last time **Def^n** group set G with operation $G \times G \to G$
$(a,b) \mapsto ab$

s.t.: identity $\exists\, e \in G$ s.t. $eg = ge = g$
inverses $\forall g \in G\ \exists g^{-1}$ s.t. $gg^{-1} = g^{-1}g = e$
associativity $\forall g_1 g_2 g_3$ $(g_1 g_2) g_3 = g_1 (g_2 g_3)$.

Def^n G is abelian if $\forall\, g, h \in G$ $gh = hg$, in this case usually write operation as $+$
$g+h = h+g$.

Def^n $\alpha : G \to H$ is a homomorphism if $\forall g,h$ $\alpha(gh) = \alpha(g)\alpha(h)$

Def^n $H \leq G$ is a subgp if $\cdot\ e_G \in H$, $\cdot\ \forall h \in H$, $h^{-1} \in H$ $\cdot\ \forall h_1, h_2 \in H$
$h_1 h_2 \in H$

Prop^n $\alpha(G) \subset H$ subgp of H $\ker(\alpha) \subset G$ subgp of G.

New groups from old $\cdot\ G \oplus H = G \times H$ with operation $(a,b) + (c,d)$
$= (a+c, b+d)$

$\cdot$ quotients: let $H \leq G$, define the cosets of H to be
the sets $gH = \{gh \mid h \in H\}$

Example $2\mathbb{Z} \subset \mathbb{Z}$ has two cosets $\{\dots, -2, 0, 2, 4, \dots\}$. H.
$1+H$ .. $\{\dots, -1, 1, 3, 5, \dots\}$ $1+H$.

$3\mathbb{Z} \subset \mathbb{Z}$ has three cosets H, $1+H$, $2+H$.
Hi **Prop^n** the cosets give a partition of G pf equivalence relation $\square$.
Prop^n If G is abelian, then the cosets form a group with set $\{gH\}$
and group operation $aH + bH = (a+b)H$.

Proof check well defined: $(a+h_1) + (b+h_2) = a+b+\underbrace{(h_1+h_2)}_{= h_3 \in H}$.
$\cdot$ identity: H $aH + H = a + h_1 + h_2 = a + (h_1 + h_2) \in H$ so $aH + H = aH$
$\cdot$ inverse: $(aH)^{-1} = (-a)H$ check: $(a+h_1) + (-a+h_2) = \underbrace{a-a}_{0 = e_G} + \underbrace{(h_1+h_2)}_{\in H} = 0+H = H$.
$\cdot$ associativity ✓. $\square$.

$G \text{ ab} \quad H \leq G$

Defn The quotient group G/H is the group of H-cosets.

Examples · $2\mathbb{Z} < \mathbb{Z}$ gives two cosets evens H $\{\dots -2, 0, 2, \dots\}$
odds $1+H$ $\{\dots, -1, 1, 3, \dots\}$

~~cyclic~~ abelian group of order 2 $\mathbb{Z}/2\mathbb{Z} = (\{0,1\} (+, \text{mod } 2))$.

· $3\mathbb{Z} < \mathbb{Z}$ gives three cosets H, $1+H$, $2+H$.
$\mathbb{Z}/3\mathbb{Z}$ gives abelian gp of order 3.

Defn G is cyclic if G is generated by a single element, i.e.
~~for all~~ $\exists\, g \in G$ s.t. for all $h \in G$ $h = ng$ for some $n \in \mathbb{Z}$.

Propn $\mathbb{Z}/d\mathbb{Z}$ is ~~a~~ the cyclic abelian gp of order d.

Defn if G is finite the order of G, $|G| = \#$ of elements in G.
Defn order of $g \in G$ is $|\langle g \rangle|$.

Notation write $\mathbb{Z}_d$ for $\mathbb{Z}/d\mathbb{Z}$ (sometimes see $\mathbb{Z}/d$).

Classification of finitely generated abelian gps

~~Thm~~ **Defn** G is finitely generated if $\exists\, g_1, \dots, g_n$ s.t. any $g \in G$ can be written as a sum of element $a_1 g_1 + a_2 g_2 + \dots + a_n g_n$

Thm If G is finitely gen abelian gp, then $G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \dots \oplus \mathbb{Z}_{d_n}$ some numbers d_i. □

Warning not true if G not fin. gen. Examples $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$.

Key observations $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ $\quad \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

Propn $\mathbb{Z}_{p^n} \not\cong \mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}$ unless $a = n, b = 0$ or $a = 0, b = n$

Propn if a, b coprime then $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \oplus \mathbb{Z}_b$.

Example $\mathbb{Z}_{4\times3\times5}$
$\cong \mathbb{Z}_{4\times3} \oplus \mathbb{Z}_5$
$\cong \mathbb{Z}_{4\times5} \oplus \mathbb{Z}_3 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \dots$

Calculation w/ free abelian groups = linear algebra over $\mathbb{Z}$ instead of $\mathbb{R}$ ①

recall $\alpha: \mathbb{Z}^n \to \mathbb{Z}^m$ homomorphism $\Rightarrow$ α is a linear map over $\mathbb{Z}$: $\alpha(\underline{x}+\underline{y}) = \alpha(\underline{x}) + \alpha(\underline{y})$

$$\alpha(a\underline{x}) = \underbrace{\alpha(x)+\alpha(x)+\cdots\ \alpha(x)}_{a \text{ times.}} = a\alpha(x).$$

$\uparrow$ $a \in \mathbb{Z}$!

recall Choose bases $e_1, \dots, e_n$ for $\mathbb{Z}^n$, $f_1, \dots, f_m$ for $\mathbb{Z}^m$ can write α as a matrix A s.t. $\alpha(x) = Ax$ $\quad x \in \mathbb{Z}^n$ so $x = x_1e_1 + x_2e_2 + \cdots + x_ne_n$

so $\alpha(x) = \alpha(\text{——}) = \alpha(x_1e_1) + \alpha(x_2e_2) + \cdots + \alpha(x_ne_n)$

$= x_1\alpha(e_1) + x_2\alpha(e_2) + \cdots + x_n\alpha(e_n)$

so $A = \begin{bmatrix} | & | & & | \\ \alpha(e_1) & \alpha(e_2) & \dots & \alpha(e_n) \\ | & | & & | \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$. columns of A are images of basis vectors under α.

$\alpha(e_1) = a_{11}f_1 + a_{21}f_2 + \vdots + a_{m1}f_m$ $\quad \alpha(e_2) = a_{12}f_1 + a_{22}f_2 + \vdots + a_{m2}f_2$ $\quad$ so $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & & & \\ \vdots & & & \\ a_{m1} & & & a_{mn} \end{bmatrix}$

$\alpha: \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^m$

can change basis here $\quad$ can change basis here.

warning $\alpha: V \to W$ $\}$ 2 bases totally different!

$\alpha: V \to V$ only one basis!