Commutative Algebra

lecture 9: some Galois theory

Misha Verbitsky

http://verbit.ru/IMPA/CA-2026/

IMPA, sala 236

April 17, 2026

Field extensions (reminder)

DEFINITION: An extension of a field k is a field K containing k. We write "K is an extension of k" as $[K : k]$.

DEFINITION: Let $k \subset K$ be a field contained in a field. In this case, we say that k is **a subfield** of K, and K is **extension** of k. An element $x \in K$ is called **algebraic** over K if x is a root of a non-zero polynomial with coefficients in k. An element which is not algebraic is called **transcendental**.

THEOREM: A sum and a product of algebraic numbers is algebraic. ■

DEFINITION: A field extension $K \supset k$ is called **algebraic** if all elements of K are algebraic over k. A field k is called **algebraically closed** if all algebraic extensions of k are trivial.

EXAMPLE: The field $\mathbb{C}$ is algebraically closed.

DEFINITION: In this lecture, **k-algebra** is a ring containg a field k, not necessarily with unity. **All k-algebras are tacitly assumed commutative. Homomorphisms of k-algebras** are k-linear map compatible with the multiplication.

Minimal polynomials (reminder)

CLAIM: Let K be a finite-dimensional k-algebra with unity and without zero divisors. **Then K is a field.**

Proof: An injective endomorphism of finite-dimensional spaces is surjective. Therefore, for each $x \in K$, there exists $y \in K$ such that $xy = 1$. ■

DEFINITION: Let v be an element of a finite-dimensional k-algebra R, and $P(t) = t^n + a_{n-1}t^{n-1} + \dots$ a polynomial of smallest possible degree with coefficients in k satisfying $P(v) = 0$. This polynomial is called **the minimal polynomial** of $v \in R$.

CLAIM: Let $v \in R$ be an element of finite-dimensional algebra R over k, and $P(t)$ its minimal polynomial. **Then the subalgebra $R_v \subset R$ generated by v is isomorphic to $k[t]/(P)$.**

Proof: By definition, R_v is a quotient of $k[t]$ by an ideal I of all polynomials $R(t)$ such that $R(v) = 0$. Since $k[t]$ is a principal ideal ring (home assignment 5), $I = (Q)$ for some polynomial $Q(t)$ satisfying $Q(v) = 0$. **Then Q is the minimal polynomial.** ■

Irreducible polynomials (reminder)

THEOREM: The polynomial ring $k[t]$ is factorial (admits the unique prime decomposition).

Proof: See assignment 5. ■

DEFINITION: A polynomial $P(t) \in k[t]$ is **irreducible** if it is not a product of polynomials $P_1, P_2 \in k[t]$ of positive degree.

PROPOSITION: Let $(P) \subset k[t]$ be a principal ideal generated by the polynomial $P(t)$. Then **the polynomial $P(t)$ is irreducible if and only if the quotient ring $k[t]/(P)$ is a field.**

Proof. Step 1: The polynomial P is irreducible if and only if (P) is prime. This follows because $k[t]$ is a factorial ring.

Step 2: The quotient ring $k[t]/(P)$ is finite-dimensional over k. Then, it is a field if and only if it has no zero divisors. ■

Primitive extensions (reminder)

DEFINITION: Let $P(t) \in k[t]$ be an irreducible polynomial. A field $k[t]/(P)$ is called **an extension of k obtained by adding a root of $P(t)$**. The extension $[k[t]/(P) : k]$ is called **primitive**.

CLAIM: Let $[K : k]$ be a finite extension. **Then K can be obtained from k by a finite chain of primitive extensions**. In other words, there exists a sequence of intermediate extensions $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$ such that each $[K_i : K_{i-1}]$ is primitive. ■

Tensor product of field extensions

LEMMA: Let R, R' be Artinian k-algebras. Denote the corresponding trace forms by g, g'. Consider the tensor product $R \otimes_k R'$ with a natural structure of Artinian k-algebra. **Then the trace form on $R \otimes_k R'$ is equal $g \otimes g'$,** that is,

$$\operatorname{tr}_{R\otimes_k R'}(x \otimes y, z \otimes t) = g(x,z)g'(y,t). \quad (*)$$

Proof: Let V, W be vector spaces over k, and μ, ρ endomorphisms of V, W. Then $\operatorname{tr}(\mu \otimes \rho) = \operatorname{tr}(\mu)\operatorname{tr}(\rho)$, which is clear from the block decomposition of the matrix $\mu \otimes \rho$. **This gives the trace for any decomposable vector $r \otimes r' \in R \otimes_k R'$.** The equation (*) is extended to the rest of $R \otimes_k R'$ because decomposable vectors generate $R \otimes_k R'$. ■

COROLLARY: Let $[K_1 : k]$, $[K_2 : k]$ be separable extensions. **Then the Artinian k-algebra $K_1 \otimes_k K_2$ is semisimple,** that is, isomorphic to a direct sum of fields.

Proof: The trace form on $K_1 \otimes_k K_2$ is non-degenerate, because $g \otimes g'$ is non-degenerate whenever g, g' is non-degenerate. ■

REMARK: In particular, **if $\operatorname{char} k = 0$, the product of finite extensions of the field k is always a direct sum of fields.**

Tensor product of fields: examples and exercises

PROPOSITION: Let $P(t) \in k[t]$ be a polynomial over k, $[K : k]$ an extension, and $K_1 = k[t]/P(t)$. **Then** $K_1 \otimes K \cong K[t]/P(t)$**.** ■

COROLLARY: Let $P(t)$ be a polynomial over k, $[K : k]$ an extension, and $K_1 = k[t]/P(t)$. Assume that $P(t)$ is a product of n distinct degree 1 polynomials over K. **Then** $K_1 \otimes K \cong K[t]/P(t) = K^{\oplus n}$.

Proof: Let $P = (t-a_1)(t-a_2)...(t-a_n)$. The natural map $K[t]/(P) \xrightarrow{\tau} \bigoplus_i K[t]/(t-a_i) = K^{\oplus n}$ is injective, because any polynomial which vanishes in $a_1, a_2, ..., a_n$ is divisible by P. Since the spaces $K[t]/(P)$ and $K[t]/(t-a_i) = K$ are n-dimensional, τ is an isomorphism. ■

REMARK: Surjectivity of τ is known as **"Chinese remainders theorem".**

EXERCISE: Let $P(t) \in \mathbb{Q}[t]$ be a polynomial which has exactly r real roots and $2s$ complex, non-real roots. **Prove that** $(\mathbb{Q}[t]/P) \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_s \mathbb{C} \oplus \bigoplus_r \mathbb{R}$**.**

REMARK: Similarly, **for any irreducible polynomial** $P(t) \in k[t]$ **which has an irreducible decomposition** $P(t) = \prod_i P_i(t)$ **in** $K[t]$**, with all** $P_i(t)$ **coprime, one has** $k[t]/(P) \otimes_k K \cong K[t]/P(t) \cong \bigoplus_i K[t]/P_i(t)$**.** Proof is the same.

Existence of an algebraic closure

DEFINITION: A field k is called **algebraically closed** if all algebraic extensions of k are trivial.

CLAIM: A field k is algebraically closed **if and only if any polynomial $P(t) \in k[t]$ is a product of linear factors.**

Proof: If $P(t)$ is not a product of linear factors, there exists an irreducible component $P_1(t)$ of positive degree, Then $k[t]/(P_1)$ is a non-trivial field extension. Conversely, any non-trivial field extension contains an algebraic element which satisfies a polynomial equation. ■

REMARK: Algebraic closure $[\overline{k} : k]$ is obtained by taking a succession of increasing algebraic extensions, adding to each the roots of irreducible polynomials, and using the Zorn lemma to prove that this will end up in a field which has no non-trivial algebraic extensions.

Tensor product of fields and algebraic closure

THEOREM: Let $[\overline{k} : k]$ be the algebraic closure of k, and $[K : k]$ a separable finite extension. **Then** $K \otimes_k \overline{k} = \bigoplus \overline{k}$.

Proof. Step 1: Consider a homomorphism $K \hookrightarrow \overline{k}$, acting as identity on k. Such a homomorphism exists by construction of the algebraic closure. Then

$$K \otimes_k \overline{k} = (K \otimes_k K) \otimes_K \overline{k}$$

by associativity of tensor product.

Step 2: Since $[K : k]$ is separable, $K \otimes_k K = \bigoplus K_i$. **There are at least 2 non-trivial summands in** $\bigoplus K_i$**,** because for each irreducible polynomial $P(t) \in k[t]$ which has roots in K, one has $K \supset k[t]/(P)$, but $K \otimes_k k[t]/(P) = \bigoplus_i K[t]/(P_i)$, where $P_i(t) \in K[t]$ are irreducible components in the prime decomposition of $P(t)$ over K, with $P(t) = \prod_i P_i(t)$. This gives non-trivial idempotents in $K \otimes_k k[t]/(P)$, hence in $K \otimes_k K \supset K \otimes_k (k[t]/(P))$.

Step 3: By associativity of tensor product,

$$K \otimes_k \overline{k} = (K \otimes_k K) \otimes_K \overline{k} = \bigoplus K_i \otimes_K \overline{k}. \quad (*)$$

Since $\dim_k K = \sum_i \dim_K K_i > \max_i \dim_K K_i$, **the equation** $K \otimes_k \overline{k} = \bigoplus \overline{k}$ **follows from (*) and induction on** $\dim_k K$**.** ■

Finite union of vector spaces over infinite fields

Proposition 1: Let $V = k^n$ be a vector space over a field k of characteristic 0, and $W_1, ..., W_n \subsetneq V$ proper subspaces. **Then $V \neq \bigcup W_i$.**

Proof. Step 1: Replacing W_i by a bigger subspace if necessarily, we can assume all W_i have codimension 1 and are defined by an equation $\lambda_i(v) = 0$. Then $X := \bigcup W_i \subset V$ is an affine subvariety which is given by an equation $\prod \lambda_i = 0$.

Step 2: Let $z_1, ..., z_n$ be coordinates in V, and $z_1, ..., z_k \in k(X)$ a transcendence basis (renumber z_i if necessarily so that algebraically independent coordinates go first). The equation $\prod \lambda_i = 0$ gives an algebraic relation between z_i, restricted to X. **Therefore $k < n$.**

Step 3: After an appropriate linear change, we find a linear projection $\Pi : W \longrightarrow W_1$, with $\dim W_1 = k$, such that $\Pi : X \longrightarrow W_1$ is finite (Noether normalization lemma).

Step 4: The fibers of $\Pi : X \longrightarrow W_1$ are finite, but the fibers of $\Pi : W \longrightarrow W_1$ are vector spaces, and they are infinite. ■

Primitive element theorem

LEMMA: Let k be a field, and $A := \bigoplus_{i=1}^{n} k$. **Then A contains only finitely many different k-algebras.**

Proof: Let $e_1, ..., e_n$ be the units in the summands of A. Then any idempotent $a \in A$ is a sum of idempotents $a = \sum e_i a$, but $e_i a$ belongs to the i-th summand of A. Then $e_i a = 0$ or $e_i a = e_i$, because k contains only two idempotents. This implies that **any k-algebra $A_i \subset A$ is generated by an idempotent a, which is sum of some a_i.** ■

THEOREM: Let $[K : k]$ be a finite field extension in char $= 0$. **Then there exists a primitive element $x \in K$,** that is, an element which generates K.

Proof. Step 1: Let $\overline{k}$ be the algebraic closure of k. **The number of intermediate fields $K \supset K' \supset k$ is finite.** Indeed, all such fields correspond to $\overline{k}$-subalgebras in $K \otimes_k \overline{k}$, and **there are finitely many k-subalgebras in $K \otimes_k \overline{k}$ because $K \otimes_k \overline{k} = \bigoplus_i \overline{k}$.**

Step 2: Take for x an element which does not belong to intermediate subfields $K \supsetneq K' \supset k$. Such an element exists, because k is infinite, and K' belong to a finite set of subspaces of positive codimension (Proposition 1). **Then x is primitive,** because it generates a subfield which is equal to K. ■

Galois extensions

DEFINITION: Let $[K:k]$ be a finite extension. It is called **a Galois extension** if the algebra $K \otimes_k K$ is isomorphic to a direct sum of several copies of K.

EXAMPLE: Let $K = k[t]/(P)$ be a primitive, separable extension, with $\deg P(t) = n$. Suppose that P has n roots in K. **Then $[K:k]$ is a Galois extension.** Indeed, $K \otimes_k K = \frac{K[t]}{(P)} = \oplus_i \frac{K[t]}{(t-a_i)}$, where $\{a_i\}$ denote the roots of P in K.

EXERCISE: Let $P(t) \in k[t]$ be an irreducible polynomial, and $K := \frac{k[t]}{(P)}$. **Prove that $[K:k]$ is a Galois extension if and only if $P(t)$ has n roots in $K[t]$.**

EXERCISE: Let $[K:k]$ be a degree 2 extension, where k is a field of characteristic 0. **Prove that $[K:k]$ is a Galois extension.**

Splitting field

DEFINITION: Let $P(t) \in k[t]$ be a polynomial of degree n without multiple roots over a field of characteristic 0. Let $K_1 := k$, and consider a sequence of finite exensions $K_1 \subset K_2 \subset ... \subset K_l$, obtained as follows. Decompose P onto irreducible factors in $K_j[t]$, $P(t) = P_1(t)P_2(t)...P_m(t)$. Take $K_{j+1} := K_j[t]/(P_1)$. This process terminates in a finite number of steps **(prove this)**, resulting field $[K : k]$ is called **the splitting field**.

REMARK: It is a Galois field. Indeed, $P(t)$ has all roots in K.

CLAIM: Splitting field is uniquely defined by k and $P(t)$.

Proof: Let $[\overline{k} : k]$ be the algebraic closure of k, and $K \subset \overline{k}$ the minimal field which contains all roots of $P(t)$. **Then K is isomorphic to its splitting field.** ■

Galois group

DEFINITION: Let $[K:k]$ be a Galois extension. Then the group $\operatorname{Aut}_k K$ is called **the Galois group of** $[K:k]$.

REMARK: K^* acts on $K \otimes_k K$ by right and by left multiplication; the orbit $K^* \times K^* \cdot 1$ generates $K \otimes_k K$ over k.

CLAIM: Let $[K:k]$ be a Galois extension. **Then there exists a natural bijection between the followind sets:**

(a) The Galois group $\operatorname{Aut}_k(K)$

(b) Prime ideals in $K \otimes_k K$, or, what is the same, the components $K \subset K \otimes_k K = \bigoplus_i K$

(c) homomorphisms $K \otimes_k K \longrightarrow K$, which are linear with respect to the left action of K.

Proof. Step 1: Bijection between (b) and (c): every prime ideal gives a projection $K \otimes_k K = \bigoplus_i K \longrightarrow K$. Since K has no zero divisors, it vanishes on all summands except one. **This gives a natural equivalence between (b) and (c).**

Step 2: Each K-linear algebra homomorphism $\mu: K \otimes_k K \longrightarrow K$ restricted to $K = k \otimes K \subset K \otimes K$ gives a k-linear homomorphism $\mu|_{k \otimes_k K}: K \longrightarrow K$. This defines a map from (c) to (a).

Step 3: For each Galois element $\nu \in \operatorname{Aut}_k(K)$, define a homomorphism $K \otimes_k K \longrightarrow K$ using $v_1 \otimes v_2 \longrightarrow v_1 \nu(v_2)$. **This gives a map from (a) to (c), inverting the correspondence from Step 2.** ■

Galois invariants

REMARK: By construction, the left and the right action of K on the summands of $K \otimes_k K$ **differ by the conjugation with the corresponding Galois element.**

More precisely:

LEMMA: Let $[K : k]$ be a Galois extension, and $K \otimes_k K = \bigoplus_{\nu \in \mathrm{Aut}_k(K)} K_\nu$ the decomposition of $K \otimes_k K$ onto K-components enumerated by elements of $\mathcal{G}al_k(K)$. Let μ_l be the left action of K^* on $K \otimes_k K$, and μ_r the right action. **Then** $\mu_l(a)e_\nu = \mu_r(\nu(a))e_\nu$.

Proof: Each $a \in K$ acts on the component $K_\mu \subset K \otimes_k K$ as $\mu_l(a)(v_1 \otimes v_2) = av_1\nu(v_2)$ and $\mu_r(a)(v_1 \otimes v_2) = v_1\nu(av_2) = \nu(a)v_1\nu(v_2)$, by definition of K_ν. ■

Corollary 1: Let $[K : k]$ be a Galois extension, and $a \in K$ a $\mathcal{G}al_k(K)$-invariant element. **Then** $a \in k \subset K$.

Proof: Since $\mu_l(a) = \mu_r(a)$ on $X \otimes_k K$, we have $a \otimes_k 1 = 1 \otimes_k a$, which implies $a \in k$. ■

Main theorem of Galois theory

LEMMA: Let $[K : k]$ be a Galois extension, and K' an intermediate field, $K \supset K' \supset k$. **Then $K' = K^{G'}$, where $G' \subset \mathrm{Aut}_{K'}(K)$ is the group of K'-linear automorphisms of K, and $K^{G'}$ is the space of G'-invariants.**

Proof: $[K : K']$ is a Galois extension, because there is a surjection $K \otimes_k K \to K \otimes_{K'} K$. Since $G' = \mathrm{Aut}_{K'}(K)$, Corollary 1 applied to the Galois extension $[K : K']$ gives $K^{G'} = K'$. ■

THEOREM: (Main theorem of Galois theory)
Let $[K : k]$ be a Galois extension, and $\mathcal{G}al_k K$ its Galois group. **Then the subgroups $H \subset \mathcal{G}al_k K$ are in bijective correspondence with the intermediate subfields $k \subset K^H \subset K$,** with K^H obtained as the set of H-invariant elements of K.

Proof: Follows from the previous lemma. ■

EXERCISE: Prove that for any $q = p^n$ there exists a finite field $\mathbb{F}_q$ of q elements. Prove that $[\mathbb{F}_q : \mathbb{F}_p]$ is a Galois extension. Prove that its Galois group is cyclic of order n, and generated by **the Frobenius automorphism** mapping x to x^p.