Complex variables 7: Artin's primitive element theorem

Rules: This is a class assignment for the next week. Exercises with [*] are extra hard and not necessary to follow the rest. Exercises with [!] are non-trivial, fundamental and necessary for further work.

Remark 7.1. In the sequel, we assume that $\operatorname{char} k = 0$ unless stated otherwise.

7.1 Galois extensions

Exercise 7.1. Let $P(t) \in K[t]$ be a degree n polynomial with n pairwise distinct roots in K. Prove that the ring $K[t]/(P)$ is isomorphic as a ring to the direct sum of n copies of K.

Definition 7.1. Let $[K:k]$ be a finite extension of a field k. We say that $[K:k]$ is a **Galois extension** if $K \otimes_k K$ is isomorphic (as a ring) to the direct sum of several copies of K.

Remark 7.2. A finite extension $[K:k]$ **has degree** n if K is n-dimensional as a vector space over k.

Exercise 7.2. Let $[K:\mathbb{Q}]$ be a degree 2 field extension. Prove that it is a Galois extension.

Hint. Show first that $K \otimes_k K$ is a direct sum of fields.

Exercise 7.3 (*). Let p be a prime number, Prove that for any root of unity of degree p, the extension $[\mathbb{Q}[\zeta]:\mathbb{Q}]$ is Galois.

Exercise 7.4. Let $P \in k[t]$ be a polynomial of degree n over a field k. Let $K_1 = k$, and consider a sequence of field extensions $K_l \supset K_{l-1} \supset \cdots \supset K_1$, obtained inductively as follows. Suppose that K_j is already constructed. Decompose P onto irreducible multipliers $P = \prod P_i$ over K_j. If all P_i have degree 1, we are done. Otherwise, let P_0 be an irreducible multiplier of P over K_j of degree $d > 0$. Take $K_{j+1} := K_j[t]/P_0$. Prove that it is a field. Prove that the sequence $K_l \supset K_{l-1} \supset \cdots \supset K_1$ terminates and gives a field $K \supset k$.

Definition 7.2. This field is called **the splitting field** of a polynomial P.

Exercise 7.5. Let K be the splitting field for a polynomial $P(t) \in k[t]$. Prove that K is isomorphic to the subfield in an algebraic closure $\bar{k}$ generated by all roots of P.

Exercise 7.6. Suppose that all roots of an irreducible polynomial $P(t)$ are pairwise distinct. Prove that the splitting field of $P(t)$ is the minimal extension of $P(t)$ containing the field $k[t]/(P)$.

Exercise 7.7. Let $P(t)$ be a polynomial of degree n, and d the degree of its splitting field. Prove that $d \leqslant n!$.

Exercise 7.8. Let $P \in k[t]$ be a degree n polynomial which has n pairwise distinct roots in the algebraic closure of k. Let $[K:k]$ be its splitting field, and $K_l \supset K_{l-1} \supset \cdots \supset K_1$ the corresponding chain of extensions. Prove that $K \otimes_{K_{i-1}} K_i$ is isomorphic to a direct sum of several copies of K.

Hint. Deduce this from Exercise 7.1.

Exercise 7.9. Let $P \in k[t]$ be a degree n polynomial which has n pairwise distinct roots in the algebraic closure of k, and K its splitting field. Prove that $[K:k]$ is a Galois extension.

Hint. Use the previous exercise and apply induction.

Exercise 7.10. Let $a_1, ..., a_n$ be integers. Prove that $\mathbb{Q}[\sqrt{a_1}, ..., \sqrt{a_n}]$ is a direct sum of Galois extensions.

7.2 Artin's primitive element theorem

Exercise 7.11. Let $R := \oplus^n K$ be a direct sum of several copies of a field K. Prove that any subalgebra $A \subset R$ contains a unity (which might be distinct from the unity in R).

Hint. Prove that A is semisimple and show that it is a direct sum of fields.

Exercise 7.12. Prove that subalgebras of $R := \oplus^n K$ are in (1,1)-correspondence with idempotents of R.

Exercise 7.13. Prove that $\oplus^n K$ has precisely $n!$ idempotents.

Exercise 7.14. Prove that $\oplus^n K$ has finitely many different subalgebras.

Exercise 7.15. Let $[K : k]$ be a finite extension in characteristic 0. Prove that there exists a Galois extension $[K' : k]$ containing K.

Exercise 7.16. Let $[K : k]$ be a finite extension, $[K' : k]$ a Galois extension containing K, and $k' \subset K$ a subfield containing k. Prove that $k' \otimes_k K'$ is a subalgebra in $K' \otimes_k K' = \oplus^n K'$. Prove that different subfields k' give different subalgebras in $\oplus^n K'$.

Exercise 7.17 (!). Let $[K : k]$ be a finite extension, $\operatorname{\mathsf{char}} k = 0$. Prove that there are only finitely many intermediate extensions $k \subset k' \subset K$.

Hint. Use the previous exercise and Exercise 7.14.

Exercise 7.18 (!). Let k be a field of characteristic 0, V a finitely-dimensional vector space, and $V_1, ...V_n \subset V$ a family of subspaces of positive codimension. Prove that $\bigcup_i V_i \neq V$.

Exercise 7.19 (!). Let $[K : k]$ be a finite extension, $\operatorname{\mathsf{char}} k = 0$, and $k_1, ..., k_n$ all intermediate subfields $k \subset k_i \subsetneq K$. Prove that $\bigcup_i k_i \neq K$.

Hint. Use the previous exercise.

Definition 7.3. Let $[K : k]$ be a field extension. An element $\alpha \in K$ is called **primitive** if it generates K.

Exercise 7.20 (!). (Artin's primitive element theorem) Prove that any finite extension $[K : k]$ in characteristic 0 is generated by a primitive element.

Hint. Use the previous exercise.

Exercise 7.21 (*). Construct a finite extension $[K : k]$ in $\operatorname{\mathsf{char}} = p$ such that K does not contain a primitive element.

Exercise 7.22. Let $k := \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Prove that it is a field. Find whether $\sqrt{2} + \sqrt{3}$ is a primitive element in $[k : \mathbb{Q}]$ or not.

Exercise 7.23 (*). Let $a_1, ..., a_n$ be integers, such that $K := \mathbb{Q}[\sqrt{a_1}, ..., \sqrt{a_n}]$ is a field. Find whether $\sum_i \sqrt{a_i}$ is a primitive element in $[k : \mathbb{Q}]$ or not.