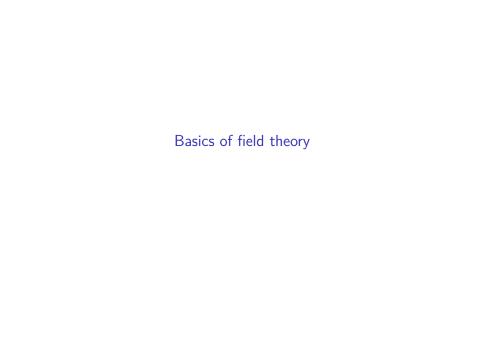
5. Field Theory Basics



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 $f:\mathbb{Z}/p/Z\to\mathbb{Z}/p\mathbb{Z}$ 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 α . Similarly for $F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

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 .