Algebra so Far (so Good)

Notation.

$\boldsymbol{x \in X}$.	x is an **element** of the set X. Note: lower-case for elements, upper-case sets
$\boldsymbol{X \subset Y}$.	X is a **subset** of Y if every $x \in X$ is also $x \in Y$.
$\boldsymbol{H < G}$.	H is a **subgroup** of G if it is a subset and also it is a group (using the same group law).
$\boldsymbol{N \lhd G}$.	N is a **normal subgroup** of G if it is a subgroup and also its cosets are a group!
$\boldsymbol{G/N}$.	The **group of cosets** for a normal subgroup is called the **quotient group**. Elements $g \in G$ are **representatives** for their coset $[g] = gN \in G/N$

Definitions.

Definition. **Union**, **intersection**, and **difference** of sets are defined as follows.

(Union) $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

(Intersection) $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

(Difference) $A \setminus B = \{x \mid x \in A \text{ but } x \notin B\}$

Definition. A set map $f : A \to B$ is an **injection** if it has the following property.
If $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$.

Definition. A map $f : A \to B$ is an **surjection** if it has the following property.
For each $b \in B$ there is at least one $a \in A$ with $f(a) = b$.

Definition. A map $f : A \to B$ is a **bijection** if it is both an injection and a surjection.
In this case we say A and B are **isomorphic** sets, written $A \cong B$.

Definition. The **product** of two sets is $A \times B = \{(a, b) \mid a \in A, \text{ and } b \in B\}$.

Definition. An **equivalence relation** on a set X is $\square \sim \square$ satisfying the following three properties.

(Reflexive) $x \sim x$ for all $x \in X$.

(Symmetric) If $x \sim y$, then $y \sim x$.

(Transitive) If $x \sim y$ and $y \sim z$, then $x \sim z$.

Definition. An **equivalence class** is a subset of all elements of X equivalent to a given element.
$[x] = \{k \in X \mid k \sim x\}$

Definition. The set of unique equivalence classes of an equivalence relation is written $X/\!\sim \; = \big\{[x] \;\big|\; x \in X\big\}$.
This is called the "**quotient set** X modulo the equivalence".

Definition. A **group** is a set G with a **binary operation** $\circ : G \times G \to G$ satisfying the following.

(Associative) $\big(a \circ b\big) \circ c = a \circ \big(b \circ c\big) \qquad = a \circ b \circ c$

(Identity Exists) There is an **identity element** $e \in G$ with $e \circ g = g \circ e = g$ for all $g \in G$.

(Inverses Exist) Every element $g \in G$ has an **inverse** $g^{-1} \in G$ with $g^{-1} \circ g = g \circ g^{-1} = e$.

Definition. If $ab = ba$ for all $a, b \in G$ then we say G is "**commutative**" or "**abelian**".

Definition. The product $[a, b] = aba^{-1}b^{-1}$ is called the **commutator** of a and b.

Definition. The product aba^{-1} is called the **conjugate** of b by a.

Definition. The **center** of a group is $Z(G) = \{g \mid g \text{ commutes with all elements of } G\}$.

Definition. A **subgroup** of a group is a subset which is also a group using the same group operation.

Definition. The **product** of two groups is $H \times G$ with operation $(h_1,\, g_1) \circ_\times (h_2,\, g_2) = (h_1 \circ_H h_2,\;\; g_1 \circ_G g_2)$.

Definition. A **permutation** of a nonempty set X is a bijection $\sigma : X \xrightarrow{\cong} X$.
The **permutation group** on X is $S_X = \big\{\sigma : X \xrightarrow{\cong} X\big\}$ using composition as the group operation.

Definition. The n^{th} symmetric group is $S_n = S_{\{1,2,\ldots n\}}$.

Definition. A **cycle**, written as an **ordered list** of **distinct** set elements, corresponds to the permutation which maps each element to the next element in the list, cycling the last element back to the first. Elements which are not included in the list are not changed.

Definition. A **swap** or **transposition** is a permutation whose only effect is to exchange two elements.
A permutation is **even** if it decomposes as a product of an even number of swaps.
A permutation is **odd** if it decomposes as a product of an odd number of swaps.

Definition. The **alternating group**, $A_n < S_n$ is the subgroup of **even** permutations.

Definition. Two groups are **isomorphic** if there is a set bijection between them which preserves all group structure.

Definition. The **cyclic subgroup** generated by an element $a \in G$ is $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

Definition. A group G is **cyclic** if there is $a \in G$ such that $G = \langle a \rangle$.

Definition. The **order of a group** is the number of elements it contains (as a set), $|G| = \#G$.

Definition. The **order of an element** $a \in G$ is the order of the subgroup it generates, $|a| = |\langle a \rangle|$.

Definition. For each $g \in G$, a subgroup $H < G$ has

$$\textbf{left coset} \quad gH = \{gh \mid h \in H\} \quad \text{and} \quad \textbf{right coset} \quad Hg = \{hg \mid h \in H\}.$$

Definition. The **index** of a subgroup H in a group G is $[G : H] = \dfrac{|G|}{|H|}$ = "number of cosets of H in G".

Definition. Given subgroups $H, K < G$ the **product set** is $HK = \{hk \in G \mid h \in H,\ k \in K\}$.

Definition. A **normal subgroup** H of G (written $H \lhd G$) is a subgroup where $\boldsymbol{gH = Hg}$ for all $g \in G$.

Definition. If $H < G$, define the **quotient set** $G/H = G/\!\sim$ where $a \sim b$ if $a = hb$ for some $h \in H$.

Class Presentations.

Proposition [Treston]. *If $A \xrightarrow{f} B \xrightarrow{g} C$ and $g \circ f$ is an injection, then f is an injection.*

Proposition [Kimi-Lee]. *If $A \xrightarrow{f} B \xrightarrow{g} C$ and $g \circ f$ is a surjection, then g is a surjection.*

Proposition [Known]. *For $e \in G$ we have $e^{-1} = e$.*

Proposition [Dariely]. *If $e_1, e_2 \in G$ both satisfy the property to be identity then $e_1 = e_2$.*

Proposition [Treston]. *If $g, h_1, h_2 \in G$ where both h_1 and h_2 both satisfy the property to be g^{-1} then $h_1 = h_2$.*

Proposition [Will]. *For $g, h \in G$ we have $(gh)^{-1} = h^{-1}g^{-1}$.*

Proposition [Kimi-Lee]. *For $g \in G$ we have $\left(g^{-1}\right)^{-1} = g$.*

Proposition [Known]. *If G is abelian, then $\{x \in G \mid x^2 = e\}$ is a subgroup of G.*

Proposition [Treston]. *If G is abelian, then $G^2 = \{x^2 \mid x \in G\}$ is a subgroup of G.*

Proposition [Dariely]. *The subset $\{2^k \mid k \in \mathbb{Z}\} \subset \mathbb{Q}^{\neq 0}$ is a subgroup (using multiplication).*

Proposition [Kimi-Lee]. *The subset $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$ is a subgroup (using addition).*

Proposition [Will]. *If $H_1, H_2 \subset G$ are both subgroups, then so is $H_1 \cap H_2$.*

Proposition [Dariely]. *If $g \in G$ then $\langle g \rangle = \langle g^{-1} \rangle$.*

Proposition [Kimi-Lee]. *If all elements of a group have order 2, then the group is abelian.*

Proposition [Treston]. *If $g, h \in G$ both have order 2 and commute, then gh also has order 2.*

Proposition [Will]. *Given $g \in G$, then $|g| = |g^2|$ if and only if g has odd order.*

Proposition [Dariely]. *Given $g \in G$ and $H < G$, then $gH = H$ if and only if $g \in H$.*

Proposition [Kimi-Lee]. *Given $a, b \in G$ and $H < G$, then $aH = bH$ if and only if $a \in bH$.*

Proposition [Treston]. *Given $a, b \in G$ and $H < G$, then $aH = bH$ if and only if $aH \cap bH \neq \emptyset$.*

Proposition [Will]. *Given $a, b \in G$ and $H < G$, then $aH = bH$ if and only if $a^{-1}b \in H$.*

Proposition [Known]. *If $H, K < G$ (nothing normal) then the following are true.*

(i) $H < HK \subset G$

(ii) $(H \cap K) < K$

Proposition [Dariely]. *If $H, K < G$ and $H \lhd G$ (one normal) then the following are true.*

(i) $H \lhd HK < G$

(ii) $(H \cap K) \lhd K$

Proposition [Will]. *If $H, K \lhd G$ (both normal) then the following are true.*

(i) $H \lhd HK \lhd G$

(ii) $(H \cap K) \lhd \boldsymbol{G}$

Proposition [Treston]. *If $K < H < G$ with $K \lhd G$ (bottom is normal) then the following are true.*

(i) $K \lhd H$

(ii) $H/K < G/K$

Proposition [Kimi-Lee]. *If $K \lhd H \lhd G$ with $K \lhd G$ (everything is normal) then the following are true.*

(i) $H/K \lhd G/K$

Other Important Propositions and Theorems.

Proposition. *If X is a set with $A \subset X$ and $B \subset X$, then $A \cup B \subset X$*

Proposition. *If X is a set with $X \subset A$ and $X \subset B$, then $X \subset A \cap B$*

Theorem. *Rules for triple operations:*

(Associative) $A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C$

$A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C$

(Distributive) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cap (A \cup C)$

Proposition. *If a composition $g \circ f : A \xrightarrow{f} B \xrightarrow{g} C$ is a injection and the first map $f : A \to B$ is a surjection, then the last map $g : B \to C$ must be an injection.*

Proposition. *If a composition $g \circ f : A \xrightarrow{f} B \xrightarrow{g} C$ is a surjection and the last map $g : B \to C$ is an injection, then the first map $f : A \to B$ must be a surjection.*

Proposition. *If $[x], [y] \in X/\!\sim$, then $[x] \neq [y]$ if and only if $[x] \cap [y] = \emptyset$*

Proposition. *Given $a, b, c \in G$, then $ba = ca$ if and only if $b = c$; similarly $ab = ac$ if and only if $b = c$.*

Proposition. *Given $a, b \in G$, then $aba^{-1}b^{-1} = e$ if and only if $ab = ba$.*

Proposition. *Given $a, b \in G$, then $[a, b]^{-1} = [b, a]$. (Recall that $[a, b] = aba^{-1}b^{1}$.)*

Proposition. $g\,[a, b]\,g^{-1} = [gag^{-1}, gbg^{-1}]$

Proposition. $\left(aba^{-1}\right)^n = ab^n a^{-1}$

Proposition. *A subset $H \subset G$ is a subgroup if the following conditions are satisfied.*

(i) The subset is nonempty $H \neq \emptyset$ (usually we show that $e \in H$).

(ii) The subset is closed under the group operation (i.e. if $a, b \in H$ then $ab \in H$).

(iii) The subset is closed under inverses (i.e. if $a \in H$ then $a^{-1} \in H$).

Proposition. *If $H < G$ and $g \in G$, then $gHg^{-1} < G$ also.*

Proposition. *If $a \in G$ generates subgroup $\langle a \rangle < G$ then every $H < G$ with $a \in H$ has $\langle a \rangle < H$ as well.*

Corollary. *If $a \in \langle b \rangle$ then $\langle a \rangle < \langle b \rangle$. In particular, if $a \in \langle b \rangle$ and $b \in \langle a \rangle$, then $\langle a \rangle = \langle b \rangle$.*

Proposition. *$\langle a \rangle$ is commutative.*

Proposition. *An element has **infinite order** if and only if $\boldsymbol{a^n \neq e}$ for any power n.*

*An element has **order** $|a| = n$ if and only if n is the smallest non-negative integer so that $\boldsymbol{a^n = e}$.*

Corollary. *If $|a| = n$ is finite, then $a^{-1} = a^{n-1}$.*

Corollary. *If $|a| = n$ is finite, then $a^i = a^j$ if and only if $i \equiv j \pmod{n}$.*

Corollary. *If $|a|$ is infinite, then $a^i = a^j$ if and only if $i = j$.*

Corollary. *If $|a| = n$ is finite, then $\left|a^k\right| = \frac{n}{\gcd(k,n)}$.*

Proposition. *All subgroups of cyclic groups are themselves cyclic.*

Corollary. *The only subgroups of $\mathbb{Z}$ are $n\mathbb{Z} = \langle n \rangle$.*

Proposition. *If G is cyclic and $H < G$, then $\big|G\big| = m\,\big|H\big|$ for some m.*

Theorem. *If G is cyclic of order n, then G has **exactly one** subgroup of order k for each divisor k of n.*

Corollary. *If $g \in G$ has order n, then $\langle g^k \rangle = \langle g^d \rangle$ where d is the greatest common divisor, $d = \gcd(k, n)$.*

Corollary. *If $g \in G$ has order n, then $\langle g^k \rangle = \langle g \rangle$ if and only if k and n are relatively prime.*

Corollary. *If $k \in \mathbb{Z}_n$, then $\langle k \rangle = \mathbb{Z}_n$ if and only if k and n are relatively prime.*

Proposition. *All cosets have the same order $\big|gH\big| = \big|H\big|$.*

Theorem [Lagrange]. *The order of a subgroup divides the order of its group.*

Corollary. *For any element of any group, $\big|g\big|$ divides $\big|G\big|$.*

Corollary. *For any element of any group, $g^n = e$ for $n = \big|G\big|$.*

Corollary (Fermat's Little Theorem). *For any integer n and prime p, we have $n^p \equiv n \pmod{p}$*

Corollary. *If G has finite prime order, then G is cyclic!*

Corollary. *If $K < H < G$ then $\big[G : K\big] = \big[G : H\big] \cdot \big[H : K\big]$.*

Proposition [Product Formula]. *The following relationship holds among orders of sets.*

$$\big|HK\big| \cdot \big|H \cap K\big| = \big|H\big| \cdot \big|K\big|$$

Corollary. *If H and K are subgroups of G then* $\dfrac{\big|H\big| \cdot \big|K\big|}{\big|H \cap K\big|} = \big|HK\big| \leq \big|G\big|$

Proposition. *The following are all equivalent to $\boldsymbol{H \triangleleft G}$.*

(i) *For all $g \in G$, $\boldsymbol{gH = Hg}$.*

(ii) *For all $g \in G$ and $h \in H$, $\boldsymbol{hg \in gH}$ (i.e. $Hg \subset gH$ for all g).*

(iii) *For all $g \in G$, $\boldsymbol{gHg^{-1} = H}$.*

(iv) *For all $g \in G$ and $h \in H$, $\boldsymbol{ghg^{-1} \in H}$ (i.e. $gHg^{-1} \subset H$ for all g).*

(v) *Every **left coset** is also a **right coset** (for each $g \in G$ there is $g' \in G$ so that $gH = Hg'$).*

Proposition. *The commutator subgroup $[G, G] < G$ defined by $[G, G] = \big\{aba^{-1}b^{-1} \mid a, b \in G\big\}$ is normal.*

Proposition. *If $H < G$ with index $[G : H] = 2$, then H is a normal subgroup.*

Corollary. *The alternating group of even permutations A_n is normal in the symmetric group S_n.*

Theorem. *If $H \triangleleft G$ then G/H is a **group**.*