Quiz 1. One question on equivalence relation.
One question on group properties.
See Sample Quiz

Notation $(G,*)$ / G

$a, b \in G$ $\quad ab = c \in G$

$a^{-1}a = aa^{-1} = e$

Chapter 3 Finite groups and Subgroups

Definition Let G be a group.

- The *order* of G, denoted by $|G|$ is the cardinality (finite or infinite) of G.
- The *order* of an element $g \in G$ is the smallest positive integer n such that $g^n = e$ if n exists.
- Else, the order of g, denoted by $|g|$, is infinite.
- A subset $H \subseteq G$ is a *subgroup* of G, denoted by $H \leq G$, if H is a group under the same binary operation.

Examples $(G,+) = (\mathbb{Z}_n, +)$, $|G| = n$

$(G,*) = (\mathbb{Z}, +)$; $|G| = \aleph_0$

$(G,*) = (\mathbb{R}, +)$, $|G| = c$

$(G,*) = (\mathbb{C}, +)$, $|G| = c$

$|\mathbb{C}| = |\mathbb{R}\times\mathbb{R}| = 2\cdot|\mathbb{R}| = c$.

$(G,*)$, $(\mathbb{R}^*, \cdot)$, $|G| = c$

Example $\mathbb{Z}_{12}$ $\quad \mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{11}\}$

$|\bar{0}| =$

$12\bar{1} + \dots + \bar{1} = \bar{0}$

$n\bar{1} + \dots + \bar{1} = \bar{0}$

$\bar{2} + \dots + \bar{2} = \bar{0}$

$\bar{3} + \dots + \bar{3} = \bar{0}$

$\bar{5} + \dots + \bar{5} = \bar{0}$ (k terms)

$5k = 12\cdot l$

$7k = 12\cdot g$

$8k = 12g$

$|\bar{0}| = 1$

$|\bar{1}| = 12$

$|\bar{2}| = 6$

$|\bar{3}| = 4$

$|\bar{4}| = 3$

$|\bar{5}| = 12$

$|\bar{6}| = 2$

$|\bar{7}| = 12$

$|\bar{8}| = 3$

$|\bar{9}| = 4$

$|\bar{10}| = 6$

Fact:

$\bar{k} \in \mathbb{Z}_n$,

$\gcd(n,k) = d$

Then $|\bar{k}| = \frac{n}{d}$.

Proof: want smallest m s.t. $mk = ng \Rightarrow m = \frac{n}{d}$

Examples $(\mathbb{R}, +)$ / $(\mathbb{Z}, +)$

$\forall x \in \mathbb{R}$ $|x| = \infty$ if $x \neq 0$

$|0| = 1$

Example $(\mathbb{C}^*, \cdot)$ / $(\mathbb{R}^*, \cdot)$

$|1| = 1$

$|i| = 4$

$|2| = \infty$

$|1| = 1$

$|-1| = 2$

$|2| = \infty$

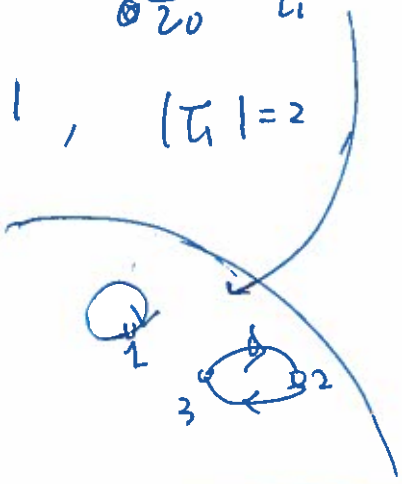
Example $S_3 = \{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \}$

τ_0 τ_1 τ_2 τ_3 τ_4 τ_5.

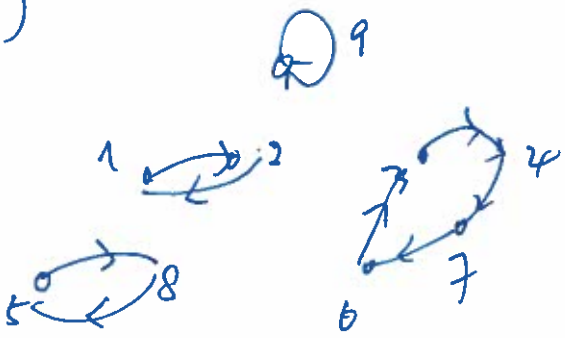
$|\tau_0| = 1$, $|\tau_1| = 2$ $|\tau_2| = 2$, $|\tau_3| = 3$

$|\tau_4| = 3$

$|\tau_5| = 2$



$\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&1&4&7&8&3&6&5&9\end{pmatrix}$



Examples:

$$(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+) \quad \checkmark$$

φ subgroup φ

$\subseteq$

$\subset$

Example $\quad (\mathbb{R}^*,\cdot) \not\leq (\mathbb{R},+)$

More terminology and notation

- If $H \leq G$ and $H \neq G$, then H is a **proper subgroup** of G and we write $H < G$;
- otherwise, H is the **improper subgroup**.
- If $H = \{e\}$, then H is the **trivial subgroup**;
- otherwise, H is a **non-trivial subgroup**.

$G \leq G$

Theorem 3.1 Let G be a group and H be a **non-empty** subset of G. Then H is a subgroup of G if and only if $ab^{-1} \in H$ whenever $a, b \in H$.

Applications

$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$

To prove $T_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : T \text{ is in upper triangular form}, \det(T) \neq 0\}$

is a subgroup of $GL_n(\mathbb{R})$ under matrix multiplication.

$T = \begin{bmatrix} t_{11} & & * \\ & \ddots & \\ 0 & & t_{nn} \end{bmatrix}$

$\det(T) = t_{11} \cdots t_{nn} \neq 0.$

(⇒) Assume $H \leq G$.

Let $a, b \in H$:

$\therefore b^{-1} \in H$ ∵ H is a group under the same operation. (G3)

$\therefore ab^{-1} \in H$ because of (G0)

(⇐) ~~$\therefore ab^{-1} \in H$~~

Assume $H \subseteq G$, $H \neq \phi$

and $ab^{-1} \in H$ whenever $a, b \in H$.

4° (G0)/(H0)

1° (G1)/(H1) → $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow (ab)c = a(bc)$

2° (G2)/(H2) $H \neq \phi \Rightarrow \exists a \in H \Rightarrow a, a \in H \Rightarrow ab^{-1} = aa^{-1} = e \in H$

3° (G3)/(G3) $b \in H \Rightarrow e, b \in H \Rightarrow eb^{-1} \in H$

Finally (4°), $a, b \in H \Rightarrow a \in H$, $b^{-1} \in H$ by (3°) $\Rightarrow a(b^{-1})^{-1} = ab \in H$

$\therefore (H, *)$ is a subgroup ∵ $(G, *)$ is the

① Check $T_n(\mathbb{R}) \neq \phi$.

$A = I_n \in T_n(\mathbb{R})$.

② Let $A, B \in T_n(\mathbb{R})$

(2.a) Show $B^{-1} \in T_n(\mathbb{R})$ $\det(B^{-1}) = \frac{1}{\det(B)}$

(2.b) $AB^{-1} \in T_n(\mathbb{R})$

$\therefore AB^{-1} \in T_n(\mathbb{R})$

Theorem 3.2 Let G be a group and H be a **non-empty** subset of G.
Then H is a subgroup of G if and only if

(1) $ab \in H$ whenever $a, b \in H$, and (2) $a^{-1} \in H$ whenever $a \in H$.

Proof (⇒) Let $H \leq G$.

(1) If $a, b \in H$. Then $ab \in H$ by (G0) on H

(2) If $a \in H$, then $a^{-1} \in H$ by (G3) on H.

(⇐) ~~(G0) by (1)~~ Assume $H \subseteq G$, $H \neq \phi$, (1) & (2) hold.

To prove (G0): By (1)

To prove (G1): $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow (ab)c = a(bc)$.

To prove (G2): $H \neq \phi \Rightarrow \exists a \in H \Rightarrow a^{-1} \in H$ by (2)

$\Rightarrow a(a^{-1}) = e \in H$ by (1)

To prove (G3): by (2)

Remark: Let $H \leq G$

$\hat{e} \in H$ is the same as $e \in G$

$a \in H$, the inverse $\hat{a}$ in H is the same as $a^{-1} \in G$.

Proof: Let $\hat{e} \in H$ be the identity in H.

i.e. $\hat{e}h = h\hat{e} = h \ \forall h \in H$

Let $e \in G$ be the identity in G. Then

$\hat{e}h = h = eh$ (h in H; eh in G) $\Rightarrow \hat{e} = e$ by cancellation

Alternatively, $\hat{e}\hat{e} = \hat{e} = e\hat{e}$

$\hat{h}h = e$ in H ✓

$h^{-1}h = e$ in G ✓

$\hat{h} = h^{-1}h$ in G