Nepal Algebra Project 2018

Tribhuvan University

Module 3 — Problem Set 2 (MW)

1. Let $t \in \mathbb{Z}$. Consider the polynomial $f(X) = X^4 - tX^3 - 6X^2 + tX + 1$.

(a) Let α be a root of f in a splitting field over $\mathbb{Q}$. Check that $\frac{\alpha-1}{\alpha+1}$ is also a root of f in the field $E = \mathbb{Q}(\alpha)$.

(b) What is the order of the matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ in the group $\mathrm{GL}_2(\mathbb{Q})$ of regular 2×2 matrices with coefficients in $\mathbb{Q}$?

(c) Find the two other roots of f in E.

(d) Check that the polynomial f is reducible over $\mathbb{Q}$ if and only if t is either 0, or 3, or -3.

For each of the three values $t = 0$, $t = 3$ and $t = -3$, write the four roots of f. What is the group $\mathrm{Aut}(E/\mathbb{Q})$? What is the Galois group of f over $\mathbb{Q}$ as a subgroup of the symmetric group $\mathfrak{S}_4$? Is-it transitive?

(e) Assume $t \notin \{0, 3, -3\}$. What is the group $\mathrm{Aut}(E/\mathbb{Q})$? What is the Galois group of f over $\mathbb{Q}$ as a subgroup of the symmetric group $\mathfrak{S}_4$? Is-it transitive?

Which are the subfields of E? For each of them give the irreducible polynomial of an element γ such that this subfield if $\mathbb{Q}(\gamma)$. Is $\mathbb{Q}(\gamma)$ a Galois extension of $\mathbb{Q}$? If so, what is its Galois group?

2. Let $m \in \mathbb{Z}$.

(a) Check that the polynomial $X^4 - m$ is reducible over $\mathbb{Q}$ if and only if either m is a square in $\mathbb{Z}$ or $m = -4k^4$ with $k \in \mathbb{Z}$.

When the polynomial $X^4 - m$ is reducible over $\mathbb{Q}$, what is its splitting field over $\mathbb{Q}$? What is its Galois group over $\mathbb{Q}$ as a subgroup of the symmetric group $\mathfrak{S}_4$? Is-it transitive?

(b) Assume $m > 0$ is not a square in $\mathbb{Z}$. Let E be the splitting field over $\mathbb{Q}$ of $X^4 - m$.
Check that E is also the splitting field over $\mathbb{Q}$ of $X^4 + 4m$.
`Hint:` compute the irreducible polynomials of $(1+i)\sqrt[4]{m}$ and $(1-i)\sqrt[4]{m}$.
What are the Galois group over $\mathbb{Q}$ of the polynomials $X^4 - m$ and $X^4 + 4m$ as subgroups of the symmetric group $\mathfrak{S}_4$? Are they transitive?
Give the list of subfields of E. For each of them, give an element γ such that this field is $\mathbb{Q}(\gamma)$. Give the Galois groups of E over $\mathbb{Q}(\gamma)$, and also of $\mathbb{Q}(\gamma)$ over $\mathbb{Q}$ when this extension is Galois.

3. Let F be a field and f an irreducible separable monic polynomial of degree 3 with coefficients in F. Let E be a splitting field of f over F, let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f in E and let G_f be the Galois group of f over F. Set

$$\delta = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2).$$

(a) For a permutation $\sigma \in \mathfrak{S}_3$, set

$$\delta_\sigma = (\alpha_{\sigma(2)} - \alpha_{\sigma(1)})(\alpha_{\sigma(3)} - \alpha_{\sigma(1)})(\alpha_{\sigma(3)} - \alpha_{\sigma(2)}).$$

Check

$$\delta_\sigma = \begin{cases} -\delta & \text{if } \sigma \text{ is a transposition } (1,2),\ (1,3),\ (2,3), \\ \delta & \text{if } \sigma \text{ belongs to the cyclic subgroup } C_3 = \{1, (1,2,3), (1,3,2)\} \text{ of } \mathfrak{S}_3. \end{cases}$$

(b) Deduce that $\Delta = \delta^2$ belongs to F.

(c) Check that G_f contains a transposition if and only if Δ is not a square in F.

(d) Deduce that G_f is
• the cyclic group C_3 of order 3 if Δ is a square in F,
• the symmetric group $\mathfrak{S}_3$ of order 6 if Δ is not a square in F.

4.

(a) For each of the prime numbers $p = 3, 5, 7, 11, 13, 17$, is the regular polygon with p sides constructible or not?
(b) Using

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1,$$

check that the Fermat number $F_5 = 2^{2^5} + 1$ is divisible by 641.
`Hint.` What is the inverse of 5^4 in the field $\mathbb{F}_{641}$?