

# Notes on the book: *Jürgen Neukirch, Algebraic Number Theory*

Meng-Gen Tsai  
plover@gmail.com

October 4, 2021

## Contents

<b>Chapter I: Algebraic Integers</b>	<b>3</b>
I.1. The Gaussian Integers . . . . .	3
Exercise I.1.1. . . . .	3
Exercise I.1.2. . . . .	3
Exercise I.1.3. (Pythagorean triples) . . . . .	4
Exercise I.1.4. . . . .	5
Exercise I.1.5. . . . .	5
Exercise I.1.6. . . . .	5
I.2. Integrality . . . . .	7
Exercise I.2.1. . . . .	7
Exercise I.2.2. . . . .	7
Exercise I.2.3. . . . .	8
Exercise I.2.4. . . . .	9
Exercise I.2.7. (Stickelberger's discriminant relation) . . . . .	10
I.3. Ideals . . . . .	11
Exercise I.3.4. . . . .	11
Exercise I.3.5. . . . .	12
Exercise I.3.6. . . . .	12
I.4. Lattices . . . . .	12
Exercise I.4.1. . . . .	12
Exercise I.4.2. . . . .	13
I.5. Minkowski Theory . . . . .	14
Exercise I.5.2. . . . .	14
Exercise I.5.3. (Minkowski bound) . . . . .	14
I.6. The Class Number . . . . .	15
Exercise I.6.3. . . . .	15
I.7. Dirichlet's Unit Theorem . . . . .	16

Exercise I.7.3. (The Battle of Hastings (October 14, 1066)) . . .	16
I.11. Localization . . . . .	16
Exercise I.11.7. (Nakayama's lemma) . . . . .	16
I.13. One-dimensional Schemes . . . . .	17
I.14. Function Fields . . . . .	17
<b>Chapter II: The Theory of Valuations</b>	<b>18</b>
II.1. The $p$ -adic Numbers . . . . .	18
Exercise II.1.2. . . . .	18
Supplement II.1.2.1. . . . .	19
II.2. The $p$ -adic Absolute Value . . . . .	19
Exercise II.2.1. . . . .	19
<b>Chapter VII: Zeta Functions and <math>L</math>-series</b>	<b>20</b>
VII.1. The Riemann Zeta Function . . . . .	20
Exercise VII.1.4. . . . .	20

# Chapter I: Algebraic Integers

## I.1. The Gaussian Integers

### Exercise I.1.1.

$\alpha \in \mathbb{Z}[i]$  is a unit if and only if  $N(\alpha) = 1$ .

*Proof.*

- (1) ( $\implies$ ) Since  $\alpha$  is a unit, there is  $\beta \in \mathbb{Z}[i]$  such that  $\alpha\beta = 1$ . So  $N(\alpha\beta) = N(1)$ , or  $N(\alpha)N(\beta) = 1$ . Since the image of  $N$  is nonnegative integers,  $N(\alpha) = 1$ .
- (2) ( $\impliedby$ )  $N(\alpha) = \alpha\bar{\alpha}$ , or  $1 = \alpha\bar{\alpha}$  since  $N(\alpha) = 1$ . That is,  $\bar{\alpha} \in \mathbb{Z}[i]$  is the inverse of  $\alpha \in \mathbb{Z}[i]$ . (Or we solve the equation  $N(\alpha) = a^2 + b^2 = 1$ , and show that all four solutions ( $\pm 1$  and  $\pm i$ ) are units.)
- (3) Conclusion: a unit  $\alpha = a + bi$  of  $\mathbb{Z}[i]$  is satisfying the equation  $N(\alpha) = a^2 + b^2 = 1$  by (1)(2). That is, the only unit of  $\mathbb{Z}[i]$  are  $\pm 1$  and  $\pm i$ .

□

### Exercise I.1.2.

Show that, in the ring  $\mathbb{Z}[i]$ , the relation  $\alpha\beta = \varepsilon\gamma^n$ , for  $\alpha, \beta$  relatively prime numbers and  $\varepsilon$  a unit, implies  $\alpha = \varepsilon'\xi^n$  and  $\beta = \varepsilon''\eta^n$ , with  $\varepsilon', \varepsilon''$  units.

*Proof.*

- (1) It suffices to prove that the conclusion holds for any unique factorization domain  $R$  (since  $\mathbb{Z}[i]$  is a unique factorization domain).
- (2) Write the unique factorizations of  $\alpha, \beta, \gamma$  as

$$\alpha = \varepsilon_1 p_1^{a_1} \cdots p_r^{a_r}, \quad \beta = \varepsilon_2 p_1^{b_1} \cdots p_r^{b_r}, \quad \gamma = \varepsilon_3 p_1^{c_1} \cdots p_r^{c_r},$$

where  $p_i$  are prime elements in  $R$ ,  $p_i \neq p_j$  if  $i \neq j$  (up to unit), and  $\varepsilon_1, \varepsilon_2, \varepsilon_3$  are units.

- (3) By the relation  $\alpha\beta = \varepsilon\gamma^n$ , we have

$$\varepsilon_1 \varepsilon_2 p_1^{a_1+b_1} \cdots p_r^{a_r+b_r} = \varepsilon \varepsilon_3^n p_1^{nc_1} \cdots p_r^{nc_r} \in R.$$

Since  $R$  is a unique factorization domain,  $a_i + b_i = nc_i$  for each  $1 \leq i \leq r$ . Since  $\alpha, \beta$  are relatively prime,  $a_i = 0$  or  $b_i = 0$  for each  $i$ . Hence

$$(a_i, b_i) = (0, nc_i) \text{ or } (nc_i, 0).$$

In any case,  $\alpha = \varepsilon_1 \xi^n$  and  $\beta = \varepsilon_2 \eta^n$  for some  $\xi, \eta \in R$ .

□

### Exercise I.1.3. (Pythagorean triples)

Show that the integer solutions of the equation

$$x^2 + y^2 = z^2$$

such that  $x, y, z > 0$  and  $(x, y, z) = 1$  (“pythagorean triples”) are all given, up to possible permutation of  $x$  and  $y$ , by the formula

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2$$

where  $u, v \in \mathbb{Z}$ ,  $u > v > 0$ ,  $(u, v) = 1$ ,  $u, v$  not both odd. (Hint: Use Exercise I.1.2 to show that necessarily  $x + iy = \varepsilon \alpha^2$  with a unit  $\varepsilon$  and with  $\alpha = u + iv \in \mathbb{Z}[i]$ .)

*Proof.*

(1) Since  $x^2 + y^2 = z^2$  and  $(x, y, z) = 1$ , we might assume that  $(x, y) = 1$ ,  $x$  is odd and  $y$  is even. Thus  $z$  is odd. Write  $z^2 = x^2 + y^2 = (x + iy)(x - iy) \in \mathbb{Z}[i]$ .

(2) Show that  $x + iy$  and  $x - iy$  are relatively prime over  $\mathbb{Z}[i]$ .

(a) Suppose  $\delta \mid x \pm iy$  for some  $\delta \in \mathbb{Z}[i]$ . Consider the norm of  $\delta$ .

$$N(\delta) \mid N(x \pm iy) = x^2 + y^2 = z^2$$

implies that  $N(\delta)$  is odd.

(b)  $\delta \mid 2x = (x + iy) + (x - iy)$  and  $\delta \mid 2iy = (x + iy) - (x - iy)$  imply that  $N(\delta) \mid 4x^2$  and  $N(\delta) \mid 4y^2$ . Since  $(x, y) = 1$ ,  $N(\delta) \mid 4$  or  $N(\delta) = 1, 2, 4$ .

(c) Hence  $N(\delta) = 1$  by (1)(2). Exercise I.1.1 shows that  $\delta$  is a unit. Therefore the conclusion holds.

(3) Exercise I.1.2 shows that  $x + iy = \varepsilon(u + iv)^2$  for some  $u, v \in \mathbb{Z}$  and a unit  $\varepsilon$ . As  $x > 0$  is odd and  $y > 0$  is even, we might take  $\varepsilon = 1$  and  $u > v$ . Hence

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2$$

where  $u, v \in \mathbb{Z}$ ,  $u > v > 0$ ,  $(u, v) = 1$ . Note that  $u, v$  cannot be both odd since  $x = u^2 - v^2$  is not even.

□

**Exercise I.1.4.**

Show that the ring  $\mathbb{Z}[i]$  cannot be ordered.

*Proof.* Similar to the fact that  $i$  cannot be ordered in  $\mathbb{C}$ . Thus  $i$  cannot be ordered in  $\mathbb{Z}[i]$  either.  $\square$

**Exercise I.1.5.**

Show that the only units of the ring  $\mathbb{Z}[\sqrt{-d}] = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$ , for any rational integer  $d > 1$ , are  $\pm 1$ .

*Proof.*

- (1) Define the norm  $N$  on  $\mathbb{Z}[\sqrt{-d}]$  by

$$N(x + y\sqrt{-d}) = (x + y\sqrt{-d})(x - y\sqrt{-d}) = x^2 + y^2d,$$

i.e., by  $N(z) = |z|^2$ . It is multiplicative.

- (2) Similar to Exercise I.1.1,

$$\begin{aligned} x + y\sqrt{-d} \in \mathbb{Z}[\sqrt{-d}] \text{ is a unit} &\iff N(x + y\sqrt{-d}) = x^2 + y^2d = 1 \\ &\iff x^2 = 1 \text{ and } y = 0 \\ &\iff x = \pm 1 \text{ and } y = 0. \end{aligned}$$

Hence the only units of the ring  $\mathbb{Z}[\sqrt{-d}]$  are  $\pm 1$  ( $d > 1$ ).

$\square$

**Exercise I.1.6.**

Show that the ring  $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ , for any squarefree rational integer  $d > 1$ , has infinitely many units.

*Proof.*

- (1) Define the norm of  $z = x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]$  by  $N(z) = z\bar{z}$  or

$$N(x + \sqrt{d}y) = \underbrace{(x + \sqrt{d}y)}_{=z} \underbrace{(x - \sqrt{d}y)}_{:=\bar{z}} = x^2 - dy^2.$$

Note that a norm is multiplicative. Similar to Exercise I.1.1,  $\alpha \in \mathbb{Z}[\sqrt{d}]$  is a unit if and only if  $N(\alpha) = 1$ .

- (2) To show  $\mathbb{Z}[\sqrt{d}]$  has infinitely many units, it suffices to show the equation  $x^2 - dy^2 = 1$  has infinitely many  $(x, y)$  solutions.
- (3) If  $\xi$  is irrational then there are infinitely many rational numbers  $\frac{x}{y}$ ,  $(x, y) = 1$  such that  $\left| \frac{x}{y} - \xi \right| < \frac{1}{y^2}$ . It is followed by the pigeonhole principle.
- (4) If  $d$  is a positive squarefree integer then there is a constant  $M := 2\sqrt{d} + 1$  such that  $|x^2 - dy^2| < M$  has infinitely many solutions over  $\mathbb{Z}$ . Write  $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$ . By part (3), there exist infinitely many pairs of relatively prime integers  $(x, y)$ ,  $y > 0$  satisfying  $|x - \sqrt{d}y| < \frac{1}{y}$ . Hence

$$\begin{aligned} |x^2 - dy^2| &= |x + \sqrt{d}y| |x - \sqrt{d}y| \\ &\leq \left( |x - \sqrt{d}y| + 2\sqrt{d}y \right) |x - \sqrt{d}y| \\ &\leq 2\sqrt{d} + 1. \end{aligned}$$

- (5) By part (4), there is an integer  $m$  such that  $x^2 - dy^2 = m$  for infinitely many solutions over  $\mathbb{Z}$ . Here  $m \neq 0$ . We might assume  $x, y > 0$  and  $x$  components of solutions are distinct.
- (6) The pigeonhole principle shows that there are two distinct solutions  $(x_1, y_1)$ ,  $(x_2, y_2)$  with  $x_1 \neq x_2$  such that

$$x_1 \equiv x_2 \pmod{|m|}, \quad y_1 \equiv y_2 \pmod{|m|}.$$

Let  $\alpha = x_1 - \sqrt{d}y_1$ ,  $\beta = x_2 + \sqrt{d}y_2$  and  $\gamma = \alpha\beta$ . Hence

$$\begin{aligned} \gamma &= (x_1 - \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) \\ &= \underbrace{(x_1x_2 - dy_1y_2)}_{\equiv 0 \pmod{|m|}} + \sqrt{d} \underbrace{(x_1y_2 - x_2y_1)}_{\equiv 0 \pmod{|m|}} \\ &:= m(u + \sqrt{d}v) \end{aligned}$$

for some  $u + \sqrt{d}v \in \mathbb{Z}[\sqrt{d}]$ . Taking norms of  $\gamma = \alpha\beta$  gives  $N(\gamma) = N(\alpha)N(\beta)$  or

$$m^2(u + \sqrt{d}v) = m^2.$$

Hence  $u + \sqrt{d}v = 1$ . By construction of  $x_1, x_2$ ,  $v \neq 0$ . Therefore the equation  $x^2 - dy^2 = 1$  has one solution with  $x, y > 0$ .

- (7) By part (6), we might take a unit  $\varepsilon = x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]$  with  $x, y > 0$ . Note that  $\varepsilon \geq 1 + \sqrt{d} > 1$ . Hence there are infinitely many units

$$\varepsilon, \varepsilon^2, \varepsilon^3, \dots$$

in  $\mathbb{Z}[\sqrt{d}]$ .

□

## I.2. Integrality

### Exercise I.2.1.

Is  $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$  an algebraic integer?

*Proof.*

- (1)  $\alpha := \frac{3+2\sqrt{6}}{1-\sqrt{6}} = -3 - \sqrt{6}$ . Since the set of all algebraic integers is a ring,  $\alpha$  is an algebraic integer.
- (2) Or show that  $\alpha$  satisfies a monic equation  $x^2 + 6x + 3 = 0 \in \mathbb{Z}[x]$ .

□

### Exercise I.2.2.

Show that, if the integral domain  $A$  is integrally closed, then so is the polynomial ring  $A[t]$ .

*Proof.*

- (1) Suppose  $A$  is integrally closed in  $B$ . Show that  $A[t]$  is integrally closed in  $B[t]$ . Suppose  $f \in B[t]$  is integral over  $A[t]$ . Write

$$f^n + g_1 f^{n-1} + \cdots + g_{n-1} f + g_n = 0$$

where  $n > 0$  and  $g_i \in A[t]$ . Hence

$$\begin{aligned} f^n + g_1 f^{n-1} + \cdots + g_{n-1} f &= -g_n \in A[t] \\ \implies f(\underbrace{f^{n-1} + g_1 f^{n-2} + \cdots + g_{n-1}}_{:=g}) &\in A[t]. \end{aligned}$$

It is possible to show that  $fg \in A[t]$  implies that  $f \in A[t]$  and  $g \in A[t]$  by using the fact that  $A$  is integrally closed in  $B$ .

- (2) Suppose  $f, g$  are monic polynomials in  $B[t]$ . Show that  $fg \in A[t]$  implies that  $f \in A[t]$  and  $g \in A[t]$ . Write

$$f = \prod (t - \xi_i), \quad g = \prod (t - \eta_j)$$

in some splitting field  $F$  of  $f$  and  $g$  containing the quotient field of  $B$ . Note that each  $\xi_i$  and each  $\eta_j$  is a root of a monic equation  $fg$  in  $A[t]$ . Since  $A$  is integrally closed in  $B$ ,  $\xi_i, \eta_j \in A$ . Hence  $f, g \in A[t]$ .

- (3) To apply part (2), we need to remedy leading coefficients of  $f$  and  $g$ . Take an integer  $m > \max\{\deg(f), \deg(g_1), \dots, \deg(g_n)\}$ . Let  $f_0 = t^m + f$  be a monic polynomial in  $B[t]$ . Hence

$$\begin{aligned} & (f_0 - t^m)^n + g_1(f_0 - t^m)^{n-1} + \dots + g_n = 0 \\ \implies & f_0^n + h_1 f_0^{n-1} + \dots + h_n = 0 \end{aligned}$$

where

$$h_n = t^{mn} + (-1)^{n-1} g_1 t^{m(n-1)} + \dots + g_n \in A[t]$$

is also monic. So

$$\begin{aligned} & f_0^n + h_1 f_0^{n-1} + \dots + h_{n-1} f = -h_n \text{ is monic in } A[t] \\ \implies & f_0 \underbrace{(f_0^{n-1} + h_1 f_0^{n-2} + \dots + h_{n-1})}_{:=h_0} \in A[t] \text{ where} \\ & f_0 \text{ and } h_0 \text{ both are monic in } B[t]. \end{aligned}$$

Now we can apply part (2) safely.

- (4) In part (1), we let  $B$  be the quotient field of  $A$  and thus the quotient field of  $A[t]$  is  $B(t)$ . Hence

$$\begin{aligned} & f \in B(t) \text{ integral over } A[t] \\ \implies & f \in B(t) \text{ integral over } B[t] & (A[t] \subseteq B[t]) \\ \implies & f \in B[t] & (B[t] \text{ is a UFD}) \\ \implies & f \in B[t] \text{ integral over } A[t] \\ \implies & f \in A[t]. & ((1)) \end{aligned}$$

□

### Exercise I.2.3.

In the polynomial ring  $A = \mathbb{Q}[x, y]$ , consider the principal ideal  $\mathfrak{p} = (x^2 - y^3)$ . Show that  $\mathfrak{p}$  is a prime ideal, but  $A/\mathfrak{p}$  is not integrally closed.

*Proof.*

- (1) It is easy to show that  $x^2 - y^3$  is irreducible in  $A$ . Hence  $\mathfrak{p} = (x^2 - y^3)$  is prime since  $A$  is a UFD.
- (2) By substituting  $x = t^3$ ,  $y = t^2$ ,  $A/\mathfrak{p} \cong \mathbb{Q}[t^3, t^2]$ , with quotient field  $\mathbb{Q}(t)$  (by noting  $t = \frac{x}{y}$ ). Note that  $\mathbb{Q}[t]$  is a UFD, thus is already integrally closed. So the integral closure will be  $\mathbb{Q}[t] \supsetneq \mathbb{Q}[t^3, t^2]$ . It suggests that  $A/\mathfrak{p}$  might not be integrally closed.



- (3) (Reductio ad absurdum) If not, then the element  $\frac{x}{y}$  satisfies a monic equation  $t^2 - y = 0 \in (A/\mathfrak{p})[t]$ . So  $\frac{x}{y} \in A/\mathfrak{p}$  or  $t \in \mathbb{Q}[t^3, t^2]$ , which is absurd.

□

*Note.*

- (1) Serre's criterion for normality.
- (2) Hence smoothness is the same as normality for affine curves in  $\mathbb{Q}[x, y]$ . Note that  $x^2 - y^3$  is an irreducible cubic with a cusp at the origin  $(0, 0)$ .
- (3) There is an affine variety  $X \in \mathbb{Q}[x, y, z]$  such that  $X$  is normal but not smooth. ( $X = V(x^2 + y^2 - z^2)$  for example.)

#### Exercise I.2.4.

Let  $D$  be a squarefree rational integer  $\neq 0, 1$  and  $d$  the discriminant of the quadratic number field  $K = \mathbb{Q}(\sqrt{D})$ . Show that

$$d = \begin{cases} D & \text{if } D \equiv 1 \pmod{4}, \\ 4D & \text{if } D \equiv 2, 3 \pmod{4}. \end{cases}$$

and that an integral basis of  $K$  is given by  $\{1, \sqrt{D}\}$  in the second case, by  $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$  in the first case, and by  $\left\{1, \frac{d+\sqrt{d}}{2}\right\}$  in both case.

*Proof.*

- (1) The Galois group of  $K|\mathbb{Q}$  has two elements, the identity and an automorphism sending  $\sqrt{D}$  to  $-\sqrt{D}$ .
- (2) Note that  $\alpha \in \mathcal{O}_K$  iff  $\text{Tr}_{K|\mathbb{Q}}(\alpha), N_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$  (by noting that the equation  $x^2 - \text{Tr}_{K|\mathbb{Q}}(\alpha)x + N_{K|\mathbb{Q}}(\alpha) = 0$  has a root  $x = \alpha$ ). So given  $\alpha = x + y\sqrt{D} \in \mathcal{O}_K$ , we have

$$\begin{aligned} \text{Tr}_{K|\mathbb{Q}}(\alpha) &= 2x \in \mathbb{Z}, \\ N_{K|\mathbb{Q}}(\alpha) &= x^2 - Dy^2 \in \mathbb{Z}. \end{aligned}$$

- (3) So  $4(x^2 - Dy^2) = (2x)^2 - D(2y)^2 \in \mathbb{Z}$ . So  $D(2y)^2 \in \mathbb{Z}$  since  $2x \in \mathbb{Z}$ . So  $2y \in \mathbb{Z}$  since  $D$  is squarefree  $\neq 0, 1$ . Let  $r = 2x, s = 2y$ . Then  $r^2 - Ds^2 \equiv 0 \pmod{4}$ . Note that a square  $\equiv 0, 1 \pmod{4}$ .

(4) If  $D \equiv 1 \pmod{4}$ , then

$$\begin{aligned}
r^2 - Ds^2 &\equiv r^2 - s^2 \pmod{4} \\
&\implies r \text{ and } s \text{ has the same parity} \\
&\implies \mathcal{O}_K = \left\{ \frac{r + s\sqrt{D}}{2} : r \equiv s \pmod{2} \right\} \\
&\implies \mathcal{O}_K = \left\{ \frac{r-s}{2} + s \cdot \frac{1+\sqrt{D}}{2} : r \equiv s \pmod{2} \right\} \\
&\implies \mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \frac{1+\sqrt{D}}{2}.
\end{aligned}$$

So  $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$  is an integral basis of  $K$ . Hence

$$d = \begin{vmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{vmatrix}^2 = D.$$

(5) If  $D \equiv 2, 3 \pmod{4}$ , then

$$\begin{aligned}
r^2 - Ds^2 &\equiv r^2 + 2s^2 \text{ or } r^2 + s^2 \pmod{4} \\
&\implies \text{both } r \text{ and } s \text{ are even} \\
&\implies \text{both } x \text{ and } y \text{ are rational integers} \\
&\implies \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}.
\end{aligned}$$

So  $\{1, \sqrt{D}\}$  is an integral basis of  $K$ . Hence

$$d = \begin{vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{vmatrix}^2 = 4D.$$

(6) By (4)(5),  $\left\{1, \frac{d+\sqrt{d}}{2}\right\}$  is an integral basis of  $K$  for any case.

□

### Exercise I.2.7. (Stickelberger's discriminant relation)

The discriminant  $d_K$  of an algebraic number field  $K$  is always  $\equiv 0 \pmod{4}$  or  $\equiv 1 \pmod{4}$ . (Hint: The discriminant  $\det(\sigma_i \omega_j)$  of an integral basis  $\omega_j$  is a sum of terms, each prefixed by a positive or a negative sign. Writing  $P$  (resp.  $N$ ) for the sum of the positive (resp. negative) terms, one find  $d_K = (P - N)^2 = (P + N)^2 - 4PN$ .)

*Proof (Hint).*

- (1) Let  $S_n$  be the symmetric group of degree  $n$ , and  $A_n$  be the alternating group of degree  $n$ . So

$$\begin{aligned}\det(\sigma_i \omega_j) &= \sum_{\pi \in S_n} \left( \operatorname{sgn}(\pi) \prod_{i=1}^n \sigma_i \omega_{\pi(i)} \right) \\ &= \underbrace{\sum_{\pi \in A_n} \prod_{i=1}^n \sigma_i \omega_{\pi(i)}}_{:=P} - \underbrace{\sum_{\pi \in S_n - A_n} \prod_{i=1}^n \sigma_i \omega_{\pi(i)}}_{:=N}.\end{aligned}$$

- (2) Note that  $\sigma_i(P + N) = P + N$  and  $\sigma_i(PN) = PN$  for all  $\sigma_i$ . Hence  $P + N, PN \in \mathbb{Q}$ . Therefore  $P + N, PN \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ .

- (3) By (1)(2),

$$\begin{aligned}d_K &= \det(\sigma_i \omega_j)^2 \\ &= (P - N)^2 \\ &= (P + N)^2 - 4PN \\ &\equiv 0, 1 \pmod{4}.\end{aligned}$$

□

### I.3. Ideals

#### Exercise I.3.4.

A Dedekind domain with a finite number of prime ideals is a principal ideal domain. (Hint: If  $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r} \neq 0$  is an ideal, then choose elements  $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$  and apply the Chinese remainder theorem for the cosets  $\pi_i^{\nu_i} \pmod{\mathfrak{p}_i^{\nu_i+1}}$ .)

*Proof.*

- (1) The hint gives all.
- (2) The existence of  $\pi_i$  is guaranteed by Theorem I.3.3 (the unique prime factorization). The Chinese remainder theorem shows that there is one element  $\pi \in \mathcal{O}$  such that  $\pi = \pi_i^{\nu_i} \pmod{\mathfrak{p}_i^{\nu_i+1}}$  for each  $i$ .
- (3) Hence  $\mathfrak{p} = (\pi)$  since they have the same prime factorization.

□

**Exercise I.3.5.**

The quotient ring  $\mathcal{O}/\mathfrak{a}$  of a Dedekind domain by an ideal  $\mathfrak{a} \neq 0$  is a principal ideal domain. (Hint: For  $\mathfrak{a} = \mathfrak{p}^n$  the only proper ideals of  $\mathcal{O}/\mathfrak{a}$  are given by  $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$ . Choose  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  and show that  $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$ .)

*Proof.*

- (1) By the Chinese remainder theorem, it suffices to show the case  $\mathfrak{a} = \mathfrak{p}^n$  where  $\mathfrak{p}$  is prime.
- (2) There is a natural correspondence between

$$\{\text{ideals of } \mathcal{O}/\mathfrak{p}^n\} \longleftrightarrow \{\text{ideals of } \mathcal{O} \text{ containing } \mathfrak{p}^n\}.$$

Hence the proper ideals of  $\mathcal{O}/\mathfrak{p}^n$  are given by  $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$ .

- (3) Similar to Exercise I.3.4, choose  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  and thus  $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$  ( $\nu = 1, \dots, n-1$ ) since they have the same prime factorization. Hence  $\mathfrak{p}^\nu/\mathfrak{p}^n = (\pi^\nu + \mathfrak{p}^n)$  is principal.

□

**Exercise I.3.6.**

Every ideal of a Dedekind domain can be generated by two elements. (Hint: Use Exercise I.3.5.)

*Proof.*

- (1) Given an ideal  $\mathfrak{a} \neq 0$  of a Dedekind domain  $\mathcal{O}$ . (Nothing to do if  $\mathfrak{a} = 0 = (0)$ .) So  $\mathcal{O}/\mathfrak{a}$  is a principal ideal domain (Exercise I.3.5).
- (2) Take any  $\alpha \in \mathfrak{a} \setminus \{0\}$ . So  $(\alpha)/\mathfrak{a} = (\beta \pmod{\mathfrak{a}})$  is a principal ideal for some  $\beta \in \mathcal{O}$ . So  $\mathfrak{a} = (\alpha, \beta)$  is generated by two elements.

□

**I.4. Lattices****Exercise I.4.1.**

Show that a lattice  $\Gamma$  in  $\mathbb{R}^n$  is complete if and only if the quotient  $\mathbb{R}^n/\Gamma$  is compact.

*Proof.*

- (1) ( $\implies$ ) Define a natural homeomorphism  $\varphi : \mathbb{R}^n/\Gamma \rightarrow \mathbb{S}^1 \times \cdots \times \mathbb{S}^1$  by sending  $(x_1, \dots, x_n)$  to  $(x_1 \pmod{1}, \dots, x_n \pmod{1})$  (where  $\mathbb{S}^1 \subseteq \mathbb{R}^2$  is a unit circle). Note that  $\mathbb{S}^1 \times \cdots \times \mathbb{S}^1$  is compact.
- (2) ( $\impliedby$ ) Let  $V_0$  be the linear subspace of  $V$  which is spanned by the set  $\Gamma$ . Since the vector space  $V/V_0$  is contained in a compact set  $V/\Gamma$ ,

$$\dim(V/V_0) = 0$$

(otherwise  $V/V_0$  is unbounded). Hence  $V_0 = V$  or  $\Gamma$  is complete.

□

#### Exercise I.4.2.

Show that Minkowski's lattice point theorem cannot be improved, by giving an example of a centrally symmetric convex set  $X \subset V$  such that  $\text{vol}(X) = 2^n \text{vol}(\Gamma)$  which does not contain any nonzero point of the lattice  $\Gamma$ . If  $X$  is compact, however, then the statement  $\text{vol}(X) > 2^n \text{vol}(\Gamma)$  does remain true in the case of equality.

*Proof.*

- (1) Let  $V = \mathbb{R}^n$ ,  $\Gamma = \mathbb{Z}^n$  be a complete lattice in  $V$ , and  $X = (-1, 1)^n \subseteq \mathbb{R}^n$  be a centrally symmetric convex set in  $V$ . Hence  $\text{vol}(X) = 2^n \text{vol}(\Gamma)$  and  $X$  does not contain any nonzero point of  $\Gamma$ .
- (2) Suppose  $X$  is compact. Consider  $X_\nu = (1 + \frac{1}{\nu})X$  for each  $\nu \in \mathbb{Z}_{>0}$ . Thus  $X_\nu$  is again a centrally symmetric convex set in  $V$  and

$$\begin{aligned} \text{vol}(X_\nu) &= \left(1 + \frac{1}{\nu}\right) \text{vol}(X) \\ &\geq \left(1 + \frac{1}{\nu}\right) 2^n \text{vol}(\Gamma) \\ &> 2^n \text{vol}(\Gamma). \end{aligned}$$

Minkowski's lattice point theorem shows that there is one nonzero lattice point  $\gamma_\nu \in \Gamma$  for  $\nu = 1, 2, 3, \dots$

- (3) By the compactness of  $X_1$ , there is a subsequence of  $\{\gamma_\nu\}$  converging to  $\gamma \in X_1$ . Since  $\Gamma$  is discrete (Proposition I.4.2), there are infinitely many  $\nu$  such that  $\gamma = \gamma_\nu \in X_\nu$ . (In particular,  $\gamma \neq 0$ .) Hence  $\gamma \in X$  by the compactness of  $X$ .

□

## I.5. Minkowski Theory

### Exercise I.5.2.

Show that the convex, centrally symmetric set

$$X = \left\{ (z_\tau) \in K_{\mathbb{R}} : \sum_{\tau} |z_\tau| < t \right\}$$

has volume  $\text{vol}(X) = 2^r \pi^s \frac{t^n}{n!}$ .

*Proof.* It is the same as Lemma III.2.15.  $\square$

### Exercise I.5.3. (Minkowski bound)

Show that in every ideal  $\mathfrak{a} \neq 0$  of  $\mathcal{O}_K$  there exists an  $a \neq 0$  such that

$$|N_{K|\mathbb{Q}}(a)| \leq M(\mathcal{O}_K : \mathfrak{a}),$$

where  $M = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$  (the so-called **Minkowski bound**.)

*Proof.*

(1) Let

$$X_t = \left\{ (z_\tau) \in K_{\mathbb{R}} : \sum_{\tau} |z_\tau| \leq t \right\}$$

be a convex, centrally symmetric set for any  $t > 0$ . Note that  $\text{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}$  (same as Exercise I.5.2).

(2) In particular, we take  $t > 0$  so that

$$\text{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!} = 2^n \text{vol}(\Gamma).$$

Thus the hypothesis of Minkowski's lattice point theorem in Exercise I.4.2 is satisfied. So there does indeed exist a lattice point  $ja \in X_t$ ,  $a \neq 0$ ,  $a \in \mathfrak{a}$ ; in other words,  $\sum_{\tau} |\tau a| \leq t$ .

(3) Hence

$$\begin{aligned}
|N_{K|\mathbb{Q}}(a)| &= \prod_{\tau} |\tau a| \\
&\leq \left( \frac{1}{n} \sum_{\tau} |\tau a| \right)^n && \text{(AM-GM inequality)} \\
&\leq \frac{t^n}{n^n} && (ja \in X_t) \\
&= \frac{1}{n^n} \frac{n!}{2^r \pi^s} 2^n \text{vol}(\Gamma) && \text{(Definition of } t^n) \\
&= \frac{1}{n^n} \frac{n!}{2^r \pi^s} 2^n \sqrt{|d_K|} (\mathcal{O}_K : \mathfrak{a}) && \text{(Proposition I.5.2)} \\
&= \underbrace{\frac{n!}{n^n} \left( \frac{4}{\pi} \right)^s}_{:=M} \sqrt{|d_K|} (\mathcal{O}_K : \mathfrak{a}). && (n = r + 2s)
\end{aligned}$$

□

## I.6. The Class Number

### Exercise I.6.3.

Show that in every ideal class of an algebraic number field  $K$  of degree  $n$ , there exists an integral ideal  $\mathfrak{a}_1$  such that

$$\mathfrak{N}(\mathfrak{a}_1) \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^s \sqrt{|d_K|}$$

(Hint: Use Exercise I.3.5, proceed as in the proof of Theorem I.6.3.)

*Proof.*

- (1) The hint gives all.
- (2) Take an arbitrary representative  $\mathfrak{a}$  of the class in the ideal class group, and a  $\gamma \in \mathcal{O}_K$ ,  $\gamma \neq 0$ , such that  $\mathfrak{b} := \gamma \mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ . By Exercise I.3.5, there exists  $\alpha \in \mathfrak{b}$ ,  $\alpha \neq 0$ , such that

$$|N_{K|\mathbb{Q}}(\alpha)| \cdot \mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}((\alpha)\mathfrak{b}^{-1}) = \mathfrak{N}(\alpha\mathfrak{b}^{-1}) \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^s \sqrt{|d_K|}.$$

The ideal

$$\mathfrak{a}_1 := \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$$

therefore has the required property.

- (3) This exercise also shows that  $\text{Cl}_K$  is a finite group.

□

## I.7. Dirichlet's Unit Theorem

### Exercise I.7.3. (The Battle of Hastings (October 14, 1066))

*“The men of Harold stood well together, as their wont was, and formed thirteen squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter their redoubts; for a single blow of a Saxon war hatched would break his lance and cut his coat of mail... When Harold threw himself into the fray the Saxons were one mighty square of men, shouting the battle-cries ‘Ut!’, ‘Olicrosee!’, ‘Godemite!’.” [Fictitious historical text, following essentially problem no. 129 in: H.E. Dundeney, Amusements in Mathematics, 1917 (Dover reprints 1958 and 1970).] Question. How many troops does this suggest Harold II had at the battle of Hastings?*

*Proof.*

- (1) Before Harold joins his men, they are in 13 squares, each square consisting of an equal number of men. Once Harold joins them, they all together rearrange themselves to form a single square.
- (2) Hence the corresponding equation is

$$13x^2 + 1 = y^2$$

and the number of troops is  $y^2$ .

- (3) So  $(x, y) = (180, 649), (233640, 842401), \dots$  by WolframAlpha. Note that the world population in 1066 was less than it is today. The number of troops was  $13 \cdot 180^2 + 1 = 649^2 = 421201$ .

□

## I.11. Localization

### Exercise I.11.7. (Nakayama's lemma)

*Let  $A$  be a local ring with maximal ideal  $\mathfrak{m}$ , let  $M$  be an  $A$ -module and  $N \subseteq M$  a submodule such that  $M/N$  is finitely generated. Then one has the implication:*

$$M = N + \mathfrak{m}M \implies M = N.$$



*Proof.*

(1) Note that

$$M = N + \mathfrak{m}M \implies M/N = (N + \mathfrak{m}M)/N = \mathfrak{m}(M/N).$$

So it suffices to show that  $M' := M/N = 0$ .

(2) (Reductio ad absurdum) If  $M' \neq 0$ , then there exists a minimal set of generators  $\{x_1, \dots, x_n\}$  for  $M'$ . Take  $x_n \in M' = \mathfrak{m}(M')$ . We have an equation of the form

$$\begin{aligned} x_n &= m_1x_1 + \dots + m_nx_n \\ \iff (1 - m_n)x_n &= m_1x_1 + \dots + m_{n-1}x_{n-1}. \end{aligned}$$

where  $m_\nu \in \mathfrak{m}$  for all  $\nu$ . Since  $\mathfrak{m}$  is the maximal ideal of a local ring,  $1 - m_n$  is a unit. So  $x_n$  is in the submodule of  $M'$  generated by  $\{x_1, \dots, x_{n-1}\}$ , contrary to the minimality of  $n$ .

□

### I.13. One-dimensional Schemes

*No exercises.*

### I.14. Function Fields

*No exercises.*

## Chapter II: The Theory of Valuations

### II.1. The $p$ -adic Numbers

#### Exercise II.1.2.

A  $p$ -adic integer  $a = a_0 + a_1p + a_2p^2 + \cdots$  is a unit in the ring  $\mathbb{Z}_p$  if and only if  $a_0 \neq 0$ .

*Proof.*

- (1) ( $\implies$ ) If  $b = b_0 + b_1p + b_2p^2 + \cdots$  is an inverse of  $a$ , then  $ab = 1$  implies that  $a_0b_0 = 1$  so that  $a_0$  is a unit in  $\mathbb{Z}/p\mathbb{Z}$  or  $a_0 \neq 0$ .
- (2) ( $\impliedby$ ) Our goal is to find

$$b = b_0 + b_1p + b_2p^2 + \cdots \in \mathbb{Z}_p$$

such that the Cauchy product

$$ab = c_0 + c_1p + c_2p^2 + \cdots$$

is equal to  $1 \in \mathbb{Z}_p$ . Here  $c_n = \sum_{\nu=0}^n a_\nu b_{n-\nu}$ . By the assumption we have that  $c_0 = 1$  and  $c_1 = c_2 = \cdots = 0$ . Hence

$$\begin{aligned} b_0 &= a_0^{-1} \\ b_1 &= -a_0^{-1}a_1b_0 \\ &\vdots \\ b_n &= a_0^{-1} \sum_{\nu=1}^n a_\nu b_{n-\nu} \\ &\vdots \end{aligned}$$

by induction.

- (3) Also see Exercise 1.5 in the textbook: *Atiyah & Macdonald, Introduction to Commutative Algebra*. Let  $A$  be a commutative ring with 1 and  $A[[x]]$  be the ring of formal power series  $f = \sum_{n=0}^{\infty} a_n x^n$  with coefficients in  $A$ . Then  $f$  is a unit in  $A[[x]]$  if and only if  $a_0$  is a unit in  $A$ .

□

### Supplement II.1.2.1.

(Exercise 1.5 (i) in the textbook: Atiyah & Macdonald, *Introduction to Commutative Algebra*.) Let  $A$  be a ring and let  $A[[x]]$  be the ring of formal power series  $f = \sum_{n=0}^{\infty} a_n x^n$  with coefficients in  $A$ . Show that  $f$  is a unit in  $A[[x]]$  if and only if  $a_0$  is a unit in  $A$ .

*Proof.*

- (1) ( $\implies$ ) If  $g = \sum_{n=0}^{\infty} b_n x^n$  is an inverse of  $f$ , then  $fg = 1$  implies that  $a_0 b_0 = 1$  so that  $a_0$  is a unit in  $A$ .
- (2) ( $\impliedby$ ) Our goal is to find  $g = \sum_{n=0}^{\infty} b_n x^n$  such that the Cauchy product  $fg = \sum_{n=0}^{\infty} c_n x^n$  is equal to  $1 \in A[x]$ . Here  $c_n = \sum_{r=0}^n a_r b_{n-r}$ . By the assumption we have that  $c_0 = 1$  and  $c_1 = c_2 = \dots = 0$ . Hence

$$\begin{aligned} b_0 &= a_0^{-1} \\ b_1 &= -a_0^{-1} a_1 b_0 \\ &\dots \\ b_n &= a_0^{-1} \sum_{r=1}^n a_r b_{n-r} \\ &\dots \end{aligned}$$

by induction.

□

## II.2. The $p$ -adic Absolute Value

### Exercise II.2.1.

$$|x - y|_p \geq ||x|_p - |y|_p|.$$

*Proof.* Note that  $|x + y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$  and  $|\pm 1|_p = 1$ . □

## Chapter VII: Zeta Functions and $L$ -series

### VII.1. The Riemann Zeta Function

#### Exercise VII.1.4.

For the power sum

$$s_k(n) = 1^k + 2^k + 3^k + \cdots + n^k$$

one has

$$s_k(n) = \frac{1}{k+1}(B_{k+1}(n) - B_{k+1}(0)).$$

*Proof.* By Exercise VII.1.3,

$$x^k = \frac{1}{k+1}(B_{k+1}(x) - B_{k+1}(x-1)).$$

Hence the telescoping sum is

$$\begin{aligned} s_k(n) &= \sum_{x=1}^n x^k \\ &= \sum_{x=1}^n \frac{1}{k+1}(B_{k+1}(x) - B_{k+1}(x-1)) \\ &= \frac{1}{k+1}(B_{k+1}(n) - B_{k+1}(0)). \end{aligned}$$

□