1/27

- Groups $(G, *, e)$ $\quad a^{-1}$

- We are going to move into the topic of subgroups

3.3

Examples will include the trivial subgroups and cyclic subgroups.

$$G \quad * : G \times G \to G$$

$$*|_{H\times H}(h_1, h_2) = *(h_1, h_2)$$

$$\emptyset \neq H \subseteq G \qquad H \times H \subseteq G \times G.$$

Ex. $\mathbb{R}$. $H = \mathbb{R} \setminus \mathbb{Q}$

Thm Subgroup Criterion Test: (one-step test)

Let H be a nonempty subset of G. H is a subgroup of G iff $\forall h_1, h_2 \in H$, $h_1 * h_2^{-1} \in H$.

Pf: $H \neq \emptyset$

$\Leftarrow$ $h_1 \in H$ By Crit. $e = h_1 \cdot h_1^{-1} \in H$

$h_1, h_2 \in H$ $\quad h_2^{-1} = e \cdot h_2^{-1} \in H$ $\qquad h_1 \cdot (h_2^{-1})^{-1} \in H$

$= h_1 h_2$

In linear algebra you learned about subspaces. There is a similar notion in Group Theory.

Def Let $(G, *, e)$ be a group. A subgroup H of G is a non-empty subset that satisfies i) $e \in H$, ii) if $h_1, h_2 \in H$, then $h_1 * h_2 \in H$, and iii) if $h \in H$, then $h^{-1} \in H$.

Condition ii) says H is "closed under the operation",

iii) says H is "closed under inverses.

$H \leq G$

$\boxed{\text{We write } H \leq G}$

Examples 1) Let $G = (\mathbb{Z}, +, 0)$. Let H be the set of even numbers.

$H = \{2n \mid n \in \mathbb{Z}\}$.

x is even if $\exists k \in \mathbb{Z}$ s.t. $x = 2k$

Then since 0 is even, $0 \in H$.

the sum of two evens is even so H is closed under $+$.

if h is even, then so is $-h$.

2) Let $G = (\mathbb{Q}^*, \cdot, 1)$ and let $H = \{2^k : k \in \mathbb{Z}\}$.

$1 = 2^0 \in H$ so the identity is in H.

Let $x, y \in H$. Then $x = 2^k$ and $y = 2^j$ for some $k, j \in \mathbb{Z}$.

ii) $xy = 2^k \cdot 2^j = 2^{k+j}$ + $k+j \in \mathbb{Z}$ so $xy \in H$

iii) $(2^k)^{-1} = 2^{-k}$ so $x^{-1} \in H$. So $H \leq \mathbb{Q}^*$.

Example Let $G = (G, *, e)$ be a group.

There are always "2" subgroups called the trivial subgroups.

The set $H = \{e\}$ is a subgroup.

i) $e \in H$ ✓, ii) $\forall x, y \in H$, $x = y = e$ so $xy = e \cdot e = e \in H$.

iii) $\forall x \in H$, $x = e$ & $x^{-1} = e^{-1} = e \in H$.

so $\{e\} \leq G$.

Clearly, $G \leq G$.

~~Def: when the only subgroups of G are the trivial ones~~

Next topic

This takes place in $\mathbb{Z}$. Let $n > 1$.

Set $n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$. non-trivial subgp

then $n\mathbb{Z} \leq \mathbb{Z}$

Pf: i) $0 = 0 \cdot n \in n\mathbb{Z}$

ii) let $x, y \in n\mathbb{Z}$ so $x = nk$, $y = nj$ some $k, j \in \mathbb{Z}$.

then $x + y = nk + nj = n(k+j) \in n\mathbb{Z}$

iii) $-x = -nk = n(-k) \in n\mathbb{Z}$.

We define relation on $\mathbb{Z}$ as follows

$a \sim b$ iff $a - b \in n\mathbb{Z}$.

Def 12 A relation on a set A is a non-empty subset $R \subseteq A \times A$.

$(a, b) \in R$ we say a is R-related to b.

- refl.
- symm.
- trans.

- anti-symm.
- irreflexive

An equivalence relation is refl., symm., transitive.

(4)

Define an equiv. relation on $\mathbb{Z}$. $\boxed{\text{First, fix } n>1}$

$(a,b)\in R$ iff . . .

$x \in n\mathbb{Z}$

this means

$\exists k \in \mathbb{Z}$ s.t.

$x = nk$

$$R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid$$

$a \sim b$ iff $a-b \in n\mathbb{Z}$

iff $\exists k \in \mathbb{Z}$ s.t. $a-b = nk$.

Thm $\sim$ is an equiv. relation

pf. worksheet

$[a] = [c]$ $\quad \exists k \in$ $\quad a-c = nk$

$[b] = [d]$ $\quad \exists j$ $\quad b-d = nj$

$(\mathbb{Z}/n\mathbb{Z}, \oplus, [0])$

is $(a+b) \sim (c+d)$

$ab - cd = n$ ____

$ab - cb + bc - cd$

5

Ex. $(GL_2(\mathbb{R}), \cdot, I_2)$ "General linear group"

The matrix $A \in M_2(\mathbb{R})$ belongs to $GL_2(\mathbb{R})$ iff $\exists B \in M_2(\mathbb{R})$ s.t.

$$AB = I_2 = BA.$$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Fact $A \in GL_2(\mathbb{R})$ iff $\det(A) \neq 0$.

(Think about proof).

Recall $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.

$\det(AB) = \det(A) \cdot \det(B)$ (can you prove it.)

$$SL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid \det(A) = 1\}.$$

$$SL_2(\mathbb{R}) \leq GL_2(\mathbb{R}).$$

Show it is proper.

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \setminus SL_2(\mathbb{R})$$

Cyclic Groups

n is fixed

MAS 4301 – Modular Arithmetic

We are defining an infinite number of eq rel. one for each $n>1$

Let $n \in \mathbb{N}$ and $n > 1$. Recall that

$$n\mathbb{Z} = \{x \in \mathbb{Z} : \exists k \in \mathbb{Z}, x = nk\}.$$

We showed that $n\mathbb{Z} \leq \mathbb{Z}$.

So what does it mean in other words for an integer to belong to $n\mathbb{Z}$?

Recall that a relation on $\mathbb{Z}$ is a subset of $\mathbb{Z} \times \mathbb{Z}$. Here we define the relation R as those

$a \sim b$ $$R = \{(a, b) \in \mathbb{Z}^2 : a - b \in n\mathbb{Z}\}.$$

We can write $a \sim b$ to mean that $(a, b) \in R$. We also say that a **is congruent to** b **modulo** n when this happens.

We show that R is an equivalence relation, that is, it is *reflexive, symmetric, and transitive.*

Reflexive Is $a \sim a$?

This is asking whether $a - a \in n\mathbb{Z}$. Find a $k \in \mathbb{Z}$ such that $a - a = kn$.

$$k = \underline{\quad 0 \quad}. \qquad 0 \in \mathbb{Z}.$$

Symmetric If $a \sim b$, then $b \sim a$.

So we assume that $a \sim b$. By definition, this means $\forall$ / $\exists$ $\underline{K} \in \mathbb{Z}$ such that $\underline{\ a-b\ } = nk$. Next, find a $j \in \mathbb{Z}$ such that $b - a = nj$.

$b-a = -(a-b)$ $\quad n(\quad)$ $\quad j = -K \in \mathbb{Z}.$
$= -(nK) = n(-K)$

Transitive If $a \sim b$ and $b \sim c$, then $a \sim c$.

We suppose that $a \sim b$ and $b \sim c$. This means that there exist $j, k \in Z$ such that $a - b = \underline{\ nj\ }$ and $\underline{\ b-c\ } = nk$. Next, add $(a - b)$ and $(b - c)$ together in two ways. The first way is the easy way and results in $(a - b) + (b - c) = \underline{\ a-c\ }$. Add them together a second way by substituting in what they equal and then factor out n. Write this out.

$a-c = (a-b)+(b-c) = nj+nK = n(j+K) \qquad j+K \in \mathbb{Z}$

We have thus shown that $\sim$ is an equivalence relation. For an $a \in \mathbb{Z}$, we let $[a] = \{b \in \mathbb{Z} : a \sim b\}$ and call this the **congruence class modulo** n **containing** a. The set of all equivalence classes modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$.

Let $i, j \in \mathbb{N}$ satisfy $0 \leq i < j < n$. Can it be the case that $j \sim i$?

$0 < j - i = nk$ $\quad \frac{j-i}{n} = k$ $\quad$ distinct.
$< n$

It follows that

$$[0], [1], \ldots [n-2], [n-1]$$

are distinct equivalence classes modulo n.

Next, let $a \in Z$. The Division Algorithm states that we can divide a by n and get a remainder that is between 0 and $n-1$. In particular, there are unique $q, r \in Z$ such that

$$a = nq + r$$

and $0 \leq r < n$. Subtract r from both sides to get

$$a - r = nq. \quad \in n\mathbb{Z}. \quad \text{so } a \sim r$$

Do you see then $a \sim r$?

Thus,

$$[0] \cup [1] \cup \ldots \cup [n-1] = \underline{\hspace{2cm}}.$$

You should be able to conclude that $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ and so

$$|\mathbb{Z}/n\mathbb{Z}| = \underline{\quad n \quad}$$

$\mathbb{Z}/n\mathbb{Z}$ the set of eq. classes mod n.

We define an addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ by

$$[a] \oplus [b] = [a+b]$$

and

$$[a] \otimes [b] = [ab]$$

$x \in \mathbb{Z}/n\mathbb{Z}$

$x = [r]$ some $0 \leq r < n$

The goal is always to take an equivalence class $[a]$ and find $0 \leq r < n$ such that $[a] = [r]$. (Divide a by n and let r be the remainder.)

Example 0.1. Let $n = 7$. What is $[6] \otimes [5]$? Multiply $6 \cdot 5$ and then divide by 7 to be left with a

remainder of __________. So $[6] \otimes [5] =$ __________

$n = 7$

$[137] \oplus [56] = [193]$
$= [4]$

$137 + 56 = 193$

$7 \overline{)193}$ $= 27$, 14, 53, 49

$[4] \oplus [0] = [4]$

$137 = 7 \cdot 19 + 4$

$n = 7$

$x = [137]$
$= [4]$

$7 \overline{)137}$ $= 19$, 7, 67, 63, 4