Nepal Algebra Project(NAP)
Central Department of Mathematics
Tribhuvan University,Kirtipur, Kathmandu,Nepal
Fields and Galois Theory

Course Instructor: Prof. Michel Waldschmidt

NAP: Module-4, Problem Set 2 Solution

1. *Galois group of a family of cubic fields.*
(a) Since $f_a(1) = -2a - 3 \neq 0$ and $f_a(-1) = 1 \neq 0$, f is irreducible over $\mathbb{Q}$.
(b) A direct computation gives

$$f\big(\sigma(z)\big) = \frac{-1}{(1+z)^3} f(z).$$

(c) The Galois group of f_a is the group of Möbius transformations (linear fractional transformations) generated by σ, it is a cyclic group of order 3:

$$\sigma^2(z) = -\frac{1+z}{z}, \quad \sigma^3(z) = z.$$

(d) It follows that the discriminant of f_a is a square.

`Remarks.`
1. The polynomial f_a has discriminant $(a^2 + 3a + 9)^2$.
2. There is a similar example in degree 4, with the family of polynomials

$$g_a(X) = X^4 - aX^3 - 6X^2 + aX + 1$$

and the Möbius transformation

$$\sigma(z) = \frac{z-1}{z+1}$$

which generates a cyclic group of order 4:

$$\sigma^2(z) = -\frac{1}{z}, \quad \sigma^3(z) = \frac{1+z}{1-z} = \frac{-1}{\sigma(z)}, \quad \sigma^4(z) = z.$$

One checks that g_a is irreducible and that if α is a root of g_a then $\sigma(\alpha)$ also. Hence the Galois group of g_a over $\mathbb{Q}$ is C_4. Notice that $X^4 g_a(-1/X) = g_a(X)$. This explains that, if α is a root of g_a, then $\sigma^2(\alpha) = -1/\alpha$ also.
3. There is a similar example in degree 6, with the family of polynomials

$$X^6 - 2aX^5 - 5(a+3)X^4 - 20X^3 + 5aX^2 + 2(a+3)X + 1$$

and the cyclic group of order 6 of Möbius transformations

$$\sigma(z) = \frac{z-1}{z+2}, \quad \sigma^2(z) = \frac{-1}{z+1}, \quad \sigma^3(z) = \frac{-z-2}{2z+1}, \quad \sigma^4(z) = \frac{-z-1}{z}, \quad \sigma^5(z) = \frac{-2z-1}{z-1}.$$

2. *Galois group of a polynomial of degree 4.*
(a) The polynomial f is even: $f(-X) = f(X)$, and reciprocal: $X^4 f(1/X) = f(X)$. Hence if α is a root, then $-\alpha$ also, and $1/\alpha$ also. We choose an ordering for the roots, say

$$\alpha_1 = \alpha, \quad \alpha_2 = -\alpha, \quad \alpha_3 = 1/\alpha, \quad \alpha_4 = -1/\alpha.$$

From

$$f(X) = (X^2 - \alpha^2)\left(X^2 - \frac{1}{\alpha^2}\right)$$

we deduce $b = \alpha^2 + 1/\alpha^2$.
(b) The derivative of f is $f'(X) = 2X(2X^2 - b)$. For $z^2 = b/2$ we have $f(z) = 1 - z^2/4$, which vanishes for $z = \pm 2$.

Hence f is separable if and only if $z \neq \pm 2$.
Since $f(1) = f(-1) = b + 2$, the polynomial f has a root in $\mathbb{Q}$ if and only if $b = -2$. If $b = -2$, then $f(X) = (X-1)^2(X+1)^2$ splits completely in $\mathbb{Q}$ and is not separable.
From now on we assume $b \neq -2$. Hence f has no root in $\mathbb{Q}$. Assume f is reducible over $\mathbb{Q}$. Then it is a product of two quadratic factors. Since the decomposition of f over $\mathbb{C}$ is unique, there are three cases:

$$\begin{array}{lllll}
(1) & \text{one factor is} & (X-\alpha)(X+\alpha), & \text{the other is} & \left(X - \dfrac{1}{\alpha}\right)\left(X + \dfrac{1}{\alpha}\right); \\
(2) & \text{one factor is} & (X-\alpha)\left(X - \dfrac{1}{\alpha}\right), & \text{the other is} & (X+\alpha)\left(X + \dfrac{1}{\alpha}\right); \\
(3) & \text{one factor is} & (X-\alpha)\left(X + \dfrac{1}{\alpha}\right), & \text{the other is} & (X+\alpha)\left(X - \dfrac{1}{\alpha}\right).
\end{array}$$

In the first case we have $\alpha^2 \in \mathbb{Z}$. From $b = \alpha^2 + 1/\alpha^2$ we deduce that $1/\alpha^2 \in \mathbb{Z}$, hence $\alpha^2 = 1$ and $b = 2$. In the case $b = 2$ the polynomial splits as $(X^2+1)^2$ and is not separable.
Assume now $b \neq \pm 2$. Hence f is separable.
In the second, case we have

$$X^4 + bX^2 + 1 = (X^2 - cX + 1)(X^2 + cX + 1)$$

with $c \in \mathbb{Z}$, hence $-2 - b = c^2$. The splitting field of f over $\mathbb{Q}$ is a quadratic extension of $\mathbb{Q}$, the Galois group of f over $\mathbb{Q}$ is the cyclic subgroup of order 2 of $\mathfrak{S}_4$ generated by the permutation $(1,3)(2,4)$. It is a non transitive subgroup of $\mathfrak{S}_4$ (since f is reducible).
In the third case, we have

$$X^4 + bX^2 + 1 = (X^2 - cX - 1)(X^2 + cX - 1)$$

with $c \in \mathbb{Z}$, hence $2 - b = c^2$. The splitting field of f over $\mathbb{Q}$ is a quadratic extension of $\mathbb{Q}$, the Galois group of f over $\mathbb{Q}$ is the cyclic subgroup of order 2 of $\mathfrak{S}_4$ generated by the permutation $(1,4)(2,3)$. It is a non transitive subgroup of $\mathfrak{S}_4$ (since f is reducible).
Assume now that $-2 - b$ and $2 - b$ are not square. Then f is irreducible over $\mathbb{Q}$, the Galois group of f over $\mathbb{Q}$ is

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

a transitive subgroup of $\mathfrak{S}_4$ of order 4. It is the abelian non cyclic group of order 4, isomorphic to the product $C_2 \times C_2$ of two cyclic groups of order 2.