4800-4

Abelian Groups

An abelian gp. A is a set with a single operation:

$$+ : A \times A \longrightarrow A$$

s.t.

(1) $a+b=b+a$ (commutative)

$a+(b+c)=(a+b)+c$ (associative)

(2) there is an additive identity $A \ni 0$ s.t. $0+a=a$.

(3) Every element $a \in A$ has an additive inverse $-a$.

$$(- : A \longrightarrow A)$$

<u>Rmks</u>: Check that 0 is unique:

$$0' = 0 + 0' = 0$$

Check that $-a$ is unique

$$(-a)' = (-a + a) + (-a)' = -a + (a + a') = -a.$$

A morphism of abelian grp.

is a <u>linear</u> function?

$$\| \; f: A \longrightarrow B \; \|$$

is <u>linear</u> <u>if</u>: ← <u>distinct</u> ~~grps~~.

- $f(0_A) = 0_B$
- $f(a_1 + a_2) = f(a_1) + f(a_2)$
- $\underline{f(-a) = -f(a)}$

$$f(-a) + f(a) = f(-a+a) = f(0) = 0$$

To be a <u>category</u>, <u>need</u>:

1_A is a <u>morphism</u> ✓

If $f : A \to B$ and

$g : B \to C$ are linear maps,

then

$g \circ f : A \to C$ is <u>linear</u>.

$g \circ f(0_A) = g(0_B) = 0_C$ ✓

✓

$g \circ f(a_1 + a_2) = g(f(a_1) + f(a_2)) = g(f(a_1)) + g(f(a_2))$.

Examples:

$$(\mathbb{Z}, +, 0)$$

A "operation" "identity element"

$$(\mathbb{Q}, +, 0)$$

$$(\mathbb{R}, +, 0)$$

$$(\mathbb{Z}/n\mathbb{Z}, +, 0) \quad n > 0$$

integers mod n

$(\mathbb{N}, +, 0)$ not (no add inv)

$$(\mathbb{Q}^*, \cdot, 1)$$

$$\parallel$$

$$(\mathbb{Q} - \{0\}) \quad \text{(Commutative)}$$

$$(\mathbb{R}^*, \cdot, 1)$$

<u>Linear ~~o~~ function</u> :

$$\underline{e^x} : (\mathbb{R}, +, 0) \to (\mathbb{R}^*, \cdot, 1)$$

is <u>injective</u>.

$$e^0 = 1 \checkmark$$

$$e^{x+y} = e^x \cdot e^y \checkmark$$

$e^x : (\mathbb{R}, +, 0) \to (\mathbb{R}^+, \cdot, 1)$

$\mathbb{R}^-$ $\mathbb{R}^+$

is a bijection. Its inverse is $\log$. $\log(ab) = \log(a) + \log(b)$

Prop: If $f : A \to B$ is linear and a bijection, then $f^{-1} : B \to A$ is also linear!

Pf. To show $f^{-1}(b_1+b_2) = f^{-1}(b_1)+f^{-1}(b_2)$,

apply f to both sides.

$$f\left(f^{-1}(b_1+b_2)\right) = f\left(f^{-1}(b_1) + f^{-1}(b_2)\right)$$

$$\parallel$$

$$b_1+b_2$$

$$= ff^{-1}(b_1) + ff^{-1}(b_2)$$

$$= b_1+b_2 \quad \checkmark$$

$\square$

Fun fact about

$$\hom(A, B) = \{f : A \to B\}$$

is also an abelian gp.

$$(f_1 + f_2)(a) = f_1(a) + f_2(a)$$

$$z(a) = 0 \quad \forall a$$

is the zero.

additive inverse of f: $\quad (-f)(a) = -(f(a))$

Products:

$$A \times B = \left\{ (a,b) \,\middle|\, \begin{matrix} a \in A \\ b \in B \end{matrix} \right\}$$

$$(a,b) + (a',b') = (a+a', b+b')$$

$$(0,0)$$

$$-(a,b) = (-a,-b).$$

$$\begin{tikzcd} & A \times B \arrow[dl, "p"'] \arrow[dr, "q"] & \\ A & & B \end{tikzcd}$$

$$\begin{tikzcd} & A \times B & \\ A \arrow[ur, "i"] & & B \arrow[ul, "j"'] \end{tikzcd}$$

$$\left\| \begin{array}{l} i(a) = (a, 0) \\ j(b) = (0, b) \end{array} \right\|$$

$$\underline{A \times B}$$

Ask about symmetries of an abelian gp.

Q: What are the symmetries of $(\mathbb{Z}, +, 0)$?

$1_{\mathbb{Z}}$ identity

$\sigma : \mathbb{Z} \to \mathbb{Z}$

$\sigma(a) = -a$

$\sigma^2 = 1$

Note: $\sigma(a) = a+1$ is not lin.

$\sigma(a+b) = \sigma(a) + \sigma(b)$!

Q: What are the symmetries of $\mathbb{Z} \times \mathbb{Z}$?

$$\sigma : \mathbb{Z}^2 \to \mathbb{Z}^2$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$$= \underline{x \begin{bmatrix} a \\ c \end{bmatrix}} + \underline{y \begin{bmatrix} b \\ d \end{bmatrix}}$$

$$f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$

2x2 matrices of integers

$$\sigma : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$ || 2x2 matrices w/ det. ± 1

$$GL(2, \mathbb{Z})$$

coefficients

invertible 2×2 matrices

Not commutative:

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

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

$$(\mathbb{Z}, +, 0) \subseteq GL(2, \mathbb{Z})$$

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

$$SL(2, \mathbb{Z}) \subseteq GL(2, \mathbb{Z})$$

$\det = 1$

<u>Def</u>: Given an abelian gp. A, then a <u>subgp</u> of A is a <u>subset</u>

$$B \subseteq A$$ that:

- contains 0
- closed under $+$
- closed under inverses

Examples:

$$n\mathbb{Z} \subseteq \mathbb{Z}$$

$$= \{\ldots, -n, 0, n, 2n, \ldots\}$$

is a subgroup.

These are the only subgps. of $\mathbb{Z}$!

Pf: Suppose: $B \subseteq \mathbb{Z}$ is a subsp. and $m, n \in B$.

Then apply **Euclid's alg.**

$\to$ $d = am + bn$ for $a \in \mathbb{Z}$, $b \in \mathbb{Z}$

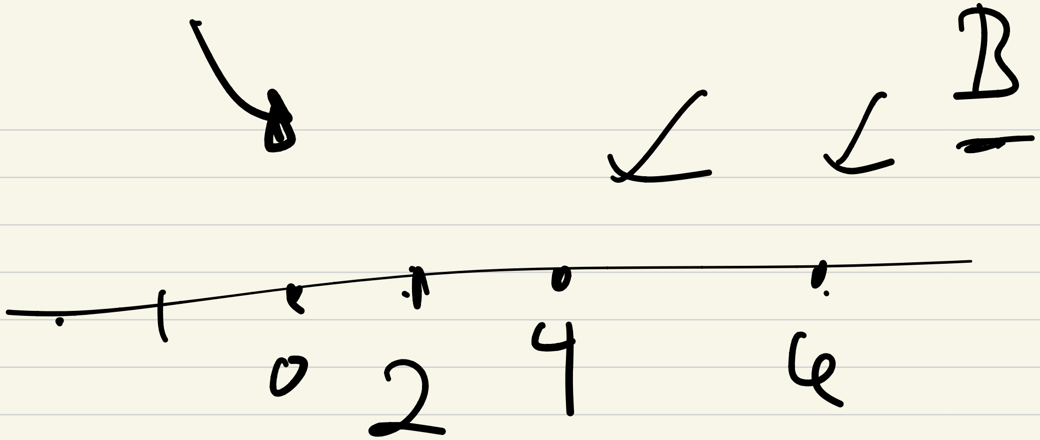
$\gcd(m,n)$

$m \in B \Rightarrow a \cdot m \in B$

$n \in B \Rightarrow b \cdot n \in B$

$\Rightarrow d \in B$

//



So $d\mathbb{Z} \subseteq B$

contains both m, n.

Either $d\mathbb{Z} = B$ or

$e \in B$. —

$\gcd(d,e)$, continue.

Key feature of abelian gps.

If $B \subseteq A$ is a subgp, then there is an abelian gp. A/B of cosets of B in A.

The coset containing $a \in A$ is:

$$a+B = \{a+b \mid b \in B\}.$$

Example:

$(0 \leq r < n)$

$$\mathbb{Z}/n\mathbb{Z} \ni r + n\mathbb{Z}$$

$$= \{\ldots, r-n, r, r+n, r+2n\}$$

$$A/B = \{\underline{a+B}\}$$

Q: When is $a+B = a'+B$?

A: It happens when

$\underline{a' = a+b}$ for some b

$$1+2\mathbb{Z} = 3+2\mathbb{Z} = -1+2\mathbb{Z} = \cdots$$

A/B is an abelian gp.

(the <u>quotient</u> of A by B).

$$(a+B)+(a'+B)=(a+a')+B$$

<u>Zero</u>: $0+B = B$

is the <u>zero</u> <u>coset</u>.

$$-(a+B)=(-a)+B$$

$\mathbb{Z}/3\mathbb{Z}$:

Elements:

$$0+3\mathbb{Z}$$
$$1+3\mathbb{Z}$$
$$2+3\mathbb{Z}$$

$$(2+3\mathbb{Z})+(2+3\mathbb{Z})$$
$$= 4+3\mathbb{Z} = 1+3\mathbb{Z}$$

$$2+2 \equiv 1 \pmod 3$$

The quotient gp. comes with a surjective linear map:

$$f : A \longrightarrow A/B$$

$$f(a) = a + B$$

$$f(a_1 + a_2) = (a_1 + B) + (a_2 + B)$$

$$= (a_1 + a_2) + B.$$

The <u>kernel</u> of a

linear map:

$$f: A \to C$$

is $B = \{a \mid f(a) = 0\}$

$\subset$

this is a <u>subspace</u>

<u>$B \subset A$:</u> $\qquad A \xrightarrow{g} A/B$

$(\ker(g) = B)$

$W \subset V$ subspace

$V \to V/W$ quotient

$$\dim W + \dim V/W = \dim V$$

$$3\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$$

$$\begin{array}{ccc} \shortparallel & & \shortparallel \\ B & A & A/B \end{array}$$

$$0+3\mathbb{Z} \quad 1+3\mathbb{Z} \quad 2+3\mathbb{Z} = \mathbb{Z}$$

Next time:

Q: What are the symmetries of $\mathbb{Z}/n\mathbb{Z}$?

The symmetries of $\mathbb{Z}/p\mathbb{Z}$ are iso. to $\mathbb{Z}/(p-1)\mathbb{Z}$