Solutions to the book: *Jürgen Neukirch, Algebraic Number Theory*

Meng-Gen Tsai
plover@gmail.com

July 16, 2021

Contents

Chapter I: Algebraic Integers **2**
I.1. The Gaussian Integers 2
Exercise I.1.1. 2
Exercise I.1.4. 2
Exercise I.1.5. 2
I.2. Integrality 3
Exercise I.2.1. 3
Exercise I.2.4. 3
Exercise I.2.7. (Stickelberger's discriminant relation) 5

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) ($\Longrightarrow$) Since α 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) ($\Longleftarrow$) $N(\alpha) = \alpha\overline{\alpha}$, or $1 = \alpha\overline{\alpha}$ since $N(\alpha) = 1$. That is, $\overline{\alpha} \in \mathbb{Z}[i]$ 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 (± 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 ± 1 and $\pm i$.

$\square$

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 ± 1.

Proof.

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

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

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

(2) Similar to Exercise I.1.1,

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

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

□

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, α is an algebraic integer.

(2) Or show that α satisfies a monic equation $x^2+6x+3 = 0 \in \mathbb{Z}[x]$.

□

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

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

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 $\operatorname{Tr}_{K|\mathbb{Q}}(\alpha), N_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$ (by noting that the equation $x^2 - \operatorname{Tr}_{K|\mathbb{Q}}(\alpha)x + N_{K|\mathbb{Q}}(\alpha) = 0$ has a root $x = \alpha$). So given $\alpha = x + y\sqrt{D} \in \mathcal{O}_K$, we have

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

(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

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

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

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

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 ω_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 σ_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),

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

□