Algebraic Number Theory
Solutions to Example Sheet 2

3. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - 2X - 2$. Compute the trace $\mathrm{Tr}_{K/\mathbb{Q}}$ of $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ and hence calculate $\Delta(1, \alpha, \alpha^2)$. Determine $\mathcal{O}_K$ and Δ_K.

Answer:

The polynomial $f(X) = X^3 - 2X - 2$ is irreducible by Eisenstein's criterion at 2. Thus $[K : \mathbb{Q}] = 3$.

Since $[K : \mathbb{Q}] = 3$ we have $\mathrm{Tr}(1) = 3$. Also α has characteristic polynomial $X^3 - 2X - 2$ so $\mathrm{Tr}(\alpha) = 0$ (minus the coefficient of X^2).

The matrix of α^2 in the basis $\{1, \alpha, \alpha^2\}$ is

$$\begin{pmatrix} 0 & 2 & 0 \\ 0 & 2 & 2 \\ 1 & 0 & 2 \end{pmatrix}.$$

Thus $\mathrm{Tr}(\alpha^2) = 2 + 2 = 4$. (There are numerous other ways in which this could be worked out.)

Now $\alpha^3 = 2\alpha + 2$ and $\alpha^4 = 2\alpha^2 + 2\alpha$ so

$$\mathrm{Tr}(\alpha^3) = 6, \qquad \mathrm{Tr}(\alpha^4) = 8.$$

Thus

$$\begin{aligned} \Delta(1, \alpha, \alpha^2) &= \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) \\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4) \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & 0 & 4 \\ 0 & 4 & 6 \\ 4 & 6 & 8 \end{pmatrix} = -76 = -2^2 \times 19. \end{aligned}$$

By Lemma 33 from lectures, if $\{1, \alpha, \alpha^2\}$ is not an integral basis, then there exists a prime p such that $p^2 \mid \Delta(1, \alpha, \alpha^2)$ and $u_0, \ldots, u_2 \in \mathbb{Z}$, not all zero, with $0 \leq u_i < p$ and

$$\frac{u_0 + u_1\alpha + u_2\alpha^2}{p} \in \mathcal{O}_K.$$

The only prime whose square divides $\Delta(1, \alpha, \alpha^2)$ is 2. But $f(X)$ satisfies Eisenstein's criterion at 2, so Proposition 34 from lectures tells us that no such u_0, u_1, u_2 exist for $p = 2$.

Thus $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\Delta_K = \Delta(1, \alpha, \alpha^2) = -76$.

5. Let α be as in Q3. Show carefully that $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt[3]{d})$ for any non-cube d. Thus not all cubic fields are of the form $\mathbb{Q}(\sqrt[3]{d})$.

Hint: Let $\eta = \sqrt[3]{d}$ and suppose $K = \mathbb{Q}(\eta)$. Then $1, \alpha, \alpha^2$ and $1, \eta, \eta^2$ are both $\mathbb{Q}$-bases for K. What do we know about the ratio $\Delta(1, \alpha, \alpha^2)/\Delta(1, \eta, \eta^2)$?

Answer:

Suppose $K = \mathbb{Q}(\eta)$ where $\eta = \sqrt[3]{d}$ for some rational number d that is non-cube. Then K has $\mathbb{Q}$-bases $1, \alpha, \alpha^2$ and $1, \eta, \eta^2$. If $C = (c_{i,j})$ is the change of basis matrix ($c_{i,j} \in \mathbb{Q}$) then

$$\Delta(1, \eta, \eta^2) = \det(C)^2 \cdot \Delta(1, \alpha, \alpha^2) = -76 \cdot c^2,$$

where $c = \det(C) \in \mathbb{Q}^*$. By question 4, $\Delta(1, \eta, \eta^2) = -27d^2$. Thus

$$76/27 = (d/c)^2.$$

As $76/27$ is not the square of a rational number we have a contradiction. Thus $K \neq \mathbb{Q}(\sqrt[3]{d})$.

7. Let p be an odd prime and let $\zeta = \zeta_p = \exp(2\pi i/p)$. Let $K = \mathbb{Q}(\zeta)$ and let $\omega = \zeta - 1$. You may want to make use of question 4 from example sheet 1 while doing this question, and you may assume that $\mathrm{Nm}_{K/\mathbb{Q}}(\omega) = p$.

   (i) Explain why the conjugates of ζ are

   $$\zeta,\ \zeta^2,\ \zeta^3,\ \ldots,\ \zeta^{p-1}.$$

   (ii) Using the determinant of a Vandermonde matrix, show that

   $$\Delta(1, \zeta, \ldots, \zeta^{p-2}) = \prod_{1 \leq i < j \leq p-1} (\zeta^i - \zeta^j)^2 = (-1)^{(p-1)/2} \cdot \prod_{\substack{1 \leq i,j \leq p-1, \\ i \neq j}} (\zeta^i - \zeta^j).$$

   (iii) Prove that

   $$\Delta(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{(p-1)/2} \left(\prod_{i=1}^{p-1} \zeta^j \right)^{p-2} \cdot \left(\prod_{k=1}^{p-1} (\zeta^k - 1) \right)^{p-2}.$$

   There is a typo on the sheet here! The first product has i as the index and j as the exponent.

   Express this in terms of $\mathrm{Nm}_{K/\mathbb{Q}}(\zeta)$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\omega)$ and deduce that

   $$\Delta(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{(p-1)/2}\, p^{p-2}.$$

   (iv) Using the fact that the minimal polynomial of ω is Eisenstein at p, show that $\frac{\omega^{p-1}}{p}$ is an algebraic integer.

   (v) Suppose that

   $$\beta = \frac{u_0 + u_1\omega + \cdots + u_{p-2}\omega^{p-2}}{p}$$

   is an algebraic integer, with $u_i \in \mathbb{Z}$ not all zero and $0 \leq u_i < p$. Let j be the smallest nonnegative integer such that $u_j \neq 0$.

   (a) By considering $\omega^{p-2-j}\beta$, show that $\frac{u_j\omega^{p-2}}{p}$ is an algebraic integer.

   (b) Calculate $\mathrm{Nm}_{K/\mathbb{Q}}(\frac{u_j\omega^{p-2}}{p})$ and obtain a contradiction.

   (vi) Show that $1, \zeta, \ldots, \zeta^{p-2}$ is an integral basis for K.

Answer:

(i) From example sheet 1, the minimal polynomial of ζ is $(X^p-1)/(X-1)$. The roots of $X^p=1$ are the p-th roots of unity: $1,\zeta,\zeta^2,\ldots,\zeta^{p-1}$. Hence the roots of $(X^p-1)/(X-1)$ are $\zeta,\zeta^2,\ldots,\zeta^{p-1}$.

(ii) As a Vandermonde determinant,

$$\Delta(1,\zeta,\ldots,\zeta^{p-2})=\prod_{1\le i<j\le p-1}(\zeta_i-\zeta_j)^2.$$

Up to sign, this is the same as

$$\prod_{1\le i\ne j\le p-1}(\zeta_i-\zeta_j).$$

The number of sign changes is

$$(p-1)+(p-2)+\cdots+1=(p-1)p/2.$$

As p is odd, this has the same parity as $(p-1)/2$. Thus

$$\Delta(1,\zeta,\ldots,\zeta^{p-2})=(-1)^{(p-1)/2}\prod_{1\le i\ne j\le p-1}(\zeta_i-\zeta_j).$$

(iii) We have

$$\Delta(1,\zeta,\ldots,\zeta^{p-2})=(-1)^{(p-1)/2}\prod_{1\le i\ne j\le p-1}\zeta^i(1-\zeta^{j-i}).$$

Each value of ζ^i occurs $p-2$ times (once for each j with $1\le j\le p-1, j\ne i$), and each value $1-\zeta^k$ occurs $p-2$ times (once for each i with $1\le i\le p-1, i+k\ne p$ since $i+k\equiv j \bmod p$ and $j\not\equiv 0 \bmod p$). Thus

$$\Delta(1,\zeta,\ldots,\zeta^{p-2})=(-1)^{(p-1/2}\left(\prod_{i=1}^{p-1}\zeta^i\right)^{p-2}\cdot\left(\prod_{k=1}^{p-1}(1-\zeta^k)\right)^{p-2}.$$

Thanks to (i),

$$\prod_{i=1}^{p-1}\zeta^i=\mathrm{Nm}_{K/\mathbb{Q}}(\zeta)\quad\text{and}\quad\prod_{k=1}^{p-1}(1-\zeta^k)=\mathrm{Nm}_{K/\mathbb{Q}}(\omega).$$

Thus

$$\Delta(1,\ldots,\zeta^{p-2})=(-1)^{(p-1)/2}\,\mathrm{Nm}_{K/\mathbb{Q}}(\zeta)^{p-2}\,\mathrm{Nm}_{K/\mathbb{Q}}(\omega)^{p-2}=(-1)^{(p-1)/2}\,p^{p-2}$$

since $\mathrm{Nm}_{K/\mathbb{Q}}(\zeta)=1$ (from its minimal polynomial) and $\mathrm{Nm}_{K/\mathbb{Q}}(\omega)=p$ (given in the question).

(iv) We have $\omega^{p-1}=-a_{p-2}\omega^{p-2}-\cdots-a_0$. Since p divides $a_{p-2},\ldots,a_0$, ω^{p-1}/p is an algebraic integer.

(v) (a) We have

$$\omega^{p-2-j}\beta=\frac{u_j\omega^{p-2}+u_{j+1}\omega^{p-1}+\cdots+u_{p-2}\omega^{2p-4-j}}{p}.$$

If β is an algebraic integer, then so is ω^{p-2-j}. By (iv),

$$\frac{u_{j+1}\omega^{p-1} + \cdots + u_{p-2}\omega^{2p-4-j}}{p}$$

is an algebraic integer. Thus the difference $u_j\omega^{p-2}/p$ is an algebraic integer.

(b) $\mathrm{Nm}_{K/\mathbb{Q}}(u_j\omega^{p-2}/p) = u_j^{p-1}p^{p-2}/p^{p-1} = u_j^{p-1}p^{-1}$. This is not an integer since $0 < u_j < p$, contradicting the fact that the norm of an algebraic integer is an integer.

(vi) Since p is the only prime which divides $\Delta(1, p, \ldots, \zeta^{p-2})$, if this is not an integral basis then Lemma 33 from lectures says that

$$\frac{u_0 + \cdots + u_{p-2}\zeta^{p-2}}{p}$$

must be an algebraic integer for some $u_i \in \mathbb{Z}$ with $0 \leq u_i \leq p-1$, not all zero. This is impossible by (v).