Nepal Algebra Project 2018

Tribhuvan University

Module 3 — Problem Set 1 (MW) - Solutions

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 $\mathrm{Aut}(E/\mathbb{Q})$?

Solution.

(a) For a monic polynomial, irreducibility over $\mathbb{Z}$ or over $\mathbb{Q}$ is the same. To check that a polynomial of degree 3 is irreducible over a field amounts to check that it has no root in this field. Since f is monic with constant coefficient 1, we just need to check that $f(1)$ and $f(-1)$ are not 0, which is true.

(b) Set $\beta = \frac{-\alpha-1}{\alpha}$. We have $\alpha = \frac{-1}{\beta+1}$. The equation

$$\alpha^3 - t\alpha^2 - (t+3)\alpha - 1 = 0$$

yields

$$-1 - t(\beta+1) + (t+3)(\beta+1)^2 - (\beta+1)^3 = 0,$$

from which we deduce

$$\beta^3 - t\beta^2 - (t+3)\beta - 1 = 0.$$

(c) Set $M = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$. We have $M^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ and $M^3 = I$ (the identity matrix). Hence M has order 3 in the group $\mathrm{GL}_2(\mathbb{Q})$ of regular 2×2 matrices with coefficients in $\mathbb{Q}$.

(d) The fractional linear transformation $z \mapsto \frac{-z-1}{z}$ is associated with the matrix M, the third root is associated with M^2, hence it is $\frac{-1}{\alpha+1}$.

(e) The field E is a Galois extension of $\mathbb{Q}$ of degree 3 with Galois group $\mathrm{Aut}(E/\mathbb{Q})$ the cyclic group of order 3.

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 $\mathbb{F}_p$. .

Solution.

(a) Since the multiplicative group $F^\times$ of F has $q-1$ elements, any nonzero element x in F satisfies $x^{q-1}=1$, hence any element x in F satisfies $x^q=x$. The polynomial X^q-X has q simple roots in F, hence F is the set of roots of this polynomial. The field F is generated by the roots of X^q-X, hence it is the splitting field over $\mathbb{F}_q$ of this polynomial.

(b) Let α be a generator of the cyclic group $F^\times$. Then

$$F=\{0,1,\alpha,\alpha^2,\ldots,\alpha^{q-2}\}$$

and therefore $F=\mathbb{F}_p[\alpha]=\mathbb{F}_p(\alpha)$. As a consequence α has degree $r=[F:\mathbb{F}_p]$ over $\mathbb{F}_p$.

(c) Applying the Frobenius $\Phi_p: x\mapsto x^p$, we deduce

$$0=\Phi_p(0)=\Phi_p(g(\gamma))=g(\Phi_p(\gamma))=g(\gamma^p),$$

hence $g(\gamma^p)=0$. Now γ^p is root of g, hence $(\gamma^p)^p=\gamma^{p^2}$ also, and by induction we deduce that for any $j\geq 0$, γ^{p^j} is a roof of g.

(e) Since α has multiplicative order $q-1$, the r conjugates $\alpha,\alpha^p,\ldots,\alpha^{p^{r-1}}$ are distinct. Since α has degree r over $\mathbb{F}_p$, these are all the conjugates. Hence

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

(f) Since $F=\mathbb{F}_p[\alpha]$, an automorphism of F (which is an $\mathbb{F}_p$ automorphism since $\mathbb{F}_p$ is the prime field) is determined by its value at α, which is a conjugate of α. Hence there are at most r automorphisms. From (e) it follows that $I,\Phi_p,\Phi_p^2,\ldots,\Phi_p^{r-1}$ are distinct elements in $\mathrm{Aut}(F)=\mathrm{Gal}(F/\mathbb{F}_p)$, therefore $\mathrm{Gal}(F/\mathbb{F}_p)=\{I,\Phi_p,\Phi_p^2,\ldots,\Phi_p^{r-1}\}$.

(g) By the fundamental theorem of Galois Theory there is a one to one correspondence between the subfields of F and the subgroups of $\mathrm{Gal}(F/\mathbb{F}_p)$. For each divisor d of r, the cyclic group $\mathrm{Gal}(F/\mathbb{F}_p)$ of order r has a unique subgroup H_d of order d, and this subgroup is cyclic. The fixed field F^{H_d} of F is an extension of $\mathbb{F}_p$ of degree r/d, hence is a field with $p^{r/d}$ elements.

Replacing d by r/d, it means that for each d dividing r, the field F contains a unique subfield with p^d elements which is Galois over $\mathbb{F}_p$ with cyclic Galois group of order d.

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 of 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 $\mathbb{Q}(\beta_1,\beta_2)$?

Solution.

(a) Write $\alpha=\sqrt[4]{2}$ for the real 4–th root of 2. Hence $\alpha^2=\sqrt{2}$. Since X^4-2 is irreducible over $\mathbb{Q}$ (there are several proofs of this easy fact) the degree of the stem field $\mathbb{Q}(\alpha)$ of X^4-2 over $\mathbb{Q}$ is 4. Since X^4-2 has non real roots, $\mathbb{Q}(\alpha)$ is not a splitting field of X^4-2 over $\mathbb{Q}$. The four roots of X^4-2 are α, $i\alpha$, $-\alpha$ and $-i\alpha$. Hence a splitting field of X^4-2 over $\mathbb{Q}$ is $E=\mathbb{Q}(\alpha,i)$, which is therefore a Galois extension of $\mathbb{Q}$ of degree 8.

The irreducible polynomial over $\mathbb{Q}$ of $i+\sqrt{2}$ is X^4-2X^2+9.

The polynomial X^4+8 is irreducible over $\mathbb{Q}$, its roots are in E, they are $(1+i)\sqrt[4]{2}$, $(1-i)\sqrt[4]{2}$, $(-1+i)\sqrt[4]{2}$, $(-1-i)\sqrt[4]{2}$. It follows that the splitting field of this polynomial is E.

(b) Let $G = \mathrm{Gal}(E/\mathbb{Q})$. The extension $E/\mathbb{Q}(i)$ has degree 4, therefore the polynomial $X^4 - 2$ is irreducible over $\mathbb{Q}(i)$, hence there exists an automorphism σ of E which maps α to $i\alpha$ and i to i. Let τ be the complex conjugation, which maps α to α and i to $-i$. One deduces

$$\mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$$

with $\sigma^4 = \tau^2 = 1$ and $\sigma\tau = \tau\sigma^3$. The images of $\alpha = \sqrt[4]{2}$, i, $\alpha^2 = \sqrt{2}$, $i\alpha^2 = i\sqrt{2}$, $(1+i)\sqrt[4]{2}$, $(1-i)\sqrt[4]{2}$ are given by the following table.

	$\sqrt[4]{2}$	i	$\sqrt{2}$	$i\sqrt{2}$	$(1+i)\sqrt[4]{2}$	$(1-i)\sqrt[4]{2}$
1	$\sqrt[4]{2}$	i	$\sqrt{2}$	$i\sqrt{2}$	$(1+i)\sqrt[4]{2}$	$(1-i)\sqrt[4]{2}$
σ	$i\sqrt[4]{2}$	i	$-\sqrt{2}$	$-i\sqrt{2}$	$(-1+i)\sqrt[4]{2}$	$(1+i)\sqrt[4]{2}$
σ^2	$-\sqrt[4]{2}$	i	$\sqrt{2}$	$i\sqrt{2}$	$(-1-i)\sqrt[4]{2}$	$(-1+i)\sqrt[4]{2}$
σ^3	$-i\sqrt[4]{2}$	i	$-\sqrt{2}$	$-i\sqrt{2}$	$(1-i)\sqrt[4]{2}$	$(-1-i)\sqrt[4]{2}$
τ	$\sqrt[4]{2}$	$-i$	$\sqrt{2}$	$-i\sqrt{2}$	$(1-i)\sqrt[4]{2}$	$(1+i)\sqrt[4]{2}$
$\tau\sigma$	$-i\sqrt[4]{2}$	$-i$	$-\sqrt{2}$	$i\sqrt{2}$	$(-1-i)\sqrt[4]{2}$	$(1-i)\sqrt[4]{2}$
$\tau\sigma^2$	$-\sqrt[4]{2}$	$-i$	$\sqrt{2}$	$-i\sqrt{2}$	$(-1+i)\sqrt[4]{2}$	$(-1-i)\sqrt[4]{2}$
$\tau\sigma^3$	$i\sqrt[4]{2}$	$-i$	$-\sqrt{2}$	$i\sqrt{2}$	$(1+i)\sqrt[4]{2}$	$(-1+i)\sqrt[4]{2}$

We can also represent the group G as a subgroup of the permutation group $\mathfrak{S}_4$ on four symbols $\{1,2,3,4\}$ (the group of symmetries of the square), by numbering the roots of $X^4 - 2$ as

$$\alpha_1 = \alpha, \quad \alpha_2 = i\alpha, \quad \alpha_3 = -\alpha \quad \text{and} \quad \alpha_4 = -i\alpha,$$

in which case $\sigma = (1,2,3,4)$ and $\tau = (2,4)$. This enables ones to check easily

$$\sigma^2 = (1,3)(2,4), \quad \sigma^3 = (1,4,3,2), \quad \tau\sigma = \sigma^3\tau = (1,4)(2,3), \quad \sigma^2\tau = \tau\sigma^2 = (1,3), \quad \tau\sigma^3 = \sigma\tau = (1,2)(3,4).$$

(c) The elements σ and $\sigma^3 = \sigma^{-1}$ have order 4, the elements σ^2, τ, $\tau\sigma$, $\tau\sigma^2$, $\tau\sigma^3$ have order 2. The element σ^2 commutes with all elements: the subgroup $\{1, \sigma^2\}$ is the *center* of G. The elements $\sigma^2, \tau, \tau\sigma^2$ have order 2 and commute, the elements $\sigma^2, \tau\sigma, \tau\sigma^3$ also have order 2 and commute. Hence there are 5 subgroups of order 2,

$$H_0 = \{1, \sigma^2\}, \quad H_1 = \{1, \tau\}, \quad H_2 = \{1, \tau\sigma\}, \quad H_3 = \{1, \tau\sigma^2\}, \quad H_4 = \{1, \tau\sigma^3\},$$

one cyclic subgroup of order 4, namely $N_0 = \{1, \sigma, \sigma^2, \sigma^3\}$, and two noncyclic subgroups of order 4 (products of two cyclic groups of order 4), which are

$$N_1 = \{1, \sigma^2, \tau, \tau\sigma^2\} \quad \text{and} \quad N_2 = \{1, \sigma^2, \tau\sigma, \tau\sigma^3\}.$$

(d) The fixed fields by the cyclic subgroups of order 2 generated respectively by

$$\sigma^2 \qquad \tau \qquad \tau\sigma \qquad \tau\sigma^2 \qquad \tau\sigma^3$$

are the following extensions of $\mathbb{Q}$ of degree 4 (quartic extensions):

$$E^{H_0} = \mathbb{Q}(i, \sqrt{2}), \qquad E^{H_1} = \mathbb{Q}(\sqrt[4]{2}), \qquad E^{H_2} = \mathbb{Q}((1-i)\sqrt[4]{2}), \qquad E^{H_3} = \mathbb{Q}(i\sqrt[4]{2}), \qquad E^{H_4} = \mathbb{Q}((1+i)\sqrt[4]{2}).$$

The only quartic extension of $\mathbb{Q}$ contained in E which is Galois over $\mathbb{Q}$ is $E^{H_0} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$, which is the splitting field over $\mathbb{Q}$ of $X^4 + 1$, namely the field of 8-th roots of unity: the four roots of $X^4 + 1$ are

$$(1+i)\frac{\sqrt{2}}{2}, \quad (1-i)\frac{\sqrt{2}}{2}, \quad (-1+i)\frac{\sqrt{2}}{2}, \quad (-1-i)\frac{\sqrt{2}}{2},$$

which are the 4 primitive 8–th roots of unity (the 4 elements of order 8). The Galois group over $\mathbb{Q}$ of $\mathbb{Q}(i, \sqrt{2})$ is non cyclic of order 4, product of two cyclic groups of order 2.

The fixed field E^{N_0} of the subgroup N_0 of G is $\mathbb{Q}(i)$, the fixed field E^{N_1} of the subgroup N_1 of G is $\mathbb{Q}(\sqrt{2})$, the fixed field E^{N_2} of the subgroup N_2 of G is $\mathbb{Q}(i\sqrt{2})$. The subgroups of order 4 have index 2 hence are normal: the quadratic extensions $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i\sqrt{2})$ are cyclic over $\mathbb{Q}$.

The extensions E/E^{H_i} for $i = 0,1,2,3,4$ are quadratic, the Galois group of E/E^{H_i} is H_i, cyclic of order 2. The extensions E/E^{N_i} for $i = 0,1,2$, are quartic, the Galois group of E/E^{N_i} is N_i, of order 4, with N_0 cyclic and N_1, N_2 products of two cyclic groups. .

(e) If we choose $\beta_1 = \alpha$ and $\beta_2 = -\alpha$, then $\mathbb{Q}(\beta_1, \beta_2) = \mathbb{Q}(\alpha)$, a non Galois quartic extension of $\mathbb{Q}$. If we choose $\beta_1 = \alpha$ and $\beta_2 = i\alpha$ then $\mathbb{Q}(\beta_1, \beta_2) = \mathbb{Q}(\alpha, i)$, a Galois extension of $\mathbb{Q}$ of degree 8. Hence the answer depends on the choice of β_1 and β_2 (cf Milne, p.30, line -10).