Nepal Algebra Project 2018

Tribhuvan University

Module 3 — Problem Set 2 (MW) Solutions

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?

Solution.

(a) Set $\alpha_1 = \alpha$ and $\alpha_2 = \frac{\alpha-1}{\alpha+1}$. We have $\alpha = \frac{\alpha_2+1}{-\alpha_2+1}$. The equation

$$\alpha^4 - t\alpha^3 - 6\alpha^2 + t\alpha + 1 = 0$$

yields

$$(\alpha_2+1)^4 - t(\alpha_2+1)^3(-\alpha_2+1) - 6(\alpha_2+1)^2(-\alpha_2+1)^2 + t(\alpha_2+1)(-\alpha_2+1)^3 + (-\alpha_2+1)^4 = 0$$

from which we deduce

$$\alpha_2^4 - t\alpha_2^3 - 6\alpha_2^2 + t\alpha_2 + 1 = 0.$$

(b) Set $M = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$, which is a matrix with determinant 1. We have $M^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $M^3 = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ and $M^4 = I$ (the identity matrix). Hence M has order 4 in the group $\mathrm{GL}_2(\mathbb{Q})$ of regular 2×2 matrices with coefficients in $\mathbb{Q}$.

(c) The two other roots of f are given by the fractional linear transformations associated with the matrices M^2 and M^3, hence the other roots are $\alpha_3 = \frac{-1}{\alpha}$ and $\alpha_4 = \frac{-\alpha-1}{\alpha-1}$.

(d) Assume f is reducible. Since it has no rational root, it is a product of two quadratic forms. The constant terms have product 1, hence they are equal (and either 1 or -1). Write

$$X^4 - tX^3 - 6X^2 + tX + 1 = (X^2 + aX + c)(X^2 + bX + c)$$

with $c = \pm 1$. By identification we get

$$a + b = -t, \quad ab + 2c = -6, \quad c(a + b) = t.$$

• In the case $t = 0$ we deduce $b = -a$, $2c - a^2 = -6$, hence $c = -1$, $a = \pm 2$, which yields

$$X^4 - 6X^2 + 1 = (X^2 - 2X - 1)(X^2 + 2X - 1).$$

The field E is $\mathbb{Q}(\sqrt{2})$, a quadratic extension of $\mathbb{Q}$ with Galois group the cyclic group or order 2, the four roots are

$$\alpha_1 = 1 + \sqrt{2}, \quad \alpha_2 = -1 + \sqrt{2}, \quad \alpha_3 = -1 - \sqrt{2}, \quad \alpha_4 = 1 - \sqrt{2}.$$

We have $X^2 - 2X - 1 = (X - \alpha_1)(X - \alpha_4)$ and $X^2 + 2X - 1 = (X - \alpha_2)(X - \alpha_3)$. Hence the Galois group of f over $\mathbb{Q}$ is

$$G_f = \{1, (1, 4), (2, 3), (1, 4)(2, 3)\}.$$

It is not transitive.

Assume $t \neq 0$. The equations $a+b=t$ and $c(a+b)=t$ yield $c=-1$. Now $ab=-4$ and a,b are the roots of the polynomial X^2+tX-4. Hence t^2+16 is a square, which is true only for $t^2=9$, $t=\pm 3$.

• For $t=3$ we have
$$X^4-3X^3-6X^2+3X+1=(X^2+X-1)(X^2-4X-1),$$
the field E is $\mathbb{Q}(\sqrt{5})$, a quadratic extension of $\mathbb{Q}$ with Galois group the cyclic group or order 2, the four roots are
$$\alpha_1=\frac{-1+\sqrt{5}}{2},\quad \alpha_2=2-\sqrt{5},\quad \alpha_3=\frac{-1-\sqrt{5}}{2},\quad \alpha_4=2+\sqrt{5}.$$
We have $X^2+X-1=(X-\alpha_1)(X-\alpha_3)$ and $X^2-4X-1=(X-\alpha_2)(X-\alpha_4)$. Hence the Galois group of f over $\mathbb{Q}$ is
$$G_f=\{1,(1,3),(2,4),(1,3)(2,4)\}.$$
It is not transitive.

• For $t=-3$ we have
$$X^4+3X^3-6X^2-3X+1=(X^2-X-1)(X^2+4X-1),$$
the field E is $\mathbb{Q}(\sqrt{5})$, a quadratic extension of $\mathbb{Q}$ with Galois group the cyclic group or order 2, the four roots are
$$\alpha_1=\frac{1+\sqrt{5}}{2},\quad \alpha_2=-2+\sqrt{5},\quad \alpha_3=\frac{1-\sqrt{5}}{2},\quad \alpha_4=-2-\sqrt{5}.$$
We have $X^2-X-1=(X-\alpha_1)(X-\alpha_3)$ and $X^2+4X-1=(X-\alpha_2)(X-\alpha_4)$. Hence the Galois group of f over $\mathbb{Q}$ is
$$G_f=\{1,(1,3),(2,4),(1,3)(2,4)\}.$$
It is not transitive.

(e) Assume $t \notin \{0,3,-3\}$, the polynomial f is irreducible, the field E is an extension of $\mathbb{Q}$ of degree 4, the Galois group $G=\mathrm{Gal}(E/\mathbb{Q})$ is cyclic of order 4. Hence it has 3 subgroups, namely $\{1\}$, G, and a cyclic subgroup of order 2: this is the subgroup of G generated by σ^2. An element of K which is fixed by σ^2 is $\gamma=\alpha+\frac{1}{\alpha}$, the irreducible polynomial of which is
$$X^2-tX-4.$$
(Write $\gamma^2+a\gamma+c=0$, replace γ in terms of α and identify). The Galois group of f over $\mathbb{Q}$ is the cyclic subgroup
$$G_f=\{1,\sigma,\sigma^2,\sigma^3\}$$
of $\mathfrak{S}_4$ with $\sigma=(1,2,3,4)$. It is transitive.

There are three subfields of E, namely $\mathbb{Q}$, E and $\mathbb{Q}(\gamma)$, associated irreducible polynomials are X, f and X^2-tX-4 respectively (these are not unique!).

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.

Solution.

Recall that an integer is a square in $\mathbb{Z}$ if and only if it is a square in $\mathbb{Q}$.

(a) If $m=k^2$, then
$$X^4-m=(X^2-k)(X^2+k)$$
is reducible over $\mathbb{Q}$. If $m=-4k^4$, then
$$X^4-m=(X^2+2k^2)^2-4k^2X^2=(X^2+2kX+2k^2)(X^2-2kX+2k^2)$$

is reducible over $\mathbb{Q}$.

Conversely, assume $X^4 - m$ is a product of two quadratic forms

$$X^4 - m = (X^2 + aX + b)(X^2 + cX + d).$$

Then

$$a + c = 0, \quad ac + b + d = 0, \quad ad + bc = 0, \quad bd = -m.$$

We consider two cases.
(1) Assume $a = 0$. Then $c = 0$, $b + d = 0$, $b^2 = m$. Hence m is a square.
(2) Assume $a \neq 0$. Then $c = -a$, $d = b$, $a^2 = 2b$, hence a is even, $a = 2k$, and then $b = 2k^2$, $m = -b^2 = -4k^2$.

When m is a fourth power in $\mathbb{Q}$ (or in $\mathbb{Z}$, it is the same), $m = k^4$, then $X^4 - m$ has two rational roots, $\alpha_1 = k$ and $\alpha_2 = -k$, and two complex roots $\alpha_3 = ik$ and $\alpha_4 = -ik$. The splitting field is $\mathbb{Q}(i)$. The Galois group of $X^4 - m$ over $\mathbb{Q}$ is the cyclic subgroup $\{1, (3,4)\}$ of $\mathfrak{S}_4$ of order 2. It is not transitive.

When m is a square, $m = k^2$, $k > 0$, but not a fourth power (k is not a square), then $X^4 - m$ splits over $\mathbb{Q}$ as a product of two irreducible factors of degree 2, namely $(X^2 - k)(X^2 + k)$, the splitting field is $E = \mathbb{Q}(\sqrt{k}, i)$, an extension of $\mathbb{Q}$ of degree 4; write $\alpha_1 = \sqrt{k}$, $\alpha_2 = -\sqrt{k}$, $\alpha_3 = i\sqrt{k}$, $\alpha_4 = -i\sqrt{k}$. Then the Galois group G_f of f over $\mathbb{Q}$ is the abelian non cyclic group of order 4

$$G_f = \{1, (1,2), (3,4), (1,2)(3,4)\}$$

which is not transitive.

(b) The situation is similar to exercise 3 of the problem set 1 which was dealing with the special case $m = 2$. The splitting field of the polynomial $X^4 - 2$ over $\mathbb{Q}$ is also the splitting field of the polynomial $X^4 + 2$ over $\mathbb{Q}$, namely $\mathbb{Q}(i, \sqrt[4]{2})$. This field contains the primitive 8–th roots of unity, namely the roots $(\pm 1 \pm i)\sqrt{2}$ of $X^4 + 1$ (the splitting field of $X^4 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt{2})$). However, when $m \neq 2k^4$ and $m \neq 8k^4$, the splitting field of the polynomial $X^4 - m$ over $\mathbb{Q}$ does not contain the primitive 8–th roots of unity.

Let $\alpha = \sqrt[4]{m}$. Since E is a quartic extension of $\mathbb{Q}(i)$, there is an element σ in the Galois group G of E over $\mathbb{Q}$ such that $\sigma(\alpha) = i\alpha$ and $\sigma(i) = i$. Let τ be the complex conjugation which maps α to α and i to $-i$. As elements of $\mathfrak{S}_4$, writing

$$\alpha_1 = \alpha, \quad \alpha_2 = i\alpha, \quad \alpha_3 = -\alpha, \quad \alpha_4 = -i\alpha$$

for the four roots of $X^4 - m$, we have $\sigma = (1,2,3,4)$ and $\tau = (2,4)$. The Galois group of $X^4 - m$ over $\mathbb{Q}$ is

$$G_f = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\} \subset \mathfrak{S}_4,$$

with $\sigma^4 = \tau^2 = 1$ and $\sigma\tau = \tau\sigma^{-1}$. It is transitive ($X^4 - m$ is irreducible over $\mathbb{Q}$).

Since m is not a square in $\mathbb{Z}$, $-4m$ is not of the form $-4k^4$, hence $X^4 + 4m$ is irreducible (according to (a)). The roots of $X^4 + 4m$ are $\beta_1 = (1+i)\sqrt[4]{m}$, $\beta_2 = (1-i)\sqrt[4]{m}$, $\beta_3 = (-1+i)\sqrt[4]{m}$ and $\beta_4 = (-1-i)\sqrt[4]{m}$. Hence the splitting field of $X^4 + 4m$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{m}, i)$, which is E. We have $\sigma(\beta_1) = \beta_3$, $\sigma(\beta_3) = \beta_4$, $\sigma(\beta_4) = \beta_2$, $\tau(\beta_1) = \beta_2$, $\tau(\beta_3) = \beta_4$, hence the Galois group of $X^4 + 4m$ over $\mathbb{Q}$ is the subgroup of $\mathfrak{S}_4$ of order 8 generated by σ and τ with

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

It is transitive ($X^4 + 4m$ is irreducible over $\mathbb{Q}$)..

The 10 subgroups of G are: $\{1\}$,

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

$$N_0 = \{1, \sigma, \sigma^2, \sigma^3\}, \quad N_1 = \{1, \sigma^2, \tau, \tau\sigma^2\} \quad N_2 = \{1, \sigma^2, \tau\sigma, \tau\sigma^3\}$$

and G. Their fixed fields are $E^{\{1\}} = E$,

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

$$E^{N_0} = \mathbb{Q}(i), \quad E^{N_1} = \mathbb{Q}(\sqrt{m}), \quad E^{N_2} = \mathbb{Q}(i\sqrt{m})$$

and $E^G = \mathbb{Q}$. The Galois groups over $\mathbb{Q}$ of these fields are $\mathrm{Gal}(E^{\{1\}}/\mathbb{Q}) = G$,

$$\mathrm{Gal}(E^{H_0}/\mathbb{Q}) = G/H_0$$

which is a non cyclic group of order 4

$$\mathrm{Gal}(E^{N_0}/\mathbb{Q}) = G/N_0, \quad \mathrm{Gal}(E^{N_1}/\mathbb{Q}) = G/N_1, \quad \mathrm{Gal}(E^{N_2}/\mathbb{Q}) = G/N_2$$

which are cyclic groups of order 2, and $\mathrm{Gal}(E^G/\mathbb{Q}) = \{1\}$. The extensions E^{H_1}, E^{H_2}, E^{H_3} and E^{H_4} of $\mathbb{Q}$ are not Galois.

The Galois groups of E over these fields are : $\mathrm{Gal}(E/E^{\{1\}}) = \{1\}$,

$$\mathrm{Gal}(E/E^{H_0}) = H_0, \qquad \mathrm{Gal}(E/E^{H_1}) = H_1, \qquad \mathrm{Gal}(E/E^{H_2}) = H_2, \qquad \mathrm{Gal}(E/E^{H_3}) = H_3, \qquad \mathrm{Gal}(E/E^{H_4}) = H_4,$$

which are cyclic groups or order 2,

$$\mathrm{Gal}(E/E^{N_0}) = N_0,$$

which a cyclic group of order 4,

$$\mathrm{Gal}(E/E^{N_1}) = N_1, \quad \mathrm{Gal}(E/E^{N_2}) = N_2$$

which are abelian non cyclic groups of order 4, and $\mathrm{Gal}(E/E^G) = G$.

`Remark.` One checks on these examples that the Galois group over F of a polynomial $f \in F[X]$ is transitive if and only f is irreducible.

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.

Solution.
(a) is trivial.
(b) From $\sigma(\Delta) = \sigma(\delta)^2 = \delta^2 = \Delta$ for all $\sigma \in G_f$ it follows that Δ belongs to the fixed field of $\mathrm{Gal}(E/F)$ which is F.
(c) If $\delta \in F$, then by Galois Theory $\sigma(\delta) = \delta$ for all $\sigma \in G_f$ hence G_f contains no transposition.
If $\delta \notin F$, then by Galois Theory there exists $\sigma \in G_f$ such that $\sigma(\delta) \neq \delta$ hence G_f contains a transposition.
(d) The order of the group G_f is a multiple of 3 since E contains $F(\alpha_1)$ which has degree 3 over F. Hence G_f contains the subgroup C_3 which is the only subgroup of $\mathfrak{S}_3$ of order 3.

The only subgroup of $\mathfrak{S}_3$ which contains no transposition and is $\neq (1)$ is the cyclic group $C_3 = \{1, (1,2,3), (1,3,2)\}$ of order 3. Hence if G_f contains no transposition then $G_f = C_3$.

If G_f contains a transposition, then since G_f also contains C_3 we have $G_f = \mathfrak{S}_3$.

`Remark`. Write $f(X) = X^3 + aX^2 + bX + c$. The relation

$$X^3 + aX^2 + bX + c = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

is equivalent to

$$\alpha_1 + \alpha_2 + \alpha_3 = -a, \quad \alpha_1\alpha_2 + \alpha_3\alpha_1 + \alpha_3\alpha_2 = b, \quad \alpha_1\alpha_2\alpha_3 = -c.$$

By expanding the formula

$$\Delta = (\alpha_2 - \alpha_1)^2(\alpha_3 - \alpha_1)^2(\alpha_3 - \alpha_2)^2$$

one can deduce that the discriminant is

$$\Delta = a^2b^2 + 18abc - 4b^3 - 4ac^3 - 27c^2.$$

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 $\mathbb{F}_{641}$?

Solution. (a) The answer is yes for $p = 3$, 5 and 17 which are Fermat primes of the form $F_n = 2^{2^n} + 1$:

$$3 = F_0, \quad 5 = F_1, \quad 17 = F_2,$$

but not for 7, 11, 13, since for these primes p the number $p - 1$ is not a power of 2.
(b) We have $5 \cdot 2^7 \equiv -1 \mod 641$, hence $5^4 \cdot 2^{28} \equiv 1 \mod 641$. Therefore the inverse of 5^4 in the field $\mathbb{F}_{641}$ is 2^{28}. Since $5^4 \equiv -2^4 \mod 641$, we deduce

$$2^{32} \equiv -1 \mod 641.$$