Assignment 1

Due on March 31, 2009

The following notations will be used in the sequel. For a positive integer m, we set $\omega_m = \exp(2\pi i/m) \in \mathbb{C}$, and let $K_m = \mathbb{Q}(\omega_m) \subset \mathbb{C}$. Let $\mathcal{O}$ = the subset of all algebraic integers in $\mathbb{C}$. For a subset $K \subset \mathbb{C}$, write $\mathcal{O}_K = K \cap \mathcal{O}$.

1. Let m_1, m_2 be two positive integers. Show that

$$\begin{aligned} K_{m_1} \cdot K_{m_2} &= K_{\overline{m}} \\ K_{m_1} \cap K_{m_2} &= K_{\underline{m}} \end{aligned}$$

where $\overline{m} = \operatorname{lcm}(m_1, m_2)$ and $\underline{m} = \gcd(m_1, m_2)$.

2. ([1, Ex 2.8])

   (a) Let p be an odd rational prime. Show that

$$K_p \ni \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ \sqrt{-p} & \text{if } p \equiv -1 \pmod 4 \end{cases}.$$

   (Hint: Recall that $\operatorname{disc}(\omega_p) = \pm p^{p-2}$ with $+$ holding iff $p \equiv 1 \pmod 4$.)

   (b) Show that K_8 contains $\sqrt{2}$.

   (c) Show that every quadratic field is contained in a cyclotomic field. In fact, $\mathbb{Q}(\sqrt{m}) \subset K_d$ where $d = \operatorname{disc} \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

3. ([1, Ex 2.11])

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

   (b) Show that there are only finitely many algebraic integers α of fixed degree n, all of whose conjugate (including α) have absolute value 1.

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

4. ([1, Ex 2.42]) Let $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ where m, n are distinct square-free integers $\neq 1$. Then K contains $\mathbb{Q}[\sqrt{k}]$, where $k = mn/(m,n)^2$.

   (a) For $\alpha \in K$. Show that $\alpha \in \mathcal{O}_K$ iff the relative norm and trace $\operatorname{Nm}^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ and $\operatorname{Tr}^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$ are in $\mathcal{O}$.

   (b) Suppose $m \equiv 3, n \equiv k \equiv 2 \pmod 4$. Show that every $\alpha \in \mathcal{O}_K$ has the form

$$\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2} \qquad (\spadesuit)$$

   for some $a, b, c, d \in \mathbb{Z}$. (Suggestion: Write α as a linear combination of $1, \sqrt{m}, \sqrt{n}, \sqrt{k}$ with rational coefficients and consider all three relative traces.) Show that a and b

must be even and $c \equiv d \pmod 2$ by considering $\mathrm{Nm}^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$. Conclude that an integral basis for $\mathcal{O}_K$ is

$$\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}.$$

(c) Suppose $m \equiv 1, n \equiv k \equiv 2$ or $3 \pmod 4$. Again show that each $\alpha \in \mathcal{O}_K$ has the form (♠). Show that $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$. Conclude that an integral basis for $\mathcal{O}_K$ is

$$\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}.$$

(d) Suppose $m \equiv n \equiv k \equiv 1 \pmod 4$. Show that every $\alpha \in \mathcal{O}_K$ has the form

$$\frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{4}$$

with $a \equiv b \equiv c \equiv d \pmod 2$. Show that by adding an appropriate integer multiple of

$$\left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right),$$

we can obtain a member of $\mathcal{O}_K$ having the form

$$\frac{r+s\sqrt{m}+t\sqrt{n}}{2}$$

with $r, s, t \in \mathbb{Z}$; moreover show that $r+s+t \equiv 0 \pmod 2$. Conclude that an integral basis for $\mathcal{O}_K$ is

$$\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right\}.$$

(e) Show that (b), (c), (d) cover all cases except for rearrangements of m, n, k.

(f) Show that

$$\operatorname{disc}\mathcal{O}_K = \begin{cases} 64mnk & \text{in (b)} \\ 16mnk & \text{in (c)} \\ mnk & \text{in (d)} \end{cases}.$$

(Suggestion: In (b), for example, compare $\operatorname{disc}\mathcal{O}_K$ with $\operatorname{disc}(1, \sqrt{m}, \sqrt{n}, \sqrt{k})$.) Verify that in all cases $\operatorname{disc}\mathcal{O}_K$ is the product of the discriminants of the three quadratic subfields.

References

[1] D.A. Marcus, *Number fields.* Universitext. Springer-Verlag, New York-Heidelberg, 1977.