Groups

FROM LAST TIME

A group is a collection of elements with one invertible operation.

Def: A group $(A,+)$ is a set with an associative binary operation

$+ : A \times A \to A$, such that: $\qquad (a+b)+c = a+(b+c)$

a) $\exists\, 0 \in A : \; 0+a = a+0 = a, \; \forall a \in A$

b) $\forall a \in A \; \exists\, -a \in A : \; \underbrace{a+(-a)}_{a-a} = 0.$

A group is **Abelian** (commutative) if: $\forall a,b \in A: \; a+b = b+a.$

! All our groups will be abelian.

Example:
- $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}\setminus\{0\}, \cdot)$, ...
- $(\mathbb{R}^n, +)$
- (rotations of S^1, composition)
- (functions: $D \to \mathbb{R}$, pointwise $+$)
- $q \in \mathbb{N}$

  $\mathbb{Z}_q = \{0, 1, \dots, q-1\}$ remainders after division by q.

  operation: $\quad a+b \pmod q \quad$ addition mod q.

  Example:
  - in $\mathbb{Z}_5$: $\quad 1+1=2 \qquad 3+4=2$

    $2+3=0 \rightsquigarrow -3=2$
  - in $\mathbb{Z}_2$: $\quad 0+0=0 \qquad 1+1=0 \qquad a+b = a \text{ XOR } b$

    $0+1=1 \qquad 1+0=1$

    exclusive or

We can also multiply in $\mathbb{Z}_q$: $\pmod q$

Example:
- In $\mathbb{Z}_5$: $\quad 2\cdot 3=1 \qquad 2\cdot 4=3 \qquad 4\cdot 4=1$

  $3\cdot 3=4 \qquad 0\cdot 3=0$

• In $\mathbb{Z}_2$: $0\cdot 0 = 0$ $\quad a\cdot b = a \wedge b$

$0 \cdot 1 = 0$

$1 \cdot 1 = 1$

Can we also divide (except by 0):

$$\frac{a}{b} = a \cdot b^{-1}$$

b^{-1}: $b \cdot b^{-1} = 1$

Example: $\mathbb{Z}_5$ $\quad 2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$, $1^{-1} = 1$

If all nonzero elements in $\mathbb{Z}_q$ have an inverse, $\mathbb{Z}_q$ is a field.

Example: $\mathbb{Z}_5$ is a field

$\mathbb{Z}_4$ is not a field: $2\cdot 2 = 0$, $2 \cdot 3 = 2$, $3 \cdot 3 = 1$ $\quad$ 2 does not have an inverse.

|| $\mathbb{Z}_q$ is a field iff q is a prime.

TODAY'S MATERIAL

Def: A homomorphism of groups A & B is a map $\varphi: A \to B$:

$$\forall a,b \in A: \quad \varphi(a+b) = \varphi(a) + \varphi(b)$$

Isomorphism $[\cong]$ is a bijective homomorphism.

$B' < A$ is a subgroup $[B' \leq A]$ if B' is itself a group. $\quad$ Ex: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$

Kernel of φ: $\operatorname{Ker} \varphi = \{a \in A;\ \varphi(a) = 0\}$

Image of φ: $\operatorname{Im} \varphi = \{\varphi(a);\ a \in A\}$

Proposition: Suppose $\varphi: A \to B$ is a homomorphism of groups. Then:

1. $\varphi(-a) = -\varphi(a)$ $\quad \forall a \in A$
2. $\varphi(k \cdot a) = k \cdot \varphi(a)$ $\quad \forall k \in \mathbb{Z},\ a \in A$
3. $\operatorname{Ker} f \leq A$, $\operatorname{Im} f \leq B$
4. φ injective $\Leftrightarrow$ $\operatorname{Ker} \varphi = 0$
5. φ is $\cong$ $\Leftrightarrow$ $\operatorname{ker} \varphi = 0$ & $\operatorname{Im} \varphi = B$.

Proof: ① $\underbrace{\varphi(a)}^{-\varphi(-a)} + \underbrace{\varphi(-a)}_{-\varphi(a)} = \varphi(a-a) = \underline{\varphi(0) = 0} \quad \Rightarrow -\varphi(a) = \varphi(-a)$

$$\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0) \Rightarrow \varphi(0) = 0 \quad \square$$

④ $\Rightarrow$ ✓ :)

$\Leftarrow$ Assume $\operatorname{Ker} \varphi = 0$

$$\varphi(a) = \varphi(b) \rightsquigarrow \varphi(a) - \varphi(b) = 0 \overset{\varphi \text{ homom.}}{\rightsquigarrow} \varphi(a-b) = 0 \overset{\operatorname{Ker}\varphi = 0}{\rightsquigarrow} a-b=0 \rightsquigarrow a = b \quad \square$$

$\blacksquare$

Def: Suppose A and B are groups. The **direct sum** $A \oplus B$ is a group:

$\to$ elements: $(a, b) \quad a \in A,\ b \in B$

$\to$ operation: $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2,\ b_1 + b_2)$.

Example: $\mathbb{Z} \oplus \mathbb{Z}_2, \dots$

Def: A group A is **finitely generated** if $\exists\ \overbrace{a_1, a_2, \dots, a_k}^{\text{generating set}} \in A$, such that each element of A can be expressed as $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_k a_k, \quad \alpha_i \in \mathbb{Z}$.

Examples: $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z},\ \mathbb{Z}_q,\quad \mathbb{Z} \oplus \mathbb{Z}_q^2 \oplus \mathbb{Z}_{2q},$ Non-examples: $\mathbb{Q}, \mathbb{R}$

Theorem: [Structure theorem for f.g. Abelian groups] Let A be a fin. gen. Abelian group. Then $\exists\ r \in \{0, 1, 2, \dots\}$ and $q_i = (p_i)^{k_i}$ powers of primes (9 ✓, 12 ✗) such that

$$A \cong \underbrace{\mathbb{Z}^r}_{\text{free part}} \oplus \underbrace{\mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \dots \oplus \mathbb{Z}_{q_m}}_{\text{torsion}}.$$

$r = \operatorname{rank}(A)$

Def: Let A be a group, $B \le A \rightsquigarrow$ equivalence relation on A:

$$a_1 \sim a_2 \Leftrightarrow a_1 - a_2 \in B \quad (\text{eq. } a_2 - a_1 \in B)$$

The set of equiv. classes $\{[a];\ a \in A\}$ forms a **quotient group** A/B.

operation: $[a_1] + [a_2] = [a_1 + a_2]$

Example: $\mathbb{Z}$, $q \cdot \mathbb{Z} = \{q \cdot k \,;\, k \in \mathbb{Z}\} = \{\dots, -2q, -q, 0, q, 2q, \dots\}$ $\quad q \in \mathbb{N}$.

$q \cdot \mathbb{Z} \leq \mathbb{Z}$, $\quad \mathbb{Z}/_{q\mathbb{Z}} = \mathbb{Z}_q$

Proposition: Let A be a fin.gen. Abelian group, $B \leq A$. Then:

ⓐ A/B is fin. generated

ⓑ $\operatorname{rank} A/B = \operatorname{rank} A - \operatorname{rank} B$.

Vector spaces

Fix $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p\}$ $\quad p$ prime

Def: V is a vector space over $\mathbb{F}$ if there exist two operations:

① $(V, +)$ is an Abelian group

② $\_\cdot\_ : \mathbb{F} \times V \longrightarrow V$ scalar multiplication:

$(a \cdot b) \cdot v = a \cdot (b \cdot v)$ $\quad \forall a, b \in \mathbb{F}$
$(a+b) \cdot v = av + bv$
$a(v+w) = av + aw$ $\quad \forall v, w \in V$
$1 \cdot v = v$

Our vector spaces will look like: $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{Z}_p^n$. $\quad$ Non-example: $\mathbb{Z}_3 \oplus \mathbb{Z}_4$

! concepts of a linear map, Ker, Im, isomorphism, linear independence, basis, dimension, matrix representation, rank, Gaussian ellimination as in typical lin. algebra!

Example: Let v_1, v_2, v_3 be a basis of V over $\mathbb{F}$.

$V = \{\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 \,;\, \alpha_i \in \mathbb{F}\}$ $\quad \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix}$

$\rightarrow$ for which prime p are $(1,3)$ & $(2,1)$ lin. dependent in $\mathbb{Z}_p^2$?

$2 \cdot (1,3) = (2,1)$
$(2,6) = (2,1) \rightsquigarrow [6] = [1] \Rightarrow p = 5$

$\longrightarrow$ if $\mathbb{F} = \mathbb{Z}_2$ our space 8 elements

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

$\longrightarrow$ if $\mathbb{F} = \mathbb{Z}_5$ our space has 125 elements.

A plane: $2 \cdot x + 3 \cdot y + z = 3$

$\downarrow$ express z

$z = 3 - 2x - 3y = 3 + 3x + 2y$

$\frac{[-1]}{3} = \frac{[4]}{3} = \frac{[9]}{3} = [3]$

$\frac{[-2]}{3} = \frac{[3]}{3} = [1]$

express $y \longrightarrow 3y = 3 - z - 2x \quad /:3$ in $\mathbb{Z}_5$

$y = 1 + 3z + x$

system of equations:

$$\left.\begin{array}{l} 2x + y = 0 \\ 2x - y = 3 \end{array}\right\} - \quad \rightsquigarrow \quad 2y = 3 \Rightarrow \boxed{\begin{array}{l} y = 1 \\ x = 2 \end{array}}$$

The definition of a quotient of vector spaces is the same as for groups.

Proposition: $W \leq V$ vector spaces. Then $\dim V/_W = \dim V - \dim W$.

$w_1, w_2, \dots, w_k$ a basis for W

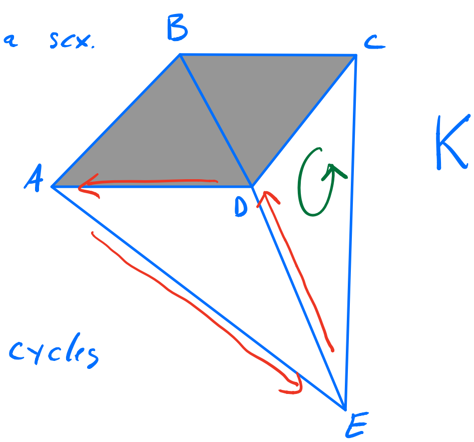
$w_1, w_2, \dots, w_k, v_1, v_2, \dots, v_n$ a basis for V.

$[v_1], [v_2], \dots, [v_n]$ a basis for V/W.

Idea of homology

We want to measure the number of holes in a scx.

A hole can be represented by



holes

$\alpha = \langle A, E\rangle + \langle E, D\rangle + \langle D, A\rangle$

$\beta = \langle E, C\rangle + \langle C, D\rangle + \langle D, E\rangle$

$\gamma = \langle E, C\rangle + \langle C, D\rangle + \langle D, A\rangle + \langle A, E\rangle$

$\gamma = \alpha + \beta$

not holes (boundaries)

$\delta = \langle D, B\rangle + \langle B, A\rangle + \langle A, D\rangle$

$\varepsilon = \langle D, C\rangle + \langle C, B\rangle + \langle B, D\rangle$

cycles

Idea for cycles: define $C_1(K) = \left\{ \sum_{\sigma_i \in K^{(1)} \text{ oriented edge}} \sigma_i \right\}$ chains

cycles: chains whose boundary is 0.

$$\partial\alpha = \partial\big(\langle A, E\rangle + \langle E, D\rangle + \langle D, A\rangle\big) =$$

$$= \langle E\rangle - \langle A\rangle + \langle D\rangle - \langle E\rangle + \langle A\rangle - \langle D\rangle = 0$$