Exercise sheet 5

Galois theory

Exercice 1. Show that if a and b are two nonzero elements of a field K of characteristic different than 2, then $K(\sqrt{a})$ is equal to $K(\sqrt{b})$ if and only if b/a is a square in K.

Exercice 2. Let $K = \mathbb{Q}(i + \sqrt{2})$. Show that K is Galois over $\mathbb{Q}$. Compute the degree of K over $\mathbb{Q}$ and the Galois group of $K/\mathbb{Q}$. Give the list of subfields of K.

Exercice 3. Let $L = \mathbb{Q}(\sqrt{5})$ and $M = \mathbb{Q}(\sqrt{2+\sqrt{5}})$. Determine the degrees of the extensions $L/\mathbb{Q}$, $M/\mathbb{Q}$ and M/L. Which of those extensions are Galois ? Give the minimal polynomial of $\sqrt{2+\sqrt{5}}$ over $\mathbb{Q}$ and over L.

Exercice 4. Let a and b be two rational numbers. Give a sufficient condition for the polynomial X^4+aX^2+b to be irreducible over $\mathbb{Q}$. Give a necessary and sufficient condition for a rupture field to be Galois over $\mathbb{Q}$. What happens in the case where b is nonpositive and a^2-4b is nonnegative, but not a rational square ?

Exercice 5. Let $K = \mathbb{Q}(\sqrt[3]{2})$ and L be its Galois closure over $\mathbb{Q}$. Compute the degree of L over $\mathbb{Q}$ and the Galois group of L/K. Give the list of subfields of L.

Exercice 6. Let G be the Galois group of $X^5 - 2$ over $\mathbb{Q}$. What is the cardinality of G ? Is it abelian, solvable ?

Exercice 7. What is the degree of the splitting field of the polynomial $(X^3 - 5)(X^3 - 7)$ over $\mathbb{Q}$?

Exercice 8. Compute the Galois group of $X^6 - 5$ over $\mathbb{Q}$ and over $\mathbb{R}$.

Exercice 9. Find a primitive element of $\mathbb{Q}(\sqrt{3}, \sqrt{7})$.

Exercice 10. Let G be the Galois group of $(X^3 - 5)(X^4 - 2)$ over $\mathbb{Q}$.

(1) Give a presentation of G by generators and relations.

(2) Is G cyclic, dihedral, symmetric ?

Exercice 11. Find a primitive element of the splitting field of $(X^2 - 2)(X^2 - 5)(X^2 - 7)$.

Exercice 12. Let ζ be a primitive 12-nth root of unity. How many extensions are there between $\mathbb{Q}(\zeta^3)$ and $\mathbb{Q}(\zeta)$?

Exercice 13. Let ζ be a primitive 5-nth root of unity.

(1) Describe the Galois group of $K = \mathbb{Q}(\zeta)/\mathbb{Q}$ and show that K a unique degree 2 subfield over $\mathbb{Q}$, namely $\mathbb{Q}(\zeta + \zeta^4)$.

(2) Give the minimal polynomial of $\zeta + \zeta^4$ over $\mathbb{Q}$.

(3) Give the Galois group of $(X^2 - 5)(X^5 - 1)$.

(4) Give the Galois group of $(X^2 + 3)(X^5 - 1)$.

Exercice 14. Let $K = \mathbb{Q}(\sqrt{-15})$, f its non-trivial automorphism and α an element of K such that the polynomial $X^3 - \alpha$ is irreducible over K.

(1) Why does such an α exist ?
We let L denote the splitting field of this polynomial, and $\theta, j\theta, j^2\theta$ its roots in L.

(2) Why are there of this form ?

(3) Show that L is a Galois extension of K of degree 6 and that L contains $\sqrt{5}$.

(4) Show that there exists two K-automorphisms σ and τ of L such that

$$\sigma(\sqrt{5}) = \sqrt{5}, \quad \sigma(\theta) = j\theta, \quad \tau(\sqrt{5}) = -\sqrt{5}, \quad \tau(\theta) = \theta.$$

(5) Determiner the order of the elements σ and τ of the group $\mathrm{Gal}(L/K)$ and compute $\tau\sigma\tau^{-1}$. Give the list of the extensions of K contained in L.

(6) We now suppose that $N_{K/\mathbb{Q}}(\alpha)$ is the cube of a rational number b. Determine the different conjugates of θ over $\mathbb{Q}$. Show that the extension $L/\mathbb{Q}$ is Galois of degree 12. Show that it is possible to extend the automorphism f of K to an automorphism ϕ of L such that $\phi(\sqrt{5}) = \sqrt{5}$ and $\phi(\theta) = b/\theta$. Compute ϕ^2, $\phi\sigma\phi^{-1}$ and $\phi\tau\phi^{-1}$. Show that $\mathbb{Q}(\sqrt{5})$ admits an extension of degree 3 contained in L and Galois over $\mathbb{Q}$.

Exercice 15. By reducing modulo 2 and 3, show that the Galois gropu of $X^5 - X - 1$ is the symmetric group S_5.