What are...(finite) fields?

Or: Fields are relatively rare

Fields are a bit weird

Field $=$ ring (using a suitable definition of ring) $+$ every element $\neq 0$ is invertible

- $\mathbb{Z}$ is not a field, $\mathbb{Q}$ is a field
- $\mathbb{Z}/4\mathbb{Z}$ is not a field, $\mathbb{Z}/3\mathbb{Z}$ is a field

World of rings

- (Co)products $\times$, $*$ exists
- Initial ring $\mathbb{Z}$, terminal ring 0 exists
- Free rings "polynomials" exists

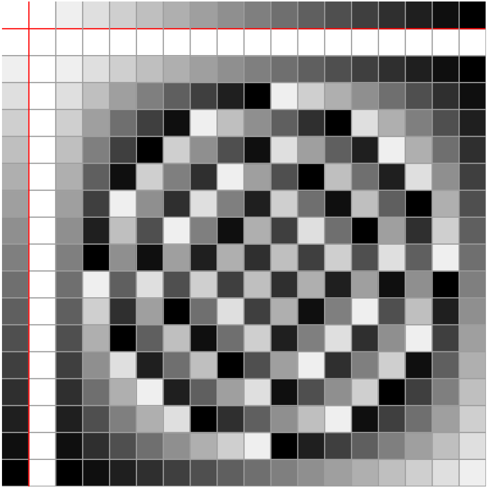
Similarly for groups/vector spaces/*etc.*

World of fields

- (Co)products $\times$, $*$ do not exists
- Initial, terminal fields do not exists
- Free fields do not exists

Algebraically weird!

Galois fields – finite blossoms



- Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ Order p
- For $q = p^k$ let $\mathbb{F}_q = \mathbb{F}_p[X]/(f \text{ irreducible, degree } k)$ Order q
- $\mathbb{F}_q$ is a field Existence

Closing Galois fields – infinite blossoms

Fact A finite field $\mathbb{K}$ is never algebraically closed

Proof $1 + \prod_{a \text{ elements of } \mathbb{K}} (X - a)$ has no roots

---

The algebraic closure of $\mathbb{F}_q$ is

$$\overline{\mathbb{F}_q} = \bigcup_k \mathbb{F}_{p^k}$$

- $\overline{\mathbb{F}_q}$ is constructed by adding roots of irreducible polynomials Existence
- $\overline{\mathbb{F}_q}$ is algebraically closed and minimal with this property Uniqueness

For completeness: The formal definition/statements

A field $\mathbb{K}$ is a set with $0, 1 \in \mathbb{K}, 0 \neq 1$ such that:

(a) $\mathbb{K}$ has an addition $+$, $\mathbb{K}$ has a multiplication $\cdot$

(b) $(\mathbb{K}, +)$ is an abelian group

(c) $(\mathbb{K} \setminus \{0\}, \cdot)$ is an abelian group Asymmetric

(d) The two rules distribute over one another

Examples.

- $\mathbb{Q}$, $\overline{\mathbb{Q}}$, $\mathbb{R}$, $\overline{\mathbb{R}} \cong \mathbb{R}(\sqrt{-1}) \cong \mathbb{C}$
- $\mathbb{F}_q$, $\overline{\mathbb{F}_q}$
- Finite extensions such as $\mathbb{Q}(\sqrt{2})$, infinite extensions such as $\mathbb{Q}(X)$
- p-adics $\mathbb{Q}_p$

There are almost no vs. quite a lot fields

Theorem

(a) There exists a field $\mathbb{F}_{p^k}$ of order p^k Existence

(b) All fields of order p^k are isomorphic Uniqueness

(c) There are no other finite fields Rare

(d) These are extremely important in algebra and beyond

Theorem

(a) There exists a field $\mathbb{K}$ of order α (any cardinal) Existence

(b) These field are far from being unique Too bad

(c) The class of fields is an honest class There are a lot fields

(d) Example. Take $\mathbb{Q}(X_i \mid i \in \alpha)$

Thank you for your attention!

I hope that was of some help.