin with. In particular, $\mathcal{O}_K(A)$ contains the A-module $Az_1 + \cdots + Az_d$, which is of finite type. Since $\mathrm{tr}_{K/Q}$ is non-degenerate, there is a dual basis $(z_1^*, \cdots, z_d^*) \in K^d$: the unique basis such that

$$\mathrm{tr}_{K/Q}(z_i z_j^*) = \delta_{ij}.$$

We claim that

$$\mathcal{O}_K(A) \subset Az_1^* + \cdots + Az_d^*.$$

Indeed for any $z \in \mathcal{O}_K(A)$ we have

$$z = \sum_i \alpha_i z_i^*$$

and $\mathrm{tr}_{K/Q}(zz_i) = \alpha_i \in A$. For the latter inclusion, note that $zz_i \in \mathcal{O}_K(A)$ and hence its trace belongs to A. In particular, $\mathcal{O}_K(A)$ is a sub-module of an f.t. A-module, so it is f.t. Moreover, if A is a PID, $\mathcal{O}_K(A)$ contains a free submodule of rank d and is contained in such a free rank d module, so it is free of rank d. □

COROLLARY III.4.1. *The ring $\mathcal{O}_K(A)$ is noetherian. If A is a PID, every non-zero ideal in $\mathcal{O}_K(A)$ is a free A-module of rank $d = [K : Q]$.*

PROOF. Since $\mathcal{O}_K(A)$ is an A-module of f.t. and A is noetherian, the same holds for any $\mathcal{O}_K(A)$-ideal and, in particular, any $\mathcal{O}_K(A)$-ideal is of f.t. over $\mathcal{O}_K(A)$. Moreover, if A is a PID, any non-zero ideal $\mathfrak{b}$ of $\mathcal{O}_K(A)$ satisfies for any $b \in \mathfrak{b} - \{0\}$ that

$$b.\mathcal{O}_K(A) \subset \mathfrak{b} \subset \mathcal{O}_K(A),$$

so $\mathfrak{b}$ is free of rank d. □

COROLLARY III.4.2. *Suppose that $K/\mathbb{Q}$ is a number field and let $\mathcal{O}_K$ be the maximal order in K; cf. Theorem II.1. Then $\mathcal{O}_K = \mathcal{O}_K(\mathbb{Z})$.*

PROOF. Exercise.

LEMMA III.4.4. *Every non-zero prime ideal of $\mathcal{O}_K(A)$ is maximal.*

PROOF. Let $\mathfrak{P} \subset \mathcal{O}_K(A)$ be a non-zero prime ideal, then

$$k_{\mathfrak{P}} := \mathcal{O}_K(A)/\mathfrak{P}$$

is a domain. Let $\mathfrak{p} = A \cap \mathfrak{P}$, and let

$$k_{\mathfrak{p}} := A/\mathfrak{p}.$$

We have the canonical injection

$$A/\mathfrak{p} \hookrightarrow \mathcal{O}_K(A)/\mathfrak{P}$$

which implies that $k_{\mathfrak{p}}$ is a domain (since $\mathcal{O}_K(A)/\mathfrak{P}$ is a domain).

In order to see that $\mathfrak{p} \neq 0$, let $z \in \mathfrak{P}$ non-zero. As z is integral over A, there is $P(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in A[X]$ satisfying $a_0 \neq 0$ and $P(z) = 0$. Then

$$0 \neq a_0 = -z^r - a_{r-1}z^r - \cdots - a_1 z \in \mathfrak{p}.$$

As A is Dedekind, it follows that $k_{\mathfrak{p}} = A/\mathfrak{p}$ is a field.

We can now show that $\mathfrak{P} \subset \mathcal{O}_K(A)$ is a maximal ideal, i.e., $\mathcal{O}_K(A)/\mathfrak{P}$ is a field. As of Proposition III.4.3, we know that $\mathcal{O}_K(A)$ is of finite type over A and, in particular, $\mathcal{O}_K(A)/\mathfrak{P}$ is $k_{\mathfrak{p}}$-algebra of finite dimension which is also a domain. We claim that any such algebra is a field. To this end, let $z \in \mathcal{O}_K(A)/\mathfrak{P}$ non-zero. Then $k_{\mathfrak{p}}[z] \subseteq \mathcal{O}_K(A)$ is a subspace and, hence, of finite dimension. In particular, there exist $a_0, \ldots, a_d \in k_{\mathfrak{p}}$ not all zero such that

$$0 = \sum_{j=0}^{d} a_j z^j.$$

Let j_* minimal such that $a_{j_*} \neq 0$, then

$$0 = \sum_{j=j_*}^{d} a_j z^j = z^{j_*} \sum_{j=j_*}^{d} a_j z^{j-j_*}$$

and, since $\mathcal{O}_K(A)/\mathfrak{P}$ is a domain, we have

$$0 = \sum_{j=j_*}^{d} a_j z^{j-j_*}.$$

In particular, we obtain

$$1 = \left(-a_{j_*}^{-1} \sum_{j=j_*+1}^{d} a_j z^{j-j_*-1} \right) z.$$

Thus z is a unit and it follows that $\mathcal{O}_K(A)/\mathfrak{P}$ is a field.

III.5. Dedekind rings: relative theory

For what follows, we let A be a Dedekind ring, $Q = \mathrm{Frac}(A)$ its field of fractions. Let K/Q a finite separable extension and we denote by $B = \mathcal{O}_K(A)$ the integral closure of A in K. We have seen that B is a Dedekind ring.

We denote by $\mathrm{Spec}(A)$ and $\mathrm{Spec}(B)$ the set of prime ideals of A and B respectively.

In what follows, given any subset $S \subset B$, we denote by $S.B \subset B$ the ideal generated by S. Using this notation, the set of ideals of A and B are related by the following maps:

$$\bullet \cap A \colon \mathfrak{b} \mapsto \mathfrak{b} \cap A, \ \bullet.B \colon \mathfrak{a} \mapsto \mathfrak{a}.B.$$

The ideal $\mathfrak{b} \cap A$ is sometimes called the *contraction* of $\mathfrak{b}$ and the ideal $\mathfrak{a}.B$ is called the *extension* of $\mathfrak{a}$. The maps are correspondingly called the contraction and the extension map.

We will examine these two maps and for by factorisation of ideals it is sufficient to focus on the sets of (non-zero) prime ideals in $\mathrm{Spec}(A)$ and $\mathrm{Spec}(B)$.

We have more or less already seen the following

LEMMA III.5.1. *Given non-zero $\mathfrak{P} \in \mathrm{Spec}(B)$, the intersection $\mathfrak{p} = \mathfrak{P} \cap A$ is a non-zero prime ideal in A.*

PROOF. We have an injective map

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$$

and therefore $A/\mathfrak{p}$ is a domain so $\mathfrak{p}$ is prime. In order to see that $\mathfrak{p}$ is non-zero, note that for any $z \in \mathfrak{P} - \{0\}$, the constant term of the minimal polynomial of z (which is non-zero) is contained in $\mathfrak{p}$. □

We have therefore a canonical projection (or contraction) map

$$\bullet \cap A : \begin{array}{ccc} \mathrm{Spec}(B) & \mapsto & \mathrm{Spec}(A) \\ \mathfrak{P} & \mapsto & \mathfrak{P} \cap A \end{array}.$$

PROPOSITION III.5.2. *The map $\bullet \cap A$ is surjective and for any non-zero $\mathfrak{p} \in \mathrm{Spec}(A)$ the preimage of $\mathfrak{p}$, i.e. the set of $\mathfrak{P} \in \mathrm{Spec}(B)$ such that $\mathfrak{p} = \mathfrak{P} \cap A$, is exactly the set of prime ideals appearing in the prime decomposition of the B-ideal $\mathfrak{p}.B$:*

$$\mathfrak{P} \cap A = \mathfrak{p} \iff \mathfrak{P} | \mathfrak{p}.B \iff v_{\mathfrak{P}}(\mathfrak{p}.B) > 0.$$

PROOF. If $\mathfrak{p}$ is the zero-ideal, then $\mathfrak{p}$ is the image of the zero ideal under the projection map.

Let now $\mathfrak{p} \in \mathrm{Spec}(A)$ non-zero. By maximality of non-zero prime ideals in A, we know that for any $\mathfrak{P} \in \mathrm{Spec}(B)$ we have

$$\mathfrak{p} = \mathfrak{P} \cap A \iff \mathfrak{p} \subset \mathfrak{P}.$$

Now we note that by definition of divisibility

$$\mathfrak{p} \subset \mathfrak{P} \iff \mathfrak{p}.B \subset \mathfrak{P} \iff \mathfrak{P} | \mathfrak{p}.B \iff v_{\mathfrak{P}}(\mathfrak{p}.B) > 0.$$

This completes the description of the preimage of $\mathfrak{p}$. It remains to prove surjectivity.

As B is a Dedekind domain, the unique factorization of ideals implies that it suffices to show that $\mathfrak{p}.B$ is proper ($\mathfrak{p}.B \neq B$): any prime $\mathfrak{P}$ dividing $\mathfrak{p}.B$ will contain $\mathfrak{p}$.

By uniqueness of prime factorization in A there is some $z \in \mathfrak{p} - \mathfrak{p}^2$ and $A.z = \mathfrak{p}\mathfrak{a}$ for some ideal $\mathfrak{a} \subset A$ coprime to $\mathfrak{p}$. Let $a \in \mathfrak{a} - \mathfrak{p}$.

If $\mathfrak{p}.B = B$, then $a.B = a\mathfrak{p}.B \subset A.z.B = B.z$ and, thus, there is $b \in B$ such that $a = b.z$. As $a, z \in A - \{0\}$, it follows that $b \in B \cap Q = A$ and thus $a \in A.z \subset \mathfrak{p}$, which is absurd.

□

Remark III.8. The main step in the proof of surjectivity was to show that $\mathfrak{p}.B \neq B$. A more general argument, which does not rely on A being integrally closed, follows the proof of the Nakayama lemma; cf. the proof of Proposition III.1. Assuming for the sake of contradiction that $B = \mathfrak{p}.B$, we fix a set of generators $z_1, \dots, z_d$ of B as an A-module and find $(a_{ij})_{i,j=1}^d \in \mathfrak{p}^{d\times d}$ such that

$$\forall i \quad \sum_{j=1}^{d} (\delta_{ij} - a_{ij}).z_j = 0.$$

Therefore there is a matrix $M \in A^{d\times d}$ such that $\det(M).b = 0$ for all $b \in B$ and $\det(M) \equiv 1 \,(\mathrm{mod}\, \mathfrak{p})$, which is absurd since B is a domain.

Definition III.9. *Given a non-zero $\mathfrak{p} \in \mathrm{Spec}(A)$, we denote by*

$$\mathrm{Spec}_{\mathfrak{p}}(B) = \{\mathfrak{P} \in \mathrm{Spec}(B) \colon \mathfrak{P}|\mathfrak{p}.B\} = \{\mathfrak{P} \colon v_{\mathfrak{P}}(\mathfrak{p}.B) > 0\}$$

the fiber of the projection map.

A prime ideal $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$ is said to "lie above" $\mathfrak{p}$ or to "divide" $\mathfrak{p}$ and we write simply $\mathfrak{P}|\mathfrak{p}$.

We have (by definition) for $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$

$$\mathfrak{p} = \mathfrak{P} \cap A.$$

We will need the following generalisation later

Lemma III.5.3. *Let $\mathfrak{p} \in \mathrm{Spec}(A)$ be a non-zero prime ideal and $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$. For any $1 \leqslant e \leqslant v_{\mathfrak{P}}(\mathfrak{p}.B)$, we have*

$$\mathfrak{p} = \mathfrak{P}^e \cap A.$$

Proof. Exercise.

Notice that $\mathrm{Spec}_{\mathfrak{p}}(B)$ is finite since this is the set of primes dividing $\mathfrak{p}.B$. We will see that the cardinality is at most $[K : Q]$.

Let us first introduce some further terminology.

Ramification index.

Definition III.10. *Given a non-zero $\mathfrak{p} \in \mathrm{Spec}(A)$, the exponent $v_{\mathfrak{P}}(\mathfrak{p}.B)$ in the decomposition*

$$\mathfrak{p}.B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{p}.B)}$$

is called the ramification index of $\mathfrak{P}$ (at $\mathfrak{p}$). It is denoted

$$v_{\mathfrak{P}}(\mathfrak{p}.B) =: e_{\mathfrak{P}/\mathfrak{p}},$$

so that

$$\mathfrak{p}.B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}.$$

Residue fields and inertia degree.

DEFINITION III.11. *Given a non-zero $\mathfrak{p} \in \mathrm{Spec}(A)$,the quotient $A/\mathfrak{p}$ is a field called the residue field of A at $\mathfrak{p}$; it is denoted $k_\mathfrak{p}$.*

Given $\mathfrak{P} \in \mathrm{Spec}_\mathfrak{p}(B)$ non-zero, let $k_\mathfrak{P}$ be the residue field of B at $\mathfrak{P}$. Since $\mathfrak{P} \cap A = \mathfrak{p}$ we have an injective map

$$k_\mathfrak{p} = A/\mathfrak{p} \hookrightarrow k_\mathfrak{P} = B/\mathfrak{P}$$

which makes $k_\mathfrak{P}$ an extension of $k_\mathfrak{p}$. Moreover, since B is an A-module of f.t., this extension is finite.

DEFINITION III.12. *The degree of the extension $k_\mathfrak{p} \hookrightarrow k_\mathfrak{P}$ is denoted*

$$[k_\mathfrak{P} : k_\mathfrak{p}] = f_{\mathfrak{P}/\mathfrak{p}}.$$

It is called the inertia degree *of $\mathfrak{P}$ (at $\mathfrak{p}$).*

NOTATION. If the base ring $A \subset Q$ is understood (so that $\mathfrak{p} = A \cap \mathfrak{P}$) we will simply write

$$f_{\mathfrak{P}/\mathfrak{p}} = f_\mathfrak{P},\ \mathfrak{P}/\mathfrak{p} = e_\mathfrak{P}.$$

III.5.1. The degree formula. Given $\mathfrak{p} \in \mathrm{Spec}(A)$ a non-zero prime ideal, the quotient

$$K_\mathfrak{p} := B/\mathfrak{p}.B$$

is a $k_\mathfrak{p}$-algebra of finite dimension. We will study the structure of this algebra in greater detail.

THEOREM III.5. *We have*

$$\dim_{k_\mathfrak{p}}(K_\mathfrak{p}) = [K : Q] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}}.$$

In particular,

$$|\mathrm{Spec}_\mathfrak{p}(B)| \leqslant [K : Q].$$

LEMMA III.5.4. *If A is a PID, then B is a free A-module of rank $d = [K : Q]$ and*

$$[K : Q] = \dim_{k_\mathfrak{p}}(K_\mathfrak{p}).$$

PROOF. Indeed, let $a \in A$ such that $\mathfrak{p} = (a)$ and let $(z_1, \dots, z_d) \in B^d$ be an A-basis of B. We claim that the images of $z_1, \dots, z_d$ mod $\mathfrak{p}.B$ are linearly independent over $k_\mathfrak{p}$. Note that $\mathfrak{p}.B$ is a free A-module with A-basis $(az_1, \dots, az_d) \in B^d$.

Suppose that $a_1, \dots, a_d \in A$ are such that

$$a_1 z_1 + \cdots + a_d z_d \in \mathfrak{p}.B,$$

i.e., there are $r_1, \dots, r_d \in A$ such that

$$(a_1 - ar_1)z_1 + \cdots + (a_d - ar_d)z_d = 0.$$

As by assumption $(z_1, \dots, z_d)$ is linearly independent over A, it follows that $a_i \in \mathfrak{p}$ for all $1 \leqslant i \leqslant d$ and thus the images of the z_i mod $\mathfrak{p}.B$ are linearly independent over $k_\mathfrak{p}$. □

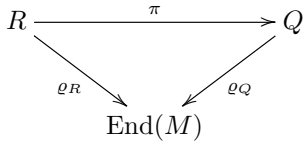
We will establish the formula

$$[K : Q] = \dim_{k_\mathfrak{p}}(K_\mathfrak{p})$$

in full generality later (as we have already seen, this is true if A is a PID; we will reduce to that case). For now we focus on the right hand side of the equality. We start with the following Lemma.

LEMMA III.5.5. *For any $e \geqslant 0$, the A-module structure on the quotient $\mathfrak{P}^e/\mathfrak{P}^{e+1}$ admits a compatible $k_\mathfrak{p}$-module structure and as such, it has $k_\mathfrak{p}$-dimension $f_{\mathfrak{P}/\mathfrak{p}}$.*

REMARK III.9. Let M be an abelian group, let $\pi\colon R \to Q$ be a ring homomorphism, and suppose that there we are given homomorphisms $\varrho_R\colon R \to \mathrm{End}(M)$ and $\varrho_Q\colon Q \to \mathrm{End}(Q)$. The induced module structures are *compatible* (with π) if the diagram



commutes. Recall that for a ring R and an R-module M, the set

$$\mathrm{Ann}(M) = \{r \in R\colon \forall m \in M\, rm = 0\}$$

is an ideal, called the annihilator. Moreover, for any ideal $I \lhd R$ the module M admits a *compatible* (for the canonical projection) R/I-module structure if and only if $I \subseteq \mathrm{Ann}(M)$.

PROOF OF LEMMA III.5.5. Since $\mathfrak{P}^{e+1} \subseteq \mathfrak{P}^e$ is a B-submodule, the quotient is a B-module and, in particular, an A-module. Clearly, we have that $\mathfrak{P} \subseteq \mathrm{Ann}(\mathfrak{P}^e/\mathfrak{P}^{e+1})$ and, therefore, both the A- and B-module structures admit compatible $k_\mathfrak{p}$- and $k_\mathfrak{P}$-structures.

Since $\dim_{k_\mathfrak{p}}(k_\mathfrak{P}) = f_{\mathfrak{P}|\mathfrak{p}}$, it is sufficient to show that $\dim_{k_\mathfrak{P}}(\mathfrak{P}^e/\mathfrak{P}^{e+1}) = 1$. For this we observe that there is a bijection between the $k_\mathfrak{P}$-subspaces of $\mathfrak{P}^e/\mathfrak{P}^{e+1}$ and the B-submodules of $\mathfrak{P}^e$ containing $\mathfrak{P}^{e+1}$ or in other terms the B-ideals satisfying $\mathfrak{P}^e \subset \mathfrak{a} \subset \mathfrak{P}^{e+1}$. But the only such ideals are either $\mathfrak{P}^e$ or $\mathfrak{P}^{e+1}$. □

PROOF OF THE SECOND EQUALITY IN THEOREM III.5. First we observe that for $\mathfrak{P}$ and $\mathfrak{P}'$ distinct and above $\mathfrak{p}$ the ideals $\mathfrak{P}^{e_\mathfrak{P}/\mathfrak{p}}$ and $\mathfrak{P}'^{e_{\mathfrak{P}'/\mathfrak{p}}}$ are coprime so by the Chinese reminder theorem, we have an isomorphism of $k_\mathfrak{p}$-algebras:

$$B/\mathfrak{p}.B \simeq \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}.$$

In particular we have

$$\dim_{k_\mathfrak{p}}(B/\mathfrak{p}.B) = \sum_{\mathfrak{P}|\mathfrak{p}} \dim_{k_\mathfrak{p}}(B/\mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}).$$

We now prove that

$$\dim_{k_\mathfrak{p}}(B/\mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}) = e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}}$$

If $e_{\mathfrak{P}|\mathfrak{p}} = 1$, this is clear. Suppose now that $1 \leqslant e < e_{\mathfrak{P}|\mathfrak{p}}$. Then we have an exact sequence of $k_\mathfrak{p}$-vector spaces

$$0 \longrightarrow \mathfrak{P}^e/\mathfrak{P}^{e+1} \longrightarrow B/\mathfrak{P}^{e+1} \longrightarrow B/\mathfrak{P}^e \longrightarrow 0.$$

so by recurrence the conclusion follows from Lemma III.5.5 below. □

III.5.2. Localization. As mentioned above, if A is a PID, then

$$\dim_{k_\mathfrak{p}} K_\mathfrak{p} = [K : Q] = d \tag{III.1}$$

and together with the previous discussion, this establishes the degree formula when A is a PID.

We will prove that (III.1) is true in general:

THEOREM III.6. *Under the above assumptions (A is a Dedekind ring and B is the integral closure of a finite separable extension of Q), we have for any non-zero $\mathfrak{p} \in \mathrm{Spec}(A)$,*

$$\dim_{k_\mathfrak{p}} B/\mathfrak{p}.B = [K : Q] = d$$

and hence

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}} = [K : Q].$$

For this we need the *localization* technique.

III.5.2.1. *Localization.* Let A be a general ring and $\mathfrak{p} \in \mathrm{Spec}(A)$ a prime ideal. By Gauss lemma, the set $S_\mathfrak{p} = A - \mathfrak{p}$ is multiplicative:

$$\forall x, y \in S_\mathfrak{p},\ x.y \in S_\mathfrak{p}.$$

Definition III.13. *The localization of A at $\mathfrak{p}$ is the set of equivalence classes*

$$\{(a,q) \in A \times S_\mathfrak{p}\}/\sim,\ (a,q) \sim (a',q') \iff \exists s \in S_\mathfrak{p}\ (aq' - a'q)s = 0.$$

The equivalence class of (a,q) is denoted as a fraction $\frac{a}{q}$. The set $A_\mathfrak{p}$ has a ring structure for the usual addition and multiplication of fractions

$$\frac{a}{q} + \frac{a'}{q'} = \frac{aq' + a'q}{qq'},\ \frac{a}{q}.\frac{a'}{q'} = \frac{aa'}{qq'}.$$

Remark III.10. The map

$$f_\mathfrak{p} : \begin{array}{ccc} A & \mapsto & A_\mathfrak{p} \\ a & \mapsto & \frac{a}{1} \end{array}$$

is a ring homomorphism which, in general, need not be injective. However, if A is a domain, then $f_\mathfrak{p}$ is injective and $A_\mathfrak{p}$ is a subring of the field of fractions Q:

$$A_\mathfrak{p} = \left\{ \frac{a}{q} : a \in A,\ q \in A - \mathfrak{p} \right\} \subset Q = \mathrm{Frac}(A)$$

(the subring formed of fractions having at least one denominator not belonging to $\mathfrak{p}$).

Proposition III.5.6. *If A is a Dedekind ring, then $A_\mathfrak{p}$ is a PID and $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}.A_\mathfrak{p}$ is the unique (proper and) maximal ideal of $A_\mathfrak{p}$. Moreover any ideal of $A_\mathfrak{p}$ is of the shape $\mathfrak{m}_\mathfrak{p}^k$ for some $k \geqslant 0$.*

Proof. Exercise. □

Definition III.14. *A generator of the ideal $\mathfrak{p}.A_\mathfrak{p}$ is called a uniformizer at $\mathfrak{p}$. It is usually denoted π or $\pi_\mathfrak{p}$.*

We compare the residue fields

$$k_\mathfrak{p} = A/\mathfrak{p} \text{ and } k_{\mathfrak{m}_\mathfrak{p}} := A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}.$$

Proposition III.5.7. *The injection $A \hookrightarrow A_\mathfrak{p}$ induces an isomorphism*

$$k_\mathfrak{p} \simeq k_{\mathfrak{m}_\mathfrak{p}}.$$

Proof. Exercise. □

Let

$$B_\mathfrak{p} = \left\{ \frac{b}{q} : b \in B,\ q \in A - \mathfrak{p} \right\} \subset K.$$

The set $B_\mathfrak{p} = B.A_\mathfrak{p}$ is a ring extension of $A_\mathfrak{p}$. In particular, $B_\mathfrak{p} \subseteq K$ is a subring containing B.

Proposition III.5.8. *The integral closure of $A_\mathfrak{p}$ in K is $B_\mathfrak{p}$.*

In particular (since $A_\mathfrak{p}$ is a PID), $B_\mathfrak{p}$ is a free module $A_\mathfrak{p}$-module of rank $[K:Q]$ and $B_\mathfrak{p}/\mathfrak{p}.B_\mathfrak{p}$ is a $k_{\mathfrak{m}_\mathfrak{p}} = k_\mathfrak{p}$-algebra of dimension $[K:Q]$.

Proof. Consider $b/q \in B_\mathfrak{p}$. We have

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0,\ a_i \in A$$

and

$$(b/q)^n + a_{n-1}q^{-1}(b/q)^{n-1} + \cdots + a_0 q^{-n} = 0$$

but $a_{n-1}q^{-1}, \cdots, a_0 q^{-n}$ belong to $A_\mathfrak{p}$. This shows that $B_\mathfrak{p}$ is contained in the integral closure of $A_\mathfrak{p}$.

Conversely suppose that $x \in K$ is $A_\mathfrak{p}$-integral, i.e., there exists

$$n \geqslant 1 \text{ and } \frac{a_i}{q_i} \in A_\mathfrak{p},\ a_i \in A,\ q_i \in A - \mathfrak{p},\ i = 1, \cdots n$$

such that

$$x^n + \frac{a_{n-1}}{q_{n-1}}x^{n-1} + \cdots + \frac{a_0}{q_0} = 0.$$

Let $q := q_0.\cdots.q_{n-1} \in A - \mathfrak{p}$. Clearing denominators, one obtains that $b = q.x$ is A-integral and therefore belongs to B. Thus b/q belongs to $B_{\mathfrak{p}}$. □

PROPOSITION III.5.9. *We have an isomorphism of $k_{\mathfrak{p}}$-algebras*

$$B/\mathfrak{p}.B \simeq B_{\mathfrak{p}}/\mathfrak{p}.B_{\mathfrak{p}}.$$

In particular

$$\dim_{k_{\mathfrak{p}}}(B/\mathfrak{p}.B) = [K : Q].$$

PROOF. We first show that $B \cap \mathfrak{p}.B_{\mathfrak{p}} = \mathfrak{p}.B$. The inclusion $\supset$ is clear. To prove $\subset$, we note that

$$\mathfrak{p}.B_{\mathfrak{p}} = \left\{ \frac{r}{q} \colon r \in \mathfrak{p}.B,\ q \in A - \mathfrak{p} \right\}$$

and therefore, for $b \in B$, we have that $b \in \mathfrak{p}.B_{\mathfrak{p}}$ if and only if there is $q \in A - \mathfrak{p}$ such that $q.b \in \mathfrak{p}.B$. In particular, for any such $b \in B$ and for any $\mathfrak{P}|\mathfrak{p}$, we have $q.b \in \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}$ and since $q \notin \mathfrak{P}$ we have $b \in \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}$. Therefore

$$b \in \bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}} = \mathfrak{p}.B.$$

This proves $\subset$.

The map $B/\mathfrak{p}.B \to B_{\mathfrak{p}}/\mathfrak{p}.B_{\mathfrak{p}}$ is therefore injective and it is surjective by the same argument as in the proof of Proposition III.5.7. □

This last proposition concludes the proof of Theorem III.6 and hence of the degree formula.

III.5.3. $\mathfrak{p}$-adic valuation. Let $A \subset Q$ be a Dedekind ring and $\mathfrak{p}$ a prime. We define the $\mathfrak{p}$-adic valuation at $\mathfrak{p}$ as the function

$$v_{\mathfrak{p}} \colon \begin{array}{ccc} Q - \{0\} & \mapsto & \mathbb{Z} \\ z & \mapsto & v_{\mathfrak{p}}(z) = v_{\mathfrak{p}}(z.A) \end{array}$$

and we set $v_{\mathfrak{p}}(0) = +\infty$. For any $p > 1$ we define the $\mathfrak{p}$-adic absolute value (in base p) as the function

$$|\bullet| \colon \begin{array}{ccc} q & \mapsto & \mathbb{R}_{\geqslant 0} \\ z & \mapsto & |z| = p^{-v_{\mathfrak{p}}(z)}. \end{array}$$

This absolute value is multiplicative

$$|z.w| = |z|.|w|$$

and satisfies an enhanced version of the triangle inequality:

$$|z + w| \leqslant \max(|z|, |w|)$$

with equality if $|z| \neq |w|$. The $\mathfrak{p}$-adic distance is the function

$$d(\bullet,\bullet) \colon \begin{array}{ccc} Q \times Q & \mapsto & \mathbb{R}_{\geqslant 0} \\ (z, z') & \mapsto & d(z, z') = |z - z'|. \end{array}$$

This gives Q the structure of a metric space such that

$$B_Q(0,1) = \{z \in Q \colon d(z,0) = |z| \leqslant 1\} = A_{\mathfrak{p}}$$
$$B_{o,Q}(0,1) = \{z \in Q \colon d(z,0) = |z| < 1\} = \mathfrak{p}.A_{\mathfrak{p}}.$$

A sequence $(u_n)_{n\geqslant 0} \in Q^{\mathbb{N}}$ is Cauchy iff

$$u_{n+1} - u_n \to 0.$$

The completion of Q with respect to this absolute value (so that any Cauchy sequence is converging) is called the $\mathfrak{p}$-adic completion of Q. This is a complete metric field such that the closed unit ball is $\overline{A_{\mathfrak{p}}}$ and the open unit ball is $\overline{\mathfrak{p}.A_{\mathfrak{p}}}$ and such that the converging series $\sum_{n\geqslant 0} u_n$ are the series whose general term u_n converge to 0.

III.6. Ramification

In this section we investigate the values of the ramification index $e_{\mathfrak{P}/\mathfrak{p}}$. In particular we show that

$$e_{\mathfrak{P}/\mathfrak{p}} = 1$$

for all but finitely many $\mathfrak{p}$.

DEFINITION III.15. *Let k be a field. A k-algebra B_k is reduced if it does not contain any non-trivial nilpotent element: i.e. an element $x \in B_k - \{0\}$ such that $x^n = 0$ for some $n \geqslant 1$.*

DEFINITION III.16. *The prime $\mathfrak{p} \in \mathrm{Spec}(A)$ is ramified in K if $B/\mathfrak{p}.B$ is not reduced. Otherwise $\mathfrak{p}$ is unramified in B.*

PROPOSITION III.6.1. *A prime $\mathfrak{p}$ is ramified in K iff $e_{\mathfrak{P}/\mathfrak{p}} > 1$ for some $\mathfrak{P}$ above $\mathfrak{p}$.*

PROOF. We have an isomorphism of $k_{\mathfrak{p}} = A/\mathfrak{p}$-algebras.

$$B/\mathfrak{p}.B \simeq \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}.$$

If $e_{\mathfrak{P}/\mathfrak{p}} = 1$ for every $\mathfrak{P}$, $B/\mathfrak{p}.B$ is a product of fields and therefore does not contain any non-trivial nilpotent element: $B/\mathfrak{p}.B$ is reduced and $\mathfrak{p}$ is unramified.

On the other hand, if $e_{\mathfrak{P}/\mathfrak{p}} > 1$ for some $\mathfrak{P}$ above $\mathfrak{p}$, any element $x \in \mathfrak{P} - \mathfrak{P}^2$ defines a class modulo $\mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}$ satisfying

$$x^{e_{\mathfrak{P}/\mathfrak{p}}-1} \neq 0 \,(\mathrm{mod}\, \mathfrak{P}^e_{\mathfrak{P}/\mathfrak{p}}) \text{ but } x^e_{\mathfrak{P}/\mathfrak{p}} = 0 \,(\mathrm{mod}\, \mathfrak{P}^e_{\mathfrak{P}/\mathfrak{p}}).$$

The algebra $B/\mathfrak{p}.B$ is then not reduced. The prime $\mathfrak{p}$ is ramified in B and one says that $\mathfrak{p}$ is ramified at $\mathfrak{P}$.

□

III.6.1. The discriminant ideal. Let us recall that a field extension K/Q of degree d is separable if and only if

- The trace linear form $\mathrm{tr}_{K/Q} : K \to Q$ is non-zero (hence onto) or equivalently,
- The trace bilinear form

$$\langle \bullet, \bullet \rangle_{K/Q} : \begin{array}{ccc} K \times K & \mapsto & Q \\ (x, y) & \mapsto & \mathrm{tr}_{K/Q}(xy) \end{array}$$

  is non-degenerate or equivalently,
- For any Q-basis $\vec{z} = (z_1, \cdots, z_d)$

$$\det(\langle z_i, z_j \rangle_{K/Q})_{i,j \leqslant d}) \neq 0.$$

DEFINITION III.17. *Let $A \subset Q \subset K$ be a Dedekind ring and $B \subset K$ its integral closure in a separable extension K/Q. The discriminant ideal is the ideal generated by the discriminants of d-tuples in B:*

$$\mathfrak{D}_{B/A} = \langle \{ \mathrm{disc}_{K/Q}(\vec{z}) \colon \vec{z} = (z_1, \cdots, z_d) \in B^d \} \rangle \subset A.$$

Observe that $\mathfrak{D}_{B/A} \subset A$ because for $\vec{z} = (z_1, \cdots, z_d) \in B^d$, the discriminant is a (multivariate) polynomial evaluated at the points $\{\mathrm{tr}_{K/Q}(z_i z_j) \colon 1 \leqslant i, j \leqslant d\}$, which are coefficients of characteristic polynomials of elements in K integral over A. Moreover, $\mathfrak{D}_{B/A}$ is a non-zero ideal: we have seen that B contains a Q-basis of K, say $\vec{z}$ and, since K/Q is separable, the trace is non-degenerate and therefore $\mathrm{disc}_{K/Q}(z_1, \cdots, z_d) \neq 0$.

Our main goal in this section is the proof of the following

THEOREM III.7 (Discriminant criterion of ramification). *If $\mathfrak{p} \in \mathrm{Spec}(A)$ is ramified, then $\mathfrak{p} | \mathfrak{D}_{B/A}$. In particular the set of ramified primes is finite.*

III.6.1.1. *The discriminant ideal for a PID.* In this section we assume that A is a PID: for instance $A = \mathbb{Z}$ or $\mathbb{F}_q[T]$ or A is the localisation at a prime of a Dedekind ring (see above).

We recall that this implies that B (and any B-ideal) is a free A-module of rank d and the discriminant ideal $\mathfrak{D}_{B/A} \subset A$ is principal.

PROPOSITION III.6.2. *For any A-basis $(z_1, \cdots, z_d) \in B^d$ of B, one has*

$$\mathfrak{D}_{B/A} = \mathrm{disc}_{K/Q}(z_1, \cdots, z_d).A.$$

PROOF. Let $(z_1, \cdots, z_d)$ be an A-basis of B then

$$\mathrm{disc}(z_1, \cdots, z_d).A \subset \mathfrak{D}_{B/A}.$$

Let $(z'_1, \cdots, z'_d) \in B^d$ be any other d-tuple. We have

$$z'_i = \sum_{j=1}^{d} a_{ij} z_j,\ a_{ij} \in A$$

and setting

$$M = (a_{ij})_{i,j \leqslant d} \in M_d(A)$$

we have

$$\mathrm{disc}(z'_1, \cdots, z'_d) = (\det M)^2 \mathrm{disc}(z_1, \cdots, z_d)$$

and since $\det M \in A$ it follows that

$$\mathrm{disc}(z'_1, \cdots, z'_d) \in \mathrm{disc}(z_1, \cdots, z_d).A$$

and therefore

$$\mathfrak{D}_{B/A} = \mathrm{disc}(z_1, \cdots, z_d).A.$$

□

REMARK III.11. If $(z_1, \cdots, z_d), (z'_1, \cdots, z'_d) \in B^d$ are A-bases of B, then the matrix $M \in M_d(A)$ is invertible and its inverse M^{-1} is also in $M_d(A)$, therefore

$$\det(M) \in A^\times$$

and $\mathrm{disc}(z'_1, \cdots, z'_d)$ and $\mathrm{disc}(z_1, \cdots, z_d)$ differ by $\det(M)^2$, the square of a unit in A. In particular, if $A = \mathbb{Z}$, $(\mathbb{Z}^\times)^2 = \{1\}$ and

$$\mathrm{disc}(z'_1, \cdots, z'_d) = \mathrm{disc}(z_1, \cdots, z_d),$$

therefore when $A = \mathbb{Z}$ the discriminant can be defined as the common value of the discriminant of any basis.

For the proof we will need a few properties of the discriminant ideal.

III.6.1.2. *Invariance under localisation.*

LEMMA III.6.3. *Let $\mathfrak{p}$ be a prime and $A_\mathfrak{p}$ and $B_\mathfrak{p}$ be the localisations of A and B at $\mathfrak{p}$. We have*

$$\mathfrak{D}_{B/A,\mathfrak{p}} = \mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$$

where $\mathfrak{D}_{B/A,\mathfrak{p}}$ is the localization of the discriminant ideal $\mathfrak{D}_{B/A}$.

PROOF. Exercise. □

The advantage of this lemma is that one can compute the discriminant ideal via localizations at various primes and the main benefit of localizing is that $A_\mathfrak{p}$ is a PID. This leads us to the next section.

III.6.1.3. *Proof of Theorem III.7.* Observe that for any prime $\mathfrak{p}$, the residual algebra $K_\mathfrak{p}$ satisifes

$$K_\mathfrak{p} = B/\mathfrak{p}.B \simeq B_\mathfrak{p}/\mathfrak{p}.B_\mathfrak{p}.$$

So in order to determine whether $\mathfrak{p}$ is ramified or not, it is sufficient to determine whether the algebra $B_\mathfrak{p}/\mathfrak{p}.B_\mathfrak{p}$ is reduced or not. We will use the trace criterion. Given $z \in B_\mathfrak{p}$ we denote by

$$\overline{z} = z \,(\mathrm{mod}\, \mathfrak{p}.B_\mathfrak{p}) \in B_\mathfrak{p}/\mathfrak{p}.B_\mathfrak{p}$$

the image under the reduction modulo $\mathfrak{p}.B_\mathfrak{p}$-map.

Since $A_\mathfrak{p}$ is a PID, $B_\mathfrak{p}$ is free of rank d. Let $(z_1, \cdots, z_d) \in B_\mathfrak{p}$ be an $A_\mathfrak{p}$-basis. Then

$$(\overline{z}_1, \cdots, \overline{z}_d) = \big(z_1 \,(\mathrm{mod}\, \mathfrak{p}.B_\mathfrak{p}), \cdots, z_d \,(\mathrm{mod}\, \mathfrak{p}.B_\mathfrak{p})\big)$$

is a $k_\mathfrak{p}$-basis of $K_\mathfrak{p}$; cf. the proof of Lemma III.5.4. For any $z \in B_\mathfrak{p}$ we have

$$[\times z]_{K/Q} B_\mathfrak{p} \subset B_\mathfrak{p},\ [\times z]_{K/Q}(\mathfrak{p}.B_\mathfrak{p}) \subset \mathfrak{p}.B_\mathfrak{p}.$$

In particular the matrix of $[\times z]_{K/Q}$ in the basis $(z_1, \cdots, z_d)$ has coefficients in $A_\mathfrak{p}$. Moreover, if $z \in \mathfrak{p}.B_\mathfrak{p}$, then $[\times z]_{K/Q}(B_\mathfrak{p}) \subset \mathfrak{p}.B_\mathfrak{p}$ and the matrix of $[\times z]_{K/Q}$ in the basis $(z_1, \cdots, z_d)$ has coefficients in $\mathfrak{p}.A_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$. It follows that the $k_\mathfrak{p}$-linear map $[\times \overline{z}]_{K_\mathfrak{p}/k_\mathfrak{p}}$ given by multiplication by $\overline{z}$ in $K_\mathfrak{p}$ is induced by the restriction to $B_\mathfrak{p}$ of $[\times z]_{K/Q}$: for $\overline{x} = x \,(\mathrm{mod}\, \mathfrak{p}.B_\mathfrak{p}) \in K_\mathfrak{p}$ we have

$$[\times \overline{z}]_{K_\mathfrak{p}/k_\mathfrak{p}}(\overline{x}) = \overline{z\overline{x}} = \overline{zx} = zx \,(\mathrm{mod}\, \mathfrak{p}.B_\mathfrak{p}) = [\times z]_{K/Q}(x) \,(\mathrm{mod}\, \mathfrak{p}.B_\mathfrak{p})$$

and that the matrix of $[\times \overline{z}]_{K_\mathfrak{p}/k_\mathfrak{p}}$ in the basis $(\overline{z}_1, \cdots, \overline{z}_d)$ is simply the reduction modulo $\mathfrak{m}_\mathfrak{p}$ of the matrix of $[\times z]_{K/Q}$; in particular we have

$$\mathrm{tr}_{K_\mathfrak{p}/k_\mathfrak{p}}(\overline{z}) = \mathrm{tr}_{K/Q}(z) \,(\mathrm{mod}\, \mathfrak{m}_\mathfrak{p})$$

and

$$\mathrm{disc}_{K_\mathfrak{p}/k_\mathfrak{p}}(\overline{z}_1, \cdots, \overline{z}_d) = \mathrm{disc}_{K/Q}(z_1, \cdots, z_d) \,(\mathrm{mod}\, \mathfrak{m}_\mathfrak{p}).$$

Suppose that $K_\mathfrak{p}/k_\mathfrak{p}$ is non-reduced, then any non-zero nilpotent element in this algebra is contained in the kernel of the dual map for the trace bilinear form $\langle \bullet, \bullet \rangle_{K_\mathfrak{p}/k_\mathfrak{p}}$: if $[\times \overline{z}]$ is nilpotent then for any $\overline{z}'$, $[\times \overline{z}\overline{z}']$ is also nilpotent and so

$$\langle \overline{z}, \overline{z}' \rangle_{K_\mathfrak{p}/k_\mathfrak{p}} = \mathrm{tr}_{K_\mathfrak{p}/k_\mathfrak{p}}(\overline{z}\overline{z}') = 0;$$

therefore the trace is degenerate and

$$\mathrm{disc}_{K_\mathfrak{p}/k_\mathfrak{p}}(\overline{z}_1, \cdots, \overline{z}_d) = 0_{k_\mathfrak{p}} = \mathrm{disc}_{K/Q}(z_1, \cdots, z_d) \,(\mathrm{mod}\, \mathfrak{m}_\mathfrak{p}).$$

This implies that

$$\mathfrak{p}.A_\mathfrak{p} | \mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = \mathfrak{D}_{B/A,\mathfrak{p}}$$

(by Lemma III.6.3) and therefore that

$$\mathfrak{p} | \mathfrak{D}_{B/A}.$$

□

For the converse we need a further assumption.

Hypothesis III.1. *The residue fields $k_\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$ are perfect: any finite extension of $k_\mathfrak{p}$ is separable.*

Theorem III.8. *Assume that Hypothesis III.1 holds. A prime $\mathfrak{p} \in \mathrm{Spec}(A)$ is ramified iff $\mathfrak{p} | \mathfrak{D}_{B/A}$.*

Proof. We need to show that if $\mathfrak{p} | \mathfrak{D}_{B/A}$ then $K_\mathfrak{p}/k_\mathfrak{p}$ is not reduced. We have $\mathfrak{p}.A_\mathfrak{p} | \mathfrak{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$ and therefore

$$\mathfrak{D}_{K_\mathfrak{p}/k_\mathfrak{p}} = \{0\} \in k_p,$$

so the trace form is degenerate on $K_\mathfrak{p}/k_\mathfrak{p}$. Since

$$K_\mathfrak{p}/k_\mathfrak{p} \simeq \prod_{\mathfrak{P}|\mathfrak{p}} B_\mathfrak{P}/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}},$$

the discriminant is the product of the discriminants of the $k_{\mathfrak{p}}$-algebras $B_{\mathfrak{P}}/\mathfrak{P}^{e_{\mathfrak{P}}}$ and one of them must be 0, say for $\mathfrak{P}$. If $e_{\mathfrak{P}|\mathfrak{p}} = 1$, then $B_{\mathfrak{P}}/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$ is the residue field $k_{\mathfrak{P}}$ and by Hypothesis III.1 is a separable extension of $k_{\mathfrak{p}}$. By the trace criterion for separability the discriminant is non zero; we must therefore have $e_{\mathfrak{P}|\mathfrak{p}} > 1$ and $B_{\mathfrak{P}}/\mathfrak{P}^{e_{\mathfrak{P}|\mathfrak{p}}}$ is not reduced. □

III.7. The Dedekind recipe, I

The Dedekind recipe is a systematic method to compute prime decompositions.

We consider the usual setting: $A \subset Q$ a Dedekind ring and $B \subset K$ its integral closure in a separable extension. Let $\mathfrak{D}_{B/A} \subset A$ be the discriminant ideal. Let $z \in B$ be such that $K = Q[z]$, let $P_z(X) \in A[X]$ be the minimal polynomial of z, and let

$$\mathrm{disc}(z) = \mathrm{disc}_{K/Q}(1, \cdots, z^{d-1}) \in A - \{0\}$$

be its discriminant. We have

$$\mathfrak{D}_{B/A} | (\mathrm{disc}(z)) \neq 0.$$

Let $\mathfrak{p}$ be a prime ideal. In many cases one can read the prime decomposition of $\mathfrak{p}$ from the decomposition of $P_z \pmod{\mathfrak{p}} \in k_{\mathfrak{p}}[X]$ into irreducible polynomials.

THEOREM III.9. *Assume that $\mathfrak{p}$ is such that*

$$v_{\mathfrak{p}}(\mathrm{disc}(z)) = v_{\mathfrak{p}}(\mathfrak{D}_{B/A}). \tag{III.2}$$

We have the equality of localized rings and ideals

$$(\mathrm{disc}(z))_{\mathfrak{p}} = \mathfrak{D}_{B/A,\mathfrak{p}}$$

and

$$B_{\mathfrak{p}} = A_{\mathfrak{p}}[z] \simeq A_{\mathfrak{p}}[X]/(P_z), \ (P_z) = P_z.A_{\mathfrak{p}}[X].$$

Set $\overline{P_z} = P_z \pmod{\mathfrak{p}} \in k_{\mathfrak{p}}[X]$ for the reduction of P_z modulo $\mathfrak{p}$ and let

$$\overline{P_z} = \prod_i \overline{P}_i^{e_i}$$

be the decomposition of the latter into irreducible factors in $k_{\mathfrak{p}}[X]$; for any such factor $\overline{P}_i$ we choose a lifting $P_i \in A[X]$ of $\overline{P}_i$, i.e., $P_i \pmod{\mathfrak{p}} = \overline{P}_i$.

The map

$$\overline{P}_i \mapsto \mathfrak{P}_{i,\mathfrak{p}} := \mathfrak{p}.B_{\mathfrak{p}} + P_i(z)B_{\mathfrak{p}} \mapsto (\mathfrak{p}.B_{\mathfrak{p}} + P_i(z)B_{\mathfrak{p}}) \cap B = \mathfrak{P}_i$$

is a bijection

$$\{\overline{P}_i, \ i\} \simeq \mathrm{Spec}(B_{\mathfrak{p}}) \simeq \mathrm{Spec}_{\mathfrak{p}}(B)$$

between the set of irreducible factors of $\overline{P}$, the set of prime ideals of $B_{\mathfrak{p}}$, and the set of prime ideals in B above $\mathfrak{p}$. Moreover in this bijection we have

$$f_{\mathfrak{P}_i/\mathfrak{p}} = \deg \overline{P}_i, \ e_{\mathfrak{P}_i/\mathfrak{p}} = e_i$$

REMARK III.12. Observe that for any prime $\mathfrak{p}$ and any $z \in B$ we have

$$v_{\mathfrak{p}}(\mathrm{disc}(z)) \geqslant v_{\mathfrak{p}}(\mathfrak{D}_{B/A}) \geqslant 0.$$

In particular, (III.2) holds as soon as $v_{\mathfrak{p}}(\mathrm{disc}(z)) = 0$, that is $\mathfrak{p} \not| \mathrm{disc}(z)$, which is the case for all but finitely many $\mathfrak{p}$. In the exercices we will see other sufficient conditions for (III.2) to hold.

REMARK III.13. In some cases, there exists $z \in B$ such that

$$B = A[z].$$

One says that B is a monogenic extension of A. In such a situation

$$\mathfrak{D}_{B/A} = \mathrm{disc}_{K/Q}(z).A$$

and (III.2) is true for every $\mathfrak{p}$.

For instance, the ring of integers $\mathcal{O}_K$ of a quadratic field $K/\mathbb{Q}$ is monogenic; this is also the case for the ring of integers of the n-th cyclotomic field

$$K = \mathbb{Q}(\zeta_n), \zeta_n = \exp\left(\frac{2\pi i}{n}\right).$$

CHAPTER IV

Galois extensions

Let A be a Dedekind domain with field of fraction Q, K a finite separable field extension of degree d and B the integral closure of A in K. We also assume that Hypothesis III.1 holds: for every $\mathfrak{p}$ and $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$, the residual extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is separable.

In this chapter we consider the case where K/Q is a Galois extension with Galois group denoted

$$G = \mathrm{Gal}(K/Q).$$

The field automorphisms in the Galois group preserve algebraic and integral structures and in particular integrality properties and prime ideals; we will investigate how these extra Galois symmetries influence the structure of rings of integers and the prime factorisation. We refer to §A.6 for the basics of Galois theory for fields.

IV.1. The decomposition and inertia subgroups

We recall that given $\varphi \in G$ we have

$$\varphi_{|Q} = \mathrm{Id}_Q$$

and in particular φ is the identity on A. Also we recall that for any $z \in K$ we have

$$P_{\mathrm{char},z,K/Q}(X) = \prod_{\varphi \in G} (X - \varphi(z)),\ \mathrm{tr}_{K/Q}(z) = \sum_{\varphi \in G} \varphi(z),\ \mathrm{Nr}_{K/Q}(z) = \prod_{\varphi \in G} \varphi(z).$$

We first make the following observations:

LEMMA IV.1.1. *For any $\varphi \in G$, we have*

$$\varphi(B) = B$$

and for any prime $\mathfrak{p} \in \mathrm{Spec}(A)$ and $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$,

$$\varphi(\mathfrak{P}) \in \mathrm{Spec}_{\mathfrak{p}}(B).$$

In other terms the group G acts on B and on $\mathrm{Spec}_{\mathfrak{p}}(B)$.

PROOF. For any $z \in B$, let $P_{\mathrm{char},z,K/Q} \in K[X]$ be its characteristic polynomial. Since $z \in B$, then $P_{\mathrm{char},z,K/Q}$ has coefficients in A and since A is invariant under φ, $\varphi(z)$ is a also root of $P_{\mathrm{char},z,K/Q}$ hence belongs to B; we recall the argument for the claim

$$0 = \varphi(P(z)) = \varphi(P)(\varphi(z)) = P(\varphi(z)).$$

Let $\mathfrak{P}$ be a prime ideal above $\mathfrak{p}$, since φ is an automorphism, we have

$$B/\mathfrak{P} \simeq \varphi(B)/\varphi(\mathfrak{P}) = B/\varphi(\mathfrak{P})$$

which is a field since $B/\mathfrak{P}$ is a field so $\varphi(\mathfrak{P}) \in \mathrm{Spec}(B)$. Moreover

$$\varphi(\mathfrak{P}) \cap A = \varphi(\mathfrak{P} \cap A) = \varphi(\mathfrak{p}) = \mathfrak{p}$$

so

$$\varphi(\mathfrak{P}) \in \mathrm{Spec}_{\mathfrak{p}}(B).$$

□

THEOREM IV.1. *The action $G \curvearrowright \mathrm{Spec}_{\mathfrak{p}}(B)$ is transitive.*

PROOF. Given $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$, suppose that there exists $\mathfrak{P}' \in \mathrm{Spec}_{\mathfrak{p}}(B)$ such that $\varphi(\mathfrak{P}') \neq \mathfrak{P}$ for any $\varphi \in G$. By the Chinese remainder theorem, there exists $x \in \mathfrak{P}$ such that for any $\varphi \in G$ we have $x \notin \varphi(\mathfrak{P}')$ and therefore $\varphi(x) \notin \mathfrak{P}'$. We have

$$\mathrm{Nr}_{K/Q}(x) = \prod_{\varphi} \varphi(x) = x \prod_{\varphi \neq \mathrm{Id}} \varphi(x) \notin \mathfrak{P}'$$

but

$$\mathrm{Nr}_{K/Q}(x) \in A \cap \mathfrak{P} = \mathfrak{p} \subset \mathfrak{P}$$

contradiction. □

COROLLARY IV.1.1. *The functions $\mathfrak{P} \to e_{\mathfrak{P}/\mathfrak{p}}$ and $\mathfrak{P} \to f_{\mathfrak{P}/\mathfrak{p}}$ are constant and noted $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ and we have*

$$d = e_{\mathfrak{p}}.f_{\mathfrak{p}}.|\mathrm{Spec}_{\mathfrak{p}}(B)|.$$

DEFINITION IV.1. *The decomposition group of $\mathfrak{P}$, $D_{\mathfrak{P}} \subset G$ is the stabilizer of the ideal $\mathfrak{P}$. Since the action is transitive all the decomposition subgroups $D_{\mathfrak{P}}$ of the primes above $\mathfrak{p}$ are conjugate to one another.*

Observe that by the orbit-stabilizer Theorem we have

$$d/|D_{\mathfrak{P}}| = |\mathrm{Spec}_{\mathfrak{p}}(B)| = d/(e_{\mathfrak{p}}.f_{\mathfrak{p}})$$

and therefore

$$|D_{\mathfrak{P}}| = e_{\mathfrak{p}}.f_{\mathfrak{p}}.$$

EXERCISE IV.1. Let $\mathfrak{P} \in \mathrm{Spec}(B)$ non-zero, $\mathfrak{p} = \mathfrak{P} \cap A$. Prove the following equivalences.

(1) $D_{\mathfrak{P}} = \{1\} \iff \mathfrak{p}$ is totally split in B, i.e., $|\mathrm{Spec}_{\mathfrak{p}}(B)| = [K\colon Q]$.
(2) $D_{\mathfrak{P}} = G \iff \mathfrak{p}$ is totally ramified in B, i.e., $|\mathrm{Spec}_{\mathfrak{p}}(B)| = 1$.

IV.1.1. The residual action of the decomposition subgroup. Since the decomposition subgroup fixes $\mathfrak{P}$, it acts on $k_{\mathfrak{P}} = B/\mathfrak{P}$:

$$\varphi(z + \mathfrak{P}) = \varphi(z) + \varphi(\mathfrak{P}) = \varphi(z) + \mathfrak{P}.$$

This action leaves $k_{\mathfrak{p}}$ invariant.

We have therefore a map (of reduction modulo $\mathfrak{P}$):

$$\bullet_{\mathfrak{P}}\colon \begin{array}{ccc} D_{\mathfrak{P}} & \mapsto & \mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, k_{\mathfrak{P}}) \\ \varphi & \mapsto & \varphi_{\mathfrak{P}} \end{array} \tag{IV.1}$$

where

$$\varphi_{\mathfrak{P}}(z \,(\mathrm{mod}\, \mathfrak{P})) := \varphi(z) \,(\mathrm{mod}\, \mathfrak{P}).$$

DEFINITION IV.2. *The kernel of the map $\bullet_{\mathfrak{P}}$ is called the inertia subgroup at $\mathfrak{P}$ and is denoted*

$$I_{\mathfrak{P}} = \{\varphi \in D_{\mathfrak{P}},\ \forall z \in B,\ \varphi(z) \equiv z \,(\mathrm{mod}\, \mathfrak{P})\}.$$

This is a normal subgroup of $D_{\mathfrak{P}}$ and all the inertia subgroups at the primes $\mathfrak{P}$ above $\mathfrak{p}$ are conjugate to one another.

THEOREM IV.2. *We assume that for every $\mathfrak{p} \in \mathrm{Spec}(A)$ the residue field $k_{\mathfrak{p}}$ is perfect.*
The extension $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is Galois, i.e.

$$\mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, \overline{k_{\mathfrak{P}}}) = \mathrm{Hom}_{k_{\mathfrak{p}}}(k_{\mathfrak{P}}, k_{\mathfrak{P}}) = \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$$

and $\bullet_{\mathfrak{P}}$ induces an isomorphism

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}). \tag{IV.2}$$

In particular we have

$$|I_{\mathfrak{P}}| = e_{\mathfrak{p}}.$$

Recall that $\mathfrak{p}$ is ramified iff

$$\exists \mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B),\ e_{\mathfrak{P}} > 1 \Longleftrightarrow \mathfrak{p} | \mathfrak{D}_{B/A}$$

and since

$$\forall \mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B),\ e_{\mathfrak{P}} = e_{\mathfrak{p}} = |I_{\mathfrak{P}}|$$

we have

COROLLARY IV.1.2. *The prime $\mathfrak{p}$ is unramified if and only if for one (and hence any) $\mathfrak{P}|\mathfrak{p}$, the inertia subgroup $I_{\mathfrak{P}}$ is trivial. In that case we have an isomorphism*

$$\bullet_{\mathfrak{P}} \colon D_{\mathfrak{P}} \simeq \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

Before starting the proof of Theorem IV.2 it will be convenient to introduce

IV.1.1.1. *The decomposition subfield.*

DEFINITION IV.3. *Let $\mathfrak{P} \in \mathrm{Spec}(B)$ non-zero. The* decomposition field $Z_{\mathfrak{P}}$ *of $\mathfrak{P}$ is the fixed field of the decomposition group of $\mathfrak{P}$, i.e.,*

$$Z_{\mathfrak{P}} = \{x \in K \colon \forall \varphi \in D_{\mathfrak{P}}, \varphi(x) = x\}.$$

By the Galois correspondence $K/Z_{\mathfrak{P}}$ is Galois with Galois group $D_{\mathfrak{P}}$.

Let

$$B_{Z_{\mathfrak{P}}} := B \cap Z_{\mathfrak{P}};$$

this is the integral closure of A in $Z_{\mathfrak{P}}$ and we can use the relative theory to study the prime ideals of $B_{Z_{\mathfrak{P}}}$.

THEOREM IV.3. *Let $\mathfrak{P} \in \mathrm{Spec}(B)$ non-zero, $\mathfrak{p} = \mathfrak{P} \cap A$, and $\mathfrak{P}_Z = \mathfrak{P} \cap B_{Z_{\mathfrak{P}}} \in \mathrm{Spec}(B_{Z_{\mathfrak{P}}}) - \{(0)\}$. We have therefore $\mathfrak{p}|\mathfrak{P}_Z|\mathfrak{P}$. Let $e_{\mathfrak{P}_Z|\mathfrak{p}}$ and $f_{\mathfrak{P}_Z|\mathfrak{p}}$ denote the ramification index and inertia degree for the extention $B_{Z_{\mathfrak{P}}}/A$.*

We have

(1) $\mathrm{Spec}_{\mathfrak{P}_Z}(B) = \{\mathfrak{P}\}$, i.e., $\mathfrak{P}_Z$ is totally ramified in B.
(2) $e_{\mathfrak{P}_Z} = e_{\mathfrak{p}}$ and $f_{\mathfrak{P}_Z} = f_{\mathfrak{p}}$ and $e_{\mathfrak{P}_Z|\mathfrak{p}} = f_{\mathfrak{P}_Z|\mathfrak{p}} = 1$.

In particular we have

$$k_{\mathfrak{P}_Z} = k_{\mathfrak{p}}.$$

PROOF. Exercise. □

IV.1.1.2. *Proof of Theorem IV.2.* By Hypothesis III.1 $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is separable. It is sufficient to show that $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is normal and that the map (IV.1) is surjective.

In what follows, we denote by $A \subset B' \subset B$ the integral closure of A in the decomposition field $Z_{\mathfrak{P}}$ of $\mathfrak{P}$. Recall that by Theorem IV.3 we have

$$k_{\mathfrak{P}_Z} = k_{\mathfrak{p}}.$$

Let $\overline{z} \in k_{\mathfrak{P}}$ be a primitive element for the separable extension $k_{\mathfrak{P}}/k_{\mathfrak{P}_Z} = k_{\mathfrak{P}}/k_{\mathfrak{p}}$ and $z \in B$ a lifting of $\overline{z}$, i.e., $z \,(\mathrm{mod}\, \mathfrak{P}) = \overline{z}$. Let

$$P_{\min,z,Z_{\mathfrak{P}}} = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in B'[X],$$

be its minimal polynomial.[1] Its roots are the $\varphi(z)$ as φ varies over $D_{\mathfrak{p}}$.

We may therefore consider its reduction modulo $\mathfrak{P}_Z$:

$$P_{\min,z,Z_{\mathfrak{P}}} \,(\mathrm{mod}\, \mathfrak{P}_Z) \in k_{\mathfrak{P}_Z}[X] = k_{\mathfrak{p}}[X].$$

Its roots are the reduction modulo $\mathfrak{P}$, of the $\varphi(z)$ as φ varies over $D_{\mathfrak{p}}$:

$$\varphi(z) \,(\mathrm{mod}\, \mathfrak{P}) = \varphi_{\mathfrak{P}}(\overline{z}) \in k_{\mathfrak{P}}.$$

[1] The integral closure of B' in K is B because this is already the integral closure of A. Hence z is integral over B'. This was proven as part of the proof of Lemma III.4.1

Since $\overline{z}$ is a primitive element of $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ whose conjugates (over $k_{\mathfrak{p}}$) are all in $k_{\mathfrak{P}}$, the field extension $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is normal hence Galois.

Moreover any automorphism $\eta \in \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is completely determined by the value $\eta(\overline{z})$ which are roots of $P_{\min,z,Z_{\mathfrak{P}}} \pmod{\mathfrak{P}_Z}$ and we have seen that any such root is of the shape $\varphi\mathfrak{P}(\overline{z})$ for some $\varphi \in D_{\mathfrak{P}}$; this implies that $\eta = \varphi\mathfrak{P}$ and the map $\bullet_{\mathfrak{P}}$ is surjective.

Since $|D_{\mathfrak{P}}| = e_{\mathfrak{p}}.f_{\mathfrak{p}}$ and $|\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})| = f_{\mathfrak{p}}$ it follows that

$$|I_{\mathfrak{P}}| = e_{\mathfrak{P}}.$$

□

IV.2. The case of finite residual fields

We make the following additional assumption:

HYPOTHESIS IV.1. *For any prime $\mathfrak{p} \in \mathrm{Spec}(A)$ the residual field $k_{\mathfrak{p}} = A/\mathfrak{p}$ is finite. In particular for $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$ the extension $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is automatically separable (and even Galois).*

EXAMPLE IV.1. This hypothesis is satisfied if $A = \mathbb{Z}$ ($Q = \mathbb{Q}$) or $A = \mathbb{F}_q[T]$ ($Q = \mathbb{F}_q(T)$) for $\mathbb{F}_q$ a finite field: in the first case $k_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and in the second case

$$\mathfrak{p} = (P) = P.\mathbb{F}_q[T],\ P(T) \in \mathbb{F}_q[T] \text{ irreducible and } k_{\mathfrak{p}} = \mathbb{F}_q[T]/(P) \simeq \mathbb{F}_q^d,\ d = \deg P.$$

Of course other cases are given by the integral closure of either of these rings in separable extensions of Q.

Let us recall that in this case the residual Galois group $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is cyclic and generated by the Frobenius:

$$\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) = \mathrm{frob}_q^{\mathbb{Z}},$$

where $q = |k_{\mathfrak{p}}|$ and

$$\mathrm{frob}_q : \begin{array}{ccc} k_{\mathfrak{P}} & \mapsto & k_{\mathfrak{P}} \\ x & \mapsto & x^q \end{array}.$$

DEFINITION IV.4. *Given $\mathfrak{p} \in \mathrm{Spec}(A)$ and $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$, the Frobenius at $\mathfrak{P}$, denoted*

$$(\mathfrak{P}, K/Q) \in D_{\mathfrak{P}}/I_{\mathfrak{P}},$$

is the preimage in $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ of frob_q under the isomorphism (IV.2).

In particular, if $\mathfrak{p}$ is unramified, $I_{\mathfrak{P}}$ is trivial and the Frobenius element

$$(\mathfrak{P}, K/Q) \in D_{\mathfrak{P}} \subset \mathrm{Gal}(K/Q)$$

belongs to the Galois group.

This element (if $\mathfrak{p}$ is unramified) is the unique element φ of $D_{\mathfrak{p}}$ such that

$$\forall z \in B,\ \varphi(z) \equiv z^q \pmod{\mathfrak{P}}. \tag{IV.3}$$

EXERCISE IV.2. Prove that if $\varphi \in \mathrm{Gal}(K/Q)$ satisfies, for some $\mathfrak{P} \in \mathrm{Spec}(B) - \{(0)\}$ which is unramified

$$\forall z \in B,\ \varphi(z) \equiv z^q \pmod{\mathfrak{P}}. \tag{IV.4}$$

(for $q = |k_{\mathfrak{p}}|$ and $\mathfrak{p} = A \cap \mathfrak{P}$) then

$$\varphi = (\mathfrak{P}, K/Q).$$

The next Lemma describes the action of the Galois group on Frobenius elements.

LEMMA IV.2.1. *For all $\varphi \in G$ we have*

$$\mathrm{Ad}(\varphi)(\mathfrak{P}, K/Q) = \varphi(\mathfrak{P}, K/Q)\varphi^{-1} = (\varphi(\mathfrak{P}), K/Q)$$

PROOF. Exercise. □

This lemma and the transitivity of the action $G \curvearrowright \mathrm{Spec}_{\mathfrak{p}}(B)$ implies that the set of Frobenius elements at the primes above $\mathfrak{p}$

$$\{(\mathfrak{P}, K/Q),\ \mathfrak{P}|\mathfrak{p}\}$$

form a single conjugacy class in G. This class bears a name:

DEFINITION IV.5. *Let $G = \mathrm{Gal}(K/Q)$ and $\mathfrak{p}$ unramified. The Frobenius at $\mathfrak{p}$ (or the Artin symbol at $\mathfrak{p}$) is the conjugacy class*

$$\mathrm{frob}_{\mathfrak{p}} := \left(\frac{K/Q}{\mathfrak{p}}\right) := \mathrm{Ad}(G)(\mathfrak{P}, K/Q) = \{(\mathfrak{P}, K/Q),\ \mathfrak{P}|\mathfrak{p}\} \subset G.$$

REMARK IV.1. If G is abelian, all conjugacy classes are composed of a single element; in particular all the elements $(\mathfrak{P}, K/Q),\ \mathfrak{P}|\mathfrak{p}$ in the Frobenius conjugacy class are equal. Abusing notations, we will write this element

$$\mathrm{frob}_{\mathfrak{p}} = (\mathfrak{p}, K/Q) = (\mathfrak{P}, K/Q) = \left(\frac{K/Q}{\mathfrak{p}}\right).$$

The importance of Frobenius elements is the following Theorem. In later chapters we will discuss more precise versions of it:

THEOREM IV.4. *Suppose that A is either $\mathbb{Z}$ or $\mathbb{F}_q[T]$ (or more generally the integral closure of either of these rings in separable extension of the field of fractions) and let B be the integral closure of A in a finite Galois extension of $Q = \mathrm{Frac}(A)$. Then the Frobenius elements $(\mathfrak{P}, K/Q)$, for $\mathfrak{P} \in \mathrm{Spec}(B)$ varying over the unramified prime s, generate $\mathrm{Gal}(K/Q)$.*

The proof of this result require the introduction of further tools from analysis.

IV.2.1. The Dedekind recipe II: Structure of the Frobenius automorphism. Related to the discussion in Section III.7 is the following version of Dedekind's recipe for Galois extensions.

Let A be a Dedekind domain such that its residue field are finite. Let $P \in A[X]$ (of degree $d \geqslant 1$) be a polynomial with coefficients in A, monic and separable, ie. the roots of P

$$\mathrm{root}_P(Q^{alg}) = \{z_1, z_2, \cdots, z_d\}$$

are distinct. In particular, its discriminant

$$\mathrm{disc}(P) = (-1)^{p(p-1)/2}\mathrm{res}(P, P') \in A - \{0\}.$$

Let

$$K = Q(P) = Q(z_1, z_2, \cdots, z_d) \subset Q^{alg}$$

be the splitting field of P and $n = [K : Q]$ be its degree; The extension K/Q is Galois with Galois group noted $G = \mathrm{Gal}(K/Q)$. Since the roots of P generate K/Q the Galois group G acts faithfully on $\mathrm{root}_P(K)$ and in that way can be identified with a subgroup of

$$\mathfrak{S}(\mathrm{root}_P(K)) \simeq \mathfrak{S}_d.$$

In other words, to $\varphi \in G$ one associates the (unique) permutation $\sigma \in \mathfrak{S}(\{1, \cdots d\})$ such that

$$\varphi(z_i) = z_{\sigma(i)},\ i = 1, \cdots, d.$$

THEOREM IV.5. *Let $\mathfrak{p} \in \mathrm{Spec}(A)$ be a prime not dividing $\mathrm{disc}(P) \in A$; then $\mathfrak{p}$ is unramified in K (in particular $\mathfrak{p} \not| \mathfrak{D}_{B/A}$).*

Let

$$P \,(\mathrm{mod}\, \mathfrak{p}) = \prod_{i=1}^{i_{\mathfrak{p}}} \overline{P}_i$$

be the decomposition of $P \pmod{\mathfrak{p}}$ *into irreducible factors (the multiplicities* e_i *are all* 1 *because* $\mathfrak{p}$ *is unramified in* $Q(z)$*). For any* $\mathfrak{P}$ *above* $\mathfrak{p}$*, the Frobenius at* $\mathfrak{P}$*,* $(\mathfrak{P}, K/Q)$*, when identified with an element of* $\mathfrak{S}_d$ *is a product of disjoint cycles of lengths*

$$f_i = \deg \overline{P_i},\ i = 1, \cdots, i_{\mathfrak{p}}.$$

REMARK IV.2. Notice that the f_i are not necessarily equal; these are the inertia degrees at the primes ideals above $\mathfrak{p}$ in the Q-extension $E = Q[z_1]$ but we do not necessarily assume that $K = E$ the f_i are not necessarily the inertia degrees of the $\mathfrak{P} \in \mathrm{Spec}_{\mathfrak{p}}(B)$. On the other hand we have

$$f_{\mathfrak{P}/\mathfrak{p}} = |D_{\mathfrak{P}}| = |(\mathfrak{P}, K/Q)^{\mathbb{Z}}| = lcm(f_i,\ i = 1, \cdots i_{\mathfrak{p}})$$

REMARK IV.3. Notice that if we chose a different $\mathfrak{P}'$ above $\mathfrak{P}$, the two Frobeniuses are conjugate to one another, so, as permutations, the lengths of the cycles in their cycle decompositions are the same.

PROOF. Let $B = \mathcal{O}_A(K)$ be the integral closure of A in K. Observe that since $\{z_1, z_2, \cdots, z_d\} \in B$. Given $\mathfrak{P}|\mathfrak{p}$ we set

$$\overline{z}_i = z_i \pmod{\mathfrak{P}} \in k_{\mathfrak{P}}.$$

We have the Sylvester factorisation formula for the discriminant

$$\mathrm{disc}(P) = \mathrm{disc}(1, z_1, z_1^2, \cdots, z_1^{d-1}) = \prod_{j>i}(z_j - z_i). \tag{IV.5}$$

This is an identify between elements of B which we can reduce modulo $\mathfrak{P}$.

Since $\mathfrak{p} \not| \mathrm{disc}(P)$ we have

$$\mathrm{disc}(P) \pmod{\mathfrak{P}} = \prod_{j>i}(\overline{z}_j - \overline{z}_i) \neq 0 \pmod{\mathfrak{P}}$$

and therefore

$$\forall i \neq j,\ z_j \not\equiv z_i \pmod{\mathfrak{P}}.$$

Let $\varphi \in D_{\mathfrak{P}} \subset G$ be such that $\sigma_{\mathfrak{P}} = \mathrm{Id}_{k_{\mathfrak{P}}}$. This implies that

$$\forall i \leqslant d,\ \varphi(z_i) = z_{\sigma(i)} \equiv z_i \pmod{\mathfrak{P}}$$

but since the $\overline{z}_i = z_i \pmod{\mathfrak{P}}$ are distinct this implies that $\varphi(z_i) = z_i$ and that $\varphi = \mathrm{Id}_K$: the map

$$\bullet_{\mathfrak{P}} : D_{\mathfrak{P}} \to \mathrm{Gal}_{k_{\mathfrak{p}}}(\overline{P})$$

is injective and $\mathfrak{p}$ is unramified (in particular $\mathfrak{p} \not| \mathfrak{D}_{B/A}$).

This also implies that

$$k_{\mathfrak{P}} = k_{\mathfrak{p}}[\overline{z}_1, z_2, \cdots, \overline{z}_d] = k_{\mathfrak{P}}(\overline{P})$$

is the splitting field of $\overline{P}$.

Moreover the orbits of $\mathrm{root}_{\overline{P}}(k_{\mathfrak{P}})$ under the action $\mathrm{Gal}_{k_{\mathfrak{p}}}(\overline{P})$ are the sets of roots of each $\overline{P}_i$ and the frobenius element $\mathrm{frob}_{\mathfrak{p}}$ acts on $\mathrm{root}_{\overline{P}}(k_{\mathfrak{P}})$ as a product of disjoint cycles of lengths $f_i = \deg \overline{P}_i,\ i \leqslant i_{\mathfrak{p}}$. Write $\sigma_{\mathfrak{P}} \in \mathfrak{S}_d$ the corresponding permulation: we have

$$\mathrm{frob}_{\mathfrak{p}}(\overline{z}_i) = \overline{z}_{\sigma_{\mathfrak{P}}(i)}.$$

Since for any i we have

$$(\mathfrak{P}, K/Q)(z_i) \equiv \mathrm{frob}_{\mathfrak{p}}(\overline{z}_i) \pmod{\mathfrak{P}} = z_{\sigma_{\mathfrak{P}}(i)} \pmod{\mathfrak{P}}$$

and the $z_i \pmod{\mathfrak{P}}$ are distinct we have

$$(\mathfrak{P}, K/Q)(z_i) = z_{\sigma_{\mathfrak{P}}(i)}.$$

□

CHAPTER V

Geometry of numbers

In the sequel we will study specifically two examples of Dedekind rings:

- Number field case: $Q = \mathbb{Q}$, $A = \mathbb{Z}$, $K/\mathbb{Q}$ is a finite extension (automatically separable) of degree n and B is the integral closure of $\mathbb{Z}$ in K. The ring B is then called the ring of algebraic integers of K and is denoted $\mathcal{O}_K$:
$$\mathcal{O}_K = \{z \in K \colon \exists P \in \mathbb{Z}[X],\ \text{monic},\ P(z) = 0\}.$$
- Function field case: Let $\mathbb{F}_q$ be a finite field of cardinality q and $A = \mathbb{F}_q[T]$, $Q = \mathbb{F}_q(T)$. Let $K/\mathbb{F}_q(T)$ be a finite separable extension of degree n and let $B = \mathcal{O}_K$ be the integral closure of $\mathbb{F}_q[T]$ in K:
$$\mathcal{O}_K = \{z \in K \colon \exists P \in \mathbb{F}_q[T][X],\ \text{monic},\ P(z) = 0\}.$$

In these two cases the ring A is a PID and the residue fields are finite fields:

- Number field case: the prime ideals of $\mathbb{Z}$ are the principal ideals $(p) = p\mathbb{Z}$ where p is a prime number so that $k_p = \mathbb{F}_p$ (and for $\mathfrak{P} \in \mathrm{Spec}_p(\mathcal{O}_K)$, $k_{\mathfrak{P}}/k_p$ is a finite extension so a finite field as well).
- Function field case: The prime ideals of $\mathbb{F}_q[T]$ are the principal ideals $(P) = P\mathbb{F}_q[T]$ generated by an irreducible polynomial $P \in \mathbb{F}_q[T]$, hence
$$k_P = \mathbb{F}_q[T]/(P) \simeq \mathbb{F}_{q^d},\ d = \deg(P).$$
(and for $\mathfrak{P} \in \mathrm{Spec}_P(\mathcal{O}_{\mathbb{F}_q[T]})$, $k_{\mathfrak{P}}/k_P$ is a finite extension so a finite field as well).

Let us recall that given a Dedekind ring $\mathcal{O}$ the ideal class group $\mathrm{Cl}(\mathcal{O})$ is the quotient of the group of fractional ideals by the principal ones. This is an abelian group which measures the obstruction to $\mathcal{O}$ to be a PID. In this chapter we will study the following finiteness theorem.

THEOREM V.1. *For $\mathcal{O}_K$ as above, the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

REMARK V.1. A general theorem of Claborn shows that given any abelian group G (possibly infinite, even possibly uncountable) there exist a Dedekind domain $\mathcal{O}$ such that
$$\mathrm{Cl}(\mathcal{O}) \simeq G.$$
Moreover $\mathcal{O}$ can even be obtained as a quadratic extension of a PID (Leedham-Green)!

One of the distinguishing feature of the number and function field cases by comparison with the general case is a finiteness result on ideals.

V.1. The norm of an ideal

LEMMA V.1.1. *For $\mathcal{O}_K$ as above, any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ has finite index in $\mathcal{O}_K$.*

PROOF. Indeed since $\mathbb{Z}$ or $\mathbb{F}_q[T]$ are PIDs, $\mathfrak{a}$ and $\mathcal{O}_K$ are free A-modules of rank $n = [K \colon Q]$ and one has
$$\mathcal{O}_K/\mathfrak{a} \simeq \prod_{i=1}^{u} A/a_i.A$$

for $a_i \in A - \{0\}$. If $A = \mathbb{Z}$ then $A/a_i.A$ is finite of order $|a_i|$ and $\mathcal{O}_K/\mathfrak{a}$ is finite of order

$$|\mathcal{O}_K/\mathfrak{a}| = \prod_i |a_i|.$$

If $A = \mathbb{F}_q[T]$, $a_i = a_i(T) \in \mathbb{F}_q[T] - \{0\}$ is a polynomial and $\mathbb{F}_q[T]/a_i(T).\mathbb{F}_q[T]$ is a $\mathbb{F}_q$-vector space of dimension $\deg a_i$ and $\mathbb{F}_q[T]/a_i(T).\mathbb{F}_q[T]$ is finite of order $q^{\deg a_i}$ so that

$$|\mathcal{O}_K/\mathfrak{a}| = q^{\sum_{i=1\cdots u} \deg a_i}.$$

□

Definition V.1. *For $\mathcal{O}_K$ as above, the numerical norm of any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ is defined as the index*

$$\mathrm{Nr}(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}| \in \mathbb{N}_{\geqslant 1}.$$

Proposition V.1.2. *The norm has the following properties*

- *Multiplicativity:*

$$\mathrm{Nr}(\mathfrak{a}.\mathfrak{b}) = \mathrm{Nr}(\mathfrak{a})\,\mathrm{Nr}(\mathfrak{b}).$$

In particular if

$$\mathfrak{a} = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{a})},$$

then

$$\mathrm{Nr}(\mathfrak{a}) = \prod_{\mathfrak{P}} \mathrm{Nr}(\mathfrak{P})^{v_{\mathfrak{P}}(\mathfrak{a})}.$$

- *If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_K$ above some prime ideal $\mathfrak{p}$ ($\mathfrak{p}$ is either $p\mathbb{Z}$ or $P\mathbb{F}_q[T]$ for P an irreducible polynomial), then we have*

$$\mathrm{Nr}(\mathfrak{P}) = \begin{cases} |\mathbb{Z}/p\mathbb{Z}|^{f_{\mathfrak{P}/p}} = p^{f_{\mathfrak{P}/p}} & \text{if } A = \mathbb{Z}, \\ |\mathbb{F}_q[T]/P|^{f_{\mathfrak{P}/P}} = q^{\deg(P) f_{\mathfrak{P}/P}} & \text{if } A = \mathbb{F}_q[T]. \end{cases} \tag{V.1}$$

Proof. By CRT the we have

$$\mathrm{Nr}(\mathfrak{a}.\mathfrak{b}) = \mathrm{Nr}(\mathfrak{a})\,\mathrm{Nr}(\mathfrak{b})$$

whenever $\mathfrak{a}$ and $\mathfrak{b}$ are coprime. It is sufficient to prove that for $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_K)$ a prime

$$\mathrm{Nr}(\mathfrak{P}^v) = \mathrm{Nr}(\mathfrak{P})^v$$

and that $\mathrm{Nr}(\mathfrak{P})$ is given by (V.1). The latter is immediate, since $k_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$ is a vector space of dimension $f_{\mathfrak{P}|\mathfrak{p}}$ over the residue field $k_{\mathfrak{p}}$ of the underlying base prime ideal $\mathfrak{p} = p\mathbb{Z}$ or $P\mathbb{F}_q[T]$. For the former, let u be any integer, then $\mathfrak{P}^u/\mathfrak{P}^{u+1}$ is a $k_{\mathfrak{P}}$-vector space of dimension 1 (cf. the Proof of Thm. III.5). In particular, by the preceding result, $|\mathfrak{P}^u/\mathfrak{P}^{u+1}| = \mathrm{Nr}(\mathfrak{P})$.

Moreover, we have the exact sequence of $\mathbb{Z}$-modules

$$0 \to \mathfrak{P}^u/\mathfrak{P}^{u+1} \to \mathcal{O}_K/\mathfrak{P}^{u+1} \to \mathcal{O}_K/\mathfrak{P}^u \to 0$$

where the second arrow is the canonical projection; therefore

$$\mathrm{Nr}(\mathfrak{P}^{u+1}) = |\mathcal{O}_K/\mathfrak{P}^{u+1}| = |\mathcal{O}_K/\mathfrak{P}^u|.|\mathfrak{P}^u/\mathfrak{P}^{u+1}| = \mathrm{Nr}(\mathfrak{P}^u)\,\mathrm{Nr}(\mathfrak{P}).$$

Thus the claim follows by induction on u. □

One reason for calling this a "norm" is the following

Proposition V.1.3. *For any $z \in \mathcal{O}_K - \{0\}$ we have*

$$\mathrm{Nr}(z.\mathcal{O}_K) = |\mathcal{O}_K/z.\mathcal{O}_K| = |A/\,\mathrm{Nr}_{K/Q}(z).A|.$$

Proof. This is a direct consequence of Prop. A.2.2 and of the definitions. □

EXERCISE V.1. Given $\mathfrak{a} \subset \mathcal{O}_K$ an ideal, its ideal norm $\mathrm{Nr}_{K/Q}(\mathfrak{a}) \subset A$ is the ideal generated by the norms of the elements of $\mathfrak{a}$. Prove that

$$\mathrm{Nr}(\mathfrak{a}) = |A/\mathrm{Nr}_{K/Q}(\mathfrak{a})|.$$

EXERCISE V.2. Let $\mathfrak{f} = \mathfrak{a}.\mathfrak{b}^{-1}$ be a fractional ideal. We define its norm as a rational number

$$\mathrm{Nr}(\mathfrak{f}) = \mathrm{Nr}(\mathfrak{a})/\mathrm{Nr}(\mathfrak{b})^{-1}.$$

Show that this is well defined and multiplicative.

The following finiteness result will be crucial.

PROPOSITION V.1.4. *For any $X \geqslant 1$ the number of ideals $\mathfrak{a} \subset \mathcal{O}_K$ of norm $\leqslant X$ is finite.*

PROOF. If $\mathrm{Nr}(\mathfrak{a}) \leqslant X$, then any prime ideal $\mathfrak{P}$ dividing $\mathfrak{a}$ has norm $\leqslant X$. Moreover, since any prime ideal is proper, i.e., $\mathrm{Nr}(\mathfrak{P}) \geqslant 2$, one has

$$v_{\mathfrak{P}}(\mathfrak{a}) \leqslant \log(X)/2,$$

so it is sufficient to show that the number of prime ideals of norm $\leqslant X$ is finite. Observe that the number of prime ideals of the base ring A of norm $\mathrm{Nr}_A(\mathfrak{p}) \leqslant X$ is finite: for $A = \mathbb{Z}$ this number is bounded by the number if positive integers $\leqslant X$ so is $\leqslant X$ and for $\mathbb{F}_q[T]$ this number is bounded by the number of monic polynomials with coefficients in $\mathbb{F}_q$ and of degree $\leqslant \log X/\log q$ so is also bounded by X. If $\mathfrak{P}$ is prime in $\mathcal{O}_K$ of norm $\mathrm{Nr}(\mathfrak{P}) \leqslant X$ then $\mathfrak{P}$ is above $\mathfrak{p} = \mathfrak{P} \cap A$ and we have

$$\mathrm{Nr}_A(\mathfrak{p}) = |k_{\mathfrak{p}}| \leqslant |k_{\mathfrak{P}}| = \mathrm{Nr}(\mathfrak{P}) \leqslant X$$

so there are only finitely many possible $\mathfrak{p}$ and above any such $\mathfrak{p}$ there are at most d primes $\mathfrak{P}$. □

EXERCISE V.3. Prove that for any $m \in \mathbb{N}_{\geqslant 1}$ and any $\varepsilon > 0$

$$r_K(m) := |\{\mathfrak{a} \subset \mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a}) = m\}| \ll \varepsilon, nm^{\varepsilon}.$$

For this, remark that $m \to r_K(m)$ is a multiplicative function and establish that bound for prime powers.

Show that as $X \to \infty$

$$|\{\mathfrak{a} \in \mathcal{O}_K :\ \mathrm{Nr}(\mathfrak{a}) \leqslant X\}| \leqslant X^{1+o(1)}.$$

Theorem V.1 is therefore a consequence of the following

THEOREM V.2. *For $\mathcal{O}_K$ as above, there is a constant $C(\mathcal{O}_K)$ such that any ideal class $[\mathfrak{a}]$ of $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a}$ of norm $\leqslant C(\mathcal{O}_K)$.*

PROOF. By the Proposition V.1.5 below, there exists $C = C(\mathcal{O}_K) > 0$ s.t. given any ideal $\mathfrak{a} \subset \mathcal{O}_K$, there exists $0 \neq a \in \mathfrak{a} \subset \mathcal{O}_K$, s.t. $\mathrm{Nr}(a) \leqslant C\,\mathrm{Nr}(\mathfrak{a})$. We have

$$\mathfrak{a} | a\mathcal{O}_K \iff a\mathcal{O}_K = \mathfrak{a}\mathfrak{b},\ \mathfrak{b} \subset \mathcal{O}_K$$

and

$$\mathrm{Nr}(a\mathcal{O}_K) = \mathrm{Nr}(\mathfrak{a})\,\mathrm{Nr}(\mathfrak{b}) \leqslant C\,\mathrm{Nr}(\mathfrak{a})$$

therefore

$$\mathrm{Nr}(\mathfrak{b}) \leqslant C.$$

Since $a\mathcal{O}_K = \mathfrak{a}\mathfrak{b}$ we have

$$[\mathfrak{b}] = [\mathfrak{a}]^{-1}.$$

When $\mathfrak{a}$ varies, the classes $[\mathfrak{b}]$ cover all of $\mathrm{Cl}(\mathcal{O}_K)$ and we are done. □

PROPOSITION V.1.5. *There exist $C = C(\mathcal{O}_K) \geqslant 0$ s.t. for any ideal $\mathfrak{a} \subset \mathcal{O}_K$ there is $a \in \mathfrak{a} - \{0\}$ for which*

$$|\,\mathrm{Nr}(a)| \leqslant C\,\mathrm{Nr}(\mathfrak{a}).$$

PROOF. We give the proof when $A = \mathbb{Z}$. Without loss of generality we may assume that the algebraic closure $\overline{\mathbb{Q}}$ is contained in $\mathbb{C}$. In particular the embeddings

$$\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}) = \{\sigma_1, \cdots, \sigma_n\}$$

take values in the complex numbers.

Let $(z_1, \cdots, z_n)$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and $m \in \mathbb{N} \geqslant 1$ be the unique integer s.t.

$$m^n \leqslant \mathrm{Nr}_{\mathcal{O}_K}(\mathfrak{a}) < (m+1)^n.$$

Consider the $(m+1)^n$ elements of $\mathcal{O}_K$ of the shape

$$\sum_{1=1}^{n} \lambda_i z_i, \ 0 \leqslant \lambda_i \leqslant m.$$

Since $(m+1)^n > \mathrm{Nr}_{\mathcal{O}_K}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ there exists (pigeonhole) $z \neq z'$ in that set such that

$$a = z - z' \in \mathfrak{a} - \{0\}$$

We have by Prop. V.1.3

$$\begin{aligned}\mathrm{Nr}_{\mathcal{O}_K}(a\mathcal{O}_K) = |\,\mathrm{Nr}_{K/\mathbb{Q}}(a)| &= \prod_{j=1}^{n} |\sigma_j(a)| \\ &\leqslant \prod_j (\sum_i |\lambda_i - \lambda_i'||\sigma_j(z_i)|) \leqslant m^n (\prod_j \sum_i |\sigma_j(z_i)|) \leqslant C m^n \leqslant C\,\mathrm{Nr}_{\mathcal{O}_K}(\mathfrak{a})\end{aligned}$$

where

$$C = \prod_j \sum_i |\sigma_j(z_i)|.$$

□

EXERCISE V.4. Prove the above proposition for $A = \mathbb{F}_q[T]$.

In the rest of this section we will provide a precise value for the constant C in the number field case ($A = \mathbb{Z}$).

V.2. Lattices

THEOREM V.3. *Let $\Lambda \subset \mathbb{R}^n$ a discrete subgroup, then Λ is free of rank $r \leqslant n$ and generated by r vectors which are $\mathbb{R}$-linearly independent.*

PROOF. Let us recall that $\Lambda \subset \mathbb{R}^n$ is discrete iff either of the two conditions are satisfied:

- For any $x \in \Lambda$ there exists an open set $V_x \subset \mathbb{R}^n$ such that $V_x \cap \Lambda = \{x\}$.
- For any compact $K \subset \mathbb{R}^n$, $K \cap \Lambda$ is finite.

Let $\mathcal{B} = (x_1, \cdots, x_r) \subset \Lambda^r$ a family of $\mathbb{R}$-linearly independent elementis with r maximal and let

$$\mathcal{P}_{\mathcal{B}} = \mathcal{P} = \{x \in \mathbb{R}^n, \ x = \sum_i \lambda_i x_i, \ \lambda_i \in [0, 1[\}.$$

Since $\mathcal{P}$ is precompact,

$$\mathcal{P} \cap \Lambda = \{x_1', \cdots x_l'\}$$

is finite. For any $x \in \Lambda$ we have

$$x = \sum_i \lambda_i x_i, \ \lambda_i \in \mathbb{R}$$

and if we set

$$[x] := \sum_i [\lambda_i] x_i \in \Lambda$$

we have

$$x - [x] \in \mathcal{P} \cap \Lambda$$

and

$$x = [x] + x'_{i_x}$$

therefore Λ is generated by $\mathcal{B} \cup \mathcal{P} \cap \Lambda$ so is of finite type hence free of rank $r' \geqslant r$ since it contains the free group of rank r

$$\Lambda_{\mathcal{B}} = \sum_i \mathbb{Z} x_i.$$

Let us prove that Λ is contained in a free group of rank r: for any $x' \in \mathcal{P} \cap \Lambda$ we set for $j \in \mathbb{Z}$

$$x'_j := jx' - [jx'] \in \mathcal{P} \cap \Lambda.$$

Since that later set is finite there exists $i \neq j \in \mathbb{Z}$ s.t. $x'_j = x'_i$ and

$$(j-i)x' = [jx'] - [ix'] \Longrightarrow x' = \frac{1}{j-i}([jx'] - [ix']).$$

hence any element of $\mathcal{P} \cap \Lambda$ is a linear combination with rational coefficients of elements of $\mathcal{B}$ and the denominators occuring belong to a finite set. Let d be a common denominator, we have

$$\mathcal{P} \cap \Lambda \subset \frac{1}{d}\Lambda_{\mathcal{B}} \Longrightarrow \Lambda \subset \frac{1}{d}\Lambda_{\mathcal{B}}.$$

□

DEFINITION V.2. *A lattice $\Lambda \subset \mathbb{R}^n$ is a discrete subgroup of rank n; in particular any $\mathbb{Z}$-basis is an $\mathbb{R}$-basis of $\mathbb{R}^n$.*

V.3. Minkowski theorems

V.3.1. Volume of a lattice.

DEFINITION V.3. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice with basis $\mathcal{B} = \{x_1, \cdots, x_n\}$. The fundamental parallelotope for $\mathcal{B}$ is defined as*

$$\mathcal{P}_{\mathcal{B}} = \{x \in \mathbb{R}^n,\ x = \sum_i \lambda_i x_i,\ \lambda_i \in [0,1[\}.$$

This is a fundamental domain for the action of $\Lambda \curvearrowright \mathbb{R}^n$. The volume of $\mathcal{P}_{\mathcal{B}}$ is the determinant

$$\mathrm{vol}(\mathcal{P}_{\mathcal{B}}) = |\det((x_{i,j})_{i,j=1\cdots,n})|$$

where the $x_{i,j}$ are the coordinates of x_i in the canonical basis[1]

$$x_i = (x_{i,1}, \cdots, x_{i,n}),\ i = 1, \cdots, n.$$

LEMMA V.3.1. *Let $\mathcal{B}'$ be another basis, er have*

$$\mathrm{vol}(\mathcal{P}_{\mathcal{B}}) = \mathrm{vol}(\mathcal{P}_{\mathcal{B}'}).$$

PROOF. If $\mathcal{B}'$ is another basis the matrix of base change (from $\mathcal{B}$ to $\mathcal{B}'$) has integral entries as does it inverse, therefore its determinant is ± 1 and

$$|\det((x_{i,j})_{i,j=1\cdots,n})| = |\det((x'_{i,j})_{i,j=1\cdots,n})|.$$

□

DEFINITION V.4. *The (co)volume of Λ is the volume of $\mathcal{P}_{\mathcal{B}}$ for any choice of a $\mathbb{Z}$-basis of Λ:*

$$\mathrm{vol}(\Lambda) := \mathrm{vol}(\mathcal{P}_{\mathcal{B}}).$$

[1] or in fact any basis

REMARK V.2. The term "volume" for the volume of Λ is a bit improper: this is rather the volume of (a fundamental domain of) the quotient space $\mathbb{R}^n/\Lambda$, so one should rather speak of the "covolume" of Λ. We will allow ourselves to speak of the volume of Λ and write $\mathrm{vol}(\Lambda)$; notice that this "volume" is a decreasing function of Λ: if $\Lambda' \subset \Lambda$ one has

$$\mathrm{vol}(\Lambda') \geqslant \mathrm{vol}(\Lambda).$$

PROPOSITION V.3.2. *If $\Lambda' \subset \Lambda$ is a sub-lattice we have*

$$\mathrm{vol}(\Lambda')/\mathrm{vol}(\Lambda) = |\Lambda/\Lambda'|.$$

PROOF. This is a direct application of the adapted basis Thm. □

V.3.2. First Theorem.

THEOREM V.4 (Minkowski). *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $V \subset \mathbb{R}^n$ a mesurable set. If*

$$\mathrm{vol}(V) > \mathrm{vol}(\Lambda)$$

there exists $v \neq v' \in V$ s.t.

$$v - v' \in \Lambda.$$

PROOF. Consider some fundamental parallelotope $\mathcal{P}$. The set $\{x + \mathcal{P},\ x \in \Lambda\}$ is a measurable partition of $\mathbb{R}^n$ so we have a measurable partition of V

$$V = \bigsqcup_{x \in \Lambda} V \cap (x + \mathcal{P})$$

so that

$$\mathrm{vol}(V) = \sum_x \mathrm{vol}(V \cap (x + \mathcal{P})).$$

Observe that by translation invariance we have

$$\mathrm{vol}(V \cap (x + \mathcal{P}) = (-x + V) \cap \mathcal{P}.$$

We have

$$\sum_{x \in \Lambda} (-x + V) \cap \mathcal{P} \subset \mathcal{P}$$

and

$$\sum_{x \in \Lambda} \mathrm{vol}((-x + V) \cap \mathcal{P}) = \sum_{x \in \Lambda} \mathrm{vol}(V \cap (x + \mathcal{P})) = \mathrm{vol}(V) > \mathrm{vol}(\mathcal{P})$$

so there exists $x \neq x' \in \Lambda$ such that

$$(-x + V) \cap \mathcal{P} \cap (-x' + V) \cap \mathcal{P} \neq \emptyset;$$

This means, there exists $v, v' \in V$ s.t.

$$-x + v = -x' + v' \Longleftrightarrow v - v' = x - x' \in \Lambda - \{0\}.$$

□

V.3.3. Second Theorem.

THEOREM V.5 (Minkowski). *Let $\Lambda \subset \mathbb{R}^n$ a lattice and $V \subset \mathbb{R}^n$ a set which is compact, convex ($v, v' \in V \Longleftrightarrow [v, v'] \in V$) symetric w.r.t. 0 ($v \in V \Longleftrightarrow -v \in V$). If*

$$\mathrm{vol}(V) \geqslant 2^n \mathrm{vol}(\Lambda)$$

then V contains a non-zero element of Λ:

$$V \cap \Lambda - \{0\} \neq \emptyset.$$

PROOF. Let us assume that $\mathrm{vol}(V) > 2^n \mathrm{vol}(\Lambda)$. By the first Theorem the set $\frac{1}{2}V$ contains $v \neq v'$ s.t.

$$x = v - v' \in \Lambda - \{0\}.$$

We have $w = -v' \in \frac{1}{2}V$ by symmetry and $2v, 2w \in V$; therefore

$$x = \frac{1}{2}(2v + 2w) \in V$$

since V is convex.

Suppose that $\mathrm{vol}(V) = 2^n \mathrm{vol}(\Lambda)$; for any $0 < \varepsilon \leqslant 1$ there is $x_\varepsilon \in (1+\varepsilon)V \cap \Lambda - \{0\}$; since for all $\varepsilon > 0$ the intersection $(1+\varepsilon)V \cap \Lambda - \{0\}$ is finite, there exists a subsequence $\varepsilon \to 0$ such that x_ε is constant.

□

V.4. Archimedean embeddings

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the subfield of algebraic numbers $\mathbb{C}$. In the sequel, all the finite extensions of $\mathbb{Q}$ we will consider are included in $\overline{\mathbb{Q}}$ so are fields of complex numbers.

Let $K/\mathbb{Q}$ a finite extension of degree n. This is therefore a subfield of $\mathbb{C}$ and for any $\sigma \in \mathrm{Hom}(K, \overline{\mathbb{Q}})$, $\sigma(K)$ is another subfield isomorphic to K and contained in $\mathbb{C}$ and the set of all such subfields is precisely

$$\sigma(K),\ \sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}).$$

REMARK V.3. Since $K/\mathbb{Q}$ is separable, $|\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})| = n$.

DEFINITION V.5. *Given $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ an embedding of K in $\mathbb{C}$. If $\sigma(K) \subset \mathbb{R}$, σ is a real embedding and complex if $\sigma(K) \not\subset \mathbb{R}$.*

We denote the complex conjugation

$$\sigma_{\mathbb{C}}(\bullet) = \overline{\bullet} : z \in \mathbb{C} \to \overline{z} \in \mathbb{C}.$$

The group $\{\mathrm{Id}, \sigma_{\mathbb{C}}\}$ acts on $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$: the real embeddings are the fixed points for this action and the complex ones decompose into pairs of complex conjugate embeddings. In particular the number of complex embedding is even. The number of real embeddings is denoted $r_1 = r_1(K)$ and the number of complex ones is denoted $2r_2 = 2r_2(K)$ so that

$$r_1 + 2r_2 = n.$$

REMARK V.4. This can be considered as an archimedean version of the degree formula.

Set

$$r = r_1 + r_2$$

and

$$\{\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots, \sigma_r\}$$

a choice of representatives of the various orbits of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ under the action of $\{\mathrm{Id}, \sigma_{\mathbb{C}}\}$: such a choice is called a *type* for K (there are 2^{r_2} possible types). In other terms given a type as above

$$\{\sigma_1, \cdots, \sigma_{r_1}\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$$

is the set of real embeddings and

$$\{\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+1}, \cdots, \overline{\sigma}_{r_1+r_2}\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) - \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R}).$$

is the set of complex ones.

Let K_∞ be the $\mathbb{R}$-algebra

$$K_\infty := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \prod_{i=1}^{r_1+r_2} K_i$$

with

$$K_i = \begin{cases} \mathbb{R} & i \leqslant r_1 \\ \mathbb{C} & i = r_1 + 1, \cdots, r_2. \end{cases}$$

We have

$$K_\infty \simeq \mathbb{R}^n$$

where we have identified $\mathbb{C}$ with $\mathbb{R}^2$ via the usual $\mathbb{R}$-linear map

$$z = x + iy \in \mathbb{C} \to (x, y) \in \mathbb{R}^2.$$

Given a type, let

$$\sigma_\infty : \begin{array}{ccc} K & \mapsto & K_\infty \\ z & \mapsto & \sigma_\infty(z) = (\sigma_1(z), \cdots, \sigma_r(z)) \end{array}.$$

This is an injective morphism of $\mathbb{Q}$-algebra called the *archimedean* embedding associated to the type. In the sequel the type is fixed once and for all.

THEOREM V.6. *When $K_\infty = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$ is endowed with the usual topology, the subgroup $\sigma_\infty(K)$ is dense and the subgroup*

$$\sigma_\infty(\mathcal{O}_K) \subset K_\infty$$

is a lattice (is discrete of rank n). Let $(z_1, \cdots, z_n)$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$, then $(\sigma_\infty(z_1), \cdots, \sigma_\infty(z_n))$ is an $\mathbb{R}$-basis of K_∞. More generally the image by σ_∞ of any fractional ideal is a lattice in K_∞.

PROOF. We start by showing that $\sigma_\infty(\mathcal{O}_K)$ is a lattice. For discreteness, it is sufficient to show that 0 is isolated in $\sigma_\infty(\mathcal{O}_K)$. Let $(z_k)_{k \geqslant 0}$ be a sequence of elements of $\mathcal{O}_K$ such that

$$\sigma_\infty(z_k) \to \mathbf{0}.$$

The sequence of characteristic polynomials converges

$$P_{K/\mathbb{Q},\mathrm{car},z_k}(X) = \prod_{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \big(X - \sigma(z_k)\big) = \prod_{i=1}^{r_1} \big(X - \sigma_i(z_k)\big) \prod_{i=r_1+1}^{r_1+r_2} \big(X - \sigma_i(z_k)\big)\big(X - \overline{\sigma_i(z_k)}\big) \to X^n$$

but the coefficients of the $P_{K/\mathbb{Q},\mathrm{car},z_k}(X)$ are integers so must be 0 for k large enough (except for the degree n coefficient).

To see that $\sigma_\infty(\mathcal{O}_K)$ has full rank, let $(z_1, \cdots, z_n)$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$; we will see that $(\sigma_\infty(z_1), \cdots, \sigma_\infty(z_n))$ is an $\mathbb{R}$-basis of K_∞ and compute the volume of $\sigma_\infty(\mathcal{O}_K)$. For $i = 1, \cdots, n$ we set

$$\sigma_j(z_i) =: x_{i,j} \in \mathbb{R} \text{ for } j = 1 \cdots r_1,$$
$$\sigma_j(z_i) =: x_{i,j} + iy_{i,j} \in \mathbb{C} \text{ for } j = r_1 + 1 \cdots r_1 + r_2.$$

Let

$$u_{i,j} = x_{i,j},\ j = 1, \cdots, r_1 + r_2,\ u_{i,j} = y_{i,j},\ j = r_2 + 1, \cdots, 2r_2.$$

It suffices to show that

$$|\det((u_{i,j})_{i,j=1,\cdots,n})| \neq 0.$$

We have

$$x_{i,j} = \frac{\sigma_j(z_i) + \overline{\sigma_j(z_i)}}{2},\ y_{i,j} = \frac{\sigma_j(z_i) - \overline{\sigma_j(z_i)}}{2i}$$

and therefore

$$|\det((u_{i,j})_{i,j=1,\cdots,n})| = 2^{-r_2} |\det((\sigma_j(z_i))_{i,j \leqslant n})|.$$

But let us recall that

$$\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}_{K/\mathbb{Q}}(z_1, \cdots, z_n) = \det((\mathrm{tr}_{K/\mathbb{Q}}(z_i z_j))_{i,j}) = \det((\sum_{k=1}^n \sigma_k(z_i z_j)))_{i,j})$$
$$= \det((\sum_{k=1}^n \sigma_k(z_i)\sigma_k(z_j)))_{i,j}) = \det((\sigma_k(z_i))_{i,k \leqslant n})^2$$

Since $\mathrm{disc}(\mathcal{O}_K) \neq 0$, $|\det((u_{i,j})_{i,j=1,\cdots,n})| \neq 0$ and $(\sigma_\infty(z_1), \cdots, \sigma_\infty(z_n))$ is an $\mathbb{R}$-basis of K_∞ therefore $\sigma_\infty(\mathcal{O}_K) \subset K_\infty$ is a lattice.

More generally for any fractional ideal $\mathfrak{a} \subset K$ there exists $N \geqslant 1$ such that $N\mathcal{O}_K \subset \mathfrak{a} \subset N^{-1}\mathcal{O}_K$ which proves that $\sigma_\infty(\mathfrak{a})$ is a lattice.

Density of $\sigma_\infty(K)$ follows from the fact that for any basis of a finite dimensional real vector space the $\mathbb{Q}$-linear hull forms a dense subset. □

The (co)volume of these lattices are given by the following formula

PROPOSITION V.4.1. *We have*

$$\mathrm{vol}(\sigma_\infty(\mathcal{O}_K)) = 2^{-r_2}|\mathrm{disc}(\mathcal{O}_K)|^{1/2}$$

and for any fractional ideal $\mathfrak{a}$*, we have*

$$\mathrm{vol}(\sigma_\infty(\mathfrak{a})) = 2^{-r_2}|\mathrm{disc}(\mathfrak{a})|^{1/2}$$

and if $\mathfrak{a} \subset \mathcal{O}_K$ *we have*

$$\mathrm{vol}(\sigma_\infty(\mathfrak{a}))/\mathrm{vol}(\sigma_\infty(\mathcal{O}_K)) = (|\mathrm{disc}(\mathfrak{a})|/|\mathrm{disc}(\mathcal{O}_K)|)^{1/2} = [\mathcal{O}_K : \mathfrak{a}] = \mathrm{Nr}_{\mathcal{O}_K}(\mathfrak{a}).$$

REMARK V.5. In the sequel and to simplify notation we will identify K with its image $\sigma_\infty(K) \subset K_\infty$ and an ideal $\mathfrak{a}$ with the corresponding lattice $\sigma_\infty(\mathfrak{a})$.

V.5. A precise form of the finiteness of the class group

PROPOSITION V.5.1. *There exists* $C = C(r_1, r_2) > 0$ *such that for any ideal* $\mathfrak{a} \subset \mathcal{O}_K$ *there is* $a \in \mathfrak{a} - \{0\}$ *such*

$$|\mathrm{Nr}_{K/\mathbb{Q}}(a)| \leqslant C|\mathrm{disc}(\mathcal{O}_K)|^{1/2}\,\mathrm{Nr}(\mathfrak{a}).$$

PROOF. For $t > 0$, let

$$B_t = \left\{(x_1, \cdots, z_1, \cdots, z_{r_2}) \in K_\infty \colon \sum_i |x_i| + 2\sum_i |z_i| \leqslant t\right\}.$$

This is a compact, convex and symetric set. We have

$$\mathrm{vol}(B_t) = \mathrm{vol}(B_1)t^n = Vt^n.$$

Let t be such that

$$\mathrm{vol}(B_t) = Vt^n = 2^n\mathrm{vol}(\sigma_\infty(\mathfrak{a})) = 2^{n-r_2}|\mathrm{disc}(\mathcal{O}_K)|^{1/2}\,\mathrm{Nr}_{\mathcal{O}_K}(\mathfrak{a}).$$

By Minkowski's second theorem there exists $a \in \mathfrak{a} - \{0\}$ s.t.

$$a \in B_t.$$

We have therefore (by the arithmetic-geometric mean inequality)

$$\begin{aligned}|\mathrm{Nr}_{K/\mathbb{Q}}(a)| &= \prod_{i=1}^{r_1}|\sigma_i(a)| \prod_{i=r_1}^{r_1+r_2}|\sigma_i(a)|^2 \leqslant \left[\frac{1}{n}\left(\sum_i |\sigma_i(a)| + 2\sum_i |\sigma_i(a)|\right)\right]^n \\ &\leqslant \frac{t^n}{n^n} = \frac{2^{n-r_2}}{Vn^n}|\mathrm{disc}(\mathcal{O}_K)|^{1/2}\,\mathrm{Nr}(\mathfrak{a}).\end{aligned}$$

□

To compute $C(r_1, r_2)$ it suffices to compute $V = \mathrm{vol}(B_1)$:

PROPOSITION V.5.2. *Let*

$$B_1 = \left\{(x_1, \cdots, z_1, \cdots, z_{r_2}) \in K_\infty \colon \sum_i |x_i| + 2\sum_i |z_i| \leqslant 1\right\}.$$

We have

$$\mathrm{vol}(B_1) = \frac{2^{r_1}(\frac{\pi}{2})^{r_2}}{n!}$$

and therefore

$$C(r_1, r_2) = \Big(\frac{4}{\pi}\Big)^{r_2} \frac{n!}{n^n}.$$

The argument leading to the finiteness of the ideal class group that we have seen before can be formalized as follows:

LEMMA V.5.3. *Given $\mathfrak{a} \subset \mathcal{O}_K$ a non zero ideal, there is a bijection*

$$(\mathfrak{a} - \{0\})/\mathcal{O}_K^\times \longleftrightarrow \mathfrak{b} \subset \mathcal{O}_K,\ [\mathfrak{b}] = [\mathfrak{a}^{-1}]$$

satisfying the following relation on the norms

$$|\operatorname{Nr}_{K/\mathbb{Q}}(a)|/\operatorname{Nr}(\mathfrak{a}) = \operatorname{Nr}(\mathfrak{b}).$$

PROOF. The bijection is induced by the map

$$a \in \mathfrak{a} - \{0\} \mapsto (a) = a.\mathcal{O}_K = \mathfrak{a}.\mathfrak{b}$$

and

$$a \in \mathfrak{a} - \{0\} \Leftrightarrow \mathfrak{a}|(a) \Leftrightarrow (a) = \mathfrak{a}.\mathfrak{b}$$

and we have

$$[\mathfrak{a}].[\mathfrak{b}] = [(a)] = [\mathcal{O}_K]$$

and for the norms

$$\operatorname{Nr}((a)) = \operatorname{Nr}(\mathfrak{a}) \operatorname{Nr}(\mathfrak{b}) = |\operatorname{Nr}_{K/\mathbb{Q}}(a)|$$

by multiplicativity of the norm and the computation of the norm of principal ideals. □

COROLLARY V.5.1. *Any ideal class $[\mathfrak{a}] \in \operatorname{Cl}(\mathcal{O}_K)$ contains a representative whose norm is*

$$\operatorname{Nr}(\mathfrak{a}) \leqslant \Big(\frac{4}{\pi}\Big)^{r_2} \frac{n!}{n^n} |\operatorname{disc}(\mathcal{O}_K)|^{1/2}.$$

REMARK V.6. In particular we have as $|\operatorname{disc}(\mathcal{O}_K)| \to \infty$

$$|\operatorname{Cl}(\mathcal{O}_K)| \leqslant |\operatorname{disc}(\mathcal{O}_K)|^{1/2 + o_n(1)}.$$

THEOREM V.7 (Hermite-Minkowski). *Let K be a number field of degree n. We have*

$$|\operatorname{disc}(\mathcal{O}_K)| \geqslant \frac{\pi}{3}\Big(\frac{3\pi}{4}\Big)^{n-1}.$$

In particular, if $K \neq \mathbb{Q}$ one has

$$|\operatorname{disc}(\mathcal{O}_K)| > 1.$$

In other terms, a number field which is not the field of rational numbers is always ramified at some prime.

PROOF. Exercise. □

REMARK V.7. This Theorem is often used the other way around: you have a finite extension $K/\mathbb{Q}$ which you can prove is everywhere unramified and from there you conclude that $K = \mathbb{Q}$. For instance this kind of argument occurs in A. Wiles proof of FLT.

THEOREM V.8 (Hermite). *Given $d \in \mathbb{Z} - \{0\}$. In $\mathbb{C}$ there are only finitely many number fields K such that*

$$\operatorname{disc}(\mathcal{O}_K) = d.$$

PROOF. By the previous inequality the degree of K is bounded in terms of $|d|$. In particular wlog we may assume that the the degree and the signature (r_1, r_2) are given.

Given $X, Y > 1$ we consider the subset

$$B(X, Y) = \{(u_i)_{i \leqslant r_1 + r_2} \in K_\infty \colon |u_1|_1 \leqslant X,\ |u_i|_i \leqslant 1/Y,\ i \geqslant 2\}$$

if $r_1 > 0$ and

$$B(X,Y) = \{(u_i)_{i\leqslant r_1+r_2} \in K_\infty \colon |\Re u_1|_1 \leqslant 1,\ |\mathrm{Im}\, u_1| \leqslant X,\ |u_i|_i \leqslant 1/Y, i \geqslant 2\}$$

if $r_1 = 0$, where $|\bullet|_i$ is either the usual absolute value if $K_i = \mathbb{R}$ or the usual complex modulus if $K_i = \mathbb{C}$. This is a product of r_1 intervals/rectangles and r_2 disks and there exists a constant $C = C(r_1, r_2) > 0$ such that

$$\mathrm{vol}(B(X,Y)) = \begin{cases} CX(1/Y)^{n-1} & \text{if } r_1 \geqslant 1, \\ CX(1/Y)^{n-2} & \text{otherwise.} \end{cases}$$

Let $X, Y > 1$ be such that

$$\mathrm{vol}(B(X,Y)) \geqslant 2^n \mathrm{vol}(\sigma_\infty(\mathcal{O}_K)).$$

By Minkowski's second Theorem, there exists $z \in \mathcal{O}_K - \{0\}$ such that

$$(\sigma_1(z), \cdots, \sigma_{r_1+r_2}(z)) \in B(X,Y)$$

and since $X > 1$ and $1/Y < 1$,

$$\sigma_1(z) \neq \sigma_i(z), \overline{\sigma_i}(z),\ i \geqslant 2.$$

This implies that z is a primitive element, i.e.

$$\mathbb{Q}(z) = K.$$

Indeed if one conjugate $\sigma_1(z)$ is distinct from all the others conjugates $\sigma_i(z)$, $i = 2, \cdots, n$, then all conjugates are distinct (because the Galois group of any finite Galois extension containing the $\{\sigma_i(z) \colon i \leqslant n\}$ acts transitively on that set and therefore $\mathbb{Q}(z) \subset K$ has degree n over $\mathbb{Q}$ so it equal to K.

Since z is an algebraic integer, the coefficients of its minimal polynomial (which is of degree n since z generates K) are integers and bounded by a constant which depends only on r_1, r_2, X, Y (since the coefficients are given by symmetric homogeneous polynomials of degree $\leqslant n$ in the roots $\{\sigma_i(z) \colon i = 1, \cdots, n\}$) so that there are only finitely many such possible z and therefore only finitely many fields generated by these numbers. □

V.6. The group of units

Another very important finiteness theorem concerns the structure of the group of units $\mathcal{O}_K^\times$.

THEOREM V.9 (Dirichlet). *Set $r := r_1 + r_2$. The abelian group of units $\mathcal{O}_K^\times$ is of finite type of rank $r - 1$. Its torsion subgroup*

$$\mathcal{O}_{K,\mathrm{tors}}^\times = \mu_K = \{z \in K \colon \exists k \geqslant 1,\ z^k = 1\}$$

(the group of roots of unity contained in K) is finite. In other terms one has an isomorphism

$$\mathcal{O}_K^\times \simeq \mu_K \times \mathbb{Z}^{r-1}$$

EXAMPLE V.1. For $n = 2$, we have two cases:

- $r_1 = 0,\ 2r_2 = 2$: the field K is called imaginary quadratic. We have $r_1 + r_2 - 1 = 0$ and therefore $\mathcal{O}_K^\times = \mu_K$ and has order $2, 4$ or 6.
- $r_1 = 2, r_2 = 0$: the field K is called real quadratic. We have $r_1 + r_2 - 1 = 1$ and $\mathcal{O}_K^\times = \mu_K \times \varepsilon_K^{\mathbb{Z}}$ with $\mu_K = \{\pm 1\}$ and wlg wma that the generator ε_K is positve. This (unique) positive generator is called the fundamental unit of $\mathcal{O}_K$. This special case of Dirichlet's unit Theorem is due to Pell.

The proof of this theorem and of more elaborate versions is by studying the action of $\mathcal{O}_K^\times$ on $K^\times$ and on $K_\infty^\times$ (when $\mathcal{O}_K^\times$ is viewed as a subgroup of $K_\infty^\times$ via the archimedean embedding σ_∞).

V.6.1. The logarithmic embedding. The group of units is a multiplicative commutative group and it will be very useful to pass to additive groups. This is done via the following group homomorphism called the *logarithmic embedding*:

$$\begin{array}{rccc} \mathrm{Log}\colon & K_\infty^\times & \mapsto & \mathbb{R}^r \\ & (z_1,\cdots,z_r) & \mapsto & (d_i \log|z_i|)_i \end{array}$$

where

$$d_i = \begin{cases} 1 & i=1,\cdots,r_1, \\ 2, & i=r_1+1,\cdots,r_1+r_2. \end{cases}$$

This is a surjective map whose kernel is

$$\ker(\mathrm{Log}) = \{z\in K_\infty^\times \colon \forall i=1,\cdots,r,\ |z_i|=1\} \simeq \{\pm 1\}^{r_1}\times(\mathbb{C}^1)^{r_2},\ \mathbb{C}^1=\{z\in\mathbb{C}^\times\colon |z|=1\}.$$

Remark V.8. The term "embedding" is somewhat improper as the kernel is not trivial (but at least it is compact).

Definition V.6. *The logarithmic embedding (of $K^\times$) is the compositum*

$$\mathrm{Log}_\infty = \mathrm{Log}\circ\sigma_\infty : K^\times \mapsto \mathbb{R}^r$$

that is for $z\in K^\times$,

$$\mathrm{Log}_\infty(z) = (\log|\sigma_1(z)|,\cdots,\log|\sigma_{r_1}(z)|, 2\log|\sigma_{r_1+1}(z)|,\cdots,2\log|\sigma_r(z)|).$$

Remark V.9. To ease notations we will usually write Log for Log_∞.

We consider the restriction of the "embedding" to $\mathcal{O}_K^\times$:

Proposition V.6.1. *The kernel $\ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times})$ is finite and its image $\mathrm{Log}(\mathcal{O}_K^\times)$ is a discrete subgroup of the hyperplane*

$$H(\mathbb{R}) := \ker(T) = \{(l_1,\cdots,l_r)\in\mathbb{R}^r\colon T(l_1,\cdots,l_r)=\sum_{i=1}^r l_i = 0\}.$$

Proof. Given $z\in\mathcal{O}_K^\times$ we have

$$\mathrm{Nr}_{K/\mathbb{Q}}(z) = \prod_{j=1}^{r_1}\sigma_j(z)\prod_{j=r_1+1}^{r_1+r_2}\sigma_j(z)\overline{\sigma_j(z)} = \pm 1$$

therefore

$$0 = \log|\mathrm{Nr}_{K/\mathbb{Q}}(z)| = \log\prod_j|\sigma_j(z)|^{d_j} = \sum_{j=1}^r d_j\log|\sigma_j(z)| = T(\mathrm{Log}_\infty(z))$$

Let $B\subset H(\mathbb{R})$ be compact and let $z\in\mathcal{O}_K^\times$ be such that

$$\mathrm{Log}_\infty(z)\in B.$$

The positive real numbers $|z_j|=|\sigma_j(z)|,\ j=1,\cdots,n$ are bounded depending on B, so are the coefficients of $P_{K/\mathbb{Q},\mathrm{car},z}$; since these are integers there are only finitely many such polynomials and therefore finitely many such z.

It follows that $\mathrm{Log}_\infty(\mathcal{O}_K^\times)\subset H(\mathbb{R})$ is discrete of rank $r'\leqslant r-1=\dim H(\mathbb{R})$. Moreover

$$\ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times}) = \{z\in\mathcal{O}_K^\times\colon\ \mathrm{Log}(z)=\mathbf{0}\}$$

is also finite. It follows that $\mathcal{O}_K^\times$ is of finite type since

$$\mathcal{O}_K^\times/\ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times}) \simeq \mathrm{Log}_\infty(\mathcal{O}_K^\times)$$

is of finite type. □

PROPOSITION V.6.2. *The finite group* $\ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times})$ *is the group of roots of unity contained in* K*:*

$$\ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times}) = \mathcal{O}_{K,\mathrm{tors}}^\times = \{z \in \mathcal{O}_K^\times \colon \exists n \in \mathbb{Z} - \{0\},\ z^n = 1\} = \mu_K.$$

PROOF. We leave it to the reader to check that $\mathcal{O}_{K,\mathrm{tors}}^\times = \mu_K$. It remains to prove that

$$\ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times}) = \mathcal{O}_{K,\mathrm{tors}}^\times.$$

Let $z \in \mathcal{O}_{K,\mathrm{tors}}^\times$, then there is $m \geqslant 1$ such that $z^m = 1$ and, therefore, $|\sigma(z)|^m = |\sigma(z^m)| = 1$ for all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. It follows that $|\sigma(z)| = 1$ for all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ and, hence,

$$\mathcal{O}_{K,\mathrm{tors}}^\times \subseteq \ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times}).$$

For the opposite inclusion, we recall that $H = \ker(\mathrm{Log}_{\infty|\mathcal{O}_K^\times})$ is finite, hence $H < K^\times$ is a finite subgroup. In particular, for all $z \in H$ we have $z^{|H|} = 1$ by Lagrange's theorem. In particular, we obtain that $H < \mu_K = \mathcal{O}_{K,\mathrm{tors}}^\times$. □

Let us compute the rank of the free part

PROPOSITION V.6.3. *We have*

$$r' = r_1 + r_2 - 1.$$

We need two lemmata

LEMMA V.6.4. *There exists* $C = C(K) > 0$ *s.t. the following holds: for any* $k \leqslant r$ *and* $a \neq 0 \in \mathcal{O}_K$*, there exists* $b = b_k \in \mathcal{O}_K - \{0\}$ *satisfying*

$$|\,\mathrm{Nr}_{K/\mathbb{Q}}(b)| \leqslant C$$

and

$$\forall i \neq k,\ \alpha_i > \beta_i.$$

Here

$$\mathrm{Log}_\infty(a) := (\alpha_1, \cdots, \alpha_r),\ \mathrm{Log}_\infty(b) := (\beta_1, \cdots, \beta_r)$$

are the coordinates of the images of a *and* b *under the logarithmic embedding.*

PROOF. Write $\mathrm{Log}_\infty(a) := (\alpha_1, \cdots, \alpha_r)$. We have

$$d_i \log|\sigma_i(a)| = \alpha_i$$

and therefore

$$|\,\mathrm{Nr}_{K/\mathbb{Q}}(a)| = \prod_{i=1}^r |\sigma_i(a)|^{d_i} = \exp\Big(\sum_i \alpha_i\Big).$$

For any $\alpha \in \mathbb{R}$ let

$$B_k(\alpha) := \{(z_1, \cdots, z_r) \in K_\infty \colon |z_i|^{d_i} \leqslant \exp(\alpha_i/2)\ i \neq k,\ |z_k| \leqslant \exp(\alpha/2)\} \subset K_\infty.$$

This is a convex, compact and symetric subset of K_∞ (a product of intervals and or disks centered at the origin) with volume

$$\mathrm{vol}(B_k(\alpha)) = C(r_1, r_2) \exp\left(\frac{1}{2}\left(\alpha + \sum_{\substack{i=1 \\ i \neq k}}^r \alpha_i\right)\right)$$

for $C(r_1, r_2) > 0$ depending only on r_1, r_2. Suppose that α is chosen such that

$$\mathrm{vol}(B_k(\alpha)) = C(r_1, r_2) \exp\left(\frac{1}{2}\left(\alpha + \sum_{\substack{i=1 \\ i \neq k}}^r \alpha_i\right)\right) = 2^n \mathrm{vol}(\mathcal{O}_K).$$

By Minkowski's second theorem there exists $b \in \mathcal{O}_K - \{0\}$ such that $b \in B_k(\alpha)$ and $\mathrm{Log}_\infty(b)$ has the required properties. Moreover, since

$$d_i \log|\sigma_i(b)| = \beta_i$$

$$|\,\mathrm{Nr}_{K/\mathbb{Q}}(b)| = \prod_{i=1}^{r} |\sigma_i(b)|^{d_i} = \exp(\sum_i \beta_i) \leqslant \exp\left(\frac{1}{2}\left(\alpha + \sum_{i\neq k}\alpha_i\right)\right) = \frac{2^n}{C(r_1,r_2)}\mathrm{vol}(\mathcal{O}_K).$$

□

Lemma V.6.5. *For any $k \in 1, \cdots, r$ there exists*

$$u_k \in \mathcal{O}_K^\times$$

such that, setting

$$\eta_k = \mathrm{Log}_\infty(u_k) = (\eta_{k,j})_{j\leqslant r} \in H(\mathbb{R}),$$

we have

$$\eta_{k,j} < 0,\ \forall j \neq k \text{ and } \eta_{k,k} > 0$$

Remark V.10. The last inequality $\eta_{k,k} > 0$ follows automatically from the previous ones since

$$\sum_{j=1}^{r} \eta_{k,j} = 0.$$

Proof. Given k. By the previous lemma we can find a sequence

$$a_1, \cdots, a_i, \cdots \in \mathcal{O}_K - \{0\}$$

such that

$$|\,\mathrm{Nr}_{K/\mathbb{Q}}(a_i)| \leqslant C(K)$$

and such that, setting

$$\mathrm{Log}_\infty(a_i) = (\alpha_{i,j})_{j=1,\cdots,r},$$

we have for any $i \geqslant 1$ and any $i \neq k$

$$\alpha_{i+1,j} < \alpha_{i,j}.$$

The number of principal ideals $a_i\mathcal{O}_K$ as i varies is finite (because all their norms are bounded by a constant depending only on K) and there exists $i < i'$ such that $a_i\mathcal{O}_K = a_{i'}\mathcal{O}_K$. We have therefore $a_{i'} = u_k a_i$ with $u_k \in \mathcal{O}_K^\times$ and for any $j \neq 0$ we have

$$\eta_{k,j} = \alpha_{i',j} - \alpha_{i,j} < 0$$

. □

We can conclude with the following

Proposition V.6.6. *Given*

$$(u_k)_{k<r} = (u_1, \cdots, u_{r-1}) \in {\mathcal{O}_K^\times}^{r-1}$$

an $(r-1)$-tuple of units such that for any k, u_k is constructed as above. Then $\big(\mathrm{Log}_\infty(u_k)\big)_{k<r}$ is $\mathbb{R}$-linearly independent.

Proof. It suffices to find, for any non-zero linear form $L : H(\mathbb{R}) \to \mathbb{R}$, an index k such that $L\big(\mathrm{Log}_\infty(u_k)\big) \neq 0$. Any linear form on $H(\mathbb{R})$ can be written in the form

$$L(l_1, \cdots, l_r) = \sum_{i=1}^{r-1} \lambda_i l_i,\ \lambda_i \in \mathbb{R}$$

(since $l_r = -(l_1 + \cdots + l_{r-1})$ in $H(\mathbb{R})$). Let k be such that $|\lambda_k|$ is maximal among the $|\lambda_i|$. Up to replacing L by $-L$ wma $\lambda_k > 0$. We claim that

$$L(\eta_k) = \sum_{i=1}^{r-1} \lambda_i \eta_{k,i} \geqslant \sum_{i=1}^{r-1} \lambda_k \eta_{k,i} = \lambda_k \sum_{i=1}^{r-1} \eta_{k,i} > 0,$$

Indeed

$$\sum_{i=1}^{r-1}(\lambda_i-\lambda_k)\eta_{k,i}=\sum_{\substack{i=1\\ i\neq k}}^{r-1}(\lambda_i-\lambda_k)\eta_{k,i}\geqslant 0$$

since $\lambda_i-\lambda_k\leqslant 0$ and $\eta_{k,i}<0$ for $i\neq k$ by construction and

$$\lambda_k\sum_{i=1}^{r-1}\eta_{k,i}=\lambda_k\sum_{i=1}^{r}\eta_{k,i}-\lambda_k\eta_{k,r}=0-\lambda_k\eta_{k,r}>0$$

since $\eta_{k,r}<0$ by construction.

□

DEFINITION V.7. *An $r-1$-tuple $(\varepsilon_1,\cdots,\varepsilon_{r-1})\in {\mathcal{O}_K^\times}^{r-1}$ such that*

$$\mathrm{Log}_\infty(\varepsilon_1,\cdots,\varepsilon_{r-1}):=(\mathrm{Log}_\infty(\varepsilon_1),\cdots,\mathrm{Log}_\infty(\varepsilon_{r-1}))$$

forms a $\mathbb{Z}$-basis of $\mathrm{Log}_\infty(\mathcal{O}_K^\times)$ is called a system of fundamental units.

The regulator of $\mathcal{O}_K$ (or K) is defined as

$$\mathrm{reg}(\mathcal{O}_K):=\mathrm{vol}\big(\mathbb{Z}\,\mathrm{Log}_\infty(\varepsilon_1)+\cdots+\mathbb{Z}\,\mathrm{Log}_\infty(\varepsilon_{r-1})\big),$$

where the volume on $H(\mathbb{R})$ is computed with respect to an orthonormal basis of $H(\mathbb{R})$ (with respect to the inner product induced by the usual Euclidean inner product on $\mathbb{R}^r$).

V.7. The class number formula

In fact the finiteness of the class number and Dirichlet's finiteness theorem for the group of units can be proved together in a single statement.

We will not do this here but at least the next Theorem shows that both complement one another. Let us recall that the number of ideals of norm m is denoted

$$r_K(m)=|\{\mathfrak{a}\subset\mathcal{O}_K\colon\ \mathrm{Nr}(\mathfrak{a})=m\}|.$$

We have seen in the exercises that $r_K(m)$ is multiplicative ($r_K(mm')=r_K(m)r_K(m')$ if $(m,m')=1$) and that

$$\forall\varepsilon>0,\ r_K(m)\ll_{K,\varepsilon} m^\varepsilon$$

and therefore the summatory function of $r_K(m)$ satisfies

$$\sum_{m\leqslant X}r_K(m)=|\{\mathfrak{a}\subset\mathcal{O}_K\colon\ \mathrm{Nr}(\mathfrak{a})\leqslant X\}|=X^{1+o_K(1)},\ X\to\infty.$$

We will prove a much more precise result.

THEOREM V.10. *[The class number formula] As $X\to+\infty$ we have*

$$\sum_{m\leqslant X}r_K(m)=\sum_{\substack{\mathfrak{a}\subset\mathcal{O}_K\\ \mathrm{Nr}(\mathfrak{a})\leqslant X}}1=\frac{2^{r_1}(2\pi)^{r_2}h(\mathcal{O}_K)\mathrm{reg}(\mathcal{O}_K)}{w_K|\mathrm{disc}(\mathcal{O}_K)|^{1/2}}X+O_K(X^{1-1/n}).$$

In this formula $h(\mathcal{O}_K)=|\mathrm{Cl}(\mathcal{O}_K)|\in\mathbb{N}_{>0}$ is the class number, $\mathrm{reg}(\mathcal{O}_K)>0$ is the regulator, $\mathrm{disc}(\mathcal{O}_K)\in\mathbb{Z}$ is the discriminant and $w_K=|\mu_K|$ is the size of the group of roots of unity in K.

PROOF. (Start) We start by splitting our sum along the various ideal classes:

$$|\{\mathfrak{a}\subset\mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a})\leqslant X\}|=\sum_{[\mathfrak{a}]\in\mathrm{Cl}(\mathcal{O}_K)}|\{\mathfrak{a}'\subset\mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a}')\leqslant X,\ \mathfrak{a}'\in[\mathfrak{a}^{-1}]\}|\tag{V.2}$$

We will now evaluate each term

$$|\{\mathfrak{a}'\subset\mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a}')\leqslant X,\ \mathfrak{a}'\in[\mathfrak{a}^{-1}]\}|$$

separately. We have already used the following:

LEMMA V.7.1. *The map*

$$a \in \mathfrak{a} - \{0\} \mapsto \mathfrak{a}' := a.\mathfrak{a}^{-1}$$

induces a bijection between the following two sets

$$\{a \in \mathfrak{a} - \{0\},\ \mathrm{Nr}(a) \leqslant X \,\mathrm{Nr}(\mathfrak{a})\}/\mathcal{O}_K^\times$$

and

$$\{\mathfrak{a}' \in [\mathfrak{a}^{-1}],\ \mathfrak{a}' \subset \mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a}') \leqslant X\}$$

PROOF. Given $\mathfrak{a}'$ in the first set, we have $\mathfrak{a}' = a.\mathfrak{a}^{-1}$ for $a \in K^\times$ uniquely defined modulo $\mathcal{O}_K^\times$. Moreover

$$\mathfrak{a}' = a.\mathfrak{a}^{-1} \subset \mathcal{O}_K \Longleftrightarrow a\mathcal{O}_K \subset \mathfrak{a} \Longleftrightarrow a \in \mathfrak{a}$$

and by multiplicativity of the norm we have

$$\mathrm{Nr}(\mathfrak{a}') = \mathrm{Nr}(a\mathfrak{a}^{-1}) = \mathrm{Nr}(a)/\,\mathrm{Nr}(\mathfrak{a}) \leqslant X \Longleftrightarrow \mathrm{Nr}(a) \leqslant X\,\mathrm{Nr}(\mathfrak{a}).$$

Moreover for any $u \in \mathcal{O}_K^\times$ we have $\mathrm{Nr}(u.a) = \mathrm{Nr}(a)$ so the constraint $\mathrm{Nr}(a) \leqslant X\,\mathrm{Nr}(\mathfrak{a})$ is invariant under the action of $\mathcal{O}_K^\times$. □

V.7.1. A counting problem. We start with a number of simple observations: let us define the norm on $K_\infty^\times$ as the continuous morphism

$$\mathrm{Nr} : z = (x_1, \cdots, x_{r_1}, z_{r_1+1}, \cdots, z_{r_1+r_2}) \in K_\infty^\times \mapsto \prod_i |x_i| \prod_j |z_j|^2 \in \mathbb{R}_{>0}.$$

This norm extend the (absolute value) of the norm on K: for any $a \in K^\times$ we have

$$|\,\mathrm{Nr}_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{r} |\sigma_i(a)|^{d_i} = \mathrm{Nr}(\sigma_\infty(a)).$$

In particular for $u \in \mathcal{O}_K^\times$ we have

$$\mathrm{Nr}(\sigma_\infty(u)) = |\,\mathrm{Nr}_{K/\mathbb{Q}}(u)| = 1.$$

This function is homogeneous of degree n: for any $x \in \mathbb{R}_{>0}$ we have

$$\mathrm{Nr}(x.z) = x^n\,\mathrm{Nr}(z).$$

Given $X > 0$ we denote by $K_{\infty,X}^\times$ the X-level set:

$$K_{\infty,X}^\times = \{z \in K_\infty^\times,\ \mathrm{Nr}(z) = X\}$$

and by

$$K_{\infty,\leqslant X}^\times = \{z \in K_\infty^\times,\ \mathrm{Nr}(z) \leqslant X\} = \bigcup_{0<X'\leqslant X} K_{\infty,X'}^\times.$$

By homogeneity we have

$$K_{\infty,X}^\times = X^{1/n}.K_{\infty,1}^\times,\ K_{\infty,\leqslant X}^\times = X^{1/n} K_{\infty,\leqslant 1}^\times.$$

We observe that the function Nr is invariant under the multiplication by the subgroup $\sigma_\infty(\mathcal{O}_K^\times)$:

$$\forall z \in K_\infty^\times,\ u \in \mathcal{O}_K^\times,\ \mathrm{Nr}(\sigma_\infty(u)z) = \mathrm{Nr}(\sigma_\infty(u))\,\mathrm{Nr}(z) = \mathrm{Nr}(z).$$

Therefore $\mathcal{O}_K^\times$ acts on $K_{\infty,X}^\times$ (through multiplication by σ_∞) and on $K_{\infty,\leqslant X}^\times$. Moreover (by homogeneity) to understand this action, it is sufficient to understand the action on $K_{\infty,1}^\times$ and on $K_{\infty,\leqslant 1}^\times$.

We can return to the proof of the class number formula: we are given a lattice $\sigma_\infty(\mathfrak{a}) \subset K_\infty$ and we wish to evaluate the numbers of ($\mathcal{O}_K^\times$-orbits of) non-zero points a in $\sigma_\infty(\mathfrak{a})$ such that

$$\mathrm{Nr}(\sigma_\infty(a)) \leqslant X\,\mathrm{Nr}(\mathfrak{a}).$$

To perform the counting, we will exhibit a "nice" precompact fundamental domain

$$\mathcal{F}_{\leqslant X\,\mathrm{Nr}(\mathfrak{a})} \subset K_{\infty,\leqslant X\,\mathrm{Nr}(\mathfrak{a})}^\times$$

representing the quotient $K_{\infty,\leqslant X^{\mathrm{Nr}(\mathfrak{a})}}^{\times}/\mathcal{O}_K^{\times}$ and then count the number of points $\sigma_\infty(a) \in \sigma_\infty(\mathfrak{a})$ contained in $\mathcal{F}_{\leqslant X^{\mathrm{Nr}(\mathfrak{a})}}$.

For this we use

V.7.2. The Lipschitz principle. The general context is the following: let $\Omega \subset \mathbb{R}^n$ be a compact measurable domain and $\Lambda \subset \mathbb{R}^n$ be a lattice. For $t > 0$, we consider the scaled compact domain

$$\Omega_t := t.\Omega$$

and we would like to count how many lattice points it contains, at least when t is large: we would like to evaluate

$$N_\Omega(t, \Lambda) = |\{\lambda \in \Lambda,\ \lambda \in t.\Omega\}|$$

as $t \to \infty$. It is reasonable to expect that the counting function is proportional to the volume

$$\mathrm{vol}(\Omega_t) = t^n \mathrm{vol}(\Omega)$$

and inverse proportional to the covolume of Λ, ie.

$$N_\Omega(t, \Lambda) \sim \frac{\mathrm{vol}(\Omega)}{\mathrm{vol}(\Lambda)} t^n,\ t \to \infty.$$

This is true if the boundary $\partial\Omega$ is sufficiently "nice".

The Lipschitz principle furnishes a sufficient condition for "niceness".

Definition V.8. *Let $\varphi : X \to Y$ be a map between metric spaces. The map φ is Lipschitz if there exists $c \geqslant 0$ such that*

$$\forall x, x' \in X,\ d(\varphi(x), \varphi(x')) \leqslant c.d(x, x').$$

Definition V.9. *A compact domain $\Omega \subset \mathbb{R}^n$ has Lipschitz boundary if its boundary $\partial\Omega$ is the union of the images of a finite set of Lipschitz maps*

$$\varphi : [0, 1]^{n-1} \to \partial\Omega.$$

Theorem V.11 (Lipschitz principle). *Let Λ be a lattice and Ω compact with Lipschitz boundary. We have as $t \to \infty$*

$$N_\Omega(t, \Lambda) = \frac{\mathrm{vol}(\Omega)}{\mathrm{vol}(\Lambda)} t^n + O_{\Lambda,\Omega}(t^{n-1}).$$

Proof. We choose a coordinate system given by a $\mathbb{Z}$-basis of Λ. In these new coordinates the boundary is still Lipschitz while the Lebesgue measure is divided by $\mathrm{vol}(\Lambda)$. We may therefore assume that $\Lambda = \mathbb{Z}^n$. We partition $\mathbb{R}^n$ into cubes with integral vertices

$$\mathbb{R}^n = \bigsqcup_{\lambda \in \mathbb{Z}^n} C(\lambda),\ C(\lambda) = \prod_{i=1}^{n} [\lambda_i, \lambda_{i+1}[$$

and

$$\Omega_t = \bigsqcup_{\lambda \in \mathbb{Z}^n} \Omega_t \cap C(\lambda).$$

We have

$$|\{\lambda,\ C(\lambda) \subset \Omega_t\}| \leqslant |\mathbb{Z}^n \cap \Omega_t| \leqslant |\{\lambda,\ C(\lambda) \cap \Omega_t \neq \emptyset\}|.$$

Computing volumes we have

$$|\{\lambda,\ C(\lambda) \subset \Omega_t\}| \leqslant \mathrm{vol}(\Omega_t) \leqslant |\{\lambda,\ C(\lambda) \cap \Omega_t \neq \emptyset\}|$$

and to conclude it is sufficient to bound the difference of the left and right most terms and to show that

$$|\{\lambda,\ C(\lambda) \cap \Omega_t \neq \emptyset\}| - |\{\lambda,\ C(\lambda) \subset \Omega_t\}| \ll t^{n-1}.$$

If

$$\lambda \in \{\lambda,\ C(\lambda) \cap \Omega_t \neq \emptyset\} - \{\lambda,\ C(\lambda) \subset \Omega_t\}$$

then λ is at distance $\leqslant \mathrm{diam}C(\Lambda) = \sqrt{n} = O(1)$ from a point in the boundary $\partial\Omega_t$.

Let $\varphi_1, \cdots, \varphi_d : [0,1]^{n-1} \to \partial\Omega$ be Lipschitz maps parametrizing $\partial\Omega$ then

$$t.\varphi_1, \cdots, t.\varphi_d : [0,1]^{n-1} \to \partial\Omega_t$$

parametrize $\partial\Omega_t = t\partial\Omega$. Let $\mathcal{P} \subset \partial\Omega_t$ be the set of points of the shape

$$t.\varphi_1(\eta/t), \cdots, t.\varphi_d(\eta/t),\ \eta \in \mathbb{Z}^{n-1} \cap [0, t[^n\}.$$

The cardinality of $\mathcal{P}$ is $O(t^{n-1})$. Any point in the cube $[0,1]^{n-1}$ is at distance $\leqslant 1/t$ from a point η/t and therefore any point of $\partial\Omega_t$ is at distance $\ll 1$ from a point of $\mathcal{P}$. It follows that the number of λ in the difference is bounded by $\ll t^{n-1}$.

□

In the course of the proof we have also obtained a bound on the number of lattice points ON the boundary:

Corollary V.7.1. *Notations and assumptions being as above, we have as $t \to \infty$*

$$N_{\partial\Omega}(t,\Lambda) = |\{\lambda \in \Lambda,\ \lambda \in \partial(\Omega_t)\}| = O(t^{n-1}).$$

Remark V.11. Alternatively we could have just applied the Lipschitz principle directly to $\partial\Omega$: if the boundary of Ω is Lipschitz it is measurable and $\mathrm{vol}(\partial\Omega) = 0$.

V.7.3. Counting lattice points in domains. Let us recall that we need to evaluate

$$|\{a \in \mathfrak{a} - \{0\},\ \mathrm{Nr}(a) \leqslant X\,\mathrm{Nr}(\mathfrak{a})\}/\mathcal{O}_K^\times|.$$

By Dirichlet's Theorem we have

$$\mathcal{O}_K^\times = \mu_K \times U$$

where $U = \prod_{i=1}^{r-1} \varepsilon_i^{\mathbb{Z}}$ is a free abelian group of rank $r-1$ (generated by a system of fundamental units $(\varepsilon_i)_{i=1\cdots r-1}$.

Setting $w_K = |\mu_K|$, we have obviously

$$|\{a \in \mathfrak{a} - \{0\},\ \mathrm{Nr}(a) \leqslant X\,\mathrm{Nr}(\mathfrak{a})\}/\mathcal{O}_K^\times| = \frac{1}{w_K}|\{a \in \mathfrak{a} - \{0\},\ \mathrm{Nr}(a) \leqslant X\,\mathrm{Nr}(\mathfrak{a})\}/U|. \tag{V.3}$$

so it is sufficient to evaluate $|\{a \in \mathfrak{a} - \{0\},\ \mathrm{Nr}(a) \leqslant X\,\mathrm{Nr}(\mathfrak{a})\}/U|$.

Let $\mathcal{F} \subset K_\infty^\times$ be a fundamental domain for the quotient $K_\infty^\times/U$ then (by homogeneity)

$$\mathcal{F}_{\leqslant X} = \{z \in \mathcal{F},\ \mathrm{Nr}(z) \leqslant X\} = \mathcal{F} \cap K_{\infty,\leqslant X}^\times$$

is a fundamental domain for the quotient $K_{\infty,\leqslant X}^\times/U$.

We will exhibit a domain $\mathcal{F}_{\leqslant X}$ which is precompact and whose boundary

$$\partial\mathcal{F}_{\leqslant X} = \overline{\mathcal{F}_{\leqslant X}} - {\mathcal{F}_{\leqslant X}}^\circ$$

is Lipschitz.

Let us recall that $\mathrm{Log}_\infty(U)$ is a lattice in the hyperplane

$$H(\mathbb{R}) = \{(l_1, \cdots, l_r) \in \mathbb{R}^r,\ T(l_1, \cdots, l_r) = l_1 + \cdots + l_r = 0\}.$$

Let

$$\mathcal{P}_U = \sum_{i=1}^{r-1} [0,1[\mathrm{Log}_\infty(\varepsilon_i) \subset H(\mathbb{R})$$

be the associated fundamental parallelepiped (a fundamental domain for the action $\mathrm{Log}_\infty(U) \curvearrowright H(\mathbb{R})$).

The preimage $\mathcal{F}_1 = \mathrm{Log}^{-1}(\mathcal{P}_U)$ is a fundamental domain representing the quotient $K_{\infty,1}^\times/U$ and (by homogeneity) the cone

$$\mathcal{F}_{\leqslant X} :=]0, X^{1/n}].\mathcal{F}_1 = \{t.z,\ t \in]0, X^{1/n}],\ z \in K_\infty^\times,\ \mathrm{Log}(z) \in \mathcal{P}\} = X^{1/n}.\mathcal{F}_{\leqslant 1}$$

is a fundamental domain for $K_{\infty,\leqslant X}^{\times}/U$. This domain is precompact and has Lipschitz boundary (because the $r-2$-dimensional faces of the parallelepiped $\mathcal{P}$ are Lipschitz and bounded and the exponential function is a smooth function). By the Lipschitz principle (and its Corollary), we have as $X \to \infty$

$$|\sigma_\infty(\mathfrak{a}) \cap \mathcal{F}_{\leqslant X}| = \frac{\mathrm{vol}(\mathcal{F}_{\leqslant 1})}{\mathrm{vol}(\sigma_\infty(\mathfrak{a}))} X + O_{\mathfrak{a}}(X^{1-1/n}) = \frac{2^{r_2}\mathrm{vol}(\mathcal{F}_{\leqslant 1})}{|\mathrm{disc}(\mathcal{O}_K)|^{1/2}\,\mathrm{Nr}(\mathfrak{a})} X + O_{\mathfrak{a}}(X^{1-1/n}).$$

Hence

$$|\sigma_\infty(\mathfrak{a}) \cap \mathcal{F}_{\leqslant X\,\mathrm{Nr}(\mathfrak{a})}| = |\{\mathfrak{a}' \in [\mathfrak{a}^{-1}],\ \mathfrak{a}' \subset \mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a}') \leqslant X\}| = \frac{2^{r_2}\mathrm{vol}(\mathcal{F}_{\leqslant 1})}{|\mathrm{disc}(\mathcal{O}_K)|^{1/2}} X + O_{\mathfrak{a}}(X^{1-1/n}).$$

From this, (V.3), (V.2) and the finiteness of the class group we obtain the asymptotic formula

$$|\{\mathfrak{a} \subset \mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a}) \leqslant X\}| = \frac{2^{r_2}\mathrm{vol}(\mathcal{F}_{\leqslant 1})h(\mathcal{O}_K)}{w_K|\mathrm{disc}(\mathcal{O}_K)|^{1/2}} X + O_K(X^{1-1/n}).$$

It remains to compute the volume of the cone $\mathrm{vol}(\mathcal{F}_{\leqslant 1})$: it is useful to write elements $z \in K_\infty^\times$ in "polar coordinates": we write

$$z = (\pm x_1, \cdots, \pm x_{r_1}, \rho_1 e(i\theta_1), \cdots, \rho_{r_2} e(i\theta_{r_2}))$$

with $x_i, \rho_j \in \mathbb{R}_{>0}$, $\theta_j \in [0, 2\pi[$. Let

$$|z| = (x_1, \cdots, x_{r_1}, \rho_1, \cdots, \rho_{r_2})$$

so that

$$\mathrm{Nr}(z) = \mathrm{Nr}(|z|) = \prod_i x_i \prod_j \rho_j^2.$$

Therefore

$$\mathrm{vol}(\mathcal{F}_{\leqslant 1}) = 2^{r_1}(2\pi)^{r_2} \int_{(*)} dx_1 \cdots dx_{r_1} \rho_1 d\rho_1 \cdots \rho_{r_2} d\rho_{r_2}$$

where the integral is over the domain of $|z| = (x_1, \cdots, x_{r_1}, \rho_1, \cdots, \rho_{r_2}) \in \mathbb{R}_{>0}^r$ satisfying

$$\mathrm{Log}(\mathrm{Nr}(|z|)^{-1/n}.|z|) \in \mathcal{P},\ \mathrm{Nr}(|z|) \leqslant 1.$$

We make the change of variable

$$|z| \in \mathbb{R}_{>0}^r \mapsto l = (l_1, \cdots, l_r) = \mathrm{Log}(|z|) \in \mathbb{R}^r$$

or in other terms

$$l_i = \log x_i,\ i \leqslant r_1,\ l_{r_1+j} = 2\log \rho_j,\ j \leqslant r_2.$$

We have

$$dx_i = e^{l_i} dl_i\ i \leqslant r_1,\ \rho_j d\rho_j = \frac{1}{2} e^{l_{r_1+j}} dl_{r_1+j},\ j \leqslant r_2.$$

and therefore we have to compute

$$2^{-r_2} \int e^{T(l_1,\cdots,l_r)} dl_1 \cdots dl_r$$

where T denote the linear form

$$T(l) = \sum_i l_i,\ l = (l_1, \cdots, l_r) \in \mathbb{R}^r,$$

and the integration is over the domain

$$T(l) \leqslant 0,\ P_H(l) \in \mathcal{P}_U$$

where

$$P_H(l) = (l_1, \cdots, l_r) - \frac{T(l)}{n}.(1, \cdots, 1)$$

is the projection of the vector l on the hyperplane $H(\mathbb{R}) = \ker(T)$. Putting $\tau = T(l) \leqslant 0$ we obtain

$$2^{-r_2} \int e^{T(l)} dl = \mathrm{vol}(\mathcal{P}_U) \int_{-\infty}^{0} e^{\tau} d\tau = 2^{-r_2} \mathrm{reg}(\mathcal{O}_K)$$

and

$$\mathrm{vol}(\mathcal{F}_{\leqslant 1}) = 2^{r_1 - r_2} (2\pi)^{r_2} \mathrm{reg}(\mathcal{O}_K)$$

which concludes the proof. □

Remark V.12. In the course of the proof we have obtained that for any ideal class $[\mathfrak{a}]$ we have

$$|\{\mathfrak{a}' \in [\mathfrak{a}],\ \mathrm{Nr}(\mathfrak{a}') \leqslant X\}| = \frac{2^{r_1} (2\pi)^{r_2} \mathrm{reg}(\mathcal{O}_K)}{w_K |\mathrm{disc}(\mathcal{O}_K)|^{1/2}} X + O_{\mathfrak{a}}(X^{1-1/n}).$$

Therefore the ideals of large norm are approximately equidistributed amongst the finitely many ideal classes of $\mathcal{O}_K$: the proportion of ideals of large norme belonging to the ideal class $[\mathfrak{a}]$ is the same and equal to $1/h(\mathcal{O}_K)$.

Such a result might be seen as an analog to the elementary fact that , given $q \geqslant 1$ some modulus and $a \in \mathbb{Z}$, the number of positive integers $n \leqslant X$ such that $n \equiv a \,(\mathrm{mod}\, q)$ (ie. contained in the congruence class $a \,(\mathrm{mod}\, q)$) have asymptotically the same size (independently of the congruence class $a \,(\mathrm{mod}\, q)$) as $X \to \infty$: indeed

$$|\{n \leqslant X,\ n \equiv a \,(\mathrm{mod}\, q)\}| = \frac{X}{q} + O(1)$$

so the main term X/q does not depend on $a \,(\mathrm{mod}\, q)$.

V.8. The Dedekind ζ-function

In this section we use the class number formula to investigate the analytic properties of the analog of Riemann's zeta function.

Proposition V.8.1. *Let s be a complex number with $\Re s > 1$ the series*

$$\zeta_K(s) := \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{\mathrm{Nr}(\mathfrak{a})^s}$$

converges absolutely and defines an holomorphic function in the half-plane $\Re s > 1$.

Proof. For $\sigma \in \mathbb{R}$ consider the series with non-negative terms

$$\zeta_K(\sigma) := \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{\mathrm{Nr}(\mathfrak{a})^{\sigma}}.$$

It is equal to

$$\sum_{m \geqslant 1} \frac{r_K(m)}{m^{\sigma}}$$

where

$$r_K(m) = |\{\mathfrak{a} \subset \mathcal{O}_K,\ \mathrm{Nr}(\mathfrak{a}) = m\}|.$$

We have seen in an exercice that for any $\varepsilon > 0$

$$N_K(X) := \sum_{m \leqslant X} r_K(m) \ll_{\varepsilon} X^{1+\varepsilon}.$$

By integration by parts (Abel summation) we have

$$\sum_{m \leqslant X} \frac{r_K(m)}{m^{\sigma}} = [x^{-\sigma} N_K(X)]_{1/2}^{X} - \int_{1/2}^{X} N_K(x) (x^{-\sigma})' dx$$

$$= N_K(X)/X^\sigma + \sigma \int_{1/2}^X N_K(x) x^{-\sigma-1} dx \ll_\varepsilon X^{1+\varepsilon-\sigma} + \sigma \int_{1/2}^X x^{\varepsilon-\sigma} dx$$

which is bounded as $X \to \infty$ as long as $\sigma > 1+\varepsilon$. The series $\zeta_K(s)$ is therefore absolutely convergent for $\Re s > 1$ and uniformly convergent in any half-plane $\Re s \geqslant 1+\eta$ for $\eta > 0$. Therefore ζ_K is holomorphic for $\Re s > 1+\eta$. □

DEFINITION V.10. *The function $s \mapsto \zeta_K(s)$ is the Dedekind ζ function of K.*

REMARK V.13. When $K = \mathbb{Q}$, $\zeta_K(s) = \zeta(s)$ is Riemann's zeta function so Dedekind's zeta function is a version of Riemann zeta function for a number field.

PROPOSITION V.8.2 (Euler product formula). *For $\Re s > 1$ we have the identity of holomorphic functions*

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - \frac{1}{\mathrm{Nr}(\mathfrak{p})^s})^{-1}$$

PROOF. We have for $\Re s > 1$

$$\zeta_K(s) = \sum_{m \geqslant 1} \frac{r_K(m)}{n^s}.$$

Since the function $m \mapsto r_K(m)$ is multiplicative, we have, in the range of absolute convergence

$$\zeta_K(s) = \prod_p (\sum_{\alpha \geqslant 0} \frac{r_K(p^\alpha)}{p^{\alpha s}}) = \prod_p \zeta_{K,p}(s).$$

For any prime p we have

$$\sum_{\alpha \geqslant 0} \frac{r_K(p^\alpha)}{p^{\alpha s}} = \sum_{\substack{\mathfrak{a} \subset \mathcal{O}_K \\ \mathrm{Nr}(\mathfrak{a}) = p-power}} \frac{1}{\mathrm{Nr}(\mathfrak{a})^s}.$$

The ideals whose norm is a p-power are exactly the ideals whose prime divisors are the prime ideals above p and therefore

$$\zeta_{K,p}(s) = \sum_{\alpha_\mathfrak{p} \geqslant 0, \mathfrak{p}|p} \frac{1}{\mathrm{Nr}(\prod_{\mathfrak{p}|p} \mathfrak{p}^{\alpha_\mathfrak{p}})^s} = \sum_{\alpha_\mathfrak{p} \geqslant 0, \mathfrak{p}|p} \frac{1}{\prod_{\mathfrak{p}|p} \mathrm{Nr}(\mathfrak{p})^{\alpha_\mathfrak{p} s}}$$

$$= \sum_{\alpha_\mathfrak{p} \geqslant 0, \mathfrak{p}|p} \frac{1}{\prod_{\mathfrak{p}|p} \mathrm{Nr}(\mathfrak{p})^{\alpha_\mathfrak{p} s}} = \prod_{\mathfrak{p}|p} (\sum_{\alpha_\mathfrak{p} \geqslant 0} \frac{1}{\prod_{\mathfrak{p}|p} \mathrm{Nr}(\mathfrak{p})^{\alpha_\mathfrak{p} s}}) = \prod_{\mathfrak{p}|p} (1 - \frac{1}{\mathrm{Nr}(\mathfrak{p})^s})^{-1}.$$

□

REMARK V.14. This factorisation is equivalent to the uniqueness of the factorisation of an ideal into a product of prime ideals just as the Euler product factorisation of Riemann's zeta function is equivalent to the fundamental theorem of arithmetic.

THEOREM V.12. *The Dedekind ζ function admits meromorphic continuation to the half-plane $\{s,\ \Re s > 1 - 1/n\}$ with a simple pole at $s = 1$. We have*

$$\mathrm{res}_{s=1} \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} h(\mathcal{O}_K) \mathrm{reg}(\mathcal{O}_K)}{w_K |\mathrm{disc}(\mathcal{O}_K)|^{1/2}}$$

where $w_K = |\mu_K|$. In particular $\zeta_K(s) \neq 0$ for $\Re s > 1$.

REMARK V.15. When $K = \mathbb{Q}$, $r_1 = 1$, $r = 1$, $h(\mathbb{Z}) = 1$, $\mathrm{reg}(\mathcal{O}_K) = 1$, $w_k = 2$, $\mathrm{disc}(\mathbb{Z}) = 1$ and the residue is 1.

We will deduce this result the class number formula:

PROOF. Let

$$\rho = \frac{2^{r_1}(2\pi)^{r_2} h(\mathcal{O}_K)\mathrm{reg}(\mathcal{O}_K)}{w_K |\mathrm{disc}(\mathcal{O}_K)|^{1/2}}$$

and

$$r_{K,0}(m) := r_K(m) - \rho.$$

We have

$$\sum_{m \leqslant X} r_{K,0}(m) = O(X^{1-1/n}).$$

For $\sigma > 1 - 1/n$ we have by integration by parts

$$\sum_{m \leqslant X} \frac{r_{K,0}(m)}{m^\sigma} = [x^{-\sigma} \sum_{m \leqslant x} r_{K,0}(m)]_{1/2}^X + \sigma \int_{1/2}^X x^{-\sigma-1} (\sum_{m \leqslant x} r_{K,0}(m)) dx$$
$$= O(1 + X^{1-1/n-\sigma}) + O(\int_{1/2}^X x^{-1/n-\sigma} dx)$$

which is bounded as long as $\sigma > 1 - 1/n$. This implies that for any $\eta > 0$ the series

$$\sum_{m \geqslant 1} \frac{r_{K,0}(m)}{m^s}$$

is absolutely uniformly converging for $\Re s > 1 - 1/n + \eta$ and is holomorphic in this half-plane. We have for any $X \geqslant 1$ the equality of partial sums

$$\sum_{m \leqslant X} \frac{r_{K,0}(m)}{m^s} = \zeta_{K,X}(s) - \rho \zeta_X(s).$$

For $\eta > 0$ and $\Re s > 1 + \eta$, $\zeta_X(s)$ converge uniformly to Riemann's zeta function ζ. Moreover $\zeta(s)$ admits meromorphic continuation to $\Re s > 1$ with a simple pole at $s = 1$ with residue 1. Therefore

$$\zeta_K(s) = \rho \zeta(s) + \sum_{m \geqslant 1} \frac{r_{K,0}(m)}{n^s}$$

admit analytic continuation to $\Re s > 1 - 1/n$ with a simple pole at $s = 1$ with residue ρ. □

REMARK V.16. Let us recall the proof of the analytic continuation of $\zeta(s)$ to $\Re s > 0$ with a simple pole at $s = 1$ of residue 1: we have for $\Re s > 1$

$$\zeta_X(s) = [[x]x^{-s}]_{1/2}^X + s \int_{1/2}^X [x] x^{-s-1} dx$$

where $[x]$ is the integral part. Writing $x = [x] + O(1)$ we have for $\Re s > 0$

$$\zeta_X(s) = X^{1-s} + O(X^{-s}) + s \int_{1/2}^X x^{-s} dx + s \int_{1/2}^X O(1) x^{-s-1} dx$$
$$= \frac{s}{s-1} 2^{s-1} + \cdots$$

where $\cdots$ is converging for $\Re s > 0$ as $X \to \infty$ with limit defining an holomorphic function in this domain.

APPENDIX A

Background material on rings, fields, and finite dimensional algebras over a field

A.1. Basic notions about rings and ideals

Let A be a ring. We will assume throughout that A is not the zero ring. We denote by $\mathcal{I}_A$ the set of all non-zero ideals of A and by $\mathcal{P}_A \subset \mathcal{I}_A$ the subset of non-zero principal ideals, that is, ideals of the shape

$$(a) := A.a,\ a \in A - \{0_A\}.$$

More generally, given a subset $S \subset A$, we denote by (S) the ideal generated by S, i.e.,

$$(S) = \bigcap \big\{\mathfrak{a} \in \mathcal{I}_A \cup \{(0)\} \colon S \subset \mathfrak{a}\big\}.$$

An ideal $\mathfrak{a} \subset A$ is *proper* if $\mathfrak{a} \neq A$.

We have the following basic operation/definitions regarding the set of ideals:

- Given two ideals $\mathfrak{a}, \mathfrak{b} \subset A$, we say that $\mathfrak{a}$ divides $\mathfrak{b}$ (denoted $\mathfrak{a}|\mathfrak{b}$) if $\mathfrak{b} \subset \mathfrak{a}$.
- Given two ideals $\mathfrak{a}, \mathfrak{b} \subset A$, we define the following ideals

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \big(\{a + b,\ a \in \mathfrak{a}, b \in \mathfrak{b}\}\big), \\ \mathfrak{a} \cap \mathfrak{b} &= \big(\{u,\ u \in \mathfrak{a}, u \in \mathfrak{b}\}\big), \\ \mathfrak{a}.\mathfrak{b} &= \big(\{a.b,\ a \in \mathfrak{a}, b \in \mathfrak{b}\}\big) \subset \mathfrak{a} \cap \mathfrak{b}. \end{aligned}$$

- A proper ideal $\mathfrak{p} \subsetneq A$ is *prime* if $A/\mathfrak{p}$ is a domain, i.e., for any $\alpha, \beta \in A/\mathfrak{p}$

$$\alpha\beta = 0 \implies \alpha = 0 \text{ or } \beta = 0.$$

  The set of prime ideals is denoted by

$$\mathrm{Spec}(A)$$

  and a typical prime will be denoted $\mathfrak{p}$.
- A proper ideal $\mathfrak{a} \subsetneq A$ is *maximal* if $A/\mathfrak{a}$ is a field or, equivalently, if $\mathfrak{a}$ is not strictly contained in any proper ideal in A. The set of maximal ideals is denoted

$$\mathrm{Spec}_{\max}(A).$$

If A is a domain we denote its field of fractions by

$$\mathrm{Frac}(A) = \left\{\frac{a}{b} \colon a, b \in A,\ b \neq 0\right\}.$$

In that case, the notion of ideal admit a slight but useful generalisation:

Definition A.1. *Let A be a domain with field of fractions Q. A* fractional (A-)ideal $\mathfrak{f} \subset Q$ *is a subset for which there exist $b \in A - \{0\}$ such that $b.\mathfrak{f}$ is an ideal in A. Let A be a domain with field of fractions Q. We denote by $\mathcal{F}_A$ the set of non-zero fractional ideals in Q and by $\mathcal{PF}_A$ the subset of non-zero principal fractional ideals, i.e., fractional ideals of the form*

$$(f) = A.f,\ f = \frac{a}{b} \in Q - \{0\}.$$

REMARK A.1. Note that any fractional A-ideal $\mathfrak{f} \subset \mathrm{Frac}(A)$ is an A-submodule, but not every A-submodule of $\mathrm{Frac}(A)$ is necessarily a fractional A-ideal. A fractional A-ideal is an A-module in Q whose elements admit some "common denominator" $b \in A - \{0\}$.

In what follows, if the underlying ring A is clear from context, we will call a fractional A-ideal in $\mathrm{Frac}(A)$ just a fractional ideal.

We assume from now on that A is a domain, denote by Q its field of fractions, and we fix once and for all an algebraic closure $\overline{Q}$ of Q. Unless specified otherwise, every algebraic extension of Q will be contained in $\overline{Q}$.

A.1.1. Noetherian rings and modules.

PROPOSITION A.1.1. *Let A be a ring and let M an A-module. The following are equivalent.*

(1) Every increasing sequence of submodules of M is eventually stationary: if

$$N_1 \subset \cdots \subset N_n \subset \cdots \subset M,$$

then $N_n = N_{n+1} = \cdots = N$ for n large enough.

(2) Every non-empty collection of submodules of M admits a maximal element (relative to inclusion).

(3) Every submodule of M is of finite type.

PROOF. If M is not of finite type, then there exists a sequence of elements $(x_i)_{i\in\mathbb{N}} \in M$ such that for all $i \geqslant 1$ we have

$$\sum_{j=1}^{i} A.x_j \subsetneq \sum_{j=1}^{i+1} A.x_j$$

and therefore we obtain an increasing sequence of submodules that is not eventually stationary.

Now suppose that every submodule of M is of finite type and let $\mathcal{C}$ be a non-empty collection of submodules of M. Assume that $c \subseteq \mathcal{C}$ is a linearly ordered by inclusion, i.e., for all $N_1, N_2 \in c$ we have $N_1 \subseteq N_2$ or $N_2 \subseteq N_1$. Define

$$N(c) = \bigcup \{N \colon N \in c\}.$$

As c is linearly ordered, it follows that $N(c)$ is a submodule of M and $N \subseteq N(c)$ for every $N \in c$. Moreover, $N(c)$ is of finite type by assumption, thus there exists a finite subset $S \subseteq N(c)$ such that

$$N(c) = \sum_{x\in S} A.x.$$

For each $x \in S$ fix a submodule $N_x \in c$ such that $x \in N_x$. As c is linearly ordered, there is $x_* \in S$ such that $N_x \subseteq N_{x_*}$ for all $x \in S$ and therefore $N(c) \subseteq N_{x_*}$. As $N_{x_*} \subseteq N(c)$ by construction, we obtain an equality and thus $N(c) = N_{x_*}$ is a maximal element in c. This shows that every linearly ordered subset of $\mathcal{C}$ contains an upper bound. Zorn's lemma therefore implies that $\mathcal{C}$ contains a maximal element.

Finally, we suppose that every non-empty collection of submodules of M contains a maximal element. We need to show that every increasing sequence of submodule eventually stabilizes. By assumption, any such sequence contains a maximal element and therefore the claim follows. □

DEFINITION A.2. *An A-module M is* Noetherian *if it satisfies any of the three equivalent conditions in Proposition A.1.1. The ring A is* Noetherian *if it is Noetherian as an A-module.*

PROPOSITION A.1.2. *Let A be noetherian and let M be an A-module of finite type, then every submodule and every quotient of M is of finite type.*

The proof of Proposition A.1.2 relies on (part of) the following Lemma.

LEMMA A.1.3. *Let A a ring and suppose that*

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0 \tag{A.1}$$

is an exact sequence of A-modules, where L and N are of finite type. Then M is of finite type.

PROOF. Let $x_1, \dots, x_r \in L$ and $z_1, \dots, z_t \in N$ such that

$$L = A.x_1 + \cdots + A.x_r,$$
$$N = A.z_1 + \cdots + A.z_t.$$

Set $y_1 = \varphi(x_1), \dots, y_r = \varphi(x_r)$. By exactness, we can find $y_{r+1}, \dots, y_{r+t} \in M$ such that $\psi(y_{r+j}) = z_j$ for all $1 \leqslant j \leqslant t$. Then M is generated by $\{y_1, \dots, y_{r+t}\}$ over A. Indeed, suppose that $y \in M$ is arbitrary and choose $a_{r+1}, \dots, a_{r+t} \in A$ such that

$$\psi(y) = \sum_{j=1}^{t} a_{r+j} z_j.$$

It follows that $y - a_{r+1}y_{r+1} - \cdots - a_{r+t}y_{r+t}$ is an element of the kernel of ψ and therefore lies in the image of φ, i.e., is an A-linear combination of $y_1, \dots, y_r$. In particular, y is an A-linear combination of $y_1, \dots, y_{r+t}$. □

PROOF OF PROPOSITION A.1.2. The second part is immediate as any generating set for M projects to a generating set for the quotient.

So we only need to show that M is noetherian. Suppose that M admits a generating set of cardinality $d \in \mathbb{N}$. Then M (and every submodule) is the homomorphic image (of a submodule) of A^d. Therefore it suffices to show that A^d is noetherian.

If $d = 1$, then this follows from the assumptions. So suppose that A^{d-1} is noetherian with $d > 1$.

Let now M be a submodule of A^d and consider the maps $\varphi : A \to A^d$ and $\psi : A^d \to A^{d-1}$ given by

$$\varphi(a) = (0, \dots, 0, a), \quad \psi(a_1, \dots, a_d) = (a_1, \dots, a_{d-1}).$$

Then

$$0 \longrightarrow \varphi(A) \cap M \longrightarrow M \longrightarrow \psi(M) \longrightarrow 0$$

is a short exact sequence of A-modules as in (A.2). Indeed, $\psi(M)$ is of finite type as it is a submodule of A^{d-1} and $\varphi(A) \cap M$ is of finite type as it is a submodule of $\varphi(A) \cong A$. □

COROLLARY A.1.1. *Let A a noetherian ring and suppose that*

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0 \tag{A.2}$$

is an exact sequence of A-modules. If M is of finite type, then so are L and L.

PROOF. By exactness, we know that ψ is surjective and thus any generating set of M is mapped onto a generating set of N. Thus N is of finite type.

Using exactness once more, we know that φ is injective and thus L is isomorphic to a submodule of M. As of Proposition A.1.2, M is noetherian and thus $\varphi(L)$ is of finite type and thus so is L. □

COROLLARY A.1.2. *Let A be a noetherian ring and R/A a ring extension. Suppose that $z \in R$ is integral over A. Then $A[z]$ is noetherian.*

PROOF. If z is A-integral, then $A[z]$ is an A-module of finite type (generated by $1, z, \cdots z^{d-1}$, where d is the degree of any monic polynomial in $A[X]$ annihilating z) and by Proposition A.1.2, any $A[z]$-ideal $\mathfrak{a} \subset A[z]$ is f.t. as an A-module and, a fortiori, as an $A[z]$-module. □

A.1.2. Prime factorisation in a PID. Recall that a ring A is noetherian if every ideal is finitely generated. In what follows, we recall properties of a special class of noetherian rings, namely the zero-divisor free rings for which every ideal is generated by a single element.

DEFINITION A.3. *A Principal Ideal Domain (PID) A is a ring which is a domain, that is,*

$$\forall a, b \in A \quad a.b = 0_A \implies a = 0_A \text{ or } b = 0_A,$$

and such that every ideal, i.e., for every ideal $\mathfrak{a} \subset A$ there is $m \in A$ such that

$$\mathfrak{a} = (m) = m.A.$$

THEOREM A.1 (Factorisation in PIDs). *Let A be a PID A.*

(1) Every non-zero prime ideal in A is maximal:

$$\mathrm{Spec}(A) \setminus \{(0)\} = \mathrm{Spec}_{\max}(A).$$

(2) For every ideal $\mathfrak{a} \in \mathcal{I}_A$ there exists a unique tuple of natural integers $(v_{\mathfrak{p}}(\mathfrak{a}))_{\mathfrak{p} \in \mathrm{Spec}(A)}$ such that

- *$v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all but finitely many $\mathfrak{p}$, and*
- *$\mathfrak{a}$ can be written as the following (finite) product*

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

where we define $\mathfrak{p}^0 = A$.

Alternatively, if one chooses for every prime ideal $\mathfrak{p}$ a generator (i.e., an element $p \in \mathfrak{p}$ such that $\mathfrak{p} = (p)$), then by considering the prime factorisation of the principal ideal generated by m

$$(m) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}((m))},$$

we obtain that any $m \in A$ can be written as a product of prime powers:

$$m = u. \prod_{\mathfrak{p}} p^{v_{\mathfrak{p}}(m)},$$

where $u \in A^\times$ and $v_{\mathfrak{p}}(m) = v_{\mathfrak{p}}\big((m)\big)$. Moreover, given a choice of a generator p for each prime ideal $\mathfrak{p}$, this factorisation of m is unique.

PROOF. The proof of both statements relies on the fact that every PID is a unique factorization domain (UFD), i.e., every element in a PID is a finite product of finitely many irreducible elements and the irreducible factors are unique up to multiplication by a unit. Moreover, in a PID every irreducible element is prime. We leave the remainder of the argument to the reader and refer to [1] for details. □

DEFINITION A.4. *Given an ideal $\mathfrak{a} \in \mathcal{I}_A$ and a prime $\mathfrak{p} \in \mathrm{Spec}(A)$, the integer $v_{\mathfrak{p}}(\mathfrak{a})$ is called the* valuation *of $\mathfrak{a}$ at $\mathfrak{p}$ or the* $\mathfrak{p}$-adic valuation *of $\mathfrak{a}$.*

Because of this, the standard factorisation properties of $\mathbb{Z}$ extend to ideals of a general PID. We have the following properties

$$\mathfrak{a} | \mathfrak{b} \iff \forall \mathfrak{p},\ v_{\mathfrak{p}}(\mathfrak{a}) \leqslant v_{\mathfrak{p}}(\mathfrak{b}).$$

$$\mathfrak{a}.\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})}$$

$$\mathfrak{a} \cap \mathfrak{b} = \text{largest ideal contained in } \mathfrak{a} \text{ and } \mathfrak{b} =: [\mathfrak{a}, \mathfrak{b}] = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))}$$

$$\mathfrak{a} + \mathfrak{b} = \text{smallest ideal containing both } \mathfrak{a} \text{ and } \mathfrak{b} =: (\mathfrak{a}, \mathfrak{b}) = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))}.$$

or in other terms

$$v_{\mathfrak{p}}(\mathfrak{a}.\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}),$$
$$v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = v_{\mathfrak{p}}([\mathfrak{a}, \mathfrak{b}]) = \max(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))$$
$$v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = v_{\mathfrak{p}}((\mathfrak{a}, \mathfrak{b})) = \min(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))$$

In particular two ideals $\mathfrak{a}, \mathfrak{b}$ in a PID are coprime (that is $\mathfrak{a} + \mathfrak{b} = A$) iff their valuation functions

$$v_\bullet(\mathfrak{a})\colon \mathfrak{p} \mapsto v_{\mathfrak{p}}(\mathfrak{a}),\ v_\bullet(\mathfrak{b})\colon \mathfrak{p} \mapsto v_{\mathfrak{p}}(\mathfrak{b})$$

have disjoint support:

$$(\mathfrak{a}, \mathfrak{b}) = A \iff \forall \mathfrak{p},\ v_{\mathfrak{p}}(\mathfrak{a}).v_{\mathfrak{p}}(\mathfrak{b}) = 0.$$

A.2. Finitely generated modules over a PID

Definition A.5. *Let A be a PID and M be an A-module.*

- *M is of finite type/finitely generated (in short, M is f.t.) if there exists a finite set $\{m_1, \cdots, m_r\} \subset M$ such that M is generated by $\{m_1, \cdots, m_r\}$ as an A-module, i.e.,*

$$M = \sum_i A.m_i = \left\{ \sum_i a_i.m_i,\ a_i \in A \right\}.$$

- *M is A-free if there is $r \geqslant 0$ such that*

$$M \simeq_A A^r.$$

In other terms, there exists (an A-basis) $\{\mathbf{e}_1, \cdots, \mathbf{e}_r\} \subset M$ such that any $m \in M$ can be written in a unique way as

$$m = \sum_{i=1}^{r} a_i.\mathbf{e}_i,\ a_i \in A.$$

The integer r is uniquely defined and is called the A-rank of M. It is denoted $\mathrm{rk}_A(M)$.

- *M is A-torsion if there exists $a \in A - \{0_A\}$ such that $a.m = 0_M$ for all $m \in M$. The set of such a (plus 0_A) is an ideal in A, the annihilating ideal of M:*

$$\mathrm{ann}(M) = \{a \in A\colon \forall m \in M\ a.m = 0_M\}.$$

We recall the following special case of Proposition A.1.2.

Proposition A.2.1. *Let A be a PID. Suppose we have an exact sequence of A-modules*

$$0 \to L \to M \to N \to 0.$$

- *If M is f.t., then so are L and N.*
- *If L and N are f.t., then so is M.*

Theorem A.2. *Let A be a PID. Any f.t. A-module M is isomorphic to a direct sum*

$$M \simeq M_{\mathrm{f}} \oplus M_{\mathrm{t}},$$

where $M_{\mathrm{f}} \simeq A^r$ is free and M_{t} is torsion. Moreover there exists $\tau \geqslant 1$ and a finite sequence of (non-zero) elements of A such that

$$A^\times \not\ni a_\tau | a_{\tau-1} | \cdots | a_1$$

and

$$M_{\mathrm{t}} \simeq \bigoplus_{i=1}^{\tau} A/(a_i).$$

In particular, M_{t} is annihilated by a_1:

$$\forall m \in M_{\mathrm{t}} \quad a_1.m = 0.$$

The tuple $(r, (a_1), \cdots, (a_\tau))$ is an invariant of M: if

$$M \simeq A^r \oplus \bigoplus_{i=1}^{\tau} A/(a_i) \simeq A^{r'} \oplus \bigoplus_{i=1}^{\tau'} A/(a'_i)$$

then $r = r'$, $\tau = \tau'$ and $(a_i) = (a'_i)$. The integer r is the A-rank of M and the ideals $(a_1)|(a_2)|\cdots|(a_\tau)$ are called the elementary divisors of M. The ideal $(a_1) = \mathrm{ann}(M)$ is called the annihilating ideal of M.

THEOREM A.3 (Adapted basis). *Suppose that $N \subset M$ is an inclusion of free A-modules of ranks r' and r respectively. Then $r \geqslant r'$ and there exist an A-basis $\{\mathbf{e}_1, \cdots, \mathbf{e}_r\}$ of M and $(a_1, \cdots, a_{r'}) \in A^{r'}$ such that $\{a_1\mathbf{e}_1, \cdots, a_{r'}\mathbf{e}_{r'}\}$ is an A-basis of N.*

In particular, if $r' = r$, the quotient module is torsion:

$$M/N \simeq \bigoplus_{i=1}^{r} A/(a_i).$$

REMARK A.2. The fundamental case is $A = \mathbb{Z}$: a $\mathbb{Z}$-module of finite type is then a finitely generated abelian group.

Since A is a domain, we write

$$Q = \mathrm{Frac}(A) = \left\{ \frac{a}{b} \colon a, b \in A,\ b \neq 0 \right\}$$

for its field of fractions.

PROPOSITION A.2.2. *Let $r \geqslant 1$ and let $f : A^r \to A^r$ be an A-linear map. We assume that f extended to a Q-linear map $f : Q^r \to Q^r$ is invertible ($\det f \neq 0$), then $A^r/f(A^r)$ is torsion and if, as above, we have*

$$A^r/f(A^r) \simeq \bigoplus_{i=1}^{r} A/(a_i),$$

then

$$(\det f) = \prod_{i=1}^{r} (a_i).$$

PROOF. Let $\mathcal{B} = \{\mathbf{e}_1, \cdots, \mathbf{e}_r\}$ be a basis of A^r adapted to $f(A^r)$ as in Theorem A.3. Then $\mathcal{B}$ is a Q-basis of Q^r. Let $f(\mathcal{B}) = (f(\mathbf{e}_1), \cdots, f(\mathbf{e}_r))$. Then $f(\mathcal{B})$ is a basis of $f(A^r)$ and a Q-basis of Q^r by assumption. Let g be the linear map such that $g\big(f(\mathbf{e}_i)\big) = a_i\mathbf{e}_i$. Then g is an automorphism of $f(A^r)$, so its matrix in the basis $f(\mathcal{B})$ as well as its inverse have coefficients in A. Therefore $\det g$ and $\det g^{-1} = (\det g)^{-1}$ are both in A; in particular, $\det g \in A^\times$. The matrix of $g \circ f$ is the diagonal matrix $\mathrm{diag}(a_1, \cdots, a_r)$ and has determinant $a_1.\cdots.a_r = \det g.\det f$. Since $\det g \in A^\times$ we have

$$(\det f) = (a_1.\cdots.a_r).$$

□

A.2.1. Lattices in $\mathbb{R}^r$. A case of particular interest to this course is given by the PID $\mathbb{Z}$, whose field of fractions embeds into $\mathbb{R}$. Under some additional topological assumption (discreteness) which will always be satisfied in the cases of interest, the theory of finitely generated $\mathbb{Z}$-modules in $\mathbb{R}^r$ admits a very geometric interpretation which we will develop in this section.

PROPOSITION A.2.3. *Let $r \in \mathbb{N}$ and suppose that $\Gamma < \mathbb{R}^r$ is a non-trivial subgroup. The following are equivalent.*

(L1) $\Gamma < \mathbb{R}^r$ is discrete.

(L2) There is $\ell \in \mathbb{N}$ and $(v_1, \ldots, v_\ell) \in (\mathbb{R}^r)^\ell$ linearly independent such that

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_\ell.$$

Definition A.6. *Let $1 \leqslant \ell \leqslant r$ and $\mathcal{B} = (v_1, \dots, v_\ell) \in (\mathbb{R}^r)^\ell$ linearly independent. Let $\Gamma < \mathbb{R}^r$ a discrete subgroup. We say that $\mathcal{B}$ is a* $\mathbb{Z}$-basis *of Γ if*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_\ell.$$

Proof of Proposition A.2.3. We first prove that (L2) implies (L1). So let's assume that (L2) holds. We have to show that there is a neighbourhood U of $0 \in \mathbb{R}^r$ such that $\Gamma \cap U = \{0\}$. If $\ell < r$, we can find $v_{\ell+1}, \dots, v_r \in \mathbb{R}$ such that $\mathcal{B} = (v_1, \dots, v_r)$ is a basis of $\mathbb{R}$. Define

$$U = \{t_1 v_1 + \cdots + t_r v_r \colon |t_i| < 1/2\}.$$

Then U is the open ball of radius $1/2$ with respect to the sup-norm defined by the basis $\mathcal{B}$, and therefore a neighbourhood of 0.

Let $v \in \Gamma \cap U$. Then there are $(n_1, \dots, n_\ell) \in \mathbb{Z}^\ell$ and $(t_1, \dots, t_r) \in (-1/2, 1/2)^r$ such that

$$v = n_1 v_1 + \cdots + n_\ell v_\ell = t_1 v_1 + \cdots + t_r v_r.$$

As the representation of v in terms of the elements of $\mathcal{B}$ is unique, it follows that for all $1 \leqslant i \leqslant r$ we have $t_1, \dots, t_r \in \mathbb{Z} \cap (-1/2, 1/2) = \{0\}$. Hence (L1) follows.

We now turn to the proof that (L1) implies (L2). Let $V = \operatorname{span}_{\mathbb{R}}(\Gamma) \subseteq \mathbb{R}^r$ be the subspace spanned by Γ and let $n = \dim(V)$. As Γ is non-trivial, we know that $n \geqslant 1$. Moreover, V is homeomorphically isomorphic to $\mathbb{R}^n$ and thus we can assume without loss of generality that $V = \mathbb{R}^r$. We will prove that (L1) implies (L2) by induction on r.

If $r = 1$, the result is standard, but we repeat it for the sake of completeness. As of (L1), we know that there is $\varepsilon > 0$ such that $(-\varepsilon, \varepsilon) \cap \Gamma = \{0\}$. In particular, there is $\gamma \in \Gamma \cap (0, \infty)$ such that $v \in \Gamma \setminus \{0\}$ implies $|v| \geqslant \gamma$. Note that $\mathbb{Z}\gamma < \Gamma$. Therefore it remains to show that $\Gamma \subseteq \mathbb{Z}\gamma$. Suppose that $v \in \Gamma$. Then there is $n \in \mathbb{Z}$ such that $v - n\gamma \in [0, \gamma)$. In particular, $|v - n\gamma| < \gamma$ and therefore $v - n\gamma = 0$. As v was arbitrary, it follows that $\Gamma \subseteq \mathbb{Z}\gamma$.

Now suppose that $r > 1$ and (L2) is true for discrete subgroups of $\mathbb{R}^k$ with $1 \leqslant k < r$. We denote by $\|\cdot\|_2$ the Euclidean norm defined with respect to the standard basis on $\mathbb{R}^r$. As Γ is discrete, there again is a shortest vector in Γ, i.e., we can find $\gamma \in \Gamma \setminus \{0\}$ such that for any $v \in \Gamma \setminus \{0\}$ we have

$$\|v\|_2 \geqslant \|\gamma\|_2.$$

Let $W = \gamma^\perp$ denote the orthogonal complement of $\operatorname{span}_{\mathbb{R}}\{\gamma\}$ in $\mathbb{R}^r$ and denote by $\pi \colon \mathbb{R}^r \to W$ the canonical projection. We claim that $\pi(\Gamma) < W$ is a discrete subgroup. To this end, let $w \in \pi(\Gamma)$ non-zero. Let $v \in \Gamma \setminus \{0\}$ such that $w = \pi(v)$. Then $v = w + t\gamma$ for some $t \in \mathbb{R}$. Note that for any $n \in \mathbb{Z}$ we have $v + n\gamma \in \Gamma$ and $\pi(v + n\gamma) = \pi(v) = w$. Thus we can assume without loss of generality that $v = w + t\gamma$ for some $t \in [-1/2, 1/2)$. As $w \perp \gamma$, we obtain that

$$\|w\|_2^2 + t^2\|\gamma\|_2^2 = \|v\|_2^2 \geqslant \|\gamma\|_2^2$$

and therefore

$$\|w\|_2 \geqslant \sqrt{1 - t^2}\|\gamma\|_2 \geqslant \frac{\sqrt{3}}{2}\|\gamma\|_2.$$

This proves discreteness of $\pi(\Gamma)$ in W. By induction, there is $(w_1, \dots, w_{r-1}) \in W^{r-1}$ linearly independent such that

$$\pi(\Gamma) = \mathbb{Z}w_1 + \cdots \mathbb{Z}w_{r-1}.$$

Let $v_1, \dots, v_{r-1} \in \Gamma$ such that $\pi(v_i) = w_i$ and let $v_r = \gamma$. Then $(v_1, \dots, v_r)$ is linearly independent. Moreover, given $v \in \Gamma$ there is a unique tuple $(n_1, \dots, n_{r-1}) \in \mathbb{Z}^{r-1}$ such that

$$\pi(v) = n_1 w_1 + \cdots + n_{r-1} w_{r-1} = \pi(n_1 v_1 + \cdots + n_{r-1} v_{r-1}).$$

Thus there is $t \in \mathbb{R}$ such that

$$v - n_1 v_1 - \cdots - n_{r-1} v_{r-1} = t\gamma \in \Gamma.$$

Again, we can write $t = n_r + \tau$ for some $n_r \in \mathbb{Z}$ and $\tau \in [-1/2, 1/2)$. Rearranging, we obtain

$$v - n_1 v_1 - \cdots - n_r v_r = \tau\gamma \in \Gamma.$$

As $\|\tau\gamma\|_2 < \|\gamma\|_2$, the choice of γ implies that $\tau = 0$ and therefore we have shown that

$$v \in \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r.$$

□

DEFINITION A.7. *Let $r \in \mathbb{N} \cup \{0\}$. A lattice in $\mathbb{R}^r$ is a discrete subgroup $\Gamma < \mathbb{R}^r$ which contains a basis of $\mathbb{R}^r$, i.e.,* $\operatorname{span}_{\mathbb{R}}(\Gamma) = \mathbb{R}^r$.

Let $\Gamma < \mathbb{R}^r$ be a discrete subgroup. A fundamental domain for the action of Γ on $\mathbb{R}^r$ is a non-empty Borel measurable set $F \subseteq \mathbb{R}^r$ satisfying

$$\mathbb{R}^r = \bigsqcup_{\gamma\in\Gamma} (F + \gamma).$$

LEMMA A.2.4. *Let $r \in \mathbb{N} \cup \{0\}$ and $\Gamma < \mathbb{R}^r$ a discrete subgroup. Then $\Gamma \curvearrowright \mathbb{R}^r$ admits a fundamental domain $F \subseteq \mathbb{R}^r$. The volume of F only depends on Γ and F can be chosen to have compact closure if and only if Γ is a lattice.*

PROOF. If $r = 0$, the only non-empty subset of $\mathbb{R}^r$ is $\{0\}$ and necessarily $\Gamma = \{0\}$. We leave it to the reader to check that $F = \{0\}$ is a fundamental domain in this case. Moreover, in this case F is necessarily unique.

Suppose now that $r \geqslant 1$ and let $(v_1, \ldots, v_m) \in (\mathbb{R}^r)^m$ be a $\mathbb{Z}$-basis of Γ and extend it to a basis $\mathcal{B} = (v_1, \ldots, v_r)$ of $\mathbb{R}^r$. We leave it as an exercise to check that the set

$$\mathcal{F}(\mathcal{B}) = \big\{t_1v_1 + \cdots + t_rv_r \colon t_1, \ldots, t_m \in [0, 1), t_{m+1}, \ldots, t_r \in \mathbb{R}\big\}$$

is a fundamental domain for $\Gamma \curvearrowright \mathbb{R}^r$. This implies the existence and clearly it has compact closure if and only if $m = r$, i.e., if and only if Γ is a lattice.

It remains to show that the volume of a fundamental domain for $\Gamma \curvearrowright \mathbb{R}^r$ depends only on Γ. Since the Lebesgue measure is finite on compact sets, this also implies that discrete subgroups which aren't lattices don't admit precompact fundamental domains.

To this end let $F_1, F_2 \subseteq \mathbb{R}^r$ be fundamental domains for $\Gamma \curvearrowright \mathbb{R}^r$ and let vol denote the Lebesgue measure on $\mathbb{R}^r$. We then have

$$\operatorname{vol}(F_1) = \sum_{\gamma\in\Gamma} \operatorname{vol}\big(F_1 \cap (F_2 + \gamma)\big) = \sum_{\gamma\in\Gamma} \operatorname{vol}\big((F_1 - \gamma) \cap F_2\big) = \operatorname{vol}(F_2).$$

Hence the volume of any two fundamental domains agrees, which implies the claim. □

Lemma A.2.4 allows us to make the following definition.

DEFINITION A.8. *Let $r \in \mathbb{N} \cup \{0\}$ and let $\Gamma < \mathbb{R}^r$ a lattice. The* covolume $\operatorname{covol}(\Gamma)$ of Γ *is defined as follows. Let $F \subseteq \mathbb{R}^r$ be any fundamental domain for $\Gamma \curvearrowright \mathbb{R}^r$, then*

$$\operatorname{covol}(\Gamma) = \operatorname{vol}(F).$$

LEMMA A.2.5. *Let $r \in \mathbb{N}$ and let $\Gamma < \mathbb{R}^r$ a lattice. Then there is $g \in \mathrm{GL}_r(\mathbb{R})$ such that*

$$\Gamma = \mathbb{Z}^r g = \{vg \colon v \in \mathbb{Z}^r\}$$

and $[0, 1)^r g$ is a fundamental domain for $\Gamma \curvearrowright \mathbb{R}^r$. In particular, $\operatorname{covol}(\Gamma) = |\det(g)|$.

PROOF. Let $\mathcal{B} = (v_1, \ldots, v_r) \in (\mathbb{R}^r)^r$ a $\mathbb{Z}$-basis of Γ and define $g \in \mathrm{Mat}_r(\mathbb{R})$ to be the matrix whose i-th row equals v_i. If $\mathcal{E} = (e_1, \ldots, e_r) \in (\mathbb{R}^r)^r$ denotes the standard basis of $\mathbb{R}^r$, then one has $v_i = e_i g$ and thus

$$\begin{aligned}\Gamma &= \{n_1v_1 + \cdots + n_rv_r \colon n_i \in \mathbb{Z}\}\\ &= \{(n_1e_1 + \cdots + n_re_r)g \colon n_i \in \mathbb{Z}\}\\ &= \{vg \colon v \in \mathbb{Z}^r\} = \mathbb{Z}^r g.\end{aligned}$$

Moreover, the same manipulations show that, using the notation from the proof of Lemma A.2.4, we have $\mathcal{F}(\mathcal{B}) = \mathcal{F}(\mathcal{E})g$ and hence

$$\operatorname{covol}(\Gamma) = \operatorname{vol}\big(\mathcal{F}(\mathcal{B})\big) = \operatorname{vol}\big(\mathcal{F}(\mathcal{E})g\big) = \operatorname{vol}\big(\mathcal{F}(\mathcal{E})\big)|\det g| = |\det g|,$$

as $\mathcal{F}(\mathcal{E}) = [0,1)$ has unit volume. □

COROLLARY A.2.1. *The map* $\mathrm{GL}_r(\mathbb{Z})\backslash \mathrm{GL}_r(\mathbb{R})$ *given by* $\mathrm{GL}_r(\mathbb{Z})g \mapsto \mathbb{Z}^r g$ *is well-defined and gives a one-to-one correspondence between the set* $\mathcal{L}(\mathbb{R}^r)$ *of lattices in* $\mathbb{R}^r$ *and the quotient* $\mathrm{GL}_r(\mathbb{Z})\backslash \mathrm{GL}_r(\mathbb{R})$.

A.2.2. $\mathbb{Q}$-lattices. In this section we return to $\mathbb{Z}$-modules in $\mathbb{Q}^r$ and use our understanding of lattices in $\mathbb{R}^r$ to give a concise description.

DEFINITION A.9. *Let V a $\mathbb{Q}$-vector space of finite dimension. A $\mathbb{Q}$-lattice $\Gamma \subseteq V$ in V is a finitely generated $\mathbb{Z}$-submodule such that* $\operatorname{span}_{\mathbb{Q}}(\Gamma) = V$.

PROPOSITION A.2.6. *Let $r \in \mathbb{N} \cup \{0\}$. The set $\mathcal{L}(\mathbb{Q}^r)$ of $\mathbb{Q}$-lattices in $\mathbb{Q}^r$ is in one-to-one correspondence with* $\mathrm{GL}_r(\mathbb{Z})\backslash \mathrm{GL}_r(\mathbb{Q})$ *via the map*

$$\begin{array}{ccc} \mathrm{GL}_r(\mathbb{Z})\backslash \mathrm{GL}_r(\mathbb{Q}) & \mapsto & \mathcal{L}(\mathbb{Q}^r) \\ \mathrm{GL}_r(\mathbb{Z})g & \mapsto & \mathbb{Z}^r g \end{array}.$$

PROOF. Extension of scalars $\mathbb{Q}^r \hookrightarrow \mathbb{Q}^r \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r$ gives rise to an embedding $\mathcal{L}(\mathbb{Q}^r) \hookrightarrow \mathcal{L}(\mathbb{R}^r)$, where a lattice $\Gamma < \mathbb{R}^r$ lies in the image of $\mathcal{L}(\mathbb{Q}^r)$ under the embedding if and only if Γ is contained in the image of $\mathbb{Q}^r$, i.e., the $\mathbb{Q}$-linear hull of $\mathcal{E}$ inside $\mathbb{R}^r$. This is the case if and only if $\Gamma = \mathbb{Z}^r g$ for some $g \in \mathrm{GL}_r(\mathbb{Q})$ and hence the claim. □

A.3. Finite dimensional algebras over a field

For the rest of this chapter our main interest concerns the case of torsion modules for the ring $Q[X]$ of polynomials over a field Q. Since $Q[X]$ is a PID and $Q[X]^\times = Q^\times$, any proper ideal is generated by a unique monic polynomial. In particular, if V is a finite dimensional Q-vector space and $z \in \mathrm{End}_Q(V)$ is a linear map, then V becomes a torsion $Q[X]$-module via the map

$$\mathrm{ev}_z \colon P \in Q[X] \mapsto P(z) \in \mathrm{End}_Q(V)$$

and the monic generator of the annihilating ideal is the minimal polynomial of z, denoted $P_{\min,z}$.

Let Q be a field, $\overline{Q}$ an algebraic closure, and K a Q-algebra (with unit) of finite dimension as a Q-vector space. We will assume that K is non-trivial and identify Q with a subfield of K, namely

$$Q \simeq Q.1_K \subset K.$$

We may and will therefore assume that

$$Q \subset K$$

and hence that $0_K = 0_Q$ and $1_K = 1_Q$.

A basic (in general non-commutative) example is the algebra $K = \mathrm{End}_Q(V)$ of endomorphisms of a finite dimensional Q-vector space V: we have $\dim_Q(K) = d^2$, where $d = \dim_Q(V)$.

Another basic example is K being a field extension of Q of finite Q-dimension.

DEFINITION A.10. *Let K/Q be a finite dimensional Q-algebra. Its dimension is also called the degree of K/Q and is denoted*

$$\dim_Q(K) = \deg(K/Q) = [K : Q].$$

A.3.1. Polynomials, minimal and characteristic.

A.3.1.1. *Minimal polynomial.* Given $z \in K$, the "evaluation at z-map"

$$\mathrm{ev}_z \colon \begin{array}{ccc} Q[X] & \mapsto & K \\ P & \mapsto & \mathrm{ev}_z(P) = P(z) \end{array}$$

is a Q-algebra morphism whose kernel is an ideal of $Q[X]$, hence principal. Since

$$Q[X]/\ker(\mathrm{ev}_z) \simeq Q[z] \subset K$$

and K is finite dimensional, the kernel is non-zero and has a unique monic generator called the *minimal polynomial* of z over Q, which is denoted $P_{Q,\min,z}$:

$$\ker(\mathrm{ev}_z) = \{P \in Q[X] \colon P(z) = 0_K\} = P_{Q,\min,z}.Q[X] = (P_{Q,\min,z}).$$

As $Q[X]/(P_{Q,\min,z}) \simeq Q[z]$, we have that

$$\deg(P_{Q,\min,z}) = \dim_Q Q[z] = \big[Q[z] : Q\big].$$

The integer

$$\deg_Q(z) = \deg(P_{Q,\min,z})$$

is called the degree of z over Q.

Remark A.3. If K is a field, then $Q[z] \subset K$ is a domain and, since

$$Q[z] \simeq Q[X]/(P_{Q,\min,z}),$$

the ideal $(P_{Q,\min,z})$ prime and hence is maximal (since $Q[X]$ is a PID): $P_{Q,\min,z}$ is an irreducible polynomial.

A.3.1.2. *Characteristic polynomial.* To any $z \in K$, we also associate the (Q-linear) "multiplication by z"-map

$$[\times z]_{K/Q} \colon \begin{array}{ccc} K & \mapsto & K \\ x & \mapsto & z.x \end{array}.$$

Remark A.4. The index $\bullet_{K/Q}$ is sometimes necessary: for instance, if we have a tower of algebras $Q \subset K \subset L$ and $z \in K$, then z acts on K and L but the maps $[\times z]_{K/Q}$ and $[\times z]_{L/Q}$ are obvioulsy different. However, if the algebra K/Q on which z acts is clear from context, we will simply write $[\times z]$ instead of $[\times z]_{K/Q}$.

Lemma A.3.1. *The map*

$$[\times \bullet]_{K/Q} \colon z \in K \to [\times z]_{K/Q} \in \mathrm{End}_Q(K)$$

is injective and K can be identified with a subalgebra of $\mathrm{End}_Q(K)$. *For any $z \in K$, define the following annihilating ideals (in $Q[X]$):*

$$\mathrm{Ann}\big([\times z]_{K/Q}\big) = \{P \in Q[X] \colon P([\times z]) = 0_{\mathrm{End}_Q(K)}\},$$
$$\mathrm{Ann}_{K/Q}(z) = \{P \in Q[X] \colon P(z) = 0_K\}.$$

Then $\mathrm{Ann}\big([\times z]_{K/Q}\big) = \mathrm{Ann}_{K/Q}(z)$ *and, therefore, the minimal polynomial $P_{K/Q,\min,z}$ of the linear map $[\times z]$ is equal to the minimal polynomial $P_{Q,\min,z}$ of z over Q.*

Proof. Given $z \in K$ s.t. $[\times z] = 0_{\mathrm{End}_Q(K)}$, we have

$$0_K = [\times z](1_K) = z.1_K = z.$$

This proves injectivity. The equality of the ideals follows from $[\times \bullet]_{K/Q}$ being a homomorphism of Q-algebras, i.e., for any $P \in Q[X]$ and for any $z \in K$ we have that

$$[\times P(z)]_{K/Q} = P\big([\times z]_{K/Q}\big).$$

□

By Cayley-Hamilton we know at least one non-zero element of $\mathrm{Ann}\big([\times z]_{K/Q}\big)$.

DEFINITION A.11. *The characteristic polynomial $P_{K/Q,\mathrm{car},z}(X) \in Q[X]$ of z is the characteristic polynomial of $[\times z]_{K/Q}$: if $d = [K : Q]$ denotes the degree, then we have*

$$P_{K/Q,\mathrm{car},z}(X) = \det(X.\mathrm{Id}_K - [\times z]_{K/Q}) = X^d - \mathrm{tr}([\times z]_{K/Q})X^{d-1} + \cdots + (-1)^d \det([\times z]_{K/Q}).$$

It belongs to $\mathrm{Ann}([\times z]_{K/Q})$ *by the Cayley-Hamilton theorem. In particular, one has*

$$P_{Q,\min,z} | P_{K/Q,\mathrm{car},z}.$$

A.3.2. Norm and trace.

DEFINITION A.12. *The $d-1$-th coefficient (multiplied by -1) and the constant coefficient (multiplied by $(-1)^d$) are respectively the trace and the determinant of $[\times z]_{K/Q}$. They are also called the K/Q-trace and the K/Q-norm of z:*

$$\mathrm{tr}([\times z]_{K/Q}) =: \mathrm{tr}_{K/Q}(z),\ \det([\times z]_{K/Q}) =: \mathrm{Nr}_{K/Q}(z).$$

REMARK A.5. If we factor the characteristic polynomial over $\overline{Q}$

$$P_{K/Q,\mathrm{car},z}(X) = \prod_{i=1}^{d}(X - z_i)$$

(the roots z_i are the eigenvalues of $[\times z]$), then we obtain the formula

$$\mathrm{tr}_{K/Q}(z) = z_1 + \cdots + z_d,\ \mathrm{Nr}_{K/Q}(z) = z_1.\cdots.z_d.$$

REMARK A.6. For any $P \in Q[X]$ we have

$$\mathrm{tr}_{K/Q}\big(P(z)\big) = P(z_1) + \cdots + P(z_d),\ \mathrm{Nr}_{K/Q}\left(P(z)\right) = P(z_1).\cdots.P(z_d)$$

since, for any $P \in Q[X]$,

$$[\times P(z)]_{K/Q} = P\big([\times z]_{K/Q}\big)$$

and the eigenvalues of $P\big([\times z]_{K/Q}\big)$ are the $P(z_i),\ i = 1, \cdots, d$.

PROPOSITION A.3.2. *The trace map*

$$\mathrm{tr}_{K/Q} \colon z \in K \to \mathrm{tr}_{K/Q}(z) \in Q$$

is a Q-linear form and the norm map

$$\mathrm{Nr}_{K/Q} \colon z \in K \to \mathrm{Nr}_{K/Q}(z) \in Q$$

is multiplicative:

$$\forall \lambda \in Q,\ z, z' \in K,\ \mathrm{tr}_{K/Q}(\lambda z + z') = \lambda \mathrm{tr}_{K/Q}(z) + \mathrm{tr}_{K/Q}(z'),$$
$$\mathrm{Nr}_{K/Q}(z.z') = \mathrm{Nr}_{K/Q}(z).\,\mathrm{Nr}_{K/Q}(z').$$

Moreover, for $\lambda \in Q$, one has

$$\mathrm{tr}_{K/Q}(\lambda) = d.\lambda,\ \mathrm{Nr}_{K/Q}(\lambda) = \lambda^d.$$

If K is a field, we have

$$\forall z \in K,\ \mathrm{Nr}_{K/Q}(z) = 0 \iff z = 0.$$

PROOF. This is a direct consequence of the linearity of the trace and the multiplicativity of the determinant and the fact that

$$z \mapsto [\times z]_{K/Q}$$

is a K-algebra morphism. Moreover for $\lambda \in Q$,

$$[\times \lambda]_{K/Q} = \lambda \mathrm{Id}_K.$$

Finally, if K is a field, using that an injective algebra homomorphism gives an isomorphism between the group of units and the group of units in the image, we obtain that

$$z \neq 0_K \iff [\times z]_{K/Q} \text{ is invertible } \iff \det\big([\times z]_{K/Q}\big) \neq 0.$$

(Note that for $z \neq 0$ we have $[\times z]_{K/Q}^{-1} = [\times z^{-1}]_{K/Q}$.) □

A.3.2.1. *Transitivity relation.* Consider an inclusion of finite dimensional Q-algebras

$$Q \subset K \subset L$$

and suppose that K is a field, then L is a K-vector space.

PROPOSITION A.3.3 (Transitivity for degree, the trace and the norm). *We have for any $z \in K$*

$$P_{L/Q,\mathrm{car},z}(X) = P_{K/Q,\mathrm{car},z}(X)^{[L:K]}.$$

In particular, we have

$$[L:Q] = [L:K].[K:Q]$$

and

$$\mathrm{tr}_{L/Q}(z) = [L:K].\mathrm{tr}_{K/Q}(z),\ \mathrm{Nr}_{L/Q}(z) = \mathrm{Nr}_{K/Q}(z)^{[L:K]}.$$

PROOF. Let $\ell = [L:K]$, $d = [K:Q]$, $(\mathbf{e}_1, \cdots, \mathbf{e}_d)$ a Q-basis of K and $(\mathbf{f}_1, \cdots, \mathbf{f}_\ell)$ a K-basis of L. Then

$$L = \bigoplus_j K.\mathbf{f}_j = \bigoplus_{i,j} Q\mathbf{e}_i.\mathbf{f}_j.$$

Moreover the Q-subspaces $K.\mathbf{f}_j = \bigoplus_i Q\mathbf{e}_i.\mathbf{f}_j$ are stable under $[\times z]_{L/Q}$ (because $z.K \subset K$). Therefore, the marix of $[\times z]_{L/Q}$ in the basis

$$(\mathbf{e}_1.\mathbf{f}_1, \ldots, \mathbf{e}_d.\mathbf{f}_1, \ldots, \mathbf{e}_1.\mathbf{f}_\ell, \ldots, \mathbf{e}_d.\mathbf{f}_\ell) \tag{A.3}$$

is block-diagonal with $[L:K]$-many blocks which are the matrices of $[\times z]_{K/Q}$ in the basis $(\mathbf{e}_1, \ldots, \mathbf{e}_d)$. Therefore, we have

$$P_{L/Q,\mathrm{car},z}(X) = P_{K/Q,\mathrm{car},z}(X)^{[L:K]}.$$

□

Regarding the minimal polynomial we have the following Proposition.

PROPOSITION A.3.4. *We have*

$$P_{L/Q,\min,z} = P_{K/Q,\min,z}.$$

PROOF. As we have seen, in the basis (A.3), the matrix of $[\times z]_{L/Q}$ is block-diagonal with diagonal blocks identical to the matrices of $[\times z]_{K/Q}$. Therefore, any polynomial in $Q[X]$ annihilating $[\times z]_{K/Q}$ also annihilates $[\times z]_{L/Q}$. On the other hand, if $P \in Q[X]$ annihilates $[\times z]_{L/Q}$, since $K \subset L$ is $[\times z]_{L/Q}$-invariant we have

$$0 = P([\times z]_{L/Q})|_K = P([\times z]_{L/Q}|_K) = P([\times z]_{K/Q})$$

and thus every polynomial that annihilates $[\times z]_{L/Q}$ also annihilates $[\times z]_{K/Q}$. In particular, we have

$$\mathrm{Ann}\big([\times z]_{L/Q}\big) = \mathrm{Ann}\big([\times z]_{K/Q}\big)$$

and therefore the claim. □

A.3.2.2. *Trace bilinear form.*

DEFINITION A.13. *The trace bilinear form of the extension K/Q is the form*

$$(z, z') \in K^2 \mapsto \langle z, z' \rangle_{K/Q} := \mathrm{tr}_{K/Q}(zz') \in Q.$$

Recall that a bilinear form is called *non-degenerate* if the dual map

$$\begin{array}{ccc} K & \mapsto & K^\star \\ z & \mapsto & z^\star := \langle z, \cdot \rangle_{K/Q} \colon z' \mapsto \langle z, z' \rangle_{K/Q} \end{array}$$

is bijective.

A.3.2.3. *Discriminant.* Let us recall a numerical criterion for a bilinear form to be non-degenerate: A bilinear form is non-degenrate if and only if its *discriminant* does not vanish.

DEFINITION A.14. *Let K/Q be a finite dimensional Q-algebra and let $\mathbf{z} = (z_1, \cdots, z_n) \in K^n$ be an n-tuple; the* discriminant *of $\mathbf{z}$ (with respect to the bilinear trace form) is the determinant of the matrix $(\langle z_i, z_j\rangle_{K/Q})_{i,j\leqslant n}$:*

$$\mathrm{disc}_{K/Q}(\mathbf{z}) := \det\big((\langle z_i, z_j\rangle_{K/Q})_{i,j}\big).$$

The most interesting case is when $(z_1, \cdots, z_n) = \mathcal{B}$ is a Q-basis of K.

PROPOSITION A.3.5. *The bilinear trace form $\langle\cdot,\cdot\rangle_{L/K}$ is non-degenerate if and only if there is at least one Q-basis $\mathcal{B} = (\mathbf{e}_1, \cdots, \mathbf{e}_n)$ of K such that*

$$\mathrm{disc}_{K/Q}(\mathcal{B}) \neq 0.$$

In that case for any Q-basis $\mathcal{B}'$ of K one has $\mathrm{disc}_{K/Q}(\mathcal{B}') \neq 0$ and for any tuple $\mathbf{z} = (z_1, \cdots, z_n) \in K^n$ one has

$$\mathrm{disc}_{K/Q}(\mathbf{z}) \neq 0 \iff \mathbf{z} \text{ is a } Q\text{-basis.}$$

REMARK A.7. Let us recall that, if $\mathbf{z} \in K^n$ is an n-tuple and M is the matrix giving the coordinates of $\mathbf{z}$ in the basis $\mathcal{B} = (\mathbf{e}_1, \cdots, \mathbf{e}_n)$, then

$$\mathrm{disc}_{K/Q}(\mathbf{z}) = (\det M)^2 \mathrm{disc}_{K/Q}(\mathcal{B}).$$

This implies the second part of Proposition A.3.5.

The following definition will be useful.

DEFINITION A.15. *Let K/Q be a finite dimensional Q algebra of dimension d and let $z \in K$. We define the discriminant of z to be*

$$\mathrm{disc}_{K/Q}(z) = \mathrm{disc}_{K/Q}(1, z, \cdots, z^{d-1}).$$

REMARK A.8. If $\mathrm{disc}_{K/Q}(z) \neq 0$, then $(1, z, \cdots, z^{d-1})$ is a Q-basis of K. In particular, z is algebraic over Q and $K = Q[z] = Q(z)$ is a field.

A.4. Commutative separable algebras

Given a field Q, we denote by $\overline{Q}$ its algebraic closure. In particular, whenever we have a finite dimensional Q-vector space V (which we identify with some Q^r by choosing some basis) and a linear endomorphism $f\colon V \to V$, we can look at the eigenvalues, eigenvectors, as well as the (generalized) eigenspaces of f (or the matrix representing f) when we pass to the algebraic closure $\overline{Q}$. In more canonical terms, we look at the spectral properties of f in the $\overline{Q}$-vector space $\overline{V} = V \otimes_Q \overline{Q}$.

We will apply this to the case where K/Q is a commutative finite dimensional Q-algebra and to the endomorphisms $[\times z]_{K/Q} \in \mathrm{End}_Q(K)$.

In particular, if we factor the minimal polynomial $P_{Q,\min,z}$ in $\overline{Q}$, say

$$P_{Q,\min,z}(X) = \prod_{i=1}^{d} (X - z_i)^{e_i},$$

its roots

$$\{z_i\colon i = 1, \cdots, d\},\ d \leqslant \deg_Q(z)$$

are the eigenvalues of the (matrix of) $[\times z]_{K/Q}$ (relative to a(ny) Q-basis of K).

DEFINITION A.16. *Let K/Q be a commutative finite dimensional Q-algebra. We say that $z \in K$ is separable (sometimes one says semisimple) if one of the following equivalent conditions is satisfied.*

- *$P_{Q,\min,z}$ has only simple roots (i.e. $d = \dim_Q(z)$ or equivalently $e_i = 1$ for $i = 1, \cdots d$).*
- *The matrix of $[\times z]_{K/Q}$ (computed in any Q-basis of K) is diagonalisable in $\overline{Q}$.*

The commutative Q-algebra K/Q is separable if every element in K is separable.

REMARK A.9. Let us observe that a polynomial $P \in Q[X]$ has only simple roots (i.e., is separable) if and only if

$$\gcd(P, P') = 1,$$

where $\gcd(P, P')$ is the unique monic generator of the ideal generated by P and P'.

Let us spell out what diagonalizability means.

Fix a Q-basis $\mathcal{B}$ of K. Given $T \in \mathrm{End}_Q(K)$, we denote by $M_{\mathcal{B},T} \in M_d(Q)$ the matrix representation of T with respect to the basis $\mathcal{B}$. Then the map

$$z \in K \mapsto M_z := M_{\mathcal{B},[\times z]_{K/Q}} \in M_d(Q)$$

identifies K with a commutative algebra of $d \times d$-matrices which we will still denote by K. Then z is separable if and only if there exists $g_z \in \mathrm{GL}_d(\overline{Q})$ (the base change matrix) such that

$$\mathrm{Ad}(g_z)(M_z) = g_z.M_z.g_z^{-1} \in M_d(\overline{Q})$$

is diagonal.

THEOREM A.4. *Let K/Q be a finite dimensional commutative Q-algebra. The set*

$$K^{sep} = \{z \in K \colon z \text{ is separable}\} \subset K$$

of separable elements of K/Q is a Q-subalgebra of K and is the maximal separable subalgebra of K. It is called the separable closure of Q in K.

In particular if K is generated as a Q-algebra by separable elements, then K is separable.

PROOF. It suffices to show that for any $z_1, z_2 \in K$ every element of $Q[z_1, z_2]$ is separable. Choose a basis $\mathcal{B}$ of K/Q and let M_{z_1} and M_{z_2} be the associated matrices of $[\times z_1]_{K/Q}$ and $[\times z_2]_{K/Q}$ respectively. Since z_1, z_2 commute, the endomorphisms $[\times z_1]_{K/Q}$ and $[\times z_2]_{K/Q}$ commute and if they are both diagonalisable they can be diagonalized simultaneously in a common basis (of $\overline{Q}^d$): this follows from the fact that the eigenspaces of M_{z_1} in $\overline{Q}^d$ are preserved by M_{z_2} (because M_{z_1} and M_{z_2} commute) and the restriction of a diagonalizable map to a subspace is again diagonalizable. That is, there exists $g \in \mathrm{GL}_d(\overline{Q})$ such that

$$g.M_{z_1}.g^{-1},\ g.M_{z_2}.g^{-1} \in \mathrm{diag}_d(\overline{Q}).$$

Since the map

$$\mathrm{Ad}(g) \colon M \in M_d(\overline{Q}) \mapsto g.M.g^{-1} \in M_d(\overline{Q})$$

is a $\overline{Q}$-algebra homomorphism, since the set of diagonal matrices $\mathrm{diag}_d(\overline{Q})$ is a subalgebra of $M_d(\overline{Q})$, and since the map

$$z \in K \mapsto M_z \in M_d(\overline{Q})$$

is also a $\overline{Q}$-algebra homomorphism, for any $P(Z_1, Z_2) \in Q[Z_1, Z_2]$ the matrix of $P([\times z_1]_{K/Q}, [\times z_2]_{K/Q})$ is also diagonalisable: we have

$$M_{P([\times z_1]_{K/Q}, [\times z_2]_{K/Q})} = P(M_{z_1}, M_{z_2})$$

and

$$\mathrm{Ad}(g)\big(P(M_{z_1}, M_{z_2})\big) = P\big(\mathrm{Ad}(g)(M_{z_1}), \mathrm{Ad}(g)(M_{z_2})\big) \in \mathrm{diag}_d(\overline{Q}).$$

The remaining two statements follow immediately from the the first part of the proposition. □

DEFINITION A.17. *A commutative algebra K/Q is separable if $K^{sep} = K$; equivalently K is separable if every element of K is separable or if K is generated as a Q-algebra by separable elements.*

A.4.1. Relation with the trace and the norm. Let K/Q be a separable commutative finite dimensional Q-algebra; since all the matrices M_z, $z \in K$, commute, these matrices can be *simultaneously diagonalized* in a common basis: there exists a matrix $g \in \mathrm{GL}_d(\overline{Q})$ such that for every $z \in K$ we have

$$\mathrm{Ad}(g)(M_z) = g.M_z.g^{-1} \in \mathrm{diag}_d(\overline{Q}) \simeq \overline{Q}^d.$$

Since

$$\mathrm{Ad}(g)\colon M_d(\overline{Q}) \mapsto M_d(\overline{Q})$$

is a $\overline{Q}$-algebra automorphism of $M_d(\overline{Q})$, we have an injective algebra homomorphism

$$\sigma = \sigma_g : z \in K \mapsto g.M_z.g^{-1} \in \mathrm{diag}_d(\overline{Q}).$$

In what follows, we assume implicitly a fixed g as above.

Given $z \in K$, we have

$$\sigma(z) = \mathrm{diag}\big(\sigma_1(z), \cdots, \sigma_d(z)\big)$$

and the entry $\sigma_i(z)$ is the i-th eigenvalue of the matrix M_z (for the ordering determined by g). Note that, as σ is a morphism of Q-algebras, for $i = 1, \cdots, d$ the maps

$$\sigma_i : z \mapsto \sigma_i(z) \in \overline{Q}$$

are Q-algebra morphisms from K to $\overline{Q}$. Observe also that the map σ is injective (being the composition of two injective maps).

Considering the characteristic polynomial, we have that for all $z \in K$

$$P_{K/Q,\mathrm{car},z}(X) = \prod_{i=1}^{d} \big(X - \sigma_i(z)\big) \tag{A.4}$$

$$\mathrm{tr}_{K/Q}(z) = \sum_{i=1}^{d} \sigma_i(z),\ \mathrm{Nr}_{K/Q}(z) = \prod_{i=1}^{d} \sigma_i(z). \tag{A.5}$$

Using these relations, we deduce the following formula for the discriminant of the trace bilinear form $\langle \cdot, \cdot \rangle_{K/Q}$:

Proposition A.4.1. *Let K be a finite dimensional commutative separable algebra over Q and denote by $d = [K : Q]$ its degree. Let $(z_1, \cdots, z_d) \in K^d$ be a d-tuple. Then*

$$\mathrm{disc}_{K/Q}(z_1, \cdots, z_d) = \det\big((\mathrm{tr}_{K/Q}(z_i z_j))_{i,j \leqslant d}\big) = \det\big((\sigma_k(z_i))_{i,k \leqslant d}\big)^2.$$

Moreover, the trace bilinear form $\langle \cdot, \cdot \rangle_{K/Q}$ is non-degenerate.

Proof. Since the σ_i, $i = 1, \cdots, d$, are algebra morphisms, we have the following identities between $d \times d$ matrices over $\overline{Q}$:

$$\begin{aligned}\big(\mathrm{tr}_{K/Q}(z_i z_j)\big)_{i,j \leqslant d} &= \left(\sum_k \sigma_k(z_i z_j)\right)_{i,j \leqslant d} = \left(\sum_k \sigma_k(z_i)\sigma_k(z_j)\right)_{i,j \leqslant d} \\ &= (\sigma_k(z_i))_{i,k \leqslant d} \times (\sigma_k(z_j))_{k,j \leqslant d} = M \times {}^tM\end{aligned}$$

and taking determinants we have

$$\det\big((\mathrm{tr}_{K/Q}(z_i z_j)\big)_{i,j \leqslant d}) = \det(M)^2 = \det\big((\sigma_k(z_i))_{i,k \leqslant d}\big)^2.$$

□

A.5. The case of fields

In this section we consider the case where K is a field containing (and of finite dimension over) Q. Without loss of generality we may assume that K is a subfield of an algebraic closure of Q:

$$Q \subset K \subset \overline{Q}.$$

The important difference in comparison to the general case of commutative algebras is that for $z \in K$ the minimal polynomial $P_{Q,\min,z}(X)$ is irreducible: indeed the evaluation map

$$P(X) \in Q[X] \mapsto \mathrm{ev}_z(P) = P(z) \in K$$

has for image the domain

$$Q[z] \simeq Q[X]/(P_{Q,\min,z})$$

and therefore $P_{Q,\min,z}$ is irreducible and $Q[z]$ is a field.

A.5.1. Non-separable elements. The next result shows that if K is a field, most if its elements are separable unless we are in a very special situation.

PROPOSITION A.5.1. *If $z \in K$ is not separable, then the characteristic of Q, p say, is non-zero and there exist $k \geqslant 1$ and an irreducible polynomial $R \in Q[X]$ with only simple roots such that the minimal polynomial $P_{Q,\min,z}(X)$ is of the form*

$$P_{Q,\min,z}(X) = R(X^{p^k}).$$

In particular,

$$p^k \deg(R) = [Q[z] : Q] | [K : Q].$$

Conversely if $P_{Q,\min,z}$ is of that shape, then z is not separable.

PROOF. Let us recall that z is separable if and only if its minimal polynomial is coprime to its first derivative:

$$(P_{Q,\min,z}, P'_{Q,\min,z}) = 1.$$

However, as K is a field, $P_{Q,\min,z}$ is irreducible and thus coplrime to $P'_{Q,\min,z}$ (and hence z is separable) unless

$$P'_{Q,\min,z} = 0.$$

Write

$$P_{Q,\min,z}(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0.$$

We have

$$P'_{Q,\min,z}(X) = dX^{d-1} + a_{d-1}(d-1)X^{d-2} + \cdots + a_1.$$

As z is non-separable, we have $P'_{Q,\min,z} = 0$ and therefore for any $k \geqslant 1$ with $a_k \neq 0$ we must have $k.1_Q = 0$. This can only occur if $\mathrm{car}(K) = p > 0$ and k is a multiple of p. Therefore

$$P_{Q,\min,z}(X) = R_1(X^p)$$

for $R_1 \in Q[X]$ irreducible. If the roots of R_1 are simple we are done. Otherwise, by the same argument there is an irreducible polynomial $R_2 \in Q[X]$ such that $R_1(X) = R_2(X^p)$ and we continue until we obtain a polynomial with simple roots. □

COROLLARY A.5.1. *A field extension of characteristic zero is separable. A field extension of degree coprime to the characteristic of Q is separable.*

COROLLARY A.5.2. *If Q is a finite field, then any finite degree extension K/Q is separable.*

PROOF. Write $Q = \mathbb{F}_q$ and $K = \mathbb{F}_{q^d}$. Any $z \in K - \{0\}$ is a root of $P = X^{q^d-1} - 1$ which has simple roots since $(X^{q^d-1} - 1)' = -X^{q^d-2}$ which is coprime to $X^{q^d-1} - 1$. As $P_{K/Q,\min,z} | P$, z is separable. □

A.5.2. Perfect fields.

DEFINITION A.18. *A field k is perfect if any algebraic extension of k is separable.*

EXAMPLE A.1. From the previous discussion we know that fields of characteristic 0 and finite fields are perfect. Obviously algebraically closed fields are perfect.

EXERCISE A.1. Let $Q \subset \overline{Q}$ be a field of characteristic p and let

$$Q^{1/p^\infty} = \{z \in \overline{Q} \colon z^{p^k} \in Q \text{ for some } k \geqslant 0\}$$

(the set of p-th power roots of elements of Q). Show that Q^{1/p^∞} is a field and that it is perfect.

A.5.3. The primitive element theorem. A fundamental result for separable extensions is

THEOREM A.5 (Primitive element). *Let K/Q be a finite separable extension. There exists $z \in K$ such that*

$$K = Q[z].$$

In particular for such z one has

$$P_{Q,\min,z}(X) = P_{K/Q,\mathrm{car},z}(X)$$

and $P_{K/Q,\mathrm{car},z}(X)$ is irreducible with simple roots.

PROOF. If Q is a finite field, then K is finite and $K^\times$ is cyclic so that $K = Q(\zeta)$ where ζ is a generator of $K^\times$.

Suppose now that K is infinite. As K is finitely generated over Q, it is sufficient to show that if $K = Q(x, y)$ with $x, y \in K$, then $K = Q(z)$ for some $z \in K$. It will turn out that we can find such z of the shape

$$z_\lambda = x + \lambda y$$

with $\lambda \in Q$. Set $K_\lambda = Q(z_\lambda)$. Let $P(X) = \prod_i (X - x_i)$ and $R(X) = \prod_j (X - y_j)$ be the minimal polynomials of x and y factorized over $\overline{Q}$ and assume $x = x_1$, $y = y_1$; since x and y are separable, the x_i are distinct and likewise for the y_j. The polynomial $R_\lambda(X) = P(z_\lambda - \lambda X)$ has coefficients in K_λ and vanishes at y so R and R_λ have y as a common root. Since K is infinite, we may choose λ so that y is the only common root: the other roots of R are y_j ($y_1 = y$) and the roots of R_λ are

$$\frac{z_\lambda - x_i}{\lambda} = \frac{x_1 - x_i + \lambda y_1}{\lambda}$$

for x_i running over the roots of P ($x = x_1$).

For such λ we find in particular, that both R and R_λ are divisible by $X - y$ in $K[X]$. As they don't share any further roots, we in fact have that $(R, R_\lambda) = X - y$. On the other hand, we have that (R, R_λ) is invariant under field extension, i.e., $(R, R_\lambda) \in K_\lambda[X]$. To this end recall that the calculation of (R, R_λ) via the Euclidean algorithm only uses arithmetic in the base field (in this case K_λ). In particular, $X - y \in K_\lambda[X]$ and therefore $y \in K_\lambda = Q(z_\lambda)$. It follows that $x = z_\lambda - \lambda y \in K_\lambda$. □

A.5.4. Separability is transitive.

PROPOSITION A.5.2. *Consider a tower of finite algebraic extensions $Q \subset K \subset L$, then L/Q is separable iff K/Q and L/K are.*

PROOF. We may assume that $\mathrm{Char}(Q) = p > 0$. Suppose L/Q separable, then K/Q is obviously separable and L/K is since for any $z \in L$, $P_{K,\min,z}$ divides $P_{Q,\min,z}$ which has only simple roots.

Conversely suppose K/Q and L/K separable. Let L^{sep} be the separable closure of L relative to Q. By assumption we have $K \subset L^{\mathrm{sep}}$. Since L/K is separable, by the previous discussion L/L^{sep} is separable.

We want to deduce that $L^{\mathrm{sep}} = L$. Given $z \in L$, its minimal polynomial is of the shape $R(X^q)$ for $q = p^k$, where k is a non-negative (possibly zero) integer and R is irreducible with simple roots

and coefficients in Q. Recall that $z \in L^{\text{sep}}$ if and only if $k = 0$ and therefore we will show $k = 1$ (respectively $k = 0$). Let $\rho_i,\ i = 1, \cdots, r$ be the simple roots of R in $\overline{Q}$. Let $\rho_i^{1/q} \in \overline{Q}$ be a root of the polynomial $X^q - \rho_i$; there is only one root in fact since

$$(X - \rho_i^{1/q})^q = X^q - \rho_i$$

and therefore

$$P_{Q,\min,z}(X) = R(X^q) = \prod_i (X^q - \rho_i) = \prod_i (X - \rho_i^{1/q})^q$$

Suppose $z = \rho_1^{1/q}$, then $z^q = \rho_1 \in L$ and ρ_1 is separable over Q since its minimal polynomial is R which has simple roots. Therefore $\rho_1 \in L^{\text{sep}}$. Now $P_{L^{\text{sep}},\min,z}$ divides $X^q - \rho_1$, which has only a single root of order q in $\overline{Q}$. Since L/L^{sep} is separable, we conclude that $q = 1$ and thus $L = L^{\text{sep}}$. □

A.5.5. A trace criterion for separability.

THEOREM A.6. *Let K/Q be a field extension of degree d. The extension is separable if and only if the trace bilinear form $\langle \cdot, \cdot \rangle_{K/Q}$ is non-degenerate.*

PROOF. If K/Q is separable, then there exists $z \in K$ such that

$$K = Q[z] = Q + Q.z + \cdots + Q.z^{d-1},\ d = [K : Q].$$

Choosing $\mathcal{B} = \{1, \cdots, z^{d-1}\}$ as a basis of K/Q, the discriminant formula gives

$$\text{disc}_{K/Q}(z) = \text{disc}_{K/Q}(1, \cdots, z^{d-1}) = \det\left((\sigma_k(z^{i-1})_{i,k\leqslant d}\right)^2 = \det(\left(\sigma_k(z)^{i-1}\right)_{i,k\leqslant d})^2$$

since the σ_k are algebra morphisms.

The determinant $\det\left((\sigma_k(z)^{i-1}\right)_{i,k\leqslant d})$ is a Vandermonde determinant and equals

$$\det\left((\sigma_k(z)^{i-1}\right)_{i,k\leqslant d}) = \prod_{j>i} (\sigma_j(z) - \sigma_i(z)).$$

Since z is a generator of K/Q we have

$$P_{K/Q,\text{car},z}(X) = P_{K/Q,\min,z}(X)$$

and the roots of the latter are the $\sigma_j(z),\ j \leqslant d$ which are all distinct (by definition of separability) so that

$$\text{disc}_{K/Q}(1, \cdots, z^{d-1}) = \det\left((\sigma_k(z)^{i-1}\right)_{i,k\leqslant d})^2 \neq 0.$$

For the converse we recall a few facts related to (in-)separability.

(1) Let $K/L/Q$ a tower of extensions. Then K/Q is separable if and only if K/L and L/Q are separable.
(2) Let K/Q be an extension, then
$$K^{\text{sep}} = \{z \in K,\ z \text{ is separable over } Q\}$$
is a subfield of K.
(3) If $K \neq K^{\text{sep}}$, then $\text{char}(Q) = p \neq 0$ and K/K^{sep} is purely inseparable, i.e. for all $z \in K$ there is some $n \in \mathbb{N}$ such that $z^{p^n} \in K^{\text{sep}}$.
(4) If K/Q is not separable, then there exists an intermediate field L such that $[K : L] = p$ and K is totally inseparable over L. More precisely, there is some $\ell \in L$ such that K is generated over L by a single root of the irreducible polynomial $X^p - \ell$.

So assuming that K/Q is inseparable, one first chooses an intermediate field $K/L/Q$ as in the last item above and proves that $\text{tr}_{K/L}$ vanishes on the basis $(1, z, \ldots, z^{p-1})$ of K over L by showing that the minimal polynomial of z^i over L is $X^p - t^i$. Then one uses that given any finite dimensional L-vector space V, letting V_Q denote V viewed as a Q-vector space, we have that

$$\text{tr}_{V_Q} = \text{tr}_{L/Q} \circ \text{tr}_V.$$

Applying this with $V = K$, it follows that for inseparable $K|Q$ the trace vanishes exactly. In particular, the trace bilinear form is not non-degenerate.

□

A.5.5.1. *The structure of separable algebra.* Let K/Q be a commutative finite dimensional Q algebra. We have the following

THEOREM A.7. *The algebra K/Q is separable iff either of the two equivalent conditions is satisfied*

- *The trace bilinear form $\langle \cdot, \cdot \rangle_{K/Q}$ is non-degenerate.*
- *The Q algebra K is isomorphic to a product of separable field extensions of Q.*

PROOF. (sketch) If K/Q is separable, then all the maps $[\times z]_{K/Q}$ are semisimple and commute. Therefore K decomposes as a direct sum

$$K \cong \bigoplus_i V_i$$

of finitely many Q-subspaces which are all invariant under $[\times z]_{K/Q}$. By finite dimensionality of K/Q we can assume that all the subspaces V_i are maximal with this property. One then shows that the subspaces V_i are subfields of K which are separable extensions of Q.

If K is a direct sum of separable field extensions of Q, then K/Q is clearly separable over Q.

The equivalence of the two conditions is left as an exercise. □

A.5.6. Embeddings.

DEFINITION A.19. *Let $Q \subset K \subset \overline{Q}$ be an extension of fields. A field K' containing Q and isomorphic to K as a Q-algebra is called a Q-conjugate of K in $\overline{Q}$.*

DEFINITION A.20. *A ring morphism $\sigma : K \to \overline{Q}$ is Q-linear if*

$$\forall \lambda \in Q,\ z \in K,\ \sigma(\lambda z) = \lambda \sigma(z).$$

The set of conjugates is parametrized by the following set

$$\mathrm{Hom}_Q(K, \overline{Q}) := \{\sigma : K \to \overline{Q}, \sigma \text{ a } Q\text{-linear ring morphism}\}$$
$$\subset \mathrm{Hom}(K, \overline{Q}) = \{\sigma : K \to \overline{Q} \text{ ring morphism}\}.$$

Observe that since K is a field, and non-zero ring homomorphism $\sigma : K \to \overline{Q}$ is injective and its image $\sigma(K) \subset \overline{Q}$ is a field isomorphic to K. Therefore $\mathrm{Hom}(K, \overline{Q})$ is also called the set of embeddings of K into $\overline{Q}$ and the subset $\mathrm{Hom}_Q(K, \overline{Q})$ is the set of Q-linear embeddings or Q-*embeddings*.

Observe that if σ is a Q-linear embedding, then $\sigma_{|Q} = \mathrm{Id}_Q$ so that $\sigma(K)$ is a field containing Q and isomorphic to K as a Q-algebra. There is therefore a bijection between the set of Q-conjugates of K and the set of Q-linear embedding given by

$$\sigma \mapsto K' = \sigma(K).$$

We have the following proposition.

PROPOSITION A.5.3. *The set of Q-conjugates of K in $\overline{Q}$ is finite; equivalently, the set of Q-linear embeddings $\mathrm{Hom}_Q(K, \overline{Q})$ is finite. More precisely*

$$|\mathrm{Hom}_Q(K, \overline{Q})| \leqslant [K : Q].$$

PROOF. Assume first that K is monogenic, i.e., there is $z \in K$ such that $K = Q[z]$. For any given $\sigma \in \mathrm{Hom}_Q(K, \overline{Q})$, the conjugate $\sigma(z)$ is a root of the minimal polynomial $P_{\min,z,K/Q}$ and hence takes one out of at most $[K : Q]$ values. For general $x \in K$ we have $x = P(z)$ for some $P \in Q[X]$ and (by Q-linaearity)

$$\sigma(x) = \sigma(P(z)) = P(\sigma(z))$$

so σ is completely determined by $\sigma(z)$. This prove the theorem in the monogenic case.

We handle the general case by recurrence on the degree. Given $z \in K - Q$ and $L = Q[z]$ the field generated by z. We may assume $L \neq K$ and we already know that $|\operatorname{Hom}_Q(L, \overline{Q})| \leqslant [L : Q]$. Given $\sigma \in \operatorname{Hom}_Q(K, \overline{Q})$, by recurrence its restriction to L can take at most $[L : Q]$ values. Let us consider the set

$$\{\tau \in \operatorname{Hom}_Q(K, \overline{Q}) \colon \tau_{|L} = \sigma_{|L}\}$$

of Q-linear embeddings whose restriction to L equals $\sigma_{|L}$. It will be sufficient to show that this set is of size at most $[K : L]$: given τ, τ' in that set and let $L' = \sigma(L) = \tau(L) = \tau'(L)$, then L' is contained in $\tau(K), \tau'(K)$ and $\sigma(K)$. Consider

$$\Psi = \tau' \circ \tau^{-1} : \tau(K) \to \tau'(K)$$

then Ψ is L'-linear so can take at most $[\tau(K) : L']$ by recurrence (since $[\tau(K) : L'] = [\tau(K) : \tau(L)] = [K : L] < [K : Q]$) □

During the proof we have also established

LEMMA A.5.4. *Given $Q \subset L \subset K$ a tower of finite extensions and $\sigma \in \operatorname{Hom}_Q(L, \overline{Q})$, the set of embeddings extending σ,*

$$\{\tau \in \operatorname{Hom}_Q(K, \overline{Q}) \colon \tau_{|L} = \sigma\},$$

is of size at most $[K : L]$.

LEMMA A.5.5 (Dedekind). *Let L be any field containing $\overline{Q}$ as a subfield.I needed linear independence over $\mathbb{C}$, so I generalized it a bit. The Q-linear embeddings*

$$\sigma_i,\ i = 1, \cdots d = |\operatorname{Hom}_Q(K, \overline{Q})|$$

are L-linearly independent.

PROOF. Suppose that

$$\sum_{i=1}^{d} \lambda_i \sigma_i = 0$$

for $\lambda_i \in L$ not all zero. We assume that the number d' of i such that $\lambda_i \neq 0$ is minimal amongst all non-trivial linear dependence relations. Necessarily $d' \geqslant 2$ (because $\sigma_1(1) = 1$).

Up to permuting the indices we may assume that this relation is of the shape

$$\sum_{i=1}^{d'} \lambda_i \sigma_i = 0$$

for some $2 \leqslant d' \leqslant d$ and with $\lambda_i \neq 0$ and that d' is minimal. We have for every $z, z' \in K$

$$\sum_{i=1}^{d'} \lambda_i \sigma_i(zz') = 0$$

and therefore since $\sigma_i(z.z') = \sigma_i(z).\sigma_i(z')$ for every $z' \in K$ we have

$$\sum_{i=1}^{d'} \lambda_i \sigma_i(z') \sigma_i = 0.$$

Choose $j \in [1, \cdots, d']$ and combine two such relations (for z' and for $z' = 1$) we have

$$0 = \sum_{i=1}^{d'} \lambda_i \sigma_i(z') \sigma_i - \sigma_j(z') \sum_{i=1}^{d'} \lambda_i \sigma_i = \sum_{i=1}^{d'} \lambda_i (\sigma_i(z') - \sigma_j(z')) \sigma_i = \sum_{\substack{i=1 \\ i \neq j}}^{d'} \lambda_i (\sigma_i(z') - \sigma_j(z')) \sigma_i.$$

This is a linear relation amongst the σ_i with $\leqslant d' - 1$ terms; moreover since for $i \neq j$ $\sigma_i \neq \sigma_j$ one can find z' such that the $\sigma_i(z') - \sigma_j(z')$, $i \neq j$ are not all zero and the relation is non trivial contradicting the minimality of d'.

□

A.5.6.1. *Conjugates.*

DEFINITION A.21. *For any $z \in K$ the set of (distincts) roots of $P_{Q,\min,z}$,*

$$\{z' \in \overline{Q} \colon P_{Q,\min,z}(z') = 0\}$$

is called the set of conjugates of z in $\overline{Q}$.

This terminology is justified by the following fact

PROPOSITION A.5.6. *The set of conjugates of z in $\overline{Q}$ is the set*

$$\{\sigma(z) \colon \sigma \in \mathrm{Hom}_Q(K, \overline{Q})\}$$

of images of z under the various Q-linear embeddings.

PROOF. Since $P_{Q,\min,z}$ has coefficients in Q, and σ is a Q-linear ring morphism, we have

$$0 = \sigma(P_{Q,\min,z}(z)) = P_{Q,\min,z}(\sigma(z)),$$

so we have one inclusion. The converse inclusion follows from the following extension lemma applied to $L = Q[z]$. □

LEMMA A.5.7. *Given $Q \subset L \subset K$ a tower of finite dimensional field extensions. For any $\sigma \in \mathrm{Hom}_Q(L, \overline{Q})$ there exists $\tau \in \mathrm{Hom}_Q(K, \overline{Q})$ such that*

$$\tau_{|K} = \sigma.$$

We will prove the

THEOREM A.8. *A finite field extension K/Q is separable if and only if*

$$|\mathrm{Hom}_Q(K, \overline{Q})| = [K : Q].$$

PROOF. Suppose K/Q is separable and let z be a primitive element of K,

$$P_{Q,\min,z} = P_{K/Q,\mathrm{car},z}$$

has degree $[K : Q]$. By separability, $P_{Q,\min,z}$ has $[K : Q]$ distinct roots which is the cardinality of $\mathrm{Hom}_Q(K, \overline{Q})$.

Suppose K/Q is not separable and let $z \in K$ be a non separable element. Let $L = K[z]$. Its minimal polynomial has degree $[L : Q]$ and is of the shape

$$P_{Q,\min,z}(X) = R(X^q),$$

where R has $r < [L : Q]$ distinct roots $\mu_i,\ i = 1 \ldots, \mu_r$ and

$$P_{Q,\min,z}(X) = \prod_i (X - \mu_i^{1/q})^q.$$

Therefore $|\mathrm{Hom}_Q(L, \overline{Q})| = r$ and by Lemma A.5.4,

$$|\mathrm{Hom}_Q(K, \overline{Q})| \leqslant r.[K : L] < [K : Q].$$

□

A.5.6.2. *Relation to the eigenvalues.* We have seen that if K/Q is separable we have a map of Q-algebras

$$\sigma \colon K \mapsto \sigma(z) = \mathrm{diag}(\sigma_1(z), \cdots, \sigma_d(z)) \in \mathrm{diag}_d(\overline{Q}).$$

Consequently for each i the i-th eigenvalue

$$\sigma_i \colon z \in K \mapsto \sigma_i(z) \in \overline{Q}$$

is a Q-linear embedding. Moreover the various embeddings $\sigma_i,\ i = 1, \cdots d$ are distinct since, if z is a generator of K/Q, the $\sigma_i(z), i = 1, \cdots, d$ are the distinct d roots of the minimal polynomial $P_{Q,\min,z}$. We have therefore

$$\mathrm{Hom}_Q(K, \overline{Q}) = \{\sigma_i \colon i = 1, \cdots d\}.$$

In particular we have

$$\forall z \in K,\ P_{K/Q,\mathrm{car},z}(X) = \prod_{\sigma \in \mathrm{Hom}_Q(K,\overline{Q})} (X - \sigma(z))$$

$$\mathrm{tr}_{K/Q}(z) = \sum_{\sigma \in \mathrm{Hom}_Q(K,\overline{Q})} \sigma(z),\ \mathrm{Nr}_{K/Q}(z) = \prod_{\sigma \in \mathrm{Hom}_Q(K,\overline{Q})} \sigma(z).$$

A.6. Galois Theory

Let K/Q be a finite separable field extension and consider the subset of K-valued embeddings

$$\mathrm{Hom}_Q(K,K) \subset \mathrm{Hom}_Q(K,\overline{Q}).$$

This is the group of Q-automorphisms of the field K: indeed $\sigma \in \mathrm{Hom}_Q(K,K)$ is K-linear injective, hence surjective .

Definition A.22. *The extension K/Q is normal if and only if*

$$\mathrm{Hom}_Q(K,K) = \mathrm{Hom}_Q(K,\overline{Q}).$$

An extension K/Q is Galois if K/Q is normal and separable:

$$|\mathrm{Hom}_Q(K,K)| = |\mathrm{Hom}_Q(K,\overline{Q})| = [K:Q].$$

The group $\mathrm{Hom}_Q(K,K)$ is called the Galois group of K/Q:

$$\mathrm{Gal}(K/Q) = \mathrm{Hom}_Q(K,K).$$

Exercise A.2. Show that a finite extension K/Q is Galois if and only if for all $z \in K$ the map $[\times z]_{K/Q}$ is diagonalizable over K.

Example A.2.
- Any extension K/Q of degree 2 is Galois.
- Any finite extension K/Q of a finite field Q is Galois: we have

$$\mathrm{Gal}(K/Q) = \mathrm{frob}_q^{\mathbb{Z}}$$

where frob_q is the Frobenius ($q = |Q|$)

$$\mathrm{frob}_q : \begin{array}{ccc} K & \mapsto & K \\ x & \mapsto & x^q. \end{array}$$

Theorem A.9 (Main Theorem of Galois Theory). *Let K/Q be a Galois extension and*

$$G = \mathrm{Gal}(K/Q) = \mathrm{Hom}_Q(K,K)$$

be the Galois group.

The map

$$K^\bullet : H \subset G \mapsto K^H = \{x \in K,\ \forall \sigma \in H,\ \sigma(x) = x\} \subset K$$

is a bijection between

- *the set of subgroups of G and*
- *the set of extensions of Q contained in K.*

Moreover K/K^H is Galois and

$$\mathrm{Gal}(K/K^H) = H.$$

Conversely, for any subextension $Q \subset K' \subset K$, the extension K/K' is Galois. The inverse of the map $K^\bullet$ is

$$\mathrm{Gal}(K/\bullet) :\ K' \mapsto \mathrm{Gal}(K/K') = \mathrm{Hom}_{K'}(K,K) \subset G.$$

The map $K^\bullet$ also induces (by restriction) a bijection between

- *the set of normal subgroups of G and*
- *the set of Galois extensions of Q contained in K (the $Q \subset K' \subset K$ such that K'/Q is Galois).*

In addition, for any such $H \triangleleft G$ we have

$$\mathrm{Gal}(K^H/Q) \simeq G/H.$$

PROOF. Given H a subgroup of G, since any $\sigma \in H$ is Q-linear, Q is in the set of fixed points of σ so $Q \subset K^H$. Moreover since σ is a field morphism, the set of fixed point of σ is stable under addition, product, and inversion. So the set of fixed points of σ is a subfield of K containing Q and so is K^H which is the intersection of the fixed points of σ over all $\sigma \in H$. The extension K/K^H is separable since K/Q is separable and it is normal since

$$\mathrm{Hom}_{K^H}(K, \overline{Q}) \subset \mathrm{Hom}_Q(K, \overline{Q}) = \mathrm{Hom}_Q(K, K)$$

(because K/Q is normal) so any K^H-linear morphism of K into $\overline{Q}$ maps K to K.

To show that this map is bijective it suffices to show that for any $H \subset G$

$$\mathrm{Gal}(K/K^H) = H \tag{A.6}$$

and that for any $Q \subset K' \subset K$, K/K' is Galois and

$$K^{\mathrm{Gal}(K/K')} = K'. \tag{A.7}$$

Indeed this will prove that the maps

$$H \mapsto K^H \text{ and } K' \mapsto \mathrm{Gal}(K/K')$$

are inverse to one another so that both sets are in bijection.

We start with (A.6). Any $\sigma \in H$ is by definition K^H-linear so $H \subset \mathrm{Gal}(K/K^H)$. We have therefore

$$|H| \leqslant |\mathrm{Gal}(K/K^H)| = [K : K^H].$$

We will prove that this is an equality which will imply (A.6).

Assume that $|H| < [K : K^H]$: there exists $x_1, \cdots, x_{|H|+1} \in K$ which are K^H-linearly independent (in particular distinct).

For $m \leqslant |H| + 1$ we consider the homogenous linear system with $|H|$ equations in m variables $(Y_1, \cdots, Y_m)$

$$\left\{ \sum_{i=1}^{m} \sigma(x_i) Y_i = 0, \ \sigma \in H \right. \tag{A.8}$$

When $m = |H| + 1$ this system has more variables than equations so admits a non-trivial solution $(y_1, \cdots, y_m) \in K^m$; let m be minimal with this property.

By minimality wlogwma $y_m = 1$. The system becomes

$$\forall \sigma \in H, \sigma(x_m) = -\sum_{i=1}^{m-1} \sigma(x_i) y_i.$$

applying $\tau \in H$ to this identity we obtain

$$\forall \tau, \sigma \in H, \ \tau(\sigma(x_m)) = -\sum_{i=1}^{m-1} \tau(\sigma(x_i)) \tau(y_i).$$

Changing variables

$$\forall \tau, \sigma \in H, \ \sigma(x_m) = -\sum_{i=1}^{m-1} \sigma(x_i) \tau(y_i),$$

and subtracting

$$\forall \tau, \sigma \in H, \ 0 = \sum_{i=1}^{m-1} \sigma(x_i)(y_i - \tau(y_i)).$$

but now

$$(\cdots, y_i - \tau(y_i), \cdots) \in K^{m-1}$$

is a solution to (A.8) in $m-1$ variables. Since m is minimal the solution must be the trivial one:

$$\forall i \leqslant m-1, \forall \tau \in H,\ y_i - \tau(y_i) = 0$$

and $y_i \in K^H$. Taking $\sigma = \mathrm{Id}_K$ we get

$$\sum_{i=1}^{m} x_i y_i = 0,$$

contradicting (remember that $m \leqslant |H|+1$) the fact that the $\{x_i\}$ are K^H-lineary independent (since $y_m = 1$ the linear relation is non-trivial). Therefore $[K : K^H] \leqslant |H|$ so $|\operatorname{Gal}(K/K^H)| = [K : K^H] = |H|$ and

$$\operatorname{Gal}(K/K^H) = H.$$

Let us prove (A.7): consider $Q \subset K' \subset K$. Repeating the beginning of the previous argument the extension K/K' is Galois. By definition we have $K' \subset K^{\operatorname{Gal}(K/K')}$ and by the previous argument applied to $H = \operatorname{Gal}(K/K')$ we have

$$[K : K'] = |\operatorname{Gal}(K/K')| = [K : K^{\operatorname{Gal}(K/K')}],$$

which by multiplicativity of the degree implies (A.7).

Let us restrict the above map to extensions $Q \subset K' \subset K$ such that K'/Q is Galois. Let $H = \operatorname{Gal}(K/K')$. By the preceding discussion, the group H is the pointwise stabilizer of K' in K and therefore for any $\sigma \in \operatorname{Gal}(K/Q)$, $\sigma.H.\sigma^{-1}$ is the stabilizer of $\sigma(K')$. But $\sigma(K') = K'$ since K'/Q is normal, so $\sigma.H.\sigma^{-1} = H$ and therefore H is a normal subgroup of G. We have

$$|\operatorname{Gal}(K'/Q)| = [K' : Q] = [K : Q]/[K : K'] = |G|/|H| = |\operatorname{Gal}(K/Q)/H|,$$

so it is sufficient to construct an injective map

$$\operatorname{Gal}(K/Q)/H \hookrightarrow \operatorname{Gal}(K'/Q).$$

Consider the restriction map

$$\mathrm{res}_{K'} : \sigma \in \operatorname{Gal}(K/Q) \mapsto \sigma_{|K'} \in \operatorname{Gal}(K'/Q).$$

This is a group homomorphism and the kernel of that map is precisely the pointwise stabilizer of K' which is H and we obtain the required injection. □

References

[1] P. Samuel, *Algebraic Theory of Numbers*, translated by Allan J. Silberger, Houghton Mifflin Co., Boston, Mass., 1970.