MATH 427

8/31/2022
We

Last time: - Defined rings 5.1
- Defined $\mathbb{Z}_n$ as the set of equivalence classes of a relation $\sim_n$
where $a \sim_n b \Leftrightarrow n \mid a-b$
Proved that there are well-defined binary operations $+, \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$.
They make $\mathbb{Z}_n$ into a ring: $0_{\mathbb{Z}_n} = [0]$, $1_{\mathbb{Z}_n} = [1]$ etc.

Today: We start groups.

Definition A group is a set G together with a map
$\ast : G \times G \to G$, $(a,b) \mapsto a \ast b$ (a binary operation)
and a distinguished element $e = e_G \in G$ so that
1) $\ast$ is associative: $(a \ast b) \ast c = a \ast (b \ast c)$ $\forall a,b,c \in G$
2) $a \ast e = a = e \ast a$ $\forall a \in G$
3) $\forall a \in G$ $\exists b \in G$ so that $a \ast b = e = b \ast a$
(b is an inverse of a)

Ex $(\mathbb{Z}, +, 0)$ is a group
$(\mathbb{N}, +, 0)$ is not a group: 1 has no inverse
$(\mathbb{Z}, \cdot, 1)$ is not a group for many reasons:
e.g. 2 has no inverse: $\nexists b \in \mathbb{Z}$ s.t. $2 \cdot b = 1$
In fact $-1, +1$ are the only elements with inverses.
$(\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}, \cdot, 1)$ is a group
$(\mathbb{Z}_n, +, 0)$ is a group.
In fact, if $(R, +, \cdot, 0, 1)$ is any ring, $(R, +, 0)$ is a group.

Ex $GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$ is a group:
the binary operation is matrix multiplication and
$e_{GL(n,\mathbb{R})} = I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, the identity matrix.
Recall: $\det(A) \neq 0 \Rightarrow A$ is invertible!

Ex $U(1) = \{ z \in \mathbb{C} \mid |z| = 1 \}$ is a group

group operation = multiplication of complex numbers

$\mathbb{1} = 1 \in \mathbb{C}$.

Note: $\forall z \in U(1)$ $z\bar{z} = |z|^2 = 1$. $\Rightarrow$ $\forall z \in U(1)$

$\bar{z}$ is the inverse.

Proposition 5.1 Let $(G, \cdot, e)$ be a group.

1) The identity e is unique: if $e' \cdot a = a = e' \cdot a$ then $e = e'$

2) inverses are unique: $\forall a \in G$ if $a \cdot b = e = b \cdot a$ and if $a \cdot b' = e = b' \cdot a$ then $b = b'$.

We write a^{-1} for the unique element s.t. $aa^{-1} = e = a^{-1}a$.

3) $(a^{-1})^{-1} = a$.

Proof 1) $e' \overset{e \text{ is an identity}}{=} e' \cdot e \underset{e' \text{ is an identity}}{=} e$

[I will now drop $\cdot$ and write cd for $c \cdot d$].

2) $b = be = b(ab') = (ba)b' = eb' = b'$

3) $(a^{-1})^{-1}$ and a are both inverses of a^{-1}. Hence by (2), $(a^{-1})^{-1} = a$. ▷

Since multiplication in a group G is associative, $\forall n \geq 1$ $\forall a_1, \dots, a_n \in G$

$$a_1(a_2(\dots(a_{n-1}a_n)\dots))$$
$$= (a_1a_2)(a_3 \dots (a_{n-1}a_n)) = \dots$$

That is, the placement of parentheses doesn't matter.

We'll write

$a_1 \dots a_n$ for $a_1(a_2 \dots (a_{n-1}a_n))\dots)$.

Example of a group Let X be a set. Consider the set

$$\mathrm{Sym}(X) := \{ f : X \to X \mid f \text{ is a bijection} \}$$

We then have a binary operation, the composition:

$$\circ : \mathrm{Sym}(X) \times \mathrm{Sym}(X) \to \mathrm{Sym}(X), \quad (f, g) \mapsto f \circ g.$$

Where $(f \circ g)(x) = f(g(x)) \quad \forall\, x \in X$

Note: (i) the composition of two bijections is a bijection

(ii) composition is associative

(iii) for any bijection $f : X \to X$, $\quad id_X \circ f = f = f \circ id_X$

where $id_X : X \to X$ is the identity map; $\quad id_X(x) = x \quad \forall\, x \in X$

$(\mathrm{Sym}(X), \circ, id_X)$ is a group.

If $X = \{1, \dots, n\}$, $\quad \mathrm{Sym}(X) =: S_n$ the symmetric group on n letters, the group of permutations.

Groups, like rings, come in two flavors: commutative and non-commutative.

Def A group $(G, \bullet, e)$ is abelian (commutative) if $\forall\, a, b \in G \quad a \bullet b = b \bullet a$.

Ex $(\mathbb{Z}, +, 0)$ is abelian, $\quad GL(n, \mathbb{R})$ is not (if $n > 1$)
[$GL(1, \mathbb{R}) = \mathbb{R}^\times$, the group of nonzero real numbers under multiplication]

Definition (Homomorphism) A homomorphism from a group $(G, *, e_G)$ to a group $(H, \bullet, e_H)$ is a function $f : G \to H$ which preserves "multiplication":

$$f(a * b) = f(a) \bullet f(b) \qquad \forall\, a, b \in G$$

Ex $\exp : \mathbb{R} \to (0, \infty)$, $\exp(x) = e^x$ satisfies

$$e^{x+y} = e^x \cdot e^y, \quad \text{so } \exp : (\mathbb{R}, +, 0) \to ((0, \infty), \cdot, 1)$$

is a homomorphism. ($\ln : (0,\infty) \to \mathbb{R}$ is also a homomorphism $\ln(ab) = \ln(a) + \ln(b)$)

<u>Ex</u> $\det : GL(n,\mathbb{R}) \to \mathbb{R}^\times$, $A \mapsto \det A$ is a homomorphism

$\det(AB) = \det A \cdot \det B \quad \forall A, B \in GL(n,\mathbb{R})$.

<u>Ex</u> trace $tr : M_n(\mathbb{R}) \to \mathbb{R}$ preserves addition:

$tr(A+B) = tr\, A + tr\, B$

So $tr : (M_n(\mathbb{R}), +, 0) \to (\mathbb{R}, +, 0)$ is a homomorphism

<u>Ex</u> $\pi : \mathbb{Z} \to \mathbb{Z}_n$ $\quad \pi(k) = [k]$ is a homomorphism since

$\pi(a+b) = [a+b] = [a] + [b]$.

In fact we <u>defined</u> $+$ on $\mathbb{Z}_n$ to make π a homomorphism.

<u>Ex</u> $f : \mathbb{Z} \to \{\pm 1\}$, $f(n) = (-1)^n$ is a homomorphism since

$(-1)^{n+k} = (-1)^n \cdot (-1)^k \quad \forall n, k \in \mathbb{Z}$.

<u>Lemma 5.2</u> Let $f : G \to H$ be a homomorphism. Then

(1) $f(e_G) = e_H$ and (2) $f(a^{-1}) = (f(a))^{-1} \quad \forall a \in G$.

<u>Proof</u> (1) $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$. $\Rightarrow$

$e_H = (f(e_G))^{-1} \cdot f(e_G) = (f(e_G))^{-1}(f(e_G) f(e_G)) = f(e_G)$

(2)

$e_H = f(e_G) = f(aa^{-1}) = f(a) f(a^{-1})$.

$\Rightarrow (f(a))^{-1} \cdot e_H = (f(a))^{-1} f(a) f(a^{-1}) = e_H f(a^{-1}) = f(a^{-1})$.

$\square$