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 $I^2 \subseteq 2I$.

□

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 $0 \le m_k < n_k$ *and* $0 \le m < n$. 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 $m_k \ge 0$ and $m \ge 0$.

If $m \ge n$, 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 $m_k' \ge 0$ and $0 \le m' < n$.

Once the degree of α^m is reduced, continue to reduce the degree of each $a_k^{m_k'}$ without affecting other a_h ($h \ne k$) 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 $0 \le m_k'' < n_k$ and $0 \le m' < n$.

(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).

$\square$

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 $1 \le k \le p-1$, show that p divides $\binom{p}{k}$.

(a) If $1 \le k \le p-1$, 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 $1 \le k \le p-1$.

(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 $f(x) = a_1 x + a_0$,

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

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

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

The inductive step is established.

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

$\square$

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

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 $N^{\mathbb{Q}[\alpha]}_{\mathbb{Q}}(2a\alpha+3b)$.

(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).

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

□

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

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

$\square$

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. $\square$

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. □