CIMPA Research School Yogyakarta

Galois Theory Exercises — February 20, 2020

1. Compute the Galois group $\mathrm{Gal}(f)$ for the polynomial $f = X^3 - 2 \in F[X]$ when F is equal to $\mathbf{R}$, $\mathbf{F}_3$, $\mathbf{F}_5$ and $\mathbf{F}_7$. Same question for $f = X^4 - 2$.

2. Show that the cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_7)$ has exactly two non-trivial intermediate fields. For each of them, find the irreducible polynomial of an element that generates the extension over $\mathbf{Q}$.

3. Find all subfields of the cyclotomic field $\mathbf{Q}(\zeta_{15})$, and indicate which subgroups of $(\mathbf{Z}/15\mathbf{Z})^*$ they correspond to.

4. Let p be a prime number and $f \in \mathbf{Q}[X]$ an irreducible polynomial of degree p having exactly $p-2$ real roots.
   a. Show that $\mathrm{Gal}(f)$ contains an element that swaps 2 roots of f, and fixes all other roots.
   b. Show that $\mathrm{Gal}(f)$ contains an element that permutes all the roots of f cyclically.
   c. Prove: $\mathrm{Gal}(f) \cong S_p$.

5. Let $p = 2k + 3$ be a prime number, and define

$$f = (X^2 + 2) \prod_{i=-k}^{k} (X - 2i) + 2 \in \mathbf{Q}[X].$$

   a. Show that f is irreducible of degree p.
   b. Show that its derivative f' does not have $p - 1$ real roots.
   [Hint: f' is *even* and $f'(0)$ has sign $(-1)^k$.]
   c. Show that f has exactly $p - 2$ real roots, and Galois group $\mathrm{Gal}(f) \cong S_p$.

6. Let $f \in K[X]$ be a polynomial of degree n with Galois group S_n. Let $L = K(\alpha)$ be the extension of K obtained through the adjunction of a zero of f, and E an intermediate field of the extension $K \subset L$. Prove: $E = K$ or $E = L$.

7. Let L be a splitting field of the polynomial $f = X^4 + 20 \in \mathbf{Q}[X]$. Determine $\mathrm{Gal}(f)$ and the diagram of intermediate fields of the extension $\mathbf{Q} \subset L$.

8. Do likewise for $f = X^4 - 4X^2 + 5$ and $f = X^4 - 5X^2 - 5$.

9. Let $L = \mathbf{Q}(X)$ be the field of rational functions over $\mathbf{Q}$. Define $\sigma_i \in \mathrm{Aut}(L)$ by

$$\sigma_1(X) = -X, \qquad \sigma_2(X) = 1/X, \qquad \sigma_3(X) = 1 - X.$$

a. Determine the field of invariants $L^{\langle\sigma_i\rangle}$ for $i \in \{1, 2, 3\}$.

a. Show that $\rho = \sigma_2\sigma_3$ has order 3 in $\mathrm{Aut}(L)$, and determine $L^{\langle\rho\rangle}$.

c. Show that $G = \langle\sigma_2, \sigma_3\rangle$ has order 6 and is isomorphic to S_3. Determine $f \in \mathbf{Q}(X)$ with $L^G = \mathbf{Q}(f)$.

10. Let $f = p/q \in \mathbf{Q}(X)$ be the quotient of coprime polynomials $p, q \in \mathbf{Q}[X]$ of degree m and n. Prove: if f is not constant, then $\mathbf{Q}(f) \subset \mathbf{Q}(X)$ is an algebraic extension of degree $\max(m, n)$.

11. Let $K = \mathbf{F}_p(X)$ be the field of rational functions over $\mathbf{F}_p$ and $\sigma \in \mathrm{Aut}(L)$ the automorphism satisfying $\sigma(X) = X + 1$. Show that $G = \langle\sigma\rangle$ is cyclic of order p, and that for $f = X^p - X$, the extension $\mathbf{F}_p(f) \subset \mathbf{F}_p(X)$ is Galois with group G.

12. For $L = \mathbf{Q}(X)$, we define $\sigma \in \mathrm{Aut}(L)$ by $\sigma(X) = X + 1$. Prove that $G = \langle\sigma\rangle$ is an infinite subgroup of $\mathrm{Aut}(L)$, and that $L^G \subset L$ is *not* an algebraic extension. Also show that, in this case, the map $H \mapsto L^H$ from the set of subgroups of G to the set of subfields of L is neither injective nor surjective.