Algebraic Number Theory Homework 2

Michael Nelson

Problem 2

Let α be an algebraic integer of degree n, and let $f(x)$ be its minimal polynomial over $\mathbb{Q}$. Define the discriminant of α, denoted $\Delta(\alpha)$, to be the discriminant of the basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ for $\mathbb{Q}(\alpha)/\mathbb{Q}$, and let $\alpha_1, \dots, \alpha_n$ be the conjugates of α.

Problem 2.a

Exercise 1. Show that

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} \prod_{1 \leq i \leq n} f'(\alpha_i). \tag{1}$$

Solution 1. The discriminant is of $\{1, \alpha, \dots, \alpha^{n-1}\}$ for $\mathbb{Q}(\alpha)/\mathbb{Q}$ is, by definition, given by

$$\Delta(\alpha) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_2 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^2 = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2.$$

To show (1), write

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

By the product rule, observe that

$$f'(\alpha_i) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\alpha_i - \alpha_j).$$

Multiplying these over all i gives us

$$\prod_{1 \leq i \leq n} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\alpha_i - \alpha_j) = \prod_{1 \leq i \leq n} f'(\alpha_i).$$

The product of $\alpha_i - \alpha_j$ runs over sets of distinct indices i and j. To rewrite thie product over index pairs where $i < j$, collect $\alpha_i - \alpha_j$ and $\alpha_j - \alpha_i$ together as $-(\alpha_j - \alpha_i)^2$. There are $\binom{n}{2}$ such pairs, so

$$\Delta(\alpha) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2 = (-1)^{\binom{n}{2}} \prod_{1 \leq i \leq n} f'(\alpha_i).$$

Problem 2.b

Exercise 2. Use part (a) to compute the discriminant of α if α is a root of the polynomial $f(x) = x^n + ax + b$ where $a, b \in \mathbb{Z}$ are chosen so that $f(x)$ is irreducible.

Solution 2. Let $\alpha_1, \dots, \alpha_n$ be the distinct roots of $f(x)$. For each $k, n \in \mathbb{N}$ the kth elementary symmetric polynomial in the variables $t_1, \dots, t_n$, denoted $e_k(t_1, \dots, t_n)$, is defined by

$$e_k(t_1, \dots, t_n) = \begin{cases} 1 & \text{if } k = 0 \\ \sum_{1 \leq i_1 < \cdots < i_k \leq n} t_{i_1} \cdots t_{i_k} & \text{if } k \leq n \\ 0 & \text{if } k > n \end{cases}$$

In particular, we have

$$\begin{aligned}
x^n + ax + b &= f(x) \\
&= \prod_{k=1}^{n}(x - \alpha_k) \\
&= x^n + \sum_{k=1}^{n}(-1)^k e_k(\alpha_1, \dots, \alpha_n) x^{n-k}.
\end{aligned}$$

Equating coefficients gives us

$$e_k(\alpha_1, \dots, \alpha_n) = \begin{cases} (-1)^n b & \text{if } k = n \\ (-1)^{n-1} a & \text{if } k = n-1 \\ 0 & \text{if } k < n-1 \end{cases}$$

Now since $f'(x) = nx^{n-1} + a$, we have

$$\begin{aligned}
\Delta(\alpha) &= (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i) \\
&= (-1)^{\binom{n}{2}} \prod_{i=1}^{n} (n\alpha_i^{n-1} + a) \\
&= (-1)^{\binom{n}{2}} \left(\sum_{k=0}^{n} (n-k)^{n-k} a^k e_{n-k}(\alpha_1, \dots, \alpha_n)^{n-1} \right) \\
&= (-1)^{\binom{n}{2}} \left(n^n e_n(\alpha_1, \dots, \alpha_n)^{n-1} + (n-1)^{n-1} e_{n-1}(\alpha_1, \dots, \alpha_n)^{n-1} a \right) \\
&= (-1)^{\binom{n}{2}} \left(n^n (-1)^{n(n-1)} b^{n-1} + (n-1)^{n-1} (-1)^{(n-1)(n-1)} a^n \right) \\
&= (-1)^{\binom{n}{2}} \left(n^n b^{n-1} + (n-1)^{n-1} (-1)^{(n-1)} a^n \right).
\end{aligned}$$

Problem 2.c

Exercise 3. Find an integral basis for the ring of integers $\mathbb{Q}(\theta)$ where θ is a root of the polynoimal $x^3 - 2x + 3$.

Solution 3. First note that $x^3 - 2x + 3$ is irreducible over $\mathbb{Q}$ since it is irreducible over $\mathbb{F}_5$. Indeed, if $x^3 - 2x + 3$ were reducible over $\mathbb{F}_5$, then it must have a root in $\mathbb{F}_5$, but a brute force calculation shows that it doesn't:

$$\begin{aligned}
0^3 - 2 \cdot 0 + 3 &\equiv 3 \mod 5 \\
1^3 - 2 \cdot 1 + 3 &\equiv 2 \mod 5 \\
2^3 - 2 \cdot 2 + 3 &\equiv 2 \mod 5 \\
3^3 - 2 \cdot 3 + 3 &\equiv 4 \mod 5 \\
4^3 - 2 \cdot 4 + 3 &\equiv 4 \mod 5
\end{aligned}$$

Using the formula above, we calculate

$$\begin{aligned}
\Delta(\theta) &= (-1)^{\binom{3}{2}} \left(3^3 \cdot 3^2 + 2^2 \cdot (-1)^{(3-1)} (-2)^3 \right) \\
&= -\left(3^5 - 2^5 \right) \\
&= -211.
\end{aligned}$$

Since 211 has no square factors, it follows from

$$\Delta(\theta) = |\mathcal{O}_{\mathbb{Q}(\theta)} / \mathbb{Z}[\theta]|^2 \Delta_{\mathbb{Q}(\theta)}$$

that $|\mathcal{O}_{\mathbb{Q}(\theta)} / \mathbb{Z}[\theta]|^2 = 1$. In other words, $\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$. In particular, $\{1, \theta, \theta^2\}$ gives an integral basis for $\mathbb{Q}(\theta)$.

Problem 2.d

Exercise 4. Find an integral basis for the ring of integers of $\mathbb{Q}(\theta)$ where θ is a root of the polynomial $x^3 - x - 4$.

Solution 4. First note that $x^3 - x - 4$ is irreducible over $\mathbb{Q}$ since it is irreducible over $\mathbb{F}_3$. Indeed, if $x^3 - x - 4$ were reducible over $\mathbb{F}_3$, then it must have a root in $\mathbb{F}_3$, but a brute force calculation shows that it doesn't:

$$\begin{aligned} 0^3 - 0 - 4 &\equiv 2 \mod 3 \\ 1^3 - 1 - 4 &\equiv 2 \mod 3 \\ 2^3 - 2 - 4 &\equiv 2 \mod 3 \end{aligned}$$

Using the formula above, we calculate

$$\begin{aligned} \Delta(\theta) &= (-1)^{\binom{3}{2}} \left(3^3 \cdot (-4)^2 + 2^2 \cdot (-1)^{(3-1)} \cdot (-1)^3\right) \\ &= -\left(3^3 \cdot 16 - 2^2\right) \\ &= -428 \\ &= -2^2 \cdot 107. \end{aligned}$$

Since 4 is the only square factor of $\Delta(\theta)$, it follows from

$$\Delta(\theta) = |\mathcal{O}_{\mathbb{Q}(\theta)}/\mathbb{Z}[\theta]|^2 \Delta_{\mathbb{Q}(\theta)}$$

that either $|\mathcal{O}_{\mathbb{Q}(\theta)}/\mathbb{Z}[\theta]|^2 = 1$ or $|\mathcal{O}_{\mathbb{Q}(\theta)}/\mathbb{Z}[\theta]|^2 = 2$. We will show that $|\mathcal{O}_{\mathbb{Q}(\theta)}/\mathbb{Z}[\theta]| = 2$ by finding an algebraic integer contained in $\mathbb{Q}(\theta)$ but which is not contained in $\mathbb{Z}[\theta]$. First note by a direct calculation, we have

$$(\theta^2 + \theta + 2)^2(\theta^2 + \theta + 2)^3 = 8(5\theta^2 + 9\theta + 11) \quad \text{and} \quad (\theta^2 + \theta + 2)^2 = 2(3\theta^2 + 5\theta + 6).$$

Therefore

$$\begin{aligned} \left(\frac{\theta^2 + \theta + 2}{2}\right)^3 - 4\left(\frac{\theta^2 + \theta + 2}{2}\right)^2 + 2\left(\frac{\theta^2 + \theta + 2}{2}\right) - 1 &= (5\theta^2 + 9\theta + 11) - (6\theta^2 + 10\theta + 12) + (\theta^2 + \theta + 2) - 1 \\ &= (5 - 6 + 1)\theta^2 + (9 - 10 + 1)\theta + (11 - 12 + 2 - 1) \\ &= 0. \end{aligned}$$

Thus $(\theta^2 + \theta + 2)/2$ is a root of the monic $x^3 - 4x^2 + 2x - 1$, so $(\theta^2 + \theta + 2)/2 \in \mathcal{O}_{\mathbb{Q}(\alpha)}$. Finally, since

$$\begin{aligned} \operatorname{disc}\left\{1, \theta, \frac{\theta^2 + \theta + 1}{2}\right\} &= \frac{1}{4} \cdot \operatorname{disc}\{1, \theta, \theta^2\} \\ &= -107, \end{aligned}$$

and 107 has no square factors, it follows that $\{1, \theta, (\theta^2 + \theta + 1)/2\}$ is an integral basis for the ring of integers of $\mathbb{Q}(\theta)$.

Problem 4

Exercise 5. Let I be an ideal in a Dedekind ring R. Show that I can be generated by 2 elements.

Solution 5. Write $I = \prod \mathfrak{p}_i^{a_i}$ with the $\mathfrak{p}_i$'s being pairwise distinct prime ideals and let $\alpha \in I$. If $I = (\alpha)$ then we are done, so assume $(\alpha) \subset I$. Since $(\alpha) \subset I$, we must have $(\alpha)I^{-1} \subseteq R$. In particular, $(\alpha)I^{-1}$ is an ideal, so it has a unique factorization in R, say

$$(\alpha)I^{-1} = \left(\prod \mathfrak{p}_i^{m_i}\right)\left(\prod \mathfrak{q}_j^{c_j}\right) \tag{2}$$

where the collection of all $\mathfrak{p}_i$'s and $\mathfrak{q}_j's$ and where $m_i \geq 0$ and $c_j \geq 1$. Multiplying both sides of (**??**) by $I = \prod \mathfrak{p}_i^{a_i}$ gives us

$$(\alpha) = \left(\prod \mathfrak{p}_i^{a_i + m_i}\right)\left(\prod \mathfrak{q}_j^{c_j}\right).$$

For each i, choose $\beta_i \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$. Since the $\mathfrak{p}_i^{a_i+1}$ and $\mathfrak{q}_j$ are pairwise relatively prime, the Chinese Remainder Theorem tells us that we can find a $\beta \in R$ such that $\beta \equiv \beta_i \mod \mathfrak{p}_i^{a_i+1}$ for all i and $\beta \equiv 1 \mod \mathfrak{q}_j$ for all j. In particular, $\beta \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$ and $\beta \notin \mathfrak{q}_j$ for all i, j. Indeed, it is clear that $\beta \notin \mathfrak{q}_j$ since $\beta \equiv 1 \mod \mathfrak{q}_j$. To see that $\beta \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$, observe that $\beta \equiv \beta_i \mod \mathfrak{p}_i^{a_i+1}$ implies

$$\beta = \beta_i + \alpha_i$$

for some $\alpha_i \in \mathfrak{p}_i^{a_i+1}$. Then $\beta \in \mathfrak{p}_i^{a_i}$ since $\alpha_i \in \mathfrak{p}_i^{a_i+1} \subseteq \mathfrak{p}_i^{a_i}$ and $\beta_i \in \mathfrak{p}_i^{a_i}$, and $\beta \notin \mathfrak{p}_i^{a_i+1}$ since $\alpha_i \in \mathfrak{p}_i^{a_i+1}$ and $\beta_i \notin \mathfrak{p}_i^{a_i+1}$. Note that since $\beta \in \mathfrak{p}_i^{a_i}$ for all i, we have

$$\begin{aligned} \beta &\in \bigcap_i \mathfrak{p}_i^{a_i} \\ &= \prod_i \mathfrak{p}_i^{a_i} \\ &= I. \end{aligned}$$

By a similar argument as for (α) above, we can write

$$(\beta) = \left(\prod \mathfrak{p}_i^{a_i+n_i}\right)\left(\prod \mathfrak{q}'^{c'_{j'}}_{j'}\right).$$

However we must have $n_i = 0$ since $\beta \notin \mathfrak{p}_i^{a_i+1}$ and we cannot have $\mathfrak{q}'_{j'} = \mathfrak{q}_j$ for some j, j' since $\beta \notin \mathfrak{q}_j$. It follows that

$$\begin{aligned} (\alpha, \beta) &= \left(\prod \mathfrak{p}_i^{\min(a_i+m_i, a_i+n_i)}\right)\left(\prod \mathfrak{q}_j^{\min(c_j,0)}\right)\left(\prod \mathfrak{q}'^{\min(0,c'_{j'})}_{j'}\right) \\ &= \left(\prod \mathfrak{p}_i^{\min(a_i+m_i, a_i)}\right)\left(\prod \mathfrak{q}_j^{\min(c_j,0)}\right)\left(\prod \mathfrak{q}'^{\min(0,c'_{j'})}_{j'}\right) \\ &= \prod \mathfrak{p}_i^{a_i} \\ &= I. \end{aligned}$$

Problem 7

Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(x) = x^3 - 2x - 2$.

Problem 7.a

Exercise 6. Show that $[K : \mathbb{Q}] = 3$ and that $\mathbb{Z}(\theta)$ is the ring of integers in K.

Solution 6. Observe that f is irreducible over $\mathbb{Q}$ since it is Eisenstein at 2. Thus f is the minimal polynomial of θ over $\mathbb{Q}$. In particular we have $[K : \mathbb{Q}] = \deg f = 3$. To show that $\mathbb{Z}(\theta)$ is the ring of integers in K, we first calculate

$$\begin{aligned} \Delta(\theta) &= (-1)^{\binom{3}{2}}\left(3^3 \cdot (-2)^2 + 2^2 \cdot (-1)^2 \cdot (-2)^3\right) \\ &= -(27 \cdot 4 - 4 \cdot 8) \\ &= -76 \\ &= -2^2 \cdot 19. \end{aligned}$$

Since 4 is the only square factor of $\Delta(\theta)$, it follows from

$$\Delta(\theta) = |\mathcal{O}_K / \mathbb{Z}[\theta]|^2 \Delta_K$$

that either $|\mathcal{O}_K / \mathbb{Z}[\theta]|^2 = 1$ or $|\mathcal{O}_K / \mathbb{Z}[\theta]|^2 = 2$. Since f is Eisenstein at 2, we can't have $|\mathcal{O}_K / \mathbb{Z}[\theta]|^2 = 2$, hence $|\mathcal{O}_K / \mathbb{Z}[\theta]|^2 = 1$. In other words, $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Problem 7.b

Exercise 7. Show that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial.

Proof. First we calculate the Minkowski bound:

$$\begin{aligned} \mathrm{M}_K &= \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|} \\ &= \frac{3!}{3^3}\left(\frac{4}{\pi}\right)^{1}\sqrt{2^2\cdot 19} \\ &\approx 2.467. \end{aligned}$$

Thus every ideal class can be represented by a nonzero ideal of norm ≤ 2. Since f is Eisenstein at 2, we see that 2 is totally ramified in $\mathcal{O}_K$. Let $\mathfrak{p}$ be the prime ideal in $\mathcal{O}_K$ which sits over 2 (so $(2) = \mathfrak{p}^3$). Since every ideal class can be represented by a nonzero ideal of norm ≤ 2, we see that either $\mathrm{Cl}(\mathcal{O}_K) = \{[1], [\mathfrak{p}]\}$ or $\mathrm{Cl}(\mathcal{O}_K)$ is trivial. Assume for a contradiction that $\mathrm{Cl}(\mathcal{O}_K)$ is not trivial, so $[\mathfrak{p}] \neq [1]$. It follows that $[\mathfrak{p}]^2 = [1]$ by Lagrange's Theorem. However we also know that $[\mathfrak{p}]^3 = [1]$ since $(2) = \mathfrak{p}^3$. In particular,

$$\begin{aligned} \mathrm{ord}[\mathfrak{p}] &\mid \gcd(2,3) \\ &= 1. \end{aligned}$$

It follows that $[\mathfrak{p}] = [1]$, which is a contradiction. $\square$

Problem 8

Exercise 8. Let $K = \mathbb{Q}(\sqrt{-6})$ and $\theta = \sqrt{-6}$. Determine which rational primes p split, ramify, and remain inert in K.

Solution 7. The minimal polynomial of θ over $\mathbb{Q}$ is $f(x) = x^2 + 6$, which has discriminant $-2^3 \cdot 3$. Since 4 is the only square factor of $\Delta(\theta)$, it follows from

$$\Delta(\theta) = |\mathcal{O}_K/\mathbb{Z}[\theta]|^2 \Delta_K$$

that either $|\mathcal{O}_K/\mathbb{Z}[\theta]|^2 = 1$ or $|\mathcal{O}_K/\mathbb{Z}[\theta]|^2 = 2$. Since f is Eisenstein at 2, we can't have $|\mathcal{O}_K/\mathbb{Z}[\theta]|^2 = 2$, hence $|\mathcal{O}_K/\mathbb{Z}[\theta]|^2 = 1$. In other words, $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Now let p be a rational prime. Since $|\mathcal{O}_K/\mathbb{Z}[\theta]| = 1$, we can determine how p factors in $\mathcal{O}_K$ by studying how $f(x)$ factors over $\mathbb{F}_p$. First note that since $\mathrm{disc}(f(x)) = -2^3 \cdot 3$, we see that the only primes which ramifies in K is either $p = 2$ or $p = 3$. Both primes ramify in K since $f(x)$ is Eisenstein at both $p = 2$ and $p = 3$. To see which primes split, observe that

$$\begin{aligned} p \text{ splits} &\iff f(x) \text{ splits over } \mathbb{F}_p \\ &\iff f(x) \text{ has a solution modulo } p \\ &\iff \left(\frac{-6}{p}\right) = 1 \\ &\iff \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \\ &\iff (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = 1 \\ &\iff (-1)^{\frac{p^2-1}{8}}\left(\frac{p}{3}\right) = 1 \\ &\iff p \equiv 1,5,7,11 \mod 24. \end{aligned}$$

Thus we have the following cases:

$$\begin{cases} \text{ramifies} & \text{if } p = 2,3 \\ \text{splits} & \text{if } p \equiv 1,5,7,11 \mod 24 \\ \text{inert} & \text{else} \end{cases}$$