Cancellation Laws

If a, b, c are elements in a group G, then:

$$ab = ac \Rightarrow b = c$$

$$ba = ca \Rightarrow b = c$$

Let $a, b, c \in G$, and suppose $ab = ac$

Since $a \in G$, $\exists a^{-1} \in G$ — inverse

$a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)b = (a^{-1}a)c$ — associativity

$eb = ec$ — identity

$\therefore b = c$

Similarly $ba = ca \Rightarrow b = c$

Unique Inverse

For every a in a group G, there is a unique element $b \in G$ such that $ba * ab = e$

i.e. the inverse is unique

Suppose that b and c are inverses of a, i.e.

$$ab = e$$

$$ac = e$$

So $ab = ac$, and by cancellation law: $b = c$

Definitions

If a is an element in a group $G \Rightarrow (G, *)$, we define

i) a^{-1} is the inverse of a

ii) For n a positive integer $a^n = \underbrace{a * a * \dots * a}_{n \text{ times}}$

iii) $a^0 = e$

iv) If n is a negative integer $a^n = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{n \text{ times}} = (a^{-1})^{|n|}$

$a^{-1} \neq \frac{1}{a}$ in general

Remarks

Cannot define $a^{1/2}$

If $m, n \in \mathbb{Z}$ then $a^m \cdot a^n = a^{m+n}$

$$(a^m)^n = a^{mn}$$

$(ab)^n \neq a^n b^n$ in general, but you can move them around if they are abelian

Socks Shoes Property

For all $a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$

Let $a, b \in G$, then $ab \in G$ — closure

so $(ab)^{-1} \in G$ — inverse

$(ab)(ab)^{-1} = e$ — identity

$a^{-1}(ab)(ab)^{-1} = a^{-1}e$

$(a^{-1}a)b(ab)^{-1} = a^{-1}$

$eb(ab)^{-1} = a^{-1}$

$b(ab^{-1}) = a^{-1}$

$b^{-1}b(ab)^{-1} = b^{-1}a^{-1}$

$e(ab)^{-1} = b^{-1}a^{-1}$

$(ab)^{-1} = b^{-1}a^{-1}$

Example 7

a) Compute 4^3 in $(\mathbb{Z}, +)$

$4^3 = 4 + 4 + 4$

b) Find 7^{-1} in $(\mathbb{Q}^*, \times)$

Here $e = 1 \Rightarrow \frac{1}{7} \times 7 = 1$ so $7^{-1} = \frac{1}{7}$

c) Find 7^{-1} in $(\mathbb{Q}, +)$

Here $e = 0 \Rightarrow -7 + 7 = 0$ so $7^{-1} = -7$

7^{-1} = inverse

Congruences and Modular Arithmetic

Let $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$

$a \equiv b \pmod{m}$ means $m \mid (a - b)$

or equivalently $a = b + km$

or $a - b = km$ for some $k \in \mathbb{Z}$

or equivalently a and b have the same remainder when divided by m.

m is the modulus

Example 8

a) True or False

$10 \equiv 1 \pmod 3$ T

$9 \equiv 21 \pmod 5$ F

b) Simplify

$15 \pmod 4$ 3

$76 \pmod 7$ 6

$263 \equiv \pmod{12}$ 11

Equivalence Relation

Suppose $a, b, c \in \mathbb{Z}$ then i) $a \equiv a \pmod m$

ii) $a \equiv b \pmod m$ then $a \equiv c \pmod m$

iii) $a \equiv b \pmod m$ then $b \equiv a \pmod m$

$\equiv$ is the equivalence relation

Proposition 6

If $a_1 \equiv b_1 \pmod m$ and $a_2 \equiv b_2 \pmod m$

then i) $a_1 + a_2 \equiv b_1 + b_2 \pmod m$

ii) $a_1 a_2 \equiv b_1 b_2 \pmod m$

iii) $ca_1 \equiv c b_1 \pmod m$

warning $ca \equiv cb \pmod m \not\Rightarrow a \equiv b \pmod m$ $18 \equiv 8 \pmod{10}$

$9 \not\equiv 4 \pmod{10}$

warning $ab \equiv 0 \pmod{m}$

$\not\Rightarrow$ $a \equiv 0 \pmod{m}$ or $b \equiv 0 \pmod{m}$

Remark $a \equiv 0 \pmod{m}$ means a is divisible by m.

Convergance classes

Suppose $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ then a can be written as $a = qm + r$ where q is the quotient and r is the remainder and $r \in \{0, 1, 2, \ldots, m-1\}$

$q, r \in \mathbb{Z}$

$m = 5$, $a = 17$ $\quad 17 = \frac{3}{q} \cdot 5 + \frac{2}{r}$

Then $a \equiv r \pmod{m}$

Summary Any $a \in \mathbb{Z}$ is congruent to r where $r \in \{0, 1, \ldots, m-1\}$

So if working modulo m, all integers can be represented by $0, 1, 2, \ldots, m-1$

Definitions

i) Let $a \in \mathbb{Z}$ $m \in \mathbb{Z}$, The congruence of a modulo m is the set

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

ii) The set of all congruence classes modulo m is called the set of integers modulo m, witten $\mathbb{Z}_m$

iii) Sometimes we write $[a]_m$ instead of $[a]$

Example 7

Write down the congruence classes modulo 5. What is the size of $\mathbb{Z}_5$? (not counting repeats)

$[0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 5\}$

$= \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 5\}$

$= \{\ldots, -10, -5, 0, 5, 10, 15 \ldots\}$

$[1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 5\}$

$= \{x \in \mathbb{Z} \mid x \text{ has a remainder of } 1 \text{ when divided by } 5\}$

$= \{\ldots -9, -4, 1, 6, 11, 16, \ldots\}$

$[2] = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 5\}$

$= \{\ldots -8, -3, 2, 7, 12, 17, \ldots\}$

$[3] = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$

$[4] = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}$

$[5] = [0]$, $[6] = [1]$, $[7] = [2]$, ...

So $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

or $= \{[5], [6], [12], [18], [-1]\}$

or $= \{[0], [-1], [-13], [2], [-2]\}$

Regardless, the size of $\mathbb{Z}_5$ is 5.

Remarks 1) size of $\mathbb{Z}_m$ is m

2) we often write just $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Example 8

Which of these are the same in $\mathbb{Z}_{10}$?

$[3]_{10}$ $[10]_{10}$ $[0]_{10}$ $[123]_{10}$ $[-7]_{10}$

Definitions

Let $a, b \in \mathbb{Z}$, and $m \in \mathbb{Z}^+$

i) $[a]_m + [b]_m = [a + b]_m$

ii) $[a]_m \cdot [b]_m = [ab]_m$

Remark Because of proposition 6, these operations are well defined.

Eg $[4]_5 + [3]_5 = [4 + 3]_5 = [7]_5 = [2]_5$

Proposition 6 tells us that we get the same answer each time

Theorem 7

Let $m \in \mathbb{Z}^+$, then $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ under addition modulo M is a group.

Example 9

Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ Find the identity and the inverses under addition mod 6.

$e = 0$

1^{-1}: $1 + 5 = 0 \pmod 6$ so $1^{-1} = 5$

2^{-1}: $2 + 4 = 0 \pmod 6$ so $2^{-1} = 4$

3^{-1}: $3 + 3 = 0 \pmod 6$ so $3^{-1} = 3$

4^{-1}: $4 + 2 = 0 \pmod 6$ so $4^{-1} = 2$

5^{-1}: $5 + 1 = 0 \pmod 6$ so $5^{-1} = 1$

Proof of Theorem 7

Closure: Adding two congruence classes gives a congruence class

Associativity: Let $[a], [b], [c] \in \mathbb{Z}_n$

$$[a] + ([b] + [c]) = [a] + [b + c]$$
$$= [a + (b + c)]$$
$$= [(a + b) + c]$$
$$= [a + b] + [c] = ([a] + [b]) + [c]$$

Identity: $e = [0]$

Inverse: Let $[a] \in \mathbb{Z}_m$, $[a]^{-1} = [m - a]$?

$$[a] + [m - a] = [a + (m - a)]$$
$$= [m] = [0] = e$$

So $(\mathbb{Z}_m, +_{\bmod n})$ is a group

Example 10

Is $\{0, 1, 2, \ldots, 8\}$ under multiplication mod 9 a group?

Identity: 1

Inverses: $1^{-1} = 1$

$2^{-1} = 2 \cdot 5 = 1$ $2^{-1} = 5$

$3^{-1} = 3 \cdot \_\_ = 1$ impossible just like 6^{-1} and 0^{-1}

The inverse is not possible because $3a - 1 \equiv k9$,

$\therefore$ not a group

Remark Numbers in $\{0, 1, 2, \ldots, m-1\}$ have inverses under multiplication modulo m iff a and m have no common factors iff a and m are relatively prime iff $\gcd(m, a) = 1$

Theorem 8

If $n \geq 2$ is an integer

$$U(n) = \{ a \in \mathbb{Z} \mid 1 \leq a \leq n \text{ and } \gcd(a, n) = 1 \}$$

under multiplication modulo n is a group called $U(n)$. proof omitted

Example 11

Find the elements in

a) $U(12)$

b) $U(7)$

a) $U(12) = \{1, 5, 7, 11\}$

b) $U(7) = \{1, 2, 3, 4, 5, 6\}$ Remark: $U(\text{prime}) = \{1, 2, \ldots, p-1\}$

See Ex 11 p46

Definition

The number of elements in a group G is called the order of the group denoted by $|G|$.

Example 12

a) $|\mathbb{Z}_m| = m$

b) $|U(12)| = 4$

c) $|U(p)| = p-1$