Definitions in Group Theory

A binary operation on a set X is a map from $X \times X$ to X.

We often denote a binary relation by $\cdot$ and write $x \cdot y$ for the image of $(x, y) \in X \times X$.

A group is a set G with a binary operation satisfying the following axioms.

Identity: There exists an element $1 \in G$, such that for all $g \in G$, $1 \cdot g = g \cdot 1 = g$ holds.

Inverse: For each $g \in G$ there exists an element $\bar{g} \in G$ such that $g \cdot \bar{g} = \bar{g} \cdot g = 1$.

Associativity: For all $g, h, k \in G$, $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ holds.

The element 1 from the first axiom is called the identity of G. The element $\bar{g}$ from the second axiom is called the inverse of g and often denoted as g^{-1}. We often write gh instead of $g \cdot h$ and call it the product of g and h.

A subgroup of a group G is a subset H of G which is itself a group, under the binary operation induced from G.

A generating set for a group G is a subset S such that every element of G is a product of elements of S and their inverses.

A cyclic group is a group which can be generated by one of its elements.

For a subset S of a group G we write $\langle S \rangle$ for the subgroup of G generated by S.

An abelian group is a group in which $gh = hg$ for all $g, h \in G$.

A dihedral group is a group which can be generated by two distinct elements of order two.

The symmetric group of a set X is the group of all permutations of X, written $\mathrm{Sym}(X)$.
Fact: Every group G is a subgroup of $\mathrm{Sym}(G)$; map g to "right multiplication by g".

The alternating group of a set X is the group of even permutations of X, writtem $\mathrm{Alt}(X)$, which is a normal subgroup of $\mathrm{Sym}(X)$ of index 2.

The order of a group G is its cardinality and denoted $|G|$.

The order of an element g of a group G is $|\langle g \rangle|$.

A right coset of a subgroup H of a group G is a subset of G of the form $Hg = \{hg \mid h \in H\}$.

Conjugate. Let g, h be elements of a group G. Then we define the conjugate of h by g as $h^g = g^{-1}hg$.

A normal subgroup of a group G is a subgroup N of G such that $n^g \in N$ for all $n \in N$ and all $g \in G$, i.e. $N^g = N$ for all $g \in G$.

The normal closure of a subset S **of a group** G is the smallest normal subgroup of G containing S, which is $\langle S^G \rangle$, the group generated by all conjugates of S.

More Definitions and some Theorems in Group Theory

For subsets S and T of a group, define $ST = \{st \mid s \in S, t \in T\}$ and $S^T = \{s^t \mid s \in S, t \in T\}$.

Lagrange's Theorem. Let U be a subgroup of the finite group G. Then $|U|$ divides $|G|$.

The index of U in G is the number of cosets of U in G, and denoted as $|G : U|$.

A homomorphism is a map α from a group G to a group H such that $(gg')^\alpha = g^\alpha g'^\alpha$ holds for all $g, g' \in G$.

An isomorphism is a surjective and injective homomorphism.

A quotient (group) of a group G is a homomorphic image of G.

The quotient group (or factor group) of G by the normal subgroup N of G is the set $G/N = \{Ng \mid g \in G\}$ of all right cosets of N in G with product $Ng \cdot N\tilde{g} = Ng\tilde{g}$.

The kernel of a homomorphism $\alpha: G \to H$ consists of those elements of G that get mapped to the identity of H, i.e $\ker(\alpha) = \{g \in G \mid g^\alpha = 1\}$.
Fact: $\ker(\alpha)$ is a normal subgroup of G. Proof: $h^\alpha = 1 \Rightarrow (h^g)^\alpha = (h^\alpha)^{g^\alpha} = 1$.

Isomorphism Theorems. Let $\alpha : G \to H$ be a group homomorphism and let $K = \ker(\alpha)$.

1. $G^\alpha \cong G/K$, i.e. the image of α is isomorphic to the quotient of G by $\ker(\alpha)$.
2. For a subgroup U of G, $U^\alpha \cong U/(U \cap K) \cong (UK)/K$.
3. For a normal subgroup N of G with $K \subset N \subset G$, we have that N/K is a normal subgroup of G/K and $(G/K)/(N/K) \cong G/N$.

The centraliser of a subset S of a group G is $C_G(S) = \{g \in G \mid s^g = s \ \forall s \in S\}$, which is a subgroup of G.

The normaliser of a subset S of a group G is $N_G(S) = \{g \in G \mid S^g = S\}$, which is a subgroup of G.
Fact: For any subset S of G, $C_G(S)$ is a normal subgroup of $N_G(S)$.

The centre of a group G is $Z(G) = C_G(G)$.

An automorphism of a group G is an isomorphism from G to itself. The set of all automorphisms of G forms a group denoted $\mathrm{Aut}(G)$. For $g \in G$ define g^ι to be "conjugation by g", i.e. $h^{g^\iota} = h^g$ for $h \in G$. Then $g^\iota \in \mathrm{Aut}(G)$ and $\iota: g \mapsto g^\iota$ is a homomorphism from G to $\mathrm{Aut}(G)$ with $\ker(\iota) = Z(G)$.

A group F is free on a set X if X is a subset of F such that (i) F is generated by X and (ii) for every group G, every map $\alpha: X \to G$ can be extended to a homomorphism $\alpha^*: F \to G$.
Theorem: For every set X there exists, up to isomorphism, a unique free group on X, denoted $F(X)$, whose elements are the (freely) reduced words over $X \cup X^{-1}$ and multiplication is concatenation followed by free reduction.

A group presentation is a pair $\langle X \mid R \rangle$, where X is a set and R is a subset of $F(X)$, which defines the group $F(X)/\langle R^{F(X)} \rangle$.