NAP 2019 - MODULE V - Problem Set 2 - Solutions

Due Tuesday July 30, 2019, at 24:00 Kathmandu time

Exercise 1

Show that if the Galois group of a rational cubic polynomial $f(x)$ is cyclic of order 3 then $f(x)$ has only real roots.

Solution

Since $f(x)$ has degree 3, it has at least one real root α (in fact every complex non-real root must be paired with its complex conjugate). Let $K = \mathbb{Q}(\alpha)$. Then $[K : \mathbb{Q}] = 3$ coincides to the order of the Galois group of $f(X)$, so that K must be a splitting field for f. But $K \subseteq \mathbb{R}$, so that all roots of $f(x)$ are real.

Exercise 2

Let f be an irreducible cubic polynomial over a finite field of characteristic different from $2, 3$. Show that its discriminant is a square.

Solution

For a cubic irreducible polynomial in $K[X]$ with discriminant Δ and Galois group G, we know that

a) if Δ is a square in K then $G \simeq A_3$;
b) if Δ is not a square in K then $G \simeq S_3$.

But we also know that the Galois group of a finite extension finite fields is cyclic. Since S_3 is not cyclic, it follows that only case a) is possible.

Exercise 3

Let K be a subfield of $\mathbb{C}$. Let $f(x) = x^3 + px + q$ be an irreducible polynomial in $K[x]$. Let α be a root of $f(x)$. Let $\beta = a + b\alpha + c\alpha^2 \in K(\alpha) \setminus K$, with $a, b, c \in K$. Determine the minimal polynomial $g(X)$ of β over K. Let Δ be the discriminant of $f(X)$ over K. Show that $K(\alpha)/K$ is an extension by radicals if and only if -3Δ is a square in K.

Solution

If $\beta \in K(\alpha)\setminus K$ then $K(\beta) = K(\alpha)$, so that $1, \beta, \beta^2$ is a basis of $K(\alpha)$ as a K-vector space. The change of basis matrix transforming coordinates w.r.t. the basis $1, \beta, \beta^2$ in coordinates w.r.t. the basis $1, \alpha, \alpha^2$ is given by

$$M = \begin{pmatrix} 1 & a & -2bcq + a^2 \\ 0 & b & -2bcp - c^2q + 2ab \\ 0 & c & -c^2p + 2ac + b^2 \end{pmatrix}$$

The inverse matrix is

$$M^{-1} = \frac{1}{bc^2p + c^3q + b^3} \begin{pmatrix} 1 & ac^2p - 2bc^2q - a^2c - ab^2 & -2abcp - ac^2q + 2b^2cq + a^2b \\ 0 & -c^2p + 2ac + b^2 & 2bcp + c^2q - 2ab \\ 0 & -c & b \end{pmatrix}.$$

The coordinates of β^3 in the basis $1, \alpha, \alpha^2$ are given by the vector

$$T = \begin{pmatrix} 3bc^2pq + c^3q^2 - 6abcq - b^3q + a^3 \\ 3bc^2p^2 + 2c^3pq - 6abcp - 3ac^2q - b^3p - 3b^2cq + 3a^2b \\ +c^3p^2 - 3ac^2p - 3b^2cp - 3bc^2q + 3a^2c + 3ab^2. \end{pmatrix}$$

Then $M^{-1} \cdot T$ gives the coordinates of β^3 in the basis $1, \beta, \beta^2$:

$$M^{-1} \cdot T = \begin{pmatrix} ac^2p^2 - bc^2pq + c^3q^2 - 2a^2cp + ab^2p + 3abcq - b^3q + a^3 \\ -c^2p^2 + 4acp - b^2p - 3bcq - 3a^2 \\ -2cp + 3a \end{pmatrix}$$

Then the minimal polynomial of β over K is

$$g(X) = X^3 + (-2cp + 3a)X^2 + (-c^2p^2 + 4acp - b^2p - 3bcq - 3a^2)X + \\ + ac^2p^2 - bc^2pq + c^3q^2 - 2a^2cp + ab^2p + 3abcq - b^3q + a^3.$$

(It is also possible to obtain $g(X)$ as the characteristic polynomial of the multiplication by β.)

It follows that β is a radical if a, b, c satisfy the equations:

$$\begin{cases} -2cp + 3a = 0 \\ c^2p^2 + 4acp - b^2p - 3bcq - 3a^2 = 0 \end{cases}$$

that is

$$\begin{cases} a = \frac{2}{3}pc \\ 3pb^2 + 9qb - p^2 = 0 \end{cases}$$

The second equation has discriminant $81p^2 + 12p^3 = -3\Delta$; therefore the above system admits a solution if and only if -3Δ is a square in K.

Exercise 4

Solve Exercise 14.5 in Garling's book.

Solution

From $3\beta^2 - 3\alpha\beta - p = 0$ we find $\alpha = \beta - \frac{p}{3\beta}$; then from $\alpha^3 + p\alpha + q = 0$ we find $27\beta^6 + 27q\beta^3 - p^3 = 0$; then

$$\beta^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Exercise 5

For each of the following polynomials, check irreducibility and give the Galois group over $\mathbb{Q}$:

a) $X^3 - 4X - 1$;
b) $X^4 + X + 1$;
c) $X^4 + X^3 + X^2 + X + 1$;
d) $X^4 + X^3 - X^2 - 2X - 2$.

Solution

a) The polynomial is irreducible, as ± 1 are not roots. The discriminant is $\Delta = -4(-4)^3 - 27(-1)^2 = 229$, not a square in $\mathbb{Q}$. Thus the Galois group is S_3.
b) The polynomial is irreducible: in fact if it was reducible then by Gauss Lemma it would be a product of two monic polynomials in $\mathbb{Z}[X]$; then it would be reducible in $\mathbb{F}_p[X]$ for every X; but it easy to see that it is irreducible in $\mathbb{F}_2[X]$. The cubic resolvent is $X^3 - 4X - 1$, which was studied at point a): it is irreducible over $\mathbb{Q}$ and the discriminant is 229, not a square in $\mathbb{Q}$. The Galois group is S_4.
c) Put $Y = X - 1$; then the polynomial is

$$\frac{X^5 - 1}{X - 1} = \frac{(Y+1)^5 - 1}{Y} = Y^4 + 5Y^3 + 10Y^2 + 10Y + 5,$$

and the latter is irreducible by Eisenstein's criterion. The discriminant is 125, not a square in $\mathbb{Q}$; and the cubic resolvent is

$$X^3 + \frac{5}{4}X^2 - \frac{45}{16}X - \frac{25}{64} = (X - \frac{5}{4})(X^2 + \frac{5}{2}X + \frac{5}{16}).$$

The splitting field of the cubic resolvent is $M = \mathbb{Q}(\sqrt{5})$, and

$$X^4 + X^3 + X^2 + X + 1 =$$
$$= (X^2 + \frac{1+\sqrt{5}}{2}X + 1)(X^2 + \frac{1-\sqrt{5}}{2}X + 1)$$

is reducible over M. Therefore the Galois group is cyclic of order 4.

d) The polunomial is reducible:

$$X^4 + X^3 - X^2 - 2X - 2 =$$
$$= (X^2 + X + 1)(X^2 - 2)$$

The splitting field over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{-3}, \sqrt{2})$. The Galois group is $\mathbb{Z}_2 \times \mathbb{Z}_2$.