Direct Products of Groups:

Definition: The **external direct product** is defined to be the following: Let $H_1, \ldots, H_n$ be groups.

$$H_1 \times H_2 \times \cdots \times H_n := \{(h_1, \ldots, h_n) \mid h_i \in H_i\}$$

and the group operation is the componentwise operation in the respective group.

For each $i$, let $H'_i = \{(1, \ldots, h_i, \ldots, 1) \mid h_i \in H_i\}$. Then the following hold (exercise):

1. Each $H_i$ is a subgroup of $G$.
2. $H_i \cong H'_i$.
3. $H'_i \lhd G$.
4. $G = H'_1 \cdots H'_n$.
5. $H'_i \cap H'_1 \cdots \hat{H}'_i \cdots H'_n = \{1\}$

Thus, the group $G$ is 'built' out of the normal subgroups $H'_1, \ldots, H'_n$ in a special way.

Definition: Let $G$ be a group and $H_1, \ldots, H_n$ subgroups of $G$. We say that $G$ is an **internal direct product** of $H_1, \ldots, H_n$ if the following hold:

1. $H_i \lhd G$.
2. $G = H_1 \cdots H_n$.
3. $H_i \cap H_1 \cdots \hat{H}_i \cdots H_n = \{1\}$

In this case, we write $G = H_1 \times H_2 \times \cdots \times H_n$. Note that we use the same notation for both internal and external direct products. This is justified by the previous exercise and the following:

Exercise: If $G$ is the internal direct product of $H_1, \ldots, H_n$ then $G$ is isomorphic to the external direct product of $H_1, \ldots, H_n$.

Proposition: Let $G$ be a finite abelian group. Then $G$ is the direct product of its sylow subgroups.

Proof: Suppose that $|G| = p_1^{n_1} \cdots p_k^{n_k}$, $p_i$ distinct primes. Let $P_i$ be a sylow $p_i$-subgroup. Then $P_i \lhd G, G = P_1 \cdots P_k$, and $P_i \cap P_1 \cdots \hat{P}_i \cdots P_k$, and therefore $G = P_1 \times P_2 \times \cdots \times P_k$, where $P_i$ is an abelian group of order $p_i^{n_i}$.

Question: What do abelian groups of order $p^n$ look like? From the structure theorem for finitely generated abelian groups, if $P$ is abelian and $|P| = p^n$, then there exists **unique** integers $n_1 \geq n_2 \geq \cdots \geq n_k$ such that

$$P \cong C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \cdots \times C_{p_k^{n_k}}$$
where $C_m$ is a cyclic group of order $m$.

**Example:** How many non-isomorphic abelian groups are there of order $2^5$?

1. $C_{32}$
2. $C_{16} \times C_2$
3. $C_8 \times C_4$
4. $C_8 \times C_2 \times C_2$
5. $C_4 \times C_4 \times C_2$
6. $C_4 \times C_2 \times C_2 \times C_2$
7. $C_2 \times C_2 \times C_2 \times C_2 \times C_2$

**Example:** How many non-isomorphic abelian groups of order $2^5 \cdot 3^2 \cdot 5^3$ are there? There are 7 possibilities of the sylow 2-subgroup, 2 possibilities of the sylow 3-subgroup, and 3 possibilities for the sylow 5-subgroup. Therefore there are 42 “isomorphism classes” of abelian groups of order $2^5 \cdot 3^2 \cdot 5^3$.

**Example:** Let $|G| = 3 \cdot 5 \cdot 7$. Then $G = C_5 \times H$ where $|H| = 21$.

**Proof:** We’ve already proved that the Sylow 5-subgroup and Sylow 7-subgroup of $G$ is normal. Let $P \in \text{Syl}_5(G), Q \in \text{Syl}_7(G), R \in \text{Syl}_7(G)$. So, $Q \triangleleft G$, and $R \triangleleft G$.

Let $H = P \cdot R$. Since $|G/R| = 15$, and $3 \nmid 5 - 1$, we know $G/R$ is cyclic. Hence, $H/R \triangleleft H \triangleleft G$. Since $G = PQR = QH\cdot Q \cap H = \{1\}$ and both $Q$ and $H$ are normal, we see that $G = Q \times H$.

We’ll see later that there are only two non-isomorphic groups of order 21 (one abelian and one non-abelian), therefore there are only two non-isomorphic groups of order 105.

**Automorphism Groups**

**Definition:** Let $G$ be a group. The **automorphism group** of $G$ is defined by:

$$\text{Aut}(G) := \{ \phi \mid \phi : G \to G \text{ is an isomorphism} \}$$

This is easily seen to be a group under the operation of composition.

The most easily understood automorphisms are those given by conjugation by an element:

**Definition:** Let $g \in G$, and define $\psi_g : G \to G$ which maps $x \in G$ to $gxg^{-1}$. Then $\psi_g$ is a group homomorphism, with additional properties:

$$(\psi_g)^{-1} = \psi_{g^{-1}}, \psi_g \circ \psi_h = \psi_{gh}$$

$\psi_g$ is called an **inner automorphism** of $G$.

The set of inner automorphisms:

$$\text{Inn}(G) := \{ \psi_g | g \in G \}$$
is a subgroup of $\text{Aut}(G)$, and in fact, we see that $\phi \psi g \phi^{-1} = \psi \phi(g)$ for all $g \in G, \phi \in \text{Aut}(G)$, so we see that $\text{Inn}(G) \lhd \text{Aut}(G)$.

Finally, if one considers the surjective group homomorphism:

$$f : G \to \text{Inn}(G)$$

$$g \to \psi_g$$

one sees that $\text{ker } f = Z(G)$, giving $\text{Inn}(G) \cong G/Z(G)$.

**Important Remark:** Let $\psi \in \text{Inn}(G)$ and $H \lhd G$. Then $\psi|_H \in \text{Aut}(H)$. (Also note that $\psi|_H$ is in general not an inner automorphism of $H$).

We want to compute the automorphism group for some “easy” groups. First, lets recall the concept of a group of units:

**Definition:** Let $R$ be a ring with identity. Let $R^* := \{u \in R|u \text{ is a unit of } R\}$

Then $R^*$ is a group under multiplication. For example, consider $\mathbb{Z}_n^*$, and it is easy to see that $\mathbb{Z}_n^*$ is a group under multiplication of order $\phi(n)$ where $\phi$ is the Euler phi-function. Also, $M_{n \times n}(\mathbb{R})^* = \text{GL}_n(\mathbb{R})$.

We are ready for a theorem.

**Theorem:** $\text{Aut}(\mathbb{C}_n) \cong \mathbb{Z}_n^*$.

**Proof:** Let $C_n = \langle a \rangle$ and suppose $\phi : \langle a \rangle \to \langle a \rangle$ is an isomorphism. Suppose $\phi(a) = a^k$. Then $\phi(a^i) = \phi(a)^i = (a^k)^i$. Therefore, $\text{im } \phi = \langle a^k \rangle$. Since $\phi$ is surjective, $\langle a^k \rangle = \langle a \rangle$. Therefore $(k, n) = 1$, so $k \in \mathbb{Z}_n^*$.

Now define

$$f : \text{Aut}(C_n) \to \mathbb{Z}_n^*$$

$$\phi \mapsto \bar{k} \text{ where } \phi(a) = a^k$$

**f is well-defined:** Suppose $\phi(a) = a^k = a^l$ Then $a^{k-l} = 1$ $\Rightarrow n|(k-l) \Rightarrow \bar{k} = \bar{l}$.

**f is a homomorphism:** Left as an exercise (easy to see).

**f is a monomorphism:** If $f(\phi) = \bar{1}$ then $\phi(a) = a$, and therefore $\phi = 1$.

**f is an endomorphism:** If $k \in \mathbb{Z}_n^*$ then $\langle a^k \rangle = \langle a \rangle$ which implies $\phi : \langle a \rangle \to \langle a \rangle$ which sends $a$ to $a^k$ is an automorphism of $C_n$. So $f(\phi) = \bar{k}$ and therefore $f$ is onto.

Note that $\mathbb{Z}_n$ is a cyclic group but $\mathbb{Z}_n^*$ is not in general. For example, $\mathbb{Z}_{12}^*$ has no element of order 8 (which is the order of the group). In fact, suppose $n = kl$ where $(k, l) = 1$ and $k, l > 2$. By the Chinese Remainder Theorem, we have $\mathbb{Z}_n \cong \mathbb{Z}_k \times \mathbb{Z}_l$ which implies that $\mathbb{Z}_n \cong (\mathbb{Z}_k \times \mathbb{Z}_l)^* \cong \mathbb{Z}_k^* \times \mathbb{Z}_l^*$, which is not cyclic, since $\phi(k)$ and $\phi(l)$ are both even (exercise).

**Theorem:** Let $F$ be a field and $H$ a finite subgroup of $F^*$. Then $H$ is cyclic.
**Proof:** It is enough to show that each Sylow subgroup of $H$ is cyclic, since $H$ is abelian, this would mean that $H$ is the direct product of cyclic subgroups of relatively prime order.) Hence, we may assume that $|H| = p^n$, for some prime $p$. Then

$$H \cong C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$$

where $n_1 \geq n_2 \geq \cdots \geq n_k$. Hence $h^{p^{n_1}} = 1$ for all $h \in H$. If $H$ is not cyclic, then $n_1 < n_2$, or equivalently, $k \geq 2$. Let $f(x) = x^{p^{n_1}} - 1 \in F[x]$. Since $f(h) = 0$ for all $h \in H \subseteq F$, $f(x)$ has at least $p^n$ roots. But $p^n > p^{n_1}$, a contradiction.

**Corollary:** If $p$ is prime, $\mathbb{Z}_p^* \cong C_{p-1}$, and in particular, $\text{Aut}(\mathbb{Z}_p) \cong C_{p-1}$.

**Example:** Find an automorphism of $C_{13}$ of order 6.
We know that $\text{Aut}(C_{13}) \cong \mathbb{Z}_{13}$. As $2^6 \equiv -1 \pmod{13}$, we see that $\mathbb{Z}_{13}^* = \langle 2 \rangle$. So, we know that $2^2 = 4$ is an element of order 6 in $\mathbb{Z}_{13}^*$. Hence, letting $C_{13} = \langle a \rangle$, an automorphism of order 6 is given by:

$$\phi : C_{13} \rightarrow C_{13}$$

$$a \mapsto a^4$$

**Example:** Find $\phi \in \text{Aut}(C_{35})$ such that $\phi$ has order 12.
We know that $\text{Aut}(C_{35}) \cong \mathbb{Z}_{35}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_7^*$. The Chinese Remainder Theorem isomorphism:

$$\mathbb{Z}_{35}^* \rightarrow \mathbb{Z}_5^* \times \mathbb{Z}_7^*$$

$$\bar{a} \mapsto (\bar{a}, \bar{a})$$

Now, $\mathbb{Z}_5^*$ is cyclic of order 4, and $\mathbb{Z}_7^*$ is cyclic of order 6. An element of order 4 in $\mathbb{Z}_5^*$ is $\bar{2}$, and an element of order 3 in $\mathbb{Z}_7^*$ is $\bar{4}$. Hence, $(\bar{2}, \bar{4}) \in \mathbb{Z}_5^* \times \mathbb{Z}_7^*$ has order 12. Therefore, we see that 32 is an element of order 12 in $\mathbb{Z}_{35}^*$. Hence, setting $C_{35} = \langle a \rangle$, we see that an automorphism of order 12 is given by:

$$\phi : C_{35} \rightarrow C_{35}$$

$$a \mapsto a^{12}$$

**Theorem:** Let $p > 2$ be prime. Then $\mathbb{Z}_{p^n}^*$ is cyclic of order $p^n - p^{n-1}$.

**Proof:** We know that $|\mathbb{Z}_{p^n}^*| = \phi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$. Since $\mathbb{Z}_{p^n}^*$ is cyclic, it is enough to show all of its Sylow subgroups are cyclic.

**Exercise:** $(1 + p)^{p^n-1} \equiv 1 \pmod{p^n}$ but $(1 + p)^{p^n-2} \not\equiv 1 \pmod{p^n}$.

Therefore, we see that $[1 + p]_{p^n} \in \mathbb{Z}_{p^n}^*$ is an element of order $p^{n-1}$. Therefore, the sylow $p$-subgroup of $\mathbb{Z}_{p^n}$ is cyclic. Now consider the group homomorphism defined by:

$$\psi : \mathbb{Z}_{p^n}^* \rightarrow \mathbb{Z}_p^*$$

$$[a]_{p^n} \mapsto [a]_p$$
Note that since \((a, p^n) = 1 \iff (a, p) = 1\), we have

\[ [a]_{p^n} \in \mathbb{Z}_{p^n}^* \iff [a]_p \in \mathbb{Z}_p^* \]

Therefore, we see that \(\psi\) is well-defined and surjective. Since \(|\mathbb{Z}_{p^n}^*| = p^{n-1}(p - 1)\) and \(|\mathbb{Z}_p^*| = p - 1\), we see that \(|\ker \psi| = p^{n-1}|.

Let \(Q\) be a Sylow \(q\)-subgroup of \(\mathbb{Z}_{p^n}^*\), with \(q \neq p\). Then, since \(Q \cap \ker \psi = \{1\}\), \(Q\) is isomorphic to a subgroup of \(\mathbb{Z}_p^*\). Since \(\mathbb{Z}_p^*\) is cyclic and subgroups of cyclic groups are cyclic, we see that \(Q\) is cyclic, completing the proof.