**Theorem 1** (The unit element is unique)**.** Let $G$ be a group and $\star$ its binary operation. Suppose that $e_1, e_2 \in G$ are both units elements. Then, $e_1 = e_2$.

**Theorem 2** (Cancellation Law)**.** For every group $G$ and $a, b, c \in G$ that satisfy $ab = ac$, we have $b = c$.

**Theorem 3** (The inverse of a group element is unique)**.** Let $G$ be a group and let $a \in G$. If $b$ and $c$ are inverses of $a$, then $b = c$.

**Theorem 4.** The order of a $k$-cycle is $k$.

**Theorem 5.** Disjoint cycles commute.

**Theorem 6** (Basic facts about homomorphisms)**.** Let $\phi : G \to H$ be a homomorphism. Then

1. $\phi(1_G) = 1_H$ (the identity of $G$ is mapped to the identity of $H$).
2. $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.

**Theorem 7.** Let $\phi : G \to H$ be a homomorphism. Then $Im(\phi) = \{\phi(g) | g \in G\} \leq H$.

**Theorem 8.** Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi) \leq G$. That is, the kernel of $\phi$ is a subgroup of $G$.

**Theorem 9** (All left cosets of $H$ have the same size)**.** Let $H \leq G$ be groups and let $a \in G$. Then $|[a]| = |aH| = |H|$

**Theorem 10** (Lagrange)**.** Let $G$ be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

**Theorem 11** (Equivalent conditions to be a normal subgroup)**.** Let $N \leq G$. Then $N \trianglelefteq G$ if one of the following holds:

1. $\forall g \in G$, $gN = Ng$
2. $\forall g \in G$, $gNG^{-1} = N$
3. $\forall g \in G$, $gNg^{-1} \subseteq N$
4. $\forall g \in G$ and $\forall n \in N$, $gng^{-1} \in N$

**Theorem 12** (The Kernal of a Homomorphism is a Normal Subgroup)**.** Let $\phi : G \to H$ be homomorphism. Then $\ker(\phi) \trianglelefteq G$.

**Theorem 13** (Every cyclic group is isomorphic to either $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$.)**.** For every group $H$ for which there exists an $x \in H$ such that $H = \langle x \rangle$, there exists a bijective homomorphism (i.e. an isomorphism) $\phi : H \to C$ where $C = \mathbb{Z}$ or $C = \mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$.

**Theorem 14.** Let $G$ be a finite cyclic group of order $n$. For every $m|n$ ($m$ that divides $n$) there exists a unique subgroup $H$ of $G$ with $|H| = m$. Furthermore, $H$ is cyclic.

**Theorem 15** (Important Identity for Dihedral Groups)**.** $\rho\epsilon = \epsilon\rho^{-1}$.

**Theorem 16.** $\rho^i\epsilon = \epsilon\rho^{-i}$

**Theorem 17.** In the above definition, $G/N$ is a group.

**Theorem 18** (The First Isomorphism Theorem)**.** If $\phi : G \to H$ is a homomorphism of groups, then $G/\ker(\phi) \cong Im\phi$.

**Theorem 19** (The Second or Diamond Isomorphism Theorem)**.** Let $H \leq G$ and $K \trianglelefteq G$. Then $HK/K \cong H/H \cap K$.

**Theorem 20** (The stabilizer of a group element is a subgroup)**.** $G_x \leq G$

**Theorem 21** (Orbit-Stabilizer Theorem)**.** There is a bijection

$$f : G/G_x \to O_x \tag{1}$$

In words, there is a bijection between the collection of all cosets of the stabilizer and the orbit. In particular,

$$[G : G_x] = |O_x| \tag{2}$$

(Recall we defined $|G/G_x|$ to be $[G : G_x]$).

**Theorem 22.** An action is transitive if and only if there exists an $x \in X$ such that $O_x = X$. That is, all elements of $X$ have the same equivalence class.

**Theorem 23** (Burnside)**.** Let $G$ act on $X$. Suppose that $G, X$ are finite. Then,

$$N = \text{ \# of orbits (equivalence classes) } = \frac{1}{|G|} \sum_{g \in G} |X^g| \tag{3}$$

**Theorem 24.** $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is a group.

**Theorem 25** (Fermat's Little Theorem)**.** For a prime number $p$ and $1 \leq x \leq p-1$, we have $x^{p-1} - 1$ is divisible by $p$.

**Theorem 26.** Let $p \neq q$ be odd primes. Then

$$(\mathbb{Z}/pq\mathbb{Z})^{\times} \cong (\mathbb{Z}/p\mathbb{Z})^{\times} \times (\mathbb{Z}/q\mathbb{Z})^{\times} \tag{4}$$

**Theorem 27.** If $\lambda : G \to S_n$ is a homomorphism, we can define an action of $G$ on $\{1, \ldots, n\}$ by

$$g(i) = \lambda(g)(i) \tag{5}$$

**Theorem 28.** Under the above assumptions: $\lambda$ is injective if and only if the action of $G$ on $X$ (which we can think of as $\{1, \ldots, n\}$) is faithful.

**Theorem 29** (Cayley)**.** Let $G$ be a group of order $n$. Then, there exists an injective homomorphism $\phi : G \to S_n$.

**Theorem 30.** If $|G| = n$, then $G$ is isomorphic to a subgroup of $S_n$. Indeed $\phi : G \to Im(\phi) \subset S_n$.

**Theorem 31.** Let $G$ be a $p$-group that acts on a finite set $X$. Let $X^G = \cap_{g \in G} X^g$ where $X^g = \{x \in X | gx = x\}$, that is those $x \in X$ such that for all $g \in G$, $gx = x$. Then $p$ divides $|X| - |X^G|$, that is

$$|X^G| \equiv |X| \quad (mod p) \tag{6}$$

**Theorem 32** (A $p$-group has a non-trivial center)**.** Let $G$ be a $p$-group. Then $Z(G) \neq \{1\}$. In words, there has to be a non-trivial element of the group that commutes with everything else.

**Corollary 1.** Let $p$ be a prime number and let $G$ be a group of order $p^2$. Then $G$ is abelian.

**Theorem 33** (Cauchy)**.** Let $G$ be a finite group and suppose that $p \big| |G|$ for some prime $p$. Then there exists an element of order $p$ in $G$.

**Theorem 34** (Correspondence Theorem)**.** Let $G, H$ be groups, and let $\phi : G \to H$ be a group homomorphism. Then there exists a correspondence (i.e. a bijection)

$$\{\text{Subgroups } K \text{ of } G \text{ containing } \ker\phi\} \iff \{\text{Subgroups } L \text{ of } H \text{ contained in } Im(\phi)\}$$

given by $K \mapsto \phi(K)$ and $L \mapsto \phi^{-1}(L)$. In addition, let $K_1$ and $K_2$ be subgroups of $G$ containing $\ker(\phi)$ and $L_1$ and $L_2$ subgroups $L$ of $H$ contained in $Im(\phi)$.

1. $K_1 \leq K_2 \implies \phi(K_1) \leq \phi(K_2)$
2. $L_1 \leq L_2 \implies \phi^{-1}(L_1) \leq \phi^{-1}(L_2)$

and

1. $K_1 \leq K_2 \implies [K_2 : K_1] = [\phi(K_2) : \phi(K_1)]$
2. $L_1 \leq L_2 \implies [L_2 : L_1] = [\phi(L_2) : \phi(L_1)]$

**Theorem 35** (Sylow's Theorem)**.** Let $p$ be a prime number, let $G$ be a finite group, and let $p^n$ be the largest power of $p$ that divides $|G|$. Then $G$ contains a subgroup $P$ of order $p^n$. $P$ is called a $p$-Sylow subgroup of $G$.

**Theorem 36** ($p$-Sylow subgroups are conjugate)**.** Let $G$ be a finite group and let $P, Q$ be $p$-Sylow subgroups of $G$. Then there exists $g \in G$ such that $gPg^{-1} = Q$.

**Corollary 2.** Let $G$ be a finite group and let $P$ be a $p$-Sylow subgroup of $G$. Then $P$ is a unique $p$-Sylow subgroup if and only if $P \trianglelefteq G$.

**Theorem 37** ($0 \cdot a = 0$)**.**

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a && \text{(0 additive identity)} \\ &= 0 \cdot a + 0 \cdot a && \text{(distributivity)} \end{aligned}$$

Then cancellation gives $0 = 0 \cdot a$.

**Theorem 38** ($-a = (-1) \cdot a$)**.** We want to show that $(-1) \cdot a$ is the additive inverse of $a$. To that end

$$\begin{aligned} a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{(1 multiplicative identity)} \\ &= (1 + -1) \cdot a && \text{(distributivity)} \\ &= 0 \cdot a \\ &= 0 \end{aligned}$$