

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

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

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

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

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

$$\begin{aligned}
p \mid m &\implies \text{Write } m = pm_1 \text{ for some } m_1 \in \mathbb{Z} \\
&\implies (pm_1)s^2 = nr^2 && (ms^2 = nr^2) \\
&\implies p \mid nr^2 \\
&\implies p \mid r^2 && (p \nmid n \text{ by assumption}) \\
&\implies p \mid r && (p \text{ is a prime}) \\
&\implies \text{Write } r = pr_1 \text{ for some } r_1 \in \mathbb{Z} \\
&\implies (pm_1)s^2 = n(pr_1)^2 && (ms^2 = nr^2) \\
&\implies m_1s^2 = npr_1^2 \\
&\implies p \mid m_1s^2 \\
&\implies p \mid m_1 && ((r, s) = 1 \text{ and } p \mid r) \\
&\implies \text{Write } m_1 = pm_2 \text{ for some } m_2 \in \mathbb{Z} \\
&\implies m = p^2m_2,
\end{aligned}$$

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.

□

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 $\varphi : \mathbb{Q}[\sqrt{m}] \rightarrow \mathbb{Q}[\sqrt{n}]$ defined by $\varphi(a + b\sqrt{m}) = a + b\sqrt{n}$. Clearly φ is well-defined, linear, injective and surjective. □

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,

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

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) $n = 0$. Nothing to do.

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

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

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

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

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 $g = f^2h$ 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 $K[x]$. □

Exercise 2.15.

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

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. □

Proof of (b). TODO. □

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 $\text{disc}(\alpha) = -(4a^3 + 27b^2)$.
- (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)

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

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

□

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,

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

□

Proof of (c).

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

□

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) $\text{disc}(\alpha) = -23$ (by (c)).
 (d) Since $\text{disc}(\alpha)$ 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) $\text{disc}(\alpha) = -31$ (by (c)).
 (d) Since $\text{disc}(\alpha)$ 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 $\text{disc}(\alpha) = 4^4 a^5 + 5^4 b^4$. (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 (mod 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)

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

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

(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 $\text{disc}(\alpha) = 4^4a^5 + 5^4b^4$.

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

□

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) $\text{disc}(\alpha) = 881$ (by (a)).
- (4) Since $\text{disc}(\alpha)$ 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 $\text{disc}(\alpha) = b^3(4^4a^5 + 5^5b)$.
- (b) ...
- (c) ...
- (d) ...

Proof of (a). TODO. □

Exercise 2.45. Obtain a formula for $\text{disc}(\alpha)$ 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)

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

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

- (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 $\text{disc}(\alpha) = (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} a^n + (-1)^{\frac{n(n-1)}{2}} n^n b^{n-1}$.

$$\text{disc}(\alpha) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(f'(\alpha)) \quad (\text{Theorem 2.8})$$

$$= (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]} \left(-\frac{(n-1)a\alpha + nb}{\alpha} \right) \quad ((1))$$

$$= (-1)^{\frac{n(n-1)}{2}} (-1)^n \frac{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}((n-1)a\alpha + nb)}{N_{\mathbb{Q}}^{\mathbb{Q}[\alpha]}(\alpha)}$$

$$= (-1)^{\frac{n(n-1)}{2}} (-1)^n \frac{-(n-1)^{n-1} a^n b + (-1)^n n^n b^n}{b} \quad ((2))$$

$$= (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} a^n + (-1)^{\frac{n(n-1)}{2}} n^n b^{n-1}.$$

□

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