Chapter 3: Structure of groups

Goal: 1. Classify finite abelian groups
2. Classify groups of small orders

Introduce: Direct product: \( H \times K \subseteq G, \quad H \cap K = \{1\} \Rightarrow HK = H \times K \)

Semi-direct product: \( H \triangleleft G, \quad K \leq G, \quad H \cap K = \{1\} \Rightarrow HK \cong H \rtimes K \)

\[ \left( H \times K, \ast \right) \]

\( \text{idea: If } H \triangleleft G, \quad K \leq G, \text{ then } HK \text{ is a group and each element has a unique way to be written as } hk, \quad h \in H, \quad k \in K \)

\[ \text{i.e., } HK \leftrightarrow \{(h, k) \mid h \in H, k \in K\} \quad \text{if } H \cap K = \{1\} \]

Using this correspondence, the set \( \{(h, k) \mid h \in H, k \in K\} \) (called the Cartesian product of \( H \times K \))

inherits a group structure from \( HK \). If \( K \triangleleft G \),

\[ (hk)(h'k') = hh'kk' \]

then \( (h, k)(h', k') = (hh', kk') \). This is the case of direct product.

§3.1 Direct Product of Groups

Def 3.1. Let \( A, B \) be two sets, the cartesian product of \( A, B \)

is the set \( A \times B = \{(a, b) \mid a \in A, b \in B\} \)

i.e. multiply component-wise.

Let \( H, K \) be two groups, the direct product of \( H \) and \( K \)

is the group \( (H \times K, \ast) \) with

\[ (h, k)(h', k') = (hh', kk') \quad \forall h, h' \in H, k, k' \in K \]

\( H, K \) are called the component groups of \( H \times K \) and there

are natural homomorphisms, the embeddings and projections

and \( H \times K \rightarrow H \) \( (h, k) \mapsto h \),

\( H \times K \rightarrow K \) \( (h, k) \mapsto k \).
Lemma 3.2 If $H, K \leq G$ and $H \cap K = \{1\}$, then $HK = H \times K$.

$\{ [h, k] \mid h \in H, k \in K \}$

$\text{pf}$ $H, K \leq G$ and $H \cap K = \{1\}$ $\Rightarrow [H, K] \leq \text{Hom}K = \{1\}$

$i$: $H, K$ commute, and the map $H \times K \rightarrow HK$ $(h, k) \mapsto hk$

$k$: $hk$ is a well-defined homomorphism. (Verify this!)

If $h \in H$, $k \in K$, $hk = 1$, then $h = k^{-1} \in \text{Hom}K = \{1\}$ and $k = h^{-1} = 1$.

Hence the homomorphism is injective and clearly surjective, so it's an isomorphism.

Assume $(m, n) = 1$

Chinese Remainder Theorem

$\exists a, b \ni 0 \leq x < mn$ s.t. $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$

i.e., $(m, n) = 1 \Rightarrow \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ (In fact, $\Rightarrow$)

$\text{pf}$ $\mathbb{Z}_{mn} = \langle a \rangle$, $\theta(a) = mn$. Take $H = \langle a \rangle$, $K = \langle a^m \rangle$.

Then $H \leq \mathbb{Z}_m$, $K \leq \mathbb{Z}_n$ and $(m, n) = 1 \Rightarrow H \cap K = \{1\}$.

By Lemma 3.2 $HK = H \times K$. Comparing orders, we have

$\mathbb{Z}_{mn} = HK = H \times K = \mathbb{Z}_m \times \mathbb{Z}_n$.

In general, we may define direct product for finitely many groups.

Definition 3.3 The direct product of the groups $G_1, G_2, \ldots, G_r$ is the group $(G_1 \times G_2 \times \cdots \times G_r, \times)$ with

$(g_1, g_2, \ldots, g_r) \in G_1 \times G_2 \times \cdots \times G_r$

and

$(g_1, g_2, \ldots, g_r) \ast (g_1', g_2', \ldots, g_r') = (g_1 g_1', g_2 g_2', \ldots, g_r g_r')$.

It has identity $(e_1, e_2, \ldots, e_r)$ and $(g_1, g_2, \ldots, g_r)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_r^{-1})$.

There are natural homomorphisms, embeddings and projections,

$h_i : G_i \rightarrow G_1 \times G_2 \times \cdots \times G_r$, $g_i : (1, 1, \ldots, 1, \ldots, 1) \rightarrow (g_i)$ and

$p_i : G_1 \times G_2 \times \cdots \times G_r \rightarrow G_i$, $(g_1, g_2, \ldots, g_r) \mapsto g_i$ for $i = 1, 2, \ldots, r$.

We identify $G_i$ with $\{1\} \times \cdots \times \{1\} \times G_i \times \{1\} \times \cdots$. It's called the $i$-th component group of $G_1 \times G_2 \times \cdots \times G_r$. 
Prop 3.4 (i) \( \forall \sigma \in S_r \), \( G_1 \times G_2 \times \cdots \times G_r \cong G_{(1)} \times G_{(2)} \times \cdots \times G_{(r)} \)

(ii) \( \ker \pi \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_r \) and \( G_i \trianglelefteq G_1 \times \cdots \times G_r \)

(iii) The component groups \( G_i \)'s commute.

(iv) \( (G_1 \times G_2) \times G_r \cong G_1 \times G_2 \times G_r \)

pf. exe. In such case, called internal direct product, called external direct product.

Theorem 3.5 If \( G_1 \triangleleft G_2 \cdots \triangleleft G_r \triangleleft G \) and \( \forall G_i \neq G_j \) for \( i \neq j \), then \( G \cong G_1 \times G_2 \times \cdots \times G_r \)

idea: The conditions \( \Rightarrow [G_i, G_j] = 1 \) \( \forall i \neq j \) and each element has unique way to be written as \( g_1 \cdots g_r \), \( g_i \in G_i \).

pf. Inductively apply Lemma 3.2 we have

\[ G_1 G_2 G_3 \cdots G_j \cong G_1 \times G_2 \times \cdots \times G_j \] \( \forall j = 1, 2, \cdots, r \)

Def. In this case, \( G \) is called internal direct product of \( G_1, G_2, \cdots, G_r \).

Remark 3.6 \( |G_1 \times \cdots \times G_r| = \prod_{i=1}^r |G_i| \) order of direct product is product of orders.

Hence direct product is finite iff all components are finite.

Example: Finite abelian groups are direct product of its Sylow subgps.

\( \begin{align*}
\text{eg. } Z_{12} &\cong Z_3 \times Z_4, \\
\text{Rank: each } n_i &\in 1, \text{ since all subgps are } Z_i.
\end{align*} \)

Theorem 3.7 If \( A \) is a finite abelian group of order \( n \geq 1 \)

Read \( \ref{5.2} \)

with prime factorization \( p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \). Then there are unique Sylow \( p_i \)-subgroups \( A_i \) such that

\( A \cong A_1 \times A_2 \times \cdots \times A_r \) \( (A_i \cong Z_{p_i^{a_i}} \times \cdots \times Z_{p_i^{a_i}}) \)

eg. order 16 = \( 2^4 \)

and this decomp is unique up to isom. \( \cong \).

How many such \( p_i \)?

pf. If \( A' \cong A_1' \times A_2' \times \cdots \times A_r' \) w/ \( \forall A_i' \cong p_i^{d_i} \), then \( A_1' \cong A_1 \)

since Sylow \( p_i \)-subgps is unique for abelian groups.
Semi-direct Product.

If $H < G$, $K < G$ and $H \cap K = 1$

$\forall h, h' \in H \Rightarrow h'h^{-1} = h^{-1}h' \in H \cap K$

Then each element in $HK \leq G$ has a unique way to be written as $hk, h \in H, k \in K$. We have a set theoretical bijection $HK \leftrightarrow H \times K$ (or sets).

"internal semi-direct product"

$$(h,k)(h',k') = (h(hk'k^{-1}), k'h)$$

Def. 3.8 Let $H \triangleleft G$ and $K < G$. Assume $H \cap K = 1$.

The semi-direct product of $H$ and $K$ is the group $(H \times K, \cdot)$ denoted $H \rtimes K$ with

$$(h, k) \cdot (h', k') = (h(h'k^{-1}), k'h')$$

for all $h, h' \in H, k, k' \in K$ where

$k'h = k'hk^{-1}$

(Verify the associativity by checking $k_1(k_2(k_3h)) = k_1(k_2(k_3h))$)

It has identity $(1, 1)$ and $(h, k)^{-1} = (h^{-1}, k^{-1})$.

Prop. 3.9 If $H \triangleleft G$ and $K < G$ with $H \cap K = 1$.

Then $G = HK \Rightarrow G \cong H \rtimes K$. In this case,

$K$ is called the complement of $H$ in $G$.

Remark 3.10 We have embeddings $H \hookrightarrow H \rtimes K, h \mapsto (h, 1)$

and $K \hookrightarrow H \rtimes K, k \mapsto (1, k)$. We have only one projection which fits into the short exact sequence

$$1 \rightarrow H \rightarrow H \rtimes K \rightarrow K \rightarrow 1.$$ 

$H$ is normal in $H \rtimes K$. If $K$ is normal in $H \rtimes K$ then $H \rtimes K = H \times K$ (and the short exact sequence splits.)

Question: How to define $H \rtimes K$ if we don’t have a $G$? $h \cdot k = ?$
an action of $K$ on $H$.

Goal: Redefine $k, h'$ so that the operation is still associative.

Solution: $k'$ need to be a homomorphism!

Theorem/Def 3.11 Given a group homomorphism $\varphi: K \rightarrow \text{Aut}(H)$, define an operation $\ast_\varphi$ on the set $H \times K$ by

$$(h, k) \ast_\varphi (h', k') = (\varphi(h) h', k k')$$

where $h, h' \in \varphi(K), k, k' \in H$. Then $(H \times K, \ast_\varphi)$ is a group. It's called the semidirect product of $H$ and $K$ under $\varphi$ and denoted by $H \rtimes K$.

pf. This is by the same reason as before (Def 3.8) with identity $(1_H, 1_K)$ and $(h, k)^{-1} = (h^{-1}, k^{-1})$ since $K$ acts on $H$ by $\varphi$.

(NB. The notation $H \rtimes K$ means it's a Cartesian product $H \times K$ with group structure given by $K$ acting on $H$ by $\varphi$. Then $H$ is a normal subgroup of $H \rtimes K$ and the conjugation is given by $k h k^{-1} = \varphi(k) h$. If you see $H \rtimes K$, then it means $K$ is normal and conjugation by $H$ is given by $\varphi(k) h$ where $\varphi: H \rightarrow \text{Aut}(K)$.)

Example 3.12 Group of order 12.

\begin{align*}
\begin{array}{c|c|c}
\varphi & 0 & 1 \\
\hline
a & \frac{1}{2} & \frac{3}{2} \\
b & \frac{1}{2} & \frac{3}{2} \\
c & \frac{1}{2} & \frac{1}{2} \\
\end{array}
\end{align*}

2 of them need to be

1. $\frac{1}{2}$
2. $\frac{3}{2}$
3. $\frac{1}{2}$

Call the ones sending to $\frac{1}{2}, a$ and $b$, the other $C$.

Case 1 $n_2 = 1, n_3 = 1$ isomorphic type $Z_4 \times Z_3$. $V_4 \times Z_3 = Z_2 \times Z_6$

Case 2 $n_2 = 3, n_3 = 1$ isomorphic type $Z_6 \times Z_3$. $V_6 \times Z_3$

where $\varphi: \frac{1}{2} \rightarrow \text{Aut}(Z_3) \cong Z_3^2$ nontrivial $(n_2 \neq 1)$.

Hence $\varphi(\frac{1}{2}) = \text{mult. by } \frac{1}{2}$

$Z_4 \times Z_3 \cong \langle a, b \mid a^4 = b^3 = 1, ab \bar{b}a^{-1} = a^2 \rangle$

and $\psi: V_4 \rightarrow \text{Aut}(Z_3)$ nontrivial, $V_4 = \{1, a, b, c\}$ $\psi(a) = \psi(b) = \text{mult.}$

$V_4 \times Z_3 = \langle q, b, d \mid q^2 = b^3 = 1, ab = ba, ada = d^2 = bd b^{-1} \rangle$
Case 3 \( n_2 = 1, \ n_3 = 4 \) isom type \( A_4 \)

Originally, we are looking for

(i) \( \mathbb{Z}_4 \times \mathbb{Z}_2 \phi: \mathbb{Z}_3 \to \text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_4^* = \{1, 5\} \)

(ii) \( V_4 \times \mathbb{Z}_3 \psi: \mathbb{Z}_8 \to \text{Aut}(V_4) \cong GL(2, \mathbb{Z}_2) \)

In case (i), \( \overline{1} \mapsto 5 \) trivial \( \Rightarrow \mathbb{Z}_3 \) normal

\( \overline{1} \mapsto 3 \) not possible by order consideration

Here \( \overline{1} \mapsto 3 \) possible if cyclic. See next section.

\( i^2 \phi: V_4 \)

Recall: \( G \cong S_3 \Delta \)

\[ G \to S_4 \] with trivial kernel

since \( N_G(Q) = Q \) if \( [G:N_G(Q)] = [G:Q] \) and kernel of \( \cap N_G(Q) \)

Thus \( G \cong S_4 \) and \( G \) contains 8 many order 3 elt.

\[ G = \langle 3 \text{-cycles} \rangle \] and \( G = A_4 \)

Lemma 3.13 If \( K \) is cyclic and

\[ \phi_1: K \to \text{Aut}(H) \]

\[ \phi_2: K \to \text{Aut}(H) \]

in particular, the same

\[ \phi_1(K) \text{ and } \phi_2(K) \text{ are conjugate} \]

Then \( H \times K \cong \overline{H \times K} \).

We omit the proof. (See Textbook Ex. 5.5.6) and do one, ex.

Prop 3.14 Let \( p, q \) be primes with \( p > q \). Then there are at most two isomorphic types of groups of order \( p \cdot q \), which are the cyclic group \( \mathbb{Z}_{pq} \) and the semi-direct product

\[ \mathbb{Z}_p \times \mathbb{Z}_q = \langle a, b \mid a^p = b^q = 1, bab^{-1} = a_{r_0} \rangle \]

for some \( r_0 \) s.t. \( 1 < r_0 < p, \ r_0 \equiv 1 \pmod{p} \). The latter occurs when \( p \equiv 1 \pmod{q} \)
pf. \( p > q \Rightarrow Sylow \ p \)-subgroup is normal and unique

\[ \text{Aut}(\mathbb{Z}_p) \sim \mathbb{Z}_p^* \text{ cyclic (HW8 \#8)} \]

Any homo \( \varphi : \mathbb{Z}_q \to \text{Aut}(\mathbb{Z}_p) \sim \mathbb{Z}_p^* \) is equal to

\[ \varphi = \mathbb{Z}_q \to \text{Aut}(\mathbb{Z}_p) \sim \mathbb{Z}_p^* \text{, } \varphi(a) = a \]

NB

\[ \Sigma = \{ \overline{1} \} \text{ for } \overline{r} \in \Sigma = \{ \overline{0} \} \]

\[ q | p - 1 \]

\( \forall \overline{r} \in \Sigma \setminus \{ \overline{1} \} \) we have \( \overline{r} = \overline{r}_0 \overline{l} \) and a map

\[ \mathbb{Z}_p^* \times \mathbb{Z}_q \to \mathbb{Z}_p^* \times \mathbb{Z}_q \]

\[ a = (1, 0) \mapsto a_0 = (1, \overline{0}) \]

\[ b = (0, 1) \mapsto b_0 = (0, \overline{0}) \]

\[ b_0 a b^{-1} = a_0 \]

\[ a^r \mapsto a_{\overline{r}} \]

and \( a_0^p, b_0^q \mapsto 1 \). The map is well-defined.

and defines a homomorphism as \( a_0, b_0 \) generate \( \mathbb{Z}_p^* \times \mathbb{Z}_q \).

Since \( \mathbb{Z}_q \) is generated by any nonzero element, so

\[ a_0, b_0^p \] also generate \( \mathbb{Z}_p^* \times \mathbb{Z}_q \). The map is an isom.

We conclude group of order 12 has only two isom types,

\( \mathbb{Z}_p^* \times \mathbb{Z}_q \) and \( \mathbb{Z}_p^* \times \mathbb{Z}_q \) (\( \cong \mathbb{Z}_p^* \times \mathbb{Z}_q \), \( r \in \Sigma \)). □

Hint to Lemma: If \( \varphi_2(k) = \sigma \varphi_1(k) \sigma^{-1} \) with K cyclic, then

\( \varphi_2(k) \) generated by \( \varphi_2(k) \) \( \Rightarrow \varphi_2(k) \) generated by \( \sigma \varphi_1(k) \sigma^{-1} \).

and hence \( \varphi_2(k) = \sigma \varphi_1(k) \sigma^{-1} \) for some \( (a, 1k_1) = 1 \).

This implies \( \varphi_2(k) = \sigma \varphi_1(k) \sigma^{-1} \) \( \forall k \in K \) and \( H \times K \cong H \times K \)

by \( (k_1, k_2) \mapsto (\sigma(k_1), k_2) \). □
§3.3 Abelian groups.

Recall in Theorem 3.7 Every abelian group of order \( n \) with prime decomposition \( p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r} \) is a direct sum of its Sylow \( p_i \)-subgroups, \( i=1,2,\ldots,r \):

\[ A = A_1 \times A_2 \times \cdots \times A_r, \quad |A_i| = p_i^{e_i} \]

Question: How to determine the structure of each abelian \( p_i \)-groups (the \( A_i \)'s)?

Idea: \( A_i = \mathbb{Z}_{p_i^{e_i}} \), where \( e_i = e \) for each \( i \).

How to determine \( p_i^{e_i} \)? - largest order!

Prop 3.15 Finite abelian \( p \)-groups are direct product of cyclic \( p \)-groups.

pf. \(|A| = p^n \), \( p \) prime, \( A \) abelian group, \( n \) some pos. int.

By the Lagrange Theorem, \( \forall a \in A \), \( 0(a) = p^m \) for some \( m \leq n \). Induction on \( n \), we assume theorem holds for abelian groups of order \( p^n \) for \( n' < n \).

We take \( a_i \in A \) s.t. \( 0(a_i) = \max \{ 0(a) \} \).

Then \( 0(a_i) = p^n \) for some \( n_i \leq n \). If \( n_1 = n \) then \( A \)

is cyclic. Assume \( n_1 < n \), then \(|A/a_i|\) is an abelian \( p \)-group of order \( p^{n-n_1} \).

By induction, \( A/a_i = \langle t_2 \rangle \times \langle t_3 \rangle \times \cdots \times \langle t_r \rangle \).

\[ b_{i_1}^{p_{i_1}} = a_i, \quad b_{i_1}^{p_{i_1}} = 1 \]

\[ p^{n_i} | b_{i_1}^{p_{i_1}}, (b_{i_1}^{p_{i_1}}) | p_{i_1}^{n_i} \]

For some \( b_2, b_3, \ldots, b_r \in A \), with some orders \( 0(b_j) = p^{n_j} \) and \( n_2, n_3, \ldots, n_r = n-n_1 \). Want to replace \( b_i \) with \( b_i^{p_i} \).

Then \( b_i^{p_i} \in \langle a_i \rangle \). \( \exists \ b_{i_1}^{p_{i_1}}, \ldots, b_{i_k}^{p_{i_k}} \) s.t. \( b_i^{p_i} = a_i \) for \( i = 1,2,\ldots,k \).

This implies \( p_i^{n_i} | b_i \), say \( b_i = p_i^{n_i} b_i' \).
Since $b_i^{p_i^{n_i}} = (a_i^{m_i})^{p_i^{n_i}}$ for some $m_i \in \mathbb{N}$, $i = 1, 2, \ldots, r$

Consider $a_i = b_i^{m_i}$. Then $a_i^{-1} b_i^{-m_i} = 1$ and $a_i = p_i^{n_i}$.

Since $o(a_i) = p_i^{n_i}$, so $p_i^{n_i} | o(a_i)$ ($A \to A/a_i$ is homo)

We have $o(a_i) = p_i^{n_i}$ and

$$1 \to \langle a_i \rangle \to A \xrightarrow{\pi} A/a_i \to 1$$

is a short exact sequence with $\pi$ the identity on $\langle a_2, a_3, \ldots, a_r \rangle$.

We get

$$\langle a_2, a_3, \ldots, a_r \rangle \cong \langle a_2 \rangle \times \langle a_3 \rangle \times \cdots \times \langle a_r \rangle$$

(by HW8 #6) $A \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_r \rangle$.

Question: If we follow the same strategy to decompose abelian group of order $n$ then what will happen?

If $o(a_i) = \text{largest } n_i$, and $A^n = 1$ for a?

Invariant factors of abelian groups

By Theorem 3.7 and Prop 3.15, we have $A$ as in Thm 3.7

Isom to

$$\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}$$

for some $e_1 + e_2 + \cdots + e_r = d_i$

$e_1 \geq e_2 \geq \cdots \geq e_r \geq 0$

for some $e_{i_1} + e_{i_2} + \cdots + e_{i_k} = d_i$.

$e_{i_1} \geq e_{i_2} \geq \cdots \geq e_{i_k} \geq 0$

$L = \max \{ e_1, e_2, \ldots, e_r \}$

$L = \max \{ e_1, e_2, \ldots, e_r \}$

$e_i 
eq 0$

This is called the elementary divisor decomposition.

The invariant factors of $A$ are the numbers

$$n_1 = p_1^{e_1}, n_2 = p_1^{e_2}, \ldots, n_r = p_1^{e_r},$$

and $n_i$ fact. decm is

$$A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}, \text{ with } n_i = n_{i-1} \cdots n_2 n_1, n = n_1 n_2 \cdots n_r.$$
Theorem 3.16. Every finite abelian group is isomorphic to
\[ \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \quad \text{with} \quad d_i \mid d_{i+1}, \quad d_i > 1 \quad \forall i \]
and \( d_1, d_2, \ldots, d_r \) : the order of the group. The numbers \( d_1, d_2, \ldots, d_r \) are called the invariant factors, and the abelian group is said to be of type \((d_r, d_{r-1}, \ldots, d_1)\).

Remark: Let \( d_i = \max \{ o(a) \} \) and \( o(a) \mid d_i \) for \( a \in A \).

Examples:

<table>
<thead>
<tr>
<th>invariant factors</th>
<th>elementary factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>2^3 \times 3 \times 7 \times 3</td>
<td>2^3, 3, 3, 5, 7</td>
</tr>
<tr>
<td>2^2 \times 5 \times 7, 2 \times 5, 5</td>
<td>2^2, 3, 5, 5, 5, 7^2</td>
</tr>
<tr>
<td>2^2 \times 3 \times 5, 2 \times 3, 7</td>
<td>2^2, 2, 2, 3, 3, 5</td>
</tr>
</tbody>
</table>

Example 3.17. Classify all abelian groups of order 16 = 2^4.
\[
\begin{align*}
\mathbb{Z}_{16}, & \quad \mathbb{Z}_8 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad 4 \\
\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, & \quad \mathbb{Z}_4^2, \quad 3+1 \\
\mathbb{Z}_2 \times \mathbb{Z}_2, & \quad \mathbb{Z}_2^4, \quad 2+1 \\
& \quad \mathbb{Z}_2^2 \times \mathbb{Z}_2, \quad 1+1+1+1 \\
& \quad \mathbb{Z}_2^4 \times \mathbb{Z}_2, \quad 1+1+1+1+1 \\
\end{align*}
\]

Remark 3.18. The elementary factors and invariant factors of any finite abelian group are uniquely determined.

Remark 3.19. Every finitely generated abelian group is isomorphic to \( \mathbb{Z}^r \times \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \), for some \( r \geq 0, d_1, d_2, \ldots, d_r \). The number \( r \) is called the rank of the abelian group.
§3.4 Classification of groups.

So far we have seen: $p > 9$ primes

1. $G = \mathbb{Z}_p$ cyclic
2. $\mathbb{Z}_p^2$, $\mathbb{Z}_p \times \mathbb{Z}_p$
3. $\mathbb{Z}_{pq}$, $\mathbb{Z}_p \times \mathbb{Z}_q$ (if $p \neq 1 \pmod{q}$)
4. $\mathbb{Z}_{p^2}$ (e.g., $p = 10$)
5. $\mathbb{Z}_9$ (e.g., $p = 12$)

You may try them, solvable if known.

$\mathbb{Z}_p^3$ (e.g., $p = 8$):

$\text{Aut}(\mathbb{Z}_p^3) \cong GL_3(\mathbb{Z}_p)$

Lemma 3.20 $\text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) \cong GL_2(\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}_{a,b,c,d \in \mathbb{Z}_p}$

pf: $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$ homeomorphism

$(1,0) \mapsto (a,b)$  $(0,0) \mapsto (c,d)$

Since the map is invertible, so is the matrix.

Such correspondences are one-to-one and respect the operations. \( \square \)

(p > 2 prime)

Prop 3.21 Nonabelian $p$-group of order $p^3$ are isomorphic to:

either $\mathbb{Z}_p^3 \times \mathbb{Z}_p = \langle a, b | a^p = b^p = 1, bab^{-1} = a^{p+1} \rangle$

or $\mathbb{Z}_p \times (\mathbb{Z}_p \times \mathbb{Z}_p) = \langle a, b, c | a^p = b^p = c^{p^2} = 1, ab = ba, bc = cb \text{ and } cac^{-1} = ab \rangle$

pf. Take $a \in G$, $o(a)$ the largest.

Case 1. If $o(a) = p^3$, then $G \cong \mathbb{Z}_p^3$ is abelian

Case 2. If $o(a) = p^2$, then $\langle a \rangle \triangleleft G$. Since $p$ is the smallest prime dividing $|G|$, $\langle a \rangle$ is the kernel of some action $G \to S_p$.

Hence $\langle a \rangle \triangleleft G$. Take any $a \notin \langle a \rangle$, $G = \langle a, \delta \rangle$. Then $a \cdot \delta = 1$, $a^p = a^\delta$ for some $1$. \( \Rightarrow k = mp \text{ for some } m \in \mathbb{N} \).
Take \( b = a^{1-m} \notin \langle a \rangle \), then \( o(b) = p \) and \( \langle a \rangle \cap \langle b \rangle = 1 \).

Hence \( G = \langle a \rangle \langle b \rangle = \mathbb{Z}_p^2 \times \mathbb{Z}_p \) for some \( q \).

\[ \varphi : \mathbb{Z}_p \to \text{Aut}(\mathbb{Z}_p^2) = \mathbb{Z}_p^{\times 2} \text{ (Cyclic by HWS #8)} \]

Since \( \mathbb{Z}_p^2 \) is abelian, the subgroup of order \( p \) is cyclic and unique, if \( \varphi(\mathbb{Z}_p) \neq 1 \), by Lemma 3.13, the semidirect product \( \mathbb{Z}_p^2 \rtimes \mathbb{Z}_p \) is unique.

Say \( \varphi : \hat{\mathbb{Z}_p^2} \to \text{mult by } p+1 \). Then \( (p+1)^p = 1 \pmod{p} \).

\[ \mathbb{Z}_p^2 \rtimes \mathbb{Z}_p \cong \langle a, b \mid a^p = b = 1, b^{-1} a^p b = a^{p+1} \rangle \]

Case 3: \( o(a) = p \). Then \( \forall g \in G, g \neq 1 \implies o(g) = p \).

By Generalised Cauchy/Sylow I, there exists a

Subgroup \( H \) of \( G \) of order \( p^2 \), and \( H \trianglelefteq G \).

Then \( H \cong \mathbb{Z}_p \times \mathbb{Z}_p \).

Take \( C \notin H \) then \( o(c) = p \) and \( \langle c \rangle \cap H = \{1\} \).

Hence \( G = \langle c \rangle \cong (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p \) for some

\[ \varphi : \mathbb{Z}_p \to \text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) = GL_2(\mathbb{Z}_p) \text{ nontrivial} \]

\[ (p^2-1)(p^2-p) = p(p-1)^2(p+1) \]

Since if \( \varphi \neq 1 \), then \( \text{im} \varphi \) is a Sylow \( p \)-subgroup, and

all such subgroups are conjugate.

by Lemma 3.13, the semidirect products are isom for all \( \varphi \) nontrivial.

Eg. \( \text{im} \varphi = \langle (1, \mathbb{Z}_p), (1, 1) \rangle \)

\[ G = \langle a, b, c \mid a^p = b = c = 1, ab = ba, cac^{-1} = ab, cbc^{-1} = b \rangle \]
Group of small orders

<table>
<thead>
<tr>
<th>Order</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$Z_2$, $V_4$</td>
</tr>
<tr>
<td>3</td>
<td>$Z_3$, $D_3$</td>
</tr>
<tr>
<td>4</td>
<td>$Z_4$, $V_4$</td>
</tr>
<tr>
<td>5</td>
<td>$Z_5$, $D_5$</td>
</tr>
<tr>
<td>6</td>
<td>$Z_6$, $S_3$</td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$Z_8$, $D_8$, $Q_8$</td>
</tr>
<tr>
<td>9</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$Z_{10}$, $D_{10}$</td>
</tr>
<tr>
<td>11</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>$Z_{12}$, $Z_2 \times Z_6$, $A_4$, $Z_4 \times Z_3$, $V_4 \times Z_3 \cong D_{12}$</td>
</tr>
<tr>
<td>13</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$Z_{14}$, $D_{14}$</td>
</tr>
<tr>
<td>15</td>
<td>$Z_{15}$, $Z_3 \times Z_5$ (abelian), $D_6 \times Z_2$, $Q_8 \times Z_2$</td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

$P \not\triangleleft G$ solvable

<table>
<thead>
<tr>
<th>Order</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$Z_2 \times Z_2$, $Z_2 \times Z_6$, $Z_4 \times Z_3 \cong D_{18}$, $(Z_3 \times Z_3) \times Z_2$</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$Z_4 \times Z_7$, $D_{20}$, $Z_4 \times Z_5$, $Z_8 \times Z_5$, $V_4 \times Z_5$</td>
</tr>
</tbody>
</table>

Can see $2^4$ is already complicated

Thm 3.22: Simple nonabelian groups of order $\leq 100$ are isomorphic to $A_5$.

Idea: Recall: groups of order $p^n$, $2p^n$, $p^1$, $2p^1$, $p^9$, $2p^9$, $p^9 r$ are solvable.

$\{24, 36, 40, 48, 56, 72, 90, 96, 100\}$

$\{3, 6, 10, 15\}$

Simple non-solvable $\Rightarrow n$ is not a power of $2$, $3$, or $5$.
Feit and Thompson: Every noncyclic finite simple gp has even order.

Braver: [key is to study centralizer of order 2 elements]

Remark: In Langlands classification of representations, one key is to look at centralizer of abelian 2-groups.

Last piece of cyclic groups.

\[ \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \quad \text{if } (m,n) = 1 \]

\[ \mathbb{Z}_{mn}^x \cong \mathbb{Z}_m^x \times \mathbb{Z}_n^x \quad \text{if } (m,n) = 1 \]

Lemma 3.23 \( \mathbb{Z}_p^x \) is cyclic of order \( p-1 \).

Prop 3.24 \( \mathbb{Z}_p^x \) is cyclic of order \( \varphi(p^n) = p^{n-1}(p-1) \) if \( p \text{ odd} \)

and \( \mathbb{Z}_p^x \cong \mathbb{Z}_2^x \times \mathbb{Z}_{2^{n+1}}^x \quad n > 2 \)

(See HW 5 solution.)

\( \langle \overline{a} \rangle = \mathbb{Z}_p^x \) i.e., \( a^{p-1} \equiv 1 \pmod{p} \)

\[ a^{p-1} = 1 + k_p p \] Assume \( p \nmid k_p \), i.e., \( a^{p-1} \not\equiv 1 \pmod{p^2} \)

\[ a^{\varphi(p^n)} = (a^{p-1})^{p^{n-1}} = (1 + k_p p)^{p^{n-1}} \equiv 1 \pmod{p^n} \]

\( o(a) \mid \varphi(p^n) \) and \( p-1 \mid o(a) \therefore o(a) = p^i(p-1) \) for some \( i \)

Proof: Induction on \( n \) that \( a^{\varphi(p^i)} = 1 + k_i p^{i} \) and \( a^{p^i} = 1 + k_i p^i \) with \( p \nmid k_i \),

where \( a \in \mathbb{Z} \Rightarrow a^{p^i} = 1 + k_i p^i \) with \( p \nmid k_i \)

Assume true for \( i < n \)

Then \( a^{p^{n-1}(p-1)} = 1 + k_{n-1} p^{n-1} \not\equiv 1 \pmod{p^n} \)

and \( a^{p^n(p-1)} = 1 + k_n p^{n-1} p + p^{n+1}k' \) for some \( k' \in \mathbb{Z} \)

\[ = 1 + (k_{n-1} + pk') p^n \]

Take \( k_n = k_{n-1} + pk' \). Then \( p \nmid k_n \). (Induct \( k_i \equiv k_1 \pmod{p} \).