Finite Fields

Additional note for reading
or "Not in syllabus".

Field. A field F is a non-empty set together with two laws of composition

[Addition] $$+ : F \times F \longrightarrow F, \text{ and}$$
$$(a, b) \longmapsto a+b$$

[Multiplication] $$\cdot : F \times F \longrightarrow F$$
$$(a,b) \longmapsto ab$$

satisfying the following axioms:

(i) $(F, +)$ is an abelian group, where identity element is denoted by 0.

(ii) $(F - \{0\}, \cdot)$ is a group, where identity element is 1.

(iii) Distributive law holds : $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Note. Axioms (i) and (ii) are independent of each other. The third axiom relates $+$ and $\cdot$.

Examples. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ etc.

$\mathbb{Z}/n\mathbb{Z}$; n is a positive integer.

Fix a positive integer n.

Define a relation '$\sim$' on $\mathbb{Z}$ by

$$l \sim m \iff n \text{ divides } m - l$$

[Notation. $n \mid m-l$ and $l \equiv m \pmod{n}$]

Remark. Note that '$\sim$' is an equivalence relation on $\mathbb{Z}$.

Remark. Equivalence relation '$\sim$' will partition the set $\mathbb{Z}$ into equivalence classes.

$$[x] = \{ m \in \mathbb{Z} \text{ s.t. } m \sim x \}$$

$$\Updownarrow$$

$$n \mid x - m$$

$$\Updownarrow$$

$$x - m = \mu \cdot n, \quad \text{where } \mu \in \mathbb{Z}$$

$$\Updownarrow$$

$$x = m + \mu n$$

or

$$m = x + \mu' n \ ; \quad \mu' \in \mathbb{Z}$$

$$[x] = \{ x + \mu' n \mid \mu' \in \mathbb{Z} \}$$
$$= \{ x, x \pm n, x \pm 2n, x \pm 3n, \dots \}$$

$[0] = \{ \mu' n \text{ s.t. } \mu' \in \mathbb{Z} \}$

$[1] = \{ 1 + \mu' n \text{ s.t. } \mu' \in \mathbb{Z} \}$

$\vdots$

$[n-1] = \{ n-1 + \mu' n \text{ s.t. } \mu' \in \mathbb{Z} \}$

The set of integers $\mathbb{Z}$ is partitioned into equivalence classes $[0], [1], \ldots, [n-1]$.

Denote by

$$\mathbb{Z}/n\mathbb{Z} = \{ [0], [1], \ldots, [n-1] \}$$

collection of equivalence classes.

– a finite set.

Define

[Addition]

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$([a], [b]) \longmapsto [a+b]$$

Question. Is $(\mathbb{Z}/n\mathbb{Z}, +)$ an abelian group?

Also, verify, why $+$ is well-defined?

'+' is well defined map: $\quad + : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

If $\quad ([l_1], [l_2]) = ([m_1], [m_2])$,

then $\quad +([l_1], [l_2]) = +([m_1], [m_2])$

Proof. Given $[l_1] = [m_1]$ and $[l_2] = [m_2]$.

$$\Downarrow \qquad\qquad \Downarrow$$

$$n \mid m_1 - l_1 \qquad\qquad n \mid m_2 - l_2$$

$$\Downarrow$$

$$l_1 = m_1 + \lambda \cdot n \qquad\qquad l_2 = m_2 + \mu \cdot n$$

where $\lambda, \mu \in \mathbb{Z}$

Now,

$$l_1 + l_2 = m_1 + m_2 + (\lambda + \mu) n$$

$$\Rightarrow \quad \underset{+([l_1],[l_2])}{\underset{\parallel}{[l_1 + l_2]}} = \underset{+([m_1],[m_2])}{\underset{\parallel}{[m_1 + m_2]}}$$

Remark. $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group.

$[0]$: identity element

Additive inverse : $\quad [l_1] + [\quad] = [0]$

Abelian

Define multiplication map

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$([a], [b]) \longmapsto [ab]$$

Remark. The map $\cdot$ is well-defined. (Exercise).

Remark. $(\mathbb{Z}/n\mathbb{Z}, \cdot)$

Is this a group?

No, $[0]$ does not have inverse.

$(\mathbb{Z}/4\mathbb{Z}, \cdot)$ $[0]$ and $[2]$ do not have inverse.

$(\mathbb{Z}/n\mathbb{Z} - [0], \cdot)$ still need not be group.

Consider a new set :

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} := \left\{ [\ell] \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. there exists } [m] \in \mathbb{Z}/n\mathbb{Z} \text{ with } [\ell m] = [1] \right\}$$

(collection of multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$)

$$\left(\mathbb{Z}/5\mathbb{Z}\right)^{\times} = \{ [1], [2], [3], [4] \}$$

$$\left(\mathbb{Z}/9\mathbb{Z}\right)^{\times} = \{ [1], [2], [4], [5], [7], [8] \}$$

Question. Can we count number of elements in $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$?

$$\varphi(n) = \left| \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} \right|$$

= number of positive integers $\ell \leq n$ which are relatively prime to n, i.e. $\gcd(\ell, n) = 1$.

Question. $\left((\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot \right)$ Is this a group?

- $\cdot([l],[m]) = [lm] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ binary operation
- verify associativity
- $[1] \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ is an identity element.
- By definition of $(\mathbb{Z}/n\mathbb{Z})^{*}$, inverse exists for every element.

YES, $\left((\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot \right)$ is a Group.

Discussion. Observe from the definition of field,

$(\mathbb{Z}/n\mathbb{Z}, +)$ Abelion group.

[This works for all $n \in \mathbb{Z}_{\geq 0}$]

$(\text{Set}, +, \cdot)$

Choose n s.t. $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is $\mathbb{Z}/n\mathbb{Z} - [0]$, in terms of elements.

[n is a prime number.]

$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$

- $(\mathbb{Z}/p\mathbb{Z}, +)$ Abelion group, identity elt $[0]$
- $(\mathbb{Z}/p\mathbb{Z} - [0], \cdot)$ is a group, identity is $[1]$.
- Distributive law holds

Lemma. Let $[a], [c], [d]$ be elements of $\mathbb{Z}/p\mathbb{Z}$ with $[a] \neq [0]$. If

$[a][c] = [a][d]$, then $[c] = [d]$.

[Cancellation law]

Proof. Set $[b] = [c] - [d]$.

then we want to show

if $[a][b] = [0]$, and $[a] \neq 0$, then $[b] = 0$.

$$
\begin{aligned}
&[a][b] = [0] \\
&\quad \| \\
&[ab] = [0] \\
&\quad \Downarrow \\
&p \text{ divides } ab \qquad (p \text{ is a prime number})
\end{aligned}
$$

[Enough to conclude: p divides a or p divides b]

if $p \nmid a$, then $p \mid b$.

Question. [Direct verification].

If p is a prime integer, then why all non-zero congruence classes modulo p have inverses ?

Answer.

$$[a] \in \mathbb{Z}/p\mathbb{Z} \quad \text{s.t.} \quad [a] \neq [0].$$

Claim. $[a]$ have inverse in $\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}, \cdot\right)$.

Consider the powers

$$\underbrace{\{ [a], [a]^2, [a]^3, \ldots\ldots \}}_{\text{infinite collection}}$$

By Pigeon-Hole principle;

$$[a]^k = [a]^m \quad \text{for some } k \text{ and } m \text{ in } \mathbb{N}.$$

$k < m$

$$[a]^k = [a]^k \cdot [a]^{m-k}$$

$$1 = [a]^{m-k}$$

$$1 = \underbrace{[a]^{m-k-1}}_{\text{inverse of } [a]} \cdot [a]$$

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

$\parallel$ Notation

$\mathbb{F}_p \longleftarrow$ p elements

$\mathbb{F}_2 = \{[0], [1]\}$

$\mathbb{F}_3 = \{[0], [1], [2]\}$

$\vdots$

$\mathbb{F}_5 = \{[0], [1], [2], [3], [4]\}$ etc.

Corollary. Consider a system $AX = B$ of n linear equations in n unknowns, where the entries of A, B are in $\mathbb{F}_p$.

The system has a unique solution in $\mathbb{F}_p$ if $\det(A) \neq 0$ in $\mathbb{F}_p$.

$GL_n(\mathbb{F}_p) = \{ n \times n$ invertible matrices with entries in $\mathbb{F}_p \}$

Example.

ⓘ $GL_2(\mathbb{F}_2)$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} & 1 \\ 1 & 1 \end{bmatrix} \right\}$$