Notes for MATH 210A

Quin Darcy

California State University, Sacramento

Sep 28, 2019

1 Exam 1

Proposition 1.1. If $(a, b) = g$, $d \mid a$, and $d \mid b$, then $d \mid g$.

Proof. Assume that $(a, b) = g$, $d \mid a$, and $d \mid b$. Since $(a, b) = g$, then there exists $x, y \in \mathbb{Z}$ such that $g = ax + by$. Moreover, since $d \mid a$ and $d \mid b$, then there exists $k_1, k_2 \in \mathbb{Z}$ such that $a = k_1 d$ and $b = k_2 d$. Substituting in for the first equation, we get that $g = (k_1 d)x + (k_2 d)y = d(k_1 x + k_2 y)$. Hence, there exists $m \in \mathbb{Z}$ such that $g = dm$, namely $m = (k_1 x + k_2 y)$. Thus, $d \mid g$. $\square$

Proposition 1.2. If $(a, c) = 1$ and $(b, c) = 1$, then $(ab, c) = 1$.

Proof. Assume that $(a, c) = 1$ and that $(b, c) = 1$. Since $(a, c) = 1$ then there exists $x, y \in \mathbb{Z}$ such that $1 = ax + cy$ and since $(b, c) = 1$, then there exists $v, w \in \mathbb{Z}$ such that $1 = bv + cw$. Thus,

$$\begin{aligned}(ax + cy)(bv + cw) &= ab(xv) + ac(xw) + bc(vy) + c^2(yw) \\ &= ab(xv) + c(axw + bvy + cyw) \\ &= 1.\end{aligned}$$

Since $xv \in \mathbb{Z}$ and $axw + bvy + cyw \in \mathbb{Z}$, then $(ab, c) = 1$. $\square$

Proposition 1.3. If $(a, n) = 1$, then there exists $x \in \mathbb{Z}$ such that $ax \equiv 1(\text{mod } n)$, and $(x, n) = 1$.

Proof. Assume that $(a, n) = 1$. Then it follows that there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Thus, $ax - 1 = ny$. Thus, $n \mid (ax - 1)$. Hence, $ax \equiv 1(\text{mod } n)$. Additionally, since $a \in \mathbb{Z}$ and $ax + ny = 1$, then $(x, n) = 1$. $\square$

Proposition 1.4. Assume $(G, \star)$ is a finite group, and $|G| = n$. If $g \in G$, then $o(g)$ is finite and if $g^t = e$, then $o(g) \mid t$.

Proof. Let G be a finite group with order n. Take $g \in G$ and assume $o(g)$ is not finite. Then there does not exist $k \in \mathbb{Z}$ with $k > 0$ such that $g^k = e$. Now let $k_1, k_2 \in \mathbb{Z}$ where $k_1, k_2 > 0$ and $k_1 \neq k_2$. Assume $g^{k_1} = g^{k_2}$. Then $g^{k_2 - k_1} = e$. Since $k_2 - k_1 \in \mathbb{Z}$, and $o(g) \leq k_2 - k_1$, then $o(g)$ is finite. Since this is a contradiction, then it is the case that for all $k_1, k_2 \in \mathbb{Z}$ where $k_1, k_2 > 0$ and $k_1 \neq k_2$, then $g^{k_1} \neq g^{k_2}$. Thus, there exists a one-to-one and onto correspondence between $\langle g \rangle$ and $\mathbb{Z}$. However, since $\langle g \rangle \subseteq G$ and $|G| = n$, then we a contradiction and $o(g)$ must be finite.

Let $t \in \mathbb{Z}$ such that $g^t = e$. Then $g^t = g^{o(g)}$ which implies $g^{t-o(g)} = e$. We now have that either $t = o(g)$, in which case $o(g) \mid t$, or $t \neq o(g)$. If $t \neq o(g)$, then either $o(g) \nmid t$ or $o(g) \mid t$. If $o(g) \nmid t$, then by the division algorithm, there exists $q, r \in \mathbb{Z}$ with $0 \leq r < o(g)$, such that $t = q(o(g)) + r$. Thus,

$$\begin{aligned}
g^t &= g^{q(o(g))+r} \\
&= g^{q(o(g))} \star g^r \\
&= \left(g^{o(g)}\right)^q \star g^r \\
&= e^q \star g^r \\
&= g^r.
\end{aligned}$$

However, since $g^t = e$ and $g^r = g^t$, then $g^r = e$. This is a contradiction since $r < o(g)$. Therefore, $o(g) \mid t$. $\square$

Proposition 1.5. If $(G, \star)$ is a group, $a \in G$, $o(a) = n$, $m \in \mathbb{Z}^+$, and $d = (m, n)$, then $o(a^m) = o(a^d)$.

Proof. Assume $(G, \star)$ is a group, $a \in G$, $o(a) = n$, $m \in \mathbb{Z}^+$, and that $d = (m, n)$. Let $t = o(a^d)$ and $y = o(a^m)$. We want to show that $t \mid y$ and $y \mid t$. Since $d = (m, n)$, then $d \mid m$. Thus, there exists $k \in \mathbb{Z}$ such that $m = dk$. Thus, $(a^m)^t = (a^{dk})^t = a^{dkt} = e$. Thus, by Proposition 1.4, $y \mid t$.

Since $d = (m, n)$, then there exists $u, v \in \mathbb{Z}$ such that $d = um + vn$. Thus, $(a^d)^y = a^{dy} = a^{(um+vn)y} = a^{umy} \star a^{vny} = (a^m)^{uy} \star (a^n)^{vy} = e^u \star e^{vy} = e$. Thus, by Proposition 1.4, $t \mid y$. Thus, $t = y$. Therefore, $o(a^m) = o(a^d)$. $\square$

Definition 1.1. A group $(G, \star)$ ***acts on a set*** S if and only if there exists $\varphi\colon G \times S \to S$ (called a ***group action***) such that for all $g, h \in G$ and $s \in S$

(i) $\varphi((g \star h, s)) = \varphi((g, \varphi(h, s)))$

(ii) $\varphi((e, s)) = s$

Definition 1.2. Given a group $(G, \star)$, a set S, an action φ, and $s \in S$, the set $G_s = \{g \in G\colon \varphi((g, s)) = s\}$ is called the ***stabilizer of*** s ***in*** G, or the ***isotropy group of*** s.

Definition 1.3. Given $s \in S$, the set $G(s) = \{\varphi((g, s))\colon g \in G\}$ is called the ***orbit of*** s ***in*** G. We will also sometimes denote the orbit of $s \in S$ as $\mathrm{orb}_\varphi(s)$.

Definition 1.4. Given a group $(G, \star)$ and an element $s \in G$, the set $N(s) = \{g \in G\colon g \star s = s \star g\}$ is called the ***centralizer*** or ***normalizer*** of s.

Proposition 1.6. Let $(G, \star)$ be a group, S be a set, φ be a action of G on S, and let $s \in S$, then $G_s \subseteq_g G$.

Proof. First we must show that $G_s \neq \varnothing$. Recall, that by Definition 1.2, $G_s = \{g \in G\colon \varphi((g, s)) = s\}$. Since φ is an action of G on S, then by (ii) of Definition 1.1, $\varphi((e, s)) = s$, for all $s \in S$. Thus, $e \in G_s$ and therefore $G_s \neq \varnothing$. Next, we want to show that $a \star b^{-1} \in G_s$ whenever $a, b \in G_s$. So let $a, b \in G_s$. It follows that $\varphi((a, s)) = s$ and that $\varphi((b, s)) = s$. Additionally, since $\varphi((e, s)) = s$, then it follows that

$$\begin{aligned}
\varphi((a, s)) &= \varphi((a, \varphi((e, s)))) \\
&= \varphi((a, \varphi((b^{-1} \star b, s)))) \\
&= \varphi((a \star b^{-1} \star b, s)) \\
&= \varphi(((a \star b^{-1}) \star b, s)) \\
&= \varphi((a \star b^{-1}, \varphi((b, s)))) \\
&= \varphi((a \star b^{-1}, s)) \\
&= s.
\end{aligned}$$

Thus, by the last equality, we have that $\varphi((a \star b^{-1}, s)) = s$. Hence, $a \star b^{-1} \in G_s$. Therefore, $G_s \subseteq_g G$. $\square$

Definition 1.5. If $\theta\colon G \to G$ is an isomorphism, then θ is called an ***automorphism*** of G.

Proposition 1.7. The set, $\mathrm{Aut}(G)$, of automorphisms of G equipped with the operation $\circ$ of composition is a group.

Proof. Since the identity map on G is an automorphism, then $i_G \in \mathrm{Aut}(G)$ and thus, $\mathrm{Aut}(G) \neq \varnothing$. Composition of maps is associative, the composition of two bijective maps is a bijective map, and since each map is bijective, it has an inverse which is also in $\mathrm{Aut}(G)$. Thus, $(\mathrm{Aut}(G), \circ)$ is a group. $\square$

Proposition 1.8. Assume that $\varphi\colon G \times S \to S$ is an action of G on S. For each $g \in G$, define $\theta_g\colon S \to S$ by $\theta_g(t) = \varphi((g,t))$. Then σ_g is a permutation of S.

Proof. We want to show that $\sigma_g\colon S \to S$ is bijective (i.e., invertible). Thus, we need to show that for all $g \in G$, σ_g has an inverse, namely $\sigma_{g^{-1}}$. We want $(\sigma_g \circ \sigma_{g^{-1}})(x) = x$, for all $x \in S$. Thus, we let $x \in S$, then

$$\begin{aligned}
(\sigma_g \circ \sigma_{g^{-1}})(x) &= \sigma_g(\sigma_{g^{-1}}(x)) \\
&= \sigma_g(\varphi(g^{-1}, x)) \\
&= \varphi(g, \varphi(g^{-1}, x)) \\
&= \varphi(gg^{-1}, x) \\
&= \varphi(e, x) \\
&= x.
\end{aligned}$$

Similarly, $(\sigma_{g^{-1}} \circ \sigma_g)(x) = x$. Thus, σ_g is invertible and therefore is a bijection. Thus, σ_g is a permutation of S. $\square$

Proposition 1.9. Recall that $A(S)$ denotes the group of all permutations is S. Define $\theta\colon G \to A(S)$ by $\theta(g) = \sigma_g$. Then θ is a homomorphism.

Proof. θ is a function by definition since, for each $g \in G$. $\theta(g) = \sigma_g \in A(S)$. To show that θ is well defined, let $g, h \in G$ and assume that $g = h$. Then $\theta(g) = \sigma_g$ and $\theta(h) = \sigma_h$. Let $t \in S$, then $\sigma_g(t) = \varphi(g,t) = \varphi(h,t) = \sigma_h(t)$. Thus, $\sigma_g = \sigma_h$. Thus, $\theta(g) = \theta(h)$ and θ is therefore well defined.

Now we will show that θ is a homomorphism. Let $g, h \in G$. Then $\theta(gh) = \sigma_{gh}$. Thus, for any $x \in S$, we have that

$$\begin{aligned}
\sigma_{gh}(x) &= \varphi(gh, x) \\
&= \varphi(g, \varphi(h, x)) \\
&= \varphi(g, \sigma_h(x)) \\
&= \sigma_g(\sigma_h(x)) \\
&= (\sigma_g \circ \sigma_h)(x).
\end{aligned}$$

Thus, $\theta(gh) = \theta(g) \circ \theta(h)$. Therefore, θ is a homomorphism. The converse of the above is also true. Assume that $\alpha\colon G \to A(S)$ is a homomorphism, and define $\varphi\colon G \times S \to S$ by $\varphi((g, s)) = (\alpha(g))(s)$. Then φ is a group action. *Therefore actions of a group G on a set S and homomorphisms from G into $A(S)$ are essentially the same.*

Note that $\square$

Proposition 1.10. Assume that $(G.\star)$ is a group, $N \triangleleft G$ and that $\varphi\colon G \times N \to N$ by $\varphi((g, n)) = g \star n \star g^{-1}$. Then φ is an action on N.

Proof. Since $N \triangleleft G$, then for all $g \in G$ and $n \in N$, $\varphi(g, n) = g \star n \star g^{-1} \in N$. Thus, $\varphi\colon GN \to N$. Now let $(g, n), (h, m) \in G \times N$ and assume $(g, n) = (h, m)$. Then since this implies that $g = h$ and $n = m$, then $\varphi(g, n) = g \star n \star g^{-1} = h \star m \star h^{-1} = \varphi(h, m)$. Thus, φ is well defined.

We want to show that for all $h, g \in G$ and all $n \in N$ that

$$\varphi(h \star g, n) = \varphi(h, \varphi(g, n)) \quad \text{and} \quad \varphi(e, n) = n.$$

Let $h, g \in G$ and let $n \in N$. Then

$$\begin{aligned}
\varphi(h \star g, n) &= (h \star g) \star n \star (h \star g)^{-1} \\
&= (h \star g) \star n \star (g^{-1} \star h^{-1}) \\
&= h \star (g \star n \star g^{-1}) \star h^{-1} \\
&= \varphi(h, g \star n \star g^{-1}) \\
&= \varphi(h, \varphi(g, n)).
\end{aligned}$$

Note that the fourth equality holds since N is normal which means that for all $g \in G$ and $n \in N$, $g \star n \star g^{-1} \in N$ and so $(h, g \star n \star g^{-1}) \in G \times N$. We have satisfied the first of the two equalities. Now consider

$$\varphi(e, n) = e \star n \star e^{-1} = e \star n \star e = n.$$

Therefore, φ is an action of G on N. $\square$

Proposition 1.11. Let G be a group, $N \triangleleft G$, and $\varphi\colon G \times N \to N$. By Proposition 1.10, we know φ is an action. Then let θ be the permutation representation associated with the action φ. Then θ is a homomorphism from G to $\mathrm{Aut}(N)$.

Proof. By Proposition 1.9, we know that $\theta\colon G \to A(N)$ is a homomorphism. We want to show that for each $g \in G$, $\theta(g) = \sigma_g$ is an isomorphism. By definition, we already have that σ_g is bijective, and so we need only that σ_g is a homomorphism. Thus, we let $m, n \in N$. Then $\sigma_g(mn) = \varphi(g, mn) = gmng^{-1} = (gmg^{-1})(gng^{-1}) = \varphi(g, m)\varphi(g, n)$. Thus, σ_g is a homomorphsim and thus σ_g is an isomorhism from N to N. Hence, for all $g \in G$, $\theta(g) = \sigma_g \in \mathrm{Aut}(N)$. Therefore, $\theta\colon G \to \mathrm{Aut}(N)$ is a homomorphism. $\square$

Note that

$$\begin{aligned}
\ker\theta &= \{g \in G \mid \theta(g) = i_G\} \\
&= \{g \in G \mid \sigma_g = i_G\} \\
&= \{g \in G \mid \forall n \in N\colon \sigma_g(n) = n\} \\
&= \{g \in G \mid \forall n \in N\colon \varphi(g,n) = n\} \\
&= \{g \in G \mid \forall n \in N\colon gng^{-1} = n\} \\
&= \{g \in G \mid \forall n \in N\colon gn = ng\} \\
&= C_G(N).
\end{aligned}$$

Proposition 1.12. Assume that G is a group, that $H \triangleleft G$, $N \triangleleft G$, and that $N \cap H = \{e\}$.Then

(i) For all $n \in N$ and for all $h \in H$, $nh = hn$.

(ii) $N \times H \cong NH$.

Proof.

(i) Let $n \in N$ and let $h \in H$. Then since N is normal in G, then $hnh^{-1} \in N$. By closure of N, it follows that $(hnh^{-1})n^{-1} \in N$. Similarly, since $h \in H$, then $h^{-1} \in H$. Additionally, since H is normal in G, then $nh^{-1}n^{-1} \in H$. By closure, it follows that $h(nh^{-1}n^{-1}) \in H$. Thus, $hnh^{-1}n^{-1} \in N \cap H$. However, since $N \cap H = \{e\}$, then it follows that $hnh^{-1}n^{-1} = e$. Thus, $hn = nh$.

(ii) Let $f\colon N \times H \to NH$ be defined by $f\big((n,h)\big) = nh$. We want to show that f is an isomorphism. First we will show that f is well defined. Let $(a,b) = (c,d)$. Then $f\big((a,b)\big) = ab$ and $f\big((c,d)\big) = cd$. Since $a = c$ and $b = d$, by assumption, then $ab = cd$. Thus, $f\big((a,b)\big) = f\big((c,d)\big)$. Thus, f is a function.

Now we will show that f is a homomorphism. Let $(a,b),(c,d) \in N \times H$. Then $f\big((a,b) \odot (c,d)\big) = f\big((ac,bd)\big) = (ac)(bd)$. However, since $cb = bc$ by (a), then $(ac)(bd) = (ab)(cd) = f\big((a,b)\big)f\big((c,d)\big)$. Thus, f is a homomorphism.

Now we will show that f is onto. Let $nh \in NH$, then $f\big((n,h)\big) = nh$. Thus, f is onto.

Assume $f\big((a,b)\big) = f\big((c,d)\big)$. Then $ab = cd$. Thus, $c^{-1}a = db^{-1}$. Since $a,c \in N$, then $c^{-1}a \in N$ and since $b,d \in H$, then $db^{-1} \in H$. Thus, $c^{-1}a \in N \cap H$ and $db^{-1} \in N \cap H$. Thus, $c^{-1}a = e$ and so $a = c$. Similarly, $db^{-1} = e$ and so $d = b$. Thus, $(a,b) = (c,d)$. Thus, f is 1-1. Therefore, f is an isomorphism and so $N \times H \cong NH$.

$\square$

Proposition 1.13. Let G be a group, $M \subseteq G$, $N \triangleleft G$, and $N \subseteq M$. Then $M/N \cong G/N$ iff $M \triangleleft G$.

Proof. □

Proposition 1.14. Assume that G is a group, $N \triangleleft G$, and that $M \triangleleft G$. Then $NM/M \cong N/N \cap M$.

Proof. □

Proposition 1.15. Let G be a group, S be a set, and let $\varphi\colon G \times S \to S$ be an action of the group G on S. Then the set of orbits of φ partition S.

Proof. Let $O = \{G(s) \mid s \in S\}$. Since $s = \varphi(e, s)$, then $s \in G(s)$ and $G(s) \subseteq \bigcup O$. Thus, $s \in \bigcup O$ and $\bigcup O \neq \varnothing$. Let $s \in S$. Then it follows that $s = \varphi(e, s) \in G(s)$. Since $G(s) \subseteq \bigcup O$, then $s \in \bigcup O$. Let $\varphi(g, s) \in \bigcup O$. Then by Definition 1.1, $\varphi\colon G \times S \to S$, then $\varphi(g, s) \in S$. Thus, $\bigcup O \subseteq S$. Hence, $\bigcup O = S$.

Assume $G(s) \cap G(t) \neq \varnothing$. Then there exists $g, h \in G$ such that $\varphi(g, s) = \varphi(h, t)$. By (ii) of Definition 1.1, $\varphi(e, s) = s$. Thus, $\varphi(g^{-1}, \varphi(g, s)) = \varphi(g^{-1}, \varphi(h, t))$. Thus, $\varphi(g^{-1}h, t) = s$. Now let $x \in G(s)$, then there exists $f \in G$, such that $x = \varphi(f, s)$. Thus, $x = \varphi(f, s) = \varphi(f, \varphi(g^{-1}h, t)) = \varphi(fg^{-1}h, t) \in G(t)$. Thus, $G(s) \subseteq G(t)$. Similarly, $G(t) \subseteq G(s)$. Thus, $G(s) = G(t)$. Therefore, O is a partition on S. □

Theorem 1.1 (Orbit-Stabilizer Theorem)**.** *Let $\varphi\colon G \times S \to S$ be an action of the group G on the set S. Then for all $s \in S$,*

$$\left|G(s)\right| = \frac{|G|}{|G_s|}.$$

Proof. Define $\theta\colon G/G_s \to G(s)$ by $\theta(G_s a) = \varphi(a^{-1}, s)$. Let $G_s a, G_s b \in G/G_s$ and assume that $G_s a = G_s b$. Then $\theta(G_s a) = \varphi(a^{-1}, s)$ and $\theta(G_s b) = \varphi(b^{-1}, s)$. Recall that, by (??), $G_s a = G_s b$ iff $ab^{-1} \in G_s$. Thus, $\varphi(ab^{-1}, s) = s$. Substituting in for s, we get that $\varphi(a^{-1}, s) = \varphi(a^{-1}, \varphi(ab^{-1}, s))$. Since φ is an action, then $\varphi(a^{-1}, s) = \varphi(a^{-1}ab^{-1}, s) = \varphi(b^{-1}, s)$. Thus, $\varphi(a^{-1}, S) = \varphi(b^{-1}, s)$. Thus, $\theta(G_s a) = \theta(G_s b)$. Hence, θ is well-defined.

Now assume that $\theta(G_s a) = \theta(G_s b)$. Then $\varphi(a^{-1}, s) = \varphi(b^{-1}, s)$. Since φ is an action, then $\varphi(e, s) = s$. Thus, $\varphi(aa^{-1}, s) = s = \varphi(bb^{-1}, s)$. Thus, we have that $\varphi(a, \varphi(a^{-1}, s)) = \varphi(b, \varphi((b^{-1}, s))$. Thus, $\varphi(a, \varphi(b^{-1}, s)) = \varphi(ab^{-1}, s) = s$. Thus, $ab^{-1} \in G_s$. Thus, $G_s a = G_s b$. Hence, θ is 1-1.

Let $\varphi(g, s) \in G(s)$. Then $\theta(G_s g^{-1}) = \varphi((g^{-1})^{-1}, s) = \varphi(g, s)$. Thus, θ is onto. Thus, θ is a well-defined bijection from G/G_s to $G(s)$. Therefore,

$$\left|G(s)\right| = \frac{|G|}{|G_s|}.$$

□

Proposition 1.16. If $\varphi\colon G \times S \to S$ is an action of a group G on a set S. Then $G_s \subseteq_g G$.

Proof. It follows from the (ii) of Definition 1.1 that $\varphi(e, s) = s$ and so $e \in G_s$. Thus, $G_s \neq \varnothing$. Now let $a, b \in G_s$. Then we have that $\varphi(a, s) = s = \varphi(b, s)$. Thus, $\varphi(e, s) = s$ and so $\varphi(b^{-1}b, s) = \varphi(b^{-1}, \varphi(b, s)) = \varphi(b^{-1}, \varphi(a, s)) = \varphi(b^{-1}a, s) = s$. Thus, $\varphi(a, s) = \varphi(a, \varphi(b^{-1}a, s)) = \varphi(ab^{-1}, \varphi(a, s)) = \varphi(ab^{-1}, s) = s$. Thus, $ab^{-1} \in G_s$. Therefore, $G_s \subseteq_g G$. $\square$

Proposition 1.17. Let G be a group of order p^n and let $\varphi\colon G \times S \to S$ be an action of the group G on the set S. Then given the set

$$S_0 = \{s \in S \mid \forall g \in G\colon \varphi(g, s) = s\},$$

the following holds

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Consider the orbit of some $s \in S$. We have that $G(s) = \{\varphi(g, s) \mid g \in G\}$. Suppose that this set has one element. Then since φ is an action, we know that $\varphi(e, s) = s \in G(s)$. Thus, it follows that for all $g \in G$, $\varphi(g, s) = s$. Thus, $s \in S_0$. Similarly, if $s \in S_0$, then $\big|G(s)\big| = 1$. Thus, $\big|G(s)\big| = 1$ iff $s \in S_0$.

Now by Theorem 1.1 we can write S as the disjoint union of all of the orbits of φ. Thus, $S = S_0 \cup G(s_1) \cup \cdots \cup G(s_n)$. With $\big|G(s_i)\big| > 1$ for all i. Hence $|S| = |S_0| + \big|G(s_1)\big| + \cdots + \big|G(s_n)\big|$. Note that by Theorem 1.1, $\big|G(s_i)\big|$ divides $|G|$. Consequently, $p \mid \big|G(s_i)\big|$ for each i. Therefore, $|S| \equiv |S_0| \pmod{p}$. $\square$

Theorem 1.2 (Cauchy's Theorem)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. Let X be the set of p-tuples of groups elements

$$X = \{(a_1, \dots, a_p) \in G^p \mid a_1 \cdots a_p = e\}.$$

It follows that a_p is uniquely determined as $(a_1 \cdots a_{p-1})^{-1}$. Thus, $|X| = n^{p-1}$, where $|G| = n$. Since $p \mid n$, then $|X| \equiv 0 (\mathrm{mod}\ p)$.

Let σ be the cycle $(12 \cdots p)$ in S_p. We can let σ act on X by

$$\varphi(\sigma, (a_1, \dots, a_p)) = (a_{\sigma(1)}, \dots, a_{\sigma(p)}) = (a_2, a_3, \dots, a_p, a_1).$$

Note that $(a_2, \dots, a_p, a_1) \in X$, for $a_1(a_2 \cdots a_p) = e$ implies that $a_1 = (a_2 \cdots a_p)^{-1}$, so $(a_2 \cdots a_p)a_1 = e$ also. Thus, σ acts on X, and we consider the subgroup $\langle\sigma\rangle$ of S_p to act on X by iteration in the natural way.

Now $(a_1, a_2, \dots, a_p) \in S_0$ iff $a_1 = \cdots = a_p$; clearly, $(e, e, \dots, e) \in S_0$. Thus, $|S_0| \neq 0$. By Proposition 1.17, $|X| \equiv |S_0| \pmod{p}$. However, $|X| \equiv 0 (\mathrm{mod}\ p)$. Thus, $|S_0| \equiv 0 (\mathrm{mod}\ p)$. Thus, $p \mid |S_0|$. Thus, there exists $a \neq e$ such that $(a, a \dots, a) \in S_0$. Hence, $a^p = e$. Thus, $o(a) = p$. $\square$

Definition 1.6. A group in which every element has order a power (≥ 0) of some fixed prime p is called a ***p-group***. If H is a subgroup of a group G and H is a p-group, H is said to be a ***p-subgroup*** of G.

Corollary 1.2.1. *A finite group G is a p-group if and only if $|G|$ is a power of p.*

***Proof*.** If G is a p-group and q is a prime which divides $|G|$, then G contains an element of order q by Theorem 1.2. Since every element of G has order a power of p, then for the element of order q, it must be the case that $q = p^\alpha$. However, for any $1 \leq \alpha$, it would follow that q is not prime. Thus, $q = p$. Hence, $|G|$ is a power of p.

Assume $|G|$ is a power of p. Then take any $a \in G$ and consider the subgroup generated by a, $\langle a \rangle$. By Langrange's Theorem, it follows that $\left|\langle a \rangle\right| \mid |G|$. Thus, if we denote $|G| = p^n$, then $\left|\langle a \rangle\right| \mid p^n$. Thus, $\left|\langle a \rangle\right| = p^m$, for some $0 \leq m \leq n$. Therefore, every element of G has order (≥ 0) of p and G is thereby a p-group. $\square$

Lemma 1.2.1. *If H is a p-subgroup of a finite group G, then*

$$[N_G(H) \colon H] = [G \colon H] (mod\ p).$$

***Proof*.** Let S be the set of left cosets of H in G and define $\varphi \colon H \times S \to S$ by $\varphi(h, aH) = haH$. It is easily shown that φ is an action. Then $|S| = [G \colon H]$. Also, note that $xH \in S_0$ iff $hxH = xH$ for all $h \in H$. This is equivalent to $x^{-1}hxH = H$ for all $h \in H$. Moreover, this is equivalent to $x^{-1}hx \in H$ for all $h \in H$. Thus, $x^{-1}Hx = H$. Thus, $xHx^{-1} = H$. Hence, $x \in N_G(H)$. Therefore, $|S_0|$ is the number of cosets xH with $x \in N_G(H)$. That is, $|S_0| = [N_G(H) \colon H]$. By Proposition 1.17, $[N_G(H) \colon H] = |S_0| \equiv |S| = [G \colon H] (\text{mod } p)$. $\square$

Corollary 1.2.2. *If H is a p-subgroup of a finite group G such that p divides $[G \colon H]$, then $N_G(H) \neq H$.*

***Proof*.** Since $p \mid [G \colon H]$ then $[G \colon H] \equiv 0 (\text{mod } p)$. Additionally, by Lemma 1.2.1, we have that $[N_G(H) \colon H] \equiv [G \colon H] (\text{mod } p)$. Thus, $[N_G(H) \colon H] \equiv 0 (\text{mod } p)$. Hence, $p \mid [N_G(H) \colon H]$ and it is always the case that $[N_G(H) \colon H] \geq 1$ since $H \subseteq_g N_G(H)$. Thus, there are at least p many cosets of H in $N_G(H)$. Therefore, $N_G(H) \neq H$. $\square$

Corollary 1.2.3. *If H is a p-subgroup of a finite group G such that $p \mid [G \colon H]$, then $N_G(H) \neq H$.*

***Proof*.** By Lemma 1.2.1, $[N_G(H) \colon H] \equiv [G \colon H] (\text{mod p})$. However, $p \mid [G \colon H]$ and thus $[G \colon H] \equiv 0 (\text{mod } p)$. Hence, $[N_G(H) \colon H] \equiv 0 (\text{mod } p)$. Thus, $p \mid [N_G(H) \colon H]$. Since $H \subseteq_g N_G(H)$, then $H \in N_G(H)/H$ and $[N_G(H) \colon H] \geq 1$. Since $p \mid [N_G(H) \colon H]$, then $[N_G(H) \colon H] > 1$ and thus, $N_G(H) \neq H$, otherwise $[N_G(H) \colon H] = 1$. $\square$

Proposition 1.18. If N is a normal subgroup of a group G, then every subgroup of G/N is of the form K/N, where K is a subgroup of G that contains N. Furthermore, K/N is normal in G/N if and only if K is normal in G.

Proof. $\square$

Proposition 1.19. Let G be a group and H be a subgroup of G. Then $N_G(H) \subseteq_g G$.

Proof. Let $\varphi\colon G \times S \to S$, where S is the set of all subgroups of G, be the group action defined by conjugation, then for any $H \subseteq_g G$, $G_H = \{g \in G\colon gH = Hg\} = N_G(H)$. Then by Proposition 1.6, $G_H \subseteq_g G$. Therefore, $N_G(H) \subseteq_g G$. $\square$

Proposition 1.20. If G is a group and H is a subgroup of G. Then H is normal in $N_G(H)$.

Proof. Let $h \in H$. Then since $hH = H = Hh$, it follows that $H \subseteq N_G(H)$. Thus, since H is a subgroup of G, and by Proposition 1.19 $N_G(H)$ is a subgroup of G, then $H \subseteq N_G(H)$ implies that $H \subseteq_g N_G(H)$. Now let $g \in N_G(H)$. Then $gH = Hg$, Thus, H is normal in $N_G(H)$. $\square$

Theorem 1.3 (First Sylow Theorem)**.** *Let G be a group of order $p^n m$, with $n \geq 1$, p prime, and $(p,m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.*

Proof. Since $p \mid |G|$, then by Theorem 1.2, there exists $a \in G$ such that $o(a) = p$. Thus, we have that $\langle a \rangle \subseteq_g G$ and $o(\langle a \rangle) = p$. Proceeding by induction assume H is a subgroup of G of order p^i $(1 \leq i < n)$. Then since G is finite, by Lagrange's Theorem , $[G\colon H] = |G| / |H| = p^{n-i}$, where $0 < p - i$ and so $p \mid [G\colon H]$. Thus, by Lemma 1.2.1, $[N_G(H)\colon H] \equiv [G\colon H] \equiv 0 (\text{mod } p)$. Moreover, by Corollary 1.2.2, $N_G(H) \neq H$. Thus, $[N_G(H)\colon H] > 1$. Hence, $[N_G(H)\colon H] \equiv 0(\text{mod } p)$ implies that $p \mid [N_G(H)\colon H]$. Also note that by Proposition 1.20, $H \triangleleft N_G(H)$. Thus, $N_G(H)/H$ is a group by Proposition ??. Since p divides the order of this group, then by Theorem 1.2, there exists an element and hence a subgroup (generated by that element) of order p. By Proposition 1.18, this subgroup is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. Since H is normal in $N_G(H)$, then it follows that H is normal in H_1. Finally, $|H_1| = |H| \left| H_1/H \right| = p^i p = p^{i+1}$. $\square$

Definition 1.7. A subgroup P of a group G is said to be a ***Sylow p-subgroup*** (p prime) if P is a maximal p subgroup of G. That is, if $P \subseteq_g H \subseteq_g G$, then if H is a p-subgroup, then $P = H$.

Corollary 1.3.1. *Let G be a group of order $p^n m$ with p prime, $n \geq 1$ and $(m, p) = 1$. Let H be a p-subgroup of G.*

(i) H is a Sylow p-subgroup of G if and only if $|H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Proof.

(i) Assume that H is a Sylow p-subgroup of G. Then by Definition 1.7, H is a p-subgroup of G. Thus, by Definition 1.6, $|H| = p^i$ for some $i \geq 0$. Now assume that P is a subgroup of G of order p^n such that $H \subseteq_g P$. The subgroup P exists by Theorem 1.3. However, since H is a Sylow p-subgorup, then $H = P$. Thus, $|H| = p^n$. Now assume that $|H| = p^n$. Then by Langrange's Theorem, $|H| \mid |G|$ and $|G| / |H| = m$. Since $(m, p) = 1$, then H is a maximal p-subgroup of G. Thus, H is a Sylow p-subgroup of G.

(ii) Let P be a Sylow p-subgroup of G and let $g \in G$. Then the set $gPg^{-1} \neq \varnothing$ since $e \in P$ and thus $geg^{-1} = e \in gPg^{-1}$. Now let $a, b \in G$ and assume that $a, b \in gPg^{-1}$. Then $a = gh_1g^{-1}$ and $b = gh_2g^{-1}$ for some $h_1, h_2 \in P$. Thus, $b^{-1} = gh_2^{-1}g^{-1}$. Thus, $ab^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = g(h_1h_2^{-1})g^{-1}$. Since $h_1h_2^{-1} \in P$, then $ab^{-1} \in gPg^{-1}$. Thus, $gPg^{-1} \subseteq_g G$.

Now let $f \colon P \to gPg^{-1}$ be defined by $f(h) = ghg^{-1}$. Let $h, t \in P$ and assume $h = t$. Then $f(h) = ghg^{-1} = gtg^{-1} = f(t)$. Thus, f is well defined. Now assume that $f(h) = f(t)$. Then $ghg^{-1} = gtg^{-1}$. Thus, $gh = gt$ and so $h = t$. Hence, f is 1-1. Now let $ghg^{-1} \in gPg^{-1}$. Then $f(g) = ghg^{-1}$ and thus f is onto. Hence, f is a bijection. Therefore, $|P| = \left|gPg^{-1}\right|$. Thus, given any Sylow p-subgroup, then for any $g \in G$, the conjugate gPg^{-1} is also a Sylow p-subgroup.

(iii) Assume that there is only one Sylow p-subgroup P. Then by (ii), for all $g \in G$, gPg^{-1} is another Sylow p-subgroup. However, since there is only one, then it follows that $gPg^{-1} = P$. Thus, P is normal in G.

$\square$

Theorem 1.4 (Sylow 1, Version 2)**.** *Let G be a group of order $n = p^\alpha m$, where $1 \le \alpha$, and $(p,m) = 1$. Then there exists $H \subseteq_g G$ such that $o(H) = p^\alpha$.*

Proof. Let $\mathscr{C} = \{C \subseteq G \mid |C| = p^\alpha\}$. It follows from this definition that $|\mathscr{C}| = \binom{n}{p^\alpha}$. Expanding this out, we see that

$$|\mathscr{C}| = \frac{n!}{(n-p^\alpha)!(p^\alpha)!}.$$

After cancelling out the appropriate terms, we obtain

$$|\mathscr{C}| = \frac{n(n-1)\cdots(n-p^\alpha+1)}{p^\alpha(p^\alpha-1)\cdots(p^\alpha-p^\alpha+1)} = \prod_{k=0}^{p^\alpha-1} \frac{(n-k)}{(p^\alpha-k)}.$$

We will replace n with $p^\alpha m$ and we note that for each $0 \le k \le p^\alpha - 1$, we can write $k = p^i L$, where $0 \le i < \alpha$ is the highest power of p that occurs in the prime factorization of k. It also follows that $p \nmid L$. Using these substitutions, the above equality becomes

$$|\mathscr{C}| = \prod_{k=0}^{p^\alpha-1} \frac{(p^\alpha m - p^i L)}{(p^\alpha - p^i L)} = \prod_{k=0}^{p^\alpha-1} \frac{(p^{\alpha-i} m - L)}{(p^{\alpha-i} - L)} = \frac{\prod_{k=0}^{p^\alpha-1}(p^{\alpha-i}m - L)}{\prod_{k=0}^{p^\alpha-1}(p^{\alpha-i} - L)}.$$

Now let $p^{\alpha-i}m - L$ be any single term in the product $\prod_{k=0}^{p^\alpha-1}(p^{\alpha-i}m - L)$. Since $i < \alpha$ and $1 < \alpha$, then $1 \le \alpha - i$ and thus, $p \mid (p^{\alpha-i}m)$. However, as stated earlier, $p \nmid L$. Thus, $p \nmid (p^{\alpha-i}m - L)$. Since $p^{\alpha-i}m - L)$ was arbitrary, then it follows that

$$p \nmid \left(\prod_{k=0}^{p^\alpha-1}(p^{\alpha-i}m - L\right).$$

Thus,

$$p \nmid \left(\frac{\prod_{k=0}^{p^\alpha-1}(p^{\alpha-i}m - L)}{\prod_{k=0}^{p^\alpha-1}(p^{\alpha-i} - L)}\right).$$

Therefore, $p \nmid |\mathscr{C}|$.

Now define the group action (prove) $\varphi\colon G \times \mathscr{C} \to \mathscr{C}$ by $\varphi(g, C) = gC$. By Proposition 1.15, we can partition $\mathscr{C}$ by the collection of orbits of φ. Thus, it follows that

$$|\mathscr{C}| = \sum_{C \in \mathscr{C}} \left|G(\hat{C})\right|.$$

Since $p \nmid |\mathscr{C}|$, then there exists $\hat{C} \in \mathscr{C}$ such that $p \nmid \left|G(\hat{C})\right|$. By Theorem 1.1,

$$\left|G(\hat{C})\right| = \frac{|G|}{\left|G_{\hat{C}}\right|} = \frac{p^{\alpha} m}{\left|G_{\hat{C}}\right|}.$$

Thus, $\left|G(\hat{C})\right|\left|G_{\hat{C}}\right| = p^{\alpha} m$. However, since $p \nmid \left|G(\hat{C})\right|$, then it follows that $p^{\alpha} \nmid \left|G(\hat{C})\right|$. Thus, $p^{\alpha} \mid \left|G_{\hat{C}}\right|$. Now let $x \in \hat{C}$, then it follows that $G_{\hat{C}}x \subseteq C$. Recall that $\left|\hat{C}\right| = p^{\alpha}$. Thus, $\left|G_{\hat{C}}x\right| = \left|G_{\hat{C}}\right| \leq \left|\hat{C}\right| = p^{\alpha}$. Thus, if $p^{\alpha} \mid \left|G_{\hat{C}}\right|$ and $\left|G_{\hat{C}}\right| \leq p^{\alpha}$, then it follows that $\left|G_{\hat{C}}\right| = p^{\alpha}$. By Proposition 1.16, $G_{\hat{C}} \subseteq_g G$. Therefore, there exists a subgroup, namely $G_{\hat{C}}$ of G with order p^{α}. □

Theorem 1.5 (Second Sylow Theorem)**.** *If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $H \subseteq xPx^{-1}$. In particular, any two Sylow p-subgroups are conjugate.*

***Proof*.** Let S be the set of left cosets of P in G and let $\varphi\colon H \times S \to S$ be an action defined by $\varphi(h, aP) = haP$. Then by Proposition 1.17, $|S| \equiv |S_0| \pmod{p}$. Since $|S| = [G\colon P]$, then $|S_0| \equiv [G\colon P] \pmod{p}$. But since P is a Sylow p-subgroup of G, then $|P| = p^n$, where p^n is the highest power of p that occurs in the prime factorization of $|G|$. Thus, $p \nmid [G\colon P]$. Hence, $p \nmid |S_0|$. Thus, $|S_0| \neq \varnothing$ and there exists $xP \in S_0$. Thus, by definition of S_0, $xP \in S$ and for all $h \in H$, $hxP = xP$. Thus, $x^{-1}hxP = P$ for all $h \in H$. Thus, since $x^{-1}hx \in x^{-1}Hx$, then $x^{-1}Hx \subseteq P$. Moreover, since $x^{-1}Hx \subseteq_g G$, then $x^{-1}Hx \subseteq_g P$. Thus, $H \subseteq_g xPx^{-1}$. Hence, if H is a Sylow p-subgroup, $|H| = |P| = \left|xPx^{-1}\right|$. Thus, $H = xPx^{-1}$. □

Theorem 1.6 (Third Sylow Theorem)**.** *If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.*

***Proof*.** By Theorem 1.5, the number of Sylow p-subgroups is the number of conjugates of any one of them, say P. But this number is $[G\colon N_G(P)]$. Since, $|G| = \left(|G| / \left|N_G(P)\right|\right)\left|N_G(P)\right|$. Hence, $[G\colon N_G(P)]$ is a divisor of $|G|$. Thus, the number of Sylow p-subgroups is a divisor of G. Now let $\gamma\colon P \times \mathrm{Syl}_P(G) \to \mathrm{Syl}_P(G)$ be the action of conjugation. Then assume $Q \in S_0$. Then $Q \in \mathrm{Syl}_P(G)$ and for all $g \in P$, $gQg^{-1} = Q$. Now consider $N_G(Q) = \{g \in G \mid gQg^{-1} = Q\}$. It follows that $P \subseteq_g N_G(Q)$. Since both P and Q are Sylow p-subgroups of G and hence of $N_G(Q)$ and are therefore conjugate in $N_G(Q)$. But since by Proposition 1.20, Q is normal in $N_G(Q)$. Thus, for all $g \in N_G(Q)$, $gQg^{-1} = Q$. Thus, $P = Q$. Hence, $S_0 = \{P\}$. By Proposition 1.17, $\left|\mathrm{Syl}_P(G)\right| \equiv |S_0| = 1 \pmod{p}$. Thus, $\left|\mathrm{Syl}_P(G)\right| = kp + 1$. □

2 Results To Be Proven and Applications

Proposition 2.1. If G is a finite group, $H \subseteq_g G$, $H \neq G$, and $o(G) \nmid [G\colon H]!$, then H contains a nontrivial normal subgroup of G.

Proof. $\square$

Proposition 2.2. If G is a finite group, $H \subseteq_g G$, $[G\colon G] = p$, p is prime, and p is the smallest prime factor of $o(G)$, then $H \triangleleft G$.

Proof. $\square$

Proposition 2.3. If $H \subseteq_g G$ and $N \triangleleft G$, then $HN = NH$ is a subgroup of G, and $o(HN) = o(H)o(N)/o(H \cap N)$. Therefore, if $H \cap N = \{e\}$, then $o(HN) = o(H)o(N)$.

Proof. $\square$

Proposition 2.4. If $N \triangleleft G$ and $M \triangleleft G$ and $N \cap M = \{e\}$, then $NM \cong N \times M$.

Proof. $\square$

Proposition 2.5. Assume that $G = \langle a \rangle$, and $o(G) = n$. Prove that $\mathrm{Aut}(G) \cong (\mathbb{Z}_{(n)}, \odot)$.

Proof. Let $f\colon \mathrm{Aut}(G) \to \mathbb{Z}_{(n)}$ be defined as $f(\theta) = [k]$ where $\theta(a) = a^k$, where $k \in \mathbb{Z}$ such that $(n, k) = 1$. By definition, f is defined over $\mathrm{Aut}(G)$. Next, we will check if f is well defined. Let $\theta, \gamma \in \mathrm{Aut}(G)$ and assume $\theta = \gamma$. Then we want to show that $f(\theta) = f(\gamma)$. We have that $\theta(a) = a^i$ and $\gamma(a) = a^j$. Thus, $f(\theta) = [i]$ and $f(\gamma) = [j]$. Since $\theta = \gamma$, then $a^i = a^j$. Thus, $\theta(a) = a^j$. Hence, $f(\theta) = [j] = f(\gamma)$. So f is well defined.

Now assume that $f(\theta) = f(\gamma)$. Then $[i] = [j]$. Thus, $i \in [j]$ and so there exists some $m \in \mathbb{Z}$ such that $i = mn + j$. Thus, $a^i = a^{mn+j} = a^{mn}a^j = a^j$. It follows that $\theta(a) = \gamma(a)$, and since a generates G, then $\theta = \gamma$. Hence, f is 1-1.

Now let $[k] \in \mathbb{Z}_{(n)}$. Now consider some φ whose domain is G, where $\varphi(a) = a^k$. Then we want to show that $\varphi \in \mathrm{Aut}(G)$. By definition, $\mathrm{ran}(\varphi) \subseteq G$ and so $\varphi\colon G \to G$. Now assume that $x, y \in G$ and that $x = y$. Then since $G = \langle a \rangle$, then $x = a^s$ and $y = a^t$, for some $s, t \in \mathbb{Z}$. Thus, $\varphi(x) = \varphi(a^s) = (a^s)^k$, and $\varphi(y) = \varphi(a^t) = (a^t)^k$. But since $a^s = a^t$, then $(a^s)^k = (a^t)^k$. Thus, $\varphi(x) = \varphi(y)$. Thus, φ is well defined. Now let $a^i, a^j \in G$. Then $\varphi(a^i a^j) = \varphi(a^{i+j}) = (a^{i+j})^k = a^{ik}a^{jk} = \varphi(a^i)\varphi(a^j)$. Thus, φ is a homomorphism. Now assume $\varphi(x) = \varphi(y)$. Thus, $(a^s)^k = (a^t)^k$, for some $s, t \in \mathbb{Z}$. Thus, $a^{k(s-t)} = e$. Then $n \mid k(s - t)$, Since $(n, k) = 1$, then $n \mid (s - t)$. Thus, $s = qn + t$, for some $q \in \mathbb{Z}$. Thus, $a^s = a^{qn+t} = a^{qn}a^t = a^t$. Hence, $x = y$ and φ is 1-1. Since $(n, k) = 1$, then $\langle a \rangle = \langle a^k \rangle$. Thus, φ is onto. Therefore, $\varphi \in \mathrm{Aut}(G)$ and $f(\varphi) = [k]$. Thus, f is onto.

Now we want to show that f is a homomorphism. Let $\theta, \gamma \in \mathrm{Aut}(G)$ and suppose $\theta(a) = a^i$ and $\gamma(a) = a^j$. Then we have that $(\theta \circ \gamma)(a) = \theta(\gamma(a)) =$

$\theta(a^j) = (a^j)^i = a^{ji}$. Then $f(\theta \circ \gamma) = [ji] = [j] \odot [i] = f(\gamma) \odot f(\theta) = f(\theta) \odot f(\gamma)$. Thus, f is a homomorphism. Therefore, f is an isomorphism. Hence, $\mathrm{Aut}(G) \cong (\mathbb{Z}_{(n)}, \odot)$. □

Proposition 2.6. If $H \subseteq_g G$, $N \triangleleft G$, $H \cap N = \{e\}$, and $G = HN$, then for every $x \in G$, there exist unique elements $h \in H$ and $n \in N$ such that $x = hn$.

Proof. □

Remark. By Proposition 2.6, if there exist $h' \in H$, $n' \in N$ such that $x = h'n'$, then $hn = h'n'$. Thus, $h'^{-1}h = n'n^{-1}$. Since $h'^{-1}h \in H$ and $n'n^{-1} \in N$, then $h'^{-1}h \in H \cap N$ and $n'n^{-1} \in H \cap N$. But $H \cap N = \{e\}$. Thus, $h'^{-1}h = e$ and $n'n^{-1} = e$. Thus, $h = h'$ and $n = n'$.

Thus, if $x, y \in G$, then there exist unique elements $g, h \in H$ and $m, n \in N$ such that $x = gm$ and $y = hn$, and $xy = gmhn = gh(h^{-1}mh)n$. Now define $\sigma_h \colon N \to N$ by $\sigma(h) = hnh^{-1}$, then by Proposition 1.11, $\sigma_h \in \mathrm{Aut}(N)$. Note that xy can be written as $xy = gh(\sigma_{h^{-1}}(m))n$. Now define $\alpha \colon H \to \mathrm{Aut}(N)$ by $\alpha(h) = \sigma_h$, then by Proposition 1.11, α is a homomorphsim. Conversely, given any homormorphism $\theta \colon H \to \mathrm{Aut}(N)$, we can determine the structure of HN by determining the possible values of $\theta(h)$.

Assume that $o(a) = n$. Recall that by Proposition 2.5, $\mathrm{Aut}(\langle a \rangle) \cong \mathbb{Z}_{(n)}$. Thus, $\mathrm{Aut}(\langle a \rangle) = \{\varphi_k \colon (n, k) = 1\}$, where $\varphi_k \colon \langle a \rangle \to \langle a \rangle$ is defined by $\varphi_k(x) = x^k$.

Example 2.1. Let $N = \langle d \rangle$, $o(d) = m$, and let $H = \langle a \rangle$, $o(a) = 2$. Then $\mathrm{Aut}(N) = \{\varphi_k \colon (k, m) = 1\}$, where $\varphi_k(x) = x^k$. Assume that $\theta \colon H \to \mathrm{Aut}(N)$ is a homomorphism, and that $\theta(h) = \varphi_k$.

If $h = e$, then since θ is a homomorphism, it must map identities to identities. Thus, $\theta(h) = i_N$. If $h = a$, then since $o(a) = 2$, then $o(\theta(a)) \mid 2$. Thus, $o(\theta(a)) = 1$ or $o(\theta(a)) = 2$. Thus, if $\theta(a) = \varphi_k$, then it follows that $\varphi_k^2 = i_N$. But also $(\varphi_k)^2(x) = \varphi_k(\varphi_k(x)) = \varphi_k(x^k) = (x^k)^k = x^{k^2} = \varphi_{k^2}(x)$. Thus, $\varphi_{k^2} = i_N$.

If $m = 3$, then $\mathrm{Aut}(N) = \{\varphi_k \colon (3, k) = 1\} = \{\varphi_1, \varphi_2\}$. Moreover, $\varphi_{1^2} = \varphi_1 = i_N$ and $\varphi_{2^2} = \varphi_4 = \varphi_1 = i_N$. Thus, both φ_1 and φ_2 work.

If $m = 5$, then $\mathrm{Aut}(N) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$. However, $\varphi_{2^2} = \varphi_4 \neq i_N$, and $\varphi_{3^2} = \varphi_9 = \varphi = \varphi_4 \neq i_N$. Thus, only φ_1 and φ_4 work.

Example 2.2. Let G be a group of order 6. Then since $6 = 2 \times 3$, by Theorem 1.6 the number of Sylow 2-subgroups, n_2 is congruent to 1 modulo 2 and the number of Sylow 3-subgroups is congruent to 1 modulo 3. Additionally, the number of Sylow 2-subgroups divides $|G| = 6$ and the number of Sylow 3-subgroups divides $|G| = 6$. Thus, $n_2 \equiv 1 (\mathrm{mod}\ 2)$, $n_2 \mid 6$, $n_3 \equiv 1 (\mathrm{mod}\ 3)$, and $n_3 \mid 6$. Thus, Since 6 has factors 1, 2, 3, and 6. Then amongst these, 1 and 3 are congruent to 1 modulo 2. Thus, $n_2 = 1$ or $n_2 = 3$. Similarly, amongst the factors 1, 2, 3, and 6, those of which are congruent to 1 modulo 3 is just 1. Thus, $n_3 = 1$. Hence, by (iii) of Corollary 1.3.1, $P_3 \triangleleft G$, where P_3 is the Sylow 3-subgroup.

Assume that $n_2 = 1$, then $P_2 \triangleleft G$, then by Proposition 2.4, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ since any groups whose order is less than or equal to 5 is abelian, and any finite abelian group of order n is isomorphic to $\mathbb{Z}_n$. Thus, G is cyclic.

Now assume that $n_2 = 3$. Then since $P_2 \cap P_3 = \{e\}$ (since P_2 contains the identity and an element of order 2, and P_3 contains the identity and 2 elements of order 3) and $G = P_2 P_3$ by Proposition ??. Additionally, $\mathrm{Aut}(P_3) = \{\varphi_1, \varphi_2\}$. Let $P_2 = \langle a \rangle$ and $P_3 = \langle b \rangle$. Then since $P_3 \triangleleft G$, $aba^{-1} \in \langle b \rangle$. Thus, $\varpi_1(aba^{-1}) = \varphi_1(a) b \varphi_1(a^{-1}) = \varphi_1(a) b (\varphi_1(a))^{-1}$. We have three choices for $\varphi_1(a)$. It can map to e, b, or b^2. If it maps to e, then that would imply $a = e$ which is not the case since it generates P_2. It can map to b, but that $\varphi_1(a) = b = \varphi_1(b)$ and since φ_1 is 1-1, then $a = b$ but this too is a contradiction. Thus, $\varphi_1(a) = b^2$. Hence, $\varphi_1(aba^{-1}) = b^2 b b^{-2} = b$. Thus, $aba^{-1} = b$ which implies that $ab = ba$. Therefore, G is abelian. Thus, $P_2 \triangleleft G$ and $G \cong \mathbb{Z}_6$. φ_2 gives us $aba^{-1} = b^2$ and thus, $ab = b^{-1}a$. Thus, $G \cong D_6$.

Theorem 2.1. *For each $n \geq 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy:*

(i) $a^n = (1)$; $a^k \neq (1)$ *if* $0 < k < n$;

(ii) $ba = a^{-1}b$.

Any group which is generated by element s$a, b \in G$ satisfying (i) and (ii) for some $n \geq 3$ (which $e \in G$ in place of (1)) is isomorphic to D_n.

Proof. □

Proposition 2.7. Let p and q be primes such that $p > q$. If $q \nmid p - 1$, then every group of order pq is isomoarphic to the cyclic group $\mathbb{Z}_{pq}$. If $q \nmid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq: the cyclic group $\mathbb{Z}_{pq}$ and a non-abelian group K generated by elements c and d such that

$$|c| = p; \quad |d| = q; \quad dc = c^s d,$$

where $s \not\equiv 1 (\text{mod p})$ and $s^q \equiv 1 (\text{mod } p)$.

Proof. □

Example 2.3. Let G be a group of order 6. Then by Cauchy's Theorem, G contains elements a and b of order 2 and 3 respectively. Thus, G has subgroups $\langle a\rangle$ and $\langle b\rangle$ of orders 2 and 3. It is clear that $\langle a\rangle$ is a 2-Sylow subgroup of G and $\langle b\rangle$ is a 3-Sylow subgroup of G. By Theorem 1.6, $n_2 \equiv 1 (\mathrm{mod}\ 2)$, $n_2 \mid 3$, $n_3 \equiv 1 (\mathrm{mod}\ 3)$, and $n_3 \mid 2$. From these relations it follows that $n_2 = 1$ or $n_2 = 3$, and $n_3 = 1$. Thus, letting $\langle a\rangle$ denote a 2-Sylow subgroup and $\langle b\rangle$ denote the 3-Sylow subgroup, from $n_3 = 1$ it follows that $\langle b\rangle \triangleleft G$. Note that for any $x \in \langle a\rangle \cap \langle b\rangle$, the order of x must divide both 2 and 3. Thus, $o(x) = 1$ and $\langle a\rangle \cap \langle b\rangle = \{e\}$. Hence, by Proposition 2.3, $o(\langle a\rangle\langle b\rangle) = 6$, and since $\langle a\rangle\langle b\rangle \subseteq_g G$, then $G = \langle a\rangle\langle b\rangle$.

Now assume that $\theta\colon \langle a\rangle \to \mathrm{Aut}(\langle b\rangle)$ is a homomorphsism, where $\theta(a^k) = \varphi_k$ and $\varphi_k(b) = a^k b a^{-k}$. TBC ...