Exercise (2.8)**.**

(a) Let $\omega = e^{2\pi i/p}$, p an odd prime. Show that $\mathbb{Q}[\omega]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p}$ if $p \equiv -1 \pmod 4$. Express $\sqrt{-3}$ and $\sqrt{5}$ as polynomials in the appropriate ω.

(b) Show that the 8th cyclotomic field contains $\sqrt{2}$.

(c) Show that every quadratic field is contained in a cyclotomic field.

Proof.

(a) First, here's a very unmotivated explicit solution (skip below the line for the "better" proof). Let $\chi(n)$ denote the Legendre symbol, so that χ depends only on the residue mod p, $\chi(0) = 0$ and otherwise $\chi(n) = 1$ if and only if n is a perfect square mod p. For $t \in \{1, \dots, p-1\}$, let t^{-1} denote the unique integer in $\{1, \dots, p-1\}$ such that tt^{-1} is 1 modulo p. Define

$$a_r = \sum_{n=1}^{p-1} \chi(n(r-n))$$

Note that:

$$a_0 = \sum_{n=1}^{p-1} \chi(-n^2) = \chi(-1)(p-1)$$

and for $1 \le r \le p-1$,

$$a_r = \sum_{n=1}^{p-1} \chi((r^{-1})^2)\chi(n(r-n)) = \sum_{n=1}^{p-1} \chi(r^{-1}n(1-r^{-1}n)) = \sum_{k=1}^{p-1} \chi(k(1-k)) = a_1$$

since multiplication by r^{-1} simply permutes $\{1, \dots, p-1\}$. Finally, define

$$f(x) = \sum_{n=0}^{p-1} \chi(n)x^n$$

If γ satisfies $\gamma^p = 1$, then

$$\begin{aligned}
(f(\gamma))^2 &= \left(\sum_{n=0}^{p-1} \chi(n)\gamma^n\right)^2 \\
&= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1} \chi(n)\chi(m)\gamma^{n+m} \\
&= \sum_{r=0}^{p-1}\sum_{m=0}^{p-1} \chi(m(r-m))\gamma^r && \text{for } r \equiv n+m \\
&= \sum_{r=0}^{p-1} a_r\gamma^r \\
&= \chi(-1)(p-1) + a_1\sum_{r=1}^{p-1}\gamma^r
\end{aligned}$$

On one hand, since $1^p = 1$, we can take $\gamma = 1$. But $f(1) = 0$ since there are exactly $(p-1)/2$ residues and nonresidues modulo p. So, this gives

$$\chi(-1)(p-1) + (p-1)a_1 = 0 \implies a_1 = -\chi(-1)$$

On the other hand, we can take $\gamma = \omega$ which gives:

$$f(\omega)^2 = \chi(-1)(p-1) + a_1\sum_{r=1}^{p-1}\omega^r = \chi(-1)(p-1) + \chi(-1) = \chi(-1)p$$

which is what we wished to show, since now $f(\omega)$ is in $\mathbb{Q}(\omega)$ and has square $\pm p$.

"Better" proof: We've shown that $\operatorname{disc}(\omega) = p^{p-2}$ if $p \equiv 1 \pmod 4$ and $\operatorname{disc}(\omega) = -p^{p-2}$ otherwise. But we can write $\operatorname{disc}(\omega) = |\sigma_i(\omega^j)|^2$, where $|\cdot|$ denotes the determinant, and i, j range over the appropriate indices. Thus, $\pm p^{p-2}$ is a square of an element in $\mathbb{Q}[\omega]$, and since p is odd, so is p^{p-3}. Hence, the quotient is a square in $\mathbb{Q}[\omega]$, namely $\sqrt{\pm p} \in \mathbb{Q}[\omega]$.

Now, we consider the explicit cases. Note that the "worse" proof actually helps here, since it was very explicit. For $p = 3$, the proof showed that

$$\sqrt{-3} = \omega - \omega^2 = \omega - \omega^{-1}$$

which is also clear since $\omega^{\pm 1} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$. For $p = 5$, the proof showed:

$$\sqrt{5} = \omega - \omega^2 - \omega^3 + \omega^4$$

To confirm this, we can square the expression:

$$(\omega - \omega^2 - \omega^3 + \omega^4)^2 = \omega^2 - 2\omega^3 - \omega^4 + 4\omega^5 - \omega^6 - 2\omega^7 + \omega^8 = 4 - \omega - \omega^2 - \omega^3 - \omega^4 = 5$$

as claimed.

(b) Let $\omega = e^{2\pi i/8}$. Then, $\omega^2 = i$, so:

$$(\omega + \omega^{-1})^2 = \omega^2 + 2 + \omega^{-2} = i + 2 - i = 2$$

i.e. $\sqrt{2} = \pm(\omega + \omega^{-1}) \in \mathbb{Q}[\omega]$.

(c) Let m be squarefree. Then we can write m as a product of primes $\pm p_1 \cdots p_k$. Consider the field $K = \mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/(8m)}$. Then, $\omega^m = \sqrt{i}$, so K contains the 8th cyclotomic field, and so contains $\sqrt{2}$. Similarly, $\omega^{2m} = i$, and so K contains $\sqrt{-1}$. Finally, for each odd prime divisor p_j, $\omega^{4m/p_j} = e^{2\pi i/p_j}$, so K contains $\sqrt{\pm p_j}$ for each j. Hence, multiplying the necessary terms, we have that K contains $\sqrt{m}$. □

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

(a) Show that $f'(\alpha) = -(2a\alpha + 3b)/\alpha$.

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

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

(d) Suppose $\alpha^3 = \alpha + 1$. Prove that $\{1, \alpha, \alpha^2\}$ is an integral basis for the ring of integers in $\mathbb{Q}[\alpha]$. Do the same if $\alpha^3 + \alpha = 1$.

Proof.

(a) We have

$$\alpha f'(\alpha) = \alpha(3\alpha^2 + a) = 3\alpha^3 + a\alpha = 3(-a\alpha - b) + a\alpha = -(2a\alpha + 3b)$$

as claimed.

(b) Now, let $\alpha_1, \alpha_2, \alpha_3$ denote the three roots of f. Then,

$$f(x) = \prod_i (x - \alpha_i)$$

and

$$\begin{aligned} N(2a\alpha + 3b) &= \prod_i (2a\alpha_i + 3b) \\ &= (-2a)^3 \prod_i \left(-\frac{3b}{2a} - \alpha_i\right) \\ &= -8a^3 f\left(-\frac{3b}{2a}\right) \\ &= -8a^3\left(-\frac{27b^3}{8a^3} - a\frac{3b}{2a} + b\right) \\ &= 27b^3 + 4a^3 b \end{aligned}$$

(c) So, we can compute the discriminant, noting that N is multiplicative and $N(\alpha) = -b$ from the constant term of f:

$$\operatorname{disc}(\alpha) = -N(f'(\alpha)) = -N\left(-\frac{2a\alpha + 3b}{\alpha}\right) = -(-1)^3 \frac{b(27b^2 + 4a^3)}{-b} = -(4a^3 + 27b^2)$$

as claimed.

(d) Finally, we consider the explicit examples. If $\alpha^3 = \alpha + 1$, then

$$\operatorname{disc}(\alpha) = -(4(-1)^3 + 27(-1)^2) = -23$$

This is squarefree, so we get that $\mathbb{Z}[\alpha]$ is the ring of integers in $\mathbb{Q}(\alpha)$. Second, if $\alpha^3 + \alpha = 1$, then

$$\operatorname{disc}(\alpha) = -(4 \cdot 1^3 + 27(-1)^2) = -31$$

which is also squarefree, giving the same result. $\square$