Content:

| | |
|---|---|
| Theorem | $A_5$ is simple. |
| Theorem | $A_6$ is simple. |
| Theorem | $A_n$ is simple for $n \geq 5$. |
| Definition | internal direct product |
| Lemma 2 | Let $G$ be the internal direct product of $H_1, H_2, \ldots, H_k$. Then we have the following. 1. $H_i \cap H_j = \{e\}$ for all $i \neq j$; 2. If $g \in G$, then there exists unique elements $h_i \in H_i$ such that $g = h_1 h_2 \cdots h_k$; 3. If $h_i \in H_i$ and $h_j \in H_j$, then $h_i h_j = h_j h_i$ for $i \neq j$. |
| Theorem 3 | If $G$ is the internal direct product of $H_1, \ldots, H_k$, then $G \cong H_1 \times \cdots \times H_k$. |
| Lemma 4 | Let $G$ be an Abelian group such that $\lvert G \rvert = p^k a$ where $p$ is prime and $(p, a) = 1$. Then there exists a unique subgroup of order $p^k$. |
| Definition | Sylow $p$-subgroup |
| Theorem 6 | Let $G$ be a finite Abelian group such that $\lvert G \rvert = p_1^{k_1} \cdots p_1^{k_1}$ where each of the $p_i$ are distinct primes. Then $G \cong G(p_1) \times \cdots \times G(p_i)$. |

To prove $A_5$ is simple, we will use the following lemmas (proved Wednesday).

**(∗) Lemma** All 3-cycles in $A_5$ are conjugate. (Extends to $A_n$ for $n \geq 5$.)

**(∗∗) Lemma** Each element in $A_n$, for $n \geq 3$ is either a 3-cycle or a product of 3-cycles.

---

**Theorem** $A_5$ is simple.

**Proof**:

Let $H \lhd A_5$ such that $H \neq \{(1)\}$. Let $\alpha \in H$ such that $\alpha \neq (1)$.
Suppose $\alpha$ is a 3-cycle. Since $H \lhd A_5$, then by definition of normal, all conjugates of $\alpha$ are in $H$. Then by (∗), all 3-cycles are in $H$ (since $H$ is in $A_5$). And by (∗∗), all 3-cycles generate $A_5$, hence $H = A_5$.

Now assume $\alpha$ is not a 3-cycle.
We only need to show $H$ contains a 3-cycle.
The only cycle structures in $A_5$ are (1), (123), (12345), (12)(34).
One of these must be in $H$. By assumption, $\alpha \neq (1)$ or (123).
Then suppose $\alpha = (12345)$. Let $\gamma = (132) \in A_5$.
Since $H$ is normal, then $\gamma\alpha\gamma^{-1} \in H$. Since $H$ is a group, then $\alpha^{-1} \in H$.
$\therefore\ \gamma\alpha\gamma^{-1}\alpha^{-1} \in H$.

$$\gamma\alpha\gamma^{-1}\alpha^{-1} = (132)(12345)(321)(54321) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} = (134). \quad \therefore\ H = A_5.$$

(Note-This works because $\alpha\gamma^{-1}\alpha^{-1}$ is a conjugate of a 3-cycle, hence a 3-cycle, and $\gamma$ is a 3-cycle.
Since a 3-cycle times a 3-cycle is a 3-cycle, then $\gamma\alpha\gamma^{-1}\alpha^{-1}$ is a 3-cycle.)

Lastly, suppose $\alpha = (12)(34)$. Then let $\sigma = (12)(35)$. Then

$$\sigma\alpha\sigma^{-1}\alpha^{-1} = (12)(35)\ (12)(34)\ (12)(35)\ (12)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix} = (354).$$

So in all cases $H = A_5$. $\therefore\ A_5$ is simple.

---

**Theorem** $A_6$ is simple.

**Proof**:
Let $H \lhd A_6$ such that $H \neq \{(1)\}$.
Suppose $\exists\ \alpha \in H$ such that $\alpha \neq (1)$ and $\alpha(i) = i$ for some $i$, where $1 \leq i \leq 6$.
Let $F = \{\sigma \in A_6 \mid \sigma(i) = i\}$.
Note (1) $\alpha \in F$ and $\alpha \in H$, so $H \cap F \neq \{(1)\}$.
(2) $F \cong A_5$ (since every element in $F$ permutes 5 things and fixes $i$)
(2.5) $F \leq A_6$.
(3) $H \lhd A_6$ so by 2nd Isomorphism theorem, $(H \cap F) \lhd F$.
(2nd Isomorphism Theorem:
If $H \lhd G$, $K \leq G$, then $HK \leq G$, $H \cap K \lhd K$, and $K/(H \cap K) \cong HK/H$.)
Since $F \cong A_5$, $F$ cannot have nontrivial normal subgroups,
so $H \cap F = \{(1)\}$ or $H \cap F = F$.
By Note (1), $H \cap F \neq \{(1)\}$.
This gives us $H \cap F = F$, which implies $F \leq H$.
But $H$ contains a 3-cycle, since $F$ does.
So, by (**), $H = A_6$.

Suppose $\forall\ \alpha \in H, \alpha(i) \neq i\ \forall\ i$.
Then $\alpha$ must have cycle structure (12)(3456) or (123)(456)
(otherwise $\alpha$ fixes some i).
If $\alpha = (12)(3456)$, then
$$\alpha^2 = (12)(3456)\ (12)(3456) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 3 & 4 \end{pmatrix} = (35)(46),$$
which fixes 1 and 2, a contradiction.
If $\alpha = (123)(456)$, then let $\beta = (234)$.
$$\alpha\beta\alpha^{-1}\beta^{-1} = (123)(456)\ (234)\ (654)(321)\ (432) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 1 & 3 & 6 \end{pmatrix} = (15324),$$
which fixes 6, a contradiction.
$\therefore$ No such normal subgroup can exist, and so $A_6$ is a simple group.

**Theorem** $A_n$ is simple for $n \geq 5$.

**Proof**:
Generalize the proof for $A_6$. Proof is in text, p. 108.

**Finite Abelian Groups (Hand out)**

**Definition** Let $H_1, H_2, \ldots, H_k$ be subgroups of G. We say that G is the *internal direct product* of $H_1, H_2, \ldots, H_k$ if the following hold.

1. $H_i \triangleleft G$, for all $H_i$.
2. $G = H_1 H_2 \cdots H_k$.
3. $H_i \cap H_1 \cdots \hat{H}_i \cdots H_k = \{e\}$.

**Lemma 2** Let $G$ be the internal direct product of $H_1, H_2, \ldots, H_k$. Then we have the following.

1. $H_i \cap H_j = \{e\}$ for all $i \neq j$.
2. If $g \in G$, then there exists unique elements $h_i \in H_i$ such that $g = h_1 h_2 \cdots h_k$.
3. If $h_i \in H_i$ and $h_j \in H_j$, then $h_i h_j = h_j h_i$ for $i \neq j$.

Proof: Exercise.

**Proof (1):**

Let $x \in H_i \cap H_j$. Then $x \in H_i$ and $x \in H_j$.

Thus $x = e_1 e_2 \cdots h_j \cdots e_k \in H_1 \cdots \hat{H}_i \cdots H_j \cdots H_k$.

But $H_i \cap H_1 \cdots \hat{H}_i \cdots H_k = \{e\}$, a contradiction.

$\therefore H_i \cap H_j = \{e\}$ for all $i \neq j$.

**Proof (2):**

Let $g \in G$. If $g = h_1 h_2 \cdots h_k = h'_1 h'_2 \cdots h'_k$, then $h'^{-1}_1 h_1 = h'_2 \cdots h'_k h_k^{-1} \cdots h_2^{-1}$.

And since $H_1 \cap \hat{H}_1 H_2 \cdots H_k = \{e\}$, then $e = h'^{-1}_1 h_1 = h'_2 \cdots h'_k h_k^{-1} \cdots h_2^{-1}$.

Hence $h_1 = h'_1, h_2 = h'_2, \ldots h_k = h'_k$.

$\therefore h_1 h_2 \cdots h_k$ is the unique factorization of $g$.

**Proof (3):**

Since $H_i$ and $H_j$ are normal subgroups, then $(h_i h_j h_i^{-1}) h_j^{-1} \in H_j$ and $h_i (h_j h_i^{-1} h_j^{-1}) \in H_i$.

Since $H_i \cap H_j = \{e\}$ by part (1), $(h_i h_j h_i^{-1}) h_j^{-1} = e$. Hence $h_i h_j = h_j h_i$ for $i \neq j$.

**Theorem 3** If $G$ is the internal direct product of $H_1, \ldots, H_k$, then $G \cong H_1 \times \cdots \times H_k$.

**Proof**:

Define $\phi$: $H_1 \times \cdots H_k \to G$ by $\phi(h_1, h_2, \ldots, h_k) = h_1 h_2 \cdots h_k$.

To show $\phi$ is surjective, let $g \in G$.

Then $g = h_1 h_2 \cdots h_k = \phi(h_1, h_2, \ldots, h_k)$ as $G = H_1 H_2 \cdots H_k$.

Since $\phi((h_1, h_2, \ldots, h_k)) = \phi((h'_1, \ldots, h'_k))$ implies

$h_1 = h'_1, h_2 = h'_2, \ldots h_k = h'_k$ by Lemma 2, part 2, then $\phi$ is injective.

And by Lemma 2, part 3, we have that

$\phi((h_1, h_2, \ldots, h_k))\phi((h'_1, \ldots, h'_k)) = h_1 h_2 \cdots h_k h'_1 h'_2 \cdots h'_k$

$= h_1 h'_1 h_2 h'_2 \cdots h_k h'_k = \phi((h_1, h_2, \ldots, h_k)(h'_1, \ldots, h'_k))$.

$\therefore$ $\phi$ is a homomorphism.

$\therefore$ $G \cong H_1 \times \cdots \times H_k$.

---

**Lemma 4** Let $G$ be an Abelian group such that $|G| = p^k a$ where $p$ is prime and $(p, a) = 1$. Then there exists a unique subgroup of order $p^k$.

**Proof**:

By Corollary 2.78 (If $G$ is a finite Abelian group and $d$ is a divisor of $|G|$, then $G$ contains a subgroup of order $d$.), we know that such a subgroup exists. So we only need to prove uniqueness.

Let $H \leq G$ such that $|H| = p^k$, and let $G(p) = \{x \in G |\ x^{p^k} = e\}$.

By exercise #4 we know $G(p) \leq G$.

(Exercise #4): $G(p) \leq G$.

Proof:

Clearly, $G(p) \subseteq G$. And, since $e^{p^k} = e$, then $e \in G(p)$, hence $G(p) \neq \varnothing$.

Let $x, y \in G(p)$. Then $x^{p^k} = e$, and $y^{p^k} = e$. Since G is Abelian,

then $\left(xy^{-1}\right)^{p^k} = \left(x\right)^{p^k}\left(y^{-1}\right)^{p^k} = \left(x\right)^{p^k}\left[\left(y\right)^{p^k}\right]^{-1} = e \bullet e^{-1} = e$.

$\therefore$ $xy^{-1} \in G(p)$, hence $G(p) \leq G$.

We claim that $H = G(p)$.

Let $h \in H$, then $h^{p^k} = e$, by corollary to Lagrange's theorem, since $|H| = p^k$ (by assumption). Hence $h \in G(p)$, so $H \subseteq G(p)$.

Let $g \in G(p)$. So $g^{p^k} = e$. Consider $gH \in G/H$. Since $|G/H| = p^k a/p^k = a$, then $\circ(gH) \mid a$ (by corollary to Lagrange's theorem. However, $\circ(gH) \mid \circ(g)$ (by exercise 2.47 (i) If $f$:$G \to H$ is a homomorphism and $x \in G$ has order $k$, $f(x) \in H$ has order $m$ where $m \mid k$.).

Since $g^{p^k} = e$, then $\circ(gH) \mid \circ(g) \Rightarrow \circ(gH) \mid p^k$. So $\circ(gH) = 1$ since $(a, p) = 1$.

Therefore $gH = H$ and hence $g \in H$. Thus $G(p) \subseteq H$ and hence $H = G(p)$.

Therefore $G(p)$ is the unique subgroup of $G$ of order $p^k$. □

---

**Definition** Let $G$ be a group such that $|G| = p^k a$ where $p$ is prime and $(p, a) = 1$. A subgroup of order $p^k$, denoted $G(p)$ is called a *Sylow p-subgroup* of $G$.

---

**Theorem 6** Let $G$ be a finite Abelian group such that $|G| = p_1^{k_1} \cdots p_l^{k_l}$ where each of the $p_i$ are distinct primes. Then $G \cong G(p_1) \times \cdots \times G(p_l)$.

**Proof**:

We will show that $G$ is the internal direct product of its Sylow $p_i$-subgroups and therefore by Theorem 3 (If $G$ is the internal direct product of $H_1, \ldots, H_k$, then $G \cong H_1 \times \cdots \times H_k$.) we get our desired result.

Firstly, since $G$ is Abelian all subgroups are normal, so $G(p_i) \lhd G$.

Next we will show $G = G(p_1)G(p_2) \cdots G(p_l)$.

Clearly $G(p_1)G(p_2) \cdots G(p_l) \subseteq G$.

Moreover, by homework problem #3, we have that

$|G(p_1)G(p_2) \cdots G(p_l)| = |G(p_1)||G(p_2)| \cdots |G(p_l)| = p_1^{k_1} \cdots p_l^{k_l} = |G|$.

Homework problem #3:
Let $H_1, \ldots, H_k$ be subgroups of a group $G$ such that $H_i \cap H_j = \{e\}$ for all $i \neq j$ in $\{1, \ldots, k\}$. Prove that $|H_1H_2 \cdots H_k| = |H_1|\,|H_2| \cdots |H_k|$.
**Proof**:
Let $G$ be a finite Abelian group. We will induct on $k$.
Let $k = 2$. Note that by Exercise 2.33
(If H≤G, K≤G, and (|H|, |K|) = 1, then H ∩ K = {1}.),
we have $H_i \cap H_j$, for all $i \neq j$ in $\{1, \ldots, k\}$.
And by Direct Product Handout, Exercise #4(c),
*(If H≤G, K≤G, then |HK| = |H||K|/|H∩K|)*, we have
$|H_1H_2| = |H_1||H_2|/|H_1 \cap H_2| = |H_1||H_2|$.
Let $k > 2$ and assume that if $H_1, \ldots, H_k$ are subgroups of $G$,
then $|H_1H_2 \cdots H_n| = |H_1|\,|H_2| \cdots |H_n|\ \forall\ n < k$.
Then if $H_1, \ldots, H_{k-1}$ are subgroups of $G$, we have
$|H_1H_2 \cdots H_{k-1}| = |H_1|\,|H_2| \cdots |H_{k-1}|$. Note that $H_1H_2 \cdots H_{k-1} \leq G$ as $G$ is Abelian.
And since $(|H_i|, |H_j|) = 1$ for all $i \neq j$, then $(|H_1H_2 \cdots H_{k-1}|, |H_k|) = 1$,
hence $H_1H_2 \cdots H_{k-1} \cap H_k = \{1\}$,
Thus $|H_1H_2 \cdots H_{k-1}H_k| = |H_1H_2 \cdots H_{k-1}||H_k| = |H_1|\,|H_2| \cdots |H_{k-1}||H_k|$.
$\therefore$ $|H_1H_2 \cdots H_k| = |H_1|\,|H_2| \cdots |H_k|$ for all $i \neq j$ in $\{1, \ldots, k\}$.

Hence $G = G(p_1)G(p_2) \cdots G(p_l)$ since $G(p_1)G(p_2) \cdots G(p_l) \subseteq G$.

Lastly we need to show that $G(p_i) \cap G(p_1) \cdots \hat{G}(p_i) \cdots G(p_l) = \{e\}$ for all $i \in \{1, 2, \ldots, k\}$.

Fix $i \in \{1, 2, \ldots, k\}$. Then we can write the order of $G$ as $p_i^{k_i} a$ where $a = p_1^{k_1} \cdots \hat{p}_i^{k_i} \cdots p_l^{k_l}$ and hence $(p_i, a) = 1$.

Again, by homework problem #3, $|\,G(p_1) \cdots \hat{G}(p_i) \cdots G(p_l)\,| = a$.

However, $|G(p_i)| = p_i^{k_i}$. Hence $(|G(p_1) \cdots \hat{G}(p_i) \cdots G(p_l)\,|, |G(p_i\,)|) = 1$.

And thus, $G(p_i) \cap G(p_1) \cdots \hat{G}(p_i) \cdots G(p_l) = \{e\}$ by Exercise 2.33

(If $H \leq G$, $K \leq G$ and $(|H|, |K|) = 1$, then $H \cap K = \{e\}$).

Therefore, $G$ is the internal product of $G(p_1), G(p_2), \ldots, G(p_i)$. and hence, by Theorem 3, $G \cong G(p_1) \times \cdots \times G(p_i)$. □