Abstract Algebra (2nd Ed.) - Dummit and Foote

Eu-Jin Goh
eujin@cs.stanford.edu

January 9, 2003

1 Introduction to Groups

2 Subgroups

3 Quotient Groups and Homomorphisms

3.1 Definitions and Examples

The study of quotient groups of G is equivalent to the study of homomorphisms of G.

Definition (Fibers). Let ϕ is a homomorphism from G to a group H. The *fibers* of ϕ are the sets of elements of G projecting to single elements of H.

Intuitively, the group G is partitioned into pieces (the fibers) and these pieces have the structure of a group (the quotient group of G). Since the multiplication of these fibers is defined from the multiplication in H, the quotient group with this multiplication is isomorphic to the image of G under the homomorphism ϕ.

Definition (Kernel). If ϕ is a homomorphism $\phi : G \to H$, the *kernel* of ϕ is the set $\{g \in G | \phi(g) = 1\}$ and will be denoted by kerϕ (here 1 is the identity of H).

Proposition 3.1. *Let G and H be groups and let $\phi : G \to H$ be a homomorphism.*

1. $\phi(1_G) = 1_H$*, where 1_G and 1_H are the identities of G and H respectively.*
2. $\phi(g^{-1}) = \phi(g)^{-1}$ *for all* $g \in G$.
3. $\phi(g^n) = \phi(g)^n$ *for all* $n \in \mathbb{Z}$.
4. *kerϕ is a subgroup of G.*
5. *im(ϕ), the image of G under ϕ, is a subgroup of H.*

Definition (Quotient Group). Let $\phi : G \to H$ be a homomorphism with kernel K. The *quotient group* is the group whose elements are the fibers of ϕ with group operation as follows: if $X \subseteq G$ is the fiber above $a \in H$ and $Y \subseteq G$ is the fiber above $b \in H$, then the product of X with Y is defined to be the fiber above the product ab.

We show that the fibers of a homomorphism can be expressed in terms of the kernel of the homomorphism (e.g. The homomorphism from $\mathbb{Z}$ to Z_n ($\mathbb{Z}/n\mathbb{Z}$) has kernel $n\mathbb{Z}$ and the fibers are translates of the form $a + n\mathbb{Z}$.

Proposition 3.2. *Let $\phi : G \to H$ be a homomorphism of groups with kernel K. Let $X \in G/K$ be the fiber above a, i.e. $X = \phi^{-1}(a)$. Then*

1. *For any $u \in X$, $X = \{uk \mid k \in K\}$*
2. *For any $u \in X$, $X = \{ku \mid k \in K\}$*

Definition (Cosets). For any subgroup N of G, and any $g \in G$, let $gN = \{gn \mid n \in N\}$ be the *left coset* and $Ng = \{ng \mid n \in N\}$ be the *right coset*. Any element of a coset is called a representative for the coset.

Using the definition of a coset, Proposition 3.2 shows that the fibers of a homomorphism are the left cosets of the kernel, i.e. the elements of the quotient G/K are the left cosets $gK, g \in G$.

The product of two left cosets X and Y in G/K is computed by choosing any representative u of X, any representative v of Y, multiplying u and v in G and forming the coset $(uv)K$.

Theorem 3.3. *Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with operation defined by $uK \circ vK = (uv)K$ forms a group, G/K.*

Multiplication is independent of the particular representatives chosen. We denote the coset uK containing a representative u as $\overline{u}$.

3.1.1 Normal Subgroups

An interesting question is if it is possible to define the quotient group G/N similarly for any subgroup N of G. In fact, it is possible to define the structure of a group on the cosets of N if and only if N is the kernel of some homomorphism.

We first show that the cosets of an arbitrary subgroup of G partition G.

Proposition 3.4. *Let N be any subgroup of the group G. The set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G, uN = vN$ if and only if $v^{-1}u \in N$ (i.e. $u = vn$ for some $n \in N$). In particular, $uN = vN$ if and only if u and v are representatives of the same coset.*

We establish some criteria for a subgroup N so that we can define the structure of a group on the cosets of N.

Proposition 3.5. *Let G be a group and let N be a subgroup of G.*

1. *The operation on the set of left cosets of N in G described by $uN \cdot vN = (uv)N$ is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.*

2. *If the above operation is well defined, then it makes the set of left cosets of N in G into a group. In particular, the identity of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$, i.e. $(gN)^{-1} = g^{-1}N$.*

Definition (Conjugate). The element gng^{-1} is called the *conjugate* of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the *conjugate* of N by g.

Definition (Normal). The element g is said to *normalize* N if $gNg^{-1} = N$. A subgroup N of a group G is called *normal* if every element of G normalizes N, i.e. if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G, we shall write $N \trianglelefteq G$.

The following theorem summarizes the results obtained for normal subgroups so far.

Theorem 3.6. *Let N be a subgroup of the group G. The following are equivalent.*

1. $N \trianglelefteq G$

2. $N_G(N) = G$

3. *$gN = Ng$ for all $g \in G$ (left cosets are equal to the right cosets)*

4. *the operation of left cosets of N in G described in Proposition 3.5 makes the set of left cosets into a group.*

Proposition 3.7. *A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.*

The homomorphism constructed in the previous proposition to show that the normal subgroup N is the kernel of a homomorphism is given a name.

Definition (Natural Projection). Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the *natural projection* of G onto G/N.

Definition (Complete Preimage). Let $N \trianglelefteq G$. If $\overline{H} \leq G/N$ is a subgroup of G/N, the *complete preimage* of $\overline{H}$ in G is the preimage of $\overline{H}$ under the natural projection homomorphism.

The complete preimage of a subgroup of G/N is a subgroup of G which contains the subgroup N since these are the elements that map to the identity $\overline{1} \in \overline{H}$.

The property of being normal is an *embedding* property, that is, it depends on the relation of N to G, not on the internal structure of N itself. A group N may be a normal subgroup of G but not be normal in a larger group containing G.

Examples. Let G be a group.

1. *The subgroups 1 and G are always normal in G*; $G/1 \cong G$ and $G/G \cong 1$.

2. *All subgroups of an Abelian group are normal.*

   If G is an abelian group, any subgroup of N is normal because for any $g \in G$ and any $n \in N$, $gng^{-1} = gg^{-1}n = n \in N$.

   If $N \leq Z(G)$, then $N \trianglelefteq G$. In particular, $Z(G) \trianglelefteq G$.

3. *Quotient groups of a cyclic group are cyclic.*

   Suppose $G = Z_k$ is the cyclic group of order k. Let x be a generator of G and let $N \leq G$. Then, $N = \langle x^d \rangle$ where d is the smallest power of x which lies in N. Now

   $$G/N = \{gN \mid g \in G\} = \{x^\alpha N \mid \alpha \in \mathbb{Z}\}$$

   and since $x^\alpha N = (xN)^\alpha$, it follows that $G/N = \langle xN \rangle$, i.e. G/N is cyclic with xN as a generator.

   If G is a finite cyclic group, then we have $|G/N| = |G|/|N|$.

3.2 More on Cosets and Lagrange's Theorem

Theorem 3.8 (Lagrange's Theorem). *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G equals $|G|/|H|$.*

Proof Sketch. Consider the left cosets of H and show that $|H| = |gH|$ by proving that the map $H \to gH$ is a bijection. □

Corollary 3.9. *If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular, $x^{|G|} = 1$ for all $x \in G$.*

Corollary 3.10. *If G is a group of prime order p, then G is cyclic, hence $G \cong Z_p$.*

Definition (Index). If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the *index* of H in G and is denoted by $|G : H|$.

Example. A subgroup of index 2 must be normal. Let G be any group containing a subgroup H of index 2. Let $g \in G - H$ and so, the two left cosets of H in G are $1H$ and gH. Since $1H = H$ and the cosets partition G, we must have $gH = G - H$. Considering the two right cosets in a similar fashion, we obtain $Hg = G - H$. Hence, $gH = Hg$ which, by Theorem 3.6, implies that $H \trianglelefteq G$. Therefore, any subgroup of index 2 must be normal.

The full converse to Lagrange's theorem is false; namely, if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n. However, if G is a finite abelian group, then the full converse is true. A partial converse which holds for arbitrary finite groups is the following theorem.

Theorem 3.11 (Cauchy's Theorem). *If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.*

The strongest converse to Lagrange's theorem for arbitrary finite groups is the following theorem.

Theorem 3.12 (Sylow). *If G is a finite group of order $p^\alpha m$, where p is a prime and p does not divide m, then G has a subgroup of order p^α.*

Properties of Cosets. The rest of this section explores some useful properties of cosets.

Definition. Let H and K be subgroups of a group. Define $HK = \{hk \mid h \in H, k \in K\}$.

Proposition 3.13. *If H and K are finite subgroups of a group,*

$$|HK| = |H||K|/|H \cap K|.$$

Note that there is no assumption on HK being a subgroup in the previous proposition.

Proposition 3.14. *If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.*

Corollary 3.15. *If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$, then HK is a subgroup for any $H \leq G$.*

Definition. If A is any subset of $N_G(K)$ (or $C_G(K)$), we say that A *normalizes* K (*centralizes* K).

With this definition, Corollary 3.15 states that HK is a subgroup if H normalizes K.

3.3 The Isomorphism Theorems

This section discusses the relations between quotient groups and homomorphisms.

Theorem 3.16 (First Isomorphism Theorem). *If $\phi : G \to H$ is a homomorphism of groups, then $ker\phi \trianglelefteq G$ and $G/ker\phi \cong \phi(G)$.*

The isomorphism in the previous theorem is $\phi(g(ker\phi)) = g$.

Corollary 3.17. *Let $\phi : G \to H$ be a homomorphism of groups.*

1. *ϕ is 1-1 if and only if $ker\phi = 1$*
2. *$|G : ker\phi| = |\phi(G)|$*

Theorem 3.18 (Second Isomorphism Theorem). *Let G be a group, let A and B be subgroups of G and assume that $A \leq N_G(B)$. Then $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.*

The isomorphism in the previous theorem is $\phi : AB \to A/(A \cap B)$ where $\phi(ab) = a(A \cap B)$ and $ker\phi = B$.

Theorem 3.19 (Third Isomorphism Theorem). *Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.*

The isomorphism in the previous theorem is $\phi : (G/H) \to G/K$ where $\phi(gH) = gK$ and $ker\phi = K/H$.

The last isomorphism theorem describes the relation between the lattice of subgroups of the quotient group G/N and the lattice of subgroups of G. There is a 1-1 correspondence between the subgroups of G containing N and the subgroups of G/N.

Theorem 3.20 (Fourth Isomorphism Theorem). *Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,*

1. *$A \leq B$ if and only if $\overline{A} \leq \overline{B}$*
2. *if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$*
3. *$\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$*
4. *$\overline{A \cap B} = \overline{A} \cap \overline{B}$*
5. *$A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.*

3.4 Composition Series and the Holder Program

The proof of a special case of Cauchy's theorem provides a good example of the use of induction in discerning information about a group G from its normal subgroup N and the quotient G/N.

Proposition 3.21. *If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.*

Proof Sketch. Use induction on $|G|$. Assume that all groups H with order less than $|G|$ have the property that if $p||H|$, then H contains an element of order p.

Assume that $p||G|$ which implies $|G| > 1$. Since $|G| > 1$, there exists $x \in G$ where $x \neq 1$.

If $|G| = p$, then $|\langle x\rangle| = p$ and hence $|x| = p$. Assume $|G| \neq p$ which implies $|G| > p$.

If $p||x|$, then $|x| = pm$ for some $m \in \mathbb{Z}$ which implies that $|x^m| = p$. Therefore, assume that $p \nmid |x|$.

Show $|G/N|$ has an element y such that $p||y|$. Consider $N \stackrel{def}{=} \langle x\rangle$. Since G is abelian, $N \trianglelefteq G$. Also, $p \nmid |N|$. By Lagrange's theorem, $|G/N| = |G|/|N|$ and so, $|G| = |G/N||N|$. Since $p||G|$ and $p \nmid |N|$, we have that $p||G/N|$. By induction, $|G/N|$ has an element, yN ($y \in G$), of order p because $|G/N| < |G|$.

Furthermore, $y \notin N$ because $yN \neq 1N$. Since $(yN)^p = 1N \Rightarrow y^pN = N$, we have $y^p \in N$. Then, $\langle y\rangle \neq \langle y^p\rangle$. Since both groups are cyclic, $|y^p| = |y|/p$ which tells us that $|y| = pn$ for some $n \in \mathbb{Z}$. Therefore, $|y^n| = p$. □

The intuitive idea behind the proof is that if we have sufficient information about some normal subgroup N of a group G, and about G/N, we can force G to have some property. We use induction because both N and G/N have smaller order than G.

An obstruction to using this method is producing a normal subgroup N of G with $N \neq 1$ or G. Groups with no nontrivial proper normal subgroups are fundamental obstructions to this method of proof.

Definition (Simple). A (finite or infinite) group G is called *simple* if $|G| > 1$ and the only normal subgroups of G are 1 and G.

By Lagrange's theorem, if $|G|$ is a prime, its only subgroups are 1 and G, so G is simple. In fact, every abelian simple group is isomorphic to Z_p for some prime p. The smallest non-abelian simple group has order 60.

Simple groups cannot be "factored" into pieces like N and G/N and so play a role analogous to the primes in $\mathbb{Z}$. This analogy is supported by a unique factorization theorem (Jordan-Hölder) for finite groups.

Definition (Composition Series). In a group G, a sequence of subgroups

$$1 = N_0 \leq \ldots \leq N_k = G$$

is called a *composition series* if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group for $0 \leq i \leq k-1$. If the above sequence is a composition series, the quotient groups N_{i+1}/N_i are called *composition factors* of G.

Theorem 3.22 (Jordan-Hölder). *Let G be a finite group with $G \neq 1$. Then*

1. *G has a composition series and*
2. *The composition factors in the composition series are unique, namely, if $1 = N_0 \leq \ldots \leq N_r = G$ and $1 = M_0 \leq \ldots \leq M_s = G$ are two composition series for G, then $r = s$ and there is some permutation, π, of $\{1, 2, \ldots, r\}$ such that $M_{\pi(i)+1}/M_{\pi(i)} \cong N_{i+1}/N_i$ for $1 \leq i \leq r-1$.*

Theorem (Feit-Thompson). *If G is a simple group of odd order, then $G \cong Z_p$ for some prime p.*

Definition (Solvable). A group G is *solvable* if there is a chain of subgroups $1 = G_0 \trianglelefteq \ldots \trianglelefteq N_s = G$ such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$.

We can generalize Sylow's theorem for solvable groups.

Theorem (Hall). *The finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, |G|/n) = 1$, G has a subgroup of order n.*

Theorem. *Let G be a group and N be a normal subgroup of G. If N and G/N are solvable, then G is solvable.*

Examples.

1. Subgroups and quotient groups of a solvable group are also solvable.
2. Every abelian group G is solvable because every subgroup of an abelian group is normal and quotients are abelian.

3.5 Transpositions and the Alternating Group

3.5.1 Transpositions and Generation of $\mathbf{S_n}$

Every element of S_n can be written as a product of disjoint cycles in a unique manner. In contrast, every element of S_n can be written in many different ways as a nondisjoint product of cycles. We can obtain a parity check by writing permutations non-uniquely as products of 2-cycles.

Definition (Transposition). A 2-cycle is called a *transposition*.

Every element of S_n can be written as a product of transpositions. For example, for any m-cycle, we can write $(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_2)$. Note that there are $m - 1$ terms on the right hand side.

3.5.2 Alternating Group

For a fixed $\sigma \in S_n$, we now show that the parity (an odd or even number of terms) is the same for any product of transpositions equaling σ.

Let $x_1, \dots, x_n$ be independent variables and let Δ be the polynomial

$$\Delta = \prod_{1 \le i \le j \le n} (x_i - x_j)$$

i.e. the product of all the terms $x_i - x_j$ for $i < j$.

For each $\sigma \in S_n$, let σ act on Δ by permuting the indices of the variables. i.e.

$$\sigma(\Delta) = \prod_{1 \le i \le j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Note that σ contains one factor $x_i - x_j$ for all $i < j$ and because σ is a bijection, $\sigma(\Delta)$ must contain either $x_i - x_j$ or $x_j - x_i$ but not both for all $i < j$. If $\sigma(\Delta)$ has a factor $x_j - x_i$ where $j > i$, we write this term as $-(x_i - x_j)$. Hence, $\sigma(\Delta) = \pm\Delta$ for all $\sigma \in S_n$.

We can now define the sign of a permutation.

Definition (Sign of a Permutation). For the polynomial Δ defined above and for each $\sigma \in S_n$, let

$$\epsilon(\sigma) = \begin{cases} +1 & \text{if } \sigma(\Delta) = \Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta. \end{cases}$$

Then, $\epsilon(\sigma)$ is called the *sign* of σ. Furthermore, σ is called an *even permutation* if $\epsilon(\sigma) = 1$ and an *odd permutation* if $\epsilon(\sigma) = -1$.

Proposition 3.23. *The map $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism where $\{\pm 1\}$ is a multiplicative version of Z_2.*

Using the homomorphism ϵ, we deduce the following fact about transpositions.

Proposition 3.24. *All transpositions are odd permutations and ϵ is onto.*

We can now define the Alternating group.

Definition (Alternating Group). The *alternating group of degree n*, denoted by A_n, is the kernel of the homomorphism $\epsilon : S_n \to \{\pm 1\}$ (i.e. the set of even permutations in S_n).

Note that by the First Isomorphism Theorem, $S_n/A_n \cong \{\pm 1\}$. By Lagrange's theorem, $|A_n| = |S_n|/2 = n!/2$. Also, $S_n - A_n$ is the coset of A_n that is not the identity coset and this is the set of all odd permutations.

Since ϵ is a homomorphism and $\sigma \in S_n$ is a product of transpositions $\epsilon(\sigma) = +1$ if σ is the product of an even number of transpositions and $\epsilon(\sigma) = -1$ if σ is the product of an odd number of transpositions. Recall that an m-cycle can be written as a series of $m - 1$ transpositions. Hence, we obtain the following proposition,

Proposition. *An m-cycle is an odd permutation if and only if m is even.*

Corollary 3.25. *The permutation σ is odd if and only if there are an odd number of cycles of even length in the cycle decomposition of σ.*

A_1, A_2 are the trivial group and $A_3 = \langle (123) \rangle \cong Z_3$. A_4 is isomorphic to the group of symmetries of a regular tetrahedron and has order 12.

4 Group Actions

In this chapter, we consider the consequences of a group acting on a set.

4.1 Group Actions and Permutation Representations

This section presents the basic theory of group actions and apply the theory to subgroups of S_n acting on $\{1, 2, \ldots, n\}$ to prove that every element of S_n has a unique cycle decomposition.

Let G be a group acting on a nonempty set A. For each $g \in G$, the map $\sigma_g : A \to A$ defined by $\sigma_g(a) = g \cdot a$ is a permutation of A. Furthermore, there is a homomorphism called the *permutation representation* associated to an action of G on A given by $\phi : G \to S_A$ defined by $\phi(g) = \sigma_g$.

Definition (Kernel of an Action). The *kernel* of a group action is the set of elements of G that act trivially on every element of A, i.e. $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.

Note that the kernel of an action is precisely the same as the kernel of the associated permutation representation. Hence, the kernel is a normal subgroup of G.

Definition (Stabilizer). For each $a \in A$, the *stabilizer* of a is the set of all elements in G that fix the element a, i.e. $\{g \in G \mid g \cdot a = a\}$. The stabilizer is denoted by G_a.

Note that stabilizer is used to describe the set of group actions that fix a set of elements. The normalizer refers to the set of elements of a group that when conjugated to a subset of a group, remain in the subset. The centralizer is the set of elements that fix a particular element (or set) during conjugation. Normalizers and centralizers can be viewed as special cases of stabilizers because conjugation is a group action.

Definition (Faithful Action). An action is *faithful* if the kernel is the identity.

As shown above, given a nonempty set A and a group action, there is a homomorphism $\phi : G \to S_A$ defined by $\phi(g) = \sigma_g$ that maps the group action into the symmetric group acting on A. The reverse also holds true, given a nonempty set A and a homomorphism $\phi : G \to S_A$, we obtain an action of G on A by defining $g \cdot a = \phi(g)(a)$. This fact gives rise to the following proposition.

Proposition 4.1. *For any group G and any nonempty set A, there is a bijection between the actions of G on A and the homomorphisms of G into S_A.*

Definition (Permutation Representation). If G is a group, a *permutation representation* of G is any homomorphism of G into the symmetric group S_A for some nonempty set A. We shall say that a given action of G on A *induces* the associated permutation representation of G.

Proposition 4.2. *Let G be a group acting on the nonempty set A. The relation on A defined by*

$$a \sim b \text{ if and only if } a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.

Let $\mathcal{C}_a = \{g \cdot a \mid g \in G\}$. Suppose $b = g \cdot a \in \mathcal{C}_a$. The bijection used in the previous proposition is given by $b = g \cdot a \to gG_a$ which is a map from $\mathcal{C}_a$ to the set of left cosets of G_a in G.

Definition (Orbit). The equivalence class $\{g \cdot a \mid g \in G\}$ is called the *orbit* of G containing a.

Definition (Transitive Action). The action of G on A is called *transitive* if there is only one orbit, i.e. given any two elements $a, b \in A$, there exists some $g \in G$ such that $a = g \cdot b$.

Examples. Let G be a group acting on the set A.

1. If G acts trivially on A, then $G_a = G$ for all $a \in A$. The orbits are the single elements of A. This action is transitive if and only if $|A| = 1$.

2. The symmetric group $G = S_n$ acts transitively in its usual action on $A = \{1, 2, \ldots, n\}$. The stabilizer in G of any point i has index $n = |A|$ in S_n because there are $n!$ permutations of A and $(n-1)!$ permutations that fix i.

Definition (Permutation Groups). A *permutation group* is a subgroup of a symmetric group.

4.2 Groups Acting on Themselves by Left Multiplication — Cayley's Theorem

It is easy to see that the action of a group on itself by left multiplication is always transitive and faithful, and that the stabilizer of any point is the identity subgroup.

We generalize the notion of the action of a group on itself by left multiplication to that of the action of a group on the left cosets of one of its subgroup.

Theorem 4.3. *Let G be a group, let H be any subgroup of G, and let A be the set of all left cosets of H in G. Consider G acting on A by left multiplication, i.e. $g \cdot aH = (ga)H$ for all $g \in G$ and $aH \in A$. Let π_H be the associated permutation representation induced by this action. Then,*

1. *G acts transitively on A*
2. *the stabilizer in G of the point $1H \in A$ is the subgroup H*
3. *the kernel of the action (i.e. the kernel of π_H) is $\cap_{x \in G} xHx^{-1}$, and $ker\pi_H$ is the largest normal subgroup of G contained in H.*

Corollary 4.4 (Cayley's Theorem). *Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.*

Note that G is isomorphic to a subgroup of the symmetric group, and not to the full symmetric group.

The next corollary generalizes the result in Section 3.2 on the normality of subgroups of index 2.

Corollary 4.5. *If G is a finite group of order n, and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.*

Proof Sketch. Consider the quotient group $G/ker\pi_H$ and the index of $ker\pi_H$ in H. □

Note that a group of order n need not have a subgroup of index p. In the previous result, since the subgroup has index 2 and cosets form a partition, this implies that $|G|$ is even and 2 is therefore the smallest prime dividing $|G|$.

4.3 Groups Acting on Themselves by Conjugation — Class Equation

A group G acting on itself by conjugation is defined as $g \cdot a = gag^{-1}$ for all $g, a \in G$ where gag^{-1} is computed in the group G.

Definition (Conjugate Elements). Two elements $a, b \in G$ are *conjugate* in G if there is some $g \in G$ such that $a = gbg^{-1}$ (i.e. if and only if they are in the same orbit of G acting on itself by conjugation).

Definition (Conjugacy Class). The orbits of G acting on itself by conjugation are called the *conjugacy classes* of G.

Examples.

1. If G is an abelian group, the action of G on itself by conjugation is the trivial action. For each $a \in G$, the conjugacy class of a is $\{a\}$.
2. If $|G| > 1$, then conjugation action of G on itself is not transitive (unlike left multiplication). $\{1\}$ is always a conjugacy class. In general, the one element subset $\{a\}$ is a conjugacy class if and only if $gag^{-1} = a$ for all $g \in G$ if and only if $a \in Z(G)$.

As in the previous section, we can generalize the notion of conjugacy to subsets of a group.

Definition (Conjugate Sets). Two subsets S and T of a group G are *conjugate* in G if there is some $g \in G$ such that $T = gSg^{-1} = \{gsg^{-1} \mid s \in S\}$ (i.e. if they are in the same orbit of G acting on its subsets by conjugation).

Applying Proposition 4.2 to this definition, we obtain the following proposition.

Proposition 4.6. *The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s is the index of the centralizer of s, $|G : C_G(s)|$.*

The action of G on itself by conjugation is a partition of G into conjugacy classes. The orders of these classes can be computed by the previous proposition.

Theorem 4.7 (Class Equation). *Let G be a finite group and let $g_1, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Note that the terms on the right hand side of the class equation must divide the order of $|G|$ (by Lagrange's theorem) since they are indices of subgroups of G.

Observe that $\langle g \rangle \leq C_G(g)$. This observation helps reduce computations of conjugacy classes.

We apply the class equation to show that groups of prime power have nontrivial centers.

Theorem 4.8. *If p is a prime and P is a group of prime order p^α for some $\alpha \geq 1$, then P has a nontrivial center.*

Corollary 4.9. *If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.*

4.3.1 Conjugacy in $\mathbf{S_n}$

In this section, we consider conjugation in S_n and prove that A_5 is simple.

Proposition 4.10. *Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition $(a_1 a_2 \ldots a_{k_1})(b_1 b_2 \ldots b_{k_2})\ldots$. Then, $\tau\sigma\tau^{-1}$ has cycle decomposition $(\tau(a_1)\tau(a_2)\ldots\tau(a_{k_1}))(\tau(b_1)\tau(b_2)\ldots\tau(b_{k_2}))\ldots$.*

Definition (Cycle Type). If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$ with $n_1 \leq n_2 \leq \ldots \leq n_r$ (including its 1-cycles), then the integers $n_1, n_2, \ldots, n_r$ are called the *cycle type* of σ.

Definition (Partition of $\mathbf{n} \in \mathbb{Z}^+$). If $n \in \mathbb{Z}^+$, a *partition* of n is any nondecreasing sequence of positive integers whose sum is n.

Note that the cycle type of a permtation is unique.

Proposition 4.11. *Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.*

Together with Proposition 4.6, the previous proposition allows us to calculate the order of the centralizer for a element in S_n.

Proposition. *Let σ be a m-cycle in S_n. Then $|C_{S_n}(\sigma)| = m \cdot (n-m)!$. Furthermore,*

$$C_{S_n}(\sigma) = \{\sigma^i \tau \mid 0 \leq i \leq m-1, \tau \in S_{n-m}\}$$

where S_{n-m} denotes the subgroup of S_n which fixes all integers appearing in σ.

Proof. Since σ is an m-cycle, the number of conjugates of σ (i.e. the number of m-cycles by Proposition 4.11) is $n!/(m \cdot (n-m)!)$. By Proposition 4.6, the number of conjugates of σ is equal to the index of the centralizer, $|S_n : C_{S_n}(\sigma)| = |S_n|/|C_{S_n}(\sigma)| = n!/|C_{S_n}(\sigma)|$. Therefore, $|C_{S_n}(\sigma)| = m \cdot (n-m)!$.

Clearly, the m elements $1, \sigma, \ldots, \sigma^{m-1}$ belong to $C_{S_n}(\sigma)$. Any cycle $\tau \in S_n$ that fixes the integers appearing in σ also belong to $C_{S_n}(\sigma)$ and there are $(n-m)!$ of them. Note that τ and σ commute. The product of elements of these two types exhaust the number of elements in $C_{S_n}(\sigma)$. Hence, $C_{S_n}(\sigma) = \{\sigma^i \tau \mid 0 \leq i \leq m-1, \tau \in S_{n-m}\}$. □

Using these techniques, we can give a combinatorial proof that A_5 is simple.

Lemma. *If $H \trianglelefteq G$, then for every conjugacy class $\mathcal{K}$ of G, either $\mathcal{K} \subseteq H$ or $H \cap \mathcal{K} = 0$ (i.e. the normal subgroups of G are the union of conjugacy classes of G.*

Theorem 4.12. *A_5 is a simple group.*

4.4 Automorphisms

Definition (Automorphism). Let G be a group. An isomorphism from G onto itself is called an *automorphism* of G. The set of all automorphisms of G is denoted by $Aut(G)$.

Note that automorphisms form a group under composition of automorphisms. Furthermore, automorphisms of a group G are permutations of the set G so $Aut(G)$ is a subgroup of S_G.

The following proposition shows that a group acts by conjugation on a normal subgroup as a structure preserving permutation.

Proposition 4.13. *Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation induced by this action is a homomorphism from G into $Aut(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.*

We can use the preceding proposition on arbitrary groups because any group is normal to itself. The conjugation action must send subgroups to subgroups, elements of order n to elements of order n.

Corollary 4.14. *If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.*

Corollary 4.15. *For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$.*

The preceding corollaries show that any information we have about the automorphism group of a subgroup H of a group G translates into information about $N_G(H)/C_G(H)$. For example, consider $H \cong Z_2$. Since H has unique elements of order 1 and 2, $Aut(H) = 1$. Then, $N_G(H)/C_G(H) \cong 1$ and so $N_G(H) = C_G(H)$. In addition, if $H \trianglelefteq G$, then $H \leq Z(G)$.

Definition (Inner Automorphism). Let G be a group and let $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $Aut(G)$ consisting of all inner automorphisms is denoted by $Inn(G)$.

The collection of inner automorphisms of G is a subgroup of $Aut(G)$. In fact, $Inn(G) \cong G/Z(G)$. Note that if H is a normal subgroup of G, conjugation by an element of G when restricted to H is an automorphism of H but need not be an inner automorphism.

Examples.

1. A group is abelian if and only if every inner automorphism is trivial.

2. If H is an abelian normal subgroup of G and H is not contained in $Z(G)$, then there is some $g \in G$ such that conjugation by g restricted to H is not an inner automorphism of H.

3. For all $n \geq 3$, $Z(S_n) = 1$ which implies that $Inn(S_n) = S_n$.

Definition (Characteristic Subgroups). A subgroup H of G is *characteristic* in G if every automorphism of G maps H to itself, i.e. $\sigma(H) = H$ for every $\sigma \in Aut(G)$. We denote this as H *char* G.

Characteristic subgroups are normal.

Proposition. *Let H be a subgroup of a group G. If H char G, then $H \trianglelefteq G$.*

Proposition. *Let H be a subgroup of a group G. If H is the unique subgroup of G of a given order, then H is characteristic in G.*

In general, if $K \trianglelefteq H \trianglelefteq G$, it is not necessarily true that $K \trianglelefteq G$. However, this relation is true for characteristic subgroups of normal subgroups.

Proposition. *Let H be a subgroup of a group G. If K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$.*

Proof. We want to show that $K \trianglelefteq G$, i.e. every inner automorphism of G maps K to itself. Since H is normal, every inner automorphism of G maps H to itself, which implies that every inner automorphism of G is an automorphism of H. Since K *char* H, every automorphism of H maps K to itself. Combining the two previous assertions, we see that every inner automorphism of G maps K to itself, i.e. $K \trianglelefteq G$. $\square$

Intuitively, we can think of characteristic subgroups as being "strongly normal".

4.4.1 Automorphism Groups of Specific Subgroups

Proposition 4.16. *The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\phi(n)$, where ϕ is the Euler function.*

Every $\psi_a \in Aut(Z_n)$ is defined $\psi(x_a) = x^a$ for some $a \in \mathbb{Z}$ and $(a, n) = 1$. The isomorphism in the previous proposition is $\Psi : Aut(Z_n) \to (\mathbb{Z}/n\mathbb{Z})^\times$ where $\Psi(\psi_a) = a$.

Proposition. *Let G be a group of order pq where p, q are primes and $p \leq q$. If $p \nmid q - 1$, G is abelian. If $p < q$ and $p \nmid q - 1$, G is cyclic.*

Proof Sketch. We prove the first assertion. If $Z(G) \neq 1$, then $|Z(G)| = p$ or q which implies that $G/Z(G)$ has prime order and is therefore cyclic. Hence, G is abelian.

Assume $Z(G) = 1$. We first show that G has to contain at least one element of order q. Suppose all the nonidentity elements of G have order p. Let x be such an element. Then, by Lagrange's theorem, the index of $\langle x \rangle$ is $|G|/p = q$. Using the class equation, $pq = 1 + kq$ for some $k \in \mathbb{Z}^+$. This is a contradiction since q divides pq and kq but not 1. Thus, G contains an element of order q. We call this element y.

Consider $H = \langle y \rangle$. We derive the order of the group of automorphisms of H two different ways and show a contradiction. H has index p because $|H| = q$. By Corollary 4.5, since p is the smallest prime dividing $|G|$, H must be normal. Since $Z(G) = 1$ and H is cyclic, the set of elements that commute with H (i.e. the centralizer of H) is H. By Corollary 4.15, $G/H = N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$. Note that $|G/H| = p$.

By Corollary 4.16, $Aut(H)$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^\times$ and has order $\phi(q) = q - 1$. Therefore, we must have $p|q - 1$ which is a contradiction. Hence, $Z(G) \neq 1$.

We now prove the second assertion. By Cauchy's theorem, G must contain an element of order p and an element of order q. Call these elements a and b respectively. If $p < q$, we know that these elements must be distinct. Then, the order of the group $\langle a, b \rangle$ must be pq which implies that G is cyclic. $\square$

Proposition 4.17. *If p is an odd prime and $n \in \mathbb{Z}^+$, then the automorphism group of the cyclic group of order p is cyclic of order $p - 1$. More generally, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p - 1)$.*

4.5 Sylow's Theorem

Definition (p-group). Let G be a group and p a prime. A group of order p^α for some $\alpha \geq 1$ is called a *p-group*. Subgroups of G which are p-groups are called p-subgroups.

Definition (Sylow p-subgroup). Let G be a group and p a prime. If G is a group of order $p^\alpha m$, where $p \nmid \alpha$, then a subgroup of p^α is called a *Sylow p-subgroup* of G.

The set of Sylow p-subgroups of G are denoted $Syl_p(G)$ and the number of Sylow p-subgroups of G are denoted by $n_p(G)$.

Theorem 4.18 (Sylow's Theorem). *Let G be a group of order p^α, where p is a prime not dividing m.*

1. *Sylow p-subgroups of G exist, i.e. $Syl_p(G) \neq 0$.*
2. *If P is a Sylow p-subgroup of G, and Q is any p-subgroup of G, then there exists a $g \in G$ such that $Q \leq gPg^{-1}$, i.e. Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.*
3. *The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e. $n_p \equiv 1 \mod p$. Furthermore, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence $n_p | m$.*

To prove Sylow's theorem, we need the following lemma.

Lemma 4.19. *Let $P \in Syl_P(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.*

Note that part 2 of Sylow's Theorem implies that any two Sylow p-subgroups (for the same prime) of a group are isomorphic.

Corollary 4.20. *Let P be a Sylow p-subgroup of G. Then the following are equivalent.*

1. *P is the unique Sylow p-subgroup of G ($n_p = 1$)*
2. *P is normal in G*
3. *P is characteristic in G*
4. *All subgroups generated by elements of p-power order are p-groups. That is, if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.*

Examples. Let G be a finite group and let p be a prime.

1. If $|G| = p^\alpha$, then G is the unique Sylow p-subgroup of G.
2. A finite abelian group has a unique Sylow p-subgroup for each prime p. This subgroup consists of all elements with a power of p order.

4.5.1 Applications of Sylow's Theorem

Proposition. Let G be a group such that $|G| = pq$ for primes p and q with $p < q$. Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$. Then, Q is normal in G. Furthermore, if P is also normal in G, then G is cyclic.