## Chapter 7. Group Actions and the Sylov Theorems

**7.1 Definition:** Let $G$ be a group. A **representation** of $G$ is a group homomorphism $\rho : G \to \text{Perm}(X)$ for some set $X$. A representation $\rho : G \to \text{Perm}(X)$ is called **faithful** when it is injective.

**7.2 Remark:** Given a faithful representation $\rho : G \to \text{Perm}(X)$, we sometimes identify the group $G$ with its isomorphic image $\rho(G)$, which is a group of permutations of $X$.

**7.3 Definition:** Let $G$ be a group and let $X$ be a set. A **group action** of $G$ on $X$ is a map $* : G \times X \to X$, where for $a \in G$ and $x \in X$ we write $*(a, x)$ as $a * x$ or simply as $ax$, such that

(1) $ex = x$ for all $x \in X$, and
(2) $(ab)x = a(bx)$ for all $a, b \in G$ and all $x \in S$.

**7.4 Note:** Given a group $G$ and a set $X$, here is a natural bijective correspondence between representations $\rho : G \to \text{Perm}(X)$ and group actions $* : G \times X \to X$. The representation $\rho$ and its corresponding group action $*$ determine one another by the formula

$$a * x = \rho(a)(x) \text{ for all } a \in G, x \in X\,.$$

As an exercise, verify that given a representation $\rho$, this formula defines a group action $*$, and conversely that given a group action $*$, the formula defines a representation $\rho$.

**7.5 Definition:** Suppose that a group $G$ acts on a set $X$. The group action is called **faithful** when the corresponding representation is faithful.

**7.6 Example:** When a group $G$ acts on itself by its own operation, so $a * x = ax = \ell_a(x)$, the corresponding representation $\rho : G \to \text{Perm}(G)$ is given by $\rho(a) = \ell_a$. This map is used in the proof of Cayley's Theorem: the representation is faithful, so it gives an isomorphism from $G$ to its image $\rho(G) \leq \text{Perm}(G)$.

**7.7 Example:** When a group $G$ acts on itself by conjugation, so $a * x = axa^{-1} = c_a(x)$, the corresponding representation $\rho : G \to \text{Perm}(G)$ is given by $\rho(a) = c_a$. This map is used to show that $G/Z(G) \cong \text{Inn}(G)$: indeed we have $\text{Ker}(\rho) = Z(G)$ and $\text{Image}(\rho) = \text{Inn}(G)$ giving the isomorphism $G/Z(G) \cong \text{Inn}(G)$.

**7.8 Example:** When $F$ is a field (or a commutative ring with 1) and the group $GL_n(F)$ acts on $F^n$ by matrix multiplication, so that $A * x = Ax = L_A(x)$, the corresponding representation $\rho : GL_n(F) \to \text{Perm}(F^n)$ is given by $\rho(A) = L_A$ (so $\rho$ sends the matrix $A$ to the linear map $L_A$ given by $L_A(x) = Ax$). The representation is faithful, so its gives an isomorphism from $GL_n(F)$ (which is a set of invertible matrices) to its image (which is a set of invertible linear maps).

**7.9 Definition:** Let $G$ be a group which acts on a set $X$. For $a \in G$ we define the **fixed set** of $a$ in $X$ to be the set

$$\text{Fix}(a) = \{x \in X \big| ax = x\} \subseteq X\,.$$

For $x \in X$ we define the **orbit** of $x$ under $G$ to be the set

$$\text{Orb}(x) = \{ax \big| a \in G\} \subseteq X\,.$$

Verify that for $x, y \in S$ we have $y \in \text{Orb}(x) \iff \text{Orb}(x) = \text{Orb}(y)$ so, for the equivalence relation on $X$ given by $x \sim y \iff \text{Orb}(x) = \text{Orb}(y)$, the equivalence class of $x$ is equal to the orbit of $x$, and $X$ is equal to the disjoint union of the orbits.
The set of distinct orbits is denoted by $X/G$ so we have

$$X/G = \{\text{Orb}(x) \big| x \in X\}\,.$$

For $x \in X$ we define the **stabilizer** of $x$ in $G$ to be the subgroup

$$\text{Stab}(x) = \{a \in G \big| ax = x\} \leq G\,.$$

Note that Stab(x) $\leq G$ because $ex = x$, if $ax = x$ and $bx = x$ then $(ab)x = a(bx) = ax = x$, and if $ax = x$ then $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}x$.

**7.10 Theorem:** (*The Orbit-Stabilizer Theorem) Let $G$ be a group which acts on a set $X$. Then for all $x \in X$*

$$|G| = \big|\text{Orb}(x)\big|\big|\text{Stab}(x)\big|\,.$$

Proof: Let $x \in X$. We shall show that $\Big|\text{Orb}(x)\Big| = \Big|G/\text{Stab}(x)\Big|$. Write $H = \text{Stab}(x)$. Define a map $\Phi : G/H \to \text{Orb}(x)$ by $\Phi(aH) = ax$. Then $\Phi$ is well-defined because for $a, b \in G$ we have $aH = bH \implies b^{-1}a \in H \implies b^{-1}a\,x = x \implies ax = bx$, $\Phi$ is injective because for $a, b \in G$ we have $ax = bx \implies b^{-1}a\,x = x \implies b^{-1}a \in H \implies aH = bH$, and the map $\Phi$ is clearly surjective.

**7.11 Exercise:** Consider $D_6$ as a subgroup of $S_6$. Find Orb(1) and Stab(1).

**7.12 Exercise:** Let $G$ be the rotation group of a cube $Q$. Label the vertices of the cube by elements of $S = \{1, 2, \cdots, 6\}$, think of the elements of $G$ as permutations of $S$ and hence identify $G$ with a subgroup of $S_6$. Find $\big|\text{Orb}(1)\big|$ and $\big|\text{Stab}(1)\big|$ and hence find $|G|$.

**7.13 Theorem:** (*The Class Equation) Let $G$ be a finite group. Choose $a_1, a_2, \cdots, a_n \in G$ with one element $a_i$ selected from each conjugacy class containing more than one element. Then*

$$|G| = \big|Z(G)\big| + \sum_{i=1}^{n} \big|G/C(a_i)\big|.$$

Proof: For $a \in G$ we have $\big|\text{Cl}(a)\big| = 1 \iff bab^{-1} = a$ for all $b \in G \iff a \in Z(G)$. Say $Z(G) = \{a_{n+1}, a_{n+2}, \cdots, a_m\}$ so that $G$ has exactly $m$ distinct conjugacy classes and the elements $a_1, \cdots, a_n, a_{n+1}, \cdots, a_m$ make up exactly one element from each class. Let $G$ act on itself by conjugation, so that $b * a = bab^{-1}$. Note that for $a \in G$, we have $\text{Orb}(a) = \{xax^{-1} \big| x \in G\} = \text{Cl}(a)$ (the conjugacy class of $a$ in $G$) and we have $\text{Stab}(a) = \{x \in G \big| xax^{-1} = a\} = C(a)$ (the centralizer of $a$ in $G$). Also, by the Orbit-Stabilizer Theorem, we have $\big|\text{Orb}(a_i)\big| = \frac{|G|}{|C(a_i)|} = \big|G/C(a_i)\big|$. Since $G$ is the disjoint union of the orbits,

$$|G| = \sum_{i=1}^{m} \big|\text{Orb}(a_i)\big| = \sum_{i=1}^{n} \big|G/C(a_i)\big| + \sum_{i=n+1}^{m} 1 = \sum_{i=1}^{n} |G/C(a_i)| + |Z(G)|.$$

**7.14 Example:** Let $X$ be the set of all subgroups of a group $G$. Let $G$ act on $X$ by conjugation, so $a * H = c_a(H) = aHa^{-1}$, where $a \in G$ and $H \leq G$. For $H \in X$, that is $H \leq G$, we have

$$\begin{aligned}\text{Stab}(H) &= \big\{a \in G \big| aHa^{-1} = H\big\} = \big\{a \in G \big| aH = Ha\big\} = N_G(H),\\ \text{Orb}(H) &= \big\{aHa^{-1} \big| a \in G\big\} = \text{Cl}(H),\end{aligned}$$

where $N_G(H)$ is the normalizer of $H$ in $G$ and $\text{Cl}(H)$ is the conjugacy class of $H$ in $G$, that is the set of all subgroups conjugate to $H$ in $G$.

**7.15 Theorem:** (*Cauchy's Theorem*) *Let $G$ be a finite group. Let $p$ be a prime divisor of $|G|$. Then $G$ contains an element of order $p$. Indeed*

$$\Big|\big\{a \in G \big| |a| = p\big\}\Big| = p - 1 \bmod p(p-1)\,.$$

Proof: Let $n$ be the number of elements of order $p$ in $G$, that is $n = \Big|\big\{a \in G \big| |a| = p\big\}\Big|$. Recall that $n = 0 \mod (p-1)$ (indeed $n$ is equal to $(p-1)$ times the number of cyclic subgroups of order $p$ in $G$ because each of these subgroups has $\phi(p) = p - 1$ generators). Let $X = \big\{(x_1, x_2, \cdots, x_p) \in G^p \big| x_1 x_2 \cdots x_p = e\big\}$. Note that $|X| = |G|^{p-1}$ since to get $(x_1, x_2, \cdots, x_p) \in X$ we can choose $x_1, x_2, \cdots, x_{p-1}$ arbitrarily and then $x_p$ must be given by $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$. Note that $\mathbb{Z}_p$ acts on $X$ by cyclic permutation, that is by

$$k * (x_1, x_2, \cdots, x_p) = (x_{1+k}, x_{2+k}, \cdots, x_p, x_1, \cdots, x_k)$$

since if $x_1 x_2 \cdots x_p = e$ then $x_1 x_2 \cdots x_k = (x_{k+1} \cdots x_p)^{-1}$ so $x_{1+k} x_{2+k} \cdots x_p x_1 \cdots x_k = e$. For $x = (x_1, x_2, \cdots, x_p) \in S$, by the Orbit/Stabilizer Theorem $\big|\text{Orb}(x)\big|$ divides $|\mathbb{Z}_p| = p$ so that $\big|\text{Orb}(x)\big| \in \{1, p\}$, so we have

$$\Big|\text{Orb}(x)\Big| = \begin{cases} 1 \text{ , if } x = (a, a, \cdots, a) \text{ for some } a \in G, \text{ and} \\ p \text{ , otherwise.} \end{cases}$$

Since $X$ is the disjoint union of the orbits, we have $|X| = k + pl$ where $k$ is the number of orbits of size 1 and $l$ is the number of orbits of size $p$. Note that $k$ is equal to the number of elements $a \in G$ with $a^p = 1$, and so $k = 1 + n$. Since $|X| = |G|^{p-1} = 0 \mod p$ we have $n = k - 1 = |S| - pl - 1 = -1 \mod p$. Since $n = -1 = p - 1 \bmod p$ and $n = 0 = p - 1 \bmod (p-1)$, we have $n = p - 1 \mod p(p-1)$ by the Chinese Remainder Theorem.

**7.16 Theorem:** *Let $G$ be a finite group and let $H \leq G$. Suppose that $|G/H| = p$, where $p$ is the smallest prime divisor of $|G|$. Then $H \trianglelefteq G$.*

Proof: Let $X = G/H = \big\{aH \big| a \in G\big\}$. Since $|X| = p$ we have $\text{Perm}(X) \cong S_p$. Let $G$ act on $X$ by left multiplication, so we have $a * (bH) = abH$ for $a, b \in G$. Let $\rho : G \to \text{Perm}(X)$ be the associated representation, so $\rho(a)(bH) = abH$. Let

$$K = \text{Ker}(\rho) = \big\{a \in G \big| abH = bH \text{ for all } b \in G\big\} \trianglelefteq G\,.$$

Note that $K \leq H$ because $a \in K \implies aeH = eH \implies a \in H$. Since $K \trianglelefteq G$ (it is the kernel of a homomorphism) and $K \leq H$, we also have $K \trianglelefteq H$. By the First Isomorphism Theorem, we have $G/K \cong \rho(G) \leq \text{Perm}(X) \cong S_p$. By Lagrange's Theorem $|G/K|$ divides $|S_p| = p!$. By another application of Lagrange's Theorem, $|G/K|$ also divides $|G|$. Since $|G/K| \big| |G|$ and $p$ is the smallest prime factor of $|G|$, $|G/K|$ has no prime factors less than $p$. Since $|G/K| \big| p!$, we must have $|G/K| = 1$ or $p$. Since $|G/K| = |G/H|\,|H/K| = p|H/K|$ we have $|G/K| = p$ and $|H/K| = 1$. Thus in fact $H = K \trianglelefteq G$.

## The Sylow Theorems

**7.17 Definition:** Let $G$ be a group with $|G| = p^m \ell$ where $p$ is prime and $\gcd(p, \ell) = 1$. A **$p$-subgroup** of $G$ is a subgroup of order $p^k$ for some $k$, and a **Sylow $p$-subgroup** of $G$ is a subgroup of order $p^m$.

**7.18 Exercise:** Find the Sylow $p$-subgroups of $S_3$ and $A_4$ for $p = 2, 3$.

**7.19 Theorem:** *(The Sylow Theorems) Let $G$ be a group with $|G| = p^m \ell$ where $p$ is prime and $\gcd(p, \ell) = 1$.*

*(1) For every $0 \leq k \leq m$, $G$ has a subgroup of order $p^k$, and when $k < n$, each subgroup of order $p^k$ is normal in a subgroup of order $p^{k+1}$. In particular, $G$ has a Sylow $p$-subgroup, and every $p$-subgroup of $G$ is contained in a Sylow $p$-subgroup.*
*(2) If $P$ is a $p$-subgroup of $G$ and $S$ is a Sylow $p$-subgroup of $G$, then there exists $a \in G$ such that $aPa^{-1} \leq S$. In particular, any two Sylow $p$-subgroups of $G$ are conjugate.*
*(3) The number of distinct Sylow $p$-subgroups of $G$ divides $|G|$ and is equal to 1 mod $p$.*

Proof: To prove Part 1, note that the trivial subgroup of $G$ is a $p$-subgroup of order $p^0$. By induction, it suffices to show that for every $p$-subgroup $P \leq G$ with $|P| = p^k$ for $0 \leq k < m$ we have $P \trianglelefteq H$ for some $H \leq G$ with $|H| = p^{k+1}$. Let $0 \leq k < m$ and let $P \leq G$ with $|P| = p^k$. Consider the action of $P$ on the set of left cosets $G/P$ given by $x * (aP) = xaP$. Note that $G/P$ is the disjoint union of the orbits, and the size of each orbit divides $|P| = p^k$. Some of the orbits have size 1 and the size of all other orbits is a multiple of $p$, and so $|G/P|$ is equal to the number of orbits of size 1, modulo $p$. For $a \in G$,

$$\begin{aligned} |\text{Orb}(aP)| = 1 &\iff xaP = aP \text{ for all } x \in P \iff a^{-1}xa \in P \text{ for all } x \in P \\ &\iff a^{-1}Pa = P \iff Pa = aP \iff a \in N(P) = N_G(P), \end{aligned}$$

so the number of orbits of size 1 is equal to the number of cosets $aP$ with $a \in N(P)$, which is equal to $N(P)/P$. Thus we have $|N(P)/P| \equiv |G/P| \equiv 0 \mod p$. By Cauchy's Theorem, since $p$ divides $|N(P)/P|$ it follows that the group $N(P)/P$ contains an element of order $p$, hence a subgroup of order $p$. This subgroup is of the form $H/P$ where $P \leq H \leq N(P) \leq G$. Since $P \trianglelefteq N(P)$ we also have $P \trianglelefteq H$. Since $|H/P| = p$ and $|P| = p^k$ we have $|H| = p^{k+1}$.

To prove Part 2, let $P$ be a $p$-subgroup of $G$ with $|P| = p^k$, and let $S$ be a Sylow $p$-subgroup of $G$. Consider the action of $P$ on the $G/S$ given by $x(aS) = xaS$. Since $G/S$ is equal to the disjoint union of the orbits, and the size of each orbit divides $|P| = p^k$, it follows that $|G/S|$ is equal to the number of orbits of size 1, modulo $p$. Since $|G/S| \neq 0 \mod p$, there is at least one orbit of size 1, so we can choose $a \in G$ such that $xaS = aS$ for all $x \in P$. Then we have $a^{-1}xa \in S$ for all $x \in P$, so that $a^{-1}Pa \leq S$, and hence $P \leq aSa^{-1}$. Finally, note that $aSa^{-1}$ is a Sylow $p$-subgroup of $G$.

To prove Part 3, let $X$ be the set of all Sylow $p$-subgroups of $G$, and choose $S \in X$. By Part 2, $G$ acts on $X$ by conjugation, that is by $a * T = aTa^{-1}$ where $a \in G$, $T \in X$, and the number of Sylow $p$-subgroups is $|X| = \big|\text{Orb}(S)\big|$, which divides $G$. Likewise, we can consider the action of $S$ on $X$ by conjugation. Since $X$ is the disjoint union of the orbits, and the size of each orbit divides $|S| = p^m$, it follows that $|X|$ is equal to the number of orbits of size 1, modulo $p$. For $T \in X$, we have

$$|\text{Orb}(T)| = 1 \iff aTa^{-1} = T \text{ for all } a \in S \iff S \leq N(T) = N_G(T).$$

Since $S$ and $T$ are Sylow $p$-subgroups of $G$, they are also Sylow $p$-subgroups of $N(T)$, and so they are conjugate in $N(T)$ by Part 2, and since $T \trianglelefteq N(T)$ it follows that $S = T$. Thus there is only one orbit of size 1, namely $\{S\}$, so we have $|X| \equiv 1 \mod p$, as required.