Reminder: Group

Definition

A group is a pair $(X, \circ)$, where

- X is a set and $\circ : X \times X \to X$ is a total function,

satisfying the following axioms:

associativity	$(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in X$.
neutral element	There exists $e \in X$ s.t. $a \circ e = e \circ a = a$ for every $a \in X$.
inverse	for every $a \in X$ there exists $a^{-1} \in X$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

The group is abelian if additionally

commutativity	$a \circ b = b \circ a$ for all $a, b \in X$.

Field

Definition

A field is a triple $(X, +, \cdot)$, where

- $(X, +)$ is an abelian group,
  - let 0 denote its neutral element and $-x$ the inverse to x,
- $(X \setminus \{0\}, \cdot)$ is an abelian group,
  - let 1 denote its neutral element and x^{-1} the inverse to x,
- $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in X$ (distributivity)

Remark: sometimes, the commutativity of $\cdot$ is not required.

Examples

- rational numbers $(\mathbf{Q}, +, \cdot)$ form a field
- real numbers $(\mathbf{R}, +, \cdot)$ form a field
- complex numbers $(\mathbf{C}, +, \cdot)$ form a field
- integers $(\mathbf{Z}, +, \cdot)$ do not form a field, since $(\mathbf{Z} \setminus \{0\}, \cdot)$ is not a group.
- regular $n \times n$ matrices do not form a field, since sum of two regular matrices does not have to be regular.

Basic properties

Lemma

If $(X, +, \cdot)$ *is a field, then*

$$0x = 0$$

for every $x \in X$*.*

Proof.

We have

$$0 = 0x + (-(0x)) = (0+0)x + (-(0x)) = 0x + 0x + (-(0x)) = 0x.$$

$\square$

Basic properties

Lemma

If $(X, +, \cdot)$ *is a field, then*

$$-x = (-1)x$$

for every $x \in X$*.*

Proof.

We have

$$x + (-1)x = 1x + (-1)x = (1 + (-1))x = 0x = 0,$$

hence $(-1)x$ is equal to the additive inverse to x. $\square$

Basic properties

Lemma

If $(X, +, \cdot)$ *is a field, then*

$$ab = 0 \text{ if and only if } a = 0 \text{ or } b = 0$$

for every $a, b \in X$*.*

Proof.

If $a \neq 0$ and $ab = 0$, then

$$b = 1b = a^{-1}ab = a^{-1}0 = 0.$$

$\square$

Linear equations over fields

Everything we did in the first three lectures only depends on the field properties. Hence, everything works with coefficients from arbitrary field:

- systems of linear equations,
- elementary row operations preserve the set of solutions,
- Gauss and Gauss-Jordan elimination to solve the equations,
- matrices and operations with them,
- regularity and inverse.

Finite fields

A field $(X, +, \cdot)$ is finite if X is a finite set.

- None of the examples we have is a finite field.
- Uses of finite fields
  - exact computations (no rounding errors, fixed size representation)
    - fast multiplication through Fourier transformation
  - cryptography
  - error-correcting codes
  - …

Reed-Solomon codes

Let $(X, +, \cdot)$ be a field with $|X| \geq n + 2$.

Encoding:

- Let $a_0, a_1, \ldots, a_{n-1} \in X$ be the message we want to encode.
- Let $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$.
- Let s_1, s_2, ..., s_{n+2} be fixed distinct elements of X.
- Encode the message as $p(s_1), p(s_2), \ldots, p(s_{n+2})$.
- Instead of sending n elements, we send $n + 2$.

Reed-Solomon codes

Let $(X, +, \cdot)$ be a field with $|X| \geq n + 2$.

Theorem (for now without proof)

If $x_1, \ldots, x_n \in X$ are pairwise distinct, and $y_1, \ldots, y_n \in X$ are arbitrary, then there exists exactly one polynomial q of degree at most $n - 1$ with coefficients in X such that

$$q(x_i) = y_i \text{ for } i = 1, \ldots, n.$$

The coefficients of q can be determined by solving linear equations. Let $q = b_0 + b_1 x + b_2 x^2 + \ldots + b_{n-1} x^{n-1}$.

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ & & \ldots & & \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \ldots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_n \end{pmatrix}$$

Reed-Solomon codes

Let $(X, +, \cdot)$ be a field with $|X| \geq n + 2$.

Decoding:

- Let $t_1, \ldots, t_{n+2}$ be the received message.
- For $1 \leq k \leq n + 2$, find a polynomial p_k of degree at most $n - 1$ such that

$$p_k(s_i) = t_i \text{ for } i \in \{1, \ldots, n + 2\} \setminus \{k\},$$

  or determine that no such polynomial exists.
- If there was no error, then all the polynomials exist and are equal to p.
- If there was exactly one error, say $t_k \neq p(s_k)$, then only the polynomial p_k exists and is equal to p.
- To decode the message, read the coefficients of p_k.

Modulo operation

Definition

For an integer $p > 0$, let $\mathbf{Z}_p = \{0, 1, \ldots, p - 1\}$.

Definition

For integers a and $p > 0$, let

$$a \bmod p$$

denote the remainder of division of a by p, that is, $a \bmod p \in \mathbf{Z}_p$ is the unique number such that $a - (a \bmod p)$ is divisible by p.

$$a \bmod p = b \bmod p \text{ if and only if } (a - b) \bmod p = 0,$$

i.e., $a - b$ is divisible by p.

Example

$$
\begin{aligned}
25 \bmod 7 &= 4 \\
25 \bmod 5 &= 0 \\
-25 \bmod 7 &= 3
\end{aligned}
$$

Modulo arithmetics

Let us define

$$a +_p b = (a + b) \bmod p$$

and

$$a \cdot_p b = (ab) \bmod p.$$

Example

$$10 +_{13} 11 = 21 \bmod 13 = 8$$
$$10 \cdot_{13} 4 = 40 \bmod 13 = 1$$

$\mathbf{Z}_p$ and addition

Lemma

For any integer $p \geq 1$, $(\mathbf{Z}_p, +_p)$ is an abelian group (called the cyclic group of order p).

Proof.

$+_p$ is commutative:

$$a +_p b = (a + b) \bmod p = (b + a) \bmod p = b +_p a$$

0 is a neutral element:

$$a +_p 0 = (a + 0) \bmod p = a \bmod p = a$$

0 is inverse to itself, and $p - a$ is inverse to a for $1 \leq a \leq p - 1$:

$$a +_p (p - a) = (a + p - a) \bmod p = p \bmod p = 0$$

□

$\mathbf{Z}_p$ and addition

Lemma

For any integer $p \geq 1$, $(\mathbf{Z}_p, +_p)$ is an abelian group (called the cyclic group of order p).

Proof.

$+_p$ is associative:

- Let $r = a +_p b$, so $a + b = mp + r$ for some $m \in \mathbf{Z}$.
- Let $s = r +_p c$, so $s \in \mathbf{Z}_p$ and $r + c = np + s$ with $n \in \mathbf{Z}$.
- Then,

$$\begin{aligned}(a +_p b) +_p c &= r +_p c = s, \text{ and}\\ a + b + c &= mp + r + c = mp + np + s\\ &= (m + n)p + s, \text{ and thus}\end{aligned}$$

$$(a +_p b) +_p c = s = (a + b + c) \bmod p.$$

- Similarly, $a +_p (b +_p c) = (a + b + c) \bmod p$.

□

$\mathbf{Z}_p$ and multiplication

Lemma

For any integer $p \geq 1$, $(\mathbf{Z}_p, \cdot_p)$ is an abelian monoid.

Proof.

$\cdot_p$ is commutative:

$$a \cdot_p b = (ab) \bmod p = (ba) \bmod p = b \cdot_p a$$

1 is a neutral element:

$$a \cdot_p 1 = (a1) \bmod p = a \bmod p = a$$

for every $a \in \mathbf{Z}_p$.

$\square$

$\mathbf{Z}_p$ and multiplication

Lemma

For any integer $p \geq 1$, $(\mathbf{Z}_p, \cdot_p)$ is an abelian monoid.

Proof.

$\cdot_p$ is associative:

- Let $r = a \cdot_p b$, so $ab = mp + r$ for some $m \in \mathbf{Z}$.
- Let $s = r \cdot_p c$, so that $s \in \mathbf{Z}_p$ and $rc = np + s$ with $n \in \mathbf{Z}$.
- Then,

$$\begin{aligned}
(a \cdot_p b) \cdot_p c &= r \cdot_p c = s, \text{ and} \\
abc &= (mp + r)c = mcp + rc = mcp + np + s \\
&= (mc + n)p + s, \text{ and thus} \\
(a \cdot_p b) \cdot_p c &= s = (abc) \bmod p.
\end{aligned}$$

- Similarly, $a \cdot_p (b \cdot_p c) = (abc) \bmod p$.

$\square$

Inverse in $\mathbf{Z}_p \setminus \{0\}$: necessary condition

Lemma

If $\mathbf{Z}_p \setminus \{0\}$ is a group, then p is prime.

Proof.

If p is not a prime, then $p = ab$ for some integers $a, b \in \mathbf{Z}_p \setminus \{0\}$. Then

$$a \cdot_p b = (ab) \bmod p = p \bmod p = 0.$$

We claim that b does not have inverse. Indeed, if $b \cdot_p c = 1$ for some $c \in \mathbf{Z}_p$, then

$$0 = 0 \cdot_p c = (a \cdot_p b) \cdot_p c = a \cdot_p (b \cdot_p c) = a \cdot_p 1 = a,$$

which is a contradiction. □

Cancellation law

Lemma

If p is prime, $a, b, c \in \mathbf{Z}_p$, $a \neq 0$ and

$$a \cdot_p b = a \cdot_p c,$$

then $b = c$.

Proof.

We have

$$a \cdot_p b = a \cdot_p c$$

if and only if

$$p \text{ divides } ab - ac = a(b - c).$$

Since p is prime, this happens only if p divides either a or $b - c$. Since $a \neq 0$ and $|b - c| \leq p - 1$, this implies $b - c = 0$. $\square$

Fermat's little theorem

Theorem (Fermat)

If p is a prime and $a \in \mathbf{Z}_p \setminus \{0\}$, then $a^{p-1} \bmod p = 1$.

Proof.

By the cancellation law, the numbers
$a \cdot_p 1, a \cdot_p 2, \ldots, a \cdot_p (p-1)$ are pairwise different.
They are non-zero, and thus
$\{a \cdot_p 1, a \cdot_p 2, \ldots, a \cdot_p (p-1)\} = \mathbf{Z}_p \setminus \{0\}$. Therefore,

$$\begin{aligned} 1 \cdot_p 2 \cdots_p (p-1) &= (a \cdot_p 1) \cdot_p (a \cdot_p 2) \cdots_p (a \cdot_p (p-1)) \\ &= (a^{p-1} \bmod p) \cdot_p (1 \cdot_p 2 \cdots_p (p-1)) \end{aligned}$$

By the cancellation law, we have

$$a^{p-1} \bmod p = 1.$$

$\square$

Fermat's little theorem and inverse

Lemma

If p is prime, then $(\mathbf{Z}_p \setminus \{0\}, \cdot_p)$ is a group. The inverse to a is equal to $a^{p-2} \bmod p$.

Proof.

$$a \cdot_p (a^{p-2} \bmod p) = a^{p-1} \bmod p = 1.$$

$\square$

Computing inverse: example

Problem

Determine inverse to 10 *in* $\mathbf{Z}_{13} \setminus \{0\}$.

We have

$$10^2 \bmod 13 = 9 \qquad 10^4 \bmod 13 = 9^2 \bmod 13 = 3$$
$$10^8 \bmod 13 = 3^2 \bmod 13 = 9$$

Hence, the inverse is

$$10^{11} \bmod 13 = 10^8 \cdot_{13} 10^2 \cdot_{13} 10^1 = (9 \cdot_{13} 9) \cdot_{13} 10 = 3 \cdot_{13} 10 = 4.$$

Indeed,

$$10 \cdot_{13} 4 = 1$$

Fermat's little theorem inverse – complexity

Computing a^{p-2} needs only $O(\log_2 p)$ arithmetic operations.

- Let $r := 1$, $A := a$, and $m := p - 2$
- While $m \neq 0$:
  - If $m \bmod 2 = 1$, then let $r := (Ar) \bmod p$.
  - Let $A := A^2 \bmod p$ and $m := \lfloor m/2 \rfloor$.

Fermat's little theorem and testing primality

To test whether p is a prime,

- Choose an integer $a \in \{1, \ldots, p-1\}$ at random, and
- check whether $a^{p-1} \bmod p = 1$.
  - If no, then p is not prime.
  - if yes, then p may or may not be prime.

Repeat k times.

- If p is composite and not one of exceptional Carmichael numbers, then the test proves that p is not a prime with probability at least $1 - \frac{1}{2^k}$.
- More involved tests avoid the flaw with Carmichael numbers.
- Requires $O(k \log p)$ arithmetic operations.
  - Brute force algorithm to find a divisor of p requires $O(\sqrt{p})$ arithmetic operations.

Euclid's algorithm

To determine the greatest common divisor of integers $a > b \geq 0$:

- If $b = 0$, then $\gcd(a, b) = a$.
- If $b > 0$, then $\gcd(a, b) = \gcd(b, a \bmod b)$.

Example:

$$\gcd(13, 10) = \gcd(10, 3) = \gcd(3, 1) = \gcd(1, 0) = 1.$$

Expressing gcd as a combination of arguments

Lemma

For all integers $a, b \geq 0$, there exist integers m and n such that

$$am + bn = \gcd(a, b).$$

Proof.

We proceed by induction on $\max(a, b)$. If $a = b$, then $\gcd(a, b) = a = a1 + b0$. Hence, assume $a > b \geq 0$.

- If $b = 0$, then $\gcd(a, b) = a = a1 + b0$.
- If $b > 0$, then let $r = a \bmod b$, so $a = bt + r$ for $t \in \mathbf{Z}$. By induction hypothesis,

$$\gcd(b, r) = bm_1 + rn_1. \text{ Hence,}$$

$$\begin{aligned} \gcd(a, b) = \gcd(b, r) &= bm_1 + rn_1 = bm_1 + (a - bt)n_1 \\ &= an_1 + b(m_1 - n_1 t). \end{aligned}$$

Example

$$\gcd(13,10) = \gcd(10,3)$$

- $13 \bmod 10 = 3$

$$\gcd(10,3) = \gcd(3,1)$$

- $10 \bmod 3 = 1$

$$\gcd(3,1) = 1 \Rightarrow 1 = 3 \cdot 0 + 1 \cdot 1$$

Example

$$\gcd(13, 10) = \gcd(10, 3) = 1$$

- $13 \bmod 10 = 3$

$$\gcd(10, 3) = \gcd(3, 1) = 1$$

- $10 \bmod 3 = 1$

$$\gcd(3, 1) = 1 \Rightarrow 1 = 3 \cdot 0 + 1 \cdot 1$$

Example

$$\gcd(13, 10) = \gcd(10, 3) = 1$$

- $13 \bmod 10 = 3$

$$\gcd(10, 3) = \gcd(3, 1) = 1$$

- $10 \bmod 3 = 1$, and thus $1 = 10 - 3 \cdot 3$.
- $3 \cdot 0 + 1 \cdot 1 = 3 \cdot 0 + (10 - 3 \cdot 3) \cdot 1 = 10 \cdot 1 + 3 \cdot (-3)$

$$\gcd(3, 1) = 1 \Rightarrow 1 = 3 \cdot 0 + 1 \cdot 1$$

Example

$$\gcd(13, 10) = \gcd(10, 3) = 1$$

- $13 \bmod 10 = 3$

$$\gcd(10, 3) = \gcd(3, 1) = 1 \Rightarrow 1 = 10 \cdot 1 + 3 \cdot (-3)$$

- $10 \bmod 3 = 1$, and thus $1 = 10 - 3 \cdot 3$.
- $3 \cdot 0 + 1 \cdot 1 = 3 \cdot 0 + (10 - 3 \cdot 3) \cdot 1 = 10 \cdot 1 + 3 \cdot (-3)$

$$\gcd(3, 1) = 1 \Rightarrow 1 = 3 \cdot 0 + 1 \cdot 1$$

Example

$$\gcd(13,10) = \gcd(10,3) = 1$$

- $13 \bmod 10 = 3$, and thus $3 = 13 - 10 \cdot 1$.
- $10\cdot 1 + 3\cdot(-3) = 10\cdot 1 + (13 - 10\cdot 1)\cdot(-3) = 13\cdot(-3) + 10\cdot 4$

$$\gcd(10,3) = \gcd(3,1) = 1 \Rightarrow 1 = 10 \cdot 1 + 3 \cdot (-3)$$

- $10 \bmod 3 = 1$, and thus $1 = 10 - 3 \cdot 3$.
- $3 \cdot 0 + 1 \cdot 1 = 3 \cdot 0 + (10 - 3 \cdot 3) \cdot 1 = 10 \cdot 1 + 3 \cdot (-3)$

$$\gcd(3,1) = 1 \Rightarrow 1 = 3 \cdot 0 + 1 \cdot 1$$

Example

$$\gcd(13,10) = \gcd(10,3) = 1 \Rightarrow 1 = 13 \cdot (-3) + 10 \cdot 4$$

- $13 \bmod 10 = 3$, and thus $3 = 13 - 10 \cdot 1$.
- $10 \cdot 1 + 3 \cdot (-3) = 10 \cdot 1 + (13 - 10 \cdot 1) \cdot (-3) = 13 \cdot (-3) + 10 \cdot 4$

$$\gcd(10,3) = \gcd(3,1) = 1 \Rightarrow 1 = 10 \cdot 1 + 3 \cdot (-3)$$

- $10 \bmod 3 = 1$, and thus $1 = 10 - 3 \cdot 3$.
- $3 \cdot 0 + 1 \cdot 1 = 3 \cdot 0 + (10 - 3 \cdot 3) \cdot 1 = 10 \cdot 1 + 3 \cdot (-3)$

$$\gcd(3,1) = 1 \Rightarrow 1 = 3 \cdot 0 + 1 \cdot 1$$

Euclid's algorithm and inverse

If p is prime and $a \in \mathbf{Z}_p \setminus \{0\}$, then

$$\gcd(a, p) = 1 = an + pm$$

for some integers m, n. Hence,

$$(an) \bmod p = (1 - pm) \bmod p = 1.$$

Therefore, $n \mod p$ is the inverse to a.

Example:

$$\gcd(10, 13) = 1 = 10 \cdot 4 + 13 \cdot (-3),$$

and thus 4 is the inverse to 10 in $\mathbf{Z}_{13} \setminus \{0\}$.

Field $\mathbf{Z}_p$

Theorem

$(\mathbf{Z}_p, +_p, \cdot_p)$ *is a field if and only if* p *is a prime.*

Proof.

- $(\mathbf{Z}_p, +_p)$ is an abelian group
- $(\mathbf{Z}_p \setminus \{0\}, \cdot_p)$ is an abelian group if and only if p is a prime
- distributivity:

$$\begin{aligned} a \cdot_p (b +_p c) &= (a(b + c)) \bmod p = (ab + ac) \bmod p \\ &= a \cdot_p b +_p a \cdot_p c \end{aligned}$$

similarly to associativity.

$\square$

Example: linear equations over a field

Problem

Lights A, B, C, D are controlled by switches 1, 2, 3, 4:

switch	controlled lights
1	A, B
2	B, C, D
3	A, C
4	A, D

Flipping a switch turns on the controlled lights that were off, and vice versa. If lights are now all off, can you turn them on?

Solve

$$\begin{array}{ccccc} x_1 & & +x_3 & +x_4 & = 1 \\ x_1 & +x_2 & & & = 1 \\ & x_2 & +x_3 & & = 1 \\ & x_2 & & +x_4 & = 1 \end{array}$$

over $\mathbf{Z}_2$.

Example: linear equations over a field

Solve

$$\begin{aligned}
x_1 \qquad\quad &+x_3 &+x_4 &= 1\\
x_1 \quad +x_2 \qquad &&&= 1\\
x_2 \quad &+x_3 &&= 1\\
x_2 \qquad && +x_4 &= 1
\end{aligned}$$

over $\mathbf{Z}_2$.

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1\\ 1 & 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0 & 1\\ 0 & 1 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & 1 & 1 & 0 & 1\\ 0 & 1 & 0 & 1 & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

Example: linear equations over a field

Solve

$$\begin{array}{ccccc}
x_1 & & +x_3 & +x_4 & = 1 \\
x_1 & +x_2 & & & = 1 \\
 & x_2 & +x_3 & & = 1 \\
 & x_2 & & +x_4 & = 1
\end{array}$$

over $\mathbf{Z}_2$.

$$\left(\begin{array}{cccc|c}
1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1
\end{array}\right)$$

$$\begin{aligned}
x_4 &= 1 \\
x_3 &= 1 \\
x_2 &= 0 - x_3 - x_4 = 0 \\
x_1 &= 1 - x_3 - x_4 = 1
\end{aligned}$$

Example: linear equations over a field

Problem

Lights A, B, C, D are controlled by switches 1, 2, 3, 4:

switch	controlled lights
1	A, B
2	B, C, D
3	A, C
4	A, D

Flipping a switch turns on the controlled lights that were off, and vice versa. If lights are now all off, can you turn them on?

$$
\begin{aligned}
x_4 &= 1 \\
x_3 &= 1 \\
x_2 &= 0 \\
x_1 &= 1
\end{aligned}
$$

Flip switches 1, 3 and 4.

Field characteristic

For integer $n \geq 1$, let

$$n \times x = \underbrace{x + x + \ldots + x}_{n \text{ times}}.$$

Definition

Let $(X, +, \cdot)$ be a field with multiplicative neutral element 1 and additive neutral element 0. The characteristic of the field is the smallest integer $n \geq 1$ such that

$$n \times 1 = 0.$$

- $\mathbf{R}$ has infinite characteristic
    - sometimes called "characteristic 0"
- $\mathbf{Z}_p$ has characteristic p.
- There exist infinite fields with finite characteristic.

Properties of characteristic

Lemma

Every finite field $(X, +, \cdot)$ has characteristic at most $|X|$.

Proof.

1×1, 2×1, ..., $|X| \times 1$, $(|X| + 1) \times 1$ are elements of X. By pigeonhole principle, there exist $1 \leq n_1 < n_2 \leq |X| + 1$ such that

$$n_1 \times 1 = n_2 \times 1.$$

Hence,

$$(n_2 - n_1) \times 1 = n_2 \times 1 - n_1 \times 1 = 0.$$

□

Properties of characteristic

Lemma

If p is the characteristic of a field $(X, +, \cdot)$ and p is finite, then p is prime.

Proof.

Suppose that $p = ab$ for $a, b < p$. Then

$$a \times (b \times 1) = (ab) \times 1 = p \times 1 = 0.$$

By the minimality of the characteristic, $b \times 1 \neq 0$, and thus there exists $(b \times 1)^{-1}$. Therefore,

$$a \times 1 = a \times (b \times 1) \cdot (b \times 1)^{-1} = 0,$$

which contradicts the minimality of the characteristic. $\square$

Characteristic of a finite field

Theorem (for now without proof)

If $\mathbf{F}$ *is a finite field of characteristic* p*, then*

$$|\mathbf{F}| = p^n$$

for some integer $n \geq 1$*.*

Corollary

If $\mathbf{F}$ *is a finite field, then*

$$|\mathbf{F}| = p^n$$

for some prime p *and integer* $n \geq 1$*.*

Existence of fields

Theorem (we will not prove)

For every prime p and integer $n \geq 1$, there exists exactly one field (up to isomorphism) of size p^n. The field is denoted by $\mathbf{F}_{p^n}$. The characteristic of $\mathbf{F}_{p^n}$ is p.

For $n = 1$, we have $\mathbf{F}_p = (\mathbf{Z}_p, +_p, \cdot_p)$.

Example: $\mathbf{F}_4$

Elements: 0, 1, x, $1 + x$.

Operations:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Remark: $\mathbf{F}_4$ is not isomorphic to $(\mathbf{Z}_4, +_4, \cdot_4)$; the latter is not a field.