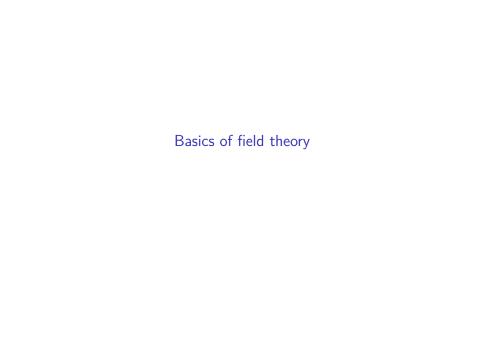
# 5. Field Theory Basics



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  $\mathbb{Z}/p\mathbb{Z}$ .
- $ightharpoonup \mathbb{Z}/p\mathbb{Z}$  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:

- ightharpoonup K = F[x]/(p(x)) is a field
- ▶ It is of degree *d* over *F*.
- ightharpoonup p(x) has a root in K (namely the residue class of x)
- ▶ The elements  $1, x, ..., x^{d-1}$  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  $\alpha$ . Similarly for  $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ .

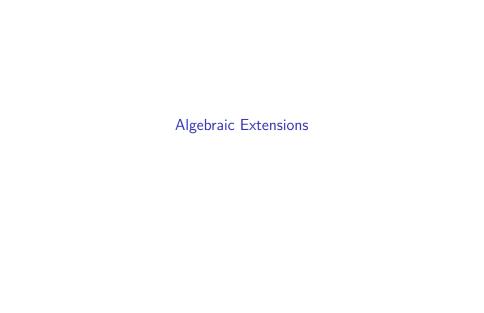
If p(x) is irreducible over F, and has a root  $\alpha$  in K, then  $F(\alpha)$  is isomorphic to F[x]/p(x) via the map  $x \mapsto \alpha$ .

# 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  $\alpha$  and  $\beta$  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  $\phi$  to the coefficients of p(x). Let K be an extension of F containing a root  $\alpha$  of p(x), and let K' be an extension of F' containing a root  $\beta$  of p'(x). Then there is an isomorphism  $\sigma: F(\alpha) \to F'(\beta)$  such that the restriction of  $\sigma$  to F is  $\phi$ .



### 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  $\alpha$  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  $\alpha$  over F. Its degree is the *degree* of  $\alpha$ .
- ▶ If  $F \subset L$ , then the minimal polynomial  $m_{\alpha,L}(x) \in L[x]$  of  $\alpha$  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  $\alpha$ .

# 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  $\alpha$ . So  $\alpha$  has degree 3 over  $\mathbb Q$  but degree 1 over  $\mathbb R$ .

# Finite extensions are algebraic

Suppose K/F is finite and let  $\alpha$  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  $\alpha$  satisfies a polynomial with F coefficients, and is therefore algebraic.

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

# 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  $\alpha_i \beta_i$  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  $K = F(\alpha_1, \dots, \alpha_n)$  for a finite set of  $\alpha_i$  in K.

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

**Proof:**  $F(\alpha, \beta)$  contains  $F(\alpha)$  and also  $\beta$ . Therefore  $F(\alpha)(\beta) \subset F(\alpha, \beta)$ . On the other hand, since  $\alpha$  and  $\beta$  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  $\alpha_i$  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  $\alpha_2$  in K but not  $F(\alpha_1)$ , and so on. This process must terminate.

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

**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

**Proposition:** If L/K is algebraic and K/F is algebraic so is L/F.

**Proof:** Choose  $\alpha \in L$ . Then  $\alpha$  satisfies a polynomial  $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$  where the  $a_i$  are in K. Therefore  $\alpha$  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  $[K_1K_2 : F] = [K_1 : F][K_2 : F]$ .