Chapter 2: Number Fields and Number Rings

Author: Meng-Gen Tsai
Email: plover@gmail.com

Exercise 2.1.

(a) *Show that every number field of degree 2 over $\mathbb{Q}$ is one of the quadratic fields $\mathbb{Q}[\sqrt{m}]$, $m \in \mathbb{Z}$.*

(b) *Show that the fields $\mathbb{Q}[\sqrt{m}]$, m squarefree, are pairwise distinct. (Hint: Consider the equation $\sqrt{m} = a + b\sqrt{n}$); use this to show that they are in fact pairwise non-isomorphic.*

Proof of (a). Let $f(x) = ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$ $(a \neq 0)$ and assume f is irreducible over $\mathbb{Q}$. Let α be a root of $f(x)$. So

$$\alpha = \frac{-b \pm \sqrt{m}}{2a}$$

where $m = b^2 - 4ac \in \mathbb{Z}$. Therefore,

$$\mathbb{Q}[\alpha] = \mathbb{Q}\left[\frac{-b \pm \sqrt{m}}{2a}\right] = \mathbb{Q}[\sqrt{m}].$$

□

Proof of (b). Show that $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are not isomorphic as fields if m and n are squarefree and $m \neq n$. Reductio ad absurdum.

(1) If $\varphi : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{n}]$ were an isomorphism as fields, then φ is an identity map on $\mathbb{Q}$, and

$$\begin{aligned} &\varphi(\sqrt{m}) = a + b\sqrt{n} \text{ for some } a, b \in \mathbb{Q} \\ \Longrightarrow &\varphi(\sqrt{m})\varphi(\sqrt{m}) = (a + b\sqrt{n})^2 \\ \Longrightarrow &\varphi(\sqrt{m}\sqrt{m}) = (a + b\sqrt{n})^2 \\ \Longrightarrow &\varphi(m) = a^2 + nb^2 + 2ab\sqrt{n} \\ \Longrightarrow &m = a^2 + nb^2 + 2ab\sqrt{n}. \end{aligned}$$

If $2ab \neq 0$, then $\sqrt{n} = \frac{m-a^2-nb^2}{2ab} \in \mathbb{Q}$, contrary to the assumption that n is squarefree. Hence $2ab = 0$.

(2) $a = 0$. Write $b = \frac{r}{s} \in \mathbb{Q}$ where $r, s \in \mathbb{Z}$ and $(r, s) = 1$. So

$$ms^2 = nr^2.$$

Hence

$$\begin{aligned}
b \neq 0 &\Longrightarrow s^2 > 0 \text{ and } r^2 > 0 \\
&\Longrightarrow m \text{ and } n \text{ have the same sign} \\
&\Longrightarrow (\exists \text{ prime } p \mid m,\ p \nmid n) \text{ or } (\exists \text{ prime } q \mid n,\ q \nmid m) \text{ since } m \neq n.
\end{aligned}$$

(a) *There is a prime $p \mid m$ but $p \nmid n$.*

$$\begin{aligned}
p \mid m &\Longrightarrow \text{Write } m = pm_1 \text{ for some } m_1 \in \mathbb{Z} \\
&\Longrightarrow (pm_1)s^2 = nr^2 && (ms^2 = nr^2) \\
&\Longrightarrow p \mid nr^2 \\
&\Longrightarrow p \mid r^2 && (p \nmid n \text{ by assumption}) \\
&\Longrightarrow p \mid r && (p \text{ is a prime}) \\
&\Longrightarrow \text{Write } r = pr_1 \text{ for some } r_1 \in \mathbb{Z} \\
&\Longrightarrow (pm_1)s^2 = n(pr_1)^2 && (ms^2 = nr^2) \\
&\Longrightarrow m_1 s^2 = npr_1^2 \\
&\Longrightarrow p \mid m_1 s^2 \\
&\Longrightarrow p \mid m_1 && ((r,s) = 1 \text{ and } p \mid r) \\
&\Longrightarrow \text{Write } m_1 = pm_2 \text{ for some } r_2 \in \mathbb{Z} \\
&\Longrightarrow m = p^2 m_2,
\end{aligned}$$

contrary to the assumption that m is squarefree.

(b) *There is a prime $q \mid n$ but $q \nmid m$.* Similar to (a).

(3) $b = 0$. $m = a^2$. Write $a = \frac{r}{s} \in \mathbb{Q}$ where $r, s \in \mathbb{Z}$ and $(r, s) = 1$. Hence $ms^2 = r^2$. Similar to the argument in (2).

(4) By (2)(3), no such isomorphism φ, that is, $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are not isomorphic as fields.

$\square$

Supplement (Isomorphic as vector spaces). *Show that $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are isomorphic as $\mathbb{Q}$-vector spaces.*

Proof. $[\mathbb{Q}[\sqrt{m}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{n}] : \mathbb{Q}] = 2$. There is a natural map $\varphi : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{n}]$ defined by $\varphi(a + b\sqrt{m}) = a + b\sqrt{n}$. Clearly φ is well-defined, linear, injective and surjective. $\square$

Exercise 2.2. *Let I be the ideal generated by 2 and $1 + \sqrt{-3}$ in the ring $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Show that $I \neq (2)$ but $I^2 = 2I$. Conclude that ideals in $\mathbb{Z}[\sqrt{-3}]$ do not factor uniquely into prime ideals. Show moreover that*

I is the unique prime ideal containing (2) and conclude that (2) is not a product of prime ideals.

Proof.

(1) *Show that $I \neq (2)$.*

  (a) *Show that $I \supseteq (2)$.* $2 \in (2, 1+\sqrt{-3}) = I$.

  (b) *Show that $I \not\subseteq (2)$.* Consider $1+\sqrt{-3} \in I$. (Reductio ad absurdum) If $1+\sqrt{-3}$ were in (2), then there exists $a+b\sqrt{-3}$ such that

$$1+\sqrt{-3} = 2(a+b\sqrt{-3}) = 2a+2b\sqrt{-3}.$$

  Thus, $a = \frac{1}{2}$ and $b = \frac{1}{2}$, which is absurd.

(2) *Show that $I^2 = 2I$.*

  (a) *Show that $I^2 \supseteq 2I$.* Since $2 \in (2, 1+\sqrt{-3}) = I$, $2I \subseteq I^2$.

  (b) *Show that $I^2 \subseteq 2I$.* All elements of I^2 are generated by

$$2 \cdot 2, 2(1+\sqrt{-3}) \text{ and } (1+\sqrt{-3})^2.$$

  Clearly, $2 \cdot 2, 2(1+\sqrt{-3}) \in 2I$. Besides,

$$(1+\sqrt{-3})^2 = -2+2\sqrt{-3} = 2(-(2)+(1+\sqrt{-3})) \in 2I.$$

  Hence $I^2 \subseteq 2I$.

(3) *Show that ideals in $\mathbb{Z}[\sqrt{-3}]$ do not factor uniquely into prime ideals.* TODO.

(4) *Show that I is the unique prime ideal containing (2).* TODO.

(5) *Show that (2) is not a product of prime ideals.* TODO.

□

Exercise 2.4. *Suppose $a_0, \ldots, a_{n-1}$ are algebraic integers and α is a complex number satisfying*

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Show that the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ has a finitely generated additive group. (Hint: Consider the products $a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m$ and show that only finitely many values of the exponents are needed.) Conclude that α is an algebraic integer.

Proof. Let $V = \mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$. Let n_k be the degree of the algebraic integer a_k where $0 \leq k \leq n-1$.

(1) *Show that V is finitely generated as an additive subgroup of $\mathbb{C}$. It suffices to show that V is generated by*

$$a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m$$

where $0 \leq m_k < n_k$ and $0 \leq m < n$. Given any $x \in V$, x is a finite sum of the product $a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m$ with $m_k \geq 0$ and $m \geq 0$.

If $m \geq n$, replace α^m by

$$\begin{aligned}
\alpha^m =& \alpha^{m-n}\alpha^n \\
=& \alpha^{m-n}(-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0) \\
=& -a_{n-1}\alpha^{m-1} - \cdots - a_1\alpha^{m-n+1} - a_0\alpha^{m-n}.
\end{aligned}$$

Repeat this process to reduce the degree of α^m less than n. Therefore, we can write x as a finite sum of the product $a_0^{m'_0} a_1^{m'_1} \cdots a_{n-1}^{m'_{n-1}} \alpha^{m'}$ with $m'_k \geq 0$ and $0 \leq m' < n$.

Once the degree of α^m is reduced, continue to reduce the degree of each $a_k^{m'_k}$ without affecting other a_h ($h \neq k$) and α. Now replace $a_k^{m'_k}$ by

$$a_k^{m'_k} = \sum_{i=0}^{n_k - 1} b_{k,i} a_k^i$$

where $b_{k,i} \in \mathbb{Z}$. Therefore, we can write x as a finite sum of the product $a_0^{m''_0} a_1^{m''_1} \cdots a_{n-1}^{m''_{n-1}} \alpha^{m'}$ with $0 \leq m''_k < n_k$ and $0 \leq m' < n$.

(4) *Show that α is an algebraic integer.* Since $\alpha \in V$, $\alpha V \subseteq V$. Thus α is an algebraic integer (Theorem 2.2).

□

Exercise 2.5. *Show that if f is any polynomials over $\mathbb{Z}/p\mathbb{Z}$ (p a prime) then $f(x^p) = (f(x))^p$. (Suggestion: Use induction on the number of terms.)*

Proof.

(1) *Let*

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

be a binomial coefficient. If $1 \leq k \leq p-1$, show that p divides $\binom{p}{k}$.

(a) If $1 \leq k \leq p-1$, then $p \nmid k!$ and $p \nmid (p-k)!$ since p is a prime.

(b) Write $a = \frac{p!}{k!(p-k)!} \in \mathbb{Z}$. Hence,

$$\begin{aligned} a = \frac{p!}{k!(p-k)!} &\Longleftrightarrow p! = ak!(p-k)! \\ &\Longrightarrow p \mid p! \text{ or } p \mid ak!(p-k)! \\ &\Longrightarrow p \mid a \quad \text{by (a)}. \end{aligned}$$

Hence p divides $\binom{p}{k}$ if $1 \leq k \leq p-1$.

(2) Note that $a^p = a \in \mathbb{Z}/p\mathbb{Z}$ for all $a \in \mathbb{Z}/p\mathbb{Z}$.

(3) Write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}/p\mathbb{Z}[x].$$

Induction on n.

(a) $n = 0$. So $f(x) = a_0$, and thus $f(x)^p = a_0^p = a_0$ by (2).

(b) $n = 1$. By $f(x) = a_1 x + a_0$,

$$\begin{aligned} f(x)^p &= (a_1 x + a_0)^p \\ &= a_1^p x^p + \sum_{k=1}^{p-1} \binom{p}{k} (a_1 x)^k a_0^{p-k} + a_0^p && \text{(Binomial theorem)} \\ &= a_1^p x^p + a_0^p && \text{((1))} \\ &= a_1 x^p + a_0 && \text{((2))} \\ &= f(x^p). \end{aligned}$$

(c) If the statement holds for $n-1$, then

$$\begin{aligned} f(x)^p &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p \\ &= [a_n x^n + (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)]^p \\ &= (a_n x^n)^p + (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p && \text{(Same as (b))} \\ &= a_n (x^p)^n + (a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p && \text{((2))} \\ &= a_n (x^p)^n + a_{n-1}(x^p)^{n-1} + \cdots + a_1 x^p + a_0 && \text{(Induction hypothesis)} \\ &= f(x^p). \end{aligned}$$

The inductive step is established.

By induction, $f(x)^p = f(x^p)$ holds for any $n \geq 0$.

□

Exercise 2.6. *Show that if f and g are polynomials over a field K and $f^2 \mid g$ in $K[x]$, then $f \mid g'$. (Hint: Write $g = f^2 h$ and differentiate.)*

Proof (Hint). Since $f^2 \mid g$ in $K[x]$, there exists $h \in K[x]$ such $g = f^2h$. Differentiate to get $g' = 2ff'h + f^2h' = f(2f'h + fh')$, or $f \mid g'$ in $K[x]$. $\square$

Exercise 2.10. *Complete the proof of Corollary 3 to Theorem 2.3, by showing if m is even, $m \mid r$, and $\varphi(r) \leq \varphi(m)$, then $r = m$.*

Proof.

(1) Since m is even, write the unique factorization of m as

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1 = 2$, all $\alpha_i \geq 1$ $(1 \leq i \leq k)$, and all p_i $(1 \leq i \leq k)$ are distinct prime numbers.

(2) Since $m \mid r$, write $r = mm_1$ for some $m_1 \in \mathbb{Z}$. Thus we can write the unique factorization of r as

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_h^{\gamma_h}$$

where all $\beta_i \geq \alpha_i \geq 1$ $(1 \leq i \leq k)$ and all p_i $(1 \leq i \leq k)$ and q_j $(1 \leq j \leq h)$ are distinct prime numbers. Here h might be zero if $m_1 = 1$, and all $q_j \mid m_1$ but $q_j \nmid m$.

(3) Thus,

$$\begin{aligned}
\varphi(m) &= m\left(1 - \frac{1}{2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
\varphi(r) &= mm_1\left(1 - \frac{1}{2}\right) \cdots \left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_h}\right) \\
&= \varphi(m)m_1\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_h}\right) \\
&\geq \varphi(m)(q_1 \cdots q_h)\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_h}\right) \\
&\geq \varphi(m)(q_1 - 1) \cdots (q_h - 1).
\end{aligned}$$

(4) Since all $q_j \neq 2$ $(1 \leq j \leq h)$, $q_j - 1 > 1$. Hence by (3) and assumption that $\varphi(r) \leq \varphi(m)$, $h = 0$ or $m_1 = 1$ or $r = m$.

$\square$

Exercise 2.11.

(a) *Suppose all roots of a monic polynomial $f \in \mathbb{Q}[x]$ has absolute value 1. Show that the coefficient of x^r has absolute value $\leq \binom{n}{r}$, where n is the degree of f and $\binom{n}{r}$ is the binomial coefficient.*

(b) *Show that there are only finitely many algebraic integers α of fixed degree n, all of whose conjugates (including α) have absolute value 1. (Note: If you don't use Theorem 2.1, your proof is probably wrong.)*

(c) *Show that α must be a root of 1. (Show that its powers are restricted to a finite set.)*

Proof of (a).

(1) Write $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ where $\alpha_i \in \mathbb{C}$, $|\alpha_i| = 1$ for $i = 1, 2, \ldots, n$.

(2) So

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)s_n$$

where

$$s_r = \sum_{1 \leq j_1 < \cdots < j_r \leq n} \alpha_{j_1} \cdots \alpha_{j_r} \in \mathbb{C}.$$

Let $c_r = (-1)^r s_{n-r}$ be the coefficient of x^r.

(3)

$$\begin{aligned}
|c_r| &= |(-1)^r s_{n-r}| \\
&= \left| \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} \alpha_{j_1} \cdots \alpha_{j_{n-r}} \right| \\
&\leq \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} |\alpha_{j_1} \cdots \alpha_{j_{n-r}}| \\
&= \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} |\alpha_{j_1}| \cdots |\alpha_{j_{n-r}}| \\
&= \sum_{1 \leq j_1 < \cdots < j_{n-r} \leq n} 1 \\
&= \binom{n}{n-r} \\
&= \binom{n}{r}.
\end{aligned}$$

$\square$

Proof of (b).

(1) Let f be an irreducible monic polynomial over $\mathbb{Z}$ of degree n such that $f(\alpha) = 0$. So f is irreducible over $\mathbb{Q}$ (Theorem 2.1), and thus all the conjugates of α (including α) are roots of f.

(2) By (a), all the coefficient of x^r has absolute value $\leq \binom{n}{r}$. Since all the coefficient of x^r are integers, there are finitely many irreducible monic polynomials $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$ with $|\alpha| = 1$.

(3) For each such f, there are only finitely many roots. Therefore, there are only finitely many such algebraic integers α.

$\square$

Proof of (c).

(1) If $\alpha_1, \ldots, \alpha_n$ are the roots of f of degree n over $\mathbb{Q}$, then for every $r \in \mathbb{Z}^+$, $\alpha_1^r, \ldots, \alpha_n^r$ are all the roots of some monic polynomial f_r of degree n over $\mathbb{Q}$ (Fundamental theorem of symmetric polynomials).

(2) Now we consider the powers of α. All the powers of α (α^r) are algebraic integers (Theorem 2.2), and of degree at most n. (Let $g \in \mathbb{Z}[x]$ be the minimal polynomial of α^r over $\mathbb{Q}$. By (1), $f_r(\alpha^r) = 0$, and thus $g \mid f_r$. Hence $\deg(g) \leq \deg(f_r) = n$.)

(3) By (b), the powers of α are restricted to a finite set, say $\alpha^r = \alpha^s$ for some $s > r \geq 1$. So $\alpha^{s-r} = 1$ with $s - r \geq 1$. That is, α is a root of unity.

$\square$

Exercise 2.12 (Kummer's Lemma). *Now we can prove Kummer's lemma on units in the p-th cyclotomic field, as stated before Exercise 1.26: Let $\omega = e^{\frac{2\pi i}{p}}$, p an odd prime, and suppose u is a unit in $\mathbb{Z}[\omega]$.*

(a) *Show that $u/\overline{u}$ is a root of 1. (Use Exercise 2.11(c) above and observe that complex conjugation is a member of the Galois group of $\mathbb{Z}[\omega]$ over $\mathbb{Q}$.) Conclude that $u/\overline{u} = \pm\omega^k$ for some k.*

(b) *Show that the + sign holds: Assuming $u/\overline{u} = -\omega^k$, we have $u^p = -\overline{u^p}$; show that this implies that u^p is divisible by p in $\mathbb{Z}[\omega]$. (Use Exercise 1.23 and 1.25) But this is impossible since u^p is a unit.*

Proof of (a). Write $\alpha = u/\overline{u}$. Then

$$\begin{aligned} |\alpha| = 1 &\Longrightarrow \alpha \text{ is a root of unity} && \text{(Exercise 2.11)} \\ &\Longrightarrow \alpha \text{ is a } 2p\text{-th root of unity} && \text{(Corollary 3 to Theorem 2.3)} \\ &\Longrightarrow \alpha = \pm\omega^k \text{ for some } k \in \mathbb{Z} \end{aligned}$$

$\square$

Proof of (b). (Reductio ad absurdum) Assume that $u/\overline{u} = -\omega^k$, then

$$\begin{aligned} u/\overline{u} = -\omega^k &\Longrightarrow (u/\overline{u})^p = (-\omega^k)^p \\ &\Longrightarrow u^p/\overline{u}^p = (-1)^p \omega^{pk} = -1 && (p \text{ is odd}) \\ &\Longrightarrow u^p = -\overline{u}^p = -\overline{u^p} \end{aligned}$$

By Exercise 1.25, $u^p \equiv a \pmod p$ for some $a \in \mathbb{Z}$. By Exercise 1.23, $\overline{u^p} \equiv \overline{a} \equiv a \pmod p$. Thus

$$\begin{aligned} u^p = -\overline{u^p} &\Longrightarrow a \equiv -a \pmod p \\ &\Longrightarrow 2a \equiv 0 \pmod p \\ &\Longrightarrow a \equiv 0 \pmod p && (p \text{ is odd}) \end{aligned}$$

or $u^p \equiv 0 \pmod p$, contradicts the assumption that u is a unit. Hence $u/\overline{u} = \omega^k$ for some k. $\square$

Exercise 2.13. *Show that* 1 *and* -1 *are the only units in the ring* $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$, *$m$ squarefree,* $m < 0$, $m \neq -1, -3$. *What if* $m = -1$ *or* -3*?*

Proof.

(1) Let $K = \mathbb{Q}[\sqrt{m}]$ and $\mathcal{O}_K = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$. Define a norm N on K by

$$N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 + |m|b^2.$$

(2) Corollary 2 to Theorem 1:

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} & (m \equiv 2, 3 \pmod 4), \\ \left\{ \frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\} & (m \equiv 1 \pmod 4). \end{cases}$$

Clearly, N maps $\mathcal{O}_K$ to nonnegative integers. That is, u is a unit in $\mathcal{O}_K$ if and only if $N(u) = 1$ (by the fact that $N(u) = u\overline{u}$).

(3) If $m \equiv 2, 3 \pmod 4$ and $u = a + b\sqrt{m} \in \mathcal{O}_K$ is a unit ($a, b \in \mathbb{Z}$), then

$$N(u) = 1 = a^2 + |m|b^2.$$

(a) *$m = -1$ or $|m| = 1$.* $1 = a^2 + b^2$ or $(a, b) = (\pm 1, 0), (0, \pm 1)$. Hence all units in $\mathcal{O}_K$ are

$$\pm 1, \pm\sqrt{-1}.$$

(b) *$m < -1$ or $|m| > 1$.* $1 = a^2 + |m|b^2$ implies that $b^2 = 0$. Hence all units in $\mathcal{O}_K$ are ± 1.

(4) If $m \equiv 1 \pmod 4$ and $u = \frac{a+b\sqrt{m}}{2} \in \mathcal{O}_K$ is a unit ($a, b \in \mathbb{Z}, a \equiv b \pmod 2$), then $N(u) = 1 = (\frac{a}{2})^2 + |m|(\frac{b}{2})^2$ or

$$4 = a^2 + |m|b^2.$$

(a) $m = -3$ *or* $|m| = 3$. $4 = a^2 + 3b^2$ or $(a, b) = (\pm 2, 0), (\pm 1, \pm 1)$. Hence all units in $\mathcal{O}_K$ are

$$\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}.$$

(b) $m < -3$ *or* $|m| > 3$. $4 = a^2 + |m|b^2$ implies that $b^2 = 0$. Hence all units in $\mathcal{O}_K$ are ± 1.

(5) By (3)(4), all units in $\mathcal{O}_K$ are

$$\begin{cases} \pm 1 & (m \neq -1, -3), \\ \pm 1, \pm\sqrt{-1} & (m = -1), \\ \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2} & (m = -3). \end{cases}$$

□

Exercise 2.14. *Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. Use the powers of $1 + \sqrt{2}$ to generate infinitely many solutions to the diophantine equation $a^2 - 2b^2 = \pm 1$. (It will be shown in Chapter 5 that all units in $\mathbb{Z}[\sqrt{2}]$ are of the form $\pm(1+\sqrt{2})^k$, $k \in \mathbb{Z}$.)*

Might assume to find nonnegative solutions to the Pell's equation $a^2 - 2b^2 = \pm 1$.

Proof.

(1) *Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$.* There is $-1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1 \in \mathbb{Z}[\sqrt{2}].$$

Hence $1 + \sqrt{2}$ is a unit.

(2) *$N(a + b\sqrt{2}) = |a^2 - 2b^2|$ is a norm on $\mathbb{Z}[\sqrt{2}]$.* To prove this, use the same argument as Exercise 1.1 and note that

$$N(a + b\sqrt{2}) = |(a + b\sqrt{2})(a - b\sqrt{2})|.$$

(3) By (1)(2), all $(1+\sqrt{2})^k$ with $k \geq 0$ are distinct solutions to the diophantine equation $a^2 - 2b^2 = \pm 1$. Explicitly, let

$$\begin{aligned}
(a_0, b_0) &= (1, 0), \\
(a_1, b_1) &= (1, 1), \\
(a_2, b_2) &= (3, 2), \\
(a_3, b_3) &= (7, 5), \\
&\cdots \\
(a_k, b_k) &= (a_{k-1} + 2b_{k-1}, a_{k-1} + b_{k-1}), \\
&\cdots
\end{aligned}$$

Note that all (a_k, b_k) are distinct and satisfying $a_k^2 - 2b_k^2 = \pm 1$. Hence we get infinitely many solutions to the Pell's equation $a^2 - 2b^2 = \pm 1$.

Note. Suppose that all units in $\mathbb{Z}[\sqrt{2}]$ are of the form $\pm(1+\sqrt{2})^k$, $k \in \mathbb{Z}$. Note that $(1+\sqrt{2})^k = (-1+\sqrt{2})^{-k}$. Thus we can find all nonnegative solutions to the Pell's equation $a^2 - 2b^2 = \pm 1$ are exactly the same as (3). $\square$

Exercise 2.15.

(a) *Show that* $\mathbb{Z}[\sqrt{-5}]$ *contains no element whose norm is* 2 *or* 3.

(b) *Verify that* $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ *is an example of non-unique factorization in the number ring* $\mathbb{Z}[\sqrt{-5}]$.

Proof of (a). Since $N(a + b\sqrt{-5}) = a^2 + 5b^2 \equiv a^2 \equiv 0, 1, 4 \pmod 5$, there is no element whose norm is 2 or 3. $\square$

Proof of (b).

(1) *Show that* $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

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

(2) *Show that* 2 *is irreducible.* Suppose $2 = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Take norm to get

$$\begin{aligned} N(2) = N(\alpha)N(\beta) &\Longrightarrow 4 = N(\alpha)N(\beta) \\ &\Longrightarrow N(\alpha) = 1 \text{ or } N(\beta) = 1 \qquad ((1)) \\ &\Longrightarrow \alpha \text{ is unit or } \beta \text{ is unit.} \end{aligned}$$

(3) *Show that* 3 *is irreducible.* Similar to (2).

(4) *Show that* $1 \pm \sqrt{-5}$ *is irreducible.* Since $N(1 \pm \sqrt{-5}) = 2$ is prime, $1 + \sqrt{-5}$ is irreducible.

Hence 6 has a non-unique factorization in the number ring $\mathbb{Z}[\sqrt{-5}]$. $\square$

Exercise 2.28. *Let* $f(x) = x^3 + ax + b$, a *and* $b \in \mathbb{Z}$, *and assume* f *is irreducible over* $\mathbb{Q}$. *Let* α *be a root of* f.

(a) *Show that* $f'(\alpha) = -\frac{2a\alpha + 3b}{\alpha}$.

(b) *Show that* $2a\alpha + 3b$ *is a root of*

$$\left(\frac{x - 3b}{2a}\right)^3 + a\left(\frac{x - 3b}{2a}\right) + b.$$

Use this to find $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b)$.

(c) *Show that disc*$(\alpha) = -(4a^3 + 27b^2)$.

(d) *Suppose* $\alpha^3 = \alpha + 1$. *Prove that* $\{1, \alpha, \alpha^2\}$ *is an integral basis for* $\mathbb{A} \cap \mathbb{Q}[\alpha]$. *(See Exercise 2.27(e).) Do the same if* $\alpha^3 + \alpha = 1$.

Proof of (a).

(1) *Show that* $\alpha \neq 0$. If α were 0, then $f(\alpha) = f(0) = b$. So $f(x) = x^3 + ax = x(x^2 + a)$ is reducible, contrary to the irreducibility of f.

(2) Since α be a root of f, $f(\alpha) = 0$, or $\alpha^3 + a\alpha + b = 0$, or $\alpha^3 = -a\alpha - b$.

(3)

$$\begin{aligned} f'(x) = 3x^2 + a \Longrightarrow f'(\alpha) &= 3\alpha^2 + a \\ \Longleftrightarrow \alpha f'(\alpha) &= 3\alpha^3 + a\alpha && (\alpha \neq 0) \\ \Longleftrightarrow \alpha f'(\alpha) &= 3(-a\alpha - b) + a\alpha && (\alpha^3 = -a\alpha - b) \\ \Longleftrightarrow \alpha f'(\alpha) &= -2a\alpha - 3b. \end{aligned}$$

So $f'(\alpha) = -\frac{2a\alpha + 3b}{\alpha}$.

$\square$

Proof of (b).

(1) Since $\alpha^3 + a\alpha + b = 0$,

$$\left(\frac{(2a\alpha + 3b) - 3b}{2a} \right)^3 + a \left(\frac{(2a\alpha + 3b) - 3b}{2a} \right) + b = 0.$$

That is, $2a\alpha + 3b$ is a root of $\left(\frac{x - 3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$.

(2) $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b)$ is the product of three roots of $\left(\frac{x - 3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$. Hence,

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha + 3b) &= (2a)^3 \left[\left(\frac{-3b}{2a} \right)^3 + a \cdot \frac{-3b}{2a} + b \right] \\ &= 8a^3 \left[\frac{-27b^3}{8a^3} - \frac{b}{2} \right] \\ &= -27b^3 - 4a^3 b. \end{aligned}$$

$\square$

Proof of (c).

$$\begin{aligned}
\operatorname{disc}(\alpha) &= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(f'(\alpha)) && \text{(Theorem 2.8)} \\
&= -N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(-\frac{2a\alpha+3b}{\alpha}\right) && (n=3 \text{ and (a)}) \\
&= \frac{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(2a\alpha+3b)}{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)} \\
&= \frac{-27b^3-4a^3b}{b} && \text{((b))} \\
&= -27b^2-4a^3.
\end{aligned}$$

□

Proof of (d).

(1) (a) $\alpha^3 = \alpha + 1$, or $\alpha^3 - \alpha - 1 = 0$.
 (b) $f(x) = x^3 - x - 1$ is irreducible over $\mathbb{Q}$ since $f(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$.
 (c) $\operatorname{disc}(\alpha) = -23$ (by (c)).
 (d) Since $\operatorname{disc}(\alpha)$ is squarefree, the result is established (Exercise 2.27(e)).

(2) (a) $\alpha^3 + \alpha = 1$, or $\alpha^3 + \alpha - 1 = 0$.
 (b) $f(x) = x^3 + x - 1$ is irreducible over $\mathbb{Q}$ since $f(x)$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$.
 (c) $\operatorname{disc}(\alpha) = -31$ (by (c)).
 (d) Since $\operatorname{disc}(\alpha)$ is squarefree, the result is established (Exercise 2.27(e)).

□

Exercise 2.43. *Let $f(x) = x^5 + ax + b$, a and $b \in \mathbb{Z}$, and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f.*

(a) *Show that $\operatorname{disc}(\alpha) = 4^4a^5 + 5^4b^4$. (Suggestion: See Exercise 2.28.)*

(b) *Suppose $\alpha^5 = \alpha + 1$. Prove that $\mathbb{A} \cap \mathbb{Q}[\alpha] = \mathbb{Z}[\alpha]$. ($x^5 - x - 1$ is irreducible over $\mathbb{Q}$; this can be shown by reducing $\pmod 3$.)*

(c) ...

(d) ...

Proof of (a)(Exercise 2.28).

(1) *Show that $f'(\alpha) = -\frac{4a\alpha+5b}{\alpha}$.*

(a) *Show that* $\alpha \neq 0$. If α were 0, then $f(\alpha) = f(0) = b$. So $f(x) = x^5 + ax = x(x^4 + a)$ is reducible, contrary to the irreducibility of f.

(b) Since α be a root of f, $f(\alpha) = 0$, or $\alpha^5 + a\alpha + b = 0$, or $\alpha^5 = -a\alpha - b$.

(c)

$$\begin{aligned} f'(x) = 5x^4 + a \Longrightarrow f'(\alpha) &= 5\alpha^4 + a \\ &\Longleftrightarrow \alpha f'(\alpha) = 5\alpha^5 + a\alpha && (\alpha \neq 0) \\ &\Longleftrightarrow \alpha f'(\alpha) = 5(-a\alpha - b) + a\alpha && (\alpha^5 = -a\alpha - b) \\ &\Longleftrightarrow \alpha f'(\alpha) = -4a\alpha - 5b. \end{aligned}$$

So $f'(\alpha) = -\frac{4a\alpha + 5b}{\alpha}$.

(2) *Show that* $4a\alpha + 5b$ *is a root of*

$$\left(\frac{x - 5b}{4a}\right)^5 + a\left(\frac{x - 5b}{4a}\right) + b.$$

Use this to show that $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b) = -4^4a^5b - 5^5b^5$.

(a) Since $\alpha^5 + a\alpha + b = 0$,

$$\left(\frac{(4a\alpha + 5b) - 5b}{4a}\right)^5 + a\left(\frac{(4a\alpha + 5b) - 5b}{4a}\right) + b = 0.$$

That is, $4a\alpha + 5b$ is a root of $\left(\frac{x-5b}{4a}\right)^5 + a\left(\frac{x-5b}{4a}\right) + b$.

(b) $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b)$ is the product of 5 roots of $\left(\frac{x-5b}{4a}\right)^5 + a\left(\frac{x-5b}{4a}\right) + b$. Hence,

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b) &= (4a)^5 \left[\left(\frac{-5b}{4a}\right)^5 + a \cdot \frac{-5b}{4a} + b\right] \\ &= 4^5a^5\left[\frac{-5^5b^5}{4^5a^5} - \frac{b}{4}\right] \\ &= -5^5b^5 - 4^4a^5b. \end{aligned}$$

(3) *Show that disc*$(\alpha) = 4^4a^5 + 5^4b^4$.

$$\begin{aligned} \operatorname{disc}(\alpha) &= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(f'(\alpha)) && \text{(Theorem 2.8)} \\ &= N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(-\frac{4a\alpha + 5b}{\alpha}\right) && (n = 5 \text{ and } (1)) \\ &= -\frac{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(4a\alpha + 5b)}{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)} \\ &= -\frac{-4^4a^5b - 5^5b^5}{b} && ((2)) \\ &= 4^4a^5 + 5^4b^4. \end{aligned}$$

□

Proof of (b)(Exercise 2.28).

(1) $\alpha^5 = \alpha + 1$, or $\alpha^5 - \alpha - 1 = 0$.

(2) $f(x) = x^5 - x - 1$ is irreducible over $\mathbb{Q}$ since $f(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$.

(3) $\mathrm{disc}(\alpha) = 881$ (by (a)).

(4) Since $\mathrm{disc}(\alpha)$ is squarefree (a prime number), the result is established (Exercise 2.27(e)).

□

Exercise 2.44. *Let $f(x) = x^5 + ax^4 + b$, a and $b \in \mathbb{Z}$, and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f and let d_1, d_2, d_3 and d_4 be as in Theorem 2.13.*

(a) *Show that $disc(\alpha) = b^3(4^4a^5 + 5^5b)$.*

(b) ...

(c) ...

(d) ...

Proof of (a). TODO. □

Exercise 2.45. *Obtain a formula for $disc(\alpha)$ if α is a root of an irreducible polynomial $x^n + ax + b$ over $\mathbb{Q}$. Do the same for $x^n + ax^{n-1} + b$.*

Assume that $n \geq 2$.

Proof of $x^n + ax + b$ (Exercise 2.28).

(1) *Show that $f'(\alpha) = -\frac{(n-1)a\alpha + nb}{\alpha}$.*

  (a) *Show that $\alpha \neq 0$.* If α were 0, then $f(\alpha) = f(0) = b$. So $f(x) = x^n + ax = x(x^{n-1} + a)$ is reducible, contrary to the irreducibility of f.

  (b) Since α be a root of f, $f(\alpha) = 0$, or $\alpha^n + a\alpha + b = 0$, or $\alpha^n = -a\alpha - b$.

  (c)

$$\begin{aligned}
f'(x) = nx^{n-1} + a \Longrightarrow f'(\alpha) &= n\alpha^{n-1} + a \\
\Longleftrightarrow \alpha f'(\alpha) &= n\alpha^n + a\alpha && (\alpha \neq 0) \\
\Longleftrightarrow \alpha f'(\alpha) &= n(-a\alpha - b) + a\alpha && (\alpha^n = -a\alpha - b) \\
\Longleftrightarrow \alpha f'(\alpha) &= -(n-1)a\alpha - nb.
\end{aligned}$$

So $f'(\alpha) = -\frac{(n-1)a\alpha+nb}{\alpha}$.

(2) *Let $\beta = (n-1)a\alpha + nb$. Show that β is a root of*

$$\left(\frac{x-nb}{(n-1)a}\right)^n + a\left(\frac{x-nb}{(n-1)a}\right) + b.$$

Use this to show that

$$N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta) = -(n-1)^{n-1}a^n b + (-1)^n n^n b^n.$$

(a) Since $\alpha^n + a\alpha + b = 0$,

$$\left(\frac{\beta-nb}{(n-1)a}\right)^n + a\left(\frac{\beta-nb}{(n-1)a}\right) + b = 0.$$

That is, β is a root of $\left(\frac{x-nb}{(n-1)a}\right)^n + a\left(\frac{x-nb}{(n-1)a}\right) + b$.

(b) $N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta)$ is the product of n roots of $\left(\frac{x-nb}{(n-1)a}\right)^n + a\left(\frac{x-nb}{(n-1)a}\right) + b$. Hence,

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\beta) &= ((n-1)a)^n\left[\left(\frac{-nb}{(n-1)a}\right)^n + a\cdot\frac{-nb}{(n-1)a} + b\right] \\ &= (n-1)^n a^n\left[\frac{(-1)^n n^n b^n}{(n-1)^n a^n} - \frac{b}{n-1}\right] \\ &= (-1)^n n^n b^n - (n-1)^{n-1}a^n b. \end{aligned}$$

(3) *Show that disc*$(\alpha) = (-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}a^n + (-1)^{\frac{n(n-1)}{2}}n^n b^{n-1}$.

$$\begin{aligned} \operatorname{disc}(\alpha) &= (-1)^{\frac{n(n-1)}{2}}N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(f'(\alpha)) && \text{(Theorem 2.8)} \\ &= (-1)^{\frac{n(n-1)}{2}}N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}\left(-\frac{(n-1)a\alpha+nb}{\alpha}\right) && ((1)) \\ &= (-1)^{\frac{n(n-1)}{2}}(-1)^n\frac{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}((n-1)a\alpha+nb)}{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)} \\ &= (-1)^{\frac{n(n-1)}{2}}(-1)^n\frac{-(n-1)^{n-1}a^n b + (-1)^n n^n b^n}{b} && ((2)) \\ &= (-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}a^n + (-1)^{\frac{n(n-1)}{2}}n^n b^{n-1}. \end{aligned}$$

□

Proof of $x^n + ax^{n-1} + b$. TODO. □