1 Group Actions

1.1 Group Actions and Permutation Representations

Definition. Let G be a group acting on a set A

1. The *kernel* of the action is the set of elements of G that act trivially on every element of A: $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.
2. For each $a \in A$ the *stabilizer* of a in G is the set of elements of G that fix the element a: $\{g \in G \mid g \cdot a = a\}$ and is denoted by G_a.
3. An action is *faithful* if its kernel is the identity.

Note. The kernel pf an action is precisely the same as the kernel of the associated permutation representation as defined in the note in section 1.7 and is rephrased below.

Proposition 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. If G is a group a *permutation representation* of G into the symmetric group S_A for some nonempty set A. We shall say a given action of G on A *affords* or *induces* the associated representation of G.

Proposition 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.

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

1. The equivalence class $\{g \cdot \mid g \in G\}$ is called the *orbit* of G containing a.
2. 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 is some $g \in G$ such that $a = g \cdot b$.

Note.

1. Every element of S_n has a unique cycle decomposition
2. Subgroups of symmetric groups are called *permutation groups*.
3. The orbits of a permutation group will refer to its orbits on $\{1, 2, \ldots, n\}$
4. The orbits of an element $\sigma \in S_n$ will refer to the orbits of the group $\langle \sigma \rangle$.

1.2 Group Acting on Themselves by Left Multiplication - Cayley's Theorem

Note. In this section G is any group and we first consider G acting on itself (i.e., $A = G$) by left multiplication:

$$g \cdot a = ga \quad \text{for all } g \in G, a \in G$$

When G is a finite group of order n it is convenient to label the elements of G with the integers $1, 2, \ldots, n$ in order to describe the permutation representation afforded by this action. In this way the elements of G are listed as $g_1, g_2, \ldots, g_n$ and for each $g \in G$ the permutation σ_g may be described as a permutation of the indices $1, 2, \ldots, n$ as follows:

$$\sigma_g(i) = j \quad \text{if and only if} \quad gg_i = g_j.$$

Theorem 3. Let G be a group, let H be a subgroup and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

1. G acts transitively on A
2. the stabilizer of G of the point $1H \in A$ us 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. (Cayley's Theorem) Every group is isomorphic to a subgroup of symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.

Corollary 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 (Note that a group of order n need not have a subgroup of order p).

1.3 Groups Acting on Themselves by Conjugation - The Class Equation

Note. In this section we consider a group G acting on itself by *conjugation*

$$g \cdot a = gag^{-1} \quad \text{for all } g \in G, a \in G$$

Definition. Two elements a and a of G are said to be *conjugate* if G if there is some $g \in G$ such that $b = gag^{-1}$ (i.e., if and only if they are in some orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called *conjugacy classes* of G.

Definition. Two subsets S and T of G are said to be *conjugate in* G if there is some $g \in G$ such that $T = gSg^{-1}$ (i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation).

Proposition 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 of G is the index of the centralizer of s, $|G : C_g(s)|$.

Theorem 7. (The Class Equation) Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

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

Theorem 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: $Z(P) \neq 1$.

Proposition 9. 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

$$(\tau(a_1)\tau(a_2)\ldots\tau(a_{k_1}))(\tau(b_1)\tau(b_2)\ldots\tau(b_{k_2}))\ldots,$$

that is $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each i in the cycle decomposition for σ by the entry $\tau(i)$.

Definition.

1. If $\sigma \in S_n$ is the product of disjoint cycles of length $n_1, n_2, \ldots, n_r$ 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.

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

Proposition 10. 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.

Theorem 11. A_5 is a simple group.

1.4 Automorphisms

Definition. 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 $\mathrm{Aut}(G)$.

Note. $\mathrm{Aut}(G)$ is a group under composition.

Proposition 12. Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$h \mapsto ghg^{-1} \qquad \text{for each } h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Corollary 13. 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 14. For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

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

Definition. A subgroup H of a group G is called *characteristic* in G, denoted H char G, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Note.

1. Characteristic subgroups are normal,
2. if H is the unique subgroup of a given order, then H is characteristic in G, and
3. if K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$.

Proposition 15. 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 Euler's function).

Proposition 16.

1. 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 grup of order p^n is cyclic of order $p^{n-1}(p-1)$.
2. For all $n \geq 3$ the automorphism group of the cyclic group of order 2^n is isomorphic to $Z_2 \times Z_{2^{n-2}}$, and in particular is not cyclic but has a cyclic subgroup of index 2.
3. Let p be a prime and let V be an abelian group (written additively)with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is

   $$\mathrm{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p).$$

   In particular, the order of $\mathrm{Aut}(V)$ is given in section 1.4.
4. For all $n \neq 6$ we have $\mathrm{Aut}(S_n) = Inn(S_n) \cong S_n$. For $n = 6$ we have $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$.
5. $\mathrm{Aut}(D_8) \cong D_8$ and $\mathrm{Aut}(Q_8) \cong S_4$.

1.5 Sylow's Theorem

Definition. Let G be a group and let p be a prime.

1. A group of order p^α for some $\alpha \geq 0$ is called a *p-group*. Subgroups of G which are p-groups are called *p-subgroups*.
2. If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G.

3. The set of Sylow p-subgroups of G will be denoted $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p when G is clear from context).

Theorem 17. (Sylow's Theorem) Let G be a group of order $p^\alpha m$, where p is a prime not dividing m. ;

1. Sylow p-subgroups of G exist, i.e., $Syl_p(G) \neq \emptyset$.

2. If P is a sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ 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.,

$$n_p = 1 \pmod{p}.$$

   Further, n_p is the indec in G of the normalizer of $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Lemma 18. Let $P \in Sly_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Corollary 19. Let P be a Sylow p-subgroup of G. Then the following are equivalent:

1. P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$

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, i.e., 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.

Proposition 20. If $|G| = 60$ and G has more than one Sylow 5-subgroups, then G is simple.

Corollary 21. A_5 is simple

Proposition 22. If G is a simple group of order 60, then $G \cong A_5$.

1.6 The Simplicity of A_n

Theorem 23. A_n is simple for all $n \geq 5$.