Galois Theory: Example Sheet 4
Michaelmas 2025

1. Let $K = \mathbb{Q}(\zeta_n)$ be the cyclotomic field with $\zeta_n = e^{2\pi i/n}$. Show that under the isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, complex conjugation is identified with the residue class of $-1 \pmod n$. Deduce that if $n \geqslant 3$, then $[K : K \cap \mathbb{R}] = 2$ and show that $K \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos 2\pi/n)$. Is this a Galois extension of $\mathbb{Q}$?

2. (i) Find all the subfields of $\mathbb{Q}(\zeta_7)$, expressing them in the form $\mathbb{Q}(\alpha)$.

   (ii) Find the quadratic subfields of $\mathbb{Q}(\zeta_{15})$.

3. (i) Let K be a field, p a prime and $K' = K(\zeta)$ for some primitive p^{th} root of unity ζ. Let $a \in K$. Show that $X^p - a$ is irreducible over K if and only if it is irreducible over K'. Is the result true if p is not assumed to be prime?

   (ii) If K contains a primitive n^{th} root of unity, then we know that $X^n - a$ is reducible over K if and only if a is a d^{th} power in K for some divisor $d > 1$ of n. Show that this need not be true if K doesn't contain a primitive n^{th} root of unity.

4. Let K be a field containing a primitive m^{th} root of unity for some $m > 1$. Let a, $b \in K$ such that the polynomials $f = X^m - a$, $g = X^m - b$ are irreducible. Show that f and g have the same splitting field if and only if $b = c^m a^r$ for some $c \in K$ and $r \in \mathbb{N}$ with $\gcd(r, m) = 1$.

5. Let K be a field of characteristic $p > 0$. Let $a \in K$, and let $f \in K[X]$ be the polynomial $f(X) = X^p - X - a$. Show that $f(X + c) = f(X)$ for every $c \in \mathbb{F}_p \subset K$. Now suppose that f does not have a root in K, and let L/K be a splitting field for f over K. Show that $L = K(\alpha)$ for any $\alpha \in L$ with $f(\alpha) = 0$, and that L/K is Galois, with Galois group cyclic of order p. [L/K is called an *Artin–Schreier extension.*]

6. Let L/K be a finite extension. Use the linear independence of field embeddings to show that L/K is separable if and only if the trace map $\mathrm{Tr}_{L/K} : L \to K$ is surjective. Deduce that the K-bilinear form $L \times L \to K; (x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is nondegenerate if and only if L/K is separable.

7. Let $\alpha = \sqrt{2 + \sqrt{2}}$. By showing that $\alpha = 2\cos(\pi/8)$, prove that $\mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$ with Galois group C_4.

   Hence, or otherwise, show that $\mathbb{Q}(\sqrt{2 + \sqrt{2 + \sqrt{2}}})$ is a Galois extension of $\mathbb{Q}$ and determine its Galois group.

8. Let $p_1, \ldots, p_n$ be distinct primes, and let $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Show that $K/\mathbb{Q}$ is a Galois extension, and that there is an injective group homomorphism $\mathrm{Gal}(K/\mathbb{Q}) \to \mu_2^n$. Then show by induction on n that $[K : \mathbb{Q}] = 2^n$.

   d

9. Let G be a finite group. Show that if G is solvable, then so is every subgroup and quotient of G.

10. Show that for any finite group G there exists a Galois extension whose Galois group is isomorphic to G. [Hint: Use Cayley's theorem.]

11. Let K be any field, and let $L = K(X)$ be the field of rational functions over K. Define mappings $\sigma, \tau : L \to L$ by the formulae

$$(\sigma f)(X) = f\left(1 - \frac{1}{X}\right), \quad (\tau f)(X) = f\left(\frac{1}{X}\right).$$

Show that σ, τ are automorphisms of L, and that they generate a subgroup $G \subset \mathrm{Aut}(L)$ isomorphic to S_3. Show that $L^G = K(h(X))$ where

$$h(X) = \frac{(X^2 - X + 1)^3}{X^2(X-1)^2}.$$

12. Let K be any field, and let $L = K(X)$.

(i) Show that for any $a \in K$ there exists a unique $\sigma_a \in \mathrm{Aut}(L/K)$ such that $\sigma_a(X) = X + a$.

(ii) Let $G = \{\sigma_a \mid a \in K\}$. Show that G is a subgroup of $\mathrm{Aut}(L/K)$, isomorphic to the additive group of K. Show that if K is infinite, then $L^G = K$.

(iii) Assume that K has characteristic $p > 0$, and let $H = \{\sigma_a \mid a \in \mathbb{F}_p\}$. Show that $L^H = K(Y)$ with $Y = X^p - X$. [Use Artin's theorem.]

Further problems

13. Show that $\mathbb{Q}(\zeta_{21})$ has exactly three subfields of degree 6 over $\mathbb{Q}$. Show that one of them is $\mathbb{Q}(\zeta_7)$, one is real, and the other is a cyclic extension $K/\mathbb{Q}(\zeta_3)$. Use a suitable Lagrange resolvent to find $a \in \mathbb{Q}(\zeta_3)$ such that $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$.

14. Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \cong C_p$, generated by σ.

(i) Show that for any $x \in L$, $\mathrm{Tr}_{L/K}(\sigma(x) - x) = 0$. Deduce that if $y \in L$ then $\mathrm{Tr}_{L/K}(y) = 0$ if and only if there exists $x \in L$ with $\sigma(x) - x = y$.

(ii) Suppose that K has characteristic p. By considering $\alpha \in L$ with $\sigma(\alpha) - \alpha = 1$, show that L/K is an extension of the form considered in Question 5.

15. Let p, q be distinct odd primes.

(i) Let L be the splitting field of the polynomial $f(X) = X^q - 1$ over $\mathbb{F}_p$ and let $\phi_p \in \mathrm{Gal}(f/K) \subset S_q$ denote the Frobenius $x \mapsto x^p$. By considering the action of ϕ_p on the roots of f, show that

$$\mathrm{sgn}(\phi_p) = \left(\frac{p}{q}\right)$$

where $\binom{p}{q}$ is the Legendre symbol. [Recall Euler's formula $\binom{a}{p} \equiv a^{\frac{p-1}{2}} \mod p$.]

(ii) Show that $\operatorname{Disc} f = (-1)^{\frac{q-1}{2}} q^q$. Hence deduce that

$$\binom{p}{q} = (-1)^{\frac{(p-1)(q-1)}{4}} \binom{q}{p}.$$

16. (i) Show that if $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ then there exists $\sigma \in \operatorname{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\sigma(\alpha) \neq \alpha$. [This shows that $\overline{\mathbb{Q}}/\mathbb{Q}$ is a Galois extension.]

    (ii) Let K be a field. By considering a suitable subfield of an algebraic closure, or otherwise, prove that there exists a separable extension K^{sep}/K in which every separable polynomial over K splits into linear factors. also that K^{sep}/K is a Galois extension. [K^{sep} is called a *separable closure* of K.]

17. Let K_1 and K_2 be algebraically closed fields of the same characteristic. Show that either K_1 is isomorphic to a subfield of K_2 or K_2 is isomorphic to a subfield of K_1. [Use Zorn's Lemma.]