Lecture 9

(1) $\Rightarrow$ (2) Suppose p is prime. Let $[a] \neq [0]$ in $\mathbb{Z}/p$.

Then $a \not\equiv 0 \pmod p$, i.e. $p \nmid a$ by def of congruence. Observe that $\gcd(a,p)$ divides p, then $\gcd(a,p) = p$ or $\gcd(a,p) = 1$ because of (1).

If $\gcd(a,p) = p$, then $p \mid a$. Contradiction!!!

Therefore, we must have $\gcd(a,p) = 1$.

Hence, $\exists\, u, v \in \mathbb{Z}$ s.t. $au + pv = 1$, i.e. $p \mid (au - 1)$. This is, $[a] \odot [u] = [1]$.

So, $x := [u]$ is a solution of $[a] \odot x = [1]$.

(2) $\Longrightarrow$ (3) Suppose $[b] \odot [c] = [0]$ in $\mathbb{Z}/p$ and $[b] \neq 0$.

From (2), $[b] \odot [u] = [1]$ for some $[u] \in \mathbb{Z}/p$. Then,

$$[0] = [u] \odot \big([b] \odot [c]\big) = \big([u] \odot [b]\big) \odot [c] = [1] \odot [c] = [c].$$

(3) $\Longrightarrow$ (1) Let $a, b \in \mathbb{Z}$ s.t. $p \mid ab$.

Then $[ab] = [0]$, i.e. $[a] \odot [b] = [0]$. From (3) we have that

$[a] = 0$ or $[b] = [0]$. This is, $p \mid a$ or $p \mid b$. By Thm 10,

p is prime. $\blacksquare$

Module 2 - Groups

Def: (1) A binary operation on a set G is a function $*: G \times G \to G$. For any $a, b \in G$ we write $a * b$ for $*(a,b)$.

(2) A binary operation on a set G is associative if for all $a, b, c \in G$ we have $(a*b)*c = a*(b*c)$.

(3) A binary operation on a set G is commutative if for all $a, b \in G$ we have $a*b = b*a$

Ex:

- $+$ and $\cdot$ are binary operations on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. They are associative and commutative.
- $-$ is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. It is not commutative.

- $-$ is not a binary operation on $\mathbb{N}$. $2-3=-1 \notin \mathbb{N}$.

- $\times$ cross product is a binary operation on $\mathbb{R}^3$. It is not associative and not commutative.

Def: (1) A group is an ordered pair $(G,*)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:

(i) $*$ is associative

(ii) Identity: $\exists e \in G \ \forall a \in G \ / \ a*e = e*a = a$.

(iii) Inverse: $\forall a \in G \ \exists a^{-1} \in G \ / \ a*a^{-1} = a^{-1}*a = e$.

(2) A group $(G,*)$ is called abelian if $*$ is commutative.

Examples:

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are abelian groups under $+$ with $e = 0$ and inverse $-a$.

⚠ $\mathbb{Z}$ is not a group under $\cdot$ because elements do not have inverses.
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are not groups under $\cdot$ because 0 does not have an inverse.

Convention: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are considered groups under $+$, unless otherwise stated.

2) $\mathbb{N}$ under $+$ is not a group because elements do not have inverses.

3) $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ are abelian groups under $\cdot$ with $e = 1$ and inverse $\frac{1}{a}$.

⚠ $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ are groups under $+$ because do not have an identity.

Convention: $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ are considered groups under $\cdot$, unless otherwise stated.

4) $\mathbb{Z}/n$ under $\oplus$ is an abelian group with $e = [0]$ and inverse $[-a]$.

⚠ $\mathbb{Z}/n$ is not a group under $\odot$ because in general elements do not have inverses.

Convention: $\mathbb{Z}/n$ is considered a group under $\oplus$, unless otherwise stated.

5) $(\mathbb{Z}/n)^\times$ under $\odot$ is an abelian group with $e = [1]$.

⚠ $(\mathbb{Z}/n)^\times$ is not a group under $\oplus$ because does not have an identity.

Convention: $(\mathbb{Z}/n)^\times$ is considered a group under $\odot$, unless otherwise stated.

6) If p is prime, $\mathbb{Z}/p \setminus \{[0]\} = (\mathbb{Z}/p)^\times$. Here $(\mathbb{Z}/p, \oplus)$ and $((\mathbb{Z}/p)^\times, \odot)$ are abelian groups.

Convention: From now on we'll write $+$ and $\cdot$ for $\oplus$ and $\odot$ in $\mathbb{Z}/n$.

7) The dihedral group of order $2n$, D_{2n}, is a nonabelian group.

8) Let $M_{m\times n}(\mathbb{R}) := \{ A \mid A \text{ is a } m\times n \text{ matrix with real entries} \}$.

$(M_{m\times n}(\mathbb{R}), +)$ is an abelian group with $e = 0_{m\times n}$ and inverse $-A$

matrix addition

9) The General Linear Group of Degree n over $\mathbb{R}$ with $n>0$.

$$GL(n, \mathbb{R}) := \{ A \in M_{n\times n}(\mathbb{R}) \mid A \text{ is invertible} \}$$

$(GL_n(\mathbb{R}), \cdot)$ is a nonabelian group with $e = I_n$ and inverse A^{-1}.

matrix multiplication

10) $L := \{1, -1, i, -i\} \subseteq \mathbb{C}$. $(L, \cdot)$ is an abelian group with $e = 1$ and

$$1^{-1} = 1, \quad (-1)^{-1} = -1, \quad i^{-1} = -i, \quad \text{and} \quad (-i)^{-1} = i$$

11) $F := \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ is continuous}\}$. If $f, g \in F$, then $(f+g)(x) = f(x) + g(x)$.

$(F, +)$ is an abelian group with $e = \mathbf{0}$ and inverse $-f$

$\mathbf{0}(x) = 0$ $\qquad (-f)(x) = -f(x)$.

12) If $(A, *)$ and $(B, \bullet)$ are groups, we can form a new group $(A \times B, \cdot)$ called the direct product of A and B where

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\} \quad \text{and} \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_1, \; b_1 \bullet b_2)$$

operation is defined componentwise

with $e = (e_A, e_B)$ and inverse (a^{-1}, b^{-1}).

Prove that $(A \times B, \cdot)$ is a group.

Prove that $(A \times B, \cdot)$ is abelian iff $(A, *)$ and $(B, \bullet)$ are abelian.

Ex:

- $(\mathbb{Z} \times \mathbb{Z}, +)$
- $(\mathbb{Z}/n \times \mathbb{Z}/m, +)$
- $(\mathbb{Z}/p \times \mathbb{Q}, \cdot)$ p prime
- $(\mathbb{R} \times \mathbb{R}, \cdot)$
- $(D_4 \times GL_3(\mathbb{R}), \cdot)$
- $((\mathbb{Z}/n)^{\times} \times \mathbb{C}, \cdot)$
- $(M_{2\times 3}(\mathbb{R}) \times L, \cdot)$

13) The trivial group $(\{e\}, *)$.

Basic Properties of Groups

Proposition 1: If G is a group under the operation $*$, then

(1) The identity of G is unique.

(2) Each element of G has unique inverse.

(3) The equations $a * x = b$ and $y * a = b$ have unique solutions in G. In particular, left and right cancellation laws hold:

$$(a*b = a*c \Rightarrow b = c) \text{ and } (b*a = c*a \Rightarrow b = c).$$

Proof: Exercise.

! One consequence of part (3) is that in order to prove $\triangle^{-1} = \square$ we don't have to show $\triangle * \square = e$ and $\square * \triangle = e$. It's enough to proof only one.

Corollary 2: (4) $(a^{-1})^{-1} = a$ for all $a \in G$.

(5) $(a * b)^{-1} = b^{-1} * a^{-1}$ (socks - shoes property)

a	putting on socks	a^{-1}	taking off socks
b	putting on shoes	b^{-1}	taking off shoes

Proof:

(1) Observe that $a^{-1} * a = e$. Therefore, the inverse of a^{-1} is a.

(2) Exercise.

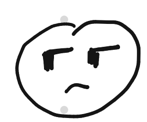
Notation: $(G, *)$ a group, $a \in G$ and $n \in \mathbb{Z}^+$

$$a^n := \underbrace{a * a * \cdots * a}_{n\text{-times}} \qquad a^{-n} := \underbrace{(a^{-1}) * (a^{-1}) * \cdots * (a^{-1})}_{n\text{-times}}$$

$$a^0 = e$$

Ex:

- $(\mathbb{Z}/3)^\times$: $\quad [2]^4 = [2] \cdot [2] \cdot [2] \cdot [2] = [16] = [1]$
- $GL_2(\mathbb{R})$: $\quad \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}^2 = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 7 & 4 \\ 12 & 7 \end{pmatrix}$

Observe that this notation does not seem suitable in $(\mathbb{Z}, +)$ because we would have that $5^3 \overset{\text{notation}}{=} 5 + 5 + 5$ , which looks bad because for us 5^3 means $5 \times 5 \times 5$, and $5 + 5 + 5$ is what we write as $3 \cdot 5$.

Types of Notation: In order to avoid that confusion, we will define two types of notation: multiplicative notation $(\cdot)$ and additive notation $(+)$

		Multiplicative Notation $(G, \cdot)$	Additive Notation $(G, +)$
Operation	$a * b$	ab	$a + b$
Identity	e	1	0
Inverse	a^{-1}	a^{-1}	$-a$
Exponents	a^0	$a^0 = 1$	$0a = 0$
$n \in \mathbb{Z}^+$	$\underbrace{a * \cdots * a}_{n\text{-times}}$	$a^n = \underbrace{a a \cdots a}_{n\text{-factors}}$	$na = \underbrace{a + a + \cdots + a}_{n\text{-summands}}$
	$\underbrace{a^{-1} * \cdots * a^{-1}}_{n\text{-times}}$	$a^{-n} = \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{n\text{-factors}}$	$(-n)a = \underbrace{-a - a - \cdots - a}_{n\text{-summands}}$

Here "·" and "+" are not multiplication and addition as we know them, they are notational symbols.