14. Automorphisms of splitting fields – examples

Let L be a field. A ***automorphism*** of L is an isomorphism $\phi : L \to L$. We write $\mathrm{Aut}(L)$ for the group of automorphisms of L. If k is a subfield of L, we write $\mathrm{Aut}(L/k)$ for the group of automorphisms of L which have $\phi(x) = x$ for $x \in k$.

Problem 14.1. Let $L = \mathbb{C}(r_1, r_2, \ldots, r_5)$. Let K be the subfield of S_5 symmetric functions in L, and write $e_1 = r_1 + r_2 + \cdots + r_5$, $e_2 = r_1r_2 + r_1r_3 + \cdots + r_4r_5$, etcetera as usual.

(1) Show that L is a splitting field of $x^5 - e_1x^4 + e_2x^3 - e_3x^2 + e_4x - e_5$ over K.
(2) Show that $\mathrm{Aut}(L/K)$ is isomorphic to S_5.

Problem 14.2. Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = \frac{-1+\sqrt{-3}}{2}$ as usual.

(1) Show that K is a splitting field of $x^3 - 2$ over $\mathbb{Q}$.
(2) Show that $\mathrm{Aut}(K/\mathbb{Q})$ is a subgroup of S_3.

Problem 14.3. Way back on Problem Set 1, we considered the polynomial $x^3 + x^2 - 2x - 1$. Let the roots of this equation in $\mathbb{R}$ be $\alpha_1 \approx -1.80194$, $\alpha_2 \approx 1.24698$ and $\alpha_3 \approx -0.445042$. On that problem set, you hopefully found that $\alpha_2 = \alpha_1^2 - 2$, $\alpha_3 = \alpha_2^2 - 2$ and $\alpha_1 = \alpha_3^2 - 2$. Let $L = \mathbb{Q}(\alpha_1)$.

(1) Show that L is a splitting field of $x^3 + x^2 - 2x - 1$ over $\mathbb{Q}$.
(2) Show that $\mathrm{Aut}(L/\mathbb{Q})$ is a subgroup of A_3.

Problem 14.4. Let ζ be a primitive 5-th root of unity and let $M = \mathbb{Q}(\zeta)$.

(1) Show M is a splitting field of $x^5 - 1$ over $\mathbb{Q}$.
(2) Show that $\mathrm{Aut}(M/\mathbb{Q})$ is a subgroup of the cyclic group with 4 elements.

Problem 14.5. Let K be a field which contains a primitive n-th root of unity ζ, let $a \in K$ and let $L = K(\sqrt[n]{a})$.

(1) Show that L is a splitting field of $x^n - a$ over K.
(2) Show that $\mathrm{Aut}(L/K)$ is a subgroup of $\mathbb{Z}_n$ (with the group operation of addition).
(3) More generally, let a_1, a_2, …, a_r be elements of K and let $L = K(\sqrt[n]{a_1}, \sqrt[n]{a_2}, \ldots, \sqrt[n]{a_r})$. Show that $\mathrm{Aut}(L/K)$ is abelian.

Problem 14.6. Let K be a field and let $L = K(\zeta)$ where ζ is a primitive n-th root of unity.

(1) Show that L is a splitting field of $x^n - 1$ over K.
(2) Show that $\mathrm{Aut}(L/K)$ is a subgroup of U_n (with the group operation of multiplication).

You may be dissatisfied that, in problems 14.2 through 14.6, we have only proved that automorphism groups are subgroups of given groups. In order to do more examples, we will need the following theorem, which we will prove next time:

> **Theorem:** Let F be a field, let $f(x)$ be a nonzero polynomial in $F[x]$ and let L be a splitting field for $f(x)$. Let ρ be any element of L and let $m(x)$ be the minimal polynomial of ρ over F. Then $m(x)$ splits in $L[x]$, and the $\mathrm{Aut}(L/F)$ orbit of ρ is the set of roots of $m(x)$.

Problem 14.7. Assume the Theorem.

(1) Show that the automorphism group in Problem 14.3 is cyclic of order 3. You may assume that $x^3 + x^2 - 2x - 1$ is irreducible over $\mathbb{Q}$.
(2) Show that the automorphism group in Problem 14.4 is cyclic of order 4. You may assume that $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$.
(3) Show that the automorhpism group in Problem 14.2 is S_3. You may assume that $x^2 + x + 1$ and $x^3 - 2$ are irreducible over $\mathbb{Q}$.