Geometric constructions and elements of Galois' theory
List 11. Galois groups of field extensions and of polynomials

Automorphisms of number fields

1. Show that the number $i\sqrt{2}$ is a square root of some rational number, and consider the quadratic extension $Q(i\sqrt{2}) = \{a + bi\sqrt{2} : a, b \in Q\}$ cia/la Q. Verify that the map $\sigma : Q(i\sqrt{2}) \to Q(i\sqrt{2})$ given by the formula $\sigma(a + bi\sqrt{2}) = a - bi\sqrt{2}$ is an automorphism of the field $Q(i\sqrt{2})$.
2. Find all automorohisms of the field $Q(\sqrt[4]{2})$. HINT: first investigate which numbers can appear as images of the number $\sqrt[4]{2}$ through an automorphism of the field $Q(\sqrt[4]{2})$ (there are only 2 potential candidates); then write formulas for all potential automorphisms, in the form $\psi(a+b\sqrt[4]{2}+c\sqrt[4]{4}+d\sqrt[4]{8}) = \ldots$; verify that each of the so obtained formulas indeed describes an automorphism (i.e. verify that $\psi(x + y) = \psi(x) + \psi(y)$ oraz $\psi(x \cdot y) = \psi(x) \cdot \psi(y)$ for any $x, y \in Q(\sqrt[4]{2})$).
3. Justify that the only automorphism of the field $Q(\sqrt[3]{2})$ is the identity, so that the group $\mathrm{Gal}(Q(\sqrt[3]{2})/Q)$ is trivial (consists of one element). HINT: first show that $\sqrt[3]{2}$ is fixed by any automorphism σ of the field $Q(\sqrt[3]{2})$, and then refer to the general form of an element in this field.
4. (a) A complex number $z_0 = a + bi$ is a root of a polynomial f with rational coefficients. Prove that then the conjugate number $\bar{z}_0 = a - bi$ is also the root of this polynomial. HINT: use the fact that $\overline{z + z'} = \bar{z} + \overline{z'}$, $\bar{z}^n = \overline{z^n}$ and that $\bar{a} = a$ for $a \in Q$.
   (b) Prove that for any polynomial $f \in Q[x]$ the complex conjugation $\psi(z) = \bar{z}$ is an automorphism of the splitting field Q_f of the polynomial f.

Galois groups

5. (a) Verify that the splitting field Q_f of the polynomial $f(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$ is the field $Q(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in Q\}$.
   (b) Find and describe all automorphisms of the above field Q_f, i.e. all automorphisms from the Galois group $\mathrm{Gal}(Q_f/Q)$. HINT: first show that for any automorphism $\psi \in \mathrm{Gal}(Q_f/Q)$ we have $\psi(\sqrt{2}) = \pm\sqrt{2}$ and $\psi(\sqrt{3}) = \pm\sqrt{3}$; use this fact in writing formulas for all potential automorphisms, in the form $\psi(a+b\sqrt{2}+c\sqrt{3}+\sqrt{6}) = \ldots$ (4 potential possibilities); check that each of the so obtained formulas indeed yields an automorphism (i.e. verify that $\psi(x + y) = \psi(x) + \psi(y)$ and $\psi(x \cdot y) = \psi(x) \cdot \psi(y)$).
   (c) Enumerate the roots of the polynomial f with numbers $1, 2, 3, 4$ and find the permutations from the group S_4 which correspond to permutations of roots induced by the automorphisms described in part (b).
   (d) Check that the group $\mathrm{Gal}(Q_f/Q)$ is abelian. Check also that this group is (isomorphic to) the Klein four-group. .
6. Let ε_5 be the principal degree 5 root of 1.
   (a) Justify that each number from the field $Q(\varepsilon_5)$ can be expressed uniquely in the form $a + b\varepsilon_5 + c\varepsilon_5^2 + d\varepsilon_5^3 + e\varepsilon_5^4$, where $a, b, c, d, e \in Q$.
   (2) Deduce that the field $Q(\varepsilon_5)$ is the splitting field of the polynomial $x^5 - 1$.

(3) Describe an automorphism σ of the field $Q(\varepsilon_5)$ such that $\sigma(\varepsilon_5) = \varepsilon_5^2$. HINT: calculate $\sigma(\varepsilon_5^k)$ for $k = 0, 1, 2, 3, 4$, then write a general formula forσ, and finally verify that this formula describes an actual automorphism.

(4) Describe the permutration of the roots $1, \varepsilon_5, \varepsilon_5^2, \varepsilon_5^3, \varepsilon_5^4$ of the polynomial $x^5 - 1$ induced by the automorphism σ.

(5) Find all other automorphisms of the field $Q(\varepsilon_5)$ (there are four of them, includind the identical one). Justify that these four automorphisms form the Galois group $\mathrm{Gal}(Q(\varepsilon_5)/Q)$. Describe this group as the group of permutations of the roots of the polynomial $x^5 - 1$, by finding the permutations induced by all these automorphisms.

(6) Check that the group $\mathrm{Gal}(Q(\varepsilon_5)/Q)$ is abelian, and that it is (isomorphic to) the cyclic group Z_4 (sometimes denoted also as C_4).

7. Verify that the splitting field of the polynomial $f(x) = (x^2 - x - 1)(x^2 + x - 1) = x^4 - 3x + 1$ is the field $Q_f = Q(\sqrt{5})$. Show that the Galois group $\mathrm{Gal}(Q_f/Q)$ consists of precisely two automorphisms, and find the permutations from the group S_4 corresponding to the permutations of the roots of f induced by these automorphisms.

8. Show that if a polynomial $W \in Q[x]$ is the product of two essentially distinct (i.e. not proportional) irreducible polynomials U and V, then
   (a) the sets of roots of the polynomials U and V are disjoint, and their union is the set of all roots of the polynomial W;
   (b) Galois group of the polynomial W permutes separately the roots of U and V.

9. [polynomial with non-abelian Galois group.]
   (a) Let ε_3 be the principal degree 3 root of 1, i.e. $\varepsilon_3 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Check that $\varepsilon_3^2 + \varepsilon_3 + 1 = 0$ and deduce that ε_3 is an algebraic number of degree 2.
   (b) Justify that the set of roots of the polynomial $f(x) = x^3 - 2$ consists of the three the numbers $\sqrt[3]{2}$, $\varepsilon_3\sqrt[3]{2}$ and $\varepsilon_3^2\sqrt[3]{2}$.
   (c) Prove that the splitting field Q_f of the polynomial $f = x^3 - 2$ is the field $Q(\sqrt[3]{2}, \varepsilon_3)$, and that the set $1, \sqrt[3]{2}, \sqrt[3]{4}, \varepsilon_3, \varepsilon_3\sqrt[3]{2}, \varepsilon_3\sqrt[3]{4}$ is a basis for the field extension $Q \subset Q_f$.
   (d) Verify that for any automorphism $\psi \in \mathrm{Gal}(Q_f/Q)$ we have $\psi(\varepsilon_3) \in \{\varepsilon_3, \varepsilon_3^2\}$ and $\psi(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \varepsilon_3\sqrt[3]{2}, \varepsilon_3^2\sqrt[3]{2}\}$.
   (e) Show that the complex numbers conjugation is an automorphism of Q_f, and that it induces the transposition of the roots $\varepsilon_3\sqrt[3]{2}$ and $\varepsilon_3^2\sqrt[3]{2}$ (leaving the root $\sqrt[3]{2}$ fixed).
   (f) Check that the assignments $\sqrt[3]{2} \mapsto \varepsilon_3\sqrt[3]{2}$ and $\varepsilon_3 \mapsto \varepsilon_3$ extend to an automorphism of Q_f, and that this automorphism induces z cyclic permutation
   $$\sqrt[3]{2} \to \varepsilon_3\sqrt[3]{2} \to \varepsilon_3^2\sqrt[3]{2} \to \sqrt[3]{2}$$
   of the roots of f.
   (g) Check that the permutations of roots induced by the automorphisms described in parts (f) and (g) do not commute. Deduce thathe group $\mathrm{Gal}(Q_f/Q)$ is non-abelian.
   (h) Prove that the group $\mathrm{Gal}(Q_f/Q)$ induces the full group S_3 as the group of induced permutations of the roots of f.