Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 1

B3.3: Algebraic Number Theory

A

Very nice presentation

27 January, 2021

Question 1

(a) Show that each of the following numbers is algebraic

$$1/2, \sqrt{-5}, \sqrt{17}+\sqrt{19}, e^{2\pi i/7}$$

(b) Assuming that the polynomials you have found are irreducible, what are the (absolute) conjugates of these numbers, and

(c) Calculate their (absolute) traces and norms.

Proof. First we recall the following facts from B3.1 Galois Theory:

- If α is algebraic over $\mathbb{Q}$, the conjugates of α is the roots of the minimal polynomial m_α of α in the splitting field.
- Suppose that the minimal polynomial of α over $\mathbb{Q}$ is

$$m_\alpha(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$$

Then the trace and norm of α are given by

$$\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = -a_{n-1}, \qquad \mathrm{Norm}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = (-1)^n a_0$$

- The conjugates of α have the same trace and norm with α.

(1) Let $\alpha = 1/2$. Since $1/2 \in \mathbb{Q}$, $1/2$ is algebraic over $\mathbb{Q}$ with minimal polynomial $m(x) = x - 1/2$.

The conjugates of $1/2$ are $1/2$ itself. $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}}(1/2) = \mathrm{Norm}_{\mathbb{Q}}^{\mathbb{Q}}(1/2) = 1/2$.

(2) Let $\alpha = \sqrt{-5}$. Then $\alpha^2 + 5 = 0$. Hence $\sqrt{-5}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $m(x) = x^2 + 5$.

The conjugates of $\sqrt{-5}$ are $\sqrt{-5}$ and $-\sqrt{-5}$.

From the minimal polynomial we know that the trace of $\sqrt{-5}$ is 0 and the norm of $\sqrt{-5}$ is 5.

(3) Let $\alpha = \sqrt{17}+\sqrt{19}$.

$$\begin{aligned} \alpha = \sqrt{17}+\sqrt{19} &\implies (\alpha - \sqrt{17})^2 = (\sqrt{19})^2 \\ &\implies \alpha^2 - 2\sqrt{17}\alpha = 2 \\ &\implies (\alpha^2 - 2)^2 = (2\sqrt{17}\alpha)^2 \\ &\implies \alpha^4 - 72\alpha^2 + 4 = 0 \end{aligned}$$

Hence $\sqrt{17}+\sqrt{19}$ is algebraic over $\mathbb{Q}$. It remains to show that $m(x) = x^4 - 72x^2 + 4$ is irreducible over $\mathbb{Q}$. The easiest way is to compute all the roots of m.

$$(x^2-2)^2 = (2\sqrt{17}x)^2 \implies (x^2 - 2\sqrt{17}x - 2)(x^2 + 2\sqrt{17}x - 2) = 0 \implies x^2 - 2\sqrt{17}x - 2 = x^2 + 2\sqrt{17}x - 2 = 0$$

Using the quadratic formula we find that the 4 roots are exactly $\pm\sqrt{17} \pm \sqrt{19}$. This shows that m is irreducible, because it does not have rational linear or quadratic factors. Hence m is the minimal polynomial of α. The conjugates of α are $\pm\sqrt{17} \pm \sqrt{19}$. The trace is 0, and the norm is 4.

(4) Let $\alpha = \mathrm{e}^{2\pi \mathrm{i}/7}$. We know that α is a primitive 7th root of unity in $\mathbb{C}$. Hence it is algebraic over $\mathbb{Q}$ and the minimal polynomial is the 7th cyclotomic polynomial

$$m(x) = \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

The conjugates of α are all primitive 7th roots of unity. Since 7 is a prime, the conjugates of α are $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$.

The trace of α is -1, and the norm of α is 1. □

A

Question 2

(a) Let $K = \mathbb{Q}(\theta)$ where $\theta^2 = d, d \in \mathbb{Z}$ not a square. Describe the embeddings σ_1, σ_2 of K into $\mathbb{C}$. Are the fields $\sigma_1(K)$, $\sigma_2(K)$ different?

(b) Let $K = \mathbb{Q}(\phi)$ where $\phi^3 = d, d \in \mathbb{Z}$ not a cube. Describe the embeddings $\sigma_1, \sigma_2, \sigma_3$ of K into $\mathbb{C}$. Are the fields $\sigma_1(K)$, $\sigma_2(K)$, $\sigma_3(K)$ different?

Proof. Suppose that $\sigma : K \to \mathbb{C}$ is an embedding (i.e. injective ring homomorphism). Then in particular σ fixes the prime subfield $\mathbb{Q}$. When $K = \mathbb{Q}(\theta)$, σ is uniquely determined by $\sigma(\theta)$, which is a conjugate of θ in $\mathbb{C}$.

(a) Since $\theta^2 = d$ and $\theta \notin \mathbb{Q}$, the conjuagte of θ is $\pm\theta$. The embeddings σ_1, σ_2 are given by $\sigma_1(\theta) = \theta$ and $\sigma_2(\theta) = -\theta$. Note that $K \mid \mathbb{Q}$ is a normal extension, because $-\theta \in K = \mathbb{Q}(\theta)$. Hence the embeddings have the same image in $\mathbb{C}$.

B

(b) Since $\phi^3 = d$ and $\phi \notin \mathbb{Q}$, the conjugates of ϕ are ϕ, $\phi\omega$, $\phi\omega^2$, where $\omega := \dfrac{-1+\sqrt{3}\mathrm{i}}{2}$ is a primitive 3rd root of unity in $\mathbb{C}$. The embeddings $\sigma_1, \sigma_2, \sigma_3$ are given by $\sigma_1(\phi) = \phi$, $\sigma_2(\phi) = \phi\omega$, and $\sigma_3(\phi) = \phi\omega^2$. The extension $K \mid \mathbb{Q}$ is not normal, because $K = \mathbb{Q}(\phi) \in \mathbb{R}$ and $\omega \notin \mathbb{R}$. In fact the images $\sigma_1(K)$, $\sigma_2(K)$ and $\sigma_3(K)$ are distinct. □

add more details

Question 3

Let $K = \mathbb{Q}(\alpha), \alpha^3 = m, m$ not a cube. Evaluate $\Delta\left(1, \alpha, \alpha^2\right)^2$ by the formula $\Delta = \det\left(\sigma_i w_j\right)$. Write down the traces of $1, \alpha, \ldots, \alpha^4$ and hence evaluate $\Delta\left(1, \alpha, \alpha^2\right)^2$ by the formula involving traces.

Proof. The conjugates of α are α, $\alpha\omega$, and $\alpha\omega^2$, where ω is a primitive 3rd root of unity in $\mathbb{C}$. Hence

$$\Delta(1, \alpha, \alpha^2) = \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha\omega & \alpha\omega^2 \\ \alpha^2 & \alpha^2\omega^2 & \alpha^2\omega \end{pmatrix} = \det\begin{pmatrix} 3 & 1 & 1 \\ 0 & \alpha\omega & \alpha\omega^2 \\ 0 & \alpha^2\omega^2 & \alpha^2\omega \end{pmatrix} = 3(\alpha^3\omega^2 - \alpha^3\omega) = 3m\omega(\omega - 1)$$

A

And

$$\Delta^2(1, \alpha, \alpha^2) = 9m^2\omega^2(\omega - 1)^2 = -27m^2$$

Alternatively we compute the traces:

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}}^K(1) &= 3 \\ \mathrm{Tr}_{\mathbb{Q}}^K(\alpha) &= \alpha + \alpha\omega + \alpha\omega^2 = 0 \\ \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^2) &= \alpha^2 + \alpha^2\omega^2 + \alpha^2\omega = 0 \\ \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^3) &= 3m \\ \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^4) &= \alpha^4 + \alpha^4\omega + \alpha^4\omega^2 = 0 \end{aligned}$$

By Lemma 2.3,

$$\Delta^2(1, \alpha, \alpha^2) = \det\begin{pmatrix} \mathrm{Tr}_{\mathbb{Q}}^K(1) & \mathrm{Tr}_{\mathbb{Q}}^K(\alpha) & \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^2) \\ \mathrm{Tr}_{\mathbb{Q}}^K(\alpha) & \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^2) & \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^3) \\ \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^2) & \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^3) & \mathrm{Tr}_{\mathbb{Q}}^K(\alpha^4) \end{pmatrix} = \det\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3m \\ 0 & 3m & 0 \end{pmatrix} = -27m^2$$

□

Question 4

Suppose that β is a root of $X^3 + pX + q = 0$, where $X^3 + pX + q$ is an irreducible polynomial in $\mathbb{Z}[X]$. Verify that $1, \beta, \beta^2, \beta^3$ have traces $3, 0, -2p, -3q$, respectively, and compute $\mathrm{Tr}\left(\beta^4\right)$. Deduce that $\Delta\left(1, \beta, \beta^2\right)^2 = -4p^3 - 27q^2$.

Proof. Suppose that $\beta_1 := \beta, \beta_2, \beta_3$ are the roots of $x^3 + px + q$. By Vieta's Theorem we have

$$\beta_1 + \beta_2 + \beta_3 = 0, \qquad \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1 = p, \qquad \beta_1\beta_2\beta_3 = -q$$

Then

$$\begin{aligned}
\operatorname{tr}(1) &= 3 \\
\operatorname{tr}(\beta) &= \beta_1+\beta_2+\beta_3 = 0 \\
\operatorname{tr}(\beta^2) &= \beta_1^2+\beta_2^2+\beta_3^2 = (\beta_1+\beta_2+\beta_3)^2 - 2(\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1) = -2p \\
\operatorname{tr}(\beta^3) &= \operatorname{tr}(-p\beta - q) = -p\operatorname{tr}(\beta) - \operatorname{tr}(q) = -3q \\
\operatorname{tr}(\beta^4) &= \operatorname{tr}(-p\beta^2 - q\beta) = -p\operatorname{tr}(\beta^2) - q\operatorname{tr}(\beta) = 2p^2
\end{aligned}$$

A

By Lemma 2.3,

$$\Delta^2(1,\beta,\beta^2) = \det\begin{pmatrix} \operatorname{tr}(1) & \operatorname{tr}(\beta) & \operatorname{tr}(\beta^2) \\ \operatorname{tr}(\beta) & \operatorname{tr}(\beta^2) & \operatorname{tr}(\beta^3) \\ \operatorname{tr}(\beta^2) & \operatorname{tr}(\beta^3) & \operatorname{tr}(\beta^4) \end{pmatrix} = \det\begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix} = -4p^3 - 27q^2$$

✓ □

Question 5

Suppose that α is a root of a monic irreducible polynomial $f(X) \in \mathbb{Z}[X]$. Prove that if $\deg(f) = n$ and $K = \mathbb{Q}(\alpha)$ then

$$\Delta^2\left(1,\alpha,\ldots,\alpha^{n-1}\right) = (-1)^{n(n-1)/2}\operatorname{Norm}_{K/\mathbb{Q}}\left(f'(\alpha)\right)$$

A

Proof. Let $\alpha_1 := \alpha, \alpha_2, ..., \alpha_n$ be the roots of f. Since $K \mid \mathbb{Q}$ is separable and f is irreducible, the roots are distinct. By Lemma 2.5, we have

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

Since f is monic, we have

$$f(x) = \prod_{i=1}^{n}(x-\alpha_i) \implies f'(x) = \sum_{i=1}^{n}\prod_{j\neq i}(x-\alpha_j) \implies f'(\alpha_k) = \sum_{i=1}^{n}\prod_{j\neq i}(\alpha_k-\alpha_j) = \prod_{j\neq k}(\alpha_k-\alpha_j)$$

Hence

$$\prod_{k=1}^{n} f'(\alpha_k) = \prod_{k=1}^{n}\prod_{j\neq k}(\alpha_k-\alpha_j) = (-1)^{\frac{n(n-1)}{2}}\prod_{k<j}^{n}(\alpha_j-\alpha_k)^2 = (-1)^{\frac{n(n-1)}{2}}\Delta^2(1,\alpha,...,\alpha^{n-1})$$

On the other hand, by the definition of norm,

$$\operatorname{Norm}_{\mathbb{Q}}^{K}(f'(\alpha)) = \prod_{i=1}^{n}\sigma_i(f'(\alpha)) = \prod_{i=1}^{n} f'(\sigma_i(\alpha)) = \prod_{i=1}^{n} f'(\alpha_i)$$

where f' commutes with the field embeddings $\sigma_i : \alpha \mapsto \alpha_i$ because f' is a polynomial. Now we can combine the results and obtain

$$\Delta^2(1,\alpha,...,\alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}}\operatorname{Norm}_{\mathbb{Q}}^{K}(f'(\alpha))$$

✓ □

Question 6

Suppose that $[K:\mathbb{Q}] = n$, and that there are r real embeddings and s pairs of complex embeddings of K into $\mathbb{C}$, where $r+2s = n$. Show that if $w = \{w_1,\ldots,w_n\}$ is an integral basis for $\mathcal{O}_K$ then the sign of $\Delta(w)^2$ is $(-1)^s$.

Proof. Let $\tau : z \mapsto \overline{z}$ be the complex conjugation. Then $\tau \in \operatorname{Gal}(\mathbb{C} \mid \mathbb{Q})$. Consider the determinant $\Delta(w_1,...,w_n) = \det(\sigma_i(w_j))_{i,j=1}^{n}$, where $\sigma_1,...,\sigma_n$ are the embeddings of K into $\mathbb{C}$, and the action of τ on it. Since the determinant is a polynomial in the elements $\sigma_i(w_j)$, we have

$$\tau\left(\Delta(w_1,...,w_n)\right) = \det(\tau\circ\sigma_i(w_j))_{i,j=1}^{n}$$

A

The action of τ on each individual $\sigma_i(w_j)$ is equivalent to exchanging the σ_i with its conjugate embedding. Therefore the action of τ on the determinant is exchanging $2s$ of n rows. We have

$$\tau\left(\Delta(w_1,...,w_n)\right) = (-1)^s\Delta(w_1,...,w_n)$$

In particular, if s is even, then $\Delta(w_1,...,w_n) \in \mathbb{R}$ and hence $\Delta^2(w_1,...,w_n) \geqslant 0$; if s is odd, then $\Delta(w_1,...,w_n) \in \mathbb{R}\mathrm{i}$ and hence

$\Delta^2(w_1,...,w_n) \leqslant 0$. We conclude that $\Delta^2(w_1,...,w_n)$ has the sign $(-1)^s$. □

Question 7. Stickelberger's Theorem

With the notation of the preceding question, let M be a splitting field containing K. Write Ω for the matrix $\left(\sigma_i\left(w_j\right)\right)$, and write P for the sum of the terms in the expansion of $\det(\Omega)$ that occur with positive sign, and N for the sum of the terms which occur with negative sign; so $\Delta(w) = P - N$ and $P + N$ is the "permanent". Show that $P + N$ and PN are both invariant by $\mathrm{Gal}(M/\mathbb{Q})$, so are both rational integers. Deduce that $\Delta(K)^2 \equiv 0, 1 \bmod 4$.

Proof. (*I suppose that the question means that M is the Galois closure of $K \mid \mathbb{Q}$.*)

The expansion of the determinant is given by:

$$\Delta(w_1,...,w_n) = \sum_{\rho\in S_n} \mathrm{sgn}(\rho) \prod_{i=1}^{n} \sigma_{\rho(i)}(w_i) = \sum_{\rho\in A_n} \prod_{i=1}^{n} \sigma_{\rho(i)}(w_i) - \sum_{\rho\in S_n\setminus A_n} \prod_{i=1}^{n} \sigma_{\rho(i)}(w_i)$$

For a field embedding $\sigma_i : K \hookrightarrow \mathbb{C}$, by normality of the extension $M \mid \mathbb{Q}$, we have $\sigma_i(K) \subseteq M$. Let $\gamma \in \mathrm{Gal}(M \mid \mathbb{Q})$. Then $\gamma \circ \sigma_i$ is also an embedding $K \hookrightarrow \mathbb{C}$. In particular, $\mathrm{Gal}(M \mid \mathbb{Q})$ acts on the set of embeddings $\{\sigma_1,...,\sigma_n\}$ by permutation. Here we identify $\mathrm{Gal}(M \mid \mathbb{Q})$ as a subgroup of S_n.

If $\gamma \in A_n$, then

$$\gamma(P) = \sum_{\rho\in A_n} \prod_{i=1}^{n} \gamma\circ\sigma_{\rho(i)}(w_i) = \sum_{\rho\in A_n} \prod_{i=1}^{n} \sigma_{\gamma\circ\rho(i)}(w_i) = \sum_{\rho\in A_n} \prod_{i=1}^{n} \sigma_{\rho(i)}(w_i) = P$$

$$\gamma(N) = \sum_{\rho\in S_n\setminus A_n} \prod_{i=1}^{n} \gamma\circ\sigma_{\rho(i)}(w_i) = \sum_{\rho\in S_n\setminus A_n} \prod_{i=1}^{n} \sigma_{\gamma\circ\rho(i)}(w_i) = \sum_{\rho\in S_n\setminus A_n} \prod_{i=1}^{n} \sigma_{\rho(i)}(w_i) = N$$

If $\gamma \in S_n \setminus A_n$, then

A

$$\gamma(P) = \sum_{\rho\in A_n} \prod_{i=1}^{n} \gamma\circ\sigma_{\rho(i)}(w_i) = \sum_{\rho\in A_n} \prod_{i=1}^{n} \sigma_{\gamma\circ\rho(i)}(w_i) = \sum_{\rho\in S_n\setminus A_n} \prod_{i=1}^{n} \sigma_{\rho(i)}(w_i) = N$$

$$\gamma(N) = \sum_{\rho\in S_n\setminus A_n} \prod_{i=1}^{n} \gamma\circ\sigma_{\rho(i)}(w_i) = \sum_{\rho\in S_n\setminus A_n} \prod_{i=1}^{n} \sigma_{\gamma\circ\rho(i)}(w_i) = \sum_{\rho\in A_n} \prod_{i=1}^{n} \sigma_{\rho(i)}(w_i) = P$$

Hence for $\gamma \in \mathrm{Gal}(M \mid \mathbb{Q})$,

$$\gamma(P+N) = P+N, \qquad \gamma(PN) = PN$$

Hence $P + N, PN \in \mathbb{Q}$. Furthermore, since $\sigma_i(w_j) \in \mathcal{O}_K$, we have $P + N, PN \in \mathcal{O}_K$. Since $\mathbb{Z}$ is integrally closed, we have $P + N, PN \in \mathbb{Z}$.

Finally,

$$\Delta^2(K) = \Delta^2(w_1,...,w_n) = (P-N)^2 = (P+N)^2 - 4PN \equiv (P+N)^2 \equiv 0, 1 \bmod 4$$

because every square in $\mathbb{Z}$ is $0, 1 \bmod 4$. □