Chapter 3  
Structure of groups

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

Introduce: Direct product: $H \times K \leq G$, $H \cap K = \{1\} \implies HK = H \times K$

Semi-direct product: $H \triangleleft G$, $K \leq G$, $H \cap K = \{1\} \implies HK \cong H \rtimes K$

This method is enough for classifying groups of order $\leq 100$.

§3.1 Direct Product of Groups

Def 3.1 Let $A$, $B$ be two sets, the Cartesian product of $A$, $B$ is the set $A \times B = \{(a, b) | a \in A, b \in B\}$.

Let $H$, $K$ be two groups, the direct product of $H$ and $K$ is the group $(H \times K, \ast)$ with

$$(h, k) \ast (h', k') = (hh', kk') \quad h, h' \in H, k, k' \in K.$$
Lemma 3.2 If $H, K \leq G$ and $H \cap K = 1$ then $HK \cong H \times K$.

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

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

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

is a well-defined homomorphism. (Verify this!)

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

Hence the Gomom is injective and clearly surjective, so it is an isomorphism.

Assume $(m,n) = 1$.

Chinese Remainder Theorem Va.6 \(
\exists 0 \leq x < mn \text{ s.t. } x \equiv a \pmod{m}, x \equiv b \pmod{n}
\)

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

pf: \(\mathbb{Z}_{mn} = \langle a \rangle \), \(0(a) = mn\). Take $H = \langle a^n \rangle$, $K = \langle a^m \rangle$.

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

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

\(\mathbb{Z}_{mn} = HK \cong H \times K \cong \mathbb{Z}_m \times \mathbb{Z}_n\).

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 $(G_1 \times G_2 \times \cdots \times G_r, *)$ with

\(r \times G_2 \times \cdots \times G_r = \{(g_1, g_2, \ldots, g_r) \mid g_i \in G_i, 1 \leq i \leq r\}\)

and

\((g_1, g_2, \ldots, g_r) * (g_1', g_2', \ldots, g_r') = (g_1g_1', g_2g_2', \ldots, g rg_r')\).

It has identity $(1, 1, \ldots, 1)$ 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,

\(l_i: G_i \rightarrow G_1 \times G_2 \times \cdots \times G_r\)

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

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

We identify $G_i$ with $l_i(G_i)$ and it's called the $i$-th component group of $G_1 \times G_2 \times \cdots \times G_r$. 
Prop 3.4
(i) \( \forall s \in S_r, \ G_1 \times G_2 \times \cdots \times G_r \cong G_{(1)} \times G_{(2)} \times \cdots \times G_{(r)} \)
(ii) \( \ker T_1 \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_r \) and \( G_i \trianglelefteq G_1 \times \cdots \times G_r \)
(iii) The component groups \( G_i \) 's commute.
(iv) \((G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)\)

pf. ex: In such case, called internal direct product, called external direct product.

Theorem 3.5
If \( G_1, G_2, \ldots, G_r \triangleleft G \) and \( G = G_1 G_2 \cdots G_r \), then
\[
G = G_1 G_2 \cdots G_r \Rightarrow G \cong G_1 \times G_2 \times \cdots \times G_r .
\]

idea: The conditions \( \{G_i, G_j\} = 1 \) \( \forall i \neq j \) and each element has unique way to be written as \( g_1 g_2 \cdots g_r \), \( g_i \in G_i \).

pf: Inductively apply Lemma 3.2, we have
\[
G_1 G_2 G_3 \cdots G_{j-1} G_j \cong G_1 G_2 \cdots G_{j-1} G_j \text{ for } j=1, 2, \ldots, r.
\]

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

Remark 3.6
\[
|G_1 \times \cdots \times G_r| = \prod_{i=1}^r |G_i|
\]

order of direct product is product of order.

Hence direct product is finite iff all components are finite.

Example: Finite abelian groups are direct product of its Sylow subgroups.
\[
\text{eg. } \mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3 .
\]

Rmk: each \( a_p = 1 \), since all subgroups are \( \mathbb{Z} \).

Theorem 3.7
If \( A \) is a finite abelian group of order \( n > 1 \) with prime factorization \( P_1^{a_1} P_2^{a_2} \cdots P_s^{a_s} \). Then there are unique Sylow \( P_i \)-subgroups \( A_i \) such that
\[
A = A_1 \times A_2 \times \cdots \times A_s .
\]

eg order 16 = 2^4
and this decomposition is unique up to isomorphism.

\[
\text{How many such } A_1, A_2, \ldots, A_s ?
\]

Ps. If \( A = A_1 \times A_2 \times \cdots \times A_s \) with \( |A_i| = p_1^{a_1} \). Then \( A_i \cong A_1 \).

2^4, (2^2, 2), (2^2, 2), (2^2, 2)
12, 2, 2, 2, 2, 2, 2

since Sylow p-subgroups are unique for abelian groups.
Semi-direct Product

Idea: If $H \triangleleft G$ and $K \triangleleft G$ and $H \cap K = \{e\}$

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 $HK \leftrightarrow H \times K$ (as sets)

"Internal semi-direct product"

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

Def 3.8 Let $H \triangleleft G$ and $K \triangleleft G$. Assume $H \cap K = \{e\}$

The semi-direct product of $H$ and $K$ is the group $(H \times K, *)$, denoted $H \rtimes K$, with $(h, k)(h', k') = (h(h'k'k^{-1}), kh'h^{-1}k^{-1})$

for all $h, h' \in H$, $k, k' \in K$ where $h'h^{-1}k^{-1}$

(Verify the associativity by checking $(h_1h_2k_2k_3)(h_3k_3k_4) = h_1(h_2k_3k_4)(k_1k_2k_3k_4)$)

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

Prop 3.9 If $H \triangleleft G$ and $K \triangleleft G$ with $H \cap K = \{e\}$

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

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

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

and $K \hookrightarrow H \times K$, $k \mapsto (1, k)$. We have only one projection

which fits into the short exact sequence

$$1 \rightarrow H \rightarrow H \times K \xrightarrow{T_h} K \rightarrow 1$$

$H$ is normal in $H \times K$. If $K$ is normal in $H \times K$ then $H \times K = H \times K$

(c and the short exact sequence split.)

Question: How to define $H \rtimes K$ if we don't have a $G$? $\triangleright H \rtimes K = ?$
an action of $K$ on $H$

Goal: Redefine $\cdot$, $\cdot'$ so that the operation is still associative.

Solution: $\cdot'$ need to be a homomorphism!

Theorem/Def 3.11: Given a group homom $K \xrightarrow{\varphi} \text{Aut}(H)$,

Define an operation $\ast_\varphi$ on the set $H \times K$ by

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

where $h, h' = \varphi(k)h' \in H$. Then $(H \times K, \ast_\varphi)$ is a group. It's called the semidirect product of $H$ and $K$ act $\varphi$ 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 $((h, k))^{-1} = (h^{-1}, k^{-1})$ so $K$ acts on $H$ by $\varphi$.

(NB. The notation $H \ltimes K$ 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 $H \times K$ and the conjugation is given by $h \varphi k \varphi^{-1} = \varphi(k)h \varphi$. If you see $H \times K$ then it means $K$ is normal and conjugation by $H$ is given by $\varphi(1)$.)

Example 3.12: Group of order 12.

Case 1: $n_2 = 1, n_3 = 1$ isomorphic type $\mathbb{Z}_4 \times \mathbb{Z}_3$, $V_4 \ltimes \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_6$

Case 2: $n_2 = 3, n_3 = 1$ isomorphic type $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$, $V_4 \rtimes \mathbb{Z}_3$

where $\varphi: \mathbb{Z}_4 \to \text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_3$ nontrivial $(n_2 \neq 1)$.

Hence $\varphi(1) = \text{mult. by } \overline{4}$. $\mathbb{Z}_4 \ltimes \mathbb{Z}_3 = \langle a, b | a^4 = b^3 = 1, bab^{-1} = a^{-1} \rangle$.

Add: $\psi: V_4 \to \text{Aut}(\mathbb{Z}_3)$ nontrivial, $V_4 = \{1, a, b, c \}$ $\psi(a) = \psi(b) = \text{mult}$

$V_4 \ltimes \mathbb{Z}_3 = \langle a, b, d | a^4 = b^3 = d^3 = 1, ab = ba, ada = d = bd b^{-1} \rangle$. 

$\psi$.
Case 3: $n_2 = 1, n_3 = 4$ isom type $A_4$

Originally, we are looking for

(i) $\mathbb{Z}_4 \times \mathbb{Z}_3 \stackrel{\varphi}{\rightarrow} \text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_4^\times = \{1, 3\}$

(ii) $\mathbb{V}_4 \times \mathbb{Z}_3 \stackrel{\psi}{\rightarrow} \text{Aut}(\mathbb{V}_4) \cong \text{GL}_2(\mathbb{Z}_2)$

In case (i), $\varphi$ is trivial $\Rightarrow \mathbb{Z}_3$ is normal.

Order 3 $\nmid 2$

(ii) It can be complicated, but it works if $\mathbb{Z}_3$ is cyclic. See next lemma.

Let $G \supset V_4$.

Recall: $G \geq Syl_3(G) \Rightarrow G \rightarrow S_4$ with trivial kernel.

Since $N_G(Q) = Q$ if $[G:N_G(Q)] = [G:Q]$ and kernel $\cong \bigcap N_C(k)$.

Hence $G \leq S_4$, 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

\[q_1 : K \rightarrow \text{Aut}(H)\]

\[q_2 : K \rightarrow \text{Aut}(H)\]

in particular, the same.

Homomorphisms st. $q_1(K)$ and $q_2(K)$ are conjugate.

Then $H \times K \cong H \times K$.

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 $p^2 q$, which are the cyclic group $\mathbb{Z}_{p^2 q}$ and the semi-direct product

$\mathbb{Z}_p \ltimes \mathbb{Z}_q = \langle a, b | a^p = b^q = 1, b^{-1}ab = a^{r_0} \rangle$

for some $r_0$ st. $1 < r_0 < p, r_0^q \equiv 1 \mod{p}$. The latter occurs when $p \equiv 1 \mod{q}$.
pf: \( p > q \Rightarrow \) Sylow \( p \)-subgroup is normal and unique 
\( \text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^{\times} \) cyclic (HW & §8)

Any homomorphism \( \varphi: \mathbb{Z}_q \to \text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^{\times} \) is equal to
\[
\varphi_q = \mathbb{Z}_q \to \text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^{\times} ; \varphi_q(\bar{e}) = \text{mult} \text{ by } \bar{e}
\]
for \( \bar{e} \in \Sigma = \{ \bar{e} \in \mathbb{Z}_p \mid \bar{e} \neq 0 \} \)

NB
\( \Sigma \neq \{ \bar{1} \} \)

\( \Sigma \) is a cyclic group, \( \exists r_0 \in \Sigma, \Sigma = \langle r_0 \rangle \)

\( q \mid p - 1 \)

\( \forall \bar{e} \in \Sigma \setminus \{1\} \) we have \( \bar{e} = r_0^l \) and a map

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

\[
a = (\bar{a}, 0), \quad \mapsto a' = (\bar{a}, 0)
\]

\[
b = (0, \bar{b}), \quad \mapsto b' = (0, \bar{b})
\]

with \( b'a'b^{-1} \to b'^{-l}a'o^l \to a'^l \)

\( a \tau \to a'^{\tau} \)

and \( a'^{p}b'^{\bar{q}} \to 1 \).

The map is well-defined.

and defines a homomorphism as \( a, b \) generate \( \mathbb{Z}_p \times \mathbb{Z}_q \).

Since \( \mathbb{Z}_q \) is generated by any nonzero element, so \( a, b \) also generate \( \mathbb{Z}_p \times \mathbb{Z}_q \). The map is an isomorphism.

We conclude that a group of order 12 has only two isomorphism types,
\( \mathbb{Z}_p \times \mathbb{Z}_q \) and \( \mathbb{Z}_p \times \mathbb{Z}_q \) (\( \cong \mathbb{Z}_p \times \mathbb{Z}_q \), \( r \in \Sigma \)). \( \square \)

**Hint to Lemma:** If \( \varphi(k) = \sigma \varphi(k) \sigma^{-1} \) with \( K \) cyclic, then \( \varphi \) generated by \( \varphi(k) \) \( \Rightarrow \) \( \varphi \) generated by \( \sigma \varphi(k) \sigma^{-1} \).

and hence \( \varphi(k) \sigma = \sigma \varphi(k) \sigma^{-1} \) for some \( (a, 1Kl) = 1 \).

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

by \( (h, k) \mapsto (\sigma(h), k^\sigma) \). \( \square \)