Today we change topics from Representation Theory (lectures 1–14) to Galois Theory (lectures 15–25).

1 Field extensions

Let K be a *field*, which we recall is a set with addition and multiplication operations, such that

- it is an abelian group under addition, with additive identity called 0;
- the nonzero elements form an abelian group under multiplication; and
- multiplication distributes over addition.

Alternatively: a commutative ring in which $0 \neq 1$ and all nonzero elements have multiplicative inverses.

There are many well-known infinite fields like $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the p-adic numbers $\mathbb{Q}_p$.

As we shall see, there is also a finite field $\mathbb{F}_q$ of each prime power order q.

A *homomorphism* of fields is a ring homomorphism from one field to another.

Such a map is required to send 0 and 1 in the domain field to the corresponding units in the codomain.

Lemma. Every field homomorphism is injective.

Proof. If $f : K \to K'$ is a field homomorphism and $f(a) = f(b)$ then $f(a-b) = 0$.

In this case $a - b = 0$ since otherwise we would have $1 = f(1) = f((a-b)^{-1})f(a-b) = 0$. □

A *field extension* of K, or *K-extension*, is an (injective) field homomorphism

$$K \hookrightarrow M$$

This injection makes M into a K-vector space.

Specifically, if ι is the map $K \to M$ then the vector space structure is defined by setting $km = \iota(k)m$.

We usually abbreviate by writing $M \mid K$ to denote a field extension $K \hookrightarrow M$.

We generally do not give any special symbol for the map itself $K \hookrightarrow M$.

We can always identify K with its image under $K \hookrightarrow M$ in order to view $K \subseteq M$ as a subset of M.

A homomorphism from one field extension $M \mid K$ to another field extension $M' \mid K$ is a field homomorphism $M \to M'$ (which is necessarily injective), which makes the diagram

$$\begin{array}{ccc} K & \longrightarrow & M \\ & \searrow & \downarrow \\ & & M' \end{array}$$

commute. An *isomorphism* of field extensions over K is a homomorphism that is a bijection.

Let $\mathrm{Aut}_K(M)$ be the group of isomorphisms of field extensions $M \mid K \to M \mid K$.

The group law is composition of maps.

In other words, the group $\mathrm{Aut}_K(M)$ is the subgroup of all K-linear ring automorphisms of M.

Remark. If $f : M \to M$ is a K-linear map then $\boxed{\dim_K \ker(f) + \dim_K \text{image}(f) = \dim_K M}$.

When f is a homomorphism $M \mid K \to M \mid K$ we have $\ker(f) = 0$ and therefore $\text{image}(f) = M$.

Thus every homomorphism of a field extension to itself is an isomorphism.

Example. Not every homomorphism from a field to itself is an isomorphism. Surjectivity can fail.

Consider the field $K = \mathbb{Q}(x_1, x_2, x_3, \dots)$ rational functions in infinitely many variables.

Then examine the operation that sends every variable $x_i \mapsto x_{i+1}$ for all i.

Check that this is a field homomorphism $K \to K$ whose image does not contain x_1.

We say that a field extension $M \mid K$ is *finite* if $\dim_K(M) < \infty$.

Write $[M : K]$ for $\dim_K(M)$. The integer $[M : K]$ is called the *degree* of the extension $M \mid K$.

Proposition. If $L \mid M$ and $M \mid K$ are finite field extensions then

$$[M : K] \cdot [L : M] = [L : K].$$

More precisely, if

- $m_1, m_2, \dots, m_s$ is a basis of M as a K-vector space, and
- $l_1, l_2, \dots, l_t$ is a basis of L as a M-vector space,

then the set $\{m_i l_j\}_{(i,j)\in[s]\times[t]}$ is a basis for L as a K-vector space.

Proof. Exercise. □

Let $M \mid K$ be a field extension and let $a \in M$. The *annihilator* of a is

$$\text{Ann}(a) = \{P(x) \in K[x] : P(a) = 0\}$$

This set is an ideal of the polynomial ring $K[x]$.

The element a is *transcendental* over K if $\text{Ann}(a) = 0$.

We say that a is *algebraic* over K if $\text{Ann}(a) \neq 0$.

If a is algebraic over K, then there is a unique monic polynomial which generates $\text{Ann}(a)$.

We denote this by m_a and call it the *minimal polynomial* of a.

The minimal polynomial has the property that it divides any polynomial in $\text{Ann}(a)$.

(See the next homework assignment.)

Remark. The ideal $\text{Ann}(a)$ is prime.

This holds as there is an injection $K[x]/\text{Ann}(a) \hookrightarrow M$ and M is an integral domain.

In fact, one can show that $\text{Ann}(a)$ is a maximal ideal.

Also, one can prove that if a is algebraic then m_a is the unique monic irreducible polynomial in $\text{Ann}(a)$.

A field extension $M \mid K$ is *algebraic* if for all $a \in M$ the element a is algebraic over K.

We say that a field extension $M \mid K$ is *transcendental* if it is not algebraic over K.

Lemma. If $M \mid K$ is finite in the sense that $[M : K] = \dim_K(M) < \infty$ then $M \mid K$ is algebraic.

Proof. Let $m \in M$. Suppose that m is transcendental over K.

Then the map $P(x) \mapsto P(m)$ is an injection of K-vector spaces $K[x] \hookrightarrow M$.

Since $K[x]$ is infinite-dimensional, this contradicts the fact that $\dim_K(M) < \infty$. □

2 Separability

Continue to let K be a field. Let $P(x) \in K[x]$ be a 1-variable polynomial. Suppose that

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$$

for some coefficients $a_0, a_1, \ldots, a_d \in K$. We define

$$P'(x) = \tfrac{d}{dx} P(x) := d a_d x^{d-1} + (d-1) a_{d-1} x^{d-2} + \cdots + a_1.$$

Here each integer $d - i$ is understood as the field element $1_K + \cdots + 1_K$ with $(d-i)$-summands.

The operation $P(x) \mapsto P'(x)$ is a formal analogue of the derivation from analysis.

It satisfies similar formal rules. It is a K-linear map from $K[x]$ to $K[x]$ and it satisfies the *Leibniz rule*

$$(P(x)Q(x))' = P'(x)Q(x) + P(x)Q'(x).$$

Definition. Let $(P(x), P'(x))$ denote the ideal of $K[x]$ generated by $P(x)$ and $P'(x)$

We say that $P(x)$ *has no multiple roots* if $(P(x), P'(x)) = K[x]$.

Otherwise, we say that $P(x)$ *has multiple roots*.

Equivalently, $P(x)$ has multiple roots if and only if $\gcd(P(x), P'(x)) \neq 1$.

The following exercise justifies this terminology: if

$$P(x) = (x - \rho_1)(x - \rho_2) \cdots (x - \rho_d)$$

then $P(x)$ has multiple roots (in the above sense) if and only if there are indices $i \neq j$ with $\rho_i = \rho_j$.

Lemma. Let $L \mid K$ be a field extension and suppose $P(x), Q(x) \in K[x]$.

Write $\gcd_L(P(x), Q(x))$ for the gcd of $P(x)$ and $Q(x)$ viewed as elements of $L[x]$. Then

$$\gcd(P(x), Q(x)) = \gcd_L(P(x), Q(x)).$$

Proof. We prove this by computing a generator of $(P(x), Q(x))$ using *Euclidean division*.

First view $P(x)$ as having coefficients in K. We may assume $\deg(Q) \leq \deg(P)$.

Apply Euclidean division and write

$$P = Q_1 Q + R_1$$

We then have $(P, Q) = (Q, R_1)$. Note that $\deg(R_1) < \deg(Q) \leq \deg(P)$.

Now apply Euclidean division again and write

$$\begin{aligned} Q &= Q_2 R_1 + R_2, \\ R_1 &= Q_3 R_2 + R_3, \\ R_2 &= Q_4 R_3 + R_4, \end{aligned}$$

and so on. Then we have

$$(Q, R_1) = (R_1, R_2) = (R_2, R_3) = \cdots \quad \text{and} \quad \deg(Q) > \deg(R_1) > \deg(R_2) > \deg(R_3) > \cdots .$$

Since the sequence of the $\deg(R_i)$ is strictly decreasing, some $k \geq 1$ must have $R_k = 0$.

But then we have $(P, Q) = (R_{k-1}, R_k) = (R_{k-1})$.

In other words, R_{k-1} is a generator of (P, Q).

Thus the polynomial $\gcd(P(x), Q(x))$ is the polynomial R_{k-1} divided by its highest nonzero coefficient.

By the uniqueness of the quotient and remainder in Euclidean division, if we view $P(x)$ and $Q(x)$ as polynomials with coefficients in L and apply the same procedure, we will obtain the same sequence of R_i.

We conclude that $\gcd(P(x), Q(x)) = \gcd_L(P(x), Q(x))$. □

The lemma has this immediate consequence:

Corollary. Let K be a field and choose $P(x) \in K[x]$. Let $L \mid K$ be a a field extension. Then:

(a) The polynomial $P(x)$ has multiple roots as a polynomial with coefficients in K if and only if it has multiple roots as a polynomial with coefficients in L.

(b) If we can write $P(x) = (x - \rho_1)(x - \rho_2) \cdots (x - \rho_d)$ for some $\rho_i \in L$, then $P(x)$ has multiple roots as a polynomial with coefficients in K if and only if there are indices $i \neq j$ with $\rho_i = \rho_j$.

Lemma. Let $P(x), Q(x) \in K[x]$ and suppose that $Q(x)$ divides $P(x)$.

Assume $P(x)$ has no multiple roots. Then $Q(x)$ also has no multiple roots.

Proof. Let $T(x) \in K[x]$ be such that $Q(x)T(x) = P(x)$. Then by the Leibniz rule

$$K[x] = (P, P') = (QT, Q'T + QT').$$

Now suppose Q, Q' are both divisible by a polynomial $W(x)$ with positive degree.

Then $Q'T + QT'$ and QT are also divisible by $W(x)$.

But this means $1 \in (QT, Q'T + QT')$ is divisible by $W(x)$, which is a contradiction. □

Lemma. Suppose that K is a field and that $P(x) \in K[x] \backslash \{0\}$.

Suppose that $\mathrm{char}(K)$ does not divide $\deg(P)$ and that $P(x)$ is irreducible. Then $(P, P') = K[x]$.

Proof. Write

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$$

where $a_d \neq 0$. By definition, we have

$$P'(x) = d a_d x^{d-1} + (d-1) a_{d-1} x^{d-2} + \cdots + a_1.$$

By assumption, we have $(d, \mathrm{char}(K)) = (1)$ and so we see that $d \neq 0 \in K$. Thus $P'(x) \neq 0$.

Now, recall that P is irreducible.

Hence any common divisor of P and P' must be either a nonzero constant, or P times a nonzero constant.

But such a divisor cannot be equal to P times a nonzero constant as $\deg(P') < \deg(P)$.

Hence it must be a nonzero constant. In particular, $(P, P') = K[x]$. □

Continue to let K be a field.

Definition. A polynomial in $K[x] \setminus \{0\}$ is *separable* if all of its irreducible factors have no multiple roots.

The results above show that this notion is invariant under field extension.

Also, we have seen that an irreducible polynomial with coefficients in K, whose degree is not divisible by the characteristic of K, is separable.

In particular, if $\mathrm{char}(K) = 0$, then any irreducible polynomial with coefficients in K is separable.

Let $L \mid K$ be an algebraic field extension.

Definition. $L \mid K$ is *separable* if the minimal polynomial over K of any element of L is separable.

Note that if K is a field and $\mathrm{char}(K) = 0$, then all the algebraic extensions of K are separable.

Lemma. let $M \mid L$ and $L \mid K$ be algebraic field extensions.

Suppose $M \mid K$ is separable. Then $M \mid L$ and $L \mid K$ are both separable.

Proof. Clearly $L \mid K$ is separable. So let $m \in M$ and let $P(x) \in K[x]$ be its minimal polynomial over K.

Let $Q(x)$ be the minimal polynomial of m over L. Then $Q(x)$ divides $P(x)$.

By assumption $P(x)$ has no multiple roots over K and so $P(x)$ also has no multiple roots over L.

Then by our lemmas $Q(x)$ also has no multiple roots over L, so it is separable.

Since $m \in M$ was arbitrary, $M \mid L$ is separable. □

Example. The following is a finite field extension that is not separable.

Let $K := \mathbb{F}_2(t)$, where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ is the field with two elements.

Let $P(x) := x^2 - t$. Since $P(x)$ is of degree 2 and has no roots in K, it is irreducible.

Let $L := K[x]/(P(x))$. Since $P(x)$ is irreducible, the ideal $(P(x))$ is maximal and L is a field.

On the other hand, $P'(x) = 0$ so $(P', P) = (P) \neq L[X]$ so $P(x)$ is not separable.

Now $P(x)$ is the minimal polynomial of $x + (P(x)) \in K[x]/(P(x)) = L$.

Hence the extension $L \mid K$ is not separable.