

# 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  $\alpha\beta = 1 \Rightarrow 1 = N(\alpha\beta) \stackrel{!}{=} \underbrace{N(\alpha)}_{\in \mathbb{Z}} \underbrace{N(\beta)}_{\in \mathbb{Z} \text{ by 2.2 v)} \Rightarrow \text{claim}$

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

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

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

**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  $\text{gcd}(m', p) = 1$ . 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 1.2.9** (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 1.2.10.**  $\varepsilon \text{ unit in } \mathbb{Z}[\zeta] \Rightarrow \varepsilon = r \zeta^s \text{ with some } r \in \mathbb{R}, s \in \mathbb{Z}.$

*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 1.2.11.** 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 1.2.12.* 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 1.3.1.** 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 1.3.2** ( $p = 3$ ). 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  $x^p \equiv x, y^p \equiv y, z^p \equiv z \pmod{p}$ .

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

□



**Lemma 1.3.3.** *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 1.3.4.* 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:

- $\gcd(x, y) = 1$  ✓
- 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

$$1 = c_1w_1 + \dots + c_rw_r$$

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  $A$ . □

**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  $b_1b_2$  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). □

**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

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

- $\text{Tr}_{L/\mathbb{Q}}(a + b\sqrt{D}) = a + b\sqrt{D} + a - b\sqrt{D} = 2a$ .
- $\mathcal{N}_{L/\mathbb{Q}}(a + b\sqrt{D}) = (a + b\sqrt{D}) \cdot (a - b\sqrt{D}) = a^2 - b^2 \cdot D$ .
- $d(\mathfrak{B}_1) = \det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^2 = (-2\sqrt{D})^2 = 4D$ .
- 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:  $\det(T)^2 = d'$

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

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

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

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

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

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:

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

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

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

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

*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.  $\square$

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

**Theorem 2.3.4.** *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 2.3.5.** *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 2.3.6.** 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 2.3.7.** 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 2.3.8.* 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 2.3.9** (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 2.3.10.** 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 2.3.11.** *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 2.3.12.** *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 2.3.13.** 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.  $\square$