Complex variables 6: Galois theory 1

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 6.1. All rings in the sequel are assumed commutative, associative and with unit.

6.1 Artinian rings

Remark 6.2. In this assignment, **algebra** over a field k denotes a vector space over a field k with k-linear, commutative multiplication, possibly without unity. **A ring** is a commutatove ring with unity. **Finite field extension** $[K : k]$ of field K over a field $k \subset K$ is a field K which contains a subfield k, which is finite-dimensional as a vector space over k.

Definition 6.1. Let R be a commutative algebra with unity over a field k. We say that R is **Artinian ring over** k if R is finite-dimensional as a vector space over k.

Remark 6.3. Let $A \in \operatorname{End} V$ be a linear endomorphism of a finite-dimensional vector space V over k. Consider the subalgebra $k[A] \subset \operatorname{End} V$ generated by unity and A. Clearly, $k[A]$ is an Artinian ring.

Exercise 6.1 (!). Let R be an Artinian ring without zero divisors. Prove that R is a field.

Hint. Prove that any injective endomorphism of a finite-dimensional space is invertible. Use this to find x^{-1} for any given $x \in R$.

Exercise 6.2. Prove that any prime ideal in an Artinian ring is maximal.

Hint. Use the previous exercise.

Definition 6.2. An Artinian ring is called **semisimple** if it does not contain non-zero nilpotents.

Definition 6.3. Let $R_1, \ldots, R_n$ be algebras over a field. Consider the direct sum $\bigoplus_i R_i$ with the natural (componentwise) addition and multiplication. This algebra is called **the direct sum of** $R_1, \ldots, R_n$.

Exercise 6.3. Prove that the direct sum of semisimple Artinian rings is semisimple.

Exercise 6.4. Let $v \in R$ be an element of a finite-dimensional algebra R over k. Consider a subspace $k[v] \subset R$ generated by $1, v, v^2, v^3, \ldots$. Suppose that $\dim k[v] = n$. Prove that $P(v) = 0$ for a polynomial $P = t^n + a_{n-1}t^{n-1} + \ldots$ with coefficients in k. Prove that this polynomial is unique.

Definition 6.4. This polynomial is called **the minimal polynomial** of $v \in \mathbb{R}$.

Exercise 6.5. Let $v \in R$ be an element of an Artinian ring over k, and $P(t)$ its minimal polynomial. Consider the subalgebra $k[v] \subset R$ generated by v and k. Prove that $R[v]$ is isomorphic to the ring $k[t]/(P)$ of residues modulo $P(t)$.

6.2 Idempotents

Definition 6.5. Suppose that $v \in R$ satisfies $v^2 = v$. Then v is called **an idempotent**.

Exercise 6.6. Let $e \in R$ be an idempotent in a ring. Prove that $1 - e$ is also an idempotent. Prove that a product of idempotents is an idempotent.

Exercise 6.7. Let $e \in R$ be an idempotent in a ring. Consider the space $eR \subset R$ (image of the multiplication by e. Prove that eR is a subalgebra in R, e is unity in eR, and $R = eR \oplus (1-e)R$.

Exercise 6.8 (!). Let $R = k[t]/P$, where $P \in k[t]$ is a polynomial decomposing as a product $P = P_1 P_2 \dots P_n$ of coprime polynomials. Prove that there exists an isomorphism $R \longrightarrow \bigoplus_i k[t]/P_i$ mapping t to $(t, t, \dots, t)$.

Hint. Use the Chinese remainder theorem.

Exercise 6.9 (!). Let R be a semisimple Artinian ring without non-unit idempotents. Prove that it is a field.

Hint. Suppose that R is not a field. Consider a subalgebra $k[x] \subset R$ generated by a non-invertible element x, and apply the previous exercise.

Definition 6.6. We say that idempotents $e_1, e_2 \in R$ **are orthogonal** if $e_1 e_2 = 0$.

Exercise 6.10. Let $e_2, e_3 \in R$ be orthogonal idempotents. Prove that $e_1 := e_2 + e_3$ is also an idempotent satisfying $e_2, e_3 \in e_1 R$ $e_1 R = e_2 R \oplus e_3 R$.

Exercise 6.11. Let $\operatorname{char} k \neq 2$, and e_1, e_2, e_3 idempotents in an algebra R over k. Suppose that $e_1 = e_2 + e_3$. Prove that e_2, e_3 are orthogonal.

Definition 6.7. An idempotent $e \in R$ is called **indecomposable** if there are no non-zero orthogonal idempotents e_2, e_3 such that $e = e_2 + e_3$.

Exercise 6.12 (!). Let R be a semisimple Artinian algebra, and $e \in R$ a non-decomposable idempotent. Prove that eR is a field.

Exercise 6.13 (!). Let R be a semisimple Artinian ring over a field k, $\operatorname{char} k \neq 2$. Prove that 1 can be decomposed to a sum of indecomposable orthogonal idempotents, $1 = \sum_{i=1}^r e_i$. Prove that such a decomposition is unique.

Hint. To prove existence, take an idempotent $e \in R$, decompose R to a direct sum of two subrings, $R = eR \oplus (1-e)R$, and use induction in $\dim_k R$. For uniqueness, take two different orthogonal decompositions, $1 = \sum_{i=1}^r e_i$, and $1 = \sum_{j=1}^s f_j$, and prove that $e_i = \sum_{j=1}^s e_i f_j$ is an orthogonal decomposition.

Exercise 6.14 (!). Let R be a semisimple Artinian ring over a field k, $\operatorname{char} k \neq 2$. Prove that R is isomorphic to a direct sum of fields. Prove that this decomposition is unique.

Hint. Use the previous exercise.

Exercise 6.15 (*). Is it true when $\operatorname{char} k = 2$?

Exercise 6.16 (*). Let R be an Artinian ring over a field k, $\operatorname{char} k \neq 2$, and $1 = e_1 + \cdots + e_n$ a decomposition of 1 to a sum of indecomposable orthogonal idempotents. Prove that R has precisely n prime ideals.

6.3 Trace form

Definition 6.8. Let R be an algebra over a field k. A bilinear symmetric form g on R is called **invariant**, if $g(x, yz) = g(xy, z)$ for all x, y, $z \in R$.

Remark 6.4. If R contains unity, then for any invariant form g, we have $g(x, y) = g(xy, 1)$. This means that g is uniquely determined by a linear functional $x \longrightarrow g(x, 1)$.

Exercise 6.17. Let R be an Artinian ring equipped with a bilinear invariant form g, and $\mathfrak{m}$ an ideal in R. Prove that its orthogonal complement $\mathfrak{m}^\perp$ is also an ideal.

Exercise 6.18 (*). Find an Artinian ring which does not admit a non-degenerate invariant bilinear form.

Definition 6.9. Let R be an Artinian ring over k. Consider the bilinear form $a, b \longrightarrow \operatorname{Tr}(ab)$, where $\operatorname{Tr}(ab)$ is the trace of the endomorphism $L_{ab} \in \operatorname{End}_k R$, $x \xrightarrow{L_{ab}} abx$. This form is called **the trace form**, denoted $\operatorname{Tr}_k(ab)$.

Exercise 6.19 (*). Let A be a linear operator on an n-dimensional vector space of characteristic 0, such that $\operatorname{Tr} A = \operatorname{Tr} A^2 = ... = \operatorname{Tr} A^n = 0$. Prove that A is nilpotent.

Exercise 6.20 (!). Let $[K : k]$ be a finite field extension in characteristic 0. Prove that the trace form is always non-degenerate.

Hint. Prove that $\operatorname{Tr}_k(x, x^{-1}) = \dim_k K$.

Definition 6.10. A finite field extension $[K : k]$ with non-degenerate trace form is called **separable**.

Exercise 6.21 (*). Find an example of non-separable finite field extension in characteristic p.

Exercise 6.22 (!). Let R be an Artinian ring over k with non-degenerate trace form. Prove that R is semisimple. Prove that for $\operatorname{char} k = 0$, the trace form is non-degenerate on any semisimple Artinian ring.

6.4 Tensor products of field extensions

Exercise 6.23. Let A, B be rings over a field k.

a. Prove that there exists a multiplicative operation $(A \otimes_k B) \times (A \otimes_k B) \longrightarrow A \otimes_k B$, mapping $a \otimes b, a' \otimes b'$ to $aa' \otimes bb'$.

b. Prove that this operation defines the ring structure on $A \otimes_k B$.

Definition 6.11. The ring $A \otimes_k B$ is called **the tensor product of the rings A and B.**

Exercise 6.24. Let R, R' be Artinian rings over k, and g, g' the trace forms on R, R'. Consider the tensor product $R \otimes_k R'$, and the bilinear symmetric form $g \otimes g'$ on $R \otimes R'$, acting as $g \otimes g'(a \otimes a', b \otimes b') := g(a, a')g'(b, b')$. Prove that $g \otimes g'$ is equal to the form $a, b \longrightarrow \operatorname{Tr}(ab)$.

Exercise 6.25 (!). Prove that the tensor product of semisimple Artinian rings is semisimple if $\operatorname{char} k = 0$.

Hint. Use the previous exercise.

Exercise 6.26. Let $[K_1 : k]$, $[K_2 : k]$ be finite extensions, $\operatorname{char} k = 0$. Prove that the algebra $K_1 \otimes_k K_2$ is semisiple.

Exercise 6.27. Let $P_1(t), P_2(t) \in k[t]$ be polynomials over k, and $K_i := k[t]/(P_i)$. Prove that $K_1 \otimes K_2 \cong K_1[t]/Q(t) \cong K_2[t]/P(t)$.

Exercise 6.28. Let $P(t) \in \mathbb{Q}[t]$ be a polynomial which has precisely r real roots and $2s$ complex roots which are not real, all roots distinct. Show that

$$(\mathbb{Q}[t]/P) \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_s \mathbb{C} \oplus \bigoplus_r \mathbb{R}.$$

Exercise 6.29 (*). Find two non-trivial finite extensions $[K_1 : \mathbb{Q}]$, $[K_2 : \mathbb{Q}]$ such that $K_1 \otimes_{\mathbb{Q}} K_2$ is also a field.

Exercise 6.30 (*). Find two finite extensions $[K_1 : k]$, $[K_2 : k]$, $\operatorname{char} k = p$ such that $K_1 \otimes K_2$ is not semisimple.