# Algebraic Number Theory
# MATH 512

## Solutions to Assignment 1

**1.** (a) Suppose $K = \mathbb{Q}(\alpha)$ where $\alpha$ is a root of $x^2 + ax + b \in \mathbb{Q}[x]$. Completing the square, we see that $K = \mathbb{Q}(\sqrt{c})$ where $c = b - \frac{1}{4}a^2 \in \mathbb{Q}^\times$. Writing $c = r/s$ with $r, s \in \mathbb{Z} \smallsetminus \{0\}$, we further see that

$$K = \mathbb{Q}(\sqrt{r/s}) = \mathbb{Q}(s\sqrt{r/s}) = \mathbb{Q}(\sqrt{rs}),$$

i.e. $K = \mathbb{Q}(\sqrt{t})$ for some non-zero integer $t$. Write $t = Dt_1^2$ with $D$ square-free and $t_1 \neq 0$. Then

$$K = \mathbb{Q}(t_1\sqrt{D}) = \mathbb{Q}(\sqrt{D}).$$

Since $K \neq \mathbb{Q}$, $D \neq 1$.

(b) Suppose $\varphi : \mathbb{Q}(\sqrt{D_1}) \to \mathbb{Q}(\sqrt{D_2})$ is an isomorphism. Write $\varphi(\sqrt{D_1}) = a + b\sqrt{D_2}$ with $a, b \in \mathbb{Q}$.

$$\begin{aligned} D_1 &= \varphi(D_1) \\ &= \varphi(\sqrt{D_1})^2 \\ &= (a + b\sqrt{D_2})^2 \\ &= a^2 + D_2 b^2 + 2ab\sqrt{D_2}. \end{aligned}$$

Since $\sqrt{D_2} \notin \mathbb{Q}$, we have $2ab = 0$, i.e. $a = 0$ or $b = 0$. If $b = 0$, then $D_1 = a^2$, which is not possible since $D_1$ is square-free and different from 1. Therefore $a = 0$. Write $b = r/s$ with $r, s$ non-zero coprime integers. Then $D_1 = D_2 r^2/s^2$, i.e. $s^2 D_1 = r^2 D_2$. Since $D_1$ and $D_2$ are square-free (and $r^2$ and $s^2$ are coprime), we must have $r^2 = s^2 = 1$, i.e. $b^2 = 1$, i.e. $D_1 = D_2$.

**2.** Let $\alpha \in L$, and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ be its minimal polynomial over $\mathbb{Q}$. Choose a non-zero integer $b$ such that $ba_i \in \mathbb{Z}$ for $i = 0, \ldots, n-1$, and let $g(x) = x^n + ba_{n-1}x^{n-1} + b^2 a_{n-2}x^{n-2} + \cdots + b^{n-1}a_1 x + b^n a_0 \in \mathbb{Z}[x]$. Setting $\beta = b\alpha$, we have $g(\beta) = 0$, and so $\beta \in \mathcal{O}_L$. Also, $b \in \mathbb{Z} \subseteq \mathcal{O}_L$. Therefore $\alpha = \beta/b$ is the quotient of two elements of $\mathcal{O}_L$.

**3.** Let $a \in L^\times$ and $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{Q}[x]$ its minimal polynomial over $\mathbb{Q}$. Observing that $b_0$ is necessarily non-zero, define

$$\tilde{f}(x) = x^n + b_1 b_0^{-1} x^{n-1} + b_2 b_0^{-1} x^{n-2} + \cdots + b_{n-1} b_0^{-1} x + b_0^{-1} \in \mathbb{Q}[x].$$

Then $b_0 a^n \tilde{f}(a^{-1}) = f(a) = 0$, so $\tilde{f}(a^{-1}) = 0$. Since $[\mathbb{Q}(a^{-1}) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] = n$, $\tilde{f}(x)$ is the minimal polynomial of $a^{-1}$ over $\mathbb{Q}$. Now, $a$ is a unit of $L$ if and only of both $a$ and $a^{-1}$ lie in $\mathcal{O}_L$, if and only if $f(x)$ and $\tilde{f}(x)$ have integral coefficients, if and only if $b_0, \ldots, b_{n-1}$ and $b_0^{-1}$ are all in $\mathbb{Z}$, if and only if $b_0, \ldots, b_{n-1} \in \mathbb{Z}$ and $b_0 = \pm 1$.

**4.** (a) Let $L = \mathbb{Q}(\alpha)$, $M = \mathbb{Q}(\alpha, \omega)$ where $\omega$ is a primitive cubic root of unity in $\bar{\mathbb{Q}}$, and $\gamma = a\alpha^2 + b\alpha + c$ with $a, b, c \in \mathbb{Q}$. We apply Corollary 5 to this data (so the element in question is $\gamma$). In the notation of that corollary, we may take the set $A$ to be $\{1, \sigma, \sigma^2\}$, where $\sigma \in \mathrm{Gal}(M/\mathbb{Q}(\omega))$ is defined by $\sigma(\alpha) = \omega\alpha$. Then, again in the notation of Corollary 5,

$$\begin{aligned} g_\gamma(x) &= (x-\gamma)(x-\sigma(\gamma))(x-\sigma^2(\gamma)) \\ &= x^3 - (\gamma + \sigma(\gamma) + \sigma^2(\gamma))x^2 \\ &\quad + (\gamma\sigma(\gamma) + \sigma(\gamma)\sigma^2(\gamma) + \sigma^2(\gamma)\gamma)x - \gamma\sigma(\gamma)\sigma^2(\gamma). \end{aligned}$$

Using only the facts that $\alpha^3 = 2$ and $\omega^2 + \omega + 1 = 0$, one can calculate the coefficients explicitly as rational numbers in terms of $a, b, c$, arriving at

$$g_\gamma(x) = x^3 - 3cx^2 + 3(c^2 - 2ab)x - (4a^3 + 2b^3 + c^3 - 6abc).$$

To make the above computation easier, one may observe that $\alpha + \sigma(\alpha) + \sigma^2(\alpha) = (1 + \omega + \omega^2)\alpha = 0$, and similarly for $\alpha^2$ in place of $\alpha$. It is then immediate that the coefficient of $x^2$ in $g_\gamma(x)$ is $-3c$. The rest is left as an exercise.

By Corollary 5, $\gamma \in \mathcal{O}_L$ if and only if $g_\gamma(x) \in \mathbb{Z}[x]$. Since we already know that $1, \alpha, \alpha^2 \in \mathcal{O}_L$, to complete part (a) it is enough to show that if $g_\gamma(x) \in \mathbb{Z}[x]$, then $a, b, c \in \mathbb{Z}$. Suppose then that

$$3c = l \tag{1}$$

$$3(c^2 - 2ab) = m \tag{2}$$

$$4a^3 + 2b^3 + c^3 - 6abc = n \tag{3}$$

with $l, m, n \in \mathbb{Z}$. We also write $a = a_1/a_2$ and $b = b_1/b_2$ with $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $b_1, b_2 > 0$, and $\gcd(a_1, a_2) = \gcd(b_1, b_2) = 1$. We therefore obtain from (1) and (2):

$$l^2 - 18ab = 3m \tag{4}$$

and

$$a_2 b_2 (l^2 - 3m) = 18 a_1 b_1. \tag{5}$$

We also obtain from (1), (2) and (3):

$$4 \cdot 3^3 a^3 + 2 \cdot 3^3 b^3 - 2l^3 + 3^2 ml - 3^3 n = 0. \tag{6}$$

**Step 1: Show** $3|l$

Let us suppose that $3 \nmid l$ and aim for a contradiction. Observe then that (5) implies that 3 divides $a_2$ or $b_2$.

Consider first the case where $3|a_2$. The case $3|b_2$ is entirely similar. We let $v : \mathbb{Q}^\times \to \mathbb{Z}$ denote the 3-adic valuation on $\mathbb{Q}$, that is to say if $h = 3^j \cdot h_1/h_2$ with $3 \nmid h_1, h_2$, then $v(h) = j$. We are assuming, then, that $v(a) \leq -1$. Then (4) implies that $2 + v(a) + v(b) = 0$. Examining the valuations of the terms in (6), we see that if $v(a) < -1$ then each term on the left-hand side of the equation has non-negative valuation except the first, which is impossible since the right-hand side is zero. Thus $v(a) = -1$, and so $v(b) = -1$ also.

Repeating the argument with $b$ in place of $a$, we obtain $v(a) = v(b) = -1$ once again. Thus, under our assumption that $3 \nmid l$, we have $v(a) = v(b) = -1$. We may therefore write $3a = \tilde{a}$ and $3b = \tilde{b}$ with $\tilde{a}, \tilde{b} \in \mathbb{Q}^\times$ and $v(\tilde{a}) = v(\tilde{b}) = 0$. We obtain from (4) and (6) the equations

$$l^2 - 2\tilde{a}\tilde{b} = 3m \tag{7}$$

and

$$4\tilde{a}^3 + 2\tilde{b}^3 - 2l^3 + 3^2 ml - 3^3 n = 0. \tag{8}$$

One sees from these equations that for $p \neq 3$, the $p$-adic valuations of $\tilde{a}$ and $\tilde{b}$ have to be non-negative. Since the 3-adic valuations are 0 by assumption, $\tilde{a}$ and $\tilde{b}$ are integers. Since $l^2 \equiv 1 \bmod 3$, (7) implies that $3|\tilde{a} + \tilde{b}$. Reducing (8) mod 3 therefore gives $l + 2\tilde{a} \equiv 0 \bmod 3$, i.e. $\tilde{a} \equiv l \bmod 3$. Hence $\tilde{b} \equiv -l \bmod 3$. This allows us to write $\tilde{a} = 3w + l$ and $\tilde{b} = 3z - l$ with $w, z \in \mathbb{Z}$.

We now return to (3), and multiply both sides by 27 to obtain

$$\begin{aligned}
27n &= 4\tilde{a}^3 + 2\tilde{b}^3 + l^3 - 6\tilde{a}\tilde{b}l \\
&= 4(3w+l)^3 + 2(3z-l)^3 + l^3 - 6(3w+l)(3z-l)l \\
&= 4(27w^3 + 27w^2 l + 9wl^2 + l^3) + 2(27z^3 - 27z^2 l + 9zl^2 - l^3) \\
&\quad + l^3 - 6(9wz - 3wl + 3zl - l^2)l \\
&\overset{(27)}{=} 4l^2(9w+l) + 2l^2(9z-l) + l^3 - 6(-3wl + 3zl - l^2)l \\
&\overset{(27)}{=} 9wl^2 + 4l^3 + 18zl^2 - 2l^3 + l^3 + 18wl^2 - 18zl^2 + 6l^3 \\
&\overset{(27)}{=} 9l^3.
\end{aligned}$$

(Here, $\overset{(27)}{=}$ means equivalence mod 27.) We thus deduce that $27|9l^3$, i.e. $3|l^3$, a contradiction. Our original assumption that $3 \nmid l$ having led to a contradiction, we therefore conclude that $3|l$, i.e. $c \in \mathbb{Z}$.

**Step 2: Show $a_2$ and $b_2$ divide 6**

We recall that we have so far proven that $c \in \mathbb{Z}$. Now, from (5) we obtain $a_2 b_2 (3c^2 - m) = 6a_1 b_1$, from which we deduce $a_2 | 6b_1$ and $b_2 | 6a_1$. Let us write $6a_1 = rb_2$ and $6b_1 = sa_2$ with $r, s \in \mathbb{Z}$. (3) gives

$$n = \frac{4a_1^3}{a_2^3} + \frac{2b_1^3}{b_2^3} + c^3 - \frac{6a_1 b_1 c}{a_2 b_2}.$$

Multiplying by $a_2^3$ and using the fact that $b_1$ and $b_2$ are coprime, we see that $b_2^3 | 2a_2^3$. The same argument with $a_2$ and $b_2$ interchanged shows that $a_2^3 | 4b_2^3$. Thus there exist positive integers $u$ and $t$ with $2a_2^3 = tb_2^3$ and $4b_2^3 = ua_2^3$. One sees that $ut = 8$, so $t = 1, 2, 4$ or 8. We may rule out $t = 1$ and $t = 4$ since they imply, respectively, that $2a_2^3 = b_2^3$ and $a_2^3 = 2b_2^3$, both impossible. We may also rule out $t = 8$, since this implies $a_2^3 = 4b_2^3$, again impossible. Hence $t = 2$, so that $a_2^3 = b_2^3$, i.e. $a_2 = b_2$ since $a_2$ and $b_2$ are both positive by assumption. Therefore the statements $a_2|6b_1$ and $b_2|6a_1$ deduced at the beginning of Step 2 become $b_2|6b_1$ and $a_2|6a_1$. Thus $a_2$ and $b_2$ both divide 6.

**Step 3: Show** $a, b \in \mathbb{Z}$

By the conclusion of Step 2, we may write $a = 6a'$ and $b = 6b'$ with $a', b' \in \mathbb{Z}$. Multiplying (3) by $6^2$ we have

$$2(a')^3 + (b')^3 + 3 \cdot 6^2 c^3 - 18a'b'c - 3 \cdot 6^2 n = 0. \tag{9}$$

This shows that $2|b'$, but then (9) implies that $2|a'$ as well (work mod 4).

Now, (2) implies $18c^2 - a'b' = 6m$, so 3 divides $a'$ or $b'$. However, (9) tells us that $(a')^3 \equiv (b')^3$ mod 3, i.e. $a' \equiv b'$ mod 3, so 3 must divide both $a'$ and $b'$. We conclude that 6 divides $a'$ and $b'$, i.e. $a, b \in \mathbb{Z}$.

This completes our proof that $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

(b) The embeddings of $L$ into $\bar{\mathbb{Q}}$ are induced by $1, \sigma, \sigma^2$, so

$$\begin{aligned} d_L &= \det \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \omega\alpha & \omega^2\alpha^2 \\ 1 & \omega^2\alpha & \omega\alpha^2 \end{pmatrix}^2 \\ &= (6(\omega^2 - \omega))^2 \\ &= -2^2 \cdot 3^3. \end{aligned}$$

**5.** If $L$ is a number field, then every prime ideal of $L$ contains a rational prime, and there are finitely many prime ideals of $L$ above any given rational prime. This shows that, if there are only finitely many rational primes, then any number field has only finitely many prime ideals. This means that the ring of integers of any number field, being in that case a Dedekind domain with only finitely many prime ideals, would be a principal ideal domain, and in particular a unique factorization domain. However, we have seen an example of a number field whose ring of integers does not have uniqueness of factorization, namely $\mathbb{Q}(\sqrt{-6})$. Thus there must be infinitely many rational primes. (Actually, a Dedekind domain is a P.I.D. if and only if it is a U.F.D., but we did not need this fact in the foregoing argument.)