MTH 617 Algebraic Number Theory

Solutions of the exercises appearing in the Second Mid Semester Examination

---

1. (a) [Newton's result on symmetric polynomials] Let A be a ring, $n \in \mathbb{N}$, $X_1, \ldots, X_n$ indeterminates over A and $\mathcal{S}_n$ the symmetry group of $\{1, 2, \ldots, n\}$. A polynomial $f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ is called symmetric, if $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n)$ for *every* $\sigma \in \mathcal{S}_n$. The r-th elementary symmetric polynomial is defined to be the symmetric polynomial

$$E_r := \sum_{1 \leqslant i_1 < \cdots < i_r \leqslant n} X_{i_1} \cdots X_{i_r}, \quad r = 1, \ldots, n.$$

Show that for any symmetric polynomial $f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ there exists $g(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ such that $f(X_1, \ldots, X_n) = g(E_1, \ldots, E_n)$.

Solution If $f = 0$, take $g := 0$. So assume that f is non-zero. Order the monomials $X_1^{j_1} \cdots X_n^{j_n}$, $(j_1, \ldots, j_n) \in \mathbb{Z}_+^n$, lexicographically, i.e., $X_1^{j_1} \cdots X_n^{j_n} < X_1^{k_1} \cdots X_n^{k_n}$ (or equivalently $(j_1, \ldots, j_n) < (k_1, \ldots, k_n)$), if and only if $j_1 = k_1, \ldots, j_{l-1} = k_{l-1}, j_l < k_l$ for some $l \in \{1, \ldots, n\}$. Note that under this ordering $1 < X_n < X_{n-1} < \cdots < X_1$. Denote by $\operatorname{lexdeg}(f) \in \mathbb{Z}_+^n$ the lexicographic degree of f, i.e., the tuple of exponents in the largest non-zero term in f. Let $(j_1, \ldots, j_n) := \operatorname{lexdeg}(f)$ and a the coefficient of the monomial $X_1^{j_1} \cdots X_n^{j_n}$ in f. Since f is symmetric by hypothesis, f must contain the term $aX_1^{j_{\sigma(1)}} \cdots X_n^{j_{\sigma(n)}}$ for each $\sigma \in \mathcal{S}_n$ and hence lexicographic ordering guarantees that $j_1 \geqslant j_2 \geqslant \cdots \geqslant j_n$. Now $\operatorname{lexdeg}(E_1^{j_1-j_2} E_2^{j_2-j_3} \cdots E_{n-1}^{j_{n-1}-j_n} E_n^{j_n}) = (j_1, \ldots, j_n)$ and $f - aE_1^{j_1-j_2} E_2^{j_2-j_3} \cdots E_{n-1}^{j_{n-1}-j_n} E_n^{j_n} \in A[X_1, \ldots, X_n]$ is again symmetric and is either zero or of lexicographic degree strictly smaller than $(j_1, \ldots, j_n)$. Proceeding in this way proves the result. The only thing we must argue is that the process terminates after finitely many steps. A naïve induction on the lexicographic degree does not help, since there are, in general, infinitely many tuples $(k_1, \ldots, k_n)$ less than $(j_1, \ldots, j_n)$. Symmetry helps here, because the added condition $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_n$ restricts the number of tuples $(k_1, \ldots, k_n) < (j_1, \ldots, j_n)$ to a finite value. That's all! •

(b) Let α be an algebraic integer and let $\alpha_1, \ldots, \alpha_n$ be all the conjugates of α. Deduce that for every $l \in \mathbb{N}$ the polynomial $(X - \alpha_1^l) \cdots (X - \alpha_n^l)$ is in $\mathbb{Z}[X]$.

Solution $\operatorname{minpoly}_\alpha(X) = (X - \alpha_1) \cdots (X - \alpha_n) = X^n - E_1(\alpha_1, \ldots, \alpha_n)X^{n-1} + E_2(\alpha_1, \ldots, \alpha_n)X^{n-2} - \cdots + (-1)^n E_n(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}[X]$ and so $E_r(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ for all $r = 1, \ldots, n$. Now each coefficient of $(X - \alpha_1^l) \cdots (X - \alpha_n^l)$ is a symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ and hence can be expressed as a polynomial with integer coefficients in the elementary symmetric polynomials $E_r(\alpha_1, \ldots, \alpha_n)$, $r = 1, \ldots, n$. •

(c) Let $\gcd(l, n) = 1$ in Part (b). Prove or disprove: $[\mathbb{Q}(\alpha^l) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Solution This is not necessarily true. For example, take α to be a primitive cube root of unity, so that $n = 2$. If $l = 3$, then $\alpha^3 = 1$ and so $[\mathbb{Q}(\alpha^3) : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1$, whereas $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. On the other hand, if $l = 5$, then $\alpha^l = \alpha^2$ is a conjugate of α and so $[\mathbb{Q}(\alpha^l) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. •

---

2. Let D_1 and D_2 be two distinct square-free integers $\neq 0, 1$, $\alpha_1 := \sqrt{D_1}$, $\alpha_2 := \sqrt{D_2}$, $\alpha := \alpha_1 + \alpha_2$ and $K := \mathbb{Q}(\alpha)$.

(a) Prove that $K = \mathbb{Q}(\alpha_1, \alpha_2)$ and that $[K : \mathbb{Q}] = 4$.

Solution Clearly $K \subseteq \mathbb{Q}(\alpha_1, \alpha_2)$. For the converse inclusion it suffices to show that $\alpha_1, \alpha_2 \in K$. Simple calculations show that $\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{pmatrix} = T \begin{pmatrix} 1 \\ \alpha_1 \\ \alpha_2 \\ \alpha_1\alpha_2 \end{pmatrix}$, where $T := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ D_1 + D_2 & 0 & 0 & 2 \\ 0 & D_1 + 3D_2 & 3D_1 + D_2 & 0 \end{pmatrix}$.

Since $\det T = -2^2(D_1 - D_2) \neq 0$, T is invertible, i.e., α_1 and α_2 can be expressed as $\mathbb{Q}$-linear combinations of $1, \alpha, \alpha^2, \alpha^3$. Explicitly one has:

$$\begin{aligned}
\alpha_1 &= \left(\frac{3D_1 + D_2}{2(D_1 - D_2)}\right)\alpha - \left(\frac{1}{2(D_1 - D_2)}\right)\alpha^3, \\
\alpha_2 &= -\left(\frac{D_1 + 3D_2}{2(D_1 - D_2)}\right)\alpha + \left(\frac{1}{2(D_1 - D_2)}\right)\alpha^3.
\end{aligned}$$

Thus $\alpha_1, \alpha_2 \in \mathbb{Q}(\alpha) = K$.

For the proof of the second statement consider the tower of extensions $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq K = \mathbb{Q}(\alpha_1)(\alpha_2)$. Now $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2$ and so it is enough to show that $[K : \mathbb{Q}(\alpha)] = 2$. Since $\text{minpoly}_{\alpha_2, \mathbb{Q}}(X) = X^2 - D_2$ is of degree 2, it is clear that $[K : \mathbb{Q}(\alpha_1)]$ is either 1 or 2. If it is 1, then $\alpha_2 \in \mathbb{Q}(\alpha_1)$, i.e., $\alpha_2 = a + b\alpha_1$ for some $a, b \in \mathbb{Q}$. Squaring gives $D_2 - a^2 - b^2 D_1 = 2ab\sqrt{D_1}$. Since $\sqrt{D_1}$ is irrational, we must have $a = 0$ or $b = 0$. If $b = 0$, then $\alpha_2 = a$ is a rational. So $a = 0$, i.e., $\alpha_2 = b\alpha_1$, i.e., $D_2 = b^2 D_1$. Since D_1 and D_2 are square-free, this implies that $b = 1$. But then $D_2 = D_1$, a contradiction. •

(b) Express the discriminants $\Delta(1, \alpha, \alpha^2, \alpha^3)$ and $\Delta(1, \alpha_1, \alpha_2, \alpha_1\alpha_2)$ in terms of D_1 and D_2.

Solution It is easy to verify that $\text{minpoly}_{\alpha, \mathbb{Q}}(X) = X^4 - 2(D_1 + D_2)X^2 + (D_1 - D_2)^2$ and that the conjugates of α are $\beta_1 := \alpha_1 + \alpha_2, \beta_2 := \alpha_1 - \alpha_2, \beta_3 := -\alpha_1 + \alpha_2, \beta_4 := -\alpha_1 - \alpha_2$. Also $\text{Tr}(\alpha) = \text{Tr}(\alpha_1) = \text{Tr}(\alpha_2) = \text{Tr}(\alpha_1\alpha_2) = 0$, where Tr means $\text{Tr}_{K|\mathbb{Q}}$. (Look at the minimal polynomials of these elements.) Therefore, we have:

$$\begin{aligned}
\Delta(1, \alpha, \alpha^2, \alpha^3) &= \prod_{\substack{i,j=1 \\ i<j}}^{d} (\beta_j - \beta_i)^2 \\
&= (-2\alpha_2)^2(-2\alpha_1)^2(-2(\alpha_1 + \alpha_2))^2(-2(\alpha_1 - \alpha_2))^2(-2\alpha_1)^2(-2\alpha_2)^2 \\
&= 2^{12}\alpha_1^4\alpha_2^4(\alpha_1^2 - \alpha_2^2)^2 \\
&= 2^{12}D_1^2D_2^2(D_1 - D_2)^2, \quad \text{and}
\end{aligned}$$

$$\begin{aligned}
\Delta(1, \alpha_1, \alpha_2, \alpha_1\alpha_2) &= \det\begin{pmatrix} \text{Tr}(1) & \text{Tr}(\alpha_1) & \text{Tr}(\alpha_2) & \text{Tr}(\alpha_1\alpha_2) \\ \text{Tr}(\alpha_1) & \text{Tr}(\alpha_1^2) & \text{Tr}(\alpha_1\alpha_2) & \text{Tr}(\alpha_1^2\alpha_2) \\ \text{Tr}(\alpha_2) & \text{Tr}(\alpha_1\alpha_2) & \text{Tr}(\alpha_2^2) & \text{Tr}(\alpha_1\alpha_2^2) \\ \text{Tr}(\alpha_1\alpha_2) & \text{Tr}(\alpha_1^2\alpha_2) & \text{Tr}(\alpha_1\alpha_2^2) & \text{Tr}(\alpha_1^2\alpha_2^2) \end{pmatrix} \\
&= \det\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4D_1 & 0 & 0 \\ 0 & 0 & 4D_2 & 0 \\ 0 & 0 & 0 & 4D_1D_2 \end{pmatrix} \\
&= 2^8 D_1^2 D_2^2.
\end{aligned}$$

Alternatively one can use the formula:

$$\Delta(1, \alpha, \alpha^2, \alpha^3) = (\det T)^2 \Delta(1, \alpha_1, \alpha_2, \alpha_1\alpha_2) = 2^4(D_1 - D_2)^2 \Delta(1, \alpha_1, \alpha_2, \alpha_1\alpha_2),$$

where T is the matrix introduced in Part (a). •

(c) Conclude that $\mathfrak{O}_K \neq \mathbb{Z}[\alpha]$.

Solution An integral basis $\mathcal{B}$ of K is a $\mathbb{Q}$-basis of K consisting of elements of $\mathfrak{O}_K$ and having minimal $|\Delta(\mathcal{B})|$. Since $\Delta(1, \alpha_1, \alpha_2, \alpha_1\alpha_2) \neq 0$, $(1, \alpha_1, \alpha_2, \alpha_1\alpha_2)$ is a $\mathbb{Q}$-basis of K. Moreover, $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ are all integers of K. Finally $|\Delta(1, \alpha, \alpha^2, \alpha^3)| > |\Delta(1, \alpha_1, \alpha_2, \alpha_1\alpha_2)|$ and, therefore, $(1, \alpha, \alpha^2, \alpha^3)$ cannot be an integral basis of K. (**Remark:** We have not proved that $(1, \alpha_1, \alpha_2, \alpha_1\alpha_2)$ is an integral basis of K, but that does not matter for this exercise. It is sufficient to note that for any integral basis $\mathcal{B}$ of K we have $|\Delta(\mathcal{B})| \leqslant |\Delta(1, \alpha_1, \alpha_2, \alpha_1\alpha_2)|$ and that all integral bases of K have the same discriminant.) •

3. (a) Show that the polynomial $f(X) := X^3 - X^2 - 2X - 8$ is irreducible in $\mathbb{Z}[X]$ (or in $\mathbb{Q}[X]$).

Solution If $f(X)$ were reducible in $\mathbb{Z}[X]$, it would admit a linear factor and this factor would be of the form $X - a$ for some $a \in \mathbb{Z}$, $a \mid 8$, and we would have $f(a) = 0$. But $f(1) = -10$, $f(-1) = -8$, $f(2) = -8$, $f(-2) = -16$, $f(4) = -32$, $f(-4) = -80$, $f(8) = 424$ and $f(-8) = -568$. Hence f must be irreducible in $\mathbb{Z}[X]$. •

(b) Let α be a root of $f(X)$, $K := \mathbb{Q}(\alpha)$ and $\beta := (\alpha^2 + \alpha)/2$. Show that $\beta^3 - 3\beta^2 - 10\beta - 8 = 0$. In particular, $\beta \in \mathfrak{O}_K$.

Solution Substituting the value of β gives $\beta^3 - 3\beta^2 - 10\beta - 8 = \frac{1}{8}(\alpha^3 - \alpha^2 - 2\alpha - 8)(\alpha^3 + 4\alpha^2 + 3\alpha + 8)$. •

(c) Compute that $\Delta(1, \alpha, \alpha^2) = -4 \times 503$ and that $\Delta(1, \alpha, \beta) = -503$.

Solution As in Part (a) it is plain to verify that $X^3 - 3X^2 - 10X - 8$ is irreducible in $\mathbb{Z}[X]$. We can, therefore, compute the following trace values:

$$\begin{aligned}
\mathrm{Tr}(1) &= 3 \\
\mathrm{Tr}(\alpha) &= 1 \\
\mathrm{Tr}(\beta) &= 3 \\
\mathrm{Tr}(\alpha^2) &= \mathrm{Tr}(2\beta - \alpha) = 2\,\mathrm{Tr}(\beta) - \mathrm{Tr}(\alpha) = 5 \\
\mathrm{Tr}(\alpha^3) &= \mathrm{Tr}(\alpha^2 + 2\alpha + 8) = \mathrm{Tr}(\alpha^2) + 2\,\mathrm{Tr}(\alpha) + 8\,\mathrm{Tr}(1) = 31 \\
\mathrm{Tr}(\alpha^4) &= \mathrm{Tr}(\alpha^3 + 2\alpha^2 + 8\alpha) = \mathrm{Tr}(\alpha^3) + 2\,\mathrm{Tr}(\alpha^2) + 8\,\mathrm{Tr}(\alpha) = 49
\end{aligned}$$

Therefore,

$$\Delta(1, \alpha, \alpha^2) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix} = \det \begin{pmatrix} 3 & 1 & 5 \\ 1 & 5 & 31 \\ 5 & 31 & 49 \end{pmatrix} = -4 \times 503.$$

Also $\begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}$, so that

$$\Delta(1, \alpha, \beta) = \left(\det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \right)^2 \Delta(1, \alpha, \alpha^2) = \frac{1}{4} \times \Delta(1, \alpha, \alpha^2) = -503.$$ •

(d) Conclude that $(1, \alpha, \beta)$ is an integral basis of K.

Solution $\Delta(1, \alpha, \beta)$ is non-zero and square-free. (503 is a prime.) •

(e) Prove that $\Delta(1, \gamma, \gamma^2)$ is even for any $\gamma \in \mathfrak{O}_K$.

Solution $(1, \alpha, \beta)$ is an integral basis of K. Let us first write the product of the elements of this basis in this basis itself:

$$\begin{aligned}
1 &= 1 \\
\alpha &= \alpha \\
\beta &= \beta \\
\alpha^2 &= -\alpha + 2\beta && \text{since } \beta = (\alpha^2 + \alpha)/2 \\
\alpha\beta &= 4 + 2\beta && \text{since } \alpha\beta = \alpha(\alpha^2 + \alpha)/2 = (\alpha^3 + \alpha^2)/2 = (\alpha^2 + 2\alpha + 8 + \alpha^2)/2 \\
\beta^2 &= 6 + 2\alpha + 3\beta && \text{since } \beta^2 = \tfrac{1}{2}\alpha\beta(\alpha + 1) = (\beta + 2)(\alpha + 1) = (2\beta + 4) + 2\alpha + \beta + 2
\end{aligned}$$

Now let $\gamma := c + a\alpha + b\beta \in \mathfrak{O}_K$, $a, b, c \in \mathbb{Z}$. Then $\gamma^2 = c^2 + 2ac\alpha + 2bc\beta + a^2\alpha^2 + 2ab\alpha\beta + b^2\beta^2$. Substituting the values of α^2, $\alpha\beta$ and β^2 as found above gives $\gamma^2 = (c^2 + 6b^2 + 8ab) + (2ac - a^2 + 2b^2)\alpha + (2a^2 + 2bc + 3b^2 + 4ab)\beta$. Therefore,

$$\Delta(1, \gamma, \gamma^2) = \left(\det \begin{pmatrix} 1 & 0 & 0 \\ c & a & b \\ c^2 + 6b^2 + 8ab & 2ac - a^2 + 2b^2 & 2a^2 + 2bc + 3b^2 + 4ab \end{pmatrix} \right)^2 \Delta(1, \alpha, \beta).$$

Reduction modulo 2 then gives $\Delta(1, \gamma, \gamma^2) \equiv a^2b^2(a + b)^2 \equiv 0 \pmod 2$. •

(f) Conclude that $\mathfrak{O}_K \neq \mathbb{Z}[\gamma]$ for any $\gamma \in \mathfrak{O}_K$.

Solution Suppose that $\mathfrak{O}_K = \mathbb{Z}[\gamma]$ for some $\gamma \in \mathfrak{O}_K$. Then $(1, \gamma, \gamma^2)$ is an integral basis of K and hence $\Delta(1, \gamma, \gamma^2) = \Delta(1, \alpha, \beta)$. But by Part (e) $\Delta(1, \gamma, \gamma^2)$ is even, whereas $\Delta(1, \alpha, \beta) = -503$ is odd, a contradiction. •