5. Field Theory Basics

Basics of field theory

Things to remember from before.

We already know quite a bit about fields.

Characteristic

If F is a field, then there is a ring homomorphism $\mathbb{Z} \to F$ sending $1 \to 1$. If this map is injective, then:

- we say F has *characteristic zero*
- F contains a copy of the rational numbers
- The field $\mathbb{Q}$ is the *prime subfield* of F.

Otherwise the kernel of this map must be a prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$. In this case:

- we say that F has *characteristic* p
- F contains a copy of $\mathbb{Z}/p\mathbb{Z}$.
- $\mathbb{Z}/p\mathbb{Z}$ is the *prime subfield* of F.

Maps

If $f : F \to E$ is a homomorphism of fields, it is automatically injective (or zero).

The only field maps $f : \mathbb{Q} \to \mathbb{Q}$ and $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ are the identity.

Extensions

If F is a field, and $F \subset E$ where E is another field, then we call E an extension field of F.

E is automatically a vector space over F. The degree of E/F, written $[E : F]$, is the dimension of E as an F-vector space.

Polynomials, quotient rings, and fields

We have the division algorithm for polynomials. $F[x]$ is a PID. An ideal is prime iff it is generated by an irreducible polynomial.

Let $p(x)$ be an irreducible polynomial of degree d over F. Then:

- $K = F[x]/(p(x))$ is a field
- It is of degree d over F.
- $p(x)$ has a root in K (namely the residue class of x)
- The elements $1, x, \ldots, x^{d-1}$ are a basis for K/F.

Adjoining roots of polynomials

If $F \subset K$ is a field extension, and $\alpha \in K$, then $F(\alpha)$ is the smallest subfield of K containing F and α. Similarly for $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

If $p(x)$ is irreducible over F, and has a root α in K, then $F(\alpha)$ is isomorphic to $F[x]/p(x)$ via the map $x \mapsto \alpha$.

Key Theorem

Let K be a field extension of F and let $p(x)$ be an irreducible polynomial over F. Suppose K contains two roots α and β of $p(x)$. Then $F(\alpha)$ and $F(\beta)$ are isomorphic via an isomorphism that is the identity on F.

More generally:

Theorem: (See Theorem 8, DF, page 519) Let $\phi : F \to F'$ be an isomorphism of fields. Let $p(x)$ be an irreducible polynomial in $F[x]$ and let $p'(x)$ be the polynomial in $F'[x]$ obtained by applying ϕ to the coefficients of $p(x)$. Let K be an extension of F containing a root α of $p(x)$, and let K' be an extension of F' containing a root β of $p'(x)$. Then there is an isomorphism $\sigma : F(\alpha) \to F'(\beta)$ such that the restriction of σ to F is ϕ.

Algebraic Extensions

Definition

Definition: Let $F \subset K$ be a field extension. An element $\alpha \in K$ is *algebraic* over F if it is the root of a nonzero polynomial in $F[x]$. Elements that aren't algebraic are called *transcendental.*

An extension K/F is algebraic if every element of K is algebraic over F.

Basics

- If α is algebraic over F, there is unique monic polynomial $m_{\alpha,F}(x)$ of minimal degree with coefficients in F such that $m_\alpha(\alpha) = 0$. (This follows from the division algorithm). This polynomial is called the *minimal polynomial* of α over F. Its degree is the *degree* of α.
- If $F \subset L$, then the minimal polynomial $m_{\alpha,L}(x) \in L[x]$ of α over L divides the minimal polynomial $m_{\alpha,F}(x)$. Again, this follows from the division algorithm for $L[x]$.
- $F(\alpha)$ is isomorphic to $F[x]/m_{\alpha,F}(x)$; and the degree $[F(\alpha) : F]$ is the degree of α.

Examples

If $n > 1$ and p is a prime, then the polynomial $x^n - p$ is irreducible over $\mathbb{Q}$, so $\alpha = \sqrt[n]{p}$ has degree n over $\mathbb{Q}$.

The polynomial $x^3 - x - 1$ is irreducible over $\mathbb{Q}$ and has one real root α. So α has degree 3 over $\mathbb{Q}$ but degree 1 over $\mathbb{R}$.

Finite extensions are algebraic

Suppose K/F is finite and let α be an element of K. Then there is an n so that the set $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent over F; so α satisfies a polynomial with F coefficients, and is therefore algebraic.

As a partial converse, if $F(\alpha)/F$ is finite if and only if α is algebraic. If α is algebraic of degree d over F, $F(\alpha) = F[x]/(m_\alpha(x))$ which is finite dimensional (with basis $1, x, x^2, \ldots, x^{d-1}$.)

Algebraic over algebraic is algebraic

Proposition: If K/F is algebraic and L/K is algebraic then L/F is algebraic.

Proof: Let α be any element of L. It has a minimal polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with the $a_i \in K$. Therefore α is algebraic over $F(a_0, \ldots, a_{d-1})$. Since the a_i are in K, they are algebraic over F, and therefore $F(a_0, \ldots, a_{d-1})$ is finite over F and so is $F(\alpha, a_0, \ldots, a_{d-1})$. Thus $F(\alpha)$ is contained in a finite extension of F and so α is algebraic over F.

Field Degrees

Multiplicativity of degrees

Proposition: Suppose that L/F and K/L are extensions. Then $[K : F] = [K : L][L : F]$.

Proof: If $\alpha_1, \ldots, \alpha_n$ are a basis for L/F, and $\beta_1, \ldots, \beta_k$ are a basis for K/L, then the products $\alpha_i\beta_j$ are a basis for K/F.

Corollary: If L/F is a subfield of K/F, then $[L : F]$ divides $[K : F]$.

Finitely generated extensions

A field K/F is finitely generated if $K = F(\alpha_1, \ldots, \alpha_n)$ for a finite set of α_i in K.

Proposition: $F(\alpha, \beta) = F(\alpha)(\beta)$.

Proof: $F(\alpha, \beta)$ contains $F(\alpha)$ and also β. Therefore $F(\alpha)(\beta) \subset F(\alpha, \beta)$. On the other hand, since α and β are in $F(\alpha)(\beta)$, we know that $F(\alpha, \beta) \subset F(\alpha)(\beta)$.

Finite is finitely generated

Proposition: A field K/F is finite if and only if it is finitely generated. If it is generated by $\alpha_1, \ldots, \alpha_k$ then it is of degree at most $n_1 n_2 \ldots n_k$ where n_i is the degree of α_i over F.

Proof: If it's finitely generated, then it's a sequence of extensions $F(\alpha_1, \ldots, \alpha_{s-1})(\alpha_s)$ each of degree at most n_i. So K/F is finite. Conversely, if K/F is finite (and of degree greater than 1), choose $\alpha_1 \in K$ of degree greater than 1. Then $F(\alpha) \subset K$ and $[K : F(\alpha)]$ is smaller than $[K : F]$. Now choose α_2 in K but not $F(\alpha_1)$, and so on. This process must terminate.

Corollary: If α and β are algebraic over F, so are $\alpha + \beta$, $\alpha\beta$, and (if $\beta \neq 0$) α/β.

Proof: All these elements lie in $F(\alpha, \beta)$ which is finite over F.

Corollary: If K/F is a field extension, the subset of K consisting of algebraic elements over F is a field (called the *algebraic closure of F in K*).

Towers of algebraic extensions are algebraic

Propositoin: If L/K is algebraic and K/F is algebraic so is L/F.

Proof: Choose $\alpha \in L$. Then α satisfies a polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ where the a_i are in K. Therefore α is algebraic over $E = F(a_0, a_1, \ldots, a_{d-1})$. But E/F is finitely generated hence finite. Therefore $[E(\alpha) : F] = [E(\alpha) : E][E : F]$ is finite. Thus every element of L is algebraic over F.

Composites

If K_1 and K_2 are subfields of a field K, then K_1K_2 is the smallest subfield of K containing these two fields. Then $[K_1K_2 : F]$ is divisible by both $[K_1 : F]$ and $[K_2 : F]$ and in addition

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F].$$

In particular, if $[K_1 : F]$ and $[K_2 : F]$ are relatively prime, then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

Classical Constructions (Ruler and Compass)

Classical ruler and compass constructions allow one to:

- find the point of intersection of two lines.
- find the point of intersection of a line and a circle.
- find the points of intersection of two circles.

Constructions

If we begin with a line segment of length 1, we can:

- construct a perpendicular, and then construct all integer lengths along that line
- construct all points with integer coordinates in the plane
- using similar triangles, construct all points in the plane with rational coordinates

Extensions

Now suppose we can construct all points with coordinates in a field F. Then:

- intersections of lines joining points of over F meet in points with coordinates in F
- intersections of a line joining two points with coordinates in F with a circle of radius in F yields points in a quadratic extension of F.
- intersections of two circles with radii in F yields points with coordinates in a quadratic extension of F.

Gauss's Theorem on constructibility

Theorem: If a line segment of length α is constructible by ruler and compass, then α lies in a field obtained from $\mathbb{Q}$ by a sequence of quadratic extensions, and $[F(\alpha) : F] = 2^k$ for some integer $k \geq 0$.

Corollary: One cannot "double the cube" , trisect an angle, or square the circle.

Here doubling the cube means given a length α construct a length β so that the cube with side length β has double the volume of the cube with side length α. This is impossible because $\sqrt[3]{2}$ does not meet Gauss's criterion.

Squaring the circle means, given α, constructing a length β so that a square of side β has the same area as a circle of radius α. This is impossible because π is not algebraic (we won't prove this).

Trisecting the angle means constructing an angle with one-third the measure of a given angle θ. If we can trisect θ, we can construct a length of $\cos(\theta/3)$. If $\theta = \pi/3$, then $\theta/3 = \pi/9$ or $\beta = \cos 20^\circ$. One can show that, if $u = 2\beta$, then

$$u^3 - 3u - 1 = 0.$$

This polynomial has no rational roots (it is irreducible mod 2 for example).

A pentagon is constructible because the $\cos(2\pi/5)$ is the root of a quadratic polynomial.

View as slides