4. Fields

4.1 Fields

$(F, +, \cdot)$ is a field $\iff$

1. $(F, +)$ = abelian group
2. $(F^*, \cdot)$ = abelian group
3. $a(b+c) = ab + ac\ \forall a, b, c \in F$

4.2 Extension Fields

Definition -- Extension fields
A field E is an extension field of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F.

Example: $\mathbb{C}$ is an extension of $\mathbb{R}$
Example

1. For the field $\mathbb{Q}$ the smallest extension field that contains $\sqrt{2}$ is $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
   $\mathbb{Q}(\sqrt{2})$ has the roots of $f(x) = x^2 - 2) \Rightarrow$ **splitting field**
2. For the field $\mathbb{Q}$ the smallest extension field that contains $i = \sqrt{-1}$ is $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$
3. We can adjoin the fields $\Rightarrow \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$
   An element $\underbrace{\alpha + \beta i}_{\alpha, \beta \in \mathbb{Q}(\sqrt{2})} = (a + b\sqrt{2}) + (c + d\sqrt{2})i$ with $a, b, c, d \in \mathbb{Q} \Rightarrow \{1, \sqrt{2}, i, i\sqrt{2}\}$ is a **basis** for our extension field

4.2.1 Algebraic extensions

- https://en.wikipedia.org/wiki/Algebraic_element
- https://en.wikipedia.org/wiki/Algebraic_extension

Let E be an extension field of a field F

Algebraic element
Let $a \in E$.
We call a **algebraic** over F if a is the zero of some nonzero polynomial in $F[x]$

$$\exists g(x) \in F, g(x) \neq 0\ s.t.\ g(a) = 0$$

If a is not algebraic over F, it is called **transcendental** over F.

Algebraic extension
An extension E of F is called an **algebraic extension** of F if every element of E is algebraic over F.
If E is not an algebraic extension of F, it is called a **transcendental extension** of F.

An extension of F of the form $F(a)$ is called a simple extension of F.

Ex: $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since is the root of $x^2 - 2$

4.3 Field automorphisms

.

Let F be a field
A **field automorphism** is a bijection $f : F \to F$ s.t $\forall a, b \in F$

- $f(a+b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$

Property
If f is an automorphism of an extension field F of $\mathbb{Q}$ then $f(q) = q\ \forall q \in \mathbb{Q}$

Intuition
The automorphism fixes everything in $\mathbb{Q}$
Proof
Suppose $f(1) = q$
$q = f(1) = f(1 \cdot 1) = f(1)f(1) = q^2$
$q = f(1) = f(1 \cdot 1 \cdot 1) = f(1)f(1)f(1) = q^3$
...
$\Rightarrow q^n = q \Rightarrow q = 1$

Perfect fields

F is called perfect if $charF = 0$ or char $charF = p$ and $F^p = \{a^p : a \in F\} = F$

Theorem

> Every finite field is perfect

Proof
Let $\phi(x) = x^p$ be a mapping. We want to prove ϕ is an automorphism

- $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$
- $\phi(a+b) = (a+b)^p = a^p + \binom{p}{1}a^{p-1}b + ... + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p$ (since $p|\binom{p}{i}$)
- Since $x^p \neq 0$ when $x \neq 0 => Ker\phi = \{0\} \Rightarrow \phi$ is injective
- F is finite => ϕ is surjective
- ϕ is bijective therefore an automorphism therefore $F^p = F$

Finite fields

> For each prime p and $n > 0$ there is, a unique finite field of order p^n

Structure

> As addition: $GF(p^n) \approx \underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus ... \oplus \mathbb{Z}_p}_{n \text{ times}}$
> As multiplication $GF(p^n) \approx \mathbb{Z}_{p^n-1}$

Subfields

> For each divisor $m|n$ $GF(p^n)$ has a unique subfield of order p^m
> These are the only subfields of $GF(p^n)$

Proof

- $p^n - 1 = (p^m - 1)(p^{n-m} + ... + p^m + 1) \Rightarrow p^m - 1|p^n - 1 \Rightarrow p^n - 1 = (p^m - 1)t$
- Let $K = \{x \in GF(p^m) : x^{p^m} = x\}$
  - $x^{p^m} - x$ has at most p^m zeros in $GF(p^n) \Rightarrow |K| \leq p^m$
  - Let $\langle a \rangle = GF(p^n)^* \Rightarrow |a^t| = p^m - 1$ and $(a^t)^{p^m-1} = 1 => a^t \in K$
  - So K is a subfield of $GF(p^n)$ of order p^m