Nepal Algebra Project 2018

Tribhuvan University

Module 3 — Problem Set 1 (MW)

1.

(a) Let $t \in \mathbb{Z}$. Check that the polynomial $f(X) = X^3 - tX^2 - (t+3)X - 1$ is irreducible in $\mathbb{Z}[X]$.
(b) Let α be a root of f in a splitting field over $\mathbb{Q}$. Check that $\frac{-\alpha-1}{\alpha}$ is also a root of f in the field $E = \mathbb{Q}(\alpha)$.
(c) What is the order of the matrix $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ in the group $\mathrm{GL}_2(\mathbb{Q})$ of regular 2×2 matrices with coefficients in $\mathbb{Q}$?
(d) Find the third root of f in E.
(e) What is the group $\mathrm{Aut}(E/\mathbb{Q})$?

2. Let F be a finite field. Let p be the characteristic of F and $q = p^r$ the number of elements in F.
(a) Check

$$X^q - X = \prod_{\alpha \in F} (X - \alpha).$$

Deduce that F is a splitting field of $X^q - X$ over the prime field $\mathbb{F}_p$.
(b) Show that there exists an element α in F such that $F = \mathbb{F}_p(\alpha)$.
`Hint.` Recall that any finite subgroup of the multiplicative group of a field is cyclic.
(c) Let $g \in \mathbb{F}_p[X]$ and let γ be a root of g in F. Check that γ^p is also a root of g. Deduce that for any $j \geq 0$, γ^{p^j} is a root of g in F.
(d) Let α be a generator of the cyclic group $F^\times$ and let f be its irreducible polynomial over $\mathbb{F}_p$. Check

$$f(X) = \prod_{j=0}^{r-1} (X - \alpha^{p^j}).$$

(e) Deduce that F is a Galois extension of $\mathbb{F}_p$, with a cyclic Galois group of order r, generated by the Frobenius $x \mapsto x^p$.
(f) Give the list of the subfields of F; for each of them, give its Galois group over $\mathbb{F}_p$. .

3. Let E be the splitting field of the polynomial $X^4 - 2$ over $\mathbb{Q}$.
(a) Compute the irreducible polynomials over $\mathbb{Q}$ of

$$i + \sqrt{2}, \quad (1+i)\sqrt[4]{2}, \quad (1-i)\sqrt[4]{2}.$$

What is the degree of E over $\mathbb{Q}$? Show that E is also be the splitting field of the polynomial $X^4 + 8$ over $\mathbb{Q}$.
(b) Show that the Galois group of E over $\mathbb{Q}$ can be written

$$\{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

with σ of order 4 and τ or order 2 and $\tau\sigma = \sigma^3\tau$.
(c) Check that G has
• One subgroup of order 1,
• 5 subgroups of order 2, generated respectively by σ^2, τ, $\sigma\tau$, $\sigma^2\tau$, $\sigma^3\tau$,
• 3 subgroup of order 4, one of them is cyclic generated by σ (or by σ^3), the two others are $\{1, \sigma^2, \sigma\tau, \sigma^2\tau\}$, and $\{1, \sigma^2, \tau, \sigma^3\tau\}$,
• One subgroup of order 8
and no other subgroup.
(d) Deduce the list of all subfields of E. For each of them, find an element γ such that this field is $\mathbb{Q}(\gamma)$. Is $\mathbb{Q}(\gamma)$ a Galois extension of $\mathbb{Q}$? If so, what is its Galois group?
(e) Let β_1 and β_2 be two roots of $X^4 - 2$ in E. Which one is the field $\mathbb{Q}(\beta_1, \beta_2)$?