Chapter 2: Number Fields and Number Rings

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

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

□

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).

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

□

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

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

□

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)(Exercise 2.28). ... □

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

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

□

Proof of $x^n + ax^{n-1} + b$ *(Exercise 2.28).* ... □