# Fields

Recall that a set $F$ is a field p.t

① $\exists$ bin operations $+, \cdot$ on $F$ s.t

a) $(F, +)$ is an abelian grp with identity $0$ $(0 \in F)$

b) $(F \setminus \{0\}, \cdot)$ is an abelian grp with identity $1$ $(1 \in F)$

c) $\forall a, b, c \in F$ $a \cdot (b+c) = a \cdot b + c \cdot a$

d) $0 \neq 1$ (redundant)

**Remark** as $0, 1 \in F$ $|F| \geq 2$ e.g $\mathbb{Z}/2\mathbb{Z}$

**Claim** $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots \overline{p-1}\}$ is a field iff $p$ is prime

**Pf** It is immediate that $(\mathbb{Z}/p\mathbb{Z}, + \bmod p)$ is an abelian grp.

Also, we have that $\bar{1}$ is the multiplicative identity, closure & associativity of $\cdot \bmod p$

We only need inverses!

Let $\bar{m} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ we must find at $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ st $a \cdot m \equiv 0$

As $m \not\equiv 0 \bmod p$ & $p$ is prime, $\gcd(m, p) = 1$

$\exists a, b \in \mathbb{Z}$ s.t $1 = am + bp$ as $bp \equiv 0 \bmod p$

$1 \equiv a \cdot m \bmod p$

So we are done and

$(\mathbb{Z}/p\mathbb{Z}, + \bmod p, \cdot \bmod p)$ is a field!

$\Leftarrow$ if $p$ isn't prime, we don't have closure or inverses.

$p = a \cdot b$ for $a, b < p \Rightarrow \bar{a} \cdot \bar{b} = p \equiv 0 \bmod p$

Claim if $x \in \mathbb{Z}/p\mathbb{Z}$ st $\gcd(x, p) = y \neq 1$ then no inv as $\exists$ nonzero $z \in \mathbb{Z}/p\mathbb{Z}$ $x \cdot z = p$. If we have an inv $z = x^{-1} p \Rightarrow z \equiv 0 \bmod p$ oops.

if it is 1 the bezout gives inv

# Characteristic

**Lemma** Suppose $F$ is a field $\exists!$ function

$$\varphi : \mathbb{Z} \to F$$

s.t.

1. $\varphi(n+m) = \varphi(n) +_F \varphi(m)$
2. $\varphi(n \cdot m) = \varphi(n) \cdot_F \varphi(m)$
3. $\varphi(1) = 1_F$

$\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0) = 2\varphi(0) \Rightarrow$ add additive inv $\Rightarrow \varphi(0) = 0_F$

note: (1) + (2) $\Rightarrow \varphi(0) = 0_F$ but not preserving mult identity which is why we have (3)

**Defn** A function $\varphi : F_1 \to F_2$ that satisfies (1), (2), (3) is a field/ring homomorphism!

So above is a ring homomorphism as $(\mathbb{Z}, +, \cdot)$ is a ring!

**Pf** (1) Existence (2) Uniqueness

(1) Consider

$$\varphi : \mathbb{Z} \to F$$

$$n \mapsto \begin{cases} 0 & n = 0 \\ \underbrace{1_F + 1_F + \cdots + 1_F}_{n} & n > 0 \\ -\varphi(-n) & n < 0 \end{cases}$$

This function satisfies everything we want!

Why is this unique? We didn't have any choice...

In fact we only need to define it for $n \geq 0$ and the rest is forced!

**Lemma** Suppose $F_1, F_2$ are fields & $\varphi: F_1 \to F_2$ is a ring homomorphism

↳ not true in prev case as $\mathbb{Z}$ not a field

Then $\varphi$ is inj

**Pf** Suppose not, $\Rightarrow$ distinct $a, b \in F_1$ s.t. $\varphi(a) = \varphi(b)$

$$0_{F_2} = \varphi(a) - \varphi(b) = \varphi(a) + \varphi(-b)$$
$$= \varphi(a-b)$$

↳ nonzero so $\exists$ mult inv in $F_1$

$$1_{F_2} = \varphi(1_{F_1})$$
$$= \varphi((a-b)\cdot(a-b)^{-1})$$
$$= \varphi(a-b)\cdot\varphi((a-b)^{-1})$$
$$= 0_{F_2}\cdot\varphi((a-b)^{-1}) = 0_{F_2}$$ oops □

**Lemma** Suppose $\varphi: \mathbb{Z} \to F$ is a ring homo described earlier Then,

$\ker(\varphi) = \{0\}$ or $\ker(\varphi) = p\mathbb{Z}$ for prime $p$

**Pf** Suppose $\ker(\varphi) \neq \{0\}$

As $\varphi: \mathbb{Z} \to F$ is a homomorphism wrt grps, $\ker(\varphi)$ is a subgp!

By new, $\ker(\varphi) = n\mathbb{Z}$ for $n \in \mathbb{N}$

Can $n = 1$? No, as $n=1 \Rightarrow \ker(\varphi) = \mathbb{Z} \Rightarrow \varphi(a) = 0_F$ $\forall a \in \mathbb{Z}$

but this is false as $\varphi(1) = 1_F$

So $n > 1$, lets show it is prime!

Let $a \cdot b \in \mathbb{N}$ s.t. $n = a \cdot b \Rightarrow 1 \leq a, b \leq n$

We see $\varphi(n) = \varphi(a)\cdot\varphi(b)$

$$0_F = \varphi(a)\cdot\varphi(b) \Rightarrow \varphi(n) = 0 \text{ or } \varphi(b) = 0$$

WLOG, $a \in \ker(\varphi) \Rightarrow a \in n\mathbb{Z} \Rightarrow a = cn$ for $c \in \mathbb{Z}$

$\Rightarrow c = 1 \Rightarrow$ n is prime

So, if

$\varphi : \mathbb{Z} \to F$ is not injective, $\ker(\varphi) = p\mathbb{Z}$ for prime $p$!

**Defn** Let $F$ be a field, consider the unique ring homomorphism

$\varphi : \mathbb{Z} \to F$

If $\varphi$ is injective $\iff \ker(\varphi) = \{0\}$ then $F$ has char 0.

Else, $\ker(\varphi) = p\mathbb{Z}$ and $F$ has char $p$

↓ $p \in$ primes

**Remark** if $F$ has char $p$, then

$$\underbrace{1_F + 1_F + \cdots 1_F}_{p \text{ times}} = 0_F$$

and $\underbrace{1_F + 1_F + \cdots 1_F}_{n \text{ times}} = 0_F \implies p \mid n$

→ immediate from considering $\varphi$!

**Eg** $\mathbb{Z}/p\mathbb{Z}$ has char $p$

$\mathbb{R}, \mathbb{Q}, \mathbb{C}$ have char 0

If $F$ is finite, it must have a nonzero char as $\varphi$ isn't injective!

**Q** can non-finite fields have non-zero char?

Yes!

# Polynomials

A polynomial over field $F$ is an expression

$a_n x^n + \cdots + a_1 x + a_0$

where $n \in \mathbb{N} \cup \{0\}$ $\quad a_n \in F \ \forall \ n \in \mathbb{N}_n \cup \{0\}$

This is **not the same as** a poly func

E.g $f, g : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$

with $f(x) = x^3 + x \qquad g(x) = 2x$

are **identically equal as poly func** but **not polys**

note: polys give rise to poly funcs! $\to$ $F \to F$, $a \mapsto p(a)$

note: the 0 polynomial is called the **trivial polynomial**!

**Defn** A non trivial polynomial can be written as

$$b(x) = b_0 + b_1 x + \cdots + b_\ell x^\ell$$

with $b_\ell \neq 0$

In this case, $b$ **has degree $\ell$**

**By convention**: The degree of the trivial poly is $(-\infty)$ or $-1$

↳ we'll stick with this!

**Remark** let $p, q$ be polynomials

$$\deg(p \cdot q) = \deg(p) + \deg(q)$$

Since we have that the degree of the trivial poly is $-\infty$ this **works in all cases!**

**Defn** We denote $F[x]$, the **set of all poly with coeff in $F$.**

↳ variable $x$

**Lemma** if $p, q \in F[x]$, $c \in F$

1. $p+q \in F[x]$
2. $pq \in F[x]$
3. $cp \in F[x]$

**Pf** obvious!

**Lemma** If $\alpha \in F$, $p \in F[x]$ & $p$ is non-zero

Then

$p(\alpha) = 0 \iff \exists\, q \in F[x]$ with $\deg(q) = \deg(p) - 1$

so, $p = (x-\alpha)(q)$

**Pf** $\Leftarrow$ immediate

$\Rightarrow$ Since $p$ is nontrivial. Space $\deg(p) = n \in \mathbb{N} \cup \{0\}$

So

$$p(x) = c_n x^n + \dots + c_1 x + c_0$$

with $c_i \in F$, $c_n \neq 0$. We see

$$p(\alpha) = c_n \alpha^n + \dots + c_1 \alpha + c_0 = 0$$

$$p(x) = p(x) - 0 = p(x) - p(\alpha) = \sum_{i=1}^{n} c_i (x^i - \alpha^i) + c_0$$

by homework

$$= (x-\alpha) \underbrace{\sum_{i=1}^{n} c_i \cdot G_{i-1}(\alpha, x)}_{\deg \text{ is } n-1}$$

$$G_\ell(\alpha, x) = \sum_{k=0}^{\ell} x^k \cdot \alpha^{\ell-k}$$

**Defn** Let $p \in F[x]$. The field elt $\beta \in F$ is a root/zero of $p$ if

$$p(\beta) = 0$$

**Corr** let $p \in F[x]$ nonzero then $p$ has, at most, $\deg(p)$ roots

**Pf** note: this holds if $\deg(p) = 0$ (as we are non-trivial)

Proceed by induction for rest

$$\mathcal{X} := \{ n \in \mathbb{N} \mid \forall q \in F[x]_{\leq n}, \ q \text{ has, at most } n \text{ roots} \}$$

($F[x]_{\leq n}$: poly of deg $\leq n$)

$\rightarrow 1 \in \mathcal{X}$!

Pose $k \in \mathcal{X}$. Let $q \in F[x]$ with deg $k+1$.

If $q$ has no roots, we're done.

If $\alpha$ is a root, we have $q(x) = (x-\alpha) r(x)$ ($r$ has deg $k$)

$\Rightarrow r$ has, at most $k$ roots.

$\Rightarrow q$ has, at most $k+1$ roots $\Rightarrow k+1 \in \mathcal{X}$ ▷

**Corollary** let $p \in F[x]$ be non trivial

Pose $\alpha_1, \dots \alpha_k \in F$ are roots of $p$.

$\exists$ nonzero poly $q \in F[x]$ s.t

① $q(\alpha_j) \neq 0 \quad \forall j \in \mathbb{N}_k$

② $\exists m_1, m_2 \dots m_k \in \mathbb{N}$ Called the multiplicity of $\alpha_j$

$$p = (x-\alpha_1)^{m_1} \cdot (x-\alpha_2)^{m_2} \cdots q$$

with $\deg(q) = \deg(p) - \sum m_j$

**Thm** Every non constant poly in $\mathbb{C}[x]$ has a root

↓ The field of complex no is algebraically closed

↓

Fundamental Thm of Alg!

**Defn** Let $\alpha \in \mathbb{C}$. We say $\alpha$ is **algebraic** if

$\exists$ **nonzero polynomial** $p \in \mathbb{Z}[x]$ → **as good as $\mathbb{Q}[x]$**

s.t. $p(\alpha) = 0$

---

**Note** The set of all algebraic numbers in $\mathbb{C}$ is denoted

$\overline{\mathbb{Q}}$ → **algebraic closure** of $\mathbb{Q}$

↳ it is thin, countable, but dense in $\mathbb{C}$.

**Defn** "**$\mathbb{Q}$ adjoin $\alpha$**" For $\alpha \in \mathbb{C}$

$$\mathbb{Q}[\alpha] := \text{span}_{\mathbb{Q}}(\alpha^i \mid i \in \mathbb{N} \cup \{0\})$$

$$= \{q_0 + q_1\alpha + q_2\alpha^2 \cdots q_n\alpha^n \cdots \mid q_i \in \mathbb{Q}, \text{ abfmc}\}$$