MAT415 Assignment 3 Solutions

November 11, 2020

Problem 1 (Exercise (1) on Pg. 54)**.** *Let K be a number field, let $\alpha \in K$, and let $T_\alpha \colon K \to K$ be the linear transformation from the $\mathbb{Q}$-vector space K to itself corresponding to multiplication by α. Show that* $\det(T_\alpha) = N_{K/\mathbb{Q}}(\alpha)$.

Solution. Let $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. Then $[K : \mathbb{Q}(\alpha)] = \frac{n}{d}$. Note that $\det(T_\alpha) = \det(T_\alpha|_{\mathbb{Q}(\alpha)})^{\frac{n}{d}}$ and $N_{K/\mathbb{Q}}(\alpha) = (N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha))^{\frac{n}{d}}$. It thus suffices to show that $\det(T_\alpha|_{\mathbb{Q}(\alpha)}) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$.

Now, let's consider T_α as an operator on $\mathbb{Q}(\alpha)$. The characteristic polynomial of T_α, $\det(xI - T_\alpha)$, is a monic degree d polynomial with coefficients in $\mathbb{Q}$. Furthermore, it has α as a root. In particular, it must be equal to the minimal polynomial of α! It thus follows that $\det(T_\alpha|_{\mathbb{Q}(\alpha)}) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$. □

Problem 2 (Exercise (2) on Pg. 55)**.** *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.*

a) Show that

$$\Delta(\alpha) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\binom{n}{2}} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f'(\alpha)).$$

b) Suppose 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. Use part a) to show that

$$\Delta(\alpha) = (-1)^{\frac{n(n-1)}{2}} \left((-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}\right)$$

In particular, show that if $f(x) = x^2 + ax + b$ then $\Delta(\alpha) = a^2 - 4b$, an $\Delta(x) = x^3 + ax + b$ then $\Delta(\alpha) = -4a^3 - 27b^2$.

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

d) 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. Consult the solutions to Problem 3 and Problem 4 on Assignment 2. □

Problem 3 (Exercise (6) on Pg. 55)**.** *Factor the ideals* (2), (3), (7), (29), *and* (31) *into prime ideals in* $R = \mathbb{Z}[\sqrt[3]{2}]$.

Solution. As we noted in Assignment 3, in order to factor the ideal (p) into prime ideals in R, it suffices to factor the polynomial $f(x) = x^3 - 2$ into irreducibles modulo p, and to apply Kummer's factorisation theorem. From Assignment 2, we already know that $(2) = (2, \sqrt[3]{2})^3$, $(3) = (3, \sqrt[3]{2}+1)^3$ and (7) are the factorisation of the ideas (2), (3) and (7) into prime ideals in R.

Modulo 29, we have $x^3 - 2 = (x + 3)(x^2 + 26x + 9)$. Hence,

$$(29) = (29, \sqrt[3]{2} + 3)(29, (\sqrt[3]{2})^2 + 26\sqrt[3]{2} + 9).$$

Modulo 31, we have $x^3 - 2 = (x + 11)(x + 24)(x + 27)$. Hence,

$$(31) = (31, \sqrt[3]{2} + 11)(31, \sqrt[3]{2} + 24)(31, \sqrt[3]{2} + 27).$$

$\square$

Problem 4 (Exercise (7) on Pg. 55-6)**.** *Let $K = \mathbb{Q}(\theta)$, where θ is a root of $f(x) = x^3 - 2x - 2$.*

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

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

Solution. a) To show that $[K : \mathbb{Q}] = 3$, it suffices to show that $f(x)$ is irreducible over $\mathbb{Q}$. This follows at once from Eisenstein's criterion or by the rational roots theorem. By Problem 2, $\{1, \alpha, \alpha^2\}$ has discriminant $-76 = 4 \times 19$. However, since the polynomial is Eisenstein at the prime 2, Proposition 2.9 tell us that $\{1, \alpha, \alpha^2\}$ is an integral basis!

b) To show that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial, we will use the Minkowski bound. Recall that the Minkowski bound is given by:

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

In our case, $M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)^1\sqrt{76} \sim 2.47$. Therefore, we only need to factor (2). Modulo 2, the polynomial f factors as x^2. Hence,

$$(2) = (2, \alpha)^2 = (\alpha)^2.$$

It follows that every ideal if principal and we conclude that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial.

$\square$

Problem 5 (Exercise (10) on Pg. 56)**.** *Determine the ideal class group of $\mathbb{Z}[\sqrt[3]{2}]$.*

Solution. We will use Minkowski's bound. Recall that the Minkowski bound is given by:

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

In our case, $M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)^1\sqrt{108} \sim 2.94$. Thus, it suffices to factor (2). We know that it factors as

$$(2) = (2, \sqrt[3]{2})^3 = (\sqrt[3]{2})^3.$$

It follows that the class group is trivial. $\square$

Problem 6 (Exercise (11) on Pg. 56)**.** *Determine the ideal class groups (not just their orders) of:*

(a) $\mathbb{Z}[\sqrt{-14}]$.

(b) $\mathbb{Z}[\sqrt{-21}]$.

Solution. Note that $-14, -21 \not\equiv 1 \pmod 4$. Therefore $\mathbb{Z}[\sqrt{-14}]$ and $\mathbb{Z}[\sqrt{-21}]$ are the rings of integers in $\mathbb{Q}(\sqrt{-14})$ and $\mathbb{Q}(\sqrt{-21})$ respectively.

a) The discriminant is -56 and the norm form is $N(a + b\sqrt{-14}) = a^2 + 14b^2$. We will use Minkowski's bound. Recall that the Minkowski bound is given by:

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

In our case, $M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1\sqrt{56} \sim 4.76$. We thus factor (2) and (3).

$$(2) = (2, \sqrt{-14})^2 = \mathfrak{p}_1^2$$
$$(3) = (3, \sqrt{-14} - 1)(3, \sqrt{-14} + 1) = \mathfrak{p}_2\,\mathfrak{p}_3\,.$$

By examining the norm form, we see that there are no elements of norm equal to 2 or 3. In particular, $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ are not principal and they generate the class group. Furthermore, since $\mathfrak{p}_1^2 = (2)$ and $\mathfrak{p}_2\,\mathfrak{p}_3 = (3)$, we have $[\mathfrak{p}_1]^2 = 1$ and $[\mathfrak{p}_2] = [\mathfrak{p}_3]^{-1}$ in the class group.

To find a relation between $\mathfrak{p}_1$ and either $\mathfrak{p}_2$ or $\mathfrak{p}_3$, we look for elements whose norm is divisible by 2 and 3 only. By examining the norm form, we see that $N(2 + \sqrt{-14}) = 18 = 2 \times 3^2$. Note that $2 + \sqrt{-14} \in \mathfrak{p}_1$ and $\mathfrak{p}_2$. Furthermore, since $2 + \sqrt{-14}$ is not a multiple of 3, it does not belong to $\mathfrak{p}_3$. Hence, we have

$$(2 + \sqrt{-14}) = \mathfrak{p}_1\,\mathfrak{p}_2^2\,.$$

From this, we conclude that $[\mathfrak{p}_2]^2 = [\mathfrak{p}_1]^{-1} = [p_1]$ in the class group . This means that the class group is generated by $[\mathfrak{p}_2]$ and that $[\mathfrak{p}_2]$ has order 4 (since $[\mathfrak{p}_2]^2 = [\mathfrak{p}_1]$ has order 2).

Therefore, $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/4\mathbb{Z}$ and the generator can be taken to be either of the two prime factors of the ideal (3).

b) The discriminant is -84 and the norm form is $N(a + b\sqrt{-21}) = a^2 + 21b^2$. We will use Minkowski's bound. Recall that the Minkowski bound is given by:

$$M_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

In our case, $M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1\sqrt{84} \sim 5.83$. We thus factor (2), (3), and (5).

$$(2) = (2, \sqrt{-21} + 1)^2 = \mathfrak{p}_1^2$$
$$(3) = (3, \sqrt{-21})^2 = \mathfrak{p}_2^2$$
$$(5) = (5, \sqrt{-21} + 2)(5, \sqrt{-21} + 3) = \mathfrak{p}_3\,\mathfrak{p}_4\,.$$

By examining the norm form, we see that there are no elements of norm 2, 3, or 5. In particular, $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_4$ are not principal and they generate the class group. We now find relations by finding elements whose norm is divisible by 2, 3, or 5. Note that $N(3+\sqrt{-21}) = 30 = 2 \times 3 \times 5$. Plainly, we have:

$$(3 + \sqrt{-21}) = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_4\,.$$

Hence, $[\mathfrak{p}_1][\mathfrak{p}_2] = [\mathfrak{p}_4]^{-1}$ in the class group. In particular, since $\mathfrak{p}_4$ is not principal and since $\mathfrak{p}_3\,\mathfrak{p}_4 = (3)$, we can conclude that $[\mathfrak{p}_1]$ and $[\mathfrak{p}_2]$ are linearly independent and that $[\mathfrak{p}_1][\mathfrak{p}_2] = [\mathfrak{p}_3]$.

Therefore, $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the generators can be taken to be prime factors of the ideals (2) and (3).

□