1. Direct Products of Groups

Definition 1.1. If $G$ and $H$ are groups, then the direct product $G \times H$ is the set $G \times H$ equipped with the binary operation

$$(g,h)(g',h') = (gg', hh').$$

Theorem 1.2. The direct product $G \times H$ of groups $G$ and $H$ is a group.

Proof. To check associativity of the product, we compute

$$((g,h)(g',h'))(g'',h'') = (gg',hh')(g'',h'') = (gg'g'', hh'h'')$$

$$= (g,h)(g'g'', h'h'') = (g,h)((g',h')(g'',h'')),$$

The axiom of identity is really one of discovery. It is natural to guess that the identity in $G \times H$ is $(e,e)$, and this is easily checked as follows:

$$(g,h)(e,e) = (ge,he) = (g,h) = (eg,eh) = (e,e)(g,h).$$

□

The axiom of inverse is also one of discovery. The only natural guess for the inverse to $(g,h)$ is $(g^{-1}, h^{-1})$, and this is easily checked as follows:

$$(g,h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e,e) = (g^{-1}g, h^{-1}h) = (g^{-1}, h^{-1})(g,h).$$

The problem with the definition of direct product is that groups are hardly ever a direct product, because in order to be one, the group has to consist of ordered pairs. What is more important is whether a group has the structure of a direct product; i.e., that it is isomorphic to a direct product. The following theorem gives an easy way of testing whether a group is isomorphic to a direct product.

Theorem 1.3. Let $H$ and $K$ be subgroups of a group $G$ such that

1. $H \cap K = \{e\}$.
2. Both $H$ and $K$ are normal in $G$.
3. $HK = G$.

Then the map $H \times K \to G$ given by $(h, k) \mapsto hk$ is an isomorphism.

Moreover, if (1) and (3) hold, then (2) is equivalent to (2)', where

$$(2)' \quad hk = kh \text{ for all } h \in H, k \in K.$$ 

Furthermore, if (1) holds and $o(G) < \infty$, then (3) is equivalent to (3)', where

$$(3)' \quad o(H)o(K) = o(G).$$
Thus when $o$ of the theorem.

It follows that if $o(G) < \infty$, then if $HK = G$, $\phi$ is surjective, so is bijective, and $o(G) = o(H \times K) = o(H)o(K)$. Thus (3) implies (3)' if (1) holds. Conversely, if $o(G) < \infty$ and $o(G) = o(H)o(K)$, then $\phi$ is an injective map between two sets of the same finite cardinality, so $\phi$ must be a bijection, and thus $G = \phi(H \times K) = HK$. Thus when $o(G) < \infty$ and (1) holds, (3)' implies (3). This shows the last assertion of the theorem.

Next, if (1) holds and $H$ and $K$ are both normal in $G$ and $h \in H$, $k \in K$, we have

$$[h, k] = hh^{-1}k(hh^{-1})^{-1} \in K \quad \text{Since } K \triangleleft G$$

$$= h(kh^{-1}k^{-1}) \in H \quad \text{Since } H \triangleleft G$$

Now let us assume that (1), (2)' and (3) hold. Since (1) holds, $\phi$ is injective, and since (3) holds, $\phi$ is surjective. Thus we need only show it is a morphism. But

$$\phi(h, k)\phi(h', k') = hh'k' = \phi(hk, kk') = \phi((h, k)(h', k'))$$

which is what we needed to show. \hfill \Box

In the situation of the above theorem we say that $G$ is the internal direct product of $H$ and $K$ and by abuse of notation, we often denote $G = H \times K$ when $G$ is an internal direct product.

**Example 1.4.** In $\mathbb{Z}_6$, let $H = \langle 3 \rangle = \{3, 0\}$ and $K = \langle 2 \rangle = \{2, 4, 0\}$. Then $H \cap K = \{0\}$, and $o(H)o(K) = 2 \cdot 3 = o(\mathbb{Z}_6)$. Since every subgroup of an abelian group is automatically normal, we can apply the theorem to conclude that

$$\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3.$$

The direct product of two abelian groups, especially if the group operation is addition, is often called their direct sum. The direct sum of $H$ and $K$ is denoted as $H \oplus K$.

**Definition 1.5.** If $\{G_\alpha | \alpha \in \Lambda\}$ is a collection of groups indexed by some set $\Lambda$, then the direct product $\Pi_\alpha G_\alpha$ is the set of all sequences $\{g_\alpha | g_\alpha \in G_\alpha\}$, with product $\{g_\alpha\}\{g'_\alpha\} = \{g_\alpha g'_\alpha\}$.

2. **DIRECT PRODUCTS OF RINGS**

**Definition 2.1.** If $A$ and $B$ are rings then the direct product of $A$ and $B$, denoted $A \times B$, is the set $A \times B$ equipped with the addition and multiplication given by

$$(a, b) + (a', b') = (a + a', b + b')$$

$$(a, b) \cdot (a', b') = (aa', bb')$$

**Exercise 2.2.** Verify that the direct product of two rings is a ring under the addition and multiplication given above.

**Proposition 2.3.** Let $A$ and $B$ be rings. Then

1. $A \times B$ is unital iff both $A$ and $B$ are unital. In this case, the multiplicative identity in $A \times B$ is just $(1, 1)$.

   2. $A \times B$ is commutative iff both $A$ and $B$ are commutative.
Exercise 2.4. Prove the above proposition.

Theorem 2.5 (Fundamental Theorem of Direct Products of Rings). Let $R$ be a ring and $A$ and $B$ be subrings. Suppose that Let $H$ and $K$ be subgroups of a group $G$ such that

1. $A \cap B = \{0\}$.
2. Both $A$ and $B$ are ideals in $R$.
3. $A + B = R$.

Then the map $A \times B \to G$ given by $(a, b) \mapsto a + b$ is an isomorphism of rings. Moreover, if (1) and (3) hold, then (2) is equivalent to (2)', where

$$ab = ba = 0 \text{ for all } a \in A, b \in B.$$ 

Proof. First we show that if (1) holds, then condition (2) implies condition (2)'. To see this, suppose that $a \in A$ and $b \in B$. Then $ab \in A$, since $A$ is an ideal, and $ab \in B$, since $B$ is an ideal. Thus $ab \in A \cap B = \{0\}$, so condition (2)' holds.

Now suppose that (3) holds. We show that in this case, condition (2)' implies condition (2). For suppose that $a \in A$ and $x \in R$. By condition (3), $x = y + z$ where $y \in A$ and $z \in B$. Then $ax = ay + az = ay \in A$, since $az = 0$ and $A$ is a subalgebra. Similarly, $xa \in A$. Thus $A$ is an ideal. A similar argument shows that $B$ is an ideal.

This shows that if (1) and (3) hold, then condition (2) holds precisely when condition (2)' holds. As a consequence, to show the main statement, we can assume that conditions (1), (2)' and (3) hold. Define $\alpha : A \times B \to R$ by $\alpha(a, b) = a + b$. Since $R$ is a commutative group under addition, which means that $A$ and $B$ are normal subgroups under addition, $\alpha$ is an isomorphism of the additive group structures. In particular, $\alpha$ is both injective and surjective. Thus we only need to show that $\alpha$ behaves correctly with respect to the multiplication structure. However, we have

$$\alpha(a, b)\alpha(a', b') = (a + b)(a' + b') = aa' + ab' + ba' + bb' = aa' + bb' = \alpha(aa', bb').$$

This shows that $\alpha$ is an isomorphism of rings. \hfill \Box

3. Semidirect Products of Groups

If $\alpha : K \to \text{Aut}(H)$ is a morphism of $K$ to the automorphism group of a group $H$, then it is typical to denote the automorphism $\alpha(k)$ by $\alpha_k$.

Definition 3.1. Suppose that $\alpha : K \to \text{Aut}(H)$ is a morphism between the group $K$ and the automorphism group of the group $H$. Then the semidirect product of $H$ and $K$ determined by $\alpha$, denoted by $H \rtimes_\alpha K$, is the set $H \times K$ equipped with the binary operation

$$(h, k)(h', k') = (h\alpha_k(h'), kk').$$

When the map $\alpha$ is implicit, we usually write $H \rtimes K$ instead of $H \rtimes_\alpha K$.

Theorem 3.2. The semidirect product $H \rtimes_\alpha K$ is a group under the binary operation introduced above.
Proof. To see associativity holds, we compute

\[(h, k)(h', k')(h'', k'') = (h\alpha_k(h'), kk')(h'', k'') = (h\alpha_k(h')\alpha_k(h''), kk'k'')
= (h\alpha_k(h)\alpha_k(h'')kk'k'') = (h\alpha_k(h'\alpha_k(h''))kk'k'')
= (h, k)(h'\alpha_k(h''), k'k'') = (h, k)((h', k')(h'', k'')) \]

It is natural to guess that the identity is \((e, e)\), and we verify this by

\[\begin{align*}
(e, e)(h, k) &= (e\alpha_e(h), ek) = (\alpha_e(h), k) = (1_H(h), k) = (h, k) \\
(h, k)(e, e) &= (h\alpha_k(e), ke) = (he, k) = (h, k).
\end{align*}\]

Thus \(y = k^{-1}\) and \(\alpha_k(x) = h^{-1}\), so applying \(\alpha_{k^{-1}}\) to both sides, we obtain that \(x = \alpha_{k^{-1}}(h^{-1})\). Thus \((x, y) = (\alpha_{k^{-1}}(h^{-1}), k^{-1})\). We need to verify that \((x, y)(h, k) = (e, e)\). But

\[\begin{align*}
(x, y)(h, k) &= (\alpha_{k^{-1}}(h^{-1}), k^{-1})(h, k) = (\alpha_{k^{-1}}(h^{-1})\alpha_{k^{-1}}(h), k^{-1}k) \\
&= (\alpha_{k^{-1}}(h^{-1}h), e) = (\alpha_{k^{-1}}(e), e) = (e, e).
\end{align*}\]

\[\square\]

Note that a direct product is a special case of a semidirect product, where the map \(\alpha\) is the trivial morphism between \(K\) and \(\text{Aut}(K)\), because in that case we have

\[(h, k)(h', k') = (h\alpha_k(h'), kk') = (h1_H(h'), kk') = (hh', kk').\]

As is the case for direct products, it is uncommon for a group to actually consist of ordered pairs, so there is little chance that a group fits the description of a semidirect product. However, what is more important is when a group is isomorphic to a semidirect product. The following theorem characterizes when \(G\) is isomorphic to a semidirect product.

**Theorem 3.3.** Suppose that \(H\) and \(K\) are subgroups of \(G\) satisfying

1. \(H \cap K = \{e\}\).
2. \(H \trianglelefteq G\).
3. \(HK = G\).

Let \(\alpha : K \to \text{Aut}(H)\) be given by \(\alpha_k(h) = khk^{-1}\) be the automorphism of \(H\) given by the restriction of the conjugation operator to \(K\), acting on \(H\). Then the map \(H \rtimes_{\alpha} K \to G\) given by \((h, k) \mapsto hk\) is an isomorphism. If \(o(G) < \infty\), then we may replace condition (3) by the condition

\[\text{(3)' } o(G) = o(H)o(K)\]

Proof. The fact that (3) is equivalent to (3)' if (1) holds is proved in the same way it was for direct products. Let \(\phi : H \rtimes_{\alpha} K \to G\) be given by \(\phi(h, k) = hk\). Then

\[\phi((h, k)(h', k')) = \phi(hkh'k'^{-1}, kk') = hh'k^{-1}kk' = hh'k' = \phi(h, k)\phi(h', k').\]

Injectivity of \(\phi\) follows from (1) and surjectivity from (3). \[\square\]
Example 3.4. Suppose that \( n \geq 2 \). Let \( H = A_n \) be the alternating subgroup of the permutation group \( S_n \). We know that \( A_n \lhd S_n \) and that \( o(A_n) = n!/2 \). Let \( K = \langle (12) \rangle = \{ (12), e \} \cong \mathbb{Z}_2 \). Since \( o(H)o(K) = n! = o(S_n) \) and \( H \cap K = \{ e \} \), we see that \( S_n = A_n \rtimes \mathbb{Z}_2 \). Thus \( S_n \) is a semidirect product. Since \( A_n \) is simple for \( n \geq 5 \), this gives a decomposition of \( S_n \) as a semidirect product of two simple groups.

4. Modules over a ring

Definition 4.1. Let \( R \) be an associative ring and \( M \) be an abelian group. Then \( M \) is called a left module over \( R \) (or a left \( R \)-module) provided that there is a map \( R \times M \to M \), usually denoted by juxtaposition, that is, \( (r, m) \mapsto rm \), satisfying

1. \( (r + r')m = rm + r'm \).
2. \( r(m + m') = rm + rm' \).
3. \( (rr')m = r(r'm) \).

The first two properties are a kind of generalized distributive rule, and the last is a generalized associativity property. There is a similar notion of a right \( R \)-module structure.

Definition 4.2. Let \( R \) be an associative ring and \( M \) be an abelian group. Then \( M \) is called a right module over \( R \) (or a right \( R \)-module) provided that there is a map \( M \times R \to M \), usually denoted by juxtaposition, that is, \( (m, r) \mapsto mr \), satisfying

1. \( m(r + r') = mr + m'r \).
2. \( (m + m')r = mr + m'r \).
3. \( m(rr') = (mr)r' \).

At first it may seem that a left \( R \)-module can be turned into a right \( R \)-module by the rule \( mr = rm \), but one can check that the third condition for a module may not be satisfied if \( R \) is not commutative. On the other hand, if \( R \) is commutative, then left and right modules are interchangeable in this manner. In particular, a vector space is just a (left) module over a field.

Definition 4.3. A bimodule \( M \) over a ring \( R \) is a left and right \( R \)-module which satisfies the following compatibility condition:

\[ (rm)r' = r(mm') \].

Notice that the compatibility condition for a bimodule is another type of generalized associativity property.

Definition 4.4. If \( M \) is a ring, and a bimodule over \( R \), then \( M \) is said to be an \( R \)-algebra provided that the following compatibility conditions hold.

1. \( r(mm') = (rm)m' \).
2. \( (mm')r = m(mm') \).
3. \( m(am') = (ma)m' \).

Notice that again, these compatibility conditions are types of generalized associativity properties.

Definition 4.5. If \( M \) and \( R \) are rings, then an \( R \)-algebra structure on \( M \) determines a semidirect product of rings on \( M \times R \), denoted by \( M \rtimes R \), given by the additive group structure on \( M \times R \) given by the direct sum of the two additive group structures, and a product given by

\[ (m, r)(m', r') = (mm' + rm' + mr', rr') \].
Proposition 4.6. The multiplication and addition structures on \( M \times R \) equip it with the structure of an associative ring.

Exercise 4.7. Prove the above proposition.

Proposition 4.8. Let \( R \) be a subalgebra of a ring \( A \) and \( M \) be an ideal in \( A \). Then the multiplication in the ring equips \( M \) with the structure of an \( R \)-algebra.

Exercise 4.9. Prove the above proposition.

Theorem 4.10. Let \( A \) be a ring and \( M \) and \( R \) be subalgebras of \( A \) satisfying

1. \( M \cap R = \{0\} \).
2. \( M \) is an ideal in \( A \).
3. \( A = M + R \).

Then the map \( M \times R \to A \) given by \((m, r) \mapsto m + r \) is an isomorphism of rings, where the semidirect product structure on \( M \times R \) is determined by the \( R \)-algebra structure on \( M \) given by the multiplication in \( A \).

Proof. Let the map \( M \times R \to A \) be denoted by \( \alpha \), so \( \alpha(m, r) = m + r \). Now this map is an isomorphism of additive structures because \( A \) is the direct sum of \( M \) and \( R \) as an additive group. To see that \( \alpha \) is a morphism of rings, we need to check the multiplication. We have

\[
\alpha(m, r)\alpha(m', r') = (m + r)(m' + r') = mm' + rm' + mr' + rr'
\]

\[
= \alpha((m, r)(m', r')).
\]

This shows that \( \alpha \) is a morphism of rings. Since \( \alpha \) is an isomorphism of the underlying additive groups, it is bijective, so it is an isomorphism of rings. \( \square \)

5. Group Actions

Definition 5.1. Let \( G \) be a group and \( X \) be a nonempty set. Then \( G \) is said to act on \( X \) if there is a map \( G \times X \to X \), \((g, x) \mapsto gx\), satisfying

1. \((gh)x = g(hx)\).
2. \(e.x = x\).

A set \( X \) equipped with an action of the group \( G \) is called a \( G \)-set.

There are other notations for group actions. It is common to see \( g \star x \) instead of \( gx \). When there is no ambiguity, the notation \( gx \) instead of \( g.x \) is commonly used.

Example 5.2. If \( G \) is a group, there are two natural actions of \( G \) on itself. The first action is multiplication, given by \( g.x = gx \) for \( g, x \in G \). The second action is conjugation, given by \( g.x = g(xg)^{-1} \).

Exercise 5.3. Verify that multiplication and conjugation satisfy the axioms of a group action.

Proposition 5.4. If \( G \) acts on \( X \), then the map \( \alpha : G \to S_X \), given by \( \alpha_g(x) = gx \) is a morphism of \( G \) to the group \( S_X \) of permutations of \( X \). Conversely, if \( \alpha : G \to S_X \) is a morphism of groups, then the map \( G \times X \to X \), given by \( g.x = \alpha_g(x) \) is a group action.

Exercise 5.5. Prove the above proposition.
A group action, as we have defined it, is also called a left group action and thus a $G$-set may be called a left $G$-set. A right group action of $G$ on $X$ is defined similarly, as a map $X \times G \to X$, given by $(x, g) \mapsto x.g$, satisfying $x.(gh) = (x.g)h$ and $x.e = x$.

**Proposition 5.6.** A left action of $G$ on $X$ induces a right action by $x.g = g^{-1}.x$. Similarly, a right action determines a left action by $g.x = x.g^{-1}$.

**Exercise 5.7.** Prove the above proposition.

**Definition 5.8.** Suppose that $G$ and $H$ are groups and $G$ acts on $H$. Then $G$ is said to *act on* $H$ by automorphisms provided that

$$g.(hh') = (g.h)(g.h').$$

**Proposition 5.9.** If $G$ and $H$ are groups and $G$ acts on $H$ by automorphisms provided that the induced morphism $\alpha : G \to S_H$ given by

$$\alpha_g(h) = gh$$

has image in the normal subgroup $\text{Aut}(H)$ of $S_H$. In other words, an action of $G$ on $H$ by automorphisms is the same thing as a morphism $\alpha : G \to \text{Aut}(H)$.

**Exercise 5.10.** Prove the above proposition.

As a consequence of the proposition above, given any action of $G$ on $H$ by automorphisms, we can define a semidirect product structure $H \rtimes G$ by

$$(h, g)(h', g') = (h(g.h'), gg').$$

**Definition 5.11.** If $G$ acts on $X$ and $x \in X$, then the $G$-orbit of $x$ or just the orbit of $x$ is the set $O_x = \{g.x | g \in G\}$. This set is often denoted by $Gx$. If there is is only one orbit, then $G$ is said to act transitively on $X$.

The set $\text{Stab}_G(x) = \{g \in G | g.x = x\}$ is called the $G$-stabilizer of $x$, or just the stabilizer of $x$. This set is often denoted as $G_x$, or $\text{Stab}(x)$.

**Definition 5.12.** If $G$ acts on $X$, then a $G$-subset of $X$ is a (nonempty) subset $Y$ of $X$ such that $g.y \in Y$ for all $y \in Y$.

**Proposition 5.13.** If $Y$ is a $G$-subset of $X$, then the map $G \times Y \to Y$ given by $(g, y) \mapsto g.y$ is a $G$-action on $Y$.

**Proposition 5.14.** $Y$ is a $G$-subset of $X$ precisely when $Y$ is a (nonempty) union of orbits. In particular, if $G$ acts on $X$ and $x \in X$, then $G$ acts on $O_x$. This restricted action is transitive.

**Theorem 5.15** (Fundamental Theorem of Transitive Group Actions). Suppose that $G$ acts transitively on $X$ and $x \in X$. Then the map $G/\text{Stab}(x) \to X$ given by $g \mapsto g.x$ is a well defined bijection. Thus $|X| = |G : \text{Stab}(x)|$. If $G$ is finite, then $|X| = |G|/|\text{Stab}(x)|$.

**Proof.** To show the map is well defined, suppose that $g' \in \bar{g}$. Then $g' = gh$ where $h \in \text{Stab}(x)$. Thus $g'.x = (gh).x = g.(h.x) = g.x$. This shows the map $\bar{g} \to X$ is well defined. Let $y \in X$. Then $y = g.x$ for some $g \in G$, since the action is transitive, which shows the map is surjective. Finally, suppose that $\bar{a}$ and $\bar{b}$ have the same image. Then $a.x = b.x$, so

$$(b^{-1}a).x = b^{-1}(a.x) = b^{-1}(b.x) = (b^{-1}b).x = e.x = x.$$
This shows that \( b^{-1}a \in \text{Stab}(x) \), so \( a = b(b^{-1}a) \in \bar{b} \). This shows that the map is injective. The other statements follow from the fact that \( |G/\text{Stab}(x)| = [G : \text{Stab}(x)] = |G|/|\text{Stab}(x)| \), the latter equality holding when \( |G| < \infty \).

**Definition 5.16.** A finite group with order \( p^n \) for a prime \( p \) and positive integer \( n \) is called a \( p \)-group.

**Definition 5.17.** If \( G \) acts on \( X \), then denote the subset of \( X \) consisting of all points in \( X \) which are fixed by every element in \( G \) by \( X_0 \). This set is also often denoted as \( \text{Fix}(G) \).

**Proposition 5.18.** Let \( G \) be a finite \( p \)-group acting on a finite set \( X \). Then \( |X_0| = |X| \mod p \).

**Proof.** Let \( S \) be the set of orbits which are not singletons. Then \( X \) is a disjoint union of \( X_0 \) and the collection \( S \). If \( O_x \in S \), then \( |O_x| = |G : \text{Stab}(x)| \) is divisible by \( p \). Thus \( p \) divides the order of the union of the elements in \( S \). It follows that \( |X| = |X_0| \mod p \).

**Definition 5.19.** If \( G \) is a group and \( a \in G \), then the centralizer of \( a \) in \( G \), denoted by \( C_G(a) \) or \( C(a) \), is the set \( C(a) = \{ g \in G | gag^{-1} = a \} \). The center of \( G \), denoted by \( Z(G) \) is the set of elements of \( G \) which commute with every element in \( G \).

**Proposition 5.20.** If \( a \in G \), then \( C(a) \) is a subgroup of \( G \).

**Theorem 5.21** (Class Equation). Let \( G \) be a finite group. Let \( S \) be a set of representatives for the conjugacy classes of \( G \) which do not consist of a single element. Then

\[
G = |Z(G)| + \sum_{x \in S} [G : C(x)].
\]

**Corollary 5.22.** Let \( G \) be a finite \( p \)-group. Then the center of \( G \) is nontrivial.

**Corollary 5.23.** Let \( G \) be a group of order \( p^2 \). Then \( G \) is abelian.

**Proof.** Since \( Z(G) \) is nontrivial, either \( |Z(G)| = p \) or \( |Z(G)| = p^2 \). If the latter case holds, then \( G \) is abelian, so assume the former. Then \( |G/Z(G)| = p \), so \( G/Z(G) \) is isomorphic to \( \mathbb{Z}_p \). However, by a theorem from Abstract Algebra I, if \( G/Z(G) \) is cyclic, then \( G \) is abelian. This shows that it is impossible for \( Z(G) \) to have order \( p \).

**Proposition 5.24.** Let \( X \) be a set. Then the symmetric group \( S_n \) acts on \( X^n \) by

\[
s_{\sigma}(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).
\]

**Proof.** (Let \( \sigma, \tau \in S_n \), and \( x = (x_1, \ldots, x_n) \in X^n \). Let \( y = (y_1, \ldots, y_n) = \tau.x \), so that \( y_i = x_{\tau^{-1}(i)} \). Then \( \sigma.(\tau.x) = z \), where \( z_i = y_{\sigma^{-1}(i)} = x_{\tau^{-1}(\sigma^{-1}(i))} = x_{(\sigma\tau)^{-1}(i)} \). But this means that \( z = (\sigma\tau).x \), which shows that \( \sigma.(\tau.x) = (\sigma\tau).x \). Since it is immediate to see that \( e.x = x \), we see that \( S_n \) act on \( X^n \).

**Corollary 5.25.** Let \( X \) be a set. Then there is an action of \( \mathbb{Z}_n \) on \( X^n \) which is completely determined by the requirement that \( 1.x = (x_2, \ldots, x_n, x_1) \), where \( x = (x_1, \ldots, x_n) \).

**Proof.** Let \( \sigma = (n, n-1, \ldots, 1) \). Then \( \sigma \) is an \( n \)-cycle, so \( o(\sigma) = n \) and \( \langle \sigma \rangle \cong \mathbb{Z}_n \). We have \( \sigma^{-1} = (1, 2, \ldots, n) \), so \( \sigma.x = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) = (x_2, \ldots, x_n, x_1) \).
Theorem 5.26 (Cauchy’s Theorem). Let $G$ be a finite group and $p$ be a prime dividing the order of $G$. Then $G$ has an element of order $p$.

Proof. $\mathbb{Z}_p$ acts on $X = \{ x \in G^p \mid x_1 x_2 \cdots x_p = e \}$ by $1 \cdot (x_1, \cdots, x_p) = (x_2, \cdots, x_p, x_1)$. Now $x \in X_0$ precisely when $x_1 = x_2 = \cdots = x_p$. The map $G^{p-1} \to X$, given by $(x_1, \ldots, x_{p-1}) \mapsto (x_1, \ldots, x_{p-1}, x_p)$, where $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$, is bijective, so $|X| = 0 \mod p$. It follows that $|X_0| = 0 \mod p$. Now $(e, \ldots, e) \in X_0$, so there must be at least $p$ elements in $X_0$. Let $x$ be an element in $X_0$ which is not $(e, \ldots, e)$. Then $x^p = e$, and $x \neq e$, so $o(x) = p$. Thus $G$ has an element of order $p$. □

Proposition 5.27. Let $H \leq G$. Then $G$ acts on $G/H$ by

$$x \bar{g} = xg.$$

Proposition 5.28. Let $K, H \leq G$ and consider the restriction of the action of $G$ on $G/H$ to $K$. Then $\bar{g} \in \text{Fix}(K)$ iff $g^{-1}Kg \subseteq H$.

Proof. We have

$$\bar{g} \in \text{Fix}(K) \iff k\bar{g} = \bar{g} \text{ for all } k \in K$$

$$\iff k\bar{g} = \bar{g} \text{ for all } k \in K$$

$$\iff g^{-1}Kg = g^{-1}\bar{g} \text{ for all } k \in K$$

$$\iff g^{-1}Kg = \bar{e} \text{ for all } k \in K$$

$$\iff g^{-1}Kg \subseteq H \text{ for all } k \in K$$

$$\iff g^{-1}Kg \subseteq H$$

□

Proposition 5.29. Let $H \leq G$, and $\pi : G \to G/H$ be the projection $\pi(g) = \bar{g}$. If $K \leq G$, then $\pi^{-1}(\pi(K)) = KH$. In particular, if $H \leq K$, then $\pi(K) = K/H$ and $\pi^{-1}(K/H) = K$.

Proof. We have

$$g \in \pi^{-1}(\pi(K)) \iff \pi(g) \in \pi(K)$$

$$\iff \bar{g} = k \text{ for some } k \in K$$

$$\iff g = kh \text{ for some } k \in K$$

$$\iff g \in KH,$$

which shows the first statement. If $H \leq K$, then $KH = K$. Moreover, the definition of $K/H$ and $\pi(K)$ coincide. □

Definition 5.30. Let $H \leq G$. Then the normalizer of $H$ in $G$, denoted by $N_G(H)$, is the set

$$N_G(H) = \{ g \in G \mid c_g(H) = H \}.$$

A subgroup $H$ is called self normalizing if $H = N_G(H)$.

Proposition 5.31. Let $H$ be a $p$-subgroup of $G$ for some prime $p$. Then

Proof. Recall that the normalizer \( N_G(H) \) of \( H \) in \( G \) is the largest subgroup of \( G \) in which \( H \) is normal, so in particular, \( H \leq N_G(H) \). Next, we already know that \( G \) acts on the coset space \( G/H \) by

\[
a \cdot \bar{g} = \overline{ag}.
\]

We also know that the \( G \) action induces an action of \( H \) on \( X = G/H \), and since \( H \) is a \( p \)-group, it follows that \( |X| = |X_0| \), mod \( p \). Thus we need to identify \( X_0 = \text{Fix}(H) \). Now,

\[
\bar{g} \in \text{Fix} \, H \iff h \cdot \bar{g} = \bar{g} \quad \text{for all } h \in H
\]

\[
\iff \overline{hg} = \bar{g} \quad \text{for all } h \in H
\]

\[
\iff g^{-1} \overline{hg} = g^{-1} \cdot \bar{g} \quad \text{for all } h \in H
\]

\[
\iff \overline{g^{-1}hg} = g^{-1} \bar{g} \quad \text{for all } h \in H
\]

\[
\iff \overline{g^{-1}hg} = \bar{e} \quad \text{for all } h \in H
\]

\[
\iff g^{-1}hg \in H \quad \text{for all } h \in H
\]

\[
\iff g \in N_G(H)
\]

\[
\iff \bar{g} \in N_G(H)/H.
\]

As a consequence, we have \( |G/H| = |N_G(H)/H| \) mod \( p \), by the fundamental theorem on \( p \)-group actions. But \( [G : H] = |G/H| \) and \( |N_G(H)/H| = |N_G(H)/H| \), so it follows that

\[
|G : H| = |N_G(H) : H| \quad \text{mod } p.
\]

\[\square\]

**Theorem 5.32** (First Sylow Theorem). Suppose that \( p^{m+1} | o(G) \) and \( o(H) = p^m \). Then there is some \( K \leq G \) such that \( H \triangleleft K \) and \( o(K) = p^{m+1} \). In particular, if \( p^m \) is the largest power of \( p \) dividing \( o(G) \), then there is a subgroup of \( G \) with order \( p^m \).

Proof. Since \( o(G/H) \) is divisible by \( p \), so is \( o(N_G(H)/H) \). Since \( N_G(H)/H \) is a group whose order is divisible by \( p \), it has a subgroup \( K \) of order \( p \). Let \( K = \pi^{-1}(K) \), where \( \pi : N_G(H) \to N_G(H)/H \) is the projection. But then \( K \triangleleft H \), by Proposition (5.29), so \(|K| = |H|K| = p^mp = p^{m+1} \). By construction, \( K \leq N_G(H) \) and \( H \leq K \), so \( H \triangleleft K \). \[\square\]

**Definition 5.33.** If \( p^m \) is the largest power of \( p \) which divides \( o(G) \), then a subgroup of order \( p^m \) is called a \( p \)-Sylow subgroup or Sylow \( p \)-subgroup of \( G \).

**Theorem 5.34** (Second Sylow Theorem). The \( p \)-Sylow subgroups of \( G \) are all conjugate.

Proof. Let \( H, K \) be two \( p \)-Sylow subgroups of \( G \), and consider the action of \( K \) on \( G/H \) by \( kg = \overline{kg} \). Since \( p \) does not divide \( N_G(H)/H \), it follows that there must be some element \( \bar{g} \) which is fixed under this action. But then \( g^{-1}\overline{Kg} \subseteq H \). Since \( H \) and \( K \) have the same order, it follows that \( g^{-1}Kg = H \). Thus \( H \) and \( K \) are conjugate. \[\square\]

**Theorem 5.35** (Third Sylow Theorem). Let \( k \) be the number of \( p \)-Sylow subgroups of \( G \). Then \( k | o(G) \) and \( k = 1 \mod p \).
implies that \( H \) is normal in a subgroup of order \( p \). Instead, consider \( X \) under the action of \( G \) of \( X \), since conjugation of \( X \) leaves \( H \) fixed, we know that \( H \in X \). Suppose that \( K \in X \). Then conjugation of \( K \) by any element in \( H \) fixes \( K \), which implies that \( H \leq N_G(K) \). But then both \( H \) and \( K \) are subgroups of \( N_G(K) \), and they must be \( p \)-Sylow subgroups of \( N_G(K) \). Therefore \( H \) and \( K \) must be conjugate as subgroups of \( N_G(K) \). Since \( K \leq N_G(K) \), it is only conjugate to itself. This means that there is only one fixed element of this action, and so \( \text{Fix}(H) \) is trivial. Let us compute the number of \( 2 \)-Sylow and \( 3 \)-Sylow subgroups. Let \( k \) be the number of \( 3 \)-Sylow subgroups, so \( k|6 \), and thus \( k \) is either 1, 2, 3 or 6. We can eliminate the multiples of 3, leaving 1 and 2. Since \( 2 \neq 1 \mod 3 \), we must have \( k = 1 \). In particular, if \( H \) is a \( 3 \)-Sylow subgroup, it must be normal in \( G \). Note, we could have seen this by using the fact that \( |G:H| = 2 \).

Next, let \( k \) be the number of \( 2 \)-Sylow subgroups. Eliminating the multiples of 2, we have \( k \) is either 1, or 3. Since both 3 and 1 are equal to \( 1 \mod 2 \), we cannot determine which is correct. Let \( K \) be a \( 2 \)-Sylow subgroup of \( G \).

Since \( H \) is normal, and \( H \cap K \) can only consist of the identity, and \( 3 \cdot 2 = 6 \), we know that \( G = H \times K \). What are the possible actions of \( Z_2 \) on \( Z_3 \)? Well, \( \text{Aut}(Z_3) = Z_2 \), so there are exactly 2 morphisms from \( Z_2 \) to \( \text{Aut}(Z_3) \), the trivial morphism, and the identity morphism.

The trivial morphism always determines the direct product structure on \( H \times K \), which is \( Z_3 \times Z_2 = Z_6 \). In this case, there is exactly one subgroup of order 2.

The identity morphism determines the group structure \( D_3 \). In this case there are 3 subgroups of order 2. Thus both possibilities given by the Sylow theorems do occur!

Example 6.2. Let \( G \) be a group of order 4. By Cauchy's Theorem, it has a subgroup \( H \) of order 2. Now, if \( G \) has an element of order 4, it is isomorphic to \( Z_4 \), so assume otherwise. Then there must be an element not in \( H \) of order 2. Let \( K \) be the subgroup generated by this element. One can use the index to show that \( H \) and \( K \) are normal, or one can use the Sylow theorem, which says that \( H \) must be normal in a subgroup of order \( 2^2 \) and similarly for \( K \). Now, \( H \cap K = \{e\} \), so we must have \( G = H \times K \), because both \( H \) and \( K \) are normal, and \( o(H) = o(K) = o(G) \). Thus \( G \cong Z_2 \times Z_2 \).

Theorem 6.3. Let \( H, K \leq G \). Then

\[
|HK| = \frac{|H| |K|}{|H \cap K|}.
\]
As a consequence, \[ |H \cap K| \geq \frac{|H| |K|}{|G|}. \]

**Proof.** Let \( H \times K \) act on \( HK \) by \((h,k) \cdot x = h x k^{-1}\). To check that this is a group action, note that

\[
(h_1, k_1) \ast (h_2, k_2) \ast x = h_1 (h_2 x k_2^{-1} k_1) = (h_1 h_2) x (k_1 k_2)^{-1} = (h_1 h_2, k_1 k_2) \ast x = ((h_1, k_1) (h_2, k_2)) \ast x.
\]

\[(e,e) \ast x = exe^{-1} = x.\]

Note that \( e = ee \in HK \), and \((h, k^{-1}) \ast e = hk\), so the action is transitive. Moreover

\[
\text{Stab}(e) = \{(h, k) \in H \times K | hk^{-1} = e\}
= \{(h, h) | h \in H \cap K\},
\]

So \(|\text{Stab}(e)| = |H \cap K|\). By the fundamental theorem of group actions, we obtain that \(|HK| = \frac{|H \times K|}{|\text{Stab}(e)|} = \frac{|H| |K|}{|H \cap K|}\). Now use the fact that \(|HK| \leq |G|\) and rearrange the inequality \(|G| \geq \frac{|H| |K|}{|H \cap K|}\) to obtain the second statement!  

**Example 6.4.** Let \( G \) be a group of order 8. If \( G \) has an element of order 8, then it is isomorphic to \( \mathbb{Z}_8 \), so assume otherwise. We know that \( G \) has an element of order 2, and thus a subgroup of order 2, which is normal in a subgroup of order 4. In particular, \( G \) has a subgroup \( H \) of order 4, which is normal in \( G \), either by the index theorem or the Sylow theory.

If every element of \( G \) has order 2, then \( G \) must be abelian. In this case, we must have \( H \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \), and there is an element not in \( H \), which must give a normal subgroup \( K \) of order 2, Thus \( G = H \times K = \mathbb{Z}_2 \times \mathbb{Z}_2 \).

As a consequence, we can assume that \( G \) has an element of order 4, which generates a subgroup \( H \) of order 4, which is normal in \( G \). If there is an element of order 2 which is not in \( H \), let \( K \) be the subgroup it generates. We have \( H \cap K = \{e\} \), and \( H \) is normal in \( G \), so \( G = H \times K \). Now \( \text{Aut}(H) = \mathbb{Z}_4 \cong \{1, 3\} \cong \mathbb{Z}_2 \). Thus there are precisely two morphisms from \( K \) to \( \text{Aut}(H) \), the trivial morphism and the identity morphism. For the trivial morphism, the group is \( H \times K = \mathbb{Z}_4 \times \mathbb{Z}_2 \), and for the identity morphism, we obtain the group \( D_4 \).

Finally, suppose that \( H \cong \mathbb{Z}_4 \), and there is no element of order 2 not in \( H \). Then there must be some element of order 4 not in \( H \) and it generates a subgroup \( K \). By the theorem above, we know that \(|H \cap K| \geq \frac{4 \times 4}{8} = 2\), so we must have \( |H \cap K| = 2\). Since \( H \) is normal in \( G \), we can form the semidirect product \( H \times K \) with product \((h,k)(h',k') = (hh'k^{-1}, kk')\), and the map \( \phi(h,k) = hk \) is a morphism from \( H \times K \to G \), whose image is \( HK \). By the theorem, \( o(HK) = \frac{|H| |K|}{|H \cap K|} = 8 \), so this morphism is surjective. Moreover, the kernel of this map is \( \ker(\phi) = \{(h, h^{-1}) | h \in H \cap K\} \). Moreover \( \ker(\phi) \leq \mathbb{Z}(H \times K) \). To see this, note that

\[
(h, h^{-1})(h', k) = (hh^{-1}h'k, h^{-1}k) = (h'h, h^{-1}k) = (h'h, khk^{-1}) = (h', k)(h, h^{-1}).
\]

In any semidirect product \( H \times K \), where \( H \cong K \cong \mathbb{Z}_4 \), note that since \( \text{Aut}(H) \cong \mathbb{Z}_2 \), there are precisely two morphisms \( K \to \text{Aut}(H) \). The trivial morphism determines the direct product \( \mathbb{Z}_4 \times \mathbb{Z}_4 \), and the subgroup \( \ker(\phi) \) corresponds to the subgroup \( \langle (2,2) \rangle \). The resulting quotient group has two elements of order 2. In the
The quotient group $Z_4 \times Z_4/(\langle 2, 2 \rangle)$, the elements $\langle 2, 0 \rangle$ and $\langle 1, 1 \rangle$ are distinct elements of order 2. Therefore, if the group $G$ has only one element of order 2, it must be determined by the nontrivial morphism $Z_4 \to \text{Aut}(Z_4)$.

Let $H = \langle \rho \rangle$ and $K = \langle \sigma \rangle$. Then the nontrivial morphism determines the action given by $\sigma \cdot \rho = \rho^3$, or if we identify $\rho$ and $\sigma$ with their images in $H \times K$, we have the commutation relation $\sigma \rho = \rho^3 \sigma$, which gives a generators and relations description $H \times K = \langle \rho, \sigma | \rho^4 = e, \sigma \rho = \rho \sigma \rangle$. The element $\rho^2 \sigma^2$ has order two and lies in the center of $H \times K$, and $G = H \times K/\langle \rho^2 \sigma^2 \rangle$. Then the group $G$ is isomorphic to the octonion group $O_8 = \{ 1, -1, i, -i, j, -j, k, -k \}$, which is the group of invertible integer quaternions, under the bijection given by

$$\bar{e} \mapsto 1, \quad \rho^2 \mapsto -1, \quad \bar{\rho} \mapsto i, \quad \bar{\sigma} \mapsto j, \quad \bar{\rho} \bar{\sigma} \mapsto k$$

Definition 6.5. Let $X$ be a $G$-set. Then the kernel $K$ of the action is the set $\{ k \in G | k.x = x \text{ for all } x \in X \}$. The action of $G$ on $X$ is called faithful if the kernel is trivial.

Proposition 6.6. The kernel $K$ of a group action of $G$ on $X$ is a normal subgroup of $G$. Moreover, $G/H$ acts faithfully on $X$ by $\bar{g}.x = g.x$.

Proof. Let $K$ be the kernel of an action of $G$ on $X$. Recall that an action of $G$ on $X$ is essentially the same thing as a morphism $G \to S_X$. Under this identification, $K$ is the kernel of this morphism, so it is a normal subgroup of $G$. Now define the action of $G/H$ by $\bar{g}.x = g.x$. To show this action is well defined, suppose that $g_1 \in \bar{g}$. Then $g_1 = gk$ for some $k \in K$. Then $g_1.x = (gk).x = g.(k.x) = g.x$, since $k.x = x$ for all $x \in X$. Thus the action is well defined. To show it is a group action, note that

$$(g_1 g_2).x = (\bar{g_1} \bar{g_2}).x = (g_1 g_2).x = g_1. (g_2.x) = \bar{g}_1. (\bar{g}_2.x).$$

\[ \square \]

7. Automorphism Group of $Z_p^n$

First, note that an element of $Z_p^n$ can be expressed in the form

$$(a_1, \ldots, a_n) = a_1 e_1 + \cdots + a_n e_n,$$

where $e_1 = (1,0, \cdots, 0)$, etc., so that the $e_i$ appear to be a basis of $Z_p^n$. This is not precisely true because the coefficients $a_i$ are taken from $Z$, which, by the way, means that $Z_p^n$ is a module over the integers.

Now is where we use the fact that in $Z_p$, we have for an integer $a$ and an element $x$ in $Z_p$, that $ax = \bar{a}x$, where $\bar{a} \in Z_p$, which is a field. This means that

$$(a_1, \ldots, a_n) = (\bar{a}_1, \ldots, \bar{a}_n),$$

which expresses $Z_p^n$ as a vector space over $Z_p$.

Now, an automorphism of $Z_p^n$ is a map $\lambda : Z_p^n \to Z_p^n$ of the form

$$\lambda e_j = \sum_{k=0}^n a_{ij} e_k, \quad \sum_{k=0}^n a_{ij} e_k.$$ 

But this means that $\lambda$ is a linear map over the field $Z_p$. Of course, the condition that $\lambda$ is a bijection is just that $\lambda$ is an invertible linear map.
Next, using Theorem 6.9 of the notes, which we have not discussed, if \( \theta \) is any automorphism of \( H \) and \( \alpha \) is a morphism from \( K \) to \( \text{Aut}(H) \), then the map \( \alpha' \), given by \( \alpha'(k) = \theta \circ \alpha_k \circ \theta^{-1} \), determines a semidirect product structure on \( H \times K \) which is isomorphic to the semidirect product structure given by \( \alpha \). What this means for our case of \( \text{Aut}(Z_p^n) \) is that two matrices which are conjugate determine the same semidirect product (up to isomorphism).

The last important step is to count the number of elements in \( \mathbb{GL}(n, \mathbb{Z}_p) \). Well, the first column can have \( p^n \) possible coefficients in the \( n \) rows, since each matrix element can be one of \( p \) numbers. We subtract 1 because the only vector not allowed in the first column is the zero vector. For the second column, we have to exclude the entire subspace spanned by the vector in the first column, which has \( p \) elements, so we have \( p^n - p \) allowable coefficients in the second column. For the third column, we have to exclude a two dimensional subspace, which has \( p^2 \) elements. Continuing on, the last column can contain \( p^n - p^{n-1} \) elements, so finally, we obtain

\[
o(\mathbb{GL}(n, \mathbb{Z}_p)) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).
\]

Notice that this number is divisible by \( p-1 \) and \( p^{n-1} \), which is interesting.

Of course, because we only care about the conjugacy classes, the number doesn’t tell us how many semidirect products we can obtain.

**Theorem 7.1.** Suppose that \( \alpha : K \to \text{Aut}(H) \) is a morphism, and \( \theta \in \text{Aut}(K) \). Let \( \alpha' = \alpha \circ \theta \). Then the map \( H \ltimes_{\alpha'} K \to H \ltimes_{\alpha} K \), given by \( (h,k) \mapsto (h,\theta(k)) \) is an isomorphism.

**Proof.** Denote the map \( H \ltimes_{\alpha'} K \to H \ltimes_{\alpha} K \) by \( \phi \). We compute

\[
\phi((h,k)(h',k')) = \phi(h\alpha'_k(h'),kk') = (h\alpha_k(h'),\theta(kk')) = (h\alpha_k(h'),\theta(k)\theta(k')(h,\theta(k))(h,\theta(k'))(h,\theta(k')) = \phi(h,k)\phi(h',k').
\]

It is easy to see that \( \phi \) is a bijection, so it is an isomorphism. \( \square \)

The theorem above says that if two morphisms \( K \to \text{Aut}(H) \) differ by an automorphism of \( K \), then they induce isomorphic semidirect products.

**Theorem 7.2.** Suppose that \( \alpha : K \to \text{Aut}(H) \) is a morphism, and \( \theta \in \text{Aut}(H) \). Define \( \alpha' \) by \( \alpha'_k = \theta \circ \alpha_k \circ \theta^{-1} \). Then the map \( H \ltimes_{\alpha} K \to H \ltimes_{\alpha'} K \), given by \( (h,k) \mapsto (\theta(h),k) \) is an isomorphism.

**Proof.** Denote the map \( H \ltimes_{\alpha} K \to H \ltimes_{\alpha'} K \) by \( \phi \). Then

\[
\phi((h,k)(h',k')) = \phi(h\alpha_k(h'),kk') = (\theta(h\alpha_k(h')),kk') = (\theta(h)\theta(\alpha_k(h'))(h',k')(h,\theta(k))(h,\theta(k'))(h,\theta(k')) = \phi(h,k)\phi(h',k').
\]

Since \( \phi \) is clearly bijective, it is an isomorphism. \( \square \)

**Example 7.3.** Let \( G \) be a group of order 12. Then the number of 3 Sylow subgroups is either 4 or 1, and the number of 2-Sylow subgroups is either 3 or 1. Therefore, we don’t immediately know if any of the Sylow subgroups is normal in \( G \).

On the other hand, suppose that there really are 4 3-Sylow subgroups. These subgroups could not have any element in common except the identity, so they would account for 8 distinct elements of order 3 in \( G \). On the other hand, if there are 3
2-Sylow subgroups. If $H$ and $K$ are distinct 2-Sylow subgroups, then $o(H \cap K) \geq 4 \cdot 4/12 > 1$, so the intersection must consist of 2 elements, since they are distinct. Thus $H \cup K$ must consist of 6 elements. Since we cannot have 14 elements in $G$, it follows that either the 3-Sylow or the 2-Sylow subgroup must be normal in $G$.

Since the 2-Sylow subgroups are conjugate, they must either all be isomorphic to $\mathbb{Z}_4$ or all be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

7.1. Case 1. Let us suppose that the 3-Sylow subgroup $H = \langle \rho \rangle$ is normal in $G$ and that $K = \langle \sigma \rangle$ is a 2-Sylow subgroup isomorphic to $\mathbb{Z}_2$. We are looking for a morphism $\alpha : \mathbb{Z}_4 \to \text{Aut}(\mathbb{Z}_3) = \mathbb{Z}_2$. There is only one nontrivial such automorphism, and it satisfies $\alpha_\sigma(\rho) = \rho^{-1} = \rho^2$. But in the group, this means that

$$\alpha_\sigma(\rho) = \sigma \rho \sigma^{-1} = \rho^2,$$

which yields the commutation relation

$$\sigma \rho = \rho^2 \sigma.$$

This gives a group given by generators and relations

$$G = \langle \rho, \sigma \rangle | \rho^4 = \sigma^4 = e, \sigma \rho = \rho^2 \sigma \rangle.$$

What this means is that to generate such a group, instead of just looking at automorphisms, we write a conjugation relation. Now it is easy to see in this group that every element is uniquely of the form $\rho^m \sigma^n$, where $0 \leq m \leq 2$ and $0 \leq n \leq 4$, which accounts for 12 elements. That is because if the element is written in some other order, we can use the commutation relation (7.1) to move a $\sigma$ to the right of a $\rho$, and we can keep doing this until the element is expressed in the standard order above.

Now let us try to count the orders of all the elements. $e$ has order 1, and $\rho$ and $\rho^2$ have order 3. The elements $\sigma$ and $\sigma^3$ have order 4, but $\sigma^2$ has order 2. Now let us compute orders of composite elements.

$$\langle \rho \sigma \rangle^2 = \rho \sigma \rho \sigma = \rho^2 \sigma \rho \sigma = \rho^2\sigma^2 = \sigma^2$$

$$\langle \rho \sigma \rangle^3 = \rho \sigma \rho \sigma^2 = \rho \sigma^3$$

$$\langle \rho \sigma \rangle^4 = \sigma^2 \rho \sigma^2 = e.$$

Thus $\rho \sigma$ has order 4. You can keep doing this for each element to find all the orders.

7.2. Case 2. Here we still have $H = \langle \rho \rangle$ and $K = \langle a, b \rangle | a^2 = b^2 = e, ab = ba \rangle$ is a 2-Sylow subgroup of order 4. The nontrivial automorphism $\lambda$ of $H$ is given by $\lambda(\rho) = \rho^2$. There are three nontrivial morphisms of $K$ to $\text{Aut}(H)$. One of them is given by $\alpha_a = \lambda$, $\alpha_b = \lambda$, which means that $\alpha_{ab} = 1_H$. This just means that $a \rho = \rho^2 a$ and $b \rho = \rho^2 b$. These two commutation relations determine the group $G$ completely, which is given in terms of generators and relations by

$$G = \langle \rho, a, b \rangle | \rho^3 = a^2 = b^2 = e, ab = ba, a \rho = \rho^2 a, b \rho = \rho^2 b \rangle.$$

Let us compute the order of some of the elements of $G$. Note that any element in $G$ is of the form $\rho^k$, $\rho^k a$, $\rho^k b$ or $\rho^k ab$ where $k \in \{0, 1, 2\}$. This gives 4 elements that can occur on the right (in the case of $\rho^k$, that element is $e$), and three elements that can occur on the left, for a total of 12 elements. Let us determine the order of $\rho a$. We have $(\rho a)^2 = \rho a \rho a = \rho \rho^2 a^2 = e$, and similarly the order of $\rho b$ is 2. In
addition, $\rho^2 a$ and $\rho^2 b$ also have order 2. Now let us compute the order of $pab$. We have

$$(pab)^2 = pabpab = \rho^2 abab = \rho^2$$

$$(pab)^3 = \rho^2 pab = ab.$$  

Since it follows from the first and second lines that $(pab)^6 = e$, and the order of $pab$ is neither 1, 2, or 3, it must have order 6, since it divides the order of the group. Similarly, the order of $\rho^2 ab$ must be 6. Thus we have accounted for 7 elements of order 2, $a, b, ab, \rho a \rho b, \rho^2 a$ and $\rho^2 b$, 2 elements of order 3, $\rho$ and $\rho^2$, two elements of order 6, $pab$ and $\rho^2 ab$, and finally one element of order 1, $e$. This gives the orders of all the elements in $G$.

There are two other nontrivial morphisms of $K$ into $\text{Aut}(H)$. One is given by $\alpha_a = \lambda$, $\alpha_b = 1_H$, and the last one is given by $\alpha_a = 1_H$ and $\alpha_b = \lambda$. Both of these maps differ from the one we used by an automorphism of $K$, and therefore, by Theorem 6.8 in the notes, they determine isomorphic semidirect products.

7.3. Case 3: The subgroup $H$, isomorphic to $\mathbb{Z}_4$, is normal in $G$. Let $H = \langle \rho \rangle$ and $K = \langle \sigma \rangle$ be a 3-Sylow subgroup. Since $\text{Aut}(\mathbb{Z}_4) = \mathbb{Z}_2$ and $K = \mathbb{Z}_3$, there is only the trivial morphism from $K$ to $\text{Aut}(H)$, and therefore the group $G = \mathbb{Z}_4 \times \mathbb{Z}_3$.

7.4. Case 4: The subgroup $H$, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ is normal in $G$. We can express $H = \langle a, b | a^2 = b^2 = e, ab = ba \rangle$. and a 3-Sylow subgroup $K = \langle \sigma \rangle$, with $\sigma^3 = e$. To translate the elements $a$, $b$, $ab$ and $e$ into ordered pairs for the matrix representation of $\text{Aut}(H)$, we can set $a = (1, 0)$ and $b = (0, 1)$, so that $ab = (1, 1)$ and $e = (0, 0)$. The matrix group $\text{GL}(2, \mathbb{Z}_2)$ has 6 = $3 \cdot 2$ elements, and since it is not abelian, it is isomorphic to $D_3 = S_3$. Let us find a matrix of order 3, to represent $\alpha_\sigma$. The matrix $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ has order 3 in $\text{GL}(2, \mathbb{Z}_2)$. It corresponds to the automorphism $\lambda$ given by $\lambda(a) = b$ and $\lambda(b) = ab$. To see this, note that the first column of the matrix represents $\lambda(a)$ and the second one represents $\lambda(b)$.

This means that if we set $\alpha_\sigma = \lambda$, then we obtain the commutation relations

$$\sigma a = ba$$

$$\sigma b = ab\sigma.$$  

This gives a group $G$ given by generators and relations

$$G = \langle a, b, \sigma | a^2 = b^2 = \sigma^3 = e, ab = ba, \sigma a = ba, \sigma b = ab\sigma \rangle.$$  

Let us compute the order of some elements.

$$(a\sigma)^2 = a\sigma a\sigma = ab\sigma^2$$

$$(a\sigma)^3 = a\sigma ab\sigma^2 = abab\sigma^2 = e.$$  

Let us stop here and remember that in the case we are studying, the 3-Sylow subgroups are not normal (since our group is not a direct product), so by the third Sylow theorem, there must be 4 of them. Each of them accounts for 2 elements of order 3, and none of these elements are shared by another 3-Sylow subgroup, so there are 8 elements of order 3. The 2-Sylow subgroup accounts for 3 elements of order 2, and one of order 1, so we have accounted for all the elements.
Finally, we can account for which group this is isomorphic to. The group $A_4$ has 12 elements, of the form $(12)(34), (13)(24), (14)(23)$ and, giving a 2-Sylow subgroup, and finally elements of the form $(1, 2, 3, 4)$ and others which are all of order 3. But that’s exactly what our group looks like!

Let $p$ and $q$ be primes, and suppose that $q < p$. Suppose that $G$ is a group of order $pq$. Let $H$ be a $p$-Sylow subgroup and $K$ be a $q$-Sylow subgroup. By the third Sylow theorem, $H$ must be normal in $G$, so $G = H \times K$. If $q \not | (p - 1)$ then $K$ is also normal in $G$, so $G = H \times K$, by a theorem decomposing a group as direct product of subgroups. Thus, we obtain only one possible group structure $\mathbb{Z}_p \times \mathbb{Z}_q = \mathbb{Z}_{pq}$.

Now, consider the case that $q | (p - 1)$. Now $\text{Aut}(H) = \text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^\times = \mathbb{Z}_{p-1}$, and therefore, there is a unique subgroup $M$ of order $q$ in $\text{Aut}(H)$, and this subgroup consists of all elements in $\text{Aut}(H)$ whose order divides $q$. Let $K = \langle \sigma \rangle$, and suppose that $K$ is written multiplicatively, so that $K = \{ \sigma^m | 1 \leq m \leq q \}$.

For each element $x \in M$, there is a morphism $\alpha^x : K \rightarrow \text{Aut}(H)$, which is uniquely determined by the condition $\alpha^x_\sigma = x$, and every morphism $\alpha : K \rightarrow \text{Aut}(K)$ must be of this form. Therefore there are exactly $q$ such morphisms.

Now, let us study these morphisms. First, there is the trivial morphism $\alpha^1$, which maps $\sigma$ to the identity of $\text{Aut}(H)$. In this case, the semidirect product is just the direct product, which gives the group $\mathbb{Z}_{pq}$.

The other $q - 1$ elements of the subgroup $M$ of $\text{Aut}(H)$ are all generators of the subgroup $M$. Moreover, if we choose $x$ to be one of these elements, then every element in $M$ is of the form $x^m$ for some $1 \leq m \leq q$, and we have $\alpha^x_\sigma = x^m$. Moreover, if $1 \leq m < q$, then the map $\theta^m : K \rightarrow K$, given by $\theta^m(\sigma) = \sigma^m$, is an isomorphism, so is an automorphism of $K$. We compute that $\alpha^{x^m}_\sigma = \alpha^x_\sigma^m = x^m$.

Therefore if $y = x^m$, we have $\alpha^y = \alpha^x \circ \theta^m$, which means that the semidirect products determined by $\alpha^x$ and $\alpha^y$ are isomorphic.

Finally, we want to give a presentation of $G$ in terms of generators and relations. Express $H = \langle \rho \rangle$, written multiplicatively, so $H = \{ \rho^m | 1 \leq m \leq p \}$. Now, the automorphism $x$ is of the form $x(\rho) = \rho^k$ for some $k$, and since $x^q$ is the identity, we have $\rho = x^q(\rho) = (x(\rho))^q = \rho^k$. Therefore $k^q = 1 \pmod{p}$. There are exactly $q$ solutions to this equation (mod $p$), and if we choose any solution $k$ except $k = 1$, we can express all $q$ of the solutions as powers of $k$. If we denote the elements $(\rho^i, \sigma^j)$ in $H \times K$ as $\rho^i \sigma^j$, then we have

$$\sigma \rho = (e, \sigma)(\rho, e) = (\alpha_\sigma^x(\rho), \sigma e) = (\rho^k, \sigma) = \rho^k \sigma.$$

Thus we can express $G$ in terms of generators and relations as $G = \langle \rho, \sigma | \rho^p = \sigma^q = e, \sigma \rho = \rho^k \sigma \rangle$.

We summarize the results in the following theorem.

**Theorem 7.4.** Let $G$ be a group of order $pq$, where $p$ and $q$ are primes with $q < p$. Then $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Moreover, if $q \not | (p - 1)$, then $G \cong \mathbb{Z}_{pq}$. If $q | (p - 1)$, then there is some $1 < k < p - 1$ such that $k^q = 1 \pmod{p}$, and if we choose any such $k$, then $G$ is isomorphic to the group given in terms of generators and relations by $G = \langle \rho, \sigma | \rho^p = \sigma^q = e, \sigma \rho = \rho^k \sigma \rangle$.

**Example 7.5.** Let $G$ be a group of order 21. Since $21 = 7 \cdot 3$ and $3 | (7 - 1)$, there are exactly two such groups, up to isomorphism. The first possibility is $G \cong \mathbb{Z}_{21}$. Let us study the other possibility. First, we need to find a $k \neq 1$ such that $k^3 = 1$.
(mod 7). Evidently, \( k = 2 \) works, but we could also have chosen \( k = 2^2 = 4 \). This means that we have a group \( G \) given by

\[
G = \langle \rho, \sigma | \rho^7 = \sigma^3 = e, \sigma \rho = \rho^2 \sigma \rangle.
\]