ALGEBRA 11: Galois theory

Galois extensions

Exercise 11.1 (!). Consider a polynomial $P(t) \in K[t]$ of degree $n$ with coefficients in a field $K$ that has $n$ distinct roots in $K$. Prove that the ring $K[t]/P$ of residues modulo $P$ is isomorphic to the direct sum of $n$ copies of $K$.

Hint. There was a similar problem in ALGEBRA 9.

Definition 11.1. Let $K$ be an algebraic extension of a field $k$ (this fact is often denoted in writing by $[K:k]$). One says that $[K:k]$ is a Galois extension if $K \otimes_k K$ is isomorphic (as an algebra) to a direct sum of several copies of $K$.

Exercise 11.2. Let $P(t) \in k[t]$ be an irreducible polynomial of degree $n$ that has $n$ distinct roots in $K = k[t]/P$. Prove that $[K:k]$ is a Galois extension.

Exercise 11.3. Prove that $[Q[\sqrt{-1}] : Q]$ is a Galois extension.

Exercise 11.4. Let $[k : Q]$ be an extension of degree 2 (i.e. $K$ is two dimensional as a vector space over $Q$). Prove that it is a Galois extension.

Exercise 11.5 (!). Let $p$ be a prime. Prove that for any root of unity $\zeta$ of degree $p$ $[Q[\zeta] : Q]$ is a Galois extension.

Exercise 11.6 (*). Is $[Q[\sqrt{2}] : Q]$ a Galois extension?

Exercise 11.7 (*). Consider $F$, a field of characteristic $p$ and $k = F(z)$, the field of rational functions over $F$. Prove that the polynomial $P(t) = t^p - z$ is irreducible over $k$. Prove that $[k[t]/P : k]$ is not a Galois extension.

Exercise 11.8. Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions. Prove that

$$K_2 \otimes_{K_3} K_1 \cong (K_2 \otimes_{K_3} K_2) \otimes_{K_2} K_1.$$

Exercise 11.9. Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions. Prove that

$$K_1 \otimes_{K_2} (K_2 \otimes_{K_3} K_2) \otimes_{K_2} K_1 \cong K_1 \otimes_{K_3} K_1.$$

Exercise 11.11. Prove that $Q[\sqrt{2}, \sqrt[3]{-1}]$ is a Galois extension.

Exercise 11.12. Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions. Prove that the natural map

$$K_1 \otimes_{K_3} K_1 \longrightarrow K_1 \otimes_{K_2} K_1$$

is a surjective homomorphism of algebras.

Exercise 11.13 (!). Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions such that $[K_1 : K_3]$ is a Galois extension. Prove that $[K_1 : K_2]$ is also a Galois extension.

Hint. Use the Problem 9.28 from ALGEBRA 9.
Exercise 11.14. Let $P \in k[t]$ be a polynomial of degree $n$ over the field $k$. Let $K_1 = k$; consider the sequence of field extensions $K_i \supset K_{i-1} \supset \cdots \supset K_1$ which is constructed as follows. Suppose $K_j$ is constructed. Decompose $P$ into irreducible factors $P = \prod P_i$ in $K_j$. If all $P_i$ are linear then the construction is over. Otherwise, let $P_0$ be an irreducible factor of $P$ of degree $> 1$. Consider $K_{j+1} = K_j[t]/P_0$. Prove that this process terminates in a finite number of steps and gives some field $K \supset k$.

Definition 11.2. This field is called a splitting field of the polynomial $P$.

Exercise 11.15 (†). Let $K$ be a splitting field of a polynomial $P(t) \in k[t]$. Prove that $K$ is isomorphic to a subfield of the algebraic closure $\overline{k}$ that is generated by all roots of $P$.

Exercise 11.16. Let $P(t)$ be a polynomial of degree $n$. Prove that the degree of its splitting field is not greater than $n!$.

Exercise 11.17. Let $P \in k[t]$ be a polynomial of degree $n$ that has $n$ pairwise disjoint roots in the algebraic closure $k$ and let $[K : k]$ be its splitting field and $K_i \supset K_{i-1} \supset \cdots \supset K_1$ the corresponding sequence of field extensions. Prove that $K \otimes_{K_{i-1}} K_i$ is isomorphic to a direct sum of several copies of $K$.

Hint. This follows immediately from Problem 11.1.

Exercise 11.18 (†). Let $P(t) \in k[t]$ be an irreducible polynomial of degree $n$ that has $n$ pairwise disjoint roots in the algebraic closure $k$ (this polynomial is said to have no multiple roots) and let $K$ be its splitting field. Prove that $[K : k]$ is a Galois extension.

Hint. Use the previous problem.

Exercise 11.19 (*). Let $P(t) \in k[t]$ be an irreducible polynomial over a field $k$ of characteristic 0. Prove that $P$ has no multiple roots.

Hint. Prove that $P(t) = t^n + a_{n-1}t^{n-1} + \ldots$ doesn’t have multiple roots if and only if $P$ has no common factors with the polynomial

$$P'(t) = nt^{n-1} + (n-1)a_{n-1}t^{n-2} + \cdots + 2a_2t + a_1.$$ 

In order to show this, prove that $(PQ)' = PQ' + Q'P$ and compute $P'(t)$ for $P = (t - b_1) \ldots (t - b_n)$.

Remark. It follows from the previous problem that over a field of characteristic 0 the splitting field of any polynomial is a Galois extension.

Exercise 11.20 (*). Give an example of a field $k$ (of non-zero characteristic) and an irreducible polynomial $P \in k[t]$ such that its splitting field is not a Galois extension.

Galois groups

Definition 11.3. Let $[K : k]$ be a Galois extension. The Galois group $[K : k]$ is the group of $k$-linear automorphisms of the field $K$. We denote the Galois group by $\text{Gal}([K : k])$ or $\text{Aut}_k(K)$.

In what follows we consider $K \otimes_k K$ as a $K$-algebra with the action of $K^*$ given by a formula $a(v_1 \otimes v_2) = av_1 \otimes v_2$. This action of $K^*$ is called the left action. It is different than the “right action” which is defined by the formula $a(v_1 \otimes v_2) = v_1 \otimes av_2$.
Exercise 11.21. Let $[K : k]$ be a Galois extension. Construct a bijection between the set of $K$-linear homomorphisms $K \otimes_k K \to K$ and the set of indecomposable idempotents in $K \otimes_k K$.

Exercise 11.22. Let $\mu : K \otimes_k K \to K$ be non-zero $K$-linear homomorphism and $k \otimes_k K \subset K \otimes_k K$ be a $k$-subalgebra naturally isomorphic to $K$. Prove that $\mu |_{k \otimes_k K}$ defines a $k$-linear automorphism $K \to K$.

Exercise 11.23. Prove that every $k$-linear automorphism $K$ can be obtained this way.

Hint. Let $\nu \in \text{Gal}([K : k])$. Define a homomorphism $K \otimes_k K \to K$ as follows: $v_1 \otimes v_2 \mapsto v_1 \nu(v_2)$.

Exercise 11.24 (!). Let $[K : k]$ be a Galois extension. Construct the natural bijection between $\text{Gal}([K : k])$ and the set of indecomposable idempotents in $K \otimes_k K$. Prove that the order of the Galois group is the $k$-vector space dimension of $K$.

Exercise 11.25. Let $[K : k]$ be a Galois extension, $\nu \in \text{Gal}([K : k])$ be an element of the Galois group and $e_\nu$ be the corresponding idempotent in $K \otimes_k K$. Let $\mu_l$ denote the standard (left) action $K^* \to K \otimes_k K$, and let $\mu_r$ denote the standard right action. Prove that $\mu_l(a)e_\nu = \mu_r(\nu(a))e_\nu$.

Exercise 11.26. Let $[K : k]$ be a Galois extension and $a \in K$ be an element invariant under the action of $\text{Gal}([K : k])$. Prove that $a \otimes 1 = 1 \otimes a$ in $K \otimes_k K$.

Hint. Use the Problem 11.25.

Exercise 11.27 (!). Let $[K : k]$ be a Galois extension and let $a \in K$ be an element invariant under the action of $\text{Gal}([K : k])$. Prove that $a \in k$.

Exercise 11.28. Let $[K : k]$ be a Galois extension and let $K'$ be an intermediate extension, $K \supset K' \supset k$. Prove that $K' = K^{G'}$ where $G' \subset \text{Gal}([K : k])$ is the group of $K'$-linear automorphisms of $K$ and $K^{G'}$ denotes the set of elements of $K$ invariant under $G'$.

Hint. Prove that $[K : K']$ is a Galois extension and use the previous problem.

Exercise 11.29 (!). Prove the Fundamental Theorem of Galois theory. Let $[K : k]$ be a Galois extension. Then $G' \to K^{G'}$ defines a bijective correspondence between the set of subgroups $G' \subset \text{Gal}([K : k])$ and the set of intermediate fields $K \supset K' \supset k$.

Exercise 11.30. Let $[K : k]$ be a Galois extension and let $K'$ be an intermediate field, $K \supset K' \supset k$. Construct the natural correspondence between the set of $k$-linear homomorphisms $K' \to K$ and the collection $\text{Gal}([K : k]) / \text{Gal}([K : K'])$ of cosets of $\text{Gal}([K : K']) \subset \text{Gal}([K : k])$ in the Galois group $\text{Gal}([K : k])$.

Exercise 11.31. Find the Galois group $[\mathbb{Q}[\sqrt{a}] : \mathbb{Q}]$.

Exercise 11.32 (!). Let $[K : k]$ be a Galois extension and let $a$ be an element of the field $K$ generates $K$ over $k$ (this element is called primitive). Prove that if $\nu_1, \nu_2, \ldots, \nu_n$ are pairwise distinct elements of $\text{Gal}([K : k])$ then $\nu_1(a), \nu_2(a), \ldots, \nu_n(a)$ are linearly independent over $k$.

Exercise 11.33 (!). Let $[K : k]$ be a Galois extension and let $V \subset K$ be the union of all intermediate fields $k \subset K' \subset K$ which are proper subfields of $K$. Suppose that $V \neq K$. 


Hint. $V$ is the union of a finitely many $k$-subspaces of $K$ that have a dimension (over $k$) lower than the dimension of $K$ as a linear space over $k$. Prove that in this case $V \neq K$.

Remark. It follows that any Galois extension $[K : k]$ of any infinite field $k$ has a primitive element.

Exercise 11.34 (!). Let $[K : k]$ be a Galois extension. Prove that for any $a \in K$ the product $P(t) = \prod_{\nu \in \text{Gal}([K:k])}(t - \nu(a))$ is a polynomial with coefficients in $k$.

Exercise 11.35 (*). In the previous problem setting, let $a$ be primitive. Prove that $P(t)$ is irreducible.

Exercise 11.36 (!). Recall that the $n$-th root of unity is called primitive if it generates the group of $n$-th roots of unity. Let $\xi \in \mathbb{C}$ be a primitive $n$-th root. Prove that the group $\text{Gal}([\mathbb{Q}[\xi] : \mathbb{Q}])$ is isomorphic to the group $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ of automorphisms of the group $\mathbb{Z}/n\mathbb{Z}$. Find its order.

Exercise 11.37 (*). Consider an integer $n$. Let $P(t) = \prod (t - \xi_i)$ where the product is taken over all primitive $n$-th roots of unity $\xi_i$. Prove that $P(t)$ has rational coefficients and is irreducible over $\mathbb{Q}$.

Remark. This polynomial is called cyclotomic polynomial.

Exercise 11.38 (*). Find a decomposition of $x^n - 1$ into factors irreducible over $\mathbb{Q}$.

Exercise 11.39. Let $a_1, \ldots, a_n \in \mathbb{Z}$ be co-prime and non-square numbers. Prove that $[\mathbb{Q}[\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n} : \mathbb{Q}]$ is a Galois extension.

Exercise 11.40. Find the Galois group of this extension.

Exercise 11.41 (!). Prove that $\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}$ are linearly independent over $\mathbb{Q}$.

Finite fields

We know the following facts about finite fields from the previous problem sheets. The order of a finite field is $p^n$ where $p$ is its characteristic. For any field $k$ of characteristic $p$ there exists the Frobenius endomorphism, $Fr : k \to k$, $x \mapsto x^p$. The finite field of $\mathbb{F}_p$ naturally embeds into any field of characteristic field $p$.

We denote the field of order $p^n$ by $\mathbb{F}_{p^n}$.

Exercise 11.42. Let $x \in \mathbb{F}_{p^n}$, $x \neq 0$. Prove that $x^{p^n - 1} = 1$.

Hint. Use Lagrange’s theorem (the order of an element divides the number of elements in the group).

Remark. It follows that the polynomial $P(t) = t^{p^n-1} - 1$ has exactly $p^n - 1$ roots in $\mathbb{F}_{p^n}$.

Exercise 11.43 (!). Prove that $\prod_{\xi \in \mathbb{F}_{p^n}\setminus \{0\}} = p^{p^n-1} - 1$.

Exercise 11.44 (!). Prove that $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ is a Galois extension.

Exercise 11.45 (!). Prove that $Fr, Fr^2, \ldots, Fr^{m-1}$ are pairwise distinct automorphisms of $\mathbb{F}_{p^n}$.

Exercise 11.46 (!). Prove that $\text{Gal}([\mathbb{F}_{p^n} : \mathbb{F}_p])$ is a cyclic group of order $n$.
Exercise 11.47 (*). Prove that the splitting field of the polynomial $t^{p^n} - 1$ over $\mathbb{F}_p$ has order $p^n$.

Exercise 11.48 (*). Prove that the field of order $p^n$ is unique up to isomorphism.

Exercise 11.49 (!). Find all subfields of $\mathbb{F}_{p^n}$.

Exercise 11.50 (!). Let $[K : k]$ be a Galois extension. Prove that $K$ has a primitive element.

Remark. We have already proved this for infinite fields, see the remark after the Problem 11.33.

Abel’s theorem

Abel’s theorem states that a generic polynomial of degree 5 is not solvable by radicals; in other words, the solution of a generic equation of degree 5 cannot be expressed using algebraic operations (multiplication, addition, division) and taking an $n$-th root. In this section we will give an example of an equation that is not solvable by radicals.

Exercise 11.51. Let $[K : k]$ be a Galois extension. Prove that the subgroup $G' \subset \text{Gal}([K : k])$ is normal if and only if $[K^{G'} : k]$ is a Galois extension.

Exercise 11.52 (!). Let $G' \subset \text{Gal}([K : k])$ be a normal subgroup. Prove that the group $\text{Gal}([K^{G'} : k])$ is isomorphic to the quotient $\text{Gal}([K : k])/G'$.

Definition 11.4. A Galois extension $[K : k]$ is called cyclic, if its Galois group is cyclic.

Exercise 11.53 (!). Let Galois group of an extension $[K : k]$ be solvable. Prove that $[K : k]$ can be broken into a sequence of Galois extensions $k = K_0 \subset K_1 \subset ... \subset K_n = K$ so that for any $i$, $\text{Gal}([K_{i-1} : K_i])$ is a cyclic group.

Exercise 11.54 (*). Let $k$ contain all $n$-th roots of unity and $[K : k]$ be a splitting field of the polynomial $t^n - a$ which does not have roots over $k$. Prove that this extension is cyclic.

Hint. Let $\alpha$ be some root of the polynomial $t^n - a$. Then all roots of $t^n - a$ are of the form $\alpha, \alpha \xi, \alpha \xi^2, \ldots, \alpha \xi^{p-1}$, where $\xi$ is a root of unity. Prove that the automorphism that maps $\alpha$ to $\alpha \xi^i$, also maps $\alpha \xi^q$ to $\alpha \xi^{q+i}$.

Exercise 11.55 (*). Take $n \in \mathbb{N}$. Let for any $k > 1$ dividing $n$, $a \in \mathbb{Q}$ does not equal $k$-th power of any rational number, and $[K : \mathbb{Q}]$ be the splitting field of the polynomial $t^n - a$. Prove that $K$ contains all $n$-th roots of unity and that $\text{Gal}([K : \mathbb{Q}])$ is isomorphic to a semi-direct product $\mathbb{Z}/n\mathbb{Z} \rtimes \text{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Exercise 11.56 (*). Let $k$ be a field of characteristic 0, and let $[K : k]$ be a splitting field of the polynomial $t^n - a$. Prove that the Galois group $\text{Gal}([K : k])$ is solvable.

Hint. If $k$ contains the $n$-th roots of unity then there is nothing to prove. Suppose not, then prove that $K$ contains the $n$-th roots. Consider an intermediate extension $K'$ generated by these roots over $k$ and prove that $[K : K']$ and $[K' : k]$ are Galois extensions with Abelian Galois groups.
Exercise 11.57. Let \([K : k]\) be a cyclic extension of order \(n\), and let \(\nu\) be a primitive element of the group \(\text{Gal}[K : k]\), \(\xi \in k\) be the primitive roots of unity of degree \(n\), and \(\alpha \in K\) is a primitive element of the extension. Consider the Lagrange’s resolvent

\[
L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \cdots + \xi^{-n+1}\nu^{n-1}(a)
\]

Prove that \(\nu(L) = \xi L\). Prove that \(L \neq 0\).

Exercise 11.58 (*). Prove that \(\prod_{i=0}^{n-1}(t - \nu^i(L)) = t^n - L^n\). Prove that \(L\) generates \(K\) over \(k\) and that \(L^n \in k\).

Hint. To see that \(L\) generates \(K\) over \(k\), use the fact that \(\text{Gal}[k[\sqrt[n]{L}], k] = \mathbb{Z}/n\mathbb{Z}\), and therefore the dimension of \(k[L]\) over \(k\) is the same as dimension of \(K\) over \(k\).

Exercise 11.59 (*). Let \([K : k]\) be a Galois extension of order \(n\), and let \(k\) contain all the \(n\)-th roots of unity. Prove that \([K : k]\) is cyclic if and only if it is generated by an \(n\)-th root of a \(a \in k\).

Exercise 11.60 (*). (Galois theorem) Deduce the following theorem. A Galois extension \([K : k]\) is obtained by successive addition of solutions of equations of the form \(t^n - a\) if and only if the group \(\text{Gal}[K : k]\) is solvable.

Remark. Let \(P(t) \in k[t]\) be a polynomial. The Galois group of \(P\) is defined to be the Galois group its splitting field. Galois theorem states that \(P(t) = 0\) is solvable by radicals if and only if the Galois group of \(P(t)\) is solvable.

Definition 11.5. Let group \(G\) act on a set \(\Sigma\). The action is called transitive if any \(x \in \Sigma\) can be mapped to any \(y \in \Sigma\) by an action of some \(g \in G\).

Exercise 11.61. Let \(G \subset S_n\) be a subgroup that contains a transposition and that acts transitively on \(\{1, 2, 3, \ldots, n\}\). Prove that \(G = S_n\).

Exercise 11.62. Let \(P \in k[t]\) be an irreducible polynomial, and let \(\xi_1, \ldots, \xi_n\) be its roots and let all these roots be distinct. Prove that the Galois group of \(P\) acts on \(\{\xi_1, \ldots, \xi_n\}\) transitively.

Hint. Consider a decomposition of \(\{\xi_1, \ldots, \xi_n\}\) into equivalence classes under the action of \(\text{Gal}(P)\). Let \(S\) be one of these equivalence classes. Prove that the polynomial \(\prod_{\xi_i \in S}(t - \xi_i)\) has coefficients in \(k\) and divides \(P\).

Exercise 11.63 (!). Let \(P \in \mathbb{Q}[t]\) be an irreducible polynomial of degree \(n\) that has exactly \(n - 2\) real roots. Prove that its Galois group is \(S_n\).

Hint. Prove that \(\text{Gal}(P)\) acts transitively on the roots of \(P\), and that the complex conjugation preserves the splitting field of \(P\) and acts on the set of roots as a transposition.

Exercise 11.64 (!). (Eisenstein theorem) Let \(Q = t^n + t^{n-1}a_{n-1} + t^{n-2}a_{n-2} + \cdots + a_0\) be a polynomial with integer coefficients such that all \(a_i\) divide a given prime number \(p\), and \(a_0 \nmid p^2\). Prove that \(Q\) is irreducible over \(\mathbb{Q}\).

Exercise 11.65 (*). Prove that \(Q(t) = x^5 - 10x + 5\) is an irreducible (over \(\mathbb{Q}\)) polynomial which has exactly 3 real roots. Deduce that its Galois group is \(S_5\).

Exercise 11.66 (*). Prove that the equation \(x^5 - 10x + 5 = 0\) is not solvable by radical.