

# 1 Small prefix

Recall:

- $L$  numberfield :  $\iff L$  is a finite extension of  $\mathbb{Q}$   
In particular:  $L/\mathbb{Q}$  is separable  $\Rightarrow L/\mathbb{Q}$  is primitive, i.e.  $L = \mathbb{Q}(\alpha), \mathbb{Q}[X] \ni f_\alpha =$  minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  and  $[L : \mathbb{Q}] = \deg(f_\alpha)$ .
- $\mathcal{O} := \{\alpha \in L \mid f_\alpha \in \mathbb{Z}[X]\}$  is called *ring of integers* (generalization of  $\mathbb{Z} \subseteq \mathbb{Q}$ ).  
 $\mathcal{O}$  is an integral domain.
- Goal: study the ring  $\mathcal{O}$
- Questions:
  1. What is  $\mathcal{O}^\times$ ? What is its structure?
  2. What are the prime ideals of  $\mathcal{O}$ ?
  3. Do we have a unique prime factorization, i.e. is  $\mathcal{O}$  a UFD?

## 1.1 Motivation

*Problem 1.1.1* (Fermat's conjecture,  $\sim 1640$ ). Show that the equation  $x^n + y^n = z^n$  has no nontrivial integer solutions, i.e. solutions  $(x, y, z)$  with  $x, y, z \in \mathbb{Z} \setminus \{0\}$  for  $n \geq 3$ .

History:

- 1770: Euler found solution for  $n = 3$
- 1825: Dirichlet and Legendre using Germain
- Kummer showed it for many primes, he showed as well that his idea doesn't work for all  $n \in \mathbb{N}_{>2}$
- Conjecture was proved by Wiles in 1997

*Remark 1.1.2.* i) If Fermat's is true for  $n$ , then also for  $nk$  for all  $k \in \mathbb{N}$ .

ii) It is sufficient to prove Fermat's conjecture for  $n = 4$  and all odd primes.

*Proof.* i) Suppose  $(x, y, z)$  is a nontrivial solution of  $x^{nk} + y^{nk} = z^{nk} \Rightarrow (x^k, y^k, z^k)$  is a nontrivial solution to  $x^n + y^n = z^n$ .

ii) Follows from i).

□

**Proposition 1.1.3** ( $n = 2$ ). Suppose  $x, y, z \in \mathbb{Z}$ ,  $\gcd(x, y, z) = 1$

- i)  $x, y, z$  are pairwise coprime if  $x^2 + y^2 = z^2$
- ii)  $x^2 + y^2 = z^2 \Rightarrow$  either  $x$  or  $y$  is even
- iii)  $x^2 + y^2 = z^2 \iff \exists r, s \in \mathbb{N}_0, \gcd(r, s) = 1$  s.t.  $x = \pm 2rs, y = \pm(r^2 - s^2), z = \pm(r^2 + s^2)$ .

*Proof.* i) clear  $\checkmark$

ii) One of  $x, y, z$  has to be even, since  $odd + odd \neq odd$ . Suppose  $z$  is even. Then look at equation mod 4, this gives a contradiction. By i) only one of  $x$  and  $y$  is even.

iii) „ $\Leftarrow$ “: calculation

„ $\Rightarrow$ “: Wlog. assume  $x, y, z \in \mathbb{N}_0$ ,  $x$  even,  $y, z$  odd:

$$\begin{aligned} \Rightarrow x = 2u, z + y = 2v, z - y = 2w, \gcd(w, v) = 1 (y, z \text{ are coprime}), x^2 + y^2 = z^2 \\ \Rightarrow 4u^2 = x^2 = z^2 - y^2 = (z - y)(z + y) = 4wv \Rightarrow u^2 = vw \\ \xRightarrow{\gcd(v, w)=1} v = r^2, w = s^2 \Rightarrow z = v + w = r^2 + s^2, y = v - w = r^2 - s^2 \\ \text{and } x = 2u = 2\sqrt{vw} = 2rs \end{aligned}$$

□

*Remark.*  $(x, y, z) \in \mathbb{Z}^3$  with  $x^2 + y^2 = z^2$  are called *pythagorean triples*.

**Proposition 1.1.4** ( $n = 4$ ). The equation  $x^4 + y^4 = z^2$  (and  $x^4 + y^4 = z^4$ ) have no nontrivial integer solutions.

*Proof.* Suppose  $x, y, z \in \mathbb{Z}$  with  $x^4 + y^4 = z^2, xyz \neq 0$ . Wlog  $x, y, z > 0, x, y, z$  coprime,  $x = 2\tilde{x}$  for some  $\tilde{x} \in \mathbb{N}$ . Choose  $z$  minimal with this conditions.

$$\begin{aligned} \text{Prop. 1.2} \Rightarrow \exists r, s \in \mathbb{N} \text{ s.t. } x^2 = 2rs, y^2 = r^2 - s^2, z = r^2 + s^2 \text{ and } \gcd(r, s) = 1 \\ \Rightarrow y^2 + s^2 = r^2 \text{ with } y, s, r \text{ coprime.} \end{aligned}$$

$$\text{Prop. 1.2} \Rightarrow \exists a, b \in \mathbb{N} \text{ s.t. } s = 2ab, y = a^2 - b^2, r = a^2 + b^2 \text{ and } \gcd(a, b) = 1.$$

$$\text{plug in} \Rightarrow x^2 = 4ab(a^2 + b^2)$$

$$\Rightarrow \tilde{x}^2 = ab(a^2 + b^2) \text{ and } a, b, a^2 + b^2 \text{ pairwise coprime}$$

As in proof of Prop. 1.2 (they are coprime but a square number)

$$\begin{aligned} \Rightarrow \exists c, d, e \in \mathbb{N} \text{ s.t. } a = c^2, b = d^2, a^2 + b^2 = e^2 \\ \Rightarrow c^4 + d^4 = a^2 + b^2 = e^2 \text{ and } e \leq a^2 + b^2 = r < z \end{aligned}$$

!since  $z$  was chosen to be minimal.

□

From now on:  $n = p$  odd prime.

*Idea 1.1.5* (by Germain). Distinguish 2 cases in Fermat's problem:

1. „First case“:  $x, y, z$  with  $p$  does not divide  $xyz$ .
2. „Second case“: exactly one of  $x, y, z$  is divided by  $p$ .

Some approach:

- Use primitive  $p$ -th root of unity  $\zeta = \zeta_p$ .
- Reminder:  $X^p - 1 = (X - 1)(X - \zeta) \dots (X - \zeta^{p-1})$
- Setting  $\tilde{y} = -y$  we get:

$$\begin{aligned}
 x^p + y^p &= x^p - \tilde{y}^p = \tilde{y}^p \left( \left( \frac{x}{\tilde{y}} \right)^p - 1 \right) \\
 &= \tilde{y}^p \left( \frac{x}{\tilde{y}} - 1 \right) \left( \frac{x}{\tilde{y}} - \zeta \right) \dots \left( \frac{x}{\tilde{y}} - \zeta^{p-1} \right) \\
 &= (x - \tilde{y})(x - \tilde{y}\zeta) \dots (x - \tilde{y}\zeta^{p-1}) \\
 &= (x + y)(x + y\zeta) \dots (x + y\zeta^{p-1})
 \end{aligned}$$

**Lemma 1.1.6.** For  $x, y, z \in \mathbb{Z}$  we have  $x^p + y^p = z^p \iff (x + y)(x + y\zeta) \dots (x + y\zeta^{p-1}) = z^p$

Idea: Look at prime divisors in  $\mathbb{Z}[\zeta]$ .

Problem: Would be good to have unique prime factorization. This will not be true in general.

## 1.2 The ring $\mathbb{Z}[\zeta]$

Suppose  $\zeta$  is a primitive  $n$ -th root of unity

*Reminder 1.2.1.* i)  $\mathbb{Q}(\zeta)/\mathbb{Q}$  is algebraic extension of degree  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$

ii)  $\mathbb{Q}(\zeta)/\mathbb{Q}$  is a Galois extension. In particular:

$$\text{Hom}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_i \text{ with } \sigma_i(\zeta) = \zeta^i \mid i \in (\mathbb{Z}/n\mathbb{Z})^\times\} \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

iii) Consider the norm map  $\mathcal{N} : \mathbb{Q}(\zeta) \rightarrow \mathbb{Q}$ ,  $\alpha \mapsto \det(\gamma \mapsto \alpha\gamma)$ . We have for  $\alpha = r(\zeta)$  ( $r \in \mathbb{Q}[X]$  polynomial) with min. polynomial  $f_\alpha = X^k + c_{k-1}X^{k-1} + \dots + c_0$ :

- If we have  $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$ , then  $\mathcal{N}(\alpha) = (-1)^{\varphi(n)} c_0$
- $\mathcal{N}(\alpha) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \sigma(\alpha) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} r(\zeta^i)$
- $\alpha \in \mathbb{Q} \Rightarrow \mathcal{N}(\alpha) = \alpha^{\varphi(n)}$

iv)  $X^{n-1} + X^{n-2} + \dots + 1 = \frac{X^n - 1}{X - 1} = (X - \zeta)(X - \zeta^2) \dots (X - \zeta^{n-1})$   
 $\xrightarrow{X=1} n = (1 - \zeta)(1 - \zeta^2) \dots (1 - \zeta^{n-1})$

*Reminder 1.2.2 (and preview).* i)  $\mathcal{O} := \mathbb{Z}[\zeta] := \{r(\zeta) \mid r \in \mathbb{Z}[X]\}$

ii)  $\mathbb{Z}[\zeta] = \{\alpha \in \mathbb{Q}(\zeta) \mid f_\alpha \in \mathbb{Z}[X]\}$  (proof later)

iii)  $\mathbb{Z}[\zeta]$  is a free  $\mathbb{Z}$ -module with basis  $\{1, \zeta, \dots, \zeta^{d-1}\}$  with  $d = \varphi(n)$  (proof later)

iv)  $\alpha \in \mathbb{Z}[\zeta] \Rightarrow \mathcal{N}(\alpha) \in \mathbb{Z}$  (proof later)

v)  $\{\alpha \in \mathcal{O} \mid |\alpha| = 1\}$  is finite (proof later)

*Reminder 1.2.3.* Suppose  $R$  is an integral domain:

i)  $\alpha \in R$  is *irreducible* :  $\iff$  If  $\alpha = \alpha_1 \alpha_2$  with  $\alpha_i \in R$ , then  $\alpha_1 \in R^\times$  or  $\alpha_2 \in R^\times$

ii)  $\alpha, \alpha' \in R$  are *associated to each other* :  $\iff \exists \varepsilon \in R^\times : \alpha = \varepsilon \alpha'$

iii)  $R$  is called *factorial* :  $\iff$  each  $\alpha \in R, \alpha \neq 0$  can be written in a unique way as  $\alpha = \varepsilon \pi_1 \cdot \dots \cdot \pi_r$  with  $\pi_i$  irreducible up to multiplication with  $\varepsilon \in R^\times$

iv)  $\alpha_1, \alpha_2 \in R$  are called *coprime* :  $\iff$  If  $\alpha' \in R$  with  $\exists \beta_1, \beta_2 \in R : \alpha_1 = \alpha' \beta_1, \alpha_2 = \alpha' \beta_2$  then  $\alpha' \in R^\times$ .

*Remark* (and correction). 1. Recall:  $L/\mathbb{Q}$  field extensions:

$$\mathcal{O} := \{\alpha \in L \mid f_\alpha \in \mathbb{Z}[X]\}$$

!! Here:  $f_\alpha$  is by definition monic, i.e. leading coefficient is 1.

Remark:  $\mathcal{O} = \{\alpha \in L \mid \exists f \in \mathbb{Z}[X] \text{ with } f \text{ monic and } f(\alpha) = 0\}$

„ $\subseteq$ “: clear

„ $\supseteq$ “: Lemma of Gauss

2. Recall: Definition of field norm for  $L/K$  finite field extension How is norm defined?

$\mathcal{N} : L \rightarrow K$  defined as follows:

Suppose  $\alpha \in L \Rightarrow \varphi_\alpha : \beta \mapsto \alpha\beta$  is linear map over  $K$ . Then:

$$\mathcal{N}_{L/K}(\alpha) := \det(\phi_\alpha)$$

Properties:

a) If  $L = K(\alpha)$  and  $X^n + c_{n-1}X^{n-1} + \dots + c_0$  is a minimal polynomial of  $\alpha$  over  $K$ , then  $\mathcal{N}_{L/K}(\alpha) = (-1)^n c_0$ .

b)  $\mathcal{N}_{L/K}(\alpha) = (\prod_{i=1}^r \sigma_i(\alpha))^q$  with  $\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_r\}$  and  $q = \text{inseparable degree, i.e. } [L : K] = [L : K]_s \cdot q$ .

c)  $\alpha \in K \Rightarrow \mathcal{N}_{L/K}(\alpha) = \alpha^d$  with  $d = [L : K]$  (see Bosch „Algebra“ 4.7).

General reference: NEUKIRCH

This chapter: BOREVICH + SHAFEREVICH Chapter 3.1.

Recall: Goal: prove for  $p$  prime and odd

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

has no non-trivial solutions. Last time:

$$x^p + y^p = z^p = (x + y)(x + y\zeta)(x + y\zeta^2) \dots (x + y\zeta^{p-1}) \in \mathbb{Z}[\zeta]$$

From now on:  $p$  odd prime,  $\zeta = e^{\frac{2\pi i}{p}}$  primitive  $p$ -th root of unity  $\mathcal{O} = \mathbb{Z}[\zeta]$ .

**Proposition 1.2.4.** *For the group of units  $\mathcal{O}^\times$  of  $\mathcal{O} = \mathbb{Z}[\zeta]$  we have:*

$$\mathcal{O}^\times = \{\alpha \in \mathcal{O} \mid \mathcal{N}(\alpha) = \pm 1\}$$

*Notation:*  $\mathcal{N} = \mathcal{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$  in this chapter.

*Proof.* „ $\subseteq$ “: “ $\alpha \in \mathcal{O}^\times \Rightarrow \exists \beta \in \mathcal{O}$  with  $\alpha\beta = 1 \Rightarrow 1 = \mathcal{N}(\alpha\beta) \stackrel{!}{=} \underbrace{\mathcal{N}(\alpha)}_{\in \mathbb{Z}} \underbrace{\mathcal{N}(\beta)}_{\in \mathbb{Z} \text{ by 2.2 v}} \Rightarrow \text{claim}$ “

„ $\supseteq$ “: Suppose  $\alpha \in \mathcal{O}$  with  $\mathcal{N}(\alpha) = \pm 1$ .

$$\Rightarrow \pm 1 = \mathcal{N}(\alpha) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \sigma(\alpha)$$

Note:  $\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2} \in \mathbb{Z}[\zeta]$

$$\Rightarrow \sigma(\alpha) = a_0 + a_1\zeta^i + \dots + a_{p-2}\zeta^{i(p-2)} \text{ for some } i \in \{1, \dots, p-1\} \Rightarrow \sigma(\alpha) \in \mathbb{Z}[\zeta]$$

$$\Rightarrow \alpha \text{ is a divisor of 1 in } \mathbb{Z}[\zeta] \Rightarrow \alpha \in \mathcal{O}^\times. \quad \square$$

**Lemma 1.2.5.** i)  $\mathcal{N}(1 - \zeta^s) = p$  for  $s \in \mathbb{Z}$  with  $s \not\equiv 0 \pmod{p}$

ii)  $1 - \zeta$  is irreducible in  $\mathcal{O} = \mathbb{Z}[\zeta]$ .

iii)  $p = \varepsilon \cdot (1 - \zeta)^{p-1}$  with some  $\varepsilon \in \mathcal{O}^\times$ .

*Proof.* i) 2.1. iv)  $\Rightarrow p = (1 - \zeta)(1 - \zeta^2) \dots (1 - \zeta^{p-1})$

$$2.1. \text{ iii) } \Rightarrow \mathcal{N}(1 - \zeta^s) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \sigma(1 - \zeta^s) = \prod_{i=1}^{p-1} (1 - \zeta^{si}) = \prod_{j=1}^{p-1} (1 - \zeta^j) = p$$

ii) We obtain from i) that  $1 - \zeta \notin \mathcal{O}^\times$ . Suppose  $1 - \zeta = \alpha\beta$  with  $\alpha, \beta \in \mathcal{O}$

$$\Rightarrow p = \mathcal{N}(1 - \zeta) = \mathcal{N}(\alpha)\mathcal{N}(\beta) \Rightarrow \mathcal{N}(\alpha) = \pm 1 \text{ or } \mathcal{N}(\beta) = \pm 1 \xrightarrow{\text{Prop 2.4}} \alpha \in \mathcal{O}^\times \text{ or } \beta \in \mathcal{O}^\times.$$

iii) Use:  $1 - \zeta^s = (1 - \zeta) \underbrace{(1 + \zeta + \zeta^2 + \dots + \zeta^{s-1})}_{\varepsilon_s} = (1 - \zeta)\varepsilon_s$

$$\Rightarrow p = \mathcal{N}(1 - \zeta^s) = \underbrace{\mathcal{N}(1 - \zeta)}_{=p} \cdot \mathcal{N}(\varepsilon_s) \Rightarrow \mathcal{N}(\varepsilon_s) = 1 \Rightarrow \varepsilon_s \in \mathcal{O}^\times$$

$$\text{Hence } p = \prod_{s=1}^{p-1} (1 - \zeta^s) = \prod_{s=1}^{p-1} \underbrace{\varepsilon_s}_{\in \mathcal{O}^\times} (1 - \zeta) = (1 - \zeta)^{p-1} \underbrace{\prod_{s=1}^{p-1} \varepsilon_s}_{\in \mathcal{O}^\times}$$

□

Notation:  $\varepsilon_s = 1 + \zeta + \dots + \zeta^s$ .

**Lemma 1.2.6.** i)  $a \in \mathbb{Z}$  with  $1 - \zeta$  divides  $a$  in  $\mathcal{O} \Rightarrow p$  divides  $a$ .

ii) An  $n$ -th root of unity lies in  $\mathbb{Q}(\zeta) \iff n$  divides  $2p$ .

*Proof.* i)  $a = (1 - \zeta)\beta$  with  $\beta \in \mathcal{O} \Rightarrow a^{p-1} = \mathcal{N}(a) = p\mathcal{N}(\beta) \xrightarrow{(\mathcal{N}(\beta) \in \mathbb{Z})} p$  divides  $a$ .

ii) „ $\Leftarrow$ “:  $-1 \in \mathbb{Q}(\zeta)$  and thus  $e^{\frac{2\pi i}{2p}} \in \mathbb{Q}(\zeta)$

„ $\Rightarrow$ “: Consider  $H := \{\omega \in \mathbb{Q}(\zeta) \mid \omega \text{ is a root of unity}\}$

- a)  $H \subseteq \mathbb{Z}[\zeta]$ : Suppose  $\omega \in H \Rightarrow \omega^n - 1 = 0$  for some  $n \in \mathbb{N} \Rightarrow f_\omega$  is a divisor of  $X^n - 1 \Rightarrow f_\omega \in \mathbb{Z}[X] \xrightarrow{2.2ii)} \omega \in \mathbb{Z}[\zeta]$ .
- b)  $\tilde{\omega}$  some conjugate of  $\omega \Rightarrow \tilde{\omega}$  is a root of  $X^n - 1 \Rightarrow |\tilde{\omega}| = 1 \xrightarrow{2.2v)} H$  is finite  $\Rightarrow H$  is a cyclic subgroup of  $\mathbb{Q}(\zeta)^\times$ .  
 Choose some generator  $\omega_0$  of  $H$  and denote  $m := \text{ord}(\omega_0)$ . Since  $\zeta \in H$  and  $\text{ord}(\zeta) = p \Rightarrow p$  divides  $m$ . Decompose  $m = p^s \cdot m'$  with  $s \geq 1$  and  $\gcd(m', p) = 1$ . Consider the field extensions chain:

$$\mathbb{Q} \subseteq \mathbb{Q}(\omega_0) \subseteq \mathbb{Q}(\zeta)$$

with degrees  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1 = \varphi(p)$  and  $[\mathbb{Q}(\omega_0) : \mathbb{Q}] = \varphi(m) = p^{s-1}(p-1)\varphi(m') \leq p-1 \Rightarrow s = 1$  and  $\varphi(m') = 1$  and thus  $m' = 1, 2 \Rightarrow \text{ord}(\omega_0) \leq 2p$ . □

### Notation 1.2.7.

1.  $L/K$  field extension,  $\alpha \in L, \bar{K}$  given algebraic closure. The elements  $\sigma(\alpha)$  with  $\sigma \in \text{Hom}_K(L, \bar{K})$  are called *conjugates of  $\alpha$* . In particular:  $L/K$  normal  $\Rightarrow$  conjugates live in  $L$ .
2.  $R$  ring,  $I$  ideal in  $R$ ,  $p : R \rightarrow R/I$  canonical projection. For  $\alpha, \beta \in R$  we denote  $\alpha \equiv \beta \pmod{I} : \iff p(\alpha) = p(\beta)$ .  
 If  $I = \langle q \rangle$  is a principal ideal, we denote  $\alpha \equiv \beta \pmod{q} : \iff \alpha \equiv \beta \pmod{\langle q \rangle}$

*Example 1.2.8.* Consider  $\mathbb{Q}(\zeta)/\mathbb{Q}$  with  $\zeta^p = 1, R = \mathcal{O} = \mathbb{Z}[\zeta], \alpha = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2}$

- i) The conjugates of  $\alpha$  are:  $\alpha_h = a_0 + a_1\zeta^h + a_2\zeta^{2h} + \cdots + a_{p-2}\zeta^{h(p-2)}$  with  $h \in \{1, \dots, p-1\}$ .
- ii) Consider  $\lambda = 1 - \zeta$  and  $I = \langle \lambda \rangle$ .  
 $1 \equiv \zeta \pmod{\lambda}$  and  $\alpha \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{\lambda} (\in \mathbb{Z})$ .
- iii)  $\alpha^p \equiv a_0^p + (a_1\zeta)^p + \cdots + (a_{p-2}\zeta^{p-2})^p = \underbrace{a_0^p + a_1^p + \cdots + a_{p-1}^p}_{\in \mathbb{Z}} \pmod{p}$

**Theorem 1** (Kummer's Lemma). *If  $\varepsilon \in \mathbb{Z}[\zeta]$  is a unit, i.e.  $\varepsilon \in \mathbb{Z}[\zeta]^\times$ ,*

$$\frac{\varepsilon}{\bar{\varepsilon}} = \zeta^a \quad \text{for some } a \in \mathbb{Z}$$

Here  $\bar{\varepsilon} = \tau(\varepsilon)$ , where  $\tau$  is the complex conjugation.

Recall:  $\tau \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ .

*Proof.* Denote  $\varepsilon = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} = r(\zeta)$  with  $r(X) = \sum_{i=0}^{p-2} a_i X^i \in \mathbb{Z}[X]$ .  
Observe:

1.  $\varepsilon \in \mathcal{O}^\times \Rightarrow \exists \varepsilon' \in \mathcal{O} \text{ s.t. } \varepsilon \varepsilon' = 1 \Rightarrow \bar{\varepsilon} \bar{\varepsilon}' = 1 \Rightarrow \bar{\varepsilon} \in \mathcal{O}^\times$
2.  $\mu := \frac{\varepsilon}{\bar{\varepsilon}} = \frac{r(\zeta)}{r(\bar{\zeta})}$  and the conjugate  $\mu_k$  of  $\mu$  is  $\frac{r(\zeta^k)}{r(\bar{\zeta}^k)} = \frac{r(\zeta^k)}{r(\zeta^k)}$ . In particular  $|\mu_k| = 1$ .  
 It follows that  $\mu_k \in \{\alpha \in \mathcal{O}^\times \mid |\alpha| = 1\}$  which is by 2.2. v) a finite subgroup of  $\mathbb{Q}(\zeta)^\times \Rightarrow \mu$  is a root of unity  
 Lemma 2.6  $\Rightarrow \mu = \pm \zeta^a$  for some  $a \in \mathbb{Z}$ .  
Claim:  $\mu = \zeta^a$   
Proof of claim: suppose  $\mu = -\zeta^a$ , i.e.  $\varepsilon = -\bar{\varepsilon} \zeta^a$   $(\star)$   
Idea: calculation mod  $\lambda = 1 - \zeta$   $\varepsilon = a_0 + a_1 \zeta + \dots + a_{p-2} \zeta^{p-2}$   
 Ex. 2.8.ii)  $\Rightarrow \varepsilon \equiv \underbrace{a_0 + a_1 + \dots + a_{p-2}}_{=: M \in \mathbb{Z}} \equiv \bar{\varepsilon} \pmod{\lambda}$   
 $(\star) \Rightarrow \varepsilon \equiv -\bar{\varepsilon} \pmod{\lambda} \Rightarrow M \equiv -M \pmod{\lambda} \Rightarrow 2M \equiv 0 \pmod{\lambda} \xrightarrow{\text{Lemma 2.6 i)}} p \text{ divides } 2M \text{ in } \mathbb{Z} \xrightarrow{p \text{ odd}} p \text{ divides } M$   
 $\Rightarrow \lambda = 1 - \zeta \text{ divides } M \text{ in } \mathcal{O} \text{ by Lemma 2.5.}$   
 $\Rightarrow \varepsilon \equiv \bar{\varepsilon} \equiv M \equiv 0 \pmod{\lambda = 1 - \zeta} \Rightarrow \text{Contradiction to } \varepsilon \text{ is unit and } 1 - \zeta \text{ is irreducible}$

□

**Corollary 1.2.9.**  $\varepsilon \text{ unit in } \mathbb{Z}[\zeta] \Rightarrow \varepsilon = r \zeta^s \text{ with some } r \in \mathbb{R}, s \in \mathbb{Z}.$

*Proof.* Prop 2.9  $\Rightarrow \exists a \in \mathbb{Z}, \varepsilon = \zeta^a \cdot \bar{\varepsilon}$ .

Choose  $s \in \mathbb{Z}$  with  $2s \equiv a \pmod{p}$

$\Rightarrow \frac{\varepsilon}{\zeta^s} = \zeta^s \cdot \bar{\varepsilon} = \frac{\bar{\varepsilon}}{\zeta^{-s}} = \frac{\bar{\varepsilon}}{\zeta^s} = r \in \mathbb{R} \text{ and } \varepsilon = r \cdot \zeta^s.$

□

**Lemma 1.2.10.** Suppose  $x, y, m, n \in \mathbb{Z}$  with  $m \not\equiv n \pmod{p}$ .  $x + y \zeta^n$  and  $x + y \zeta^m$  are relatively prime  $\iff (x \text{ and } y \text{ are relatively prime}) \text{ and } (x + y \text{ not divisible by } p)$

*Proof.* „ $\Rightarrow$ “:

- $d \mid x \text{ and } d \mid y \Rightarrow d \mid x + \zeta^n y \text{ and } d \mid x + \zeta^m y \nmid$
- „ $p \mid x + y$ “ Recall:  $p = \varepsilon(1 - \zeta)^{p-1}$  with  $\varepsilon \in \mathcal{O}^\times$   
 $\Rightarrow x + \zeta^m y = \underbrace{x + y}_{\text{divisible by } p} + y \cdot \underbrace{(\zeta^m - 1)}_{(\zeta - 1)(1 + \zeta + \zeta^2 + \dots + \zeta^{m-1})} \equiv 0 \pmod{1 - \zeta}$   
 same way  $x + \zeta^n y \equiv 0 \pmod{1 - \zeta} \nmid$

„ $\Leftarrow$ “: Idea: show:  $\exists \alpha_0, \beta_0 \in \mathcal{O}$  with:

$$1 = \alpha_0(x + \zeta^m y) + \beta_0(x + \zeta^n y)$$

Consider:  $A := \{\alpha(x + \zeta^m y) + \beta(x + \zeta^n y) \mid \alpha, \beta \in \mathcal{O}\}$

$A$  is an ideal in  $\mathcal{O}$ . We have:

1.  $(x + \zeta^m y) - (x + \zeta^n y) = \zeta^m(1 - \zeta^{n-m})y = \underbrace{\zeta^n \varepsilon_{n-m}}_{\in \mathcal{O}^\times} (1 - \zeta)y \Rightarrow (1 - \zeta)y \in A$

2.  $\zeta^n(x + \zeta^m y) - \zeta^m(x + \zeta^n y) = (\zeta^n - \zeta^m)x = \zeta^n \cdot (1 - \zeta^{n-m})x = \underbrace{\zeta^n \varepsilon_{m-n}}_{\in \mathcal{O}^\times} \cdot (1 - \zeta)x \Rightarrow (1 - \zeta)x \in A.$
3.  $\gcd(x, y) = 1 \Rightarrow \exists a, b \in \mathbb{Z} \text{ with } 1 = ax + by \Rightarrow (1 - \zeta)xa + (1 - \zeta)yb = 1 - \zeta \xrightarrow{1. \& 2.} 1 - \zeta \in A$
4.  $x + y = \underbrace{x + \zeta^n y}_{\in A} + \underbrace{(1 - \zeta^n)y}_{\in A} \in A$
5.  $\gcd(p, x + y) = 1 \Rightarrow \exists \bar{a}, \bar{b} \in \mathbb{Z} : 1 = \underbrace{\bar{a}p}_{\in A} + \underbrace{\bar{b}(x + y)}_{\in A} \in A.$   
 $\Rightarrow$  Hence  $x + \zeta^n y$  and  $x + \zeta^m y$  are coprime.

□

*Remark 1.2.11.* Suppose  $\alpha = a_0 + a_1\zeta + \dots + a_{p-1}\zeta^{p-1} \in \mathcal{O}$  with  $a_i \in \mathbb{Z}$  and at least one  $a_j \neq 0$ .

If  $n \in \mathbb{Z}$  with  $n$  divides  $\alpha$  in  $\mathcal{O}$ , then  $n$  divides all  $a_i$

*Proof.* Recall from 2.2 (preview):  $1, \zeta, \zeta^2, \dots, \zeta^{p-2}$  is a basis of  $\mathcal{O}$ .

Furthermore:  $1 + \zeta + \dots + \zeta^{p-1} = 0$

$\Rightarrow \{1, \zeta, \dots, \zeta^{p-1}\} \setminus \{\zeta^j\}$  is a basis  $\Rightarrow$  claim.

□

### 1.3 First case of Fermat in case of $\mathbb{Z}[\zeta]$ is a UFD (unique factorization domain)

Reference: BOREVICH + SHAFEREVIC + WASHINGTON Chapter 1

As before:  $p$  odd prime,  $\zeta = e^{\frac{2\pi i}{p}}$   $p$ -th root of unity.

**Theorem 2.** Suppose that  $\mathbb{Z}[\zeta]$  is a UFD, then  $x^p + y^p = z^p$  has no non-trivial solutions  $(x, y, z)$ , such that neither  $x, y$  nor  $z$  is divisible by  $p$ .

**Theorem 3** ( $p = 3$ ). Suppose  $x, y, z \in \mathbb{Z}$  with  $x^3 + y^3 = z^3 \pmod{9} \Rightarrow 3$  divides  $x, y$  or  $z$ .

*Proof.* Recall: Little Fermat's theorem  $x^p \equiv x, y^p \equiv y, z^p \equiv z \pmod{p}$ .

$$\begin{aligned}
 x^3 + y^3 &\equiv z^3 \pmod{3} \Rightarrow x + y \equiv z \pmod{3} \\
 &\Rightarrow z = x + y + 3u \text{ with } u \in \mathbb{Z} \\
 \Rightarrow \underline{x^3 + y^3} &\equiv (x + y + 3u)^3 \equiv \underline{x^3 + y^3} + 3xy^2 + 3x^2y \pmod{9} \\
 &\Rightarrow 0 \equiv xy^3 + x^2y \equiv xy(x + y) \equiv xyz \pmod{3} \\
 &\Rightarrow x, y \text{ or } z \text{ is divisible by } 3
 \end{aligned}$$

□



**Lemma 1.3.1.** *Let  $p \geq 5$ . Suppose  $x, y, z \in \mathbb{Z}$  with  $x^p + y^p = z^p$ . If  $x \equiv y \equiv -z \pmod{p}$ , then  $p|z$ .*

*Proof.*  $z \equiv z^p = x^p + y^p \equiv -2z^p \equiv -2z \pmod{p} \Rightarrow 3z \equiv 0 \pmod{p} \xrightarrow{p \neq 3} p|z$ .  $\square$

*Remark 1.3.2.* It follows from Lemma 3.2 that in the first case of Fermat we may assume for  $p \geq 5$  that  $x \not\equiv y \pmod{p}$  because we can replace  $x^p + y^p = z^p$  by  $x^p + (-z)^p = (-y)^p$  and  $x \not\equiv -z \pmod{p}$ .

*of Thm. 1.*  $p = 3 \Rightarrow$  claim follows from Prop 3.1.

Now:  $p \geq 5$ . Suppose  $x, y, z \in \mathbb{Z}$  with  $p$  divides neither  $x, y$  nor  $z$ ,  $x, y, z$  are pairwise coprime and  $x \not\equiv y \pmod{p}$ . Suppose  $z^p = x^p + y^p = (x + y)(x + \zeta y) \dots (x + \zeta^{p-1}y)$ .

Apply Lemma 2.11:

- $\gcd(x, y) = 1 \checkmark$
- Little Fermat  $\Rightarrow x + y \equiv x^p + y^p \equiv z^p \not\equiv 0 \pmod{p}$

$\xrightarrow{2.11} x + y, x + \zeta y, \dots, x + \zeta^{p-1}y$  are pairwise coprime.

$\xrightarrow{\mathbb{Z}[\zeta] \text{ UFD}} \text{„}x + \zeta^i y \text{ have to be } p\text{-power“}$  More precisely:  $x + \zeta y = \varepsilon \alpha^p$  with  $\varepsilon \in \mathcal{O}^\times, \alpha \in \mathcal{O}$ , since they are coprime factors of a  $p$ -th power.

1. Cor. 2.10  $\Rightarrow \varepsilon = r\zeta^s$  with  $r \in \mathbb{R}, s \in \mathbb{Z}$
2. Example 2.8. iii)  $\Rightarrow \exists a \in \mathbb{Z}$  with  $\alpha^p \equiv a \pmod{p}$ .

$$\begin{aligned} x + \zeta y &= r\zeta^s \alpha^p \equiv r\zeta^s a \pmod{p} \\ x + \zeta^{-1}y &= \overline{x + \zeta y} \equiv r\zeta^{-s} a \pmod{p} \\ \Rightarrow \zeta^{-s}(x + \zeta y) &\equiv ra \equiv \zeta^s(x + \zeta^{-1}y) \pmod{p} \\ \Rightarrow \underbrace{x + \zeta y - \zeta^{2s}x - \zeta^{2s-1}y}_{=x \cdot 1 + y\zeta - x\zeta^{2s} - y\zeta^{2s-1}} &\equiv 0 \pmod{p} \end{aligned}$$

Idea: Use Rem. 2.12

Case 1:  $1, \zeta, \zeta^{2s-1}, \zeta^{2s}$  are distinct  $\xrightarrow{p \geq 5, \text{ Rem } 2.12} p|x$  and  $p|y$ . Contradiction to first case.

$\square$

Recall:  $L = \mathbb{Q}(\zeta)$ ,  $\mathcal{O} = \mathbb{Z}[\zeta]$ , where  $\zeta$  is a  $p$ -th root of unity

**Last time:**

- (1)  $a_1 1 + a_2 \zeta + \dots + a_p \zeta^{p-1} = \alpha$  and at least one  $a_j = 0$   
If  $\alpha$  is divided by  $n \in \mathbb{Z}$  then all the  $a_i$  are divided by  $n$ .
- (2)  $x + y\zeta - x\zeta^{2s} - y\zeta^{2s-1} \equiv 0 \pmod{p}$

*Continuation of proof of Theorem 1.* “Case 2”  $1, \zeta, \dots, \zeta^{2s}$  are not distinct.

Observe:  $1 \neq \zeta$  and  $\zeta^{2s-1} \neq \zeta^{2s}$

“Case 2A”  $1 = \zeta^{2s} (\Leftrightarrow p|s)$ .

(2) implies  $y\zeta - y\zeta^{2s-1} \equiv 0 \pmod{p}$  such that Remark 2.12 yields the contradiction  $p|y$ .

“Case 2B”  $1 = \zeta^{2s-1} (\Leftrightarrow \zeta = \zeta^{2s})$ .

(2) implies  $(x - y)1 + (y - x)\zeta \equiv 0 \pmod{p}$  such that Remark 2.12 yields  $p|y - x$ , which contradicts the assumption  $x \not\equiv y \pmod{p}$ .

“Case 2C”  $\zeta = \zeta^{2s-1}$ .

(2) implies  $x - x\zeta^2 \equiv 0 \pmod{p}$  such that Remark 2.12 yields the contradiction  $p|x$ .  $\square$

### Questions:

(1) Under which assumption is  $\mathcal{O}$  a UFD?

(2) What can we do if  $\mathcal{O}$  is not a UFD?

→ Idea of Kummer: “calculate with ideals”

**Prospect:** Theorem (Montgomery, Uchida, 1971)

$\mathbb{Z}[\zeta]$  is a UFD if and only if  $p \leq 19$ ,  $p$  prime.

**Preview:** From Kummer’s idea we obtain a better criterion for  $p$  called **regular**, which ensures that Fermat’s conjecture holds for  $p$ .

**Conjecture.** *There are infinitely many regular primes.*

## 2 Ring of integers

In this chapter, all rings are assumed to be commutative with 1.

### 2.1 Integral ring extensions

**Definition 2.1.1** (“ganze Ringerweiterungen”). Let  $A \subset B$  be a ring extension.

- (i)  $b \in B$  is **integral** over  $A$  if there exists a monic polynomial  $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in A[X]$  with  $f(b) = 0$ .
- (ii)  $B$  is **integral** over  $A$  if all  $b \in B$  are integral over  $A$ .

**Proposition 2.1.2.** Let  $A \subset B$  be a ring extension and  $b_1, \dots, b_n \in B$ . Then  $b_1, \dots, b_n$  are integral over  $A$  if and only if

$$A[b_1, \dots, b_n] = \{f(b_1, \dots, b_n) \mid f \in A[X_1, \dots, X_n]\}$$

is a finitely generated  $A$ -module.

*Reminder 2.1.3* (“Adjunkte”). Let  $R$  be a ring and  $A \in R^{n \times n}$

- (i)  $A^\# = (a_{i,j}^\#)$  with  $a_{i,j}^\# = (-1)^{i+j} \det(A_{j,i})$ , where  $A_{j,i}$  is obtained from  $A$  by deleting the  $j$ -th row and  $i$ -th column of  $A$ .
- (ii) We have  $AA^\# = A^\#A = \det(A)I$ . In particular,  $Ax = 0$  implies  $A^\#Ax = 0$  such that  $\det(A)x = 0$ .

*Proof of Proposition 1.2.* “ $\Rightarrow$ ” If  $n = 1$  and  $b$  is integral over  $A$ , then there is an  $f \in A[X]$  with  $f$  monic such that  $f(b) = 0$ . Let  $g \in A[X]$  be arbitrary. Then

$$g(X) = q(X)f(X) + r(X)$$

with  $q, r \in A[X]$  and  $\deg r < \deg f = d$ . Hence  $g(b) = r(b)$  with  $\deg r < d$ . Thus  $\{1, b, \dots, b^{d-1}\}$  generate  $A[b]$  as an  $A$ -module. The case  $n \geq 2$  follows by induction.

“ $\Leftarrow$ ”  $A[b_1, \dots, b_n]$  is finitely generated as an  $A$ -module by  $w_1, \dots, w_r$ . If  $b \in A[b_1, \dots, b_n]$  then

$$bw_i = \sum_{j=1}^r a_{j,i} w_j$$

such that

$$(bI - (a_{i,j}))w = 0.$$

Thus,  $\det(bI - (a_{i,j}))w = 0$  and hence

$$\det(bI - (a_{i,j}))w_i = 0$$

for all  $i = 1, \dots, r$ . If we now use that

$$1 = c_1 w_1 + \dots + c_r w_r$$

we can infer  $\det(bI - (a_{i,j}))1 = 0$ . Consider

$$M = bI - (a_{i,j}) = \begin{pmatrix} b - a_{1,1} & -a_{1,2} & \cdots & -a_{1,r} \\ -a_{2,1} & b - a_{2,2} & \cdots & -a_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{r,1} & -a_{r,2} & \cdots & b - a_{r,r} \end{pmatrix}.$$

By the Leibniz formula we have

$$\det(M) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n m_{\sigma(i),i}$$

which is a polynomial over  $b$  with leading coefficient 1. Hence  $b$  is integral over  $A$ .  $\square$

**Corollary 2.1.4** (And Definition). (i) If  $A \subset B$  is an extension of rings then

$$\overline{A} = \{b \in B \mid b \text{ is integral over } A\}$$

is a ring. It is called the **integral closure** of  $A$  in  $B$ . If  $\overline{A} = A$  then  $A$  is called **integrally closed** in  $B$ .

(ii) We have transitivity, that is to say, if  $A, B, C$  are rings with  $A \subset B \subset C$  such that  $C$  is integral over  $B$  and  $B$  is integral over  $A$  then  $C$  is integral over  $A$ .

(iii) The integral closure of  $A$  in  $B$  is integrally closed, i.e.,  $\overline{\overline{A}} = \overline{A}$ .

*Proof.* “(i)” If  $b_1, b_2 \in \overline{A}$  then  $A[b_1], A[b_2]$  are finitely generated  $A$ -modules. Hence  $A[b_1, b_2]$  is a finitely generated  $A$ -module. Thus, by Proposition 1.3,  $b_1 + b_2$  and  $b_1 b_2$  are integral, i.e., elements of  $\overline{A}$ .

“(ii)” If  $c \in C$  then  $c$  is integral over  $B$  and hence there is a monic polynomial  $f = X^n + b_{n-1}X^{n-1} + \dots + b_0 \in B[X]$  with  $f(c) = 0$ . This shows that  $c$  is integral over  $R = A[b_1, \dots, b_{n-1}]$  such that Proposition 1.3 shows that  $R[c]$  is a finitely generated  $R$ -module. Furthermore,  $b_0, \dots, b_{n-1}$  are integral over  $A$  such that another application of Proposition 1.3 shows that  $R$  is a finitely generated  $A$ -module. Hence,  $R[c]$  is a finitely generated  $A$  module such that  $c$  is integral over  $A$  by Proposition 1.3.

“(iii)” Follows from (ii).  $\square$

**Definition 2.1.5** (“ganzer Abschluss und normaler Ring”). If  $A$  is an integral domain we call its integral closure  $\overline{A}$  in  $K = \text{Quot}(A)$  the **normalization** or the **integral closure** of  $A$ . We say  $A$  is **integrally closed** if  $A$  is integrally closed in  $K$ .

*Remark 2.1.6.* If  $A$  is a UFD then  $A$  is integrally closed.

*Proof.* Suppose  $b = \frac{a}{a'} \in \text{Quot}(A)$  with  $\gcd(a, a') = 1$  is integral over  $A$ . Then there exist  $a_0, \dots, a_{n-1} \in A$  with

$$\left(\frac{a}{a'}\right)^n + a_{n-1} \left(\frac{a}{a'}\right)^{n-1} + a_{n-2} \left(\frac{a}{a'}\right)^{n-2} + \dots + a_0 = 0$$

such that

$$a^n + a_{n-1}a'a^{n-1} + a_{n-2}a'^2a^{n-2} + \dots + a_0a'^n = 0.$$

Let  $a' = \varepsilon \pi_1 \cdots \pi_r$  be the prime factorization of  $a'$  with  $\varepsilon \in A^\times$  and  $\pi_1, \dots, \pi_r$  primes. Since  $\pi_i | a'$  the above equation shows that actually  $\pi_i | a^n$ . But this implies  $\pi_i | a$  which is a contradiction to  $\gcd(a, a') = 1$ . Hence we have  $a' = \varepsilon \in A^\times$  such that  $b \in A$ .  $\square$

## 2.2 Integral closures in field extensions

**Setting:**

- $A$  is an integral domain.
- $A$  is integrally closed.
- $K = \text{Quot}(A)$ .
- $L/K$  is a finite field extension with  $\overline{A}_K = A \subset K = \text{Quot}(A) \hookrightarrow L \supset B = \overline{A}_L$ .
- $B$  is the integral closure of  $A$  in  $L$ . Observe:  $B \cap K = A$

*Remark 2.2.1.* (i)  $B$  is integrally closed in  $L$ .

(ii) If  $\beta \in L$  then there are  $b \in B$  and  $a \in A \setminus \{0\}$  such that  $\beta = \frac{b}{a}$ .

In particular,  $L = \text{Quot}(B)$ .

(iii) For  $\beta \in L$  we have  $\beta \in B$  if and only if  $f_\beta \in A[X]$ , where  $f_\beta$  is the minimal polynomial of  $\beta$  over  $K$ .

*Proof.* “(i)” Follows from the transitivity in Corollary 1.4.

“(ii)” Choose  $a \in A$  with  $a^n f_\beta(X) = a^n X^n + a^{n-1} c_{n-1} X^{n-1} + \dots + c_0 \in A[X]$ . Then we have

$$a^n \beta^n + c_{n-1} a^{n-1} \beta^{n-1} + \dots + c_0 = 0$$

and hence

$$(a\beta)^n + c_{n-1} (a\beta)^{n-1} + \dots + c_0 = 0$$

such that  $a\beta$  is integral over  $A$ . Consequently,  $b = a\beta \in B$  and  $\beta = \frac{b}{a}$ .

“(iii)” “ $\Leftarrow$ ” Obvious. “ $\Rightarrow$ ” Let  $\beta$  be a zero of  $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ . Then  $f_\beta$  divides  $g$ . If  $\beta_1, \dots, \beta_n$  are the zeros of  $f_\beta$  in  $\overline{K}$  then they are also zeros of  $g$  and thus integral over  $A$ . Hence the coefficients of  $f_\beta$  are integral over  $A$  and are elements of  $K$  such that  $f_\beta \in A[X]$  as claimed.  $\square$

*Reminder 2.2.2* (Trace, Norm). Let  $K \subseteq L$  be a finite field extension. For  $\alpha$  in  $L$  consider the map  $T_\alpha : \beta \mapsto \alpha\beta$ . The following holds

- i)  $\text{Tr}_{L/K}(\alpha) = \text{Tr}(T_\alpha)$  and  $\mathcal{N}_{L/K}(\alpha) = \det(T_\alpha)$ ,
- ii) If  $L = K(\alpha)$  and  $f_\alpha(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$  then

$$\text{Tr}_{L/K}(\alpha) = -a_{n-1} \text{ and } \mathcal{N}_{L/K}(\alpha) = (-1)^n \cdot a_0,$$

- iii) Since  $T_{\alpha+\beta} = T_\alpha + T_\beta$  and  $T_{\alpha\beta} = T_\alpha \circ T_\beta$ , we conclude that

$$\text{Tr}_{L/K} : (L, +) \rightarrow (K, +) \text{ and } \mathcal{N}_{L/K} : (L^*, \cdot) \rightarrow (K^*, \cdot)$$

are group homomorphisms,

- iv) Suppose  $K \subseteq L$  is a separable field extension with  $L = K(\alpha)$ . Further assume  $\text{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$ . Then the following holds

- $f_\alpha = \prod_{i=1}^n (X - \sigma_i(\alpha))$ ,
- $\text{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ ,
- $\mathcal{N}_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ ,

- v) Trace and norm are transitive, i.e., for field extensions  $K \subseteq L \subseteq M$  it holds

- $\mathcal{N}_{L/K} \circ \mathcal{N}_{M/L} = \mathcal{N}_{M/K}$ ,
- $\text{Tr}_{L/K} \circ \text{Tr}_{M/L} = \text{Tr}_{M/K}$ .

**Definition 2.2.3** (Discriminant). Let  $K \subseteq L$  be a separable field extension and let  $\alpha_1, \dots, \alpha_n$  be a  $K$ -basis of  $L$ . Further let  $\text{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$ . Consider the matrix

$$A := \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} = (\sigma_i(\alpha_j))_{i,j} \in L^{n \times n}.$$

We call  $d(\alpha_1, \dots, \alpha_n) := \det(A^2)$  the **discriminant** of  $L$  over  $K$  with respect to the basis  $\alpha_1, \dots, \alpha_n$ .

*Remark 2.2.4.* In the situation of Definition (2.2.3) the following holds.

- i) Consider the matrix  $B = (\text{Tr}_{L/K}(\alpha_i \alpha_j))_{i,j}$  in  $K^{n \times n}$ . Then the discriminant is given by  $d(\alpha_1, \dots, \alpha_n) = \det(B)$ . In particular, the discriminant  $d(\alpha_1, \dots, \alpha_n)$  lies in  $K$ .
- ii) Suppose we have  $\Theta$  in  $L$  such that  $1, \Theta, \dots, \Theta^{n-1}$  forms a basis of  $L$ . Then the following equality holds

$$d(1, \Theta, \dots, \Theta^{n-1}) = \prod_{1 \leq i < j \leq n} (\Theta_i - \Theta_j)^2.$$

Here  $\Theta_i$  denotes  $\sigma_i(\Theta)$ . If  $L = K(\Theta)$  then  $d(1, \Theta, \dots, \Theta^{n-1})$  coincides with the discriminant of the minimal polynomial  $f_\Theta$ . Note that we use the notion of discriminants for polynomials here.

*Proof.* We begin by proving statement i). One computes

$$\det(A)^2 = \det(A^t) \cdot \det(A) = \det(A^t \cdot A).$$

The following calculation proves the claim

$$\begin{aligned} A^t \cdot A &= (\sigma_j(\alpha_i))_{i,j} \cdot (\sigma_k(\alpha_\ell))_{k,\ell} \\ &= \left( \sum_{j=1}^n \sigma_j(\alpha_i) \cdot \sigma_j(\alpha_\ell) \right)_{i,\ell} \\ &= \left( \sum_{j=1}^n \sigma_j(\alpha_i \cdot \alpha_\ell) \right)_{i,\ell} \\ &= (\text{Tr}_{L/K}(\alpha_i \cdot \alpha_\ell))_{i,\ell} \\ &= B. \end{aligned}$$

For statement ii), we will compute the determinant of the following Vandermonde matrix

$$\det(A) = \det \begin{pmatrix} 1 & \Theta_1 & \dots & \Theta_1^{n-1} \\ 1 & \Theta_2 & \dots & \Theta_2^{n-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \Theta_n & \dots & \Theta_n^{n-1} \end{pmatrix} =: V_n(\Theta_1, \dots, \Theta_n).$$

By induction, we prove that  $V_n(\Theta_1, \dots, \Theta_n)$  is nonzero and that the following equality holds

$$V_n(\Theta_1, \dots, \Theta_n) = \prod_{1 \leq i < j \leq n} (\Theta_j - \Theta_i).$$

For  $n = 2$ , we have

$$\det(A) = \det \begin{pmatrix} 1 & \Theta_1 \\ 1 & \Theta_2 \end{pmatrix} = \Theta_2 - \Theta_1 \neq 0.$$

Hence the claim holds for  $n = 2$ . Now we assume that the claim holds for a  $n \in \mathbb{N}_{\geq 2}$ . We want to prove that viewed as polynomials in  $Z$  the following equality holds

$$V_{n+1}(\Theta_1, \dots, \Theta_n, Z) = V_n(\Theta_1, \dots, \Theta_n) \cdot \prod_{i=1}^n (Z - \Theta_i). \quad (2.1)$$

This implies that

$$V_n(\Theta_1, \dots, \Theta_{n+1}) = V_n(\Theta_1, \dots, \Theta_n) \cdot \prod_{i=1}^n (\Theta_{n+1} - \Theta_i) = \prod_{1 \leq i < j \leq n} (\Theta_j - \Theta_i).$$

To show equality (2.1), recall that

$$V_{n+1}(\Theta_1, \dots, \Theta_n, Z) = \det \begin{pmatrix} 1 & \Theta_1 & \dots & \Theta_1^n \\ 1 & \Theta_2 & \dots & \Theta_2^n \\ \vdots & \vdots & \dots & \vdots \\ 1 & \Theta_n(\alpha_2) & \dots & \Theta_n^n \\ 1 & Z & \dots & Z^n \end{pmatrix}.$$

One sees that the polynomials on both sides of equality (2.1) have degree  $n$ . Moreover,  $\{\Theta_1, \dots, \Theta_n\}$  is the set of zeros for both polynomials. Since the leading coefficient in both cases is  $V_n(\Theta_1, \dots, \Theta_n)$ , the polynomials are equal. This proves the claim.  $\square$

*Example 2.2.5.* Consider  $L = \mathbb{Q}(\sqrt{D})$  for a square free integer  $D$  different from 0 and 1. Then the following holds

- $\mathfrak{B}_1 = \{1, \sqrt{D}\}$  is a  $\mathbb{Q}$ -basis of  $L$ .
- Define  $\sigma_2 : L \rightarrow \overline{\mathbb{Q}}, a + b\sqrt{D} \mapsto a - b\sqrt{D}$ . Then we have

$$\text{Hom}_{\mathbb{Q}}(L, \overline{\mathbb{Q}}) = \{\sigma_1 = \text{id}, \sigma_2\}.$$

- $\text{Tr}_{L/\mathbb{Q}}(a + b\sqrt{D}) = a + b\sqrt{D} + a - b\sqrt{D} = 2a$ .
- $\mathcal{N}_{L/\mathbb{Q}}(a + b\sqrt{D}) = (a + b\sqrt{D}) \cdot (a - b\sqrt{D}) = a^2 - b^2 \cdot D$ .
- $d(\mathfrak{B}_1) = \det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^2 = (-2\sqrt{D}) = 4D$ .
- We have

$$(\alpha_i \alpha_j)_{i,j} = \begin{pmatrix} 1 & \sqrt{D} \\ \sqrt{D} & D \end{pmatrix}.$$

Hence we compute

$$\det((\text{Tr}(\alpha_i \alpha_j))_{i,j}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D.$$



- Consider the  $\mathbb{Q}$ -basis of  $L$  given by  $\mathfrak{B}_2 = \{1 + \sqrt{D}, 1 - \sqrt{D}\}$ . Computing the discriminant for this basis yields

$$d(1 + \sqrt{D}, 1 - \sqrt{D}) = \det \begin{pmatrix} 1 + \sqrt{D} & 1 - \sqrt{D} \\ 1 - \sqrt{D} & 1 + \sqrt{D} \end{pmatrix}^2 = 16D.$$

Hence we see that the discriminant depends on the basis we choose.

**Proposition 2.2.6.** *Let  $K \subseteq L$  be a separable field extension.*

i) *The bilinear map*

$$h : L^2 \rightarrow K, (x, y) \mapsto \text{Tr}_{L/K}(xy)$$

*is non degenerate, i.e.,  $h(x, y) = 0$  for all  $y \in L$  implies that  $x = 0$ .*

ii) *If  $\alpha_1, \dots, \alpha_n$  forms a basis of  $L/K$  then  $d(\alpha_1, \dots, \alpha_n) \neq 0$ .*

*Proof.* For statement i), we choose a primitive element  $\Theta$ . Then  $1, \Theta, \dots, \Theta^{n-1}$  is a  $K$ -basis of  $L$ . Let  $B$  be the matrix representation of  $h$  with respect to this basis. We find

$$\begin{aligned} \det(B) &\stackrel{(2.4) \text{ i)}}{=} d(1, \Theta, \dots, \Theta^{n-1}) \\ &\stackrel{(2.4) \text{ ii)}}{=} \prod_{1 \leq i < j \leq n} (\Theta_i - \Theta_j)^2 \neq 0. \end{aligned}$$

Here  $\Theta_i$  denotes  $\sigma_i(\Theta)$ . This shows that  $h$  is non degenerate. We now prove statement ii). Observe that the matrix  $M = (\text{Tr}_{L/K}(\alpha_i \alpha_j))_{i,j}$  is the matrix representation of  $h$  with respect to  $\alpha_1, \dots, \alpha_n$ . By Remark (2.4), we conclude

$$d(\alpha_1, \dots, \alpha_n) = \det(M).$$

Now, i) implies that  $\det(M)$  is nonzero. □

*Remark 2.2.7.* Let  $A \subseteq B$  be an integral ring extension with  $B \subseteq L$  and  $A = B \cap K \subseteq K$ . Assuming that  $\text{Hom}_K(L, \overline{K}) = \{\text{id} = \sigma_1, \dots, \sigma_n\}$  the following holds

- i) If  $x \in B$  then  $\sigma_i(x) \in B$  for all  $1 \leq i \leq n$ .
- ii) For all  $x \in B$  the trace  $\text{Tr}_{L/K}(x)$  and the norm  $\mathcal{N}_{L/K}(x)$  lie in  $A$ .
- iii) Let  $x \in B$ . Then  $x$  lies in  $B^*$  if and only if the norm  $\mathcal{N}_{L/K}(x)$  lie in  $A^*$ .

*Proof.* We start by proving i). Let  $x$  in  $B$ . By Remark (2.1), we have that the minimal polynomial  $f_x$  lies in  $A[X]$ . Since  $\sigma(x)$  is also a zero of  $f_x$ , it is contained in  $B$ . This shows i). Now, statement ii) follows from i), Remark (2.2) iv) and the fact that  $A = B \cap K$ . For iii), assume that  $x$  is a unit in  $B$ , i.e., we find  $y$  in  $B$  with  $xy = 1$ . Hence

$$\mathcal{N}_{L/K}(x) \cdot \mathcal{N}_{L/K}(y) = \mathcal{N}_{L/K}(xy) = 1.$$

Using ii), we deduce that  $\mathcal{N}_{L/K}(x)$  lies in  $A^*$ . This proves one direction. For the other direction, assume that  $\mathcal{N}_{L/K}(x)$  lies in  $A^*$ , i.e., we find  $a \in A$  with

$$\begin{aligned} 1 &= a \cdot \mathcal{N}_{L/K}(x) \\ &= a \cdot \prod_{i=1}^n \sigma_i(x) \\ &= a \cdot x \cdot \underbrace{\prod_{i=2}^n \sigma_i(x)}_{\in B, \text{ by i)}}. \end{aligned}$$

Hence  $x$  lies in  $B^*$ . This proves iii).  $\square$

**Proposition 2.2.8.** Suppose  $\alpha_1, \dots, \alpha_n \in B$  forms a  $K$ -basis of  $L$ . Let  $d$  denote the discriminant  $d(\alpha_1, \dots, \alpha_n) \in A$ . Then  $d \cdot B$  is contained in  $A\alpha_1 + \dots + A\alpha_n$ .

*Proof.* Suppose  $\alpha = \sum_{j=1}^n c_j \alpha_j \in B$  for  $c_i \in K$ . We want to solve for  $(c_1, \dots, c_n)$ . Applying the trace to the equalities

$$\alpha_i \alpha = \sum_{j=1}^n c_j \alpha_i \alpha_j, \quad 1 \leq i \leq n,$$

we obtain

$$\text{Tr}_{L/K}(\alpha_i \alpha) = \sum_{j=1}^n c_j \text{Tr}_{L/K}(\alpha_i \alpha_j), \quad 1 \leq i \leq n.$$

Hence  $x = (c_1, \dots, c_n)$  is the solution of the linear system  $Mx = y$ , where

$$M = ((\text{Tr}_{L/K}(\alpha_i \alpha_j)))_{i,j} \in A^{n \times n}, \quad y = (\text{Tr}_{L/K}(\alpha_i \alpha))_i \in A^n.$$

By Remark (1.3), we have

$$\det(M) \cdot x = M^\# Mx = M^\# y \in A^n.$$

Using Remark (2.4), we know  $\det(M) = d(\alpha_1, \dots, \alpha_n) =: d$ . We conclude that  $dc_i$  lies in  $A$  for  $1 \leq i \leq n$ , which proves the claim.  $\square$

**Definition 2.2.9** (Ganzheitsbasis). Suppose  $\omega_1, \dots, \omega_n \in B$  forms a basis of  $B$  over  $A$ , i.e., every  $\alpha \in B$  can be written in a unique way as an  $A$ -linear combination  $\sum_{i=1}^n c_i \omega_i$ . Then  $\omega_1, \dots, \omega_n$  is called an **integral basis** of  $B$  over  $A$ .

*Example 2.2.10.* Same situation as in Ex. 2.5.  $\mathcal{B}_1 = \{1, \sqrt{D}\} \subseteq B$ . Consider:

$$\begin{aligned} \alpha &= \frac{1}{2}(1 + \sqrt{D}) \Rightarrow 2\alpha = 1 + \sqrt{D} \\ \Rightarrow (2\alpha - 1)^2 &= D \Rightarrow 4\alpha^2 - 4\alpha + 1 = D \\ \Rightarrow f_\alpha(X) &= X^2 - X + \frac{1-D}{4} \end{aligned}$$

Hence if  $D \equiv 1 \pmod{4} \Rightarrow \alpha \in B$  and  $\mathcal{B}_1$  is not an integral basis.

**Proposition 2.2.11.** *Let  $D \in \mathbb{Z}$ ,  $D$  square-free,  $D \neq 0, 1$ ,  $B :=$  integral closure of  $\mathbb{Z}$  in  $\mathbb{Q}(\sqrt{D}) = L$ .*

- i)  $D \equiv 2, 3 \pmod{4} \Rightarrow \{1, \sqrt{D}\}$  is an integral basis of  $B/\mathbb{Z}$  in particular  $B = \mathbb{Z}[\sqrt{D}]$ .
- ii)  $D \equiv 1 \pmod{4} \Rightarrow \{1, \frac{1}{2}(\sqrt{D}+1)\}$  is an integral basis of  $B/\mathbb{Z}$ . and  $B = \mathbb{Z}[\frac{1}{2}(1+\sqrt{D})]$ .

*Proof.* Consider  $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$  with  $a, b \in \mathbb{Q}$ .

$$\Rightarrow f_\alpha = X^2 - 2aX + a^2 - b^2D.$$

Rem 2.1:  $\alpha \in B \iff f_\alpha \in \mathbb{Z}[X] \iff 2a \in \mathbb{Z} \text{ and } a^2 - b^2D \in \mathbb{Z}$ .

- (1) Show:  $\alpha \in B \Rightarrow 2b \in \mathbb{Z}$ .

$$\alpha \in B \Rightarrow 4a^2 - 4b^2D = 4z \text{ with } z \in \mathbb{Z}. \text{ Write } b = \frac{p}{q} \text{ with } p, q \in \mathbb{Z}, \gcd(p, q) = 1$$

$$\Rightarrow 4p^2D = ((2a)^2 - 4z)q^2 \quad (\star)$$

$$\Rightarrow q = 1 \text{ or } 2.$$

- (2) Show:  $q = 2 \Rightarrow D \equiv 1 \pmod{4}$

$$(\star) \Rightarrow p^2D = (2a)^2 - 4z \equiv (2a)^2 \pmod{4}$$

$$p \text{ is odd, hence } p^2 \equiv 1 \pmod{4} \Rightarrow (2a)^2 \text{ is odd (i.e. } a = \frac{2n-1}{2} \in \mathbb{Q})$$

$$\Rightarrow (2a)^2 \equiv 1 \pmod{4} \Rightarrow D \equiv 1 \pmod{4}.$$

- (3) It follows from (2) if  $D \equiv 1 \pmod{4}$ :

$$\alpha \in B \iff \alpha = a + b\sqrt{D} \text{ or } \alpha = \frac{1}{2}(a + b\sqrt{D}) \text{ with } a, b \in \mathbb{Z}. \text{ Hence we obtain:}$$

$$B = \begin{cases} \mathbb{Z}[\sqrt{D}] & , \text{ if } D \equiv 2, 3 \pmod{4} \\ \mathbb{Z}[\frac{1}{2}(1 + \sqrt{D})] & , \text{ if } D \equiv 1 \pmod{4} \end{cases}$$

For the second case observe that  $\frac{a}{2} + \frac{b}{2}\sqrt{D} = \frac{a-b}{2} + \frac{b}{2}(1 + \sqrt{D}) \in \mathbb{Z}[\frac{1}{2}(1 + \sqrt{D})]$ .

This implies the claim. □

**Proposition 2.2.12.** *Suppose  $L/K$  separable and  $A$  is a principal ideal domain. Let  $M \neq 0$  be a finitely generated  $B$ -submodule of  $L \Rightarrow M$  is a free  $A$ -module. In particular:  $B$  is a free  $A$ -module of rank  $n := [L : K]$ .*

*Reminder 2.2.13.* Suppose  $A$  is a principal ideal domain and  $M_0$  is a finitely generated free  $A$ -module.

- i) Any submodule  $M$  of  $M_0$  is free.

- ii)  $\text{rank}(M_0) \geq \text{rank}(M)$

*of Prop 2.12.* Let  $\mu_1, \dots, \mu_r \in M \subseteq L$  be generators of  $M$  as  $B$ -module and let  $\alpha_1, \dots, \alpha_n$  be a basis of  $L/K$  in  $B$  and  $d := d(\alpha_1, \dots, \alpha_n) \in A$ .

Recall:  $L = \{\frac{b}{a} \mid b \in B, a \in A \setminus \{0\}\}$ .

- (1) Prop 2.7  $\Rightarrow dB \subseteq A\alpha_1 + \dots + A\alpha_n$

$$(2) \exists a \in A : a\mu_1, \dots, a\mu_r \in B$$

Hence:  $daM \subseteq dB \subseteq A\alpha_1 + \dots + A\alpha_n =: M_0$

( $M_0$  is a free  $A$ -module, since  $\alpha_1, \dots, \alpha_n$  are basis of  $L/K$ ).

Reminder 2.13  $\Rightarrow adM$  is a free  $A$ -module  $\Rightarrow M$  is a free  $A$ -module.

Furthermore:  $\text{rank}(M) = \text{rank}(adM) \stackrel{\text{Rem. 2.13}}{\leq} \text{rank}(M_0) = n$ .

Suppose that  $M = B$ . So far we got that  $B$  is a free  $A$ -module and  $\text{rank}(B) \leq n$ .

Show:  $\text{rank}(B) \geq n$ .

Let  $\mu_1, \dots, \mu_r$  be a basis of  $B$  as  $A$ -module. By  $L = \{\frac{b}{a} \mid b \in B, a \in A \setminus \{0\}\}$  we have that  $\mu_1, \dots, \mu_r$  generate  $L$  over  $K$ .  $\square$

Hence: if  $A$  is a principal ideal domain, then  $B$  has always an integral basis.

**Proposition 2.2.14.** *Suppose we are in the following situation:*

- $L/K$  and  $L'/K$  are Galois extensions of degree  $n$  and  $m$  in some field  $E$
- $A$  a subring of  $K$  such that  $K = \text{Quot}(A)$  and  $B$  and  $B'$  are the integral closures of  $A$  in  $L$  and  $L'$ .
- $\{\omega_1, \dots, \omega_n\}$  and  $\{\omega'_1, \dots, \omega'_m\}$  are integral basis for  $B/A$  and  $B'/A$ .
- $d := d(\omega_1, \dots, \omega_n)$  and  $d' := d(\omega'_1, \dots, \omega'_m) \in A$  with  $d$  and  $d'$  are coprime in  $A$ , i.e.  $\exists x, x' \in A$  with  $1 = dx + d'x'$ .
- $K = L \cap L'$

Then we have:  $\{\omega_i \omega'_j \mid i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$  is an integral basis and its discriminant is  $d^m (d')^n$ .

*Proof.* Recall:  $L \cap L' = K \Rightarrow [LL' : K] = nm$  and  $\{\omega_i \omega'_j\}$  is a basis of the field extension  $LL'/K$ .

$\text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$  and  $\text{Gal}(L'/K) = \{\sigma'_1, \dots, \sigma'_m\}$

$\Rightarrow$  obtain unique lifts  $\hat{\sigma}_i \in \text{Gal}(LL'/L')$  and  $\hat{\sigma}'_j \in \text{Gal}(LL'/L)$  and  $\text{Gal}(LL'/K) = \{\hat{\sigma}_i \hat{\sigma}'_j \mid i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$ .

Consider:  $\alpha \in \tilde{B} :=$  integral closure of  $A$  in  $LL'$ .

Write  $\alpha = \sum_{i,j} \alpha_{i,j} \omega_i \omega'_j = \sum_j \beta_j \omega'_j$  with  $\alpha_{i,j} \in K$  and  $\beta_j = \sum_i \alpha_{i,j} \omega_i \in L$ .

$\Rightarrow \hat{\sigma}'_i(\alpha) = \sum_j \beta_j \hat{\sigma}'_i(\omega'_j)$ , since  $\hat{\sigma}'_i \in \text{Gal}(LL'/L)$ .

$\Rightarrow$  We have a linear system:

$$a = Tb \text{ with } a = \begin{pmatrix} \hat{\sigma}'_1(\alpha) \\ \vdots \\ \hat{\sigma}'_m(\alpha) \end{pmatrix} \in \tilde{B}^m, \quad b = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} \in L^m, \quad T = (\hat{\sigma}'_i(\omega'_j))_{(i,j)} \in \tilde{B}^{m \times m}$$

Observe:  $\det(T)^2 = d'$

$\Rightarrow \det(T)b = T^\# T b = T^\# a \in \tilde{B}^m \Rightarrow d'b \in \tilde{B}^m$

$$\Rightarrow \forall j : d'\beta_j = \sum_i d'\alpha_{i,j}\omega_i \in \tilde{B} \cap L = B$$

$\Rightarrow d'\alpha_{i,j} \in A$ , since  $\{\omega_1, \dots, \omega_n\}$  is an integral basis.

$\Rightarrow d\alpha_{i,j} \in A$  in the same way

$$\Rightarrow \alpha_{i,j} = (x'd' + xd)\alpha_{i,j} = x'd'\alpha_{i,j} + xd\alpha_{i,j} \in A.$$

Hence:  $\{\omega_i\omega'_j \mid (i,j) \in \{(1,1), \dots, (n,m)\}\}$  is an integral basis of  $\tilde{B}/A$ .

For calculating the discriminant consider the matrix  $M = (\hat{\sigma}_k \circ \hat{\sigma}'_l(\omega_i\omega'_j))_{(k,l),(i,j)} = (\hat{\sigma}_k(\omega_i)\hat{\sigma}'_l(\omega'_j))$ .

Consider  $Q = (\hat{\sigma}_k(\omega_i))$

$$\Rightarrow M = \begin{pmatrix} Q & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & Q \end{pmatrix} \cdot \begin{pmatrix} I \cdot \hat{\sigma}'_1(\omega'_1) & \dots & I \cdot \hat{\sigma}'_1(\omega'_1) \\ \vdots & & \vdots \\ \vdots & & \vdots \\ I \cdot \hat{\sigma}'_m(\omega'_m) & \dots & I \cdot \hat{\sigma}'_m(\omega'_m) \end{pmatrix}$$

Observe:

$$(1) \det(Q)^2 = d(\omega_1, \omega_n) = d$$

$$(2) \text{ The second matrix can be transformed by switching rows and columns to } \begin{pmatrix} Q' & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & Q' \end{pmatrix}$$

with  $Q' = (\hat{\sigma}'_l(\omega'_j))$  and  $\det(Q') = d'$

$$\Rightarrow \det(M)^2 = \det(Q)^{2m} \cdot \det(Q')^{2n} = d^m d'^n. \quad \square$$

*Remark 2.2.15* (and Definition). Suppose  $K = \mathbb{Q}$ ,  $A = \mathbb{Z}$ ,  $L$  a number field and  $B = \mathcal{O}_K$ .

(i) There is always an integral basis  $w_1, \dots, w_n$ .

(ii) The **discriminant**  $d_K = d_K(\mathcal{O}_K) = d(w_1, \dots, w_n)$  does not depend on the choice of integral basis.

*Proof.* “(i)” Proposition 2.12 “(ii)” Let  $w'_1, \dots, w'_n$  be another integral basis. Then there exists a base change matrix  $T \in \text{GL}_n(\mathbb{Z})$  with

$$\begin{pmatrix} w'_1 \\ \vdots \\ w'_n \end{pmatrix} = T \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}.$$

Hence

$$\begin{pmatrix} \sigma(w'_1) \\ \vdots \\ \sigma(w'_n) \end{pmatrix} = T \begin{pmatrix} \sigma(w_1) \\ \vdots \\ \sigma(w_n) \end{pmatrix}.$$

such that

$$d(w'_1, \dots, w'_n) = \underbrace{\det T}_{\in \{1, -1\}}^2 d(w_1, \dots, w_n) = d_k.$$

□

*Example 2.2.16.* Let  $L = \mathbb{Q}(\sqrt{D})$  with  $D \in \mathbb{Z}$  square-free. By Proposition 2.14 we have:

- (i)  $\mathcal{O}_k = \mathbb{Z}[\sqrt{D}]$  and  $\{1, \sqrt{D}\}$  is an integral basis for  $D \equiv 2, 3 \pmod{4}$  and  $d_k = 4D$ .
- (ii)  $\mathcal{O}_k = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$  and  $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$  is an integral basis for  $D \equiv 1 \pmod{4}$  and  $d_k = D$ .

In particular, this holds for  $D = -1$ , i.e., the Gaussian integers  $\mathbb{Z}[i]$ .

## 2.3 Ideals

Let  $R$  be a commutative ring with 1.

**Problem:**  $\mathcal{O}_k$  is not a UFD in many cases, e.g. in  $\mathbb{Z}[\sqrt{-5}]$  we have

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

that is, two different ways to factor 6 in irreducible elements.

**Idea:**

- (1) Maybe we have too few elements, i.e.,

$$1 + \sqrt{-5} = p_1 p_2, 1 - \sqrt{-5} = p_3 p_4 \text{ and } 2 = p_2 p_3, 3 = p_1 p_4$$

for some primes  $p_i$ .

- (2) An element is determined (up to units) by the set of elements it divides, e.g.

$$p_i \longleftrightarrow \{x \in \mathcal{O}_k; p_i | x\} = p_i \mathcal{O}_k \text{ (this is an ideal)}.$$

**Notation 2.3.1.** Let  $I, J \subset R$  be ideals. We define

- $I + J = \{a + b; a \in I, b \in J\}$ ,
- $IJ = \{\sum_i a_i b_i; a_i \in I, b_i \in J\}$ .

**Definition 2.3.2** (and Reminder). Let  $I \subsetneq R$  be an ideal.

- (a)  $I$  is called **prime** if for all  $a, b \in R$  with  $ab \in I$  we already have  $a \in I$  or  $b \in I$ .  
 $\Leftrightarrow$  For all ideals  $A, B \subset R$  with  $AB \subset I$  we have  $A \subset I$  or  $B \subset I$ .
- (b)  $I$  is called **maximal** if for any ideal  $I \subset J \subset R$  we have  $J = I$  or  $J = R$ .  
 $\Leftrightarrow R/I$  is a field.
- (c)  $R$  is called **Noetherian** if every ascending chain of ideals

$$I_1 \subset I_2 \subset \dots$$

becomes stationary, i.e., if there is an  $N \in \mathbb{N}$  such that  $I_n = I_N$  for all  $n \geq N$ .

$\Leftrightarrow$  Every ideal in  $R$  is finitely generated.

- (d)  $R$  is called a **Dedekind domain** if
- $R$  is an integral domain,
  - $R$  is integrally closed,
  - $R$  is Noetherian, and
  - every prime ideal in  $R$  is maximal.

**Proposition 2.3.3.** *If  $\mathcal{O}$  is the integral closure of  $\mathbb{Z}$  in a number field then  $\mathcal{O}$  is a Dedekind domain.*

*Proof.* It is clear that  $\mathcal{O}$  is an integral domain and integrally closed. Furthermore, by Proposition 2.12 each  $\mathbb{Z}$ -submodule is finitely generated as a  $\mathbb{Z}$ -module, thus also as an  $\mathcal{O}$ -module. Hence  $\mathcal{O}$  is Noetherian.

Now, let  $I \subset \mathcal{O}$  be a prime ideal. Then  $I \cap \mathbb{Z} \subset \mathbb{Z}$  is a prime ideal such that  $\mathbb{Z}/(I \cap \mathbb{Z}) = \mathbb{F}_p$ . Using  $\mathcal{O} = \mathbb{Z}[w_1, \dots, w_n]$  we conclude

$$\mathcal{O}/I = \mathbb{Z}/(I \cap \mathbb{Z})[w'_1, \dots, w'_n] = \mathbb{F}_p[w'_1, \dots, w'_n] = \mathbb{F}_p(w'_1, \dots, w'_n),$$

where  $w'_i \equiv w_i \pmod{I}$ . Thus  $\mathcal{O}/I$  is a field and hence  $I$  maximal. □

**From now on:** Let  $\mathcal{O}$  denote a Dedekind domain.

**Theorem 4.** *Every ideal  $0 \neq I \subset \mathcal{O}$  has a unique factorization*

$$I = P_1 \cdots P_n$$

*into prime ideals  $P_i \subset \mathcal{O}$ .*

**Lemma 2.3.4.** *For every ideal  $0 \neq I \subset \mathcal{O}$  there exist nonzero prime ideals  $P_i \subset \mathcal{O}$  such that*

$$P_1 \cdots P_n \subset I.$$

*Proof.* Set  $M = \{0 \neq I \subset \mathcal{O} \text{ ideal; } I \text{ does not have such } P_i\}$  and suppose  $M \neq \emptyset$ . Then  $M$  is partially ordered by inclusion and since  $\mathcal{O}$  is Noetherian, every chain in  $M$  has an upper bound. Thus, the Lemma of Zorn yields a maximal element  $I_0 \in M$ . Since  $I_0$  cannot be prime there are  $a, b \in \mathcal{O}$  such that  $ab \in I_0$  but  $a, b \notin I_0$ . Consider the ideals  $I_1 = (a) + I_0$  and  $I_2 = (b) + I_0$  which satisfy  $I_0 \subsetneq I_1$ ,  $I_0 \subsetneq I_2$  and  $I_1 I_2 \subset I_0$ . Since  $I_0$  is a maximal ideal in  $M$ , we have  $I_{1,2} \notin M$  hence we find prime ideals  $P_1, \dots, P_n, P'_1, \dots, P'_m \subset \mathcal{O}$  with

$$P_1 \dots P_n \subset I_1 \text{ and } P'_1 \dots P'_m \subset I_2.$$

Finally, we conclude  $P_1 \dots P_n P'_1 \dots P'_m = I_1 I_2 \subset I_0 \Rightarrow I_0 \notin M \nRightarrow M = \emptyset$ .  $\square$

**Lemma 2.3.5.** Let  $0 \neq P \subset \mathcal{O}$  be a prime ideal,  $I \subset \mathcal{O}$  an ideal and  $K = \text{Quot}(\mathcal{O})$ . Then:

$$(i) \ P^{-1} := \{x \in K; xP \subset \mathcal{O}\} \supsetneq \mathcal{O}$$

$$(ii) \ I \subsetneq P^{-1}I := \{\sum_i a_i x_i; a_i \in I, x_i \in P^{-1}\}$$

*Proof.* “(i)” Let  $0 \neq a \in P$ ,  $P_1 \dots P_n \subset (a) \subset P$  as in Lemma 3.5 with  $n$  minimal.

**Claim:** Without loss of generality we can assume that  $P_1 = P$ .

**Proof of the claim:** Since  $P_1 \dots P_n \subset P$  and  $P$  is prime, there is an index  $i$  such that  $P_i \subset P$ , by reindexing we may assume that  $i = 1$ . However, we assumed  $\mathcal{O}$  to be Dedekind, hence  $P_1$  is a maximal ideal in  $\mathcal{O}$ . Thus,  $P_1 \subset P \subsetneq \mathcal{O}$  implies that  $P_1 = P$  as claimed.

Now, since  $n$  was chosen minimal we have  $P_2 \dots P_n \not\subset (a)$ , i.e., there exists an element  $b \in (a) \setminus P_2 \dots P_n$ . On the one hand we thus have

$$a^{-1}b \notin \mathcal{O}$$

and on the other hand  $bP \subset (a)$  such that  $a^{-1}bP \subset \mathcal{O}$  and hence

$$a^{-1}b \in P^{-1}.$$

Both of this together shows that  $P^{-1} \supsetneq \mathcal{O}$ .

“(ii)” Assume there is an ideal  $I \subset \mathcal{O}$  such that  $P^{-1}I \subset I$ . Let  $\{\alpha_1, \dots, \alpha_n\} \subset I$  be a generating set and choose  $x \in P^{-1} \setminus \mathcal{O}$ . Then,

$$x\alpha_i = \sum_j a_{ij}\alpha_j$$

for some  $a_{ij} \in \mathcal{O}$ . Consider the matrix  $A = xE_n - (a_{ij})_{i,j}$ , which satisfies

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0.$$

Since  $A^\# A = \det A$  we conclude  $\det A = 0$  such that  $x$  is a zero of the monic polynomial  $\det(XE_n - (a_{ij})_{i,j})$  over  $\mathcal{O}$ . But since  $\mathcal{O}$  is integrally closed this implies  $x \in \mathcal{O}$ , a contradiction.  $\square$



*Proof of Theorem 3.4. Existence of a factorization:* Let

$$M = \{0 \neq I \subset \mathcal{O} \text{ ideal}; I \text{ has no factorization}\}$$

and assume that  $M \neq \emptyset$ . As in Lemma 3.5, let  $I_0 \in M$  be a maximal element and let  $P \supset I_0$  be a maximal ideal containing  $I_0$ . Since  $I_0$  is not prime we have  $I_0 \neq P$  such that by Lemma 3.6,

$$I_0 \subsetneq P^{-1}I_0 \subset P^{-1}P = \mathcal{O}.$$

Note that  $I_0 = I_0\mathcal{O} = I_0P^{-1}P$  and  $I_0 \neq P$  imply  $P^{-1}I_0 \subsetneq \mathcal{O}$ . Since  $I_0$  was maximal in  $M$  we thus have  $P^{-1}I_0 \notin M$ , i.e., there are prime ideals  $P_1, \dots, P_n \subset \mathcal{O}$  with  $P^{-1}I = P_1 \cdots P_n$ . This leads to the contradiction  $I = PP_1 \cdots P_n$ .

**Uniqueness of the factorization:** Suppose that

$$I = P_1 \cdots P_n = Q_1 \cdots Q_m$$

are two prime factorizations. Then  $P_1 \supset I = Q_1 \cdots Q_m$ , hence without loss of generality we can assume that  $Q_1 \subset P_1$ . Since  $\mathcal{O}$  is Dedekind we conclude  $Q_1 = P_1$  such that

$$P_2 \cdots P_n = P_1^{-1}I = Q_2 \cdots Q_m.$$

The claim follows by induction. □

**Definition 2.3.6.** We call two ideals  $0 \neq I, J \subset \mathcal{O}$  **coprime**  $:\Leftrightarrow I + J = \mathcal{O}$ . For example, one could take two distinct prime ideals in a Dedekind ring.

*Remark 2.3.7.* Let  $P_1, \dots, P_n \subset \mathcal{O}$  be pairwise coprime. Then  $P_1$  and  $P_2 \cdots P_n$  are coprime and we have  $\prod_{i=1}^n P_i = \bigcap_{i=1}^n P_i$ .

*Proof.* Induction on  $n$ : The case  $n = 2$  is clear. Let  $n > 2$ . Since  $P_1$  and  $P_2$  are coprime,  $\exists p_1 \in P_1, p_2 \in P_2$ , such that we can write  $1 = p_1 + p_2$ . By induction hypothesis,  $\exists p'_1 \in P_1, p \in P_3 \cdots P_n$ , such that  $1 = p'_1 + p$ . It follows

$$1 = p_1 + p_2 \cdot (p'_1 + p) = \underbrace{p_1 + p_2 p'_1}_{\in P_1} + \underbrace{p_2 p}_{\in P_2 \cdots P_n},$$

which yields the first claim.

For the second claim, first note that  $\prod P_i \subset \bigcap P_i$  is clear.

For the converse, let  $a \in \bigcap P_i$ , which of course implies that  $a \in P_i$  for all  $i$ . As above, we write  $1 = p_1 + p$ ,  $p_1 \in P_1, p \in P_2 \cdots P_n$ . We get  $a = ap_1 + ap$ , which implies that  $a \in aP_1 + P_1 \cdot \prod_{i=2}^n P_i$  for all  $i$  and by induction hypothesis, we get  $a \in \prod P_i$ . □

**Theorem 5** (Chinese Remainder Theorem). *Let  $P_1, \dots, P_n \subset \mathcal{O}$  be pairwise coprime ideals,  $I = \bigcap_{i=1}^n P_i$ . Then we have*

$$\mathcal{O}/I \cong \bigoplus_{i=1}^n \mathcal{O}/P_i$$

*Proof.* Consider the map

$$\phi : \mathcal{O} \longrightarrow \bigoplus_i \mathcal{O}/P_i, \quad a \mapsto \bigoplus_i a \pmod{P_i}.$$

Obviously,  $\ker(\phi) = I$ . It remains to show, that  $\phi$  is surjective. Let first  $n = 2$ : For  $p_1 \in P_1, p_2 \in P_2$  let  $1 = p_1 + p_2$  and for any  $a_1, a_2 \in \mathcal{O}$  write  $a = a_2 p_1 + a_1 p_2$ . Then  $\phi(a) = a_1 \oplus a_2 \in \mathcal{O}/P_1 \oplus \mathcal{O}/P_2$ .

In general, by **3.8**, we know that  $\exists y_i \in \mathcal{O}$  with  $y_i \equiv 1 \pmod{P_i}$  and  $y_i \equiv 0 \pmod{\bigcap_{j \neq i} P_j}$ . Hence the element  $a = \sum_{i=1}^n a_i y_i$  is mapped to  $\bigoplus_{i=1}^n a_i \pmod{P_i}$   $\square$

**Definition 2.3.8.** A **fractional ideal** of  $K$  is a finitely generated  $\mathcal{O}$ -module  $0 \neq I$  of  $K$ . Since  $\mathcal{O}$  is noetherian, this is equivalent to:  $\exists c \in \mathcal{O}$ , such that  $c \cdot I \subset \mathcal{O}$  is an ideal (since every submodule of  $\mathcal{O}$  is finitely generated). The product of two fractional ideals is denoted in the same way as introduced in **3.3**. Ideals in  $\mathcal{O}$  are called **integral ideals**.

**Theorem 6.** *The fractional ideals of  $K$ , together with the product, form an abelian group, which we denote by  $\mathcal{J}_K$ .*

*Proof.* Commutativity and associativity are clear. The unit in  $\mathcal{J}_K$  is given by  $\mathcal{O}$ . We define  $I^{-1} := \{x \in K \mid x \cdot I \subset \mathcal{O}\}$  and show, that this defines an inverse for all  $I \in \mathcal{J}_K$ .

For a prime ideal  $P \subset \mathcal{O}$ , we have already seen in **3.4** that  $P^{-1}P = \mathcal{O}$  and for an integral ideal  $I = P_1 \cdots P_n$ , we have  $J = P_1^{-1} \cdots P_n^{-1}$  as an inverse:

$J \subset I^{-1}$  is clear. For the converse, let  $x \in I^{-1}$ , we then have  $x \cdot IJ \subset \mathcal{O}$ , with  $x \cdot I \subset \mathcal{O}$  and  $IJ = \mathcal{O}$ , therefore  $x \cdot 1 \in J$  and  $I^{-1} \subset J$  follows.

Let now  $I$  be fractional. Then  $\exists c \in \mathcal{O}$ , such that  $cI$  is integral. But then  $(cI)^{-1} = c^{-1}I^{-1}$  and hence  $II^{-1} = (cI)(c^{-1}I^{-1}) = \mathcal{O}$   $\square$

**Corollary 2.3.9.** *Every fractional ideal  $I$  has a unique factorization  $I = \prod P_i^{n_i}$ , with  $n_i \in \mathbb{Z}$ ,  $P_i \subset \mathcal{O}$  distinct prime ideals and only finitely many  $n_i \neq 0$ . In particular,  $\mathcal{J}_K$  is a free abelian group on the prime ideals of  $\mathcal{O}$ .*

*Proof.* By **3.11**, every element  $I \in \mathcal{J}_K$  can be written as  $I = AB^{-1}$  for some integral ideals  $A, B \subset \mathcal{O}$ . Therefore, by **3.4**, we get  $I = \prod P_i^{n_i}$  and by multiplying denominators, we see that this presentation is unique.  $\square$

**Definition 2.3.10.** The principle ideals generate a subgroup  $\mathcal{P}_K$  of  $\mathcal{J}_K$ . We call the quotient group  $\text{Cl}_K := \mathcal{J}_K/\mathcal{P}_K$  the **ideal class group**. We have an exact sequence of groups

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow K^\times \xrightarrow{a \mapsto a\mathcal{O}} \mathcal{J}_K \longrightarrow \text{Cl}_K \longrightarrow 1.$$

## 2.4 Lattices and Minkowski

**Definition 2.4.1.** Let  $V$  be an  $n$ -dimensional  $\mathbb{R}$ -vector space. A **lattice**  $\Lambda \subset V$  is a subgroup of the form  $\mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$ , where  $v_1, \dots, v_m$  are linearly independent over  $V$ . We call  $(v_1, \dots, v_m)$  a **basis** of  $\Lambda$  and  $\phi := \{x_1v_1 + \dots + x_mv_m \mid x_i \in [0, 1)\}$  a **fundamental domain** of  $\Lambda$ . We call  $\Lambda$  **complete**, if  $n = m$ .

**CAUTION:** For many people, lattices are always complete!

*Example 2.4.2.* (a)  $\mathbb{Z} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{Z} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \subset \mathbb{R}^2$  is a complete lattice

(b)  $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$  is not a lattice, since 1 and  $\sqrt{2}$  are not linearly independent.

(c)  $\mathbb{Z} \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} \subset \mathbb{R}^2$  is a non-complete lattice.

**Proposition 2.4.3.** A subgroup  $\Lambda \subset V$  is a lattice  $\Leftrightarrow \Lambda$  is a discrete subgroup of  $V$ .

*Proof.* " $\Rightarrow$ ": Take  $\{\lambda + x_1v_1 + \dots + x_nv_n + \text{rest of basis} \mid |x_n| < 1\}$  as a neighbourhood for  $\lambda \in \Lambda$ .

" $\Leftarrow$ ": Let  $V_0 = \langle \Lambda \rangle_{\mathbb{R}}$ . Then we can choose a basis  $v_1, \dots, v_m$  of  $V_0$  in  $\Lambda$ , such that  $\Lambda_0 := \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$  is a lattice in  $V_0$ .

**Claim:** The index  $[\Lambda : \Lambda_0]$  is finite.

**Proof of the claim:** Since  $\Lambda_0$  is complete,  $V = \bigsqcup_{\lambda \in \Lambda_0} \phi_0 + \lambda$ . Since  $\Lambda$  is discrete and  $\phi_0$  bounded,  $\Lambda \cap \phi_0$  is finite. Hence we have only finitely many residue classes  $\lambda + \Lambda_0$  of  $\Lambda$  and therefore  $[\Lambda : \Lambda_0] =: d < \infty$ .

From this follows, that  $\Lambda \subset \frac{1}{d}\Lambda_0 = \mathbb{Z}(\frac{1}{d}v_1) + \dots + \mathbb{Z}(\frac{1}{d}v_m)$ . Therefore,  $\Lambda$  has a  $\mathbb{Z}$ -basis  $w_1 = v_1n_1, \dots, w_r = v_rn_r$  for some  $n_i \in \frac{1}{d}\mathbb{N}$  and since  $\Lambda$  spans  $V_0$ , we get  $r = m$  and they are linearly independent.  $\square$

Let  $\Gamma = v_1\mathbb{Z} + \dots + v_n\mathbb{Z} \subset \mathbb{R}^n$  be a complete lattice. We define

$$\text{vol } \Gamma = \text{vol } \phi = |\det(v_1, \dots, v_n)|.$$

Note that this definition is independent of the chosen basis since for a transformation

$$A(v_1, \dots, v_n) = (v'_1, \dots, v'_n)$$

between two bases we have  $\det A = \pm 1$ .

**Theorem 7** (Minkowski). Let  $X \subset \mathbb{R}^n$  be a convex, symmetric central (i.e.,  $x \in X$  implies  $-x \in X$ ) subset and let  $\Gamma \subset \mathbb{R}^n$  be a complete lattice. If

$$\text{vol } X > 2^n \text{vol } \Gamma$$

then there exists some  $\gamma \in \Gamma \setminus \{0\}$  such that  $\gamma \in X$ .

*Proof.* **Claim:** It suffices to show that there are  $\gamma_1, \gamma_2 \in \Gamma$ ,  $\gamma_1 \neq \gamma_2$ , such that

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

**Proof of claim:** Let  $x = \frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$  with some  $x_1, x_2 \in X$ . Then

$$y = \frac{1}{2}(x_1 - x_2) = \gamma_2 - \gamma_1 \in \Gamma \setminus \{0\}$$

with  $y \in X$  since  $X$  is symmetrical central.

Now let us assume that the family  $\left(\frac{1}{2}X + \gamma\right)_{\gamma \in \Gamma}$  is pairwise disjoint. Then

$$\left(\left[\frac{1}{2}X + \gamma\right] \cap \phi\right)_{\gamma \in \Gamma}$$

also consists of pairwise disjoint sets such that we obtain the contradiction

$$\begin{aligned} \text{vol } \Gamma = \text{vol } \phi &\geq \sum_{\gamma \in \Gamma} \text{vol} \left( \left[\frac{1}{2}X + \gamma\right] \cap \phi \right) = \sum_{\gamma \in \Gamma} \text{vol} \left( \frac{1}{2}X \cap [\phi - \gamma] \right) \\ &= \text{vol} \left( \frac{1}{2}X \right) = \frac{1}{2^n} \text{vol } X. \end{aligned}$$

□

## 2.5 Minkowski theory

Let  $[K : \mathbb{Q}] = n$  be a field extension,  $\tau_i: K \hookrightarrow \mathbb{C}$  different embeddings and consider the embedding

$$j: K \hookrightarrow K_{\mathbb{C}} = \prod_{\tau_i} \mathbb{C}, \quad a \mapsto (\tau_1(a), \dots, \tau_n(a)).$$

Define a hermitian scalar product on  $K_{\mathbb{C}}$  by

$$\langle (x_{\tau_i}), (y_{\tau_i}) \rangle = \sum_{\tau_i} x_{\tau_i} \overline{y_{\tau_i}}$$

and consider the complex conjugation  $F \in \text{Gal}(\mathbb{C}/\mathbb{R})$  given by  $\mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$ . Let

$$F(\tau) = \bar{\tau}: a \mapsto \overline{\tau(a)}$$

and extend it to  $K_{\mathbb{C}}$  by

$$F: K_{\mathbb{C}} \rightarrow K_{\mathbb{C}}, (x_{\tau}) \mapsto (\bar{x}_{\bar{\tau}}).$$

*Example.* Let  $D > 0$  be square-free. Consider

$$\mathbb{Q}(\sqrt{D}) \hookrightarrow \mathbb{Q}(\sqrt{D})_{\mathbb{C}} = \prod_{\tau_i} \mathbb{C}$$

with

$$\tau_1(a + b\sqrt{D}) = a + b\sqrt{D} \quad \text{and} \quad \tau_2(a + b\sqrt{D}) = a - b\sqrt{D}.$$

Then

$$j(a + b\sqrt{D}) = (a + b\sqrt{D}, a - b\sqrt{D})$$

and  $F(\tau_1) = \tau_1, F(\tau_2) = \tau_2$  such that

$$F(x_{\tau_1}, x_{\tau_1}) = (\bar{x}_{\tau_1}, \bar{x}_{\tau_2}).$$

*Remark.* •  $F(\langle x, y \rangle) = \langle F(x), F(y) \rangle$

•  $\text{Tr}: K_{\mathbb{C}} \rightarrow \mathbb{C}, (x_{\tau}) \mapsto \sum_{\tau} x_{\tau}$  such that  $(\text{Tr} \circ j)(a) = \text{Tr}_{K/\mathbb{Q}}(a)$

Now define the  $F$ -invariant  $\mathbb{R}$ -vector space

$$K_{\mathbb{R}} = K_{\mathbb{C}}^+ = \{x \in K_{\mathbb{C}} \mid F(x) = x\} = \{x \in K_{\mathbb{C}} \mid x_{\bar{\tau}} = \overline{x_{\tau}} \text{ for all } \tau\}.$$

Since  $\bar{\tau}(a) = \overline{\tau(a)}$  for all  $a \in K$  and all  $\tau$ , we have  $j(K) \subset K_{\mathbb{R}}$ . We call  $K_{\mathbb{R}}$  the **Minkowski space** and  $\langle \cdot, \cdot \rangle|_{K_{\mathbb{R}}}$  the **canonical metric**.

*Remark.* Note that  $j: K \rightarrow K_{\mathbb{R}} \cong K \otimes_{\mathbb{Q}} \mathbb{R}$ , where the isomorphism is given by  $a \otimes x \mapsto j(a)x$  for  $x \in \mathbb{R}$ .

**Explicit description of  $K_{\mathbb{R}}$ :** Let  $n = r + 2s$ , where  $r$  and  $s$  are the number of embeddings

$$\varphi_1, \dots, \varphi_r: K \hookrightarrow \mathbb{R}$$

and

$$\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s}: K \hookrightarrow \mathbb{C},$$

respectively. Notice that  $F(\varphi_i) = \varphi_i$  and  $F(\sigma_j) = \overline{\sigma_j}$ . Then elements of  $K_{\mathbb{C}}$  are of the form

$$x = (x_{\varphi(1)}, \dots, x_{\varphi(r)}, x_{\sigma_1}, x_{\overline{\sigma_1}}, \dots, x_{\sigma_s}, x_{\overline{\sigma_s}})$$

with

$$F(x) = (\overline{x_{\varphi_1}}, \dots, \overline{x_{\varphi_r}}, \overline{x_{\sigma_1}}, \overline{x_{\sigma_1}}, \dots, \overline{x_{\sigma_s}}, \overline{x_{\sigma_s}}).$$

Hence we have

$$K_{\mathbb{R}} = \{x \in K_{\mathbb{C}} \mid x_{\varphi_i} \in \mathbb{R}, x_{\overline{\sigma_j}} = \overline{x_{\sigma_j}}\}.$$

**Proposition 2.5.1.** *The map*

$$f: K_{\mathbb{R}} \xrightarrow{\cong} \mathbb{R}^{r+2s} = \prod_{\tau} \mathbb{R},$$

$$x \mapsto (x_{\varphi_1}, \dots, x_{\varphi_r}, \operatorname{Re} x_{\sigma_1}, \operatorname{Im} x_{\sigma_1}, \dots, \operatorname{Re} x_{\sigma_s}, \operatorname{Im} x_{\sigma_s}).$$

*is an isomorphism. It transforms the canonical metric into the scalar product*

$$\langle x, y \rangle = \sum_{\tau} \alpha_{\tau} x_{\tau} y_{\tau},$$

*where*

$$\alpha_{\tau} = \begin{cases} 1, & \tau = \varphi_i \text{ for some } i, \\ 2, & \tau = \sigma_j \text{ for some } j. \end{cases}$$

*Proof.* Obviously,  $f$  is an isomorphism. For  $x = (x_{\tau}), y = (y_{\tau}) \in K_{\mathbb{R}}$  we have

$$\begin{aligned} \langle x, y \rangle|_{K_{\mathbb{R}}} &= \sum_{\tau} x_{\tau} \overline{y_{\tau}} \\ &= \sum_{\varphi_i} x_{\varphi_i} y_{\varphi_i} + \sum_{\sigma_j} x_{\sigma_j} \overline{y_{\sigma_j}} + \sum_{\overline{\sigma_j}} \overline{(x_{\sigma_j} y_{\sigma_j})} \\ &= \dots = (f(x), f(y)). \end{aligned}$$

□

*Remark.* • The canonical metric induces a volume  $\operatorname{vol}_{\text{can}}$  on  $K_{\mathbb{R}}$  and thus on  $\mathbb{R}^{r+2s}$ .

- If we denote the Lebesgue measure on  $\mathbb{R}^{r+2s}$  by  $\operatorname{vol}_{\text{Leb}}$  then, for  $X \subset K_{\mathbb{R}}$ ,

$$2^s \operatorname{vol}_{\text{Leb}} f(X) = \operatorname{vol}_{\text{can}} X.$$

- We will thus consider  $K \supset U \xrightarrow{j} j(U) \xrightarrow{f} \mathbb{R}^{r+2s}$ .

*Example.* Let  $e_j = (0, \dots, 1, \dots, 0)$ . Note that we have  $\langle e_{\varphi_i}, e_{\varphi_i} \rangle = 1$  and  $\langle e_{\sigma_j}, e_{\varphi_j} \rangle = 2$ , such that  $\langle \frac{e_{\sigma_j}}{\sqrt{2}}, \frac{e_{\sigma_j}}{\sqrt{2}} \rangle = 1$ . Hence

$$\left\{ e_{\varphi_1}, \dots, e_{\varphi_r}, \frac{e_{\sigma_1}}{\sqrt{2}}, \frac{e_{\overline{\sigma_1}}}{\sqrt{2}}, \dots \right\}$$

is an orthonormal basis. Using the correspondence

$$X \subset K_{\mathbb{R}} \leftrightarrow f(X) \subset \mathbb{R}^{r+2s}$$

we thus define

$$\operatorname{vol}_{\text{can}} X = \operatorname{vol}_{\text{can}} f(X) = 2^s \operatorname{vol}_{\text{Leb}} f(X).$$

**Proposition 2.5.2.** *If  $I \neq 0$  is an  $\mathcal{O}_k$ -ideal then  $\Gamma = j(I)$  is a complete lattice in  $K_{\mathbb{R}}$ . Its fundamental domain has volume*

$$\text{vol } \Gamma = \text{vol } \phi = \sqrt{|d_k|} \cdot [\mathcal{O}_k : I].$$

*Proof.* Choose  $\alpha_i$  such that  $I = \alpha_1\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$ . Then  $\Gamma = j(I) = j(\alpha_1)\mathbb{Z} + \cdots + j(\alpha_n)\mathbb{Z}$ . Define

$$A = (j(\alpha_1), \dots, j(\alpha_n))^T = \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \tau_1(\alpha_n) & \cdots & \tau_n(\alpha_n) \end{pmatrix}$$

such that

$$\text{vol } \phi = |\det A| = \sqrt{|d_k|} \cdot [\mathcal{O}_k : I].$$

Furthermore,

$$d(I) = d(\alpha_1, \dots, \alpha_n) = |\det A|^2 = d(\mathcal{O}_k) \cdot [\mathcal{O}_k : I]^2,$$

with  $[\mathcal{O}_k : I] = |\det M|$  for the change of basis  $M$  from  $\mathcal{O}_k$  to  $I$ .  $\square$

**Theorem 8.** *Let  $I \neq 0$  be an ideal in  $\mathcal{O}_k$ . Let  $(c_\tau)_\tau$  be a collection of real number such that  $c_\tau > 0$ ,  $c_\tau = c_{\bar{\tau}}$  and*

$$\prod_{\tau} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_k|} \cdot [\mathcal{O}_k : a].$$

*Then there exists  $a \in I \setminus \{0\}$  such that*

$$|\tau(a)| < c_\tau$$

*for all  $\tau \in \text{Hom}(K, \mathbb{C})$ .*

*Proof.* Consider the convex, central symmetric set

$$X = \{(x_\tau) \in K_{\mathbb{R}} \mid |x_\tau| < c_\tau \text{ for all } \tau\}$$

and let  $f: K_{\mathbb{R}} \rightarrow \mathbb{R}^n$ ,  $n = r + 2s$ , as in Proposition 5.1. Notice that for  $x \in X$  we have  $f(x) = (x_{\varphi_1}, \dots, x_{\varphi_r}, a_1, b_1, \dots, a_s, b_s)$  with  $|x_{\varphi_i}| < c_{\varphi_i}$  and  $a_j^2 + b_j^2 < c_{\sigma_j}^2$ . Hence

$$\text{vol}_{\text{can}} X = 2^s \text{vol}_{\text{Leb}} f(X) = 2^s \left( \prod_{i=1}^r 2c_{\varphi_i} \right) \left( \prod_{j=1}^s \pi c_{\sigma_j}^2 \right) = 2^{r+s} \pi^s \prod_{\tau} c_\tau,$$

and thus, by Proposition 5.2,

$$\begin{aligned} 2^n \text{vol } \Gamma &= 2^{r+2s} \sqrt{|d_k|} \cdot [\mathcal{O}_k : I] \\ &= 2^{r+s} \pi^s \left[ \left(\frac{2}{\pi}\right)^s \sqrt{|d_k|} \cdot [\mathcal{O}_k : a] \right] \\ &< 2^{r+s} \pi^s \prod_{\tau} c_\tau \\ &= \text{vol}_{\text{can}} X. \end{aligned}$$

Consequently, by Minkowski's theorem, there exists  $j(a) \in \Gamma \setminus \{0\}$  with  $j(a) \in X$  and  $|\tau(a)| < c_\tau$  for all  $\tau$ .  $\square$

## Multiplicative Minkowsky theory

Define

$$j: K^* \hookrightarrow K_{\mathbb{C}}^* = \prod_{\tau} \mathbb{C}^*, a \mapsto (\tau(a))_{\tau}$$

and

$$\mathcal{N}: K_{\mathbb{C}}^* \rightarrow \mathbb{C}^*, (x_{\tau}) \mapsto \prod_{\tau} x_{\tau}.$$

Denote the composition of these maps by  $\mathcal{N}_{K/\mathbb{Q}} = \mathcal{N} \circ j$ . Furthermore, consider

$$l: \mathbb{C}^* \rightarrow \mathbb{R}, z \mapsto \log |z|$$

and its extension

$$l: K_{\mathbb{C}}^* \rightarrow \prod_{\tau} \mathbb{R}, (x_{\tau}) \mapsto (\log |x_{\tau_1}|, \dots, \log |x_{\tau_n}|).$$

All in all, we have

$$\begin{array}{ccccc} K^* & \xrightarrow{j} & K_{\mathbb{C}}^* & \xrightarrow{l} & \prod_{\tau} \mathbb{R} \\ \mathcal{N}_{K/\mathbb{Q}} \downarrow & & \downarrow \mathcal{N} & & \downarrow \text{Tr} \\ \mathbb{Q}^* & \xrightarrow{i} & \mathbb{C}^* & \xrightarrow{l} & \mathbb{R} \end{array}$$

with

$$\left[ \prod_{\tau} \mathbb{R} \right]^+ = \prod_{\varphi_i} \mathbb{R} \times \prod_{\sigma_j} [\mathbb{R} \times \mathbb{R}]^+ \xrightarrow{\cong} \mathbb{R}^{r+s},$$

where the isomorphism is given by

$$(x_{\varphi_1}, \dots, x_{\varphi_r}, x_{\sigma_1}, x_{\overline{\sigma_1}}, \dots, x_{\sigma_s}, x_{\overline{\sigma_s}}) \mapsto (x_{\varphi_1}, \dots, x_{\varphi_r}, 2x_{\sigma_1}, \dots, 2x_{\sigma_s}),$$

and we have

$$K_{\mathbb{R}} \rightarrow \mathbb{R}^{r+s}, (x_{\tau}) \mapsto (\log |x_{\varphi_1}|, \dots, \log |x_{\varphi_r}|, \log |x_{\sigma_1}|^2, \dots, \log |x_{\sigma_s}|^2).$$

## 2.6 The class number

Let  $n = [K : \mathbb{Q}]$ , denote by  $J_K$  the group of fractional ideals of  $K$ , by  $P_k$  its subgroup of principal ideals and by  $\text{Cl}_k = J_k/P_k$  the ideal class group. Define the **absolute norm** of an ideal  $I \subset \mathcal{O}_k$  by

$$n(I) = [\mathcal{O}_k : I].$$

For  $I = (\alpha)$ , we have  $n(I) = \mathcal{N}_{K/\mathbb{Q}}(\alpha)$ . If  $\mathcal{O}_k = w_1\mathbb{Z} + \dots + w_n\mathbb{Z}$  and  $I = \alpha w_1\mathbb{Z} + \dots + \alpha w_n\mathbb{Z}$  we have

$$\alpha w_i = \sum_j a_{ij} w_j$$

for some matrix  $A = (a_{ij})$  such that  $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = |\det A| = [\mathcal{O}_k : I]$ .



**Proposition 2.6.1.** *If  $I = P_1^{\nu_1} \cdots P_r^{\nu_r}$  then  $n(I) = n(P_1)^{\nu_1} \cdots n(P_r)^{\nu_r}$ .*

*Proof.* By the Chinese remainder theorem,

$$\mathcal{O}_k/I \cong (\mathcal{O}_k/P_1^{\nu_1}) \oplus \cdots \oplus (\mathcal{O}_k/P_r^{\nu_r}),$$

such that

$$n(I) = [\mathcal{O}_k : I] = \prod_j [\mathcal{O}_k : P_j^{\nu_j}] = \prod_j n(P_j)^{\nu_j}.$$

**Claim:**  $P \supsetneq P^2 \supsetneq \cdots \supsetneq P^\nu$  and  $P^i/P^{i+1}$  is a  $(\mathcal{O}_k/P)$ -vector space of dimension 1

**Proof of Claim:** Let  $a \in P^i/P^{i+1}$ . Then we have

$$P^i \supset J = (a) + P^{i+1} \supsetneq P^{i+1}$$

and

$$\mathcal{O}_k \supset J' = JP^{-i} \supsetneq P = P^{i+1}P^{-i}.$$

Since  $J'|P$  we have  $J = P^i$  and thus  $[a] \in P^i/P^{i+1}$  is a basis.

Now, the Claim yields

$$n(P^\nu) = [\mathcal{O}_k : P^\nu] = [\mathcal{O}_k : P] [P : P^2] \cdots [P^{\nu-1} : P^\nu] n(P)^\nu.$$

□

In particular, for integral ideals  $I, J$  we have  $n(IJ) = n(I)n(J)$  such that we can extend  $n$  to  $J_k$  by

$$n: J_k \rightarrow \mathbb{R}_+^*, I = P_1^{\nu_1} \cdots P_r^{\nu_r} \mapsto n(I) = n(P_1)^{\nu_1} \cdots n(P_r)^{\nu_r}.$$

*Reminder 2.6.2.*  $\mathcal{J}_K$  = group of fractional ideals = abelian group generated by all prime ideals

$\mathcal{P}_K$  = group of all principal fractional ideals.

$\text{Cl}_K := \mathcal{J}_K/\mathcal{P}_K$

$\Rightarrow$  obtain following exact sequence:

$$1 \rightarrow \underbrace{\mathcal{O}_K^\times}_{\text{How big?}} \rightarrow K^\times \rightarrow \mathcal{J}_K \rightarrow \underbrace{\text{Cl}_K}_{\text{How big?}} \rightarrow 1$$

$$a \mapsto (a) = a\mathcal{O}_K$$

Last Time:  $\mathfrak{a}$  ideal in  $\mathcal{O}_K, \mathfrak{a} \neq 0$ .

- $\mathcal{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$  absolute norm.

In particular:  $\mathcal{N}((a)) := |\mathcal{N}_{K/\mathbb{Q}}(a)|$ .

- $\mathfrak{a} = \mathcal{P}_1^{\nu_1} \cdots \mathcal{P}_r^{\nu_r}$  decomposition into primes  
 $\Rightarrow \mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathcal{P}_1)^{\nu_1} \cdots \mathcal{N}(\mathcal{P}_r)^{\nu_r}$

In particular:  $\mathcal{N}(\mathfrak{a}_1\mathfrak{a}_2) = \mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)$ .

- Hence  $\mathcal{N}$  can be extended to fractional ideals:  $\mathcal{N} : \mathcal{J}_K \rightarrow \mathbb{R}_+^\times$ .

Goal: Show that  $\text{Cl}_K$  is finite.

Idea:

- Find in each integral ideal  $\mathfrak{a}$  an element  $a \neq 0$  of norm bounded by  $\mathcal{N}(\mathfrak{a})$ .
- Show: For  $M > 0$  there are only finitely many integral ideals  $\mathfrak{a}$  with  $\mathcal{N}(\mathfrak{a}) \leq M$ .
- Show: Each class  $[\mathfrak{a}] \in \text{Cl}_K$  contains an integral ideal  $\mathfrak{a}_1$  s.t.  $\mathcal{N}(\mathfrak{a}_1) \leq M_0 = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$ .  
Recall:  $s$  = number of not-real embeddings of  $K$  into  $\mathbb{C}$ .

**Lemma 2.6.3.** *Suppose:  $\mathfrak{a} \neq 0$  is an integral ideal  $\Rightarrow \exists a \in \mathfrak{a}, a \neq 0$  s.t.  $|\mathcal{N}_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \mathcal{N}(\mathfrak{a})$ .*

*Proof.*  $M_0 := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$

Idea: Use „Thm. 5.3“

given:  $c_\tau \in \mathbb{R}_{>0} (\tau \in \text{Hom}(K, \mathbb{C}))$  with  $c_\tau = c_{\bar{\tau}}$  and  $\prod_\tau c_\tau > M_0 \mathcal{N}(\mathfrak{a})$

$\Rightarrow \exists a \in \mathfrak{a}, a \neq 0$  with  $|\tau(a)| < c_\tau$  for all  $\tau$ .

For each  $\varepsilon > 0$  choose a sequence  $c_\tau \in \mathbb{R}_{>0}$  with  $c_\tau = c_{\bar{\tau}}$  and  $\prod_\tau c_\tau = M_0 \mathcal{N}(\mathfrak{a}) + \varepsilon$

$\xRightarrow{\text{Thm 5.3}}$  Find  $a_\varepsilon \neq 0$  in  $\mathfrak{a}$  with

$$|\mathcal{N}_{K/\mathbb{Q}}(a)| = \prod_\tau |\tau(a)| < M_0 \mathcal{N}(\mathfrak{a}) + \varepsilon$$

Since left side is integer, we obtain:  $\exists a \neq 0$  in  $\mathfrak{a}$  with  $|\mathcal{N}_{K/\mathbb{Q}}(a)| \leq M_0 \mathcal{N}(\mathfrak{a})$ .  $\square$

**Lemma 2.6.4.** *Let  $M \in \mathbb{R}_{>0}$ . There are only finitely many integral ideals  $\mathfrak{a}$  with  $\mathcal{N}(\mathfrak{a}) \leq M$ .*

*Proof.* (1) Consider first only prime ideals  $\mathcal{P} \neq 0$ : Suppose  $\mathcal{N}(\mathcal{P}) \leq M$

Recall:  $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$  with  $p$  prime number (Prop. 3.3)

$\Rightarrow$  obtain embedding  $\mathcal{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathcal{P} \Rightarrow \mathcal{N}(\mathcal{P}) = (\mathcal{O}_K : \mathcal{P}) = \#\mathcal{O}_K/\mathcal{P} = p^f$

Hence:  $p^f \leq M$ . In particular  $P$  is bounded.

Furthermore: There are only finitely many prime ideals  $\mathcal{P}$  with  $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ .

Since  $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z} \Rightarrow p \in \mathcal{P} \Rightarrow (p) \subseteq \mathcal{P}$  But there are only finitely many prime ideals in  $\mathcal{O}_K$  which divide  $(p)$ .

(2) Suppose now  $\mathfrak{a}$  is an arbitrary integral ideal,  $\mathfrak{a} \neq 0$ :

$\Rightarrow \mathfrak{a} = \mathcal{P}_1^{\nu_1} \cdots \mathcal{P}_r^{\nu_r}$  with  $\mathcal{P}_i$  prime ideal and  $\nu_i \in \mathbb{N}$  and  $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathcal{P}_1)^{\nu_1} \cdots \mathcal{N}(\mathcal{P}_r)^{\nu_r}$ .

Now the claim follows from (1).  $\square$

**Theorem 9** (Finiteness of  $\text{Cl}_K$ ). *The ideal class group of  $\text{Cl}_K = \mathcal{J}_K/\mathcal{P}_K$  is finite.*

*Proof.* Let  $M_0 := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$

Show that each class  $[\mathfrak{a}] \in \text{Cl}_K$  contains an integral ideal  $\mathfrak{a}_1$  with  $\mathcal{N}(\mathfrak{a}_1) \leq M_0$ . Then the

claim follows from Lemma 6.3.

Let  $[a] \in \text{Cl}_K$ . Choose  $\gamma \in \mathcal{O}_K, \gamma \neq 0$  with  $\gamma a^{-1}$  is integral.

$$\begin{aligned} \text{Lemma 6.2} &\Rightarrow \exists b \in \mathfrak{b} := \gamma a^{-1} \text{ with } b \neq 0 \text{ and } |\mathcal{N}_{K/\mathbb{Q}}(b)| \leq M_0 \mathcal{N}(\mathfrak{b}) \\ &\Rightarrow \mathcal{N}((b)\mathfrak{b}^{-1}) = \mathcal{N}((b))\mathcal{N}(\mathfrak{b}^{-1}) \leq M_0 \end{aligned}$$

Observe: The factorial ideal  $(b)\mathfrak{b}^{-1} = (b)\gamma^{-1}a \in [a]$ , hence  $a_1 := b\gamma^{-1}a$  does the job.  $a_1$  is an integral ideal, since  $(b) \subseteq \gamma a^{-1}$   $\square$

**Definition 2.6.5** („Klassenzahl“).  $h_K := \# \text{Cl}_K := (\mathcal{J}_K : \mathcal{P}_K)$  is called the class number of  $K$ .

**Proposition 2.6.6.** Suppose  $R$  is a Dedekind domain.

$R$  is a UFD  $\iff R$  is a PID (principal ideal domain).

*Proof.* „ $\Leftarrow$ “: true for general domains.

„ $\Rightarrow$ “: Suppose  $R$  is a UFD.

Step 1: Every prime ideal is principal.

Let  $\mathcal{P}$  be a prime ideal,  $\mathcal{P} \neq 0$ . Choose  $a \in \mathcal{P}, a \neq 0$ . Let  $a = p_1 \cdots p_n$  be its prime factor decomposition.  $\mathcal{P}$  prime  $\Rightarrow p_i \in \mathcal{P}$  for one of the  $i$ 's  $\Rightarrow \mathcal{P} \supseteq (p_i) \Rightarrow \mathcal{P} = (p_i)$ , since  $(p_i)$  is a prime ideal and  $R$  is a Dedekind domain.

Step 2:  $\mathfrak{a}$  arbitrary ideal.

$\Rightarrow \mathfrak{a} = \mathcal{P}_1 \cdots \mathcal{P}_n$  is a product of prime ideals

$\Rightarrow \mathfrak{a}$  is principal, since each  $\mathcal{P}_i$  is.  $\square$

**Corollary 2.6.7.** We have for a number field  $K$ :

$h_K = 1 \iff \mathcal{O}_K$  is a principal domain  $\iff \mathcal{O}_K$  is a UFD.

## 2.7 The theorem of Dirichlet

Goal: Describe  $\mathcal{O}_K^\times$

Recall:

- $\mathcal{O}^\times = \{\varepsilon \in \mathcal{O}_K \mid \mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = \pm 1\}$
- $\mu(K) := \{x \in \mathcal{O}_K \mid \exists n \in \mathbb{N} \text{ with } x^n = 1\} \subseteq \mathcal{O}_K^\times$  is a finite subgroup.

Idea: Use multiplicative Minkowsky theory:

- $\text{Hom}(K, \mathbb{C}) = \{\tau_1, \dots, \tau_r, \tau_{r+1}, \overline{\tau_{r+1}}, \tau_{r+s}, \overline{\tau_{r+s}}\}$
- $j : K^\times \hookrightarrow K_\mathbb{R}^\times = \{x \in \prod_\tau \mathbb{C}^\times \mid x_{\bar{\tau}} = \overline{x_\tau}\}, a \mapsto (\tau(a))_\tau$
- $l : K_\mathbb{R}^\times \rightarrow [\prod_\tau \mathbb{R}]^+ := \{z \in \prod_\tau \mathbb{R} \mid z_{\bar{\tau}} = z_\tau\}, x = (x_\tau) \mapsto (\log |x_\tau|)_\tau$

$\Rightarrow$  commutative diagramm:

$$\begin{array}{ccccc}
 \mathcal{O}_K^\times & & S & & H \\
 \downarrow \text{in} & & \downarrow \text{in} & & \downarrow \text{in} \\
 K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{l} & [\prod_{\tau} \mathbb{R}]^+ \\
 \downarrow \mathcal{N}_{K/\mathbb{Q}} & & \downarrow \mathcal{N} & & \downarrow \text{Tr} \\
 \mathbb{Q}^\times & \longrightarrow & \mathbb{R} & \xrightarrow{\log|\cdot|} & \mathbb{R}
 \end{array}$$

with  $\mathcal{N}(x) = \prod_{\tau} x_{\tau}$ ,  $\text{Tr}(z) = \sum_{\tau} z_{\tau}$ .

Consider the three groups:

- (1)  $\mathcal{O}_K^\times = \{\varepsilon \in \mathcal{O}_K \mid \mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = \pm 1\}$
- (2)  $S := \{x \in K_{\mathbb{R}}^\times \mid \mathcal{N}(x) = \pm 1\}$  „Norm 1 hyper surface“
- (3)  $H := \{z \in [\prod_{\tau} \mathbb{R}]^+ \mid \text{Tr}(z) = 0\}$  „Trace 0 hypersurface“

$\Rightarrow$  Morphisms restrict to

$$\mathcal{O}_K^\times \xrightarrow{j} S \xrightarrow{l} H.$$

Define  $\Gamma := l \circ j(\mathcal{O}_K^\times) = \text{image of } l \circ j$ .

Recall from additive Minkowski-Theory:  $j(\mathcal{O}_K)$  is a complete lattice in  $K_{\mathbb{R}}$

**Proposition 2.7.1.** *The sequence*

$$1 \rightarrow \mu(K) \rightarrow \mathcal{O}_K^\times \xrightarrow{l \circ j} \Gamma \rightarrow 1$$

*is an exact sequence.*

*Proof.*  $\lambda := l \circ j$

We have to show:  $\ker(\lambda) = \mu(K)$ .

Observe:  $a \in \ker(\lambda) \iff \forall \tau \in \text{Hom}(K, \mathbb{C}) : \log |\tau(a)| = 0 \iff |\tau(a)| = 1$

Hence:  $\ker(\lambda) = \{a \in \mathcal{O}^\times \mid |\tau(a)| = 1\}$ .

„ $\supseteq$ “:  $\checkmark$

„ $\subseteq$ “:  $j(\ker(\lambda))$  is bounded as subset of  $K_{\mathbb{R}}^\times$ . Furthermore:  $j(\ker(\lambda)) \subseteq j(\mathcal{O})$  which is a lattice in  $K_{\mathbb{R}} \Rightarrow j(\ker(\lambda))$  is finite and thus also  $\ker(\lambda)$ .

Altogether:  $\ker(\lambda)$  is a finite subgroup of  $K^\times \Rightarrow$  every element in  $\ker(\lambda)$  has finite order  $\Rightarrow$  every element is a root of unity.  $\square$

Goal: Describe  $\Gamma$

Recall:  $\alpha, \alpha' \in \mathcal{O}_K$  are associated :  $\iff \exists \varepsilon \in \mathcal{O}_K^\times$  s.t.  $\alpha' = \alpha \cdot \varepsilon$ .

**Proposition 2.7.2.** *Let  $a \in \mathbb{Z}$ . There are at most  $(\mathcal{O}_K : a\mathcal{O}_K) = \mathcal{N}((a))$  elements  $\alpha \in \mathcal{O}_K$  up to associates with  $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \pm a$ .*

*Proof.* Suppose w.l.o.g.:  $a > 1$ .

Consider the cosets of  $\mathcal{O}_K$  modulo the subgroup  $a\mathcal{O}_K$ . Show that each coset contains at most one such  $\alpha$  up to associates.

Suppose:  $\alpha \in \mathcal{O}$  with  $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \pm a$  and suppose  $\beta = \alpha + a\gamma$  with  $\gamma \in \mathcal{O}_K$  also satisfies  $\mathcal{N}_{K/\mathbb{Q}}(\beta) = \pm a \Rightarrow \frac{\beta}{\alpha} = 1 \pm \frac{\mathcal{N}_{K/\mathbb{Q}}(\alpha)}{\alpha} \gamma$ .

Recall:  $\frac{\mathcal{N}(\alpha)}{\alpha} \in \mathcal{O}_K \Rightarrow \frac{\beta}{\alpha} \in \mathcal{O}_K$ .

Obtain in the same way  $\frac{\alpha}{\beta} \in \mathcal{O}_K$ . Hence  $\frac{\alpha}{\beta}$  and  $\frac{\beta}{\alpha}$  are in  $\mathcal{O}_K^\times \Rightarrow \alpha$  and  $\beta$  are associated.  $\square$

**Lemma 2.7.3.** *Let  $V$  be an  $\mathbb{R}$ -vector space of dimension  $n$ ,  $\Gamma$  a lattice in  $V$ .*

*$\Gamma$  is complete  $\iff \exists M \subseteq V$  with  $M$  bounded s.t.  $\bigcup_{\gamma \in \Gamma} M + \gamma = V$ .*

*Proof.* „ $\Rightarrow$ “:  $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n \Rightarrow M := \phi := \{r_1v_1 + \dots + r_nv_n \mid 0 \leq r_i < 1\}$  does it.

„ $\Leftarrow$ “: Consider:  $V_0 := \mathbb{R}$ -vector space generated by  $\Gamma$ . Have to show:  $V_0 = V$ .

Let  $v \in V$ . Consider the sequence  $kv$  ( $k \in \mathbb{N}$ ).

Precondition  $\Rightarrow \forall k \exists a_k \in M$  and  $\gamma_k \in \Gamma$  with  $kv = a_k + \gamma_k$

$M$  bounded  $\Rightarrow \frac{1}{k}a_k \rightarrow 0 \Rightarrow v = \lim_{k \rightarrow \infty} \frac{1}{k}a_k + \frac{1}{k}\gamma_k = \lim_{k \rightarrow \infty} \frac{1}{k}\gamma_k \Rightarrow v \in V_0$ , since  $V_0$  is closed.  $\square$

**Theorem 10.** *The group  $\Gamma$  is a complete lattice in  $H = \{x \in [\prod_\tau \mathbb{R}]^+ \mid \text{Tr}(x) = 0\} \cong \mathbb{R}^{r+s-1}$ . Hence  $\Gamma$  is isomorphic to  $\mathbb{Z}^{r+s-1}$ .*

*Proof.* Step 1: Show that  $\Gamma$  is a lattice, i.e. show that  $\Gamma$  is a discrete subgroup of  $H$ .

More precisely: show that  $\forall c > 0$ :

$$\Gamma \cap \{(z_\tau)_\tau \in \prod_\tau \mathbb{R} \mid |z_\tau| \leq c\} =: Q_c$$

is finite.

Observe:  $l^{-1}(Q_c) = \{(x_\tau)_\tau \in \prod_\tau \mathbb{C}^\times \mid e^{-c} \leq |x_\tau| \leq e^c\}$  since  $l((x_\tau)_\tau) = (\log|x_\tau|)_\tau$ .

$\Rightarrow l^{-1}(Q_c) \cap j(\mathcal{O}_K^\times)$  is finite, since  $j(\mathcal{O}_K)$  is a lattice in  $K_\mathbb{R}$ . This shows the claim.

Step 2: Show that  $\Gamma$  is complete.

Idea: Use Lemma 7.3.

Hence: find  $M \subseteq H$  as required in the lemma.

Equivalently: find  $T \subseteq S$ , s.t.  $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} T \cdot j(\varepsilon)$  and  $T$  is bounded.

Then we have for  $M := l(T) : H = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} M + l(j(\varepsilon)) = \bigcup_{\gamma \in \Gamma} M + \gamma$ .

Furthermore:  $T$  bounded  $\Rightarrow \exists C > 0 : \forall x \in T : \forall \tau : |x_\tau| < C$ .

Since  $\prod_\tau |x_\tau| = 1 \Rightarrow \exists c > 0 : \forall x \in T : \forall \tau : |x_\tau| > c \Rightarrow M = l(T)$  is bounded in  $H$ .

Step 3: Definition of  $T$

- Choose sequence  $(c_\tau)$  with  $c_\tau > 0$ ,  $c_{\bar{\tau}} = c_\tau$  and  $C := \prod c_\tau > M_0 = (\frac{2}{\pi})^s \sqrt{d_K}$  and define  $X := \{(x_\tau)_\tau \mid |x_\tau| < c_\tau\}$ .
- Choose  $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K$  s.t. each  $\alpha \in \mathcal{O}_K, \alpha \neq 0$  with  $|\mathcal{N}_{K/\mathbb{Q}}(\alpha)| \leq C$  is associated to one  $\alpha_i$  (by Prop 7.2. possible).

Define  $T := S \cap \bigcup_{i=1}^n X \cdot j(\alpha_i)^{-1}$ .

Step 4:  $T$  does the job:

- (1)  $X$  is bounded  $\Rightarrow Xj(\alpha_i)^{-1}$  is bounded  $\Rightarrow T$  is bounded.
- (2) Observe:  $y = (y_\tau) \in S \Rightarrow Xy = \{(x_\tau) \in K_{\mathbb{R}} \mid |x_\tau| < c'_\tau\}$  with  $c'_\tau = c_\tau \cdot |y_\tau|$   
 $\Rightarrow c'_\tau = c'_\tau$  and  $\prod_\tau c'_\tau = \prod_\tau c_\tau \underbrace{\prod_\tau |y_\tau|}_{=1(y \in S)} = C$ .  
 $\Rightarrow \exists \alpha \in \mathcal{O}_K$  with  $|\tau(\alpha)| < c'_\tau \forall \tau \Rightarrow j(\alpha) \in Xy$
- (3) Show that:  $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} Tj(\varepsilon)$   
 Suppose  $y \in S \stackrel{(2)}{\Rightarrow} \exists \alpha \in \mathcal{O}_K \setminus \{0\}$  with  $j(\alpha) \in Xy^{-1} \Rightarrow j(\alpha) = xy^{-1}$  for some  $x \in X$ .  
 Furthermore:  $|\mathcal{N}_{K/\mathbb{Q}}(\alpha)| = |\mathcal{N}(xy^{-1})| = |\mathcal{N}(x)| < \prod_\tau c_\tau = C$ .  
 $\Rightarrow \alpha$  is associated to some  $\alpha_i$ , hence  $\alpha_i = \varepsilon \alpha$  with  $\varepsilon \in \mathcal{O}_K^\times$ .  
 $\Rightarrow y = xj(\alpha)^{-1} = xj(\alpha_i^{-1}\varepsilon)$ .  
 Finally:  $y$  and  $j(\varepsilon) \in S \Rightarrow xj(\alpha_i)^{-1} \in S \cap Xj(\alpha_i)^{-1} \subseteq T \Rightarrow y \in Tj(\varepsilon)$ .

□

**Corollary 2.7.4.**  $\mathcal{O}_K^\times \cong \mathbb{Z}^{r+s-1} \times \mu(K)$ .

*Proof.* We have the exact sequence

$$1 \rightarrow \mu(K) \rightarrow \mathcal{O}_K^\times \xrightarrow{l} \Gamma \cong \mathbb{Z}^{r+s-1} \rightarrow 1$$

Fix a basis  $v_1, \dots, v_t$  ( $t := r + s - 1$ ) of  $\Gamma$  and preimages  $\varepsilon_1, \dots, \varepsilon_t$  in  $\mathcal{O}_K^\times$ .

Let  $A := \langle \varepsilon_1, \dots, \varepsilon_t \rangle \subseteq \mathcal{O}_K^\times$ .

Then  $\lambda|_A$  is an isomorphism and thus  $A \cap \mu(K) = \{1\}$ . In particular every  $\alpha \in \mathcal{O}_K^\times$  decomposes in a unique way as  $\alpha = \nu \cdot \mu$  with  $\nu \in A$  and  $\mu \in \mu(K)$ . □

## 2.8 Prime ideals in $\mathcal{O}_K$

**Question:** Describe the prime ideals in  $\mathcal{O}_K$  that "live above a prime ideal  $\mathfrak{p} \subset \mathbb{Z}$ ".

Consider the following, more general situation: Let

- $\mathcal{O}$  be a Dedekind domain,
- $K = \text{Quot}(\mathcal{O})$ ,
- $L \mid K$  a finite and separable field extension,
- $\hat{\mathcal{O}}$  the integral closure of  $\mathcal{O}$  in  $L$ .

**Definition 2.8.1.** In the setting above, we say that a prime ideal  $\hat{\mathfrak{p}} \in \hat{\mathcal{O}}$  lies above a prime ideal  $\mathfrak{p} \in \mathcal{O} : \Leftrightarrow \hat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}$ .

**Proposition 2.8.2.**  $\hat{\mathcal{O}}$  is a Dedekind domain.

*Proof.* (1)  $\hat{\mathcal{O}}$  is an integral domain and is integrally closed (see **Remark 2.1**).

- (2) We show, that every prime ideal  $0 \neq \hat{\mathfrak{p}} \in \hat{\mathcal{O}}$  is maximal: We know that  $\mathfrak{p} := \hat{\mathfrak{p}} \cap \mathcal{O}$  is a prime ideal in  $\mathcal{O}$ .

(Claim:)  $\mathfrak{p} \neq 0$ . Choose  $0 \neq x \in \hat{\mathfrak{p}}$ . Since  $\hat{\mathcal{O}}$  is integrally closed,  $\exists a_0, \dots, a_{n-1}$ , such that

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0.$$

We may assume that the equation is minimal, i.e.  $a_0 \neq 0$ . Then we have

$$0 \neq a_0 = -a_1x - \dots - a_{n-1}x^{n-1} - x^n \in \hat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}.$$

Since  $\mathfrak{p}$  is a prime ideal of  $\mathcal{O}$ , it is also maximal, i.e.  $\mathcal{O}/\mathfrak{p}$  is a field. Hence  $\hat{\mathcal{O}}/\hat{\mathfrak{p}}$  is a finite extension of  $\mathcal{O}/\mathfrak{p}$  as an  $\mathcal{O}/\mathfrak{p}$ -algebra. Therefore  $\mathcal{O}/\mathfrak{p}$  a field  $\Rightarrow \hat{\mathcal{O}}/\hat{\mathfrak{p}}$  is a field  $\Rightarrow \hat{\mathfrak{p}}$  is a maximal ideal.

- (3)  $\hat{\mathcal{O}}$  is Noetherian: Choose a basis  $\alpha_1, \dots, \alpha_n$  of  $L | K$  with  $\alpha_1, \dots, \alpha_n \in \hat{\mathcal{O}}$ . Let  $d := d(\alpha_1, \dots, \alpha_n) \neq 0$  (**Proposition 2.6**). Recall that  $d \cdot \hat{\mathcal{O}} \subset \mathcal{O}\alpha_1 + \dots + \mathcal{O}\alpha_n$  (**Proposition 2.8**) and that therefore  $\hat{\mathcal{O}} \subset \mathcal{O}\frac{\alpha_1}{d} + \dots + \mathcal{O}\frac{\alpha_n}{d}$ . Hence every ideal  $I \subset \hat{\mathcal{O}}$  can be regarded as a submodule of the  $\mathcal{O}$ -module  $\mathcal{O}\frac{\alpha_1}{d} + \dots + \mathcal{O}\frac{\alpha_n}{d}$ . But since this module is finitely generated and  $\mathcal{O}$  is Noetherian,  $I$  must be finitely generated as well.

□

**Proposition 2.8.3.** *Let  $\mathfrak{p} \subset \mathcal{O}$  be a prime ideal. Then  $\mathfrak{p} \cdot \hat{\mathcal{O}} \subsetneq \hat{\mathcal{O}}$ .*

*Proof.* We may assume  $\mathfrak{p} \neq 0$ .

- (1) Choose  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ . Then we can write  $\pi \cdot \mathcal{O} = \mathfrak{p} \cdot \mathfrak{u}$  with  $\mathfrak{p}, \mathfrak{u}$  coprime, i.e.  $\mathcal{O} = \mathfrak{p} + \mathfrak{u} \Rightarrow \exists s \in \mathfrak{u}, t \in \mathfrak{p} : 1 = s + t$ . In particular,  $s \notin \mathfrak{p}$  since  $1 \notin \mathfrak{p}$  and  $s \cdot \mathfrak{p} \subset \mathfrak{u} \cdot \mathfrak{p} = \pi \cdot \mathcal{O}$ .
- (2) Suppose  $\mathfrak{p}\hat{\mathcal{O}} = \hat{\mathcal{O}}$ . Then  $s \cdot \hat{\mathcal{O}} = s\mathfrak{p}\hat{\mathcal{O}} \subset \pi\hat{\mathcal{O}} \Rightarrow s = \pi x$  with some  $x \in \hat{\mathcal{O}} \cap K = \mathcal{O} \Rightarrow s \in \pi\mathcal{O} \subset \mathfrak{p}$ , a contradiction.

□

*Remark 2.8.4.* Let  $\mathfrak{p} \neq 0$  be a prime ideal in  $\mathcal{O}$ . Then:

- (i)  $\mathfrak{p} \cdot \hat{\mathcal{O}} = \mathfrak{p}_1^{e_1} \cdot \dots \cdot \mathfrak{p}_r^{e_r}$  with  $e_1, \dots, e_r \in \mathbb{N}$  and  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  prime ideals in  $\hat{\mathcal{O}}$ .
- (ii) A prime ideal  $\hat{\mathfrak{p}}$  in  $\hat{\mathcal{O}}$  satisfies:  $\hat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p} \Leftrightarrow \hat{\mathfrak{p}} = \mathfrak{p}_i$  for some  $i$ .

*Proof.* (i) follows from **Proposition 8.2+8.3**.

- (ii) " $\Leftarrow$ ":  $\mathfrak{p}\hat{\mathcal{O}} = \mathfrak{p}_1^{e_1} \cdot \dots \cdot \mathfrak{p}_r^{e_r} \Rightarrow \mathfrak{p}\mathcal{O} \subset \mathfrak{p}_i \Rightarrow \mathfrak{p} \subset \mathfrak{p}_i \cap \mathcal{O}$ . We have  $\mathfrak{p}_i \cap \mathcal{O} \neq 0$ ,  $1 \notin \mathfrak{p}_i \cap \mathcal{O}$  and  $\mathfrak{p}$  is maximal, hence  $\mathfrak{p} = \mathfrak{p}_i \cap \mathcal{O}$ .
- " $\Rightarrow$ ":  $\hat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p} \Rightarrow \mathfrak{p}\hat{\mathcal{O}} \subset \hat{\mathfrak{p}} \Rightarrow \hat{\mathfrak{p}}$  divides  $\mathfrak{p}\hat{\mathcal{O}}$ .

□

**Definition 2.8.5.** Let  $0 \neq \mathfrak{p}$  be a prime ideal in  $\mathcal{O}$  and  $\mathfrak{p}\hat{\mathcal{O}} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$  the decomposition into prime ideals.

- (i)  $e_i$  is called **ramification index** of  $\mathfrak{p}_i$ .  
 $\mathfrak{p}_i$  is called **unramified**  $:\Leftrightarrow e_i = 1$ .  
 $\mathfrak{p}$  is called **unramified**, if all  $\mathfrak{p}_i$  are unramified.  
 $\mathfrak{p}$  is called **totally ramified**  $:\Leftrightarrow r = 1$ .
- (ii)  $f_i := \dim_K \hat{\mathcal{O}}/\mathfrak{p}_i$  with  $K := \mathcal{O}/\mathfrak{p}$  is called **local degree** or **relative degree** of  $\mathfrak{p}_i$ .

**Theorem 11.** In the situation of **Definition 8.5**, we have the fundamental equation:

$$\sum_{i=1}^r e_i \cdot f_i = n \quad \text{with } n = [L : K]$$

*Proof.* We can write

$$\hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}} = \bigoplus_{i=1}^r \hat{\mathcal{O}}/\mathfrak{p}_i^{e_i}$$

by the Chinese Remainder Theorem. Let  $k = \mathcal{O}/\mathfrak{p}$

Step 1: We show, that  $\dim_k \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}} = n$ . Choose a basis  $\bar{\omega}_1, \dots, \bar{\omega}_m$  of  $\hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}$  over  $k$  and choose preimages  $\omega_1, \dots, \omega_m$  in  $\hat{\mathcal{O}}$ . We will show, that  $\omega_1, \dots, \omega_m$  is a basis of  $L \mid K$ , i.e  $m = n$ , from which the claim follows.

- (1) Suppose  $\omega_1, \dots, \omega_m$  are linearly dependant, i.e  $\exists \alpha_1, \dots, \alpha_m \in K$ , not all zero and such that

$$\alpha_1 \omega_1 + \cdots + \alpha_m \omega_m = 0. \quad (*)$$

Since  $K = \text{Quot}(\mathcal{O})$ , we may choose  $\alpha_1, \dots, \alpha_m \in \mathcal{O}$ , since we can just clear denominators. Consider the ideal  $\mathfrak{u} := \langle \alpha_1, \dots, \alpha_m \rangle \subset \mathcal{O}$ .  $\mathfrak{p} \neq 0 \Rightarrow \mathfrak{u}^{-1}\mathfrak{p} \subsetneq \mathfrak{u}^{-1}$ . Choose some  $\alpha \in \mathfrak{u}^{-1} \setminus \mathfrak{u}^{-1}\mathfrak{p} \Rightarrow \alpha \cdot \mathfrak{u} \not\subseteq \mathfrak{p} \Rightarrow \alpha\alpha_1, \dots, \alpha\alpha_m \in \mathcal{O}$ , but not all lie in  $\mathfrak{p}$ .

$\xRightarrow{(*)} \alpha\alpha_1\omega_1 + \cdots + \alpha\alpha_m\omega_m = 0 \pmod{\mathfrak{p}}$  with at least one of the  $\alpha\alpha_i \notin \mathfrak{p}$ . Hence  $\alpha\alpha_1\bar{\omega}_1 + \cdots + \alpha\alpha_m\bar{\omega}_m = 0$  with at least one  $\alpha\alpha_i \neq 0$ , which contradicts the assumption that  $\bar{\omega}_1, \dots, \bar{\omega}_m$  is a basis.

- (2) Consider  $M := \mathcal{O}\omega_1 + \cdots + \mathcal{O}\omega_m$  and  $N := \hat{\mathcal{O}}/M$ . Since  $\hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}} = K\bar{\omega}_1 + \cdots + K\bar{\omega}_m$ , we have  $\hat{\mathcal{O}} = M + \mathfrak{p}\hat{\mathcal{O}} \xrightarrow{\text{mod } M} N = \mathfrak{p}N$ . The proof of **Proposition 8.2** implies, that  $\hat{\mathcal{O}}$  and  $N$  are finitely generated as  $\mathcal{O}$ -modules. Choose generators  $\bar{\alpha}_1, \dots, \bar{\alpha}_s$  of  $N$ .  $N = \mathfrak{p}N \Rightarrow \exists \alpha_{i,j} \in \mathfrak{p}$  with  $\bar{\alpha}_i = \sum_{j=1}^s \alpha_{i,j} \bar{\alpha}_j$ . Consider  $A = (\alpha_{i,j})_{i,j=1}^s - I$ . Then



$$A \cdot \begin{pmatrix} \bar{\alpha}_1 \\ \vdots \\ \bar{\alpha}_s \end{pmatrix} = 0.$$

Furthermore,  $d := \det(A) = (-1)^s \pmod{\mathfrak{p}} \Rightarrow d \neq 0$ . We now see

$$0 = A^\# A \begin{pmatrix} \bar{\alpha}_1 \\ \vdots \\ \bar{\alpha}_s \end{pmatrix} = d \cdot \begin{pmatrix} \bar{\alpha}_1 \\ \vdots \\ \bar{\alpha}_s \end{pmatrix} \Rightarrow d \cdot N = 0,$$

hence  $d \cdot \hat{\mathcal{O}} \subset M = \mathcal{O}\omega_1 + \dots \mathcal{O}\omega_m$ . Now, for some  $\beta \in L$ , we have  $\beta = d \underbrace{\beta'}_{\in L} = d \cdot \frac{b}{a} = \frac{1}{a}db$ , with  $b \in \hat{\mathcal{O}}$  and  $a \in \mathcal{O}$ . Hence  $\beta \in K\omega_1 + \dots + K\omega_m \Rightarrow m = n$  and  $\omega_1, \dots, \omega_m$  generate  $L \mid K$ .

Step 2: We show, that  $\dim_K \hat{\mathcal{O}}/\mathfrak{p}_i^{e_i} = e_i f_i$ . Consider the chain

$$\hat{\mathcal{O}}/\mathfrak{p}_i^{e_i} \supsetneq \mathfrak{p}_i/\mathfrak{p}_i^{e_i} \supsetneq \dots \supsetneq \mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i} \supsetneq 0$$

as a chain of  $K$ -vectorspaces. Choose an  $\alpha \in \mathfrak{p}_i^j \setminus \mathfrak{p}_i^{j+1}$  and consider the homomorphism

$$\begin{aligned} \hat{\mathcal{O}} &\longrightarrow \mathfrak{p}_i^j/\mathfrak{p}_i^{j+1} \\ a &\longmapsto \alpha \cdot a, \end{aligned}$$

which is surjective with kernel  $\mathfrak{p}_i$  (since  $\mathfrak{p}_i^{j+1}$  is coprime to  $\alpha\hat{\mathcal{O}}$ ). Therefore  $\mathfrak{p}_i^j/\mathfrak{p}_i^{j+1} \cong \hat{\mathcal{O}}/\mathfrak{p}_i$  and we have

$$\dim_K \hat{\mathcal{O}}/\mathfrak{p}_i^{e_i} = \sum_{j=0}^{e_i-1} \dim_K \mathfrak{p}_i^j/\mathfrak{p}_i^{j+1} = e_i \cdot f_i$$

□

Next, we will examine the example of the Gaussian integers  $\mathbb{Z}[i]$ . By **Proposition 2.10**,  $\mathbb{Z}[i]$  is the ring of integers  $\hat{\mathcal{O}}$  of the field extension  $\mathbb{Q}[i] \mid \mathbb{Q}$ .

*Reminder 2.8.6.* (i)  $\mathbb{Z}[i]$  is an euclidean ring  $\Rightarrow \mathbb{Z}[i]$  is a PID  $\Rightarrow \mathbb{Z}[i]$  is an UFD

(ii) In particular, all prime ideals  $\mathfrak{p} = \langle \pi \rangle$  with  $\pi$  prime.

*Remark 2.8.7.* Let  $R$  be a domain,  $a, b \in R$ . Then  $\langle a \rangle = \langle b \rangle \Leftrightarrow a$  and  $b$  are associated.

*Proof.* " $\Rightarrow$ ":  $\langle a \rangle = \langle b \rangle \Rightarrow \exists r, r' \in R : b = ra$  and  $a = r'b \Rightarrow b = rr'b \Rightarrow (1 - rr')b = 0 \xrightarrow{R \text{ domain}} r, r' \in R^\times$ .

" $\Leftarrow$ ":  $a = \epsilon b$  with  $\epsilon \in R^\times \Rightarrow b = \epsilon^{-1}a \Rightarrow \langle a \rangle = \langle b \rangle$ .  $\square$

*Remark 2.8.8.* For  $L = \mathbb{Q}[i]$  and  $K = \mathbb{Q}$ , we have

- (i)  $\text{Gal } L | K = \{\text{id}, (a + bi \mapsto a - bi)\}$
- (ii)  $\mathcal{N}_{L/K}(a + bi) = (a + bi) \cdot (a - bi) = a^2 + b^2$ .
- (iii) Since  $\mathbb{Z}[i]$  is a UFD, an element is prime  $\Leftrightarrow$  it is irreducible.
- (iv)  $\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] \mid \mathcal{N}_{L/K}(\alpha) = 1\} = \{1, -1, i, -i\}$ .
- (v) For  $\alpha = a + bi$ , its associated elements are  $-a - bi$ ,  $ai - b$ ,  $-ai + b$ .

**Proposition 2.8.9** (Theorem of Wilson). *Let  $p \in \mathbb{Z}$  be a prime number. Then:*

- (i)  $(p - 1)! \equiv -1 \pmod{p}$ .
- (ii) If  $p = 4n + 1$  with  $n \in \mathbb{N}$ , then  $(2n)!^2 \equiv -1 \pmod{p}$ .

*Proof.* (i) Since the statement is obvious for  $p = 2$ , let  $p > 2$ . Consider  $X^{p-1} - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ . Then  $1, \dots, p-1$  are all zeroes and

$$X^{p-1} - 1 = (x - 1) \cdot (x - 2) \cdot \dots \cdot (x - (p - 1)) \in \mathbb{Z}/p\mathbb{Z}[X].$$

When we look at the constant term, we see that  $-1 = (-1)^{p-1} \cdot (p - 1)! = (p - 1)!$

- (ii)  $(-1) \equiv (p-1)! \equiv (4n)! = 1 \cdot 2 \cdot \dots \cdot 2n \cdot (p-1) \cdot \dots \cdot (p-2n) \equiv (2n)! \cdot (-1)^{2n} \cdot (2n)! \equiv (2n)!^2 \pmod{p}$ .

$\square$

**Proposition 2.8.10.** *If  $p$  is a prime in  $\mathbb{Z}$  with  $p \equiv 1 \pmod{4}$ , then  $p$  is not a prime in  $\mathbb{Z}[i]$ .*

*Proof.* Write  $p = 4n + 1$ . By the Theorem of Wilson, we have  $X^2 \equiv -1 \pmod{p}$  for  $x = (2n)!$ . Then  $p \mid X^2 + 1 = (x + i)(x - i) \in \mathbb{Z}[i]$ , but  $\frac{x \pm i}{p} \notin \mathbb{Z}[i]$ .  $\square$

**Proposition 2.8.11.** *Each prime element  $\pi \in \mathbb{Z}[i]$  is associated to one of the following prime elements of  $\mathbb{Z}[i]$ :*

- (1)  $\pi = 1 + i$ .
- (2)  $\pi = a + bi$ , with  $a^2 + b^2 = p$  prime in  $\mathbb{Z}$  and  $p \equiv 1 \pmod{4}$ .
- (3)  $\pi = p$  prime in  $\mathbb{Z}$  and  $p \equiv 3 \pmod{4}$ .

*Proof.* We proof the proposition in 3 steps.

Step 1: If  $\pi$  is as in (1) or (2), then  $\pi$  is prime. Suppose  $\pi = \alpha\beta$ . Then  $p = \mathcal{N}(\pi) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta) \in \mathbb{Z}$ , so either  $\mathcal{N}(\alpha) = 1$  or  $\mathcal{N}(\beta) = 1$ , i.e.  $\alpha$  or  $\beta$  is a unit.

Step 2: If  $\pi$  is as in (3), then  $\pi$  is a prime in  $\mathbb{Z}$ . Suppose  $\pi = \alpha\beta \in \mathbb{Z}[i]$ . Then  $p^2 = \mathcal{N}(\pi) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta)$ . If  $\alpha, \beta \notin \mathbb{Z}[i]^\times$ , then  $\mathcal{N}(\alpha) = \mathcal{N}(\beta) = p$ . Write  $\alpha = a + bi$ . Then  $p = \mathcal{N}(\alpha) = a^2 + b^2 \not\equiv 3 \pmod{4}$ , since it is always  $a^2 + b^2 \equiv 0, 1 \pmod{4}$ , a contradiction.

Step 3: We have now shown, that the elements (1) – (3) are prime. Let now  $\pi_0 \in \mathbb{Z}[i]$  be a prime element. We will show, that  $\pi_0$  is associated to one of the three elements above. Look at  $\mathcal{N}(\pi_0) = p_1 \cdots p_r$  with  $p_1, \dots, p_r$  primes in  $\mathbb{Z}$ . Since  $\pi_0$  is prime, it divides  $p := p_i$ ,  $1 \leq i \leq r \Rightarrow \mathcal{N}(\pi_0)$  divides  $\mathcal{N}(p) = p^2$ , i.e.  $\mathcal{N}(\pi_0) = p$  or  $p^2$ .

Case 1:  $\mathcal{N}(\pi_0) = p$ . If  $p = 2$ , then  $\pi_0 \in \{1 + i, 1 - i, -1 + i, -1 - i\}$ , i.e.  $\pi_0$  is associated to  $1 + i$ . If  $p > 2$ , then  $p = \mathcal{N}(\pi_0) = a^2 + b^2 \equiv 1 \pmod{4} \Rightarrow \pi_0$  is associated to an element as in (2).

Case 2:  $\mathcal{N}(\pi_0) = p^2 \Rightarrow \pi_0 | p^2 \Rightarrow \pi_0 | p \Rightarrow \frac{p}{\pi_0} \in \mathbb{Z}[i]$  and  $\mathcal{N}(\frac{p}{\pi_0}) = \frac{\mathcal{N}(p)}{\mathcal{N}(\pi_0)} = \frac{p^2}{p^2} = 1$ , i.e.  $\frac{p}{\pi_0}$  is a unit, hence  $\pi_0$  is associated to  $p$ . By **Proposition 8.10**,  $p \not\equiv 1 \pmod{4}$ . Also  $p \neq 2$ , since  $2 = (1 + i)(1 - i)$  is not prime in  $\mathbb{Z}[i]$ . Hence  $p \equiv 3 \pmod{4}$  and  $\pi_0$  is associated to an element as in (3). □

**Corollary 2.8.12** (Fermat). (i) If  $p$  is prime then  $p = a^2 + b^2 \Leftrightarrow p \not\equiv 3 \pmod{4}$

(ii)  $\forall n \in \mathbb{N} : n = a^2 + b^2 \Leftrightarrow \nu_p(n)$  is even for all primes  $p \equiv 3 \pmod{4}$ .

*Proof.* (i) " $\Rightarrow$ ": Same as in Step 2 of 8.11

" $\Leftarrow$ ": If  $p = 2$ , then  $2 = 1 + 1$ . If  $p \equiv 1 \pmod{4}$ , then by **Proposition 8.10**,  $p = \alpha\beta \in \mathbb{Z}[i]$  with  $\mathcal{N}(\alpha) = \mathcal{N}(\beta) = p$ . Write  $\alpha = a + bi$  and get  $p = \mathcal{N}(\alpha) = a^2 + b^2$ .

(ii) " $\Rightarrow$ ":  $n = a^2 + b^2 \Rightarrow n = \mathcal{N}(\alpha)$  with  $\alpha = a + bi \in \mathbb{Z}[i]$ . Write  $\alpha = \epsilon \cdot \pi_1 \cdots \pi_r \cdot \pi_{r+1} \cdots \pi_{r+s}$  with  $\pi_1, \dots, \pi_r$  as in (3) and  $\pi_{r+1}, \dots, \pi_{r+s}$  as in (1) or (2). Then  $\mathcal{N}(\alpha) = \prod_{i=1}^r \mathcal{N}(\pi_i) = p_1^2 \cdots p_r^2 \cdot p_{r+1} \cdots p_{r+s}$  with  $p_1, \dots, p_r \equiv 3 \pmod{4}$  and  $p_{r+1}, \dots, p_{r+s} \not\equiv 3 \pmod{4}$ .

" $\Leftarrow$ ":  $n = p_1^2 \cdots p_r^2 \cdot p_{r+1} \cdots p_{r+s}$  as above. By (i),  $p_j \not\equiv 3 \pmod{4}$  and hence  $p_j = a_j^2 + b_j^2$  for  $r+1 \leq j \leq r+s$ . Define  $\alpha := p_1 \cdots p_r \cdot (a_{r+1} + ib_{r+1}) \cdots (a_{r+s} + ib_{r+s})$ . Then  $\mathcal{N}(\alpha) = n$ . □

**Corollary 2.8.13.** The prime ideals  $\mathfrak{p}_i$  in  $\mathbb{Z}[i]$  that lie over a prime ideal  $\mathfrak{p} = \langle p \rangle$  in  $\mathbb{Z}$  are obtained as follows:

(i)  $p = 2 \Rightarrow \langle 2 \rangle \mathbb{Z}[i] = \langle 1 + i \rangle \langle 1 - i \rangle = \langle 1 + i \rangle^2$ . Hence  $r = 1$ ,  $e_1 = 2$ ,  $f_1 = 1$ .

(ii)  $p \equiv 1 \pmod{4} \xrightarrow{p=a^2+b^2} \langle p \rangle \mathbb{Z}[i] = \langle a + bi \rangle \langle a - bi \rangle$ . Hence  $r = 2$ ,  $e_1 = e_2 = 1$ ,  $f_1 = f_2 = 1$ .

(iii)  $p \equiv 3 \pmod{4} \Rightarrow \langle p \rangle \mathbb{Z}[i]$  is a prime ideal. Hence  $r = 1$ ,  $e_1 = 1$ ,  $f_1 = 2$ .

□

**GOAL:** Describe prime ideals explicitly for all simple extensions  $L = K[\Theta]$  with  $\Theta \in \hat{\mathcal{O}}$ .

**Caution:** Before, we had  $\mathbb{Z}[i] = \hat{\mathcal{O}}$ . In general, we might have  $\hat{\mathcal{O}}' := \mathcal{O}[\Theta] \subsetneq \hat{\mathcal{O}}$ .

**Idea:** Take the largest ideal of  $\hat{\mathcal{O}}$  which also lies in  $\hat{\mathcal{O}}'$ .

**Definition 2.8.14.** The set  $\mathcal{F} := \{\alpha \in \hat{\mathcal{O}} \mid \alpha \hat{\mathcal{O}} \subset \hat{\mathcal{O}}'\}$  is called **conductor**.

*Example 2.8.15.* If  $\hat{\mathcal{O}} = \mathbb{Z}[i]$  and  $\Theta = i$ , then  $\hat{\mathcal{O}}' = \mathcal{O}[\Theta] \Rightarrow \mathcal{F} = \hat{\mathcal{O}}$ .

**Proposition 2.8.16.** In the situation above, let  $f(X) := f_{\Theta}(X)$  be the minimal polynomial of  $\Theta$ . Let  $\mathfrak{p}$  be a prime ideal in  $\mathcal{O}$  and  $K := \mathcal{O}/\mathfrak{p}$ . Consider the image  $\bar{f}$  of  $f$  in  $K[X]$  and let  $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r}$  be the prime factorization in  $K[X]$ . Choose preimages  $f_1, \dots, f_r \in \mathcal{O}[X]$ . Then:

If  $\mathfrak{p}$  is coprime to  $\mathcal{F}$ , i.e.  $\mathfrak{p} + \mathcal{F} \cap \mathcal{O} = \mathcal{O}$ , then the ideals in  $\hat{\mathcal{O}}$  which lie over  $\mathfrak{p}$  are given as follows:  $\mathfrak{p}_i := \mathfrak{p}\hat{\mathcal{O}} + f_i(\Theta)\hat{\mathcal{O}}$ ,  $1 \leq i \leq r$  and the local degree of  $\mathfrak{p}_i$  is equal to  $\deg(\bar{f}_i)$ .

**Proposition 2.8.17.** Let  $R$  and  $S$  be rings and  $\varphi: R \rightarrow S$  a ring homomorphism.

(i) If  $\mathfrak{q}$  is a prime ideal in  $S$  then  $\varphi^{-1}(\mathfrak{q})$  is a prime ideal in  $R$ .

(ii) If  $\varphi$  is surjective and  $\mathfrak{p}$  is a prime ideal in  $R$  with  $\ker \varphi \subset \mathfrak{p}$  then  $\varphi(\mathfrak{p})$  is a prime ideal in  $S$ .

*Proof.* “(i)” Preimages of ideals are ideals. Suppose  $ab \in \varphi^{-1}(\mathfrak{q})$ . Then  $\varphi(a)\varphi(b) \in \mathfrak{q}$  such that, without loss of generality,  $\varphi(a) \in \mathfrak{q}$  and hence  $a \in \varphi^{-1}(\mathfrak{q})$ .

“(ii)” Images of ideals under surjective homomorphisms are ideals. Let  $\bar{a}\bar{b} \in \varphi(\mathfrak{p})$ . Since  $\varphi$  is surjective there are  $a, b \in R$  with  $\varphi(a) = \bar{a}$ ,  $\varphi(b) = \bar{b}$  and there is  $c \in \mathfrak{p}$  with  $\varphi(c) = \bar{a}\bar{b}$ . Hence

$$ab - c \in \ker \varphi \subset \mathfrak{p}$$

such that  $ab \in \mathfrak{p}$ . We may assume that  $a \in \mathfrak{p}$  and conclude  $\bar{a} = \varphi(a) \in \varphi(\mathfrak{p})$ . □

**Definition 2.8.18.** In the situation of Proposition 2.8.17 we define:

(i)  $\text{Spec}(R) = \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ is a prime ideal}\}$

(ii)  $\text{Spec}_S(R) = \{\mathfrak{p} \subset \text{Spec}(R) \mid \mathfrak{p} \supset \ker \varphi\}$

**Corollary 2.8.19.** In the situation of Proposition 2.8.17 we have:

(i) If  $\varphi: R \rightarrow S$  is a homomorphism of rings then  $\varphi$  induces a map

$$\varphi^*: \text{Spec}(S) \rightarrow \text{Spec}_S(R), \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}).$$

(ii) If  $\varphi$  is surjective then  $\varphi^*$  is a bijection with inverse map

$$\varphi_*: \operatorname{Spec}_S(R) \rightarrow \operatorname{Spec}(S), \mathfrak{p} \mapsto \varphi(\mathfrak{p}).$$

*Reminder 2.8.20.* For  $a \in \mathbb{Z}$  and  $p$  prime in  $\mathbb{Z}$  the **Legendre symbol** is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \text{ divides } a, \\ 1, & \text{there is an } x \in \mathbb{Z}/p\mathbb{Z} \text{ such that } x^2 \equiv a \pmod{p}, \\ -1, & \text{else.} \end{cases}$$

*Example 2.8.21.* Apply Proposition 8.15 for quadratic number fields,  $D$  square-free:

$$\begin{array}{ccccc} \hat{\mathcal{O}} & = & \mathbb{Z}[\theta] & \subset & \mathbb{Q}(\sqrt{D}) \\ & & \uparrow & & \uparrow \\ \mathcal{O} & = & \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

*Reminder 2.8.22.* If  $D \not\equiv 1 \pmod{4}$  then we can choose  $\theta = \sqrt{D}$  and obtain  $f = f_\theta = X^2 - D$  and  $d(f_\theta) = 4D$ .

If  $D \equiv 1 \pmod{4}$  then we can choose  $\theta = \frac{1}{2}(1 + \sqrt{D})$  and obtain  $f = f_\theta = X^2 - X - \frac{D-1}{4}$  and  $d(f_\theta) = D$ .

Consider  $p \in \mathbb{Z}$  prime and define  $\bar{f} = \bar{f}_\theta$  as the image of  $f$  in  $\mathbb{Z}/p\mathbb{Z}[X]$ .

**Observe:**  $\bar{f}$  has two equal zeroes in  $\mathbb{Z}/p\mathbb{Z}$  iff  $d(f) = 0$  in  $\mathbb{Z}/p\mathbb{Z}$  iff

$$\begin{cases} \left(\frac{4D}{p}\right) = 0, & D \not\equiv 1 \pmod{4}, \\ \left(\frac{D}{p}\right) = 0, & D \equiv 1 \pmod{4}. \end{cases}$$

$\bar{f}$  has two different zeroes in  $\mathbb{Z}/p\mathbb{Z}$  iff  $d(f)$  is a non-zero square in  $\mathbb{Z}/p\mathbb{Z}$  iff

$$\begin{cases} \left(\frac{4D}{p}\right) = 1, & D \not\equiv 1 \pmod{4}, \\ \left(\frac{D}{p}\right) = 1, & D \equiv 1 \pmod{4} \end{cases} \Leftrightarrow \left(\frac{D}{p}\right) = 1.$$

$\bar{f}$  has no zeroes in  $\mathbb{Z}/p\mathbb{Z}$  iff  $\left(\frac{D}{p}\right) = -1$ .

Proposition 8.15 then implies in the first case that  $p\hat{\mathcal{O}} = \hat{\mathcal{P}}_1^2$  with

$$\mathcal{P}_1 = \begin{cases} p\hat{\mathcal{O}} + \theta\hat{\mathcal{O}}, & D \not\equiv 1 \pmod{4}, \\ p\hat{\mathcal{O}} + \left(\theta - \frac{1}{2}\right)\hat{\mathcal{O}}, & D \equiv 1 \pmod{4}, \end{cases}$$

In the second case we obtain  $p\hat{\mathcal{O}} = \hat{\mathcal{P}}_1\hat{\mathcal{P}}_2$  with  $\hat{\mathcal{P}}_{1,2} = p\hat{\mathcal{O}} + (\theta \pm x)\hat{\mathcal{O}}$ , where  $x^2 \equiv D \pmod{p}$ .

In the third case  $p\hat{\mathcal{P}}$  is a prime ideal.

*Example.* Let  $D \not\equiv 1 \pmod{p}$ ,  $\left(\frac{4D}{p}\right) = 0$  and  $p \neq 2$ . Consider the map  $\pi: \hat{\mathcal{O}} \rightarrow \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}$  with  $\hat{\mathcal{O}} = \mathbb{Z}[\sqrt{D}]$  and  $\mathfrak{p}\hat{\mathcal{O}} = \{a + b\sqrt{D} \mid p|a \text{ and } p|b\}$  and thus

$$\begin{aligned} \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}} &\cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}[\sqrt{D}] \cong (\mathbb{Z}/p\mathbb{Z}[X])/(X^2 - D), \\ \theta &\leftrightarrow (0, \sqrt{D}) \leftrightarrow \bar{X}. \end{aligned}$$

We have

$$\hat{\mathcal{P}}_1 = \pi^{-1}((\bar{\theta})) = \{a + b\sqrt{D} \mid p \text{ divides } a\}.$$

*Example.* Let  $D \not\equiv 1 \pmod{p}$  and  $\left(\frac{4D}{p}\right) = 1$ . Then there exists  $x \in \mathbb{Z}$  with  $x^2 \equiv D \pmod{p}$  and  $p \nmid x$ . Here,  $\pi: \hat{\mathcal{O}} \rightarrow \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}$  is the map

$$\begin{aligned} \mathbb{Z}[\sqrt{D}] &\rightarrow \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}[\sqrt{D}] \\ &\cong (\mathbb{Z}/p\mathbb{Z}[X])/(X - x)(X + x) \\ &\cong (\mathbb{Z}/p\mathbb{Z}[X])/(X - x) \oplus (\mathbb{Z}/p\mathbb{Z}[X])/(X + x) \end{aligned}$$

given by

$$a + b\sqrt{D} \mapsto \bar{a} + \bar{b}\sqrt{D} \cong \bar{a} + \bar{b}X \cong (\bar{a} + \bar{b}x, \bar{a} - \bar{b}x).$$

Recall that  $\bar{f}(X) = (X - x)(X + x) = \bar{f}_1\bar{f}_2$  with  $\bar{f}_1, \bar{f}_2 \in \mathbb{Z}[X]$  and

$$f_1(\theta) = \theta - x = \sqrt{D} - x = -x + \sqrt{D}$$

with  $\pi(f_1(\theta)) \leftrightarrow (0, -2\bar{x})$ . Observe that for  $\bar{x} \in \mathcal{F}_p^x$  we have the correspondence

$$(\pi(f_1(\theta))) \leftrightarrow \mathcal{O} \oplus (\mathbb{Z}/p\mathbb{Z}[X])/(X + p) \cong \mathcal{O} \oplus \mathbb{Z}/p\mathbb{Z}$$

and hence  $\hat{\mathcal{P}}_1 = \pi^{-1}(\mathcal{O} \oplus \mathbb{Z}/p\mathbb{Z})$ .

*Proof of Prop. 8.16.* Consider the map  $\pi: \hat{\mathcal{O}} \rightarrow \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}$ . By Corollary 8.19 we have a bijection

$$\{\hat{\mathcal{P}} \mid \hat{\mathcal{P}} \text{ prime ideal in } \hat{\mathcal{O}} \text{ with } \hat{\mathcal{P}} \cap \mathcal{O} = \mathfrak{p}\} \leftrightarrow \{\mathfrak{q} \mid \mathfrak{q} \text{ prime ideal in } \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}\}.$$

We show:

$$\hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}} \cong \hat{\mathcal{O}}'/\mathfrak{p}\hat{\mathcal{O}}' \cong k[X]/(\bar{f}),$$

where  $k = \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}$  and  $\hat{\mathcal{O}}' = \mathcal{O}[\theta]$ .

**Step 1:**  $\hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}} \cong \hat{\mathcal{O}}'/\mathfrak{p}\hat{\mathcal{O}}'$

Consider the homomorphism  $\varphi: \hat{\mathcal{O}}' \rightarrow \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}$  induced by the inclusion  $\hat{\mathcal{O}}' \hookrightarrow \hat{\mathcal{O}}$ .

“(1)”  $\varphi$  is surjective: If  $\mathfrak{p} + (\mathcal{F} \cap \mathcal{O}) = \mathcal{O}$  then  $\mathfrak{p}\hat{\mathcal{O}} + \mathcal{F} = \hat{\mathcal{O}}$  and hence  $\mathfrak{p}\hat{\mathcal{O}} + \hat{\mathcal{O}}' = \hat{\mathcal{O}}$  (multiply both sides of first equation with  $\hat{\mathcal{O}}$ ).

“(2)”  $\ker \varphi = \mathfrak{p}\hat{\mathcal{O}}'$ : “ $\supset$ ” Clear. “ $\subset$ ” We have  $\ker \varphi = \hat{\mathcal{O}}' \cap \mathfrak{p}\hat{\mathcal{O}}$ . Use  $\mathfrak{p} + (\mathcal{F} \cap \mathcal{O}) = \mathcal{O}$  and write  $1 = p + a$  with  $p \in \mathfrak{p}$  and  $a \in \mathcal{F} \cap \mathcal{O}$ . For  $x \in \hat{\mathcal{O}}' \cap \mathfrak{p}\hat{\mathcal{O}}$  we have:

$$x = 1 \cdot x = (p + a)x = px + ax \in \mathfrak{p}\hat{\mathcal{O}}'.$$

**Step 2:**  $\hat{\mathcal{O}}'/\mathfrak{p}\hat{\mathcal{O}}' \cong k[X]/(\bar{f})$

Recall that  $\hat{\mathcal{O}}' = \mathcal{O}[\theta] \cong \mathcal{O}[X]/(f)$ . Consider  $\Psi: \mathcal{O}[X] \rightarrow k[X]/(\bar{f})$ , which is surjective. It holds that  $\ker \Psi = (\mathfrak{p}, f)$  and hence  $\Psi$  induces an isomorphism  $\hat{\mathcal{O}}'/\mathfrak{p}\hat{\mathcal{O}}' \rightarrow k[X]/(\bar{f})$ .

**Step 3:** Consider now  $R = k[X]/(\bar{f})$  and determine  $\text{Spec}(R)$ .

“(1)” Recall the prime decomposition  $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r}$  in  $k[X]$  and consider the projection  $k[X] \twoheadrightarrow k[X]/(\bar{f})$ . By Corollary 8.19 we have the correspondence

$$\text{Spec}(R) \leftrightarrow \{\mathfrak{p} \text{ prime ideal in } k[X] \mid \bar{f} \in \mathfrak{p}\}$$

and hence  $\text{Spec}(R) = \{(\bar{f}_i) \mid i = 1, \dots, r\}$ .

“(2)” Notice that

$$R/(\bar{f}_i) = (k[X]/(\bar{f})) / (\bar{f}_i) \cong k[X]/(\bar{f}_i)$$

is a  $k$ -vector space of dimension  $\deg(\bar{f}_i)$  such that

$$[R/(\bar{f}_i) : k] = \deg(\bar{f}_i).$$

“(3)” In  $R$  we have

$$\bigcap_{i=1}^r (\bar{f}_i)^{e_i} = (\bar{f}) = 0.$$

**Step 4:** Use the isomorphism

$$k[X]/(\bar{f}) \rightarrow \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}, g \mapsto g(\theta)$$

and obtain from Step 3 with  $\mathcal{P}_i = (f_i(\theta))$  that:

$$(i) \quad \text{Spec}(\hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}) = \{\mathcal{P}_i \mid i = 1, \dots, r\}$$

$$(ii) \quad \left[ (\hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}) / \mathcal{P}_i : k \right] = \deg(\bar{f}_i)$$

$$(iii) \quad \bigcap_{i=1}^r \mathcal{P}_i^{e_i} = 0$$

**Step 5:** Take preimages in  $\hat{\mathcal{O}}$  via  $\hat{\mathcal{O}} \rightarrow \hat{\mathcal{O}}/\mathfrak{p}\hat{\mathcal{O}}$  and observe that (iii) implies  $\bigcap_{i=1}^r \hat{\mathcal{P}}_i^{e_i} \subset \mathfrak{p}\hat{\mathcal{O}}$  such that  $\mathfrak{p}\hat{\mathcal{O}}$  divides  $\bigcap_{i=1}^r \hat{\mathcal{P}}_i^{e_i}$ . Furthermore,

$$[L : K] = n = \deg(f) = \sum_{i=1}^r e_i f_i$$

such that by Theorem 11,  $\mathfrak{p}\hat{\mathcal{O}} = \prod_{i=1}^r \hat{\mathcal{P}}_i^{e_i}$ . □

$$\begin{array}{ccccccc}
& & \hat{\mathcal{P}} & \subseteq & \hat{\mathcal{O}} & \subseteq & L \\
& & \uparrow & & \uparrow & & \uparrow \\
\hat{\mathcal{O}}\mathcal{P} = \hat{\mathcal{P}}_1^{e_1} \cdots \hat{\mathcal{P}}_r^{e_r} & & \mathcal{P} & \subseteq & \mathcal{O} & \subseteq & K
\end{array}$$

**Proposition 2.8.23.** *There are only finitely many prime ideals  $\hat{\mathcal{P}}$  in  $\hat{\mathcal{O}}$  which are ramified over  $\mathcal{P} = \hat{\mathcal{P}} \cap \mathcal{O}$ .*

*Proof.* Choose primitive element  $\theta$  of  $L|K$  in  $\hat{\mathcal{O}}$ . Let  $f_\theta \in \mathcal{O}[X]$  be the minimal polynomial of  $\theta$  and  $d := \text{discr}(f_\theta) = \text{discr}(1, \theta, \dots, \theta^{n-1}) = \prod_{i < j} (\theta_i - \theta_j)^2 \in \mathcal{O}$ .

Here  $\theta_i, \theta_j$  are the zeroes of  $f_\theta$  in the algebraic closure.

Claim: If  $\mathcal{P}$  is a prime ideal in  $\mathcal{O}$  s.t.

- $\mathcal{P}$  is coprime to  $(d)$  and
- $\mathcal{P}$  is coprime to  $\mathcal{F} \cap \mathcal{O}$

then  $\mathcal{P}$  is unramified, i.e. all  $\hat{\mathcal{P}}$  lying above  $\mathcal{P}$  are unramified.

From the claim we obtain that there are only finitely many  $\mathcal{P}$  which allow ramification.

Proof of the claim: Write  $\hat{\mathcal{O}}\mathcal{P} = \hat{\mathcal{P}}_1^{e_1} \cdots \hat{\mathcal{P}}_r^{e_r}$ . Consider  $\bar{f}_\theta \in \mathcal{O}/\mathcal{P}[X]$ . As in Prop. 8.15

$$\bar{f}_\theta = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r} \quad (\star)$$

a prime decomposition.  $(d)$  and  $\mathcal{P}$  are coprime  $\Rightarrow \bar{d} = \text{image of } d \text{ in } \mathcal{O}/\mathcal{P} \neq 0 \Rightarrow \bar{f}_\theta$  has only single zeroes in an algebraic closure of  $\mathcal{O}/\mathcal{P} \xrightarrow{(\star)} e_1 = \cdots = e_r = 1$   $\square$

**Definition 2.8.24.**

- $\mathcal{P}$  is said to split completely or to be totally split :  $\iff e_i = f_i = 1 \ \forall i \in \underline{r}$ .
- $\mathcal{P}$  is said to be indecomposed, nonsplit or totally ramified :  $\iff r = 1$ .

## 2.9 Hilbert's theorem of ramification

Idea: Consider Galois extensions  $L|K \rightarrow$  life becomes much nicer.

Same setting as in 8. Suppose further that  $L|K$  normal and consider  $G = \text{Gal}(L|K)$ .

*Remark 2.9.1.* i)  $\hat{\mathcal{P}}$  prime ideals in  $\hat{\mathcal{O}}$  with  $\mathcal{P} := \hat{\mathcal{P}} \cap \mathcal{O}$ . For  $\sigma \in \text{Gal}(L|K)$  we have  $\sigma(\hat{\mathcal{P}})$  is a prime ideal in  $\hat{\mathcal{O}}$  above  $\mathcal{P}$ .

ii)  $\text{Gal}(L|K)$  acts transitively on the set of prime ideals  $\hat{\mathcal{P}}$  in  $\hat{\mathcal{O}}$  over  $\mathcal{P}$ .

*Proof.* i) Recall from Rem 2.1 iii) that  $\sigma(\hat{\mathcal{O}}) = \hat{\mathcal{O}}$   
 $\Rightarrow \sigma(\hat{\mathcal{P}})$  is again a prime ideal in  $\hat{\mathcal{O}}$ .  
 $\sigma(\hat{\mathcal{P}}) \cap \mathcal{O} = \sigma(\hat{\mathcal{P}} \cap \mathcal{O}) = \sigma(\mathcal{P}) = \mathcal{P}$   
 $\Rightarrow \sigma(\hat{\mathcal{P}})$  lies above  $\mathcal{P}$ .



- ii) follows from i) that we have such an action. Let  $\hat{\mathcal{P}}$  and  $\hat{\mathcal{P}}'$  be prime ideals above  $\mathcal{P} = \hat{\mathcal{P}} \cap \mathcal{O} = \hat{\mathcal{P}}' \cap \mathcal{O}$ . Assume that  $\hat{\mathcal{P}}$  and  $\hat{\mathcal{P}}'$  are not in the same  $G$ -orbit. Hence  $\hat{\mathcal{P}}'$  and  $\sigma(\hat{\mathcal{P}})$  are coprime for each  $\sigma \in G$ .  
 $\Rightarrow \hat{\mathcal{P}}'$  is coprime to  $\sigma_1(\hat{\mathcal{P}}) \cdot \dots \cdot \sigma_n(\hat{\mathcal{P}})$ , where  $G = \{\sigma_1, \dots, \sigma_n\}$ .  
 CRT  $\Rightarrow \exists x \in \hat{\mathcal{O}}$  with  $x \equiv 0 \pmod{\hat{\mathcal{P}}'}$  and  $x \equiv 1 \pmod{\sigma(\hat{\mathcal{P}})}$  for all  $\sigma \in G$ .  
 In particular:  $\mathcal{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \hat{\mathcal{P}}' \cap \mathcal{O} = \mathcal{P}$   
 Also:  $\forall \sigma \in G : x \notin \sigma(\hat{\mathcal{P}}) \Rightarrow \forall \sigma \in G : \sigma(x) \notin \mathcal{P}$   
 $\Rightarrow \mathcal{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \notin \hat{\mathcal{P}} \cap \mathcal{O} = \mathcal{P} \text{ !}$

□

**Definition 2.9.2.** Let  $\hat{\mathcal{P}}$  be a prime ideal of  $\hat{\mathcal{O}}$  above  $\mathcal{P}$ .

- i)  $G_{\hat{\mathcal{P}}} := \text{Stab}_G(\hat{\mathcal{P}}) = \{\sigma \in G \mid \sigma(\hat{\mathcal{P}}) = \hat{\mathcal{P}}\}$  is called decomposition group („Zerlegungsgruppe“)  
 ii)  $Z_{\hat{\mathcal{P}}} := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G_{\hat{\mathcal{P}}}\}$  is called decomposition field („Zerlegungskörper“)

*Remark 2.9.3.* Let  $\hat{\mathcal{P}}_0$  be a prime ideal which lies above  $\mathcal{P}$ .

- i)  $G/G_{\hat{\mathcal{P}}_0} := \{gG_{\hat{\mathcal{P}}_0} \mid g \in G\} \xleftrightarrow{1:1} \{\hat{\mathcal{P}} \mid \hat{\mathcal{P}} \text{ lies above } \mathcal{P}\}$   
 ii)  $G_{\hat{\mathcal{P}}_0} = \{1\} \iff [G : G_{\hat{\mathcal{P}}_0}] = [L : K] = n \iff \mathcal{P} \text{ is totally split} \iff Z_{\hat{\mathcal{P}}_0} = L$  ( $r = [G : G_{\hat{\mathcal{P}}_0}]$ )  
 iii)  $G_{\hat{\mathcal{P}}_0} = G \iff [G : G_{\hat{\mathcal{P}}_0}] = 1 \iff \mathcal{P} \text{ is nonsplit} \iff Z_{\hat{\mathcal{P}}_0} = K$   
 iv)  $G_{\sigma(\hat{\mathcal{P}}_0)} = \sigma \circ G_{\hat{\mathcal{P}}_0} \circ \sigma^{-1}$

*Proof.* Follows from Prop 9.1 + definitions + group actions. □

*Remark 2.9.4.* Suppose  $\mathcal{P}\hat{\mathcal{O}} = \hat{\mathcal{P}}_1^{e_1} \cdot \dots \cdot \hat{\mathcal{P}}_r^{e_r}$  with local degrees  $f_i = [\hat{\mathcal{O}}/\hat{\mathcal{P}}_i : \mathcal{O}/\mathcal{P}]$ . Then  $e_1 = \dots = e_r$  and  $f_1 = \dots = f_r$ .

*Proof.* Prop. 9.1  $\Rightarrow \exists \sigma_i \in G$  s.t.  $\sigma_i(\hat{\mathcal{P}}_1) = \hat{\mathcal{P}}_i$   
 $\Rightarrow \hat{\mathcal{O}}/\hat{\mathcal{P}}_1 \cong \hat{\mathcal{O}}/\hat{\mathcal{P}}_i, a \pmod{\hat{\mathcal{P}}_1} \mapsto \sigma_i(a) \pmod{\hat{\mathcal{P}}_i}$  as  $k = \mathcal{O}/\mathcal{P}$ -vectorspaces  $\Rightarrow f_1 = f_i$  and  $\hat{\mathcal{P}}_i^k \supseteq \mathcal{P}\hat{\mathcal{O}} \iff \hat{\mathcal{P}}_i^k = (\sigma_i(\hat{\mathcal{P}}_1))^k \supseteq \mathcal{P}\hat{\mathcal{O}} = \sigma_i(\mathcal{P}\hat{\mathcal{O}}) \Rightarrow e_i = e_1$ . □

Consider the field extensions  $K \subseteq Z_{\hat{\mathcal{P}}} \subseteq L$ . We have:

$$\begin{array}{ccccccc}
 & & \hat{\mathcal{P}} & \subseteq & \hat{\mathcal{O}} & \subseteq & L \\
 & & | & & | & & | \\
 \hat{\mathcal{P}}_Z & := & \hat{\mathcal{P}} \cap Z_{\hat{\mathcal{P}}} & \subseteq & \hat{\mathcal{O}} \cap Z_{\hat{\mathcal{P}}} & \subseteq & Z_{\hat{\mathcal{P}}} \\
 & & | & & | & & | \\
 & & \mathcal{P} & \subseteq & \mathcal{O} & \subseteq & K
 \end{array}$$

Observe  $\hat{\mathcal{O}} \cap Z_{\hat{\mathcal{P}}}$  is the integral closure of  $\mathcal{O}$  in  $Z_{\hat{\mathcal{P}}}$ .

**Proposition 2.9.5.** Suppose  $\mathcal{P}\hat{\mathcal{O}} = (\prod_{\sigma} \sigma(\hat{\mathcal{P}}))^e$  with local degree  $f$ .

- i)  $\hat{\mathcal{P}}_Z$  is non-split in  $\hat{\mathcal{O}}$ , i.e.  $\hat{\mathcal{P}}$  is the only prime ideal above  $\hat{\mathcal{P}}_Z$ .
- ii)  $\hat{\mathcal{P}}/\hat{\mathcal{P}}_Z$  has ramification index  $e$  and local degree  $f$ .
- iii)  $\hat{\mathcal{P}}_Z/\mathcal{P}$  has ramification index 1 and local degree 1, i.e.  $\hat{\mathcal{P}}_Z/\mathcal{P}$  is totally split.

*Proof.* i)  $Z_{\hat{\mathcal{P}}} = L^{G_{\hat{\mathcal{P}}}} \Rightarrow \text{Gal}(L/Z_{\hat{\mathcal{P}}}) = G_{\hat{\mathcal{P}}}$ . Now statement follows from 9.3 iii)

ii)+iii) Let  $e' = \text{ramification index of } \hat{\mathcal{P}}/\hat{\mathcal{P}}_Z$  and  $e'' = \text{ramification index of } \hat{\mathcal{P}}_Z/\mathcal{P}$

Let  $f' = \text{local degree of } \hat{\mathcal{P}}/\hat{\mathcal{P}}_Z$  and  $f'' = \text{local degree of } \hat{\mathcal{P}}_Z/\mathcal{P}$ .

Hence:  $\hat{\mathcal{P}}_Z\hat{\mathcal{O}} = \hat{\mathcal{P}}^{e'}$  and  $\mathcal{P}(\hat{\mathcal{O}} \cap Z_{\hat{\mathcal{P}}}) = \hat{\mathcal{P}}_Z^{e''} \cdot \dots \Rightarrow \mathcal{P}\hat{\mathcal{O}} = (\hat{\mathcal{P}}^{e'})^{e''} \cdot \dots$

$\Rightarrow e = e' \cdot e''$  (★).

Also we have for the field extensions

$$\hat{\mathcal{O}}/\hat{\mathcal{P}} \supseteq \underbrace{\hat{\mathcal{O}} \cap Z_{\hat{\mathcal{P}}}/\hat{\mathcal{P}}_Z}_{f'} \supseteq \underbrace{\mathcal{O}/\mathcal{P}}_{f''}$$

$\Rightarrow f = f' \cdot f''$  (★★).

Thm. 11  $\Rightarrow$  1) For  $L|K$  :  $n = [L : K] = e \cdot f \cdot r$  with  $r = [G : G_{\hat{\mathcal{P}}}]$  ( $n = |G|$ ).

2) For  $L|Z_{\hat{\mathcal{P}}} : |G_{\hat{\mathcal{P}}}| = \frac{n}{r} \stackrel{\text{Thm. 11}}{=} e' \cdot f' \cdot \underbrace{r'}_{=1(\text{by i})} \stackrel{1)}{=} e \cdot f \Rightarrow e' = e, f' = f$  and

$e'' = 1 = f'' \Rightarrow \text{Claim.}$

□

**Definition 2.9.6.** In our general setting we call  $\kappa(\hat{\mathcal{P}}) := \hat{\mathcal{O}}/\hat{\mathcal{P}}$  the residue class field („Restklassenkörper“).

*Remark 2.9.7.* Prop 9.5 iii)  $\Rightarrow [\kappa(\hat{\mathcal{P}}_Z) : \kappa(\mathcal{P})] = 1$  hence,  $\kappa(\hat{\mathcal{P}}_Z) = \kappa(\mathcal{P}) = \mathcal{O}/\mathcal{P} =: k$ .

**Proposition 2.9.8.** If  $\hat{\mathcal{P}}/\mathcal{P}$  is non-split, i.e.  $\hat{\mathcal{P}}$  is the only prime ideal over  $\mathcal{P}$ , then we obtain the following surjective group homomorphism:  $\varphi : G = \text{Gal}(L/K) \rightarrow \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P}))$ .

*Proof.* Step 1:  $\varphi$  is well-defined:

Since  $\hat{\mathcal{P}}/\mathcal{P}$  is totally split, we have  $\sigma(\hat{\mathcal{P}}) = \hat{\mathcal{P}}$ . Therefore  $\sigma \in \text{Gal}(L/K)$  induces an automorphism of  $\kappa(\hat{\mathcal{P}})$ .

Step 2:  $\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P})$  is a normal extension:

Denote  $k := \kappa(\mathcal{P})$  and  $\kappa := \kappa(\hat{\mathcal{P}})$ . Consider  $\bar{\theta} \in \kappa$  and let  $\bar{g} \in k[X]$  be its minimal polynomial over  $k$ . Have to show that  $\bar{g}$  decomposes into linear factors over  $\kappa$ . Let  $\theta$  be a preimage of  $\bar{\theta}$  in  $\hat{\mathcal{O}}$  and  $f \in \mathcal{O}[X]$  its minimal polynomial  $\Rightarrow f(\bar{\theta}) = 0$ . Let  $\bar{f}$  be the image of  $f$  in  $k[X]$ , hence  $\bar{f}(\bar{\theta}) = 0$  and thus  $\bar{g}$  divides  $\bar{f}$ .

Furthermore:  $L/K$  is normal  $\Rightarrow f$  decomposes into linear factors over  $L \Rightarrow$  also over  $\hat{\mathcal{O}}$ , since Galois-Automorphisms preserve  $\hat{\mathcal{O}} \Rightarrow \bar{f}$  decomposes into linear factors over  $\kappa = \hat{\mathcal{O}}/\mathcal{P} \Rightarrow \bar{g}$  does so.

Step 3:  $\varphi$  is surjective:

Let  $\bar{\sigma} \in \text{Aut}(\kappa/k)$ . Consider the field extension:  $k \subseteq E \subseteq \underbrace{\kappa}_{\text{purely inseparable} \Rightarrow \text{Aut}(\kappa/E)=\{1\}}$   $(\star)$

with  $E$  is the maximal separable field extension.

$\Rightarrow \exists \bar{\theta} \in E$  with  $E = k(\bar{\theta})$  and  $\theta \in \hat{\mathcal{O}}$  a preimage. Let again  $\bar{g} \in k[X]$  be the minimal polynomial of  $\bar{\theta}$  and  $f, \bar{f}$  as in Step 2.

$\Rightarrow \bar{\sigma}(\bar{\theta})$  is a zero of  $\bar{g}$ , hence  $(X - \bar{\sigma}(\bar{\theta}))$  divides  $\bar{g}$  and hence  $\bar{f}$  since  $\bar{g}, f$  and  $\bar{f}$  decompose into linear factors.

$\Rightarrow \exists \theta' \in \hat{\mathcal{O}}$  with  $\theta' \bmod \hat{\mathcal{P}} = \bar{\sigma}(\bar{\theta})$  and  $\theta'$  is a zero of  $f$  (there is a linear factor  $(X - \theta')$  of  $f$  which is sent to the factor  $(X - \bar{\sigma}(\bar{\theta}))$  of  $\bar{f}$ )

$\Rightarrow \exists \sigma \in \text{Gal}(L/K)$  with  $\sigma(\theta) = \theta'$  and thus  $\sigma(\theta) \equiv \theta' \equiv \bar{\sigma}(\bar{\theta}) \bmod \hat{\mathcal{P}}$ .

$\Rightarrow \varphi(\sigma)|_E = \bar{\sigma}|_E \xrightarrow{(\star)} \varphi(\sigma) = \bar{\sigma}$  □

*Remark 2.9.9.* Observe that for Step 2 we did not need that  $\hat{\mathcal{P}}/\mathcal{P}$  is non-split. Hence we have in the general situation of this section:

$$L/K \text{ normal} \Rightarrow \kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P}) \text{ is normal.}$$

**Proposition 2.9.10.** *In general, we obtain the following surjective group homomorphism:*

$$G_{\hat{\mathcal{P}}} \rightarrow \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P})) , \sigma \mapsto (a \bmod \hat{\mathcal{P}} \mapsto \sigma(a) \bmod \hat{\mathcal{P}})$$

*Proof.* Idea: Consider  $\kappa \subseteq Z_{\hat{\mathcal{P}}} \subseteq L$ . Remark 9.7  $\Rightarrow \kappa(\hat{\mathcal{P}}_Z) = k := \kappa(\mathcal{P})$

Lemma 9.8  $\Rightarrow \underbrace{\text{Gal}(L/Z_{\hat{\mathcal{P}}})}_{=G_{\hat{\mathcal{P}}}} \twoheadrightarrow \underbrace{\text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\hat{\mathcal{P}}_Z))}_{\text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P}))} \Rightarrow \text{Claim.}$  □

**Definition 2.9.11** („Trägheitsgruppe“/„Trägheitskörper“). Let  $\varphi : G_{\hat{\mathcal{P}}} \twoheadrightarrow \text{Gal}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P}))$  be the surjective group homomorphism from Prop. 9.10.

i)  $I_{\hat{\mathcal{P}}} := \ker(\varphi)$  is called inertia group.

ii)  $T_{\hat{\mathcal{P}}} := \{x \in L \mid \sigma(x) = x \forall \sigma \in I_{\hat{\mathcal{P}}}\}$  is called inertia field.

*Remark 2.9.12.* i) We obtain the following chain of field extensions:

$$\kappa \subseteq Z_{\hat{\mathcal{P}}} \subseteq T_{\hat{\mathcal{P}}} \subseteq L$$

ii) We have the following short exact sequence:

$$1 \rightarrow I_{\hat{\mathcal{P}}} \rightarrow G_{\hat{\mathcal{P}}} \rightarrow \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P})) \rightarrow 1$$

**Proposition 2.9.13.** *In the situation of 9.12 we have:*

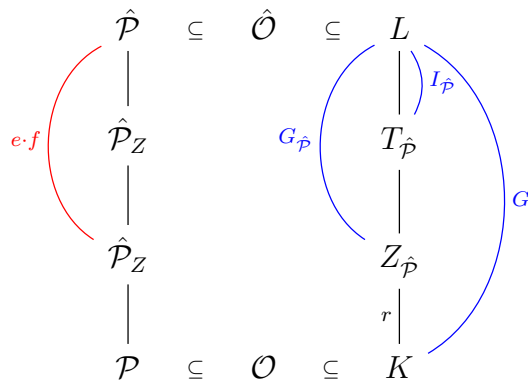
i)  $T_{\hat{\mathcal{P}}}/Z_{\hat{\mathcal{P}}}$  is normal and  $\text{Gal}(T_{\hat{\mathcal{P}}}/Z_{\hat{\mathcal{P}}}) \cong \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P}))$ .

Furthermore:  $\text{Gal}(L/T_{\hat{\mathcal{P}}}) \cong I_{\hat{\mathcal{P}}}$ .

ii) If  $\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P})$  is separable, then:  $\#I_{\hat{\mathcal{P}}} = [L : T_{\hat{\mathcal{P}}}] = e$  and  $[G_{\hat{\mathcal{P}}} : I_{\hat{\mathcal{P}}}] = [T_{\hat{\mathcal{P}}} : Z_{\hat{\mathcal{P}}}] = f$

iii) If  $\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P})$  is separable and  $\hat{\mathcal{P}}_T := \hat{\mathcal{P}} \cap T_{\hat{\mathcal{P}}}$ , then we have

- The ramification index of  $\hat{\mathcal{P}}$  over  $\hat{\mathcal{P}}_T$  is  $e$  and the local degree is 1.
- The ramification index of  $\hat{\mathcal{P}}_T$  over  $\hat{\mathcal{P}}_Z$  is 1 and the local degree is  $f$ .



*Proof.* i) •  $I_{\hat{\mathcal{P}}}$  is normal in  $G_{\hat{\mathcal{P}}}$ .

- $\text{Gal}(T_{\hat{\mathcal{P}}}/Z_{\hat{\mathcal{P}}}) \cong G_{\hat{\mathcal{P}}}/I_{\hat{\mathcal{P}}} \stackrel{\text{Rem 9.12}}{\cong} \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P}))$
- $T_{\hat{\mathcal{P}}}$  is the fixed field of  $I_{\hat{\mathcal{P}}}$

$$\text{ii) } \kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P}) \text{ is separable} \Rightarrow \# \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\mathcal{P})) = \underbrace{[\kappa(\hat{\mathcal{P}}) : \kappa(\mathcal{P})]}_{\hat{\mathcal{O}}/\hat{\mathcal{P}}} \stackrel{9.12}{=} \underbrace{\#G_{\hat{\mathcal{P}}}}_{e \cdot f} / \#I_{\hat{\mathcal{P}}} = f$$

iii) We will show below that  $\kappa(\hat{\mathcal{P}}_T) = \kappa(\hat{\mathcal{P}})$ . This implies:

- local degree of  $\hat{\mathcal{P}}_T/\hat{\mathcal{P}}$  is 1
- ramification index of  $\hat{\mathcal{P}}_T/\hat{\mathcal{P}}$  is  $e$  since  $[L/T_{\hat{\mathcal{P}}}] = \#I_{\hat{\mathcal{P}}} = e$
- multiplicativity of  $e$  and  $f \Rightarrow \text{rest } \checkmark$

Show that  $\kappa(\hat{\mathcal{P}}_T) = \kappa(\hat{\mathcal{P}})$ :

Use Lemma 9.8  $\Rightarrow$  Obtain surjective group homomorphism

$$I_{\hat{\mathcal{P}}} = \text{Gal}(L/T_{\hat{\mathcal{P}}}) \xrightarrow{\varphi} \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\hat{\mathcal{P}}_T))$$

By definition of  $I_{\hat{\mathcal{P}}}$  the image of this homomorphism is trivial.

$$\Rightarrow \text{Aut}(\kappa(\hat{\mathcal{P}})/\kappa(\hat{\mathcal{P}}_T)) = \{1\} \stackrel{\text{normal} + \text{separable}}{\implies} [\kappa(\hat{\mathcal{P}}) : \kappa(\hat{\mathcal{P}}_T)] = 1.$$

□

**Morning session of 8th January come here**

**Lemma 2.10.5.** *s. morning session*

*Proof.* Step 2: Show:  $f_1 = f_2 = \dots = f_r = h_0 := \min\{k \mid p^k \equiv 1 \pmod{n}\}$

Recall:  $f(X) = \phi_n(X)$ ,  $h(X) := \text{image in } \mathcal{F}_p[X] = h_1^{l_1}(X) \cdot \dots \cdot h_r^{l_r}(X)$

Consider the field  $L := \mathcal{F}_{p^{h_0}}$  with  $p^{h_0}$  elements as field extension of  $\mathcal{F}_p$ . Write  $p^{k_0} - 1 = nw$  with  $w \in \mathbb{N}$ .

Observe:  $L^\times = \langle a \rangle$  with  $\text{ord}(a) = nw \Rightarrow \bar{\zeta} = a^w$  is a primitive  $n$ -th root of unity and  $h$  decomposes into linear factors over  $L$ .

Furthermore:  $L = \mathcal{F}_p(\bar{\zeta})$  by minimality of  $k_0$ , since  $\#\mathcal{F}_p[\bar{\zeta}] = p^M$  for some  $M$  and  $\text{ord}(\bar{\zeta}) = n$  divides  $p^M - 1 \Rightarrow k_0 = M$ .

Let  $\bar{f}_1(X)$  be the minimal polynomial of  $\bar{\zeta}$  over  $\mathcal{F}_p \Rightarrow$

- $\bar{f}_1$  is an irreducible divisor of  $h(X) \Rightarrow \text{w.l.o.g. } \bar{f}_1 = h_1$
- $f_1 = \deg(h_1) = \deg(\bar{f}_1) = [L : \mathcal{F}_p] = k_0 \Rightarrow f_1 = k_0$

□

**Proposition 2.10.6** (CHARACTERISATION OF PRIME IDEALS). *Let  $n = p_1^{k_1} \dots p_r^{k_r}$  be the prime decomposition of  $n$  and  $p$  some arbitrary prime number.*

*Then  $p\mathcal{O} = (\hat{\mathcal{P}}_1 \dots \hat{\mathcal{P}}_r)^{e_p}$  with  $e_p = \varphi(p^{k_p})$  is the factorisation into prime ideals and each prime ideal  $\hat{\mathcal{P}}_i$  is of local degree  $f_p := \min\{k \in \mathbb{N} \mid p^k \equiv 1 \pmod{\frac{n}{p^{k_p}}}\}$*

*Proof.* Again: Use Prop. 8.15 which applies to all prime ideals in  $\mathcal{O}$

$\Rightarrow \phi_n(X) \in \mathbb{Z}[X]$  min. polynomial of  $\zeta \Rightarrow \bar{\phi}_n(X) \in \mathcal{F}_p[X]$  image in  $\mathcal{F}_p[X]$ .

Denote  $n = mp$  with  $\gcd(p, m) = 1$ , i.e.  $a = k_p$ .

Remember  $U_m^\times = \{\text{primitive } m\text{-th roots of unity}\} \cong ((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$  ( $\zeta^k \leftrightarrow k$ ).

Use the isomorphism:

$$\begin{aligned} U_m^\times \times U_{p^a}^\times &\rightarrow U_n, (\xi, \eta) \mapsto \xi \cdot \eta \\ \Rightarrow \phi_n(X) &= \prod_{g \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^g) = \prod_{\substack{\xi \in U_m^\times, \\ \eta \in U_{p^a}^\times}} (X - \xi\eta) \end{aligned}$$

Step 1: Show that  $\phi_n(X) \equiv \phi_m(X)^{\varphi(p^a)} \pmod{p}$

(1) Observe:  $X^{p^a} - 1 \equiv (X - 1)^{p^a} \pmod{p}$ . For prime ideal  $\hat{\mathcal{P}}$  over  $(p)$ :

$$X^{p^a} - 1 \equiv (X - 1)^{p^a} \pmod{\hat{\mathcal{P}}}$$

Let  $\eta_1, \dots, \eta_{\varphi(p^a)}$  be the  $p^a$ -th roots of unity.

$$0 = \eta_j^{p^a} - 1 \equiv (\eta_j - 1)^{p^a} \pmod{\hat{\mathcal{P}}} \Rightarrow \eta_j \equiv 1 \pmod{\hat{\mathcal{P}}}.$$

(2)

$$\begin{aligned} \phi_n(X) &= \prod_{\substack{\xi \in U_m^\times, \\ \eta \in U_{p^a}^\times}} (X - \xi\eta) = \prod_{g \in (\mathbb{Z}/m\mathbb{Z})^\times} (X - \xi)^{\varphi(p^a)} = \phi_m^{\varphi(p^a)} \pmod{\hat{\mathcal{P}}} \\ \Rightarrow \phi_n(X) &\equiv \phi_m(X)^{\varphi(p^a)} \pmod{p} \end{aligned}$$

Step 2: Use Lemma 10.5:

Proof of Lemma 10.5  $\Rightarrow$  exponents of  $\phi_m(X) \bmod p$  are all 1  $\Rightarrow$  all exponents of  $\phi_n(X) \bmod p$  are  $\varphi(p^a)$ . The local degree of the prime factors are by Lemma 10.5  $f = \min\{k \in \mathbb{N} \mid p^k \equiv 1 \bmod \underbrace{m}_{=n/p^a}\}$ .  $\square$

**Corollary 2.10.7.** *i)  $p$  is ramified in  $\mathbb{Q}(\zeta) \iff n \equiv 0 \bmod p$  and we have not  $p = 2 = \gcd(4, n)$ .*

*ii)  $p \neq 2$ . Then  $p$  is totally split  $\iff p \equiv 1 \bmod n$ .*

*Proof.* i) Prop. 10.6  $\Rightarrow p$  is unramified  $\iff e = 1 \xrightarrow{\text{Prop 10.6}} \varphi(p^{k_p}) = 1 \iff k_p = 0$  or  $p^{k_p} - p^{k_p-1} = p^{k_p-1}(p - 1) = 1 \iff k_p = 0$  or  $(p = 2 \text{ and } 2 = \gcd(4, n))$ .

ii)  $p \neq 2 : e = 1 \iff k_p = 0 \iff p \nmid n$   
 $f = 1 \iff \min\{k \mid p^k \equiv 1 \bmod \frac{n}{p^k}\} = 1 \iff p \equiv 1 \bmod n$ .  $\square$

*Remark 2.10.8.* We have now in particular proved I.2.2.

# 3 Fermat's theorem for regular primes

## 3.1 The proof using a lemma of Kummer

Setting:  $K$ -number field,  $\mathcal{O}$  = ring of integers

Recall:  $\mathcal{J}_K$  := group of fractional ideals,  $\mathcal{P}_K$  = subgroup of principal ideals,  $\text{Cl}_K = \mathcal{J}_K / \mathcal{P}_K$ ,  $h_K = \# \text{Cl}_K$

**Definition 3.1.1.** A prime  $p \in \mathbb{N}$  is regular :  $\iff h_K$  is not divisible by  $p$  where  $K = \mathbb{Q}(\zeta_p)$ .

*Remark 3.1.2.* Suppose  $p$  regular. Then we have for each ideal  $I$  in  $\mathcal{O}$  = ring of integers in  $K$ :

If  $I^p$  is a principal ideal, then  $I$  is a principal ideal.

*Proof.*  $p \nmid h_K \Rightarrow$  No element of  $\text{Cl}_K$  has order  $p$ . □

Recall: (Lemma I.2.11)  $x, y \in \mathbb{Z}$ ,  $\gcd(x, y) = 1$ ,  $x + y \not\equiv 0 \pmod{p}$   
 $\Rightarrow x + \zeta^i y$  and  $x + \zeta^j y$  are coprime, if  $i \not\equiv j \pmod{p}$ .

**Theorem 12.** If  $p$  is a regular prime, then Fermat's theorem holds, i.e.

$$x^p + y^p = z^p \text{ in } \mathbb{Z} \Rightarrow xyz = 0.$$

Recall:

- (1)  $x^p + y^p = (x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y)$  in  $\mathbb{Z}[\zeta]$ .
- (2)  $\lambda = 1 - \zeta$  is prime in  $\mathcal{O} = \mathbb{Z}[\zeta]$
- (3)  $1 - \zeta \sim 1 - \zeta^g$  for all  $g \not\equiv 0 \pmod{p}$

**Lemma 3.1.3.** Suppose that  $x, y \in \mathcal{O}$  with  $x, y$  are coprime and  $p$  does not divide  $y$ .

Then we have: either the ideals  $(x + \zeta^i y)$  (with  $i \in \{0, \dots, p-1\}$ ) are relatively prime or they all have  $(1 - \zeta)$  as a common factor and the ideals  $(\frac{x + \zeta^i y}{1 - \zeta})$  (with  $i \in \{0, \dots, p-1\}$ ) are relatively prime.

*Proof.* Use from the proof of Lemma I.2.11: Let  $0 \leq j < i \leq p-1$ .  $A := (x + \zeta^i y, x + \zeta^j y) \Rightarrow$

- (1)  $(1 - \zeta) \cdot y \in A$

$$(2) (1 - \zeta)x \in A$$

$$(3) 1 - \zeta \in A \text{ and thus } p \in A$$

$$(4) x + y \in A$$

Suppose  $q$  is a prime ideal with  $q|(x + \zeta^i \cdot y)$  and  $q|(x + \zeta^j \cdot y)$ .

Hence  $q \supseteq A \ni 1 - \zeta \xrightarrow{1-\zeta \text{ prime}} q = (1 - \zeta)$ .

Hence  $q = (1 - \zeta)$  is the only prime ideal which possibly divides  $(x + \zeta^i \cdot y), (x + \zeta^j \cdot y)$ .

Show: If  $q = (1 - \zeta)$  divides  $(x + \zeta^i \cdot y)$ , then it divides  $(x + \zeta^{i+1} \cdot y)$ .

This follows from the following calculation:  $x + \zeta^{i+1} \cdot y = x + \zeta^i \cdot y + \zeta^i(\zeta - 1) \cdot y$

Finally show: If  $(1 - \zeta)$  divides  $x + \zeta^i \cdot y$ , then the  $(\frac{x+\zeta^i \cdot y}{1-\zeta})$  and  $(\frac{x+\zeta^j \cdot y}{1-\zeta})$  are coprime for  $0 \leq j < i \leq p-1$ .

Recall:  $p \nmid y \Rightarrow 1 - \zeta \nmid y$

Proof:  $x + \zeta^i \cdot y - (x + \zeta^j \cdot y) = \zeta^j \cdot y \underbrace{(\zeta^{i-j} - 1)}_{\sim (\zeta-1)} \Rightarrow \frac{x+\zeta^i \cdot y}{1-\zeta} - \frac{x+\zeta^j \cdot y}{1-\zeta} \sim y$ .

But  $(1 - \zeta) \nmid y \Rightarrow$  Claim. □

**Proposition 3.1.4** (“First Case”). Suppose  $p$  is a regular prime with  $p \geq 5$  such that  $x^p + y^p = z^p$  and  $p \nmid xyz$  with  $x, y, z \in \mathbb{Z}$ . Then  $xyz = 0$ .

*Proof.* Without loss of generality we may assume that  $x, y, z$  are coprime. Proceed as in the proof of Theorem 1:

- $z^p = x + y^p = (x + y)(x + \zeta y) \cdots (x + \zeta^{p-1}y)$
- Since  $p \nmid z$  we have  $x + y \equiv x^p + y^p = z^p \equiv z \not\equiv 0$  by little Fermat’s theorem such that  $p \nmid x + y$ .
- Lemma 2.11 implies that  $(x + y), (x + \zeta y), \dots, (x + \zeta^{p-1}y)$  are pairwise coprime such that the first bullet point together with the regularity of  $p$  and Remark 1.2 yields  $(x + \zeta^i y) = (\alpha_i)^p$  for some  $\alpha_i \in \mathcal{O}$ . Thus  $x + \zeta^i y = \varepsilon_i \alpha_i^p$  with  $\varepsilon_i \in \mathcal{O}^\times$ .

Now continue as in the proof of Theorem 1. □

*Recall* (Example 1.2.8). If  $\alpha \in \mathcal{O}$  then  $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$  such that

$$\alpha^p \equiv \underbrace{a_0^p + a_1^p + \cdots + a_{p-2}^p}_{=a \in \mathbb{Z}} \pmod{p}.$$

**Lemma 3.1.5** (Kummer’s Lemma II). Suppose  $p$  is a regular prime. If  $u \in \mathcal{O}^\times$  such that  $u \equiv a \pmod{p}$  for some  $a \in \mathbb{Z}$  then there is an  $\alpha \in \mathcal{O}^\times$  such that  $u = \alpha^p$ .

The proof is hard and needs more theory.

*Remark 3.1.6.*  $1, 1 - \zeta, \dots, (1 - \zeta)^{p-2}$  is an integral basis of  $\mathcal{O} = \mathbb{Z}[\zeta]$ .



*Proof.*  $1, \zeta, \dots, \zeta^{p-2}$  is an integral basis by Proposition 2.10.4. Furthermore,

$$\zeta^i = (1 - (1 - \zeta))^i = \sum_{k=0}^i \binom{k}{i} (-1)^{i-k} (1 - \zeta)^{i-k}$$

and  $1 - \zeta$  has minimal polynomial of degree lesser equal than  $p - 1$ .  $\square$

**Lemma 3.1.7.** *If  $\alpha \in \mathcal{O} \setminus (1 - \zeta)$  then there exist  $a \in \mathbb{Z}$  and  $l \in \mathbb{N}_0$  such that*

$$\zeta^l \alpha \equiv a \pmod{(1 - \zeta)^2}.$$

*Proof.* We do the proof in multiple steps:

(1) Since  $1, 1 - \zeta, \dots, (1 - \zeta)^{p-2}$  is an integral basis of  $\mathcal{O}$  we have

$$\alpha \equiv a_0 1 + a_1 (1 - \zeta) \pmod{(1 - \zeta)^2}$$

with  $a_0, a_1 \in \mathbb{Z}$ .

(2) Since  $1 - \zeta \nmid \alpha$  we have  $1 - \zeta \nmid a_0$  such that  $p \nmid a_0$  and hence there is  $l \in \mathbb{Z}$  with  $a_0 l \equiv a_1 \pmod{p}$ .

(3) Since  $\zeta = 1 - (1 - \zeta)$  we have

$$\zeta^l \equiv 1 - l(1 - \zeta) \pmod{(1 - \zeta)^2}.$$

(4) By (1), (2) and (3) we conclude

$$\begin{aligned} \zeta^l \alpha &\equiv (1 - l(1 - \zeta)) (a_0 + a_1 (1 - \zeta)) \\ &\equiv a_0 + (a_1 - l a_0) (1 - \zeta) \\ &\equiv a_0 \pmod{(1 - \zeta)^2}. \end{aligned}$$

$\square$

**Proposition 3.1.8** (“Second case”). *Suppose  $p$  is a regular prime with  $p \geq 5$  such that  $x^p + y^p = z^p$  and  $p \mid xyz$  with  $x, y, z \in \mathbb{Z}$ . Then  $xyz = 0$ .*

*Proof.* Without loss of generality  $x, y, z$  are pairwise coprime. By changing the role of  $x, y$  and  $z$  and possibly replacing  $x$  by  $-x$ ,  $y$  by  $-y$  and  $z$  by  $-z$  we can furthermore assume that  $p \mid z$ ,  $p \nmid x$  and  $p \nmid y$ . Then, by 2.10.1,

$$z = p^m z_0 = \varepsilon (1 - \zeta)^{(p-1)m} z_0$$

with  $z_0 \in \mathbb{Z}$ ,  $m \geq 1$ ,  $\gcd(z_0, p) = 1$  and  $\varepsilon \in \mathcal{O}^\times$  such that

$$x^p + y^p = \varepsilon^p (1 - \zeta)^{(p-1)mp} z_0^p.$$

By assumption:

- $x, y$  and  $z_0$  are pairwise coprime since  $x, y$  and  $z$  are pairwise coprime.
- $1 - \zeta$  and  $z_0$  are coprime since  $p$  and  $z$  are coprime.
- $x$  and  $1 - \zeta$  are coprime since  $p \nmid x$ . The same holds for  $y$  and  $1 - \zeta$ .

Hence the following Lemma 1.9 yields  $xyz_0 = 0$  such that  $xyz = 0$  as claimed.  $\square$

**Lemma 3.1.9.** *Suppose  $p$  is a regular prime with  $p \geq 5$ ,  $x, y, z_0 \in \mathcal{O}$ ,  $\varepsilon \in \mathcal{O}^\times$  and  $x, y, z_0, 1 - \zeta$  are pairwise coprime. If  $x^p + y^p = \varepsilon(1 - \zeta)^{kp} z_0^p$  with  $k \in \mathbb{N}$ , then  $xyz_0 = 0$ .*

*Proof.* Assume that there are  $x, y, z_0$  as in the lemma with  $xyz_0 \neq 0$ . We may assume that  $k$  is minimal.

“**Step 1:**” Show that  $(1 - \zeta)^2 | x + y$ .

(1) By assumption we have

$$\varepsilon(1 - \zeta)^{kp} z_0^p = (x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y) \quad (*)$$

such that, since  $1 - \zeta$  is prime, there is  $i \in \{0, \dots, p-1\}$  with  $1 - \zeta | x + \zeta^i y$ . Hence  $1 - \zeta$  divides all  $x + \zeta^i y$  by Lemma 1.3, in particular  $x + y$ .

(2) By Lemma 1.7 there are  $a, b \in \mathbb{Z}$  and  $l, j \in \mathbb{N}_0$  such that

$$\zeta^l x \equiv a \pmod{(1 - \zeta)^2} \quad \text{and} \quad \zeta^j y \equiv b \pmod{(1 - \zeta)^2}.$$

(3) We may replace  $x$  by  $x\zeta^l$  and  $y$  by  $y\zeta^j$  and thus can assume that  $x \equiv a, y \equiv b \pmod{(1 - \zeta)^2}$  with  $a, b \in \mathbb{Z}$ .

(4)  $1 - \zeta | x + y$  implies  $1 - \zeta | a + b$  such that  $(1 - \zeta)^{p-1} | a + b$  and hence  $(1 - \zeta)^2 | x + y$ . In particular,  $k \geq 2$ .

“**Step 2:**” Show that  $(1 - \zeta)^{(k-1)p+1} | x + y$ .

Since the quotients  $\frac{x + \zeta^i y}{1 - \zeta}$  are pairwise coprime, all “extra powers” of  $1 - \zeta$  have to divide  $x + y$ . Thus,

$$(1 - \zeta)^{kp-(p-1)} | x + y.$$

Furthermore:

$$1 - \zeta \nmid \frac{x + y}{(1 - \zeta)^{kp-(p-1)}}$$

“**Step 3:**” Show that  $\frac{x + \zeta^i y}{1 - \zeta}$  is associated to a  $p$ -power.

From (\*) we obtain

$$((1 - \zeta)^{k-1} z_0)^p = \prod_{i=0}^{p-1} \left( \frac{x + \zeta^i y}{1 - \zeta} \right).$$

Since the ideals on the right side are pairwise coprime,  $\left(\frac{x+\zeta^i y}{1-\zeta}\right)$  is a  $p$ -th power. Thus Remark 1.2 yields

$$\frac{x + \zeta^i y}{1 - \zeta} = \varepsilon_i \alpha_i^p$$

with  $\alpha_i \in \mathcal{O}$  and  $\varepsilon \in \mathcal{O}^\times$ . Furthermore, the  $\alpha_i$  are pairwise coprime.

**“Step 4:”** Find  $\varepsilon', \eta \in \mathcal{O}^\times$  and  $\beta \in \mathcal{O}$  with  $\varepsilon'(1 - \zeta)^{(k-1)p} \beta^p = -\alpha_1^p + \eta \alpha_{-1}^p$ .

By Step 2,  $(1 - \zeta)^{k-1}$  divides  $\alpha_0$ . More precisely,  $\alpha_0 = (1 - \zeta)^{k-1} \beta$  with  $\beta \in \mathcal{O}$  and  $1 - \zeta, \beta$  coprime. Do some ugly calculation:

$$y = \frac{x + y - (x + \zeta y)}{1 - \zeta} = \varepsilon_0 \alpha_0^p - \varepsilon_1 \alpha_1^p = \varepsilon_0 (1 - \zeta)^{(k-1)p} \beta^p - \varepsilon_1 \alpha_1^p \quad (\text{A})$$

$$y = \frac{(x + \zeta^{-1} y) - (x + y)}{\zeta^{-1}(1 - \zeta)} = \zeta \varepsilon_{-1} \alpha_{-1}^p - \zeta \varepsilon_0 \alpha_0^p = \zeta \varepsilon_{-1} \alpha_{-1}^p - \zeta \varepsilon_0 (1 - \zeta)^{(k-1)p} \beta^p \quad (\text{B})$$

Then (B) – (A) yields

$$0 = \zeta \varepsilon_{-1} \alpha_{-1}^p + \varepsilon_1 \alpha_1^p + \varepsilon_0 (1 - \zeta)^{p(k-1)} \beta^p (-\zeta - 1).$$

Now define

$$\varepsilon' = \frac{(1 + \zeta) \varepsilon_0}{-\varepsilon_1} \quad \text{and} \quad \eta = \frac{\zeta \varepsilon_{-1}}{-\varepsilon_1}$$

to obtain

$$\varepsilon' (1 - \zeta)^{p(k-1)} \beta^p = \eta \alpha_{-1}^p = \alpha_1^p. \quad (**)$$

**“Step 5:”** Show that  $\eta$  is a  $p$ -th power.

By (\*\*) we have  $0 \equiv \eta \alpha_{-1}^p - \alpha_1^p \pmod{p}$  such that Example 1.2.8 ascertains the existence of  $a_{-1}, a_1 \in \mathbb{Z}$  with  $\alpha_{-1}^p \equiv a_{-1}, \alpha_1^p \equiv a_1 \pmod{p}$ .  $\square$