Sections 11 & 13

Examples of groups so far: $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +_n)$, $(\mathbb{R}, +)$, S_n, A_n, D_n, ...

Can build new groups from these:

Def Let $G_1, G_2, \ldots, G_n$ be groups. The direct product of the G_i, denoted $G_1 \times \cdots \times G_n$ or $\prod_{i=1}^{n} G_i$ is

$$\prod_{i=1}^{n} G_i = \{(g_1, \ldots, g_n) \mid g_i \in G_i\},$$

with product

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Thm This makes $\prod_{i=1}^{n} G_i$ a group.

Identity element $(e_1, \ldots, e_n)$, e_i identity in G_i

Inverse of $(a_1, \ldots, a_n)$ is $(a_1^{-1}, \ldots, a_n^{-1})$.

Example $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

Consider $\langle (1,1) \rangle \leq \mathbb{Z}_2 \times \mathbb{Z}_3$.

$1(1,1) = (1,1)$,

$2(1,1) = (1,1) + (1,1) = (0,2)$

$3(1,1) = 2(1,1) + (1,1) = (1,0)$, $4(1,1) = (0,1)$, $5(1,1) = (1,2)$

$6(1,1) = (0,0)$.

$n = 6$ is the minimal $n > 0$ such that $n(1,1) = (0,0) \Rightarrow |\langle (1,1) \rangle| = 6$

$\Rightarrow \langle (1,1) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$.

"$\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic with generator $(1,1)$."

Example $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$. For any $a, b \in \mathbb{Z}_2$, $2(a,b) = (0,0)$, so we do not have $\langle (a,b) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \simeq V$, Klein 4-group.

Thm Let $m_1, \ldots, m_n \in \mathbb{Z}^+$. The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic if and only if, for each $i \neq j$, $\gcd(m_i, m_j) = 1$.

If $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic, $\prod_{i=1}^{n} \mathbb{Z}_{m_i} \simeq \mathbb{Z}_{\prod_{i=1}^{n} m_i}$.

Proof in case $n=2$: Have m_1, m_2, $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. Let $d = \gcd(m_1, m_2)$.

Let $n = \operatorname{lcm}(m_1, m_2)$ = "least common multiple of m_1 & m_2"
= smallest positive number such that m_1 & m_2 divides it.

Fact: $n = \operatorname{lcm}(m_1, m_2) = \dfrac{m_1 m_2}{\gcd(m_1, m_2)} = \dfrac{m_1 m_2}{d}$.

Case I $d = 1$. Claim $(1,1)$ is generator of $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.

If $k(1,1) = 0$, then $k1 = 0$ in $\mathbb{Z}_{m_1}$ & $k1 = 0$ in $\mathbb{Z}_{m_2}$

$\Updownarrow$

m_1 divides k & m_2 divides k.

Hence n is smallest number s.t. $n(1,1) = 0 \Rightarrow |\langle (1,1) \rangle| = n = m_1 m_2$

$\Rightarrow \langle (1,1) \rangle = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.

Case II $d > 1$. Then for any $(a,b) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, have

$$n(a,b) = \frac{m_1 m_2}{d}(a,b) = \left(\frac{m_2}{d} m_1 a, \frac{m_1}{d} m_2 b\right) = (0,0),$$

so order of (a,b) is $\leq n = \dfrac{m_1 m_2}{d} < m_1 m_2$. Hence $\langle (a,b) \rangle \neq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.

Since this holds for all $(a,b) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, the group is not cyclic.

Example If $n = p_1^{r_1} \cdots p_k^{r_k}$ is prime factorisation (p_i distinct), then

$$\mathbb{Z}_n = \prod_{i=1}^{k} \mathbb{Z}_{p_i^{r_i}}.$$

Generators of a group (Section 7)

Let G be a group, I a set, and for each $i \in I$, $a_i \in G$.
The subgroup generated by $\{a_i \mid i \in I\}$ is the smallest subgroup H of G containing each a_i.
Elements of H are all the finite products of the form

$$a_{i_1}^{n_1} a_{i_2}^{n_2} \cdots a_{i_k}^{n_k} \in G.$$

If $H = G$, say $\{a_i \mid i \in I\}$ generates G. If G is generated by $\{a_i \mid i \in I\}$ with I finite, say G is finitely generated.

Example
- $\mathbb{Z}$ is generated by $\{1\}$, (or by $\{-1\}$), $\mathbb{Z}_n$ generated by $\{1\}$.
- S_n is generated by $\{(ij) \mid 1 \le i < j \le n\}$.
- $(\mathbb{Q}, +)$ is not finitely generated.
- If G is finite, it is finitely generated by $\{g \in G\}$.
- $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is generated by

$$\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 1)\},$$ since

since every $(k_1, \ldots, k_r) = k_1(1, 0, \ldots, 0) + k_2(0, 1, 0 \ldots, 0) + \cdots + k_r(0, \ldots 0, 1)$.

Thm (Fundamental theorem of finitely generated abelian groups)
Let G be a finitely generated abelian group.
Then

$$G = \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{b},$$

for p_i primes, $r_i \in \mathbb{Z}^+$. The numbers $p_i^{r_i}$ & b are uniquely determined.

Example If $|G| = 18$ & G is fin. generated & abelian, have one of the following:

$18 = 2 \cdot 3^2 \cdot 3$ $\quad G \simeq \mathbb{Z}_2 \times \mathbb{Z}_9$

or $\quad G \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Homomorphisms: Let G, G' be groups.

Recall $\phi : G \longrightarrow G'$ is homomorphism if for all $a, b \in G$,

$$\phi(ab) = \phi(a)\phi(b).$$

Examples: • For any G, $\phi \equiv e : G \longrightarrow G$ by $\phi(x) = x$ is a homomorphism.

• For any G, G', $\phi : G \longrightarrow G'$ by $\phi(x) = e'$ is a homomorphism, since

$\phi(ab) = e' = e'e' = \phi(a)\phi(b)$.

• Let $\phi : S_n \longrightarrow \mathbb{Z}_2$ be given by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ even} \\ 1 & \text{if } \sigma \text{ odd.} \end{cases}$$

Check homomorphism; $\phi(\sigma_1\sigma_2) \stackrel{?}{=} \phi(\sigma_1) + \phi(\sigma_2)$. 4 cases

σ_1, σ_2 even $\Rightarrow \sigma_1\sigma_2$ even $\Rightarrow \phi(\sigma_1\sigma_2) = 0 = 0 + 0 = \phi(\sigma_1) + \phi(\sigma_2)$

σ_1 even, σ_2 odd $\Rightarrow \sigma_1\sigma_2$ odd $\Rightarrow \phi(\sigma_1\sigma_2) = 1 = 0 + 1 = \phi(\sigma_1) + \phi(\sigma_2)$

σ_1 odd, σ_2 even similar

σ_1, σ_2 odd $\Rightarrow \sigma_1\sigma_2$ even $\Rightarrow \phi(\sigma_1\sigma_2) = 0 = 1 + 1 = \phi(\sigma_1) + \phi(\sigma_2)$.

• **Reduction modulo n**: Let $\gamma : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ be given by $\gamma(m) = r$, where r is remainder of m divided by n. $\left(\begin{matrix} m = qn + r \\ 0 \le r < n \end{matrix}\right)$.

Then γ is a homomorphism.

Proof: Let $m_1, m_2 \in \mathbb{Z}$, want $\gamma(m_1 + m_2) = \gamma(m_1) +_n \gamma(m_2)$.

Write $m_1 = q_1 n + r_1$, $m_2 = q_2 n + r_2$,