Lecture 5 & 6 (MA 2070 - Introduction to Group Theory)

Jan 18, 2022

Jan 21, 2022

Revision of basics.

A (binary) relation on a set A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.

Equivalence relation. Let X be a set. An equivalence relation $\sim$ is a relation on X, which is

$\leq$ or R $\quad aRb \quad a \leq_R b \quad a \sim b$

(a) (Reflexive) For every $x \in X$, $x \sim x$ $\quad a = a$

(b) (Symmetric) for every $x, y \in X$, if $x \sim y$, then $y \sim x$.

(c) (Transitive) for every $x, y, z \in X$, if $\underline{x \sim y}$ and $\underline{y \sim z}$, then $\underline{x \sim z}$.

$\boxed{\mathbb{Z}, \sim \text{ congruence relation}}$

Examples.

1. $X = Sym_n(\mathbb{R})$ $\quad \sim \quad A \sim B$ if $\underline{A = B^T}$

$A = B^T$

2. $\mathbb{R}$ $\quad \sim$

$a \sim b$ if $a = b$

$(\mathbb{R}, \sim)$ where $a \sim b$ if $a < b$

read as tilde $\leq$, R

Equivalence class. Let $\sim$ or $\leq$ or R be an equivalence relation on a set X. Let $a \in X$ be an element of X. The equivalence class of a is

$$\{ b \in X \mid b \sim a \}$$

$$[a] = \{ b \in X \text{ such that } b \sim a \}.$$

Examples.

1. $\mathbb{R}$, $\sim$

$a \sim b$ if $a = b$

$$[a] = \{a\}$$

2.

$\mathbb{Z}/_{n\mathbb{Z}}$: The integers modulo n.

Let n be a fixed positive integer.

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

$a \sim b$ if and only if n divides $b-a$

Exercise. Verify that $\sim$ is an equivalence relation.

divides

$$a \sim b \iff n \mid b-a$$

$$\Updownarrow$$

$a \equiv b \pmod{n}$

" a is <u>congruent to b mod n</u> ".

Equivalence class of a is

$$[a] = \{ b \in \mathbb{Z} \text{ such that } b \sim a \}$$

$$= \{ a + kn \text{ such that } k \in \mathbb{Z} \}$$

$$= \{ a,\ a \pm n,\ a \pm 2n, \dots \}$$

divides

$n \mid a-b$

$\Rightarrow a-b = \mu n ;\ \mu \in \mathbb{Z}$

$\Downarrow$

$a - \mu n = b$

$\shortparallel$

$a + \mu' n = b$

$\mu' \in \mathbb{Z}$

There are precisely n distinct equivalence classes modulo n,

namely,

$$[0] = \{ kn \mid k \in \mathbb{Z} \}$$

$$[1] = \{ 1 + kn \mid k \in \mathbb{Z} \}$$

$$[2] = \{ 2 + kn \mid k \in \mathbb{Z} \}$$

$$\vdots$$

$$[n-1] = \{ n-1 + kn \mid k \in \mathbb{Z} \}$$

$x \in \mathbb{Z}$

Notation. $[a]$ or $\bar{a}$

$[a] = \bar{a}$

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

$$[0] = \bar{0}, \quad [1] = \bar{1}, \quad [n-1] = \overline{n-1}$$

same notations

Define

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

map = f

$$(\bar{a}, \bar{b}) \longmapsto +(\bar{a}, \bar{b}) = \overline{a+b}$$

f

$\overline{a+b} = (a+b) \bmod n$

Define

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

$$(\bar{a}, \bar{b}) \longmapsto \cdot(\bar{a}, \bar{b}) := \overline{ab}$$

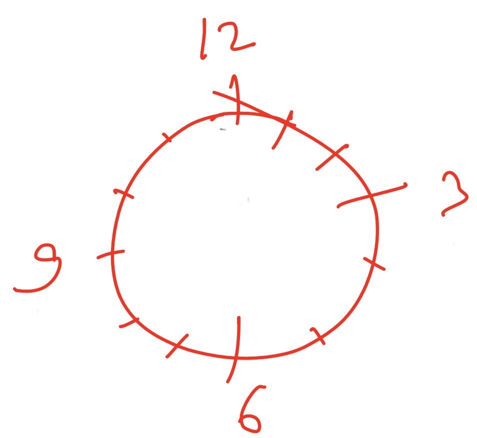
$$= ab \bmod n$$

Question. Why $+$ and $\cdot$ are well-defined?

[Exercise].

Examples.

clock



1. $(\mathbb{Z}/12\mathbb{Z}, +)$

2. $(\mathbb{Z}/7\mathbb{Z}, +)$

3. $(\mathbb{Z}/24\mathbb{Z}, +)$ 24 hr. clock.

4. $(\mathbb{Z}/5\mathbb{Z}, +)$

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

Exercise. Number of elements in $(\mathbb{Z}/n\mathbb{Z})^{\times}$ = ??

$$\# \left\{ [a] \text{ s.t. } \exists\ [c] \text{ with } [a]\cdot[c] = [1] \right\}$$

no. of equivalence classes.

Exercise. Prove that $\left((\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot \right)$ is a group.

A

$$\underset{\text{binary operation}}{\cdot} : \underset{A}{(\mathbb{Z}/n\mathbb{Z})^{\times}} \times \underset{A}{(\mathbb{Z}/n\mathbb{Z})^{\times}} \longrightarrow \underset{A}{(\mathbb{Z}/n\mathbb{Z})^{\times}}$$

$$(\bar{a}, \bar{b}) \longmapsto \cdot(\bar{a}, \bar{b}) = \bar{a}\cdot\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$$

To prove $\left((\mathbb{Z}/n\mathbb{Z})^{\times}, \cdot \right)$ is a group, we need the following

- $\bar{a}\cdot\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ [To check $\cdot$ is a binary operation]
- $(\bar{a}\cdot\bar{b})\cdot\bar{c} = \bar{a}\cdot(\bar{b}\cdot\bar{c})$ [Associativity] (Exercise) $\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$
- Existence of identity $[1]$
- Existence of inverse for every element $[a]\cdot[c] = [1]$ (by definition)

Definition. Consider the following set

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} = \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \text{ such that there exists } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a}\cdot\bar{c} = \bar{1} \right\}$$

$\times$ ← multiplicative set

$\bar{a} = [a]$, $\bar{c} = [c]$

$[a]\cdot[c] = [1]$

$[a]\cdot[c] = [a\cdot c]$

$$\left(\mathbb{Z}/3\mathbb{Z}\right)^{\times} = \left\{ \cancel{[0]}\ [1], [2] \right\}$$

$\underbrace{[0], [1], [2]}$

$$\left(\mathbb{Z}/9\mathbb{Z}\right)^{\times} = \left\{ \cancel{[0]}, [1], [2], [5] \right\}$$

$[0], [1], [2], \ldots, [8]$

not possible

$[0]\cdot[c] = [1]$

$[0\cdot c] = [1]$

$\cancel{[0] = [1]}$

no. of element in $\left(\mathbb{Z}/9\mathbb{Z}\right)^{\times} = 6$

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

$\bar{a}$

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

$\varphi(9) = 6$

$\bar{c} \to \bar{1}, \bar{5}, \bar{7}, \bar{2}, \bar{4}, \bar{8}$

$\bar{a}\cdot\bar{c} \Rightarrow \bar{1}, \overline{10}, \overline{28}, \overline{10}, \overline{28}, \overline{64}$

$\qquad\quad\ \ = \bar{1}, \bar{1}, \bar{1}, \bar{1}, \bar{1}, \bar{1}$

Definition. Let $n \in \mathbb{Z}^+$.

Euler φ-function

$\varphi(n) :=$ number of positive integers $a \leq n$ which are relatively prime to n

$$\begin{gathered} \| \\ \# \{ a \in \mathbb{Z}^+ \text{ s.t. } \gcd(a,n) = 1 \} \end{gathered}$$

number of

Exercise. p, q prime numbers in $\mathbb{Z}$.

(i) $\varphi(p) = p-1$ $\quad (\mathbb{Z}/p\mathbb{Z})^\times$

(ii) $\varphi(pq) = (p-1)(q-1)$ $\quad (\mathbb{Z}/pq\mathbb{Z})^\times$

(iii) $\varphi(p^n) = p^{n-1}(p-1)$

(iv) $\varphi(mn) = \varphi(m)\varphi(n)$ if $\gcd(m,n) = 1$

Use Euclid division algorithm
$\exists\, x, y \in \mathbb{Z}$ s.t.
$ax + ny = 1$
$ax = 1 - ny$
Apply mod n now.

Exercise. If $a \in \mathbb{Z}$ and $\gcd(a,n) = 1$, then

$$ax \equiv 1 \mod (n) \quad \text{for some } x \in \mathbb{Z}$$

Using previous exercise, we conclude that

$\bar{x}$ is the multiplicative inverse of $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$

$\bar{c}$ behaves like inverse of $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} = \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \text{ such that there exists } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a}\cdot\bar{c} = \bar{1} \right\}$$

"Collection of multiplicative inverse"

$$\boxed{\#\left(\mathbb{Z}/n\mathbb{Z}\right)^{*} = \varphi(n)}$$

Definition.

$A = \{1, 2, 3\}$

Notation $|A| = 3$, $\# A = 3$ both are commonly used

Cardinality of a set $:=$ the number of elements of A

When the set A has a group structure, we often call it order of A (instead of cardinality of A)

$(G, *)$ $\quad x \in G$

Order of an element. Let G be a group, and $x \in G$.

The order of x is the smallest positive integer n such that $x^n = 1$ ← identity element

$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\operatorname{ord}(A) = 1$

$$x^n = [x * x * \cdots * x] \quad [n \text{ times}]$$

$G = (M_2(\mathbb{R}), \cdot)$

Is this a group?

ord G = infinite

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Notation.

$$\left\{ \begin{array}{c} \operatorname{ord}(x) = n \\ \text{or} \\ |x| = n \end{array} \right.$$

$A = \begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix}$

$\operatorname{ord}(A) = \infty$

If no positive powers of x is the identity, we define $\operatorname{ord}(x) := \infty$

[We say x is of infinite order]

$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}^n =$

$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^n =$

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ✗

$\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$

Exercise. For any $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 * a_2 * \cdots * a_n$ is independent of how expression is bracketed.

$(G, *)$ some group

Infinite order elements	Finite order elements

identity

$(\mathbb{Z}, +)$ $\quad e = 0$

$\underbrace{1+1+\cdots+1}_{n \text{ times}} = n1 \neq 0$

$(\mathbb{Q}, +)$

$(\mathbb{R}, +)$

$(\mathbb{C}, +)$

$a + a + \cdots + a = 1$

not possible

Every non-zero (non-identity) element has infinite order.

identity 1

$(\mathbb{R} - \{0\}, \cdot)$ $\quad r \cdot 1 = 1 \cdot r = r$

$(\mathbb{Q} - \{0\}, \cdot)$

$\text{ord}(2) = \infty$

$2^n \neq 1$

$\text{ord}(-1) = 2$

$(-1)\cdot(-1) = 1$

$2 \neq 1 \quad 2^2 \neq 1 \quad 2^3 \neq 1 \quad \cdots$

$(\mathbb{Z}/9\mathbb{Z}, +)$ or $(\mathbb{Z}/3\mathbb{Z}, +)$

$(GL_2(\mathbb{R}), \cdot)$

$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ $\quad \text{ord}(A) = \infty$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 0 \end{bmatrix}$$

Proposition. Let $(G, *)$ be a group. Then the following holds

(1). The identity of G is unique.

Proof. Suppose e_1 and e_2 are both identity element in G.

Then $e_1 * e_2 = e_1$ and $e_1 * e_2 = e_2$.

Hence $e_1 = e_2$.

(2). For each $a \in G$, a^{-1} is uniquely determined.

Proof.

Assume that b and c are both inverses of a.

Then

$$a * b = e \quad \text{and} \quad c * a = e.$$

Now, write

$$\begin{aligned}
c &= c * e && [\text{by definition of identity}] \\
&= c * (a * b) && [\text{Since } e = a * b] \\
&= (c * a) * (b) && [\text{Associative law holds in } G \text{ w.r.t. } *] \\
&= e * b && [\text{Since } e = c * a] \\
&= b && [\text{by definition of identity}]
\end{aligned}$$

Hence $c = b$.

(3). $(a^{-1})^{-1} = a$ for every $a \in G$.

Exercise.

Here: $(a^{-1})^{-1} = a$ mean a is the inverse of a^{-1}.

(4). $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Proof.

Note that $a*b \in G$, and hence $(a*b)^{-1} \in G$.

Assume that $(a*b)^{-1} = c$ some element in G.

Then $(a*b) * c = e$.

$$\|$$

$$a * (b*c) = e$$

$$a^{-1} * (a * (b*c)) = a^{-1} * e \qquad \text{[Multiply both sides by } a^{-1}\text{]}$$

$$\underbrace{(a^{-1} * a)}_{e} * (b*c) = a^{-1} \qquad \text{[Associative law]}$$

$$b*c = a^{-1}$$

Again multiply both sides by b^{-1} and use associative law to get $c = b^{-1} * a^{-1}$.

5. For any $a_1, a_2, \cdots, a_n \in G$,

$a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed.

Proof. Exercise.

Notations.

*	When * is multiplication	When * is additive
$a * b$	$a \cdot b$ or ab	$a+b$
identity element (e or 1)	identity or one	zero
a^{-1}	Multiplicative inverse of a	$-a$ [Additive inverse of a]
a^n	Power of a $\underbrace{a \cdot a \cdots a}_{n \text{ times}}$	Multiple of a $\underbrace{a+a+\cdots+a}_{n \text{ times}}$
ab^{-1}	Quotient	$a-b$ Difference

a^n under multiplication

$a \cdot a \ldots a$ (n times)

[This does not depend upon how bracketing]

$a^{-n} = a^{-1} \cdot a^{-1} \ldots a^{-1}$ (n times)

[Assuming a is invertible]

$a^0 = 1$ [1 for the identity element]

---

a^n under addition

$a^n = a + a + \ldots + a$ (n times)

$a^{-n} = -a - a \ldots - a = (-a) + (-a) + \ldots + (-a)$

$a^0 = 0 \cdot a = 0$ [identity element is zero, 0]

$\cancel{\alpha} \cdot u = \cancel{\alpha} \cdot v$

$u = v$

$\cancel{0} \cdot 1 = \cancel{0} \cdot 2$

$\Rightarrow 1 = 2$ $\times$

Proposition. [Concellation Law]

$AX = B$

Let a, b be element of G. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$.

In particular, the left and right concellation low holds in G.

(i) If $au = av$, then $u = v$

(ii) If $ub = \cancel{u}vb$, then $u = v$.

Proof.

Given equation $ax = b$,

$$a^{-1} \cdot ax = a^{-1} \cdot b$$

$$\Rightarrow \boxed{x = a^{-1}b.}$$

[inverse if exists is unique]

Similarly, get $y = ba^{-1}$

(i) If $au = av$, then $a^{-1}au = a^{-1}av$

$$\Rightarrow u = v$$

Similarly (ii).

$GL_n(\mathbb{R}) = \{ n \times n$ matrices A with $\det(A) \neq 0 \}$.

$A, B, C \in GL_n(\mathbb{R})$; with $AB = AC$.

Then $A^{-1} \cdot AB = A^{-1} \cdot AC$

$\Rightarrow B = C$.

Recall. A subset H of a group G is called a Subgroup if it has the following properties:

[a] Closure If $a \in H$ and $b \in H$, then $ab \in H$

[b]. Identity $1 \in H$

[c]. Inverse If $a \in H$, then $a^{-1} \in H$.

Note. The "Associative Law" is not mentioned above. It carries over automatically from G to H.

Proper Subgroup. We say H is a proper subgroup of G if $H \neq \{1\}$, and $H \neq G$.

trivial   whole group

$$H \subseteq (\mathbb{Z}, +)$$

$2H = 2\mathbb{Z}$

$3H = 3\mathbb{Z}$

Subgroups of additive group $(\mathbb{Z}, +)$

Define for an integer b;

$$b\mathbb{Z} = \{ bm \text{ such that } m \in \mathbb{Z} \}$$

$$= \{ n \in \mathbb{Z} \text{ such that } n = bm \text{ for some } m \in \mathbb{Z} \}$$

We proved that $(b\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$

$$\left\{ \begin{array}{lll} bn_1 + bn_2 = b(n_1 + n_2) \in b\mathbb{Z} & & \text{Closure} \\ -(bn) = b(-n) & & \text{Inverse} \\ 0 \in b\mathbb{Z} & & \end{array} \right.$$

Proposition. For any integer b, the subset $b\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$.

Moreover, *every subgroup* of $(\mathbb{Z},+)$ is of the form $H = b\mathbb{Z}$ for some integer b.

Proof.

$b\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$.

2^{nd} Claim. Every subgroup is of the form $b\mathbb{Z}$ for some b.

Proof.

Cases: (i) If 0 is the only element of H, then

$$H = 0\cdot\mathbb{Z}$$

$\mathbb{Z}$

$\cup$

$H = \{2, 3, 0, -5\}$

$-3 \quad -2 \quad 5$

(ii) If there are more elements in H, lets say some positive / negative integers $\in H$

$a \in H \implies -a \in H$ [by definition of subgroup

Clearly $H \supseteq \{$ some $-$ve integers, 0, some $+$ve integers$\}$

$H = \{$ some $-$ve integers, 0, $\underbrace{\text{some +ve integers}}\}$

$n \in$

Let b be the smallest positive integer in H.

Claim $H = b\mathbb{Z}$

$A = B$

$A \subseteq B$

$B \subseteq A$

To show this, we need to show

$b\mathbb{Z} \subseteq H$, ... (i)

$H \subseteq b\mathbb{Z}$ ... (ii)

$(H, +) \leq (\mathbb{Z}, +)$

(i). $b\mathbb{Z} \subseteq H$.

$bk = b + b + \cdots + b$ (k times) (Assume wlog k is positive)

$\in H$

$b(-k) = -bk \in H$

& $b \cdot 0 = 0 \in H$

$b \in H$

$\underbrace{b + b + \cdots + b}_{q \text{ tim}} \in H$

r must be in H

$\in H$

$n \in H$, $\cancel{b \in H}$; $0 \leq r < b$

$n = b \cdot q + r$

??

$\boxed{r = 0}$

(ii) $H \subseteq b\mathbb{Z}$

Let $n \in H$, then $n = bq + r$; where $0 \leq r < b$

Prove that $r = 0$.

$\Rightarrow$ $n = bq \in b\mathbb{Z}$. This completes the proof.