Lecture 9:

Some lemmas:

Lemma: e is unique.

proof Assume e_1, e_2 both satisfy the condition

$$\forall x \in G, \quad x * e = e * x = x.$$

Then $e_1 * e_2 = e_1$ because e_2 is identity

$e_1 * e_2 = e_2$ because e_1 is identity.

□

Lemma: $\forall a, b, c \in G$, $a * b = a * c \Rightarrow b = c$.

and: $b * a = c * a \Rightarrow b = c$

proof: $a * b = a * c \Rightarrow \underbrace{a^{-1} * a}_{e} * b = \underbrace{a^{-1} * a}_{e} * c$

$\Rightarrow b = c.$

similarly for $b * a = c * a \Rightarrow b = c$. □

Lemma: G a group, $a, b \in G$, then the equation $a * x = b$ has a unique solution x.

proof: $a * x = b \Leftrightarrow a^{-1} * a * x = a^{-1} * b$

$\Leftrightarrow x = a^{-1} * b.$

(Corollary of 2nd lemma)

Lemma: (Inverses are unique) If $a * b = b * a = 1$ and $a * c = c * a = 1$

then $b = c$.

proof: $a * b = a * c \Rightarrow b = c$ by lemma above.

Subgroups:

So far, examples of groups we looked at:

$(\mathbb{Z},+)$, $(\mathbb{Z}/n\mathbb{Z},+)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$

$(U,\cdot)$, $(M_n(\mathbb{R}),+)$, $(GL_n(\mathbb{R}),\cdot)$

U: unit circle in $\mathbb{C}$, i.e. $e^{i\alpha}$'s.

$GL_n(\mathbb{R})$: invertible matrices with matrix multiplication.

If G $(=(G,*))$ is a group, and $H \subset G$ is a subset, then we can look at the induced operation: $*: H\times H \to G$.

Def: If this induced operation is a binary operation on H and $(H,*)$ is a group, then H is called a subgroup of G.

(denoted $H \leq G$)

Proposition: ($(G,*)$ a group.) $H \subset G$ is a subgroup iff:

(1) H is closed under $*$. (ie $\forall x,y\in H,\ x*y\in H$)

(2) $e\in H$

(3) $\forall a\in H,\ a^{-1}\in H$ (closed under taking inverses)

Proof: Assume $H\leq G$ is a subgroup. Then by group axioms for H, (1), (2), (3) must hold.

On the other hand, if (1),(2),(3) hold for H: ~~then~~ (1) implies that $*$ is a binary operation on H.

(2) implies that there is identity in H.

(3) implies that there are inverses in H.

(associativity follows from associativity in G). $\square$

Examples:

(1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (under addition)

are subgroups.

(2) $\{e\} \subset G$ is a subgroup for any group.

↑ trivial group.
trivial subgroup

(3) $U_n \leq U \leq \mathbb{C}$ are subgroups.

$U_n : \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$

$\zeta = e^{i\frac{2\pi}{n}}$

- same operation.
- $(\zeta^k)^{-1} = \zeta^{n-k}$ ✓ closed under inverses
- $\zeta^a \zeta^b = \zeta^{a+b \pmod n}$ ✓ closed under the operation
- $1 \in U_n$.

Similarly for $U \leq \mathbb{C}$.

(4) What are the subgroups of $\mathbb{Z}/2\mathbb{Z}$?

$\{\bar{0}\}$, $\mathbb{Z}/2\mathbb{Z}$

↑ trivial

(5) What are the subgroups of $\mathbb{Z}/4\mathbb{Z}$?

$\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$, $\mathbb{Z}/4\mathbb{Z}$

$\bar{1}+\bar{1}$ ↙ ↘ $\bar{1}+\bar{1}+\bar{1}=\bar{3}$

why? if $\bar{1} \in H$, then $\bar{2}, \bar{3} \in H$ too.
but $\bar{0}$ is e so it will be in any subgroup.
If $\bar{3} \in H$, then $\bar{3}+\bar{3} = \bar{2} \in H$ and $\bar{2}+\bar{3} = \bar{1} \in H$ too..

(6) $GL_n(\mathbb{R}) \geq SL_n(\mathbb{R})$

↳ $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$.

$SL_n(\mathbb{R})$ is a subgroup because.

- it is closed under "$\cdot$". Indeed if $\det A = \det B = 1$ then $\det(AB) = \det A \det B = 1$.
- closed under inverses.

$$\det(A^{-1}) = \frac{1}{\det A}$$

→ because $\det(AA^{-1}) = \det(I) = 1$

$\det(A)\det(A^{-1})$

so if $A \in SL_n(\mathbb{R})$, then $A^{-1} \in SL_n(\mathbb{R})$.

- $I \in SL_n(\mathbb{R})$.

Def: If G is a group, the number of elements $|G|$ is called the order of G.

ex: $|\mathbb{Z}/4\mathbb{Z}| = 4$.

$|U_n| = n$.

Remark. if $G \cong G'$ then $|G| = |G'|$.

(isomorphic)

Def: (Product group:). If G, G' are groups, $(G, *_1), (G', *_2)$ then $G \times G' = \{(g, g') \mid g \in G, g' \in G'\}$ is a group with operation:

$$(g, g') * (h, h') = (g *_1 h, g' *_2 h')$$

Exercise: check group axioms for $G \times G'$.

Example: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$

has subgroups $\{(\bar{0}, \bar{0})\}$, $\{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\}$, $\{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$, $\{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\}$.

SO THIS GROUP IS NOT ISOMORPHIC TO $\mathbb{Z}/4\mathbb{Z}$!!!