II.4. Group Actions

(4.1) A **group action** of a group $G$ acting on a set $S$ is a map from $G \times S$ to $S$ (written as $g \cdot s$ or $g(s)$ for $g \in G$ and $s \in S$) such that $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$ and $e_G \cdot s = s$.

If a group $G$ is acting on a set $S$, we call $S$ a $G$-**set**. Suppose $S$ is a $G$-set. Define a relation $s_1 \sim s_2 \iff s_1 = g(s_2)$ for some $g \in G$, then $\sim$ is an equivalence relation. (The equivalence classes are called **orbits** of $S$ under $G$. If an orbit contains $s \in S$, then the orbit is called the **orbit of** $s$. The orbit of $s := s_G = \{g(s) | g \in G\}$.)

**Proof:** Check definition of equivalence relation.

(4.1a) Let $H \leq G$ and $S$ be the left cosets of $H$. Then $g \cdot aH = (ga)H$ is an action of $G$ on $S$, called the left multiplication action.

(4.1b) Let $H$ be a subgroup of $G$, and $a, b \in G$. Define $a \sim b \iff$ for some $g \in H$, $a = hbh^{-1}$. Verify that $\sim$ is an equivalence relation. Then $h \cdot a = hah^{-1}$ is an action of $H$ on $G$, (called the action of $H$ on $G$ by conjugation). The orbits of $G$ acting on $G$ by conjugation are called **conjugacy classes**.

(4.1c) Let $G \leq S_\Omega$. Then $G$ acts on $\Omega$ by $g \cdot s = g(s)$. If $G = \langle g \rangle$, then the cycle decomposition of $g$ gives the orbits of this action.

(4.2) Suppose that $G$ is acting on a set $\Omega$. For $s \in \Omega$, the **stabilizer** of $s$ in $G$ is

$$G_s = \{g \in G | gs = s\}.$$

The **kernel** of the action is

$$ker(G/\Omega) = \{g \in G | gs = s, \forall s \in \Omega\}.$$

Then

(i) $G_s \leq G$.

(ii) There is a group homomorphism $\phi : G \rightarrow S_\Omega$ such that $ker(G/\Omega) = ker(\phi) \leq G$.

**Proof:** (i) For $g_1, g_2 \in G_s$, $g_1 g_2(s) = g_1(g_2(s)) = g_1(s) = s$, and $g_1^{-1}(s) = g_1^{-1}(g_1(s)) = e(s) = s$.

(ii) $\forall g \in G$, let $\phi(g) : \Omega \rightarrow \Omega$ be given by $\phi(g)(s) = g(s)$. Since $g^{-1}(g(s)) == e(s) = s$, $\phi(g)$ is onto. Since $g(s_1) = g(s_2)$ implies that $s_1 = g^{-1}(g(s_1)) = g^{-1}(g(s_2)) = s_2$, $\phi(g)$ is 1-1. Therefore, $\phi(g) \in S_\Omega$. That $g_1(g_2(s)) = (g_1 g_2)(s)$ implies that $\phi$ is a group homomorphism. Finally,

$$ker(\phi) = \{g \in G : \phi(g) = \text{identity in } S_\Omega\} = \{g \in G : \phi(g)(s) = s, \forall s \in \Omega\} = ker(G/\Omega).$$
(4.2a) Let $A \subseteq G$ and let $G$ acts on $S = G$ by **conjugation**, i.e. $g(x) = gxg^{-1}, \forall x \in S, g \in G$. Then $\ker(G/A) = C_G(A)$. In particular, $\ker(G/G) = Z(G)$.

**Proof** Checking definition.

(4.2b) Conjugation in $S_n$: If $\sigma = (a_1a_2\cdots a_k)(b_1b_2\cdots b_k)\cdots$ and $\tau \in S_n$, then

$$\tau \sigma \tau^{-1} = (\tau(a_1)\tau(a_2)\cdots \tau(a_k)) (\tau(b_1)\tau(b_2)\cdots \tau(b_k)) \cdots$$

(4.2c) Definition: for a positive integer $n$, a partition of $n$ is a nondecreasing sequence of integers $0 < n_1 \leq n_2 \cdots n_r$ such that $\sum_{i=1}^{r} n_i = n$. If a permutation $\sigma \in S_n$ is the product of disjoint cycles of length $n_1, n_2, \ldots, n_r$, respectively, where $0 < n_1 < \cdots < n_r$ is a partition of $n$, then the **cycle type** of $\sigma$ is $n_1, n_2, \ldots, n_r$.

Two elements of $S_n$ are conjugate if and only if they have the same cycle type. The number of conjugacy classes of $S_n$ is the same as the number of partitions of $n$.

(4.3) A group $G$ acts **transitively** on a set $S$ if for any pair $s, s' \in S$, there is a $g \in G$ such that $g(s) = s'$. (In other words, $G$ has only one orbit: $G = s_G$ for any $s \in S$).

Let $H \leq G$, and let $G$ acts on the set $X$ of left cosets of $H$ by left multiplication $(g(fH)) = (gf)H$. Then

(i) $G$ acts transitively.

(ii) $G_H = H$.

(iii) $\ker(G/X) = \cap_{g \in G} gHg^{-1}$, which is the largest normal subgroup of $G$ contained in $H$.

**Proof** (i) and (ii) follows by definition.

$$\ker(G/X) = \{g \in G \mid g(xH) = xH, \forall x \in G\}$$

$$= \{g \in G \mid x^{-1}gx \in H, \forall x \in G\}$$

$$= \{g \in G \mid g \in xHx^{-1}, \forall x \in G\}.$$

Thus $\ker(G/X) \leq G$. When $x = 1$, we have $\ker(G/X) \leq H$. Use definition to show that if $N \leq G$ and $N \leq H$, then $N \leq \ker(G/X)$.

(4.3a) (Cayley, Thm 4.6) Every group is isomorphic to a subgroup of a symmetric group $S_{|G|}$.

**Proof** Let $G$ acts on $G$ by left (or right) multiplication.

(4.3b) If $|G| = n < \infty$ and if $p$ is the smallest prime dividing $n$, then any subgroup $H$ of index $p$ is normal.

**Proof:** Assume $|G : H| = p$. Let $L$ be the collection of left coset of $H$ in $G$ and let $G$ act on $L$ by left multiplication: $g(xH) = (gx)H$. Let $K = \ker(G/L)$ be the kernel of the action. (want to show $H = K$) By (4.3)(iii), $K \leq H$, and so by the index formula:

By the 1st Iso Thm, $G/K$ is iso to a subgroup of $S_p$ (since $|L| = |G : H| = p$), and so by Lagrange’s Thm,

$$p|H : K| = |G/K|$$

is a factor of $|S_p| = p! \implies |H : K|$ is a factor of $(p - 1)!$.

Since $p$ is the smallest prime factor of $|G|$, $|H : K| = 1$.

(4.4) (Thm 4.3) If $X$ is an $G$-set and if $x \in X$, then $|x_G| = |G : G_x|$.

Proof Define $\phi : x_G \to \{\text{ left cosets of } G_x\}$ by: $\phi(g(x)) = gG_x$. Verify that $\phi$ is well defined: If $h(x) = g(x)$, then $g^{-1}h \in G_x$ and so $gG_x = hG_x$.

$\phi$ is an injection: $\phi(g(x)) = \phi(h(x)) \iff gG_x = hG_x \iff g = hk$ for some $k \in G_x$.

$\phi$ is onto: Definition.

(4.5) (Burnside) Let $G$ be a finite group and $X$ be a finite $G$-set. For each $g \in G$, define $X_g = \{x \in X | g(x) = x\}$. If $r$ denotes the number of orbits in $X$ under $G$, then

$$r|G| = \sum_{g \in G} |X_g|.$$

Proof: Let $(x_1)_G, (x_2)_G, \cdots, (x_r)_G$ be the orbits of $X$ under $G$. Let $P$ denote all the pairs $(x, g)$ where $g(x) = x$. ($P$ is number of 1’s in the $|X| \times |G|$ (0,1)-matrix where the $(x, g)$ entry is 1 iff $g(x) = x$. Thus $|X_g|$ = number of 1’s in the $g$th column and $|G_x|$ = number of 1’s in the $x$th row.) Hence

$$|P| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$

By (1.4), $|G_x| = |G|/|x_G|$, and so

$$\sum_{x \in X} |G_x| = |G| \sum_{x \in X} \frac{1}{|x_G|} = |G| \sum_{i=1}^{r} \sum_{x \in (x_i)_G} \frac{1}{|x_G|} = |G| \sum_{i=1}^{r} 1 = |G|r.$$

(4.6) Let $X$ be a $G$-set. The fixed points of the action is

$$X_G = \{x \in X | g(x) = x \forall g \in G\}.$$

$X_G$ is the union of all single element orbits. If $(x_1)_G, (x_2)_G, \cdots, (x_s)_G$ are the orbits of $X$ under $G$ that are non-single-element orbits, then

$$|X| = |X_G| + \sum_{i=1}^{s} |(x_i)_G|.$$
Proof: By (4.1).

(4.6a) (The Class Equation, Cor 4.5) Let \(|G| < \infty\) and let \(g_1, g_2, \cdots, g_r\) be representatives of the distinct conjugacy classes of \(G - Z(G)\). Then

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

Proof: Let \(G\) acts on \(X = G\) by conjugation. Then \(X_G = Z(G)\) and \(C_G(g_i) = Gg_i\). (4.6a) follows by (4.4).

(4.7) Let \(G\) be a group of order \(p^n\) for some prime \(p\), and let \(X\) be a finite \(G\)-set. Then

\[ |X| \equiv |X_G| \pmod{p}. \]

Proof: By (4.4), each \(|(x_i)_G|\) is a factor of \(|G| = p^n\). (4.6b) follows then by (4.6).

(4.7a) If \(|G| = p^n\) for some prime \(p\), then \(|Z(G)| > 1\).

Proof: \(G\) acts on \(X = G\) by conjugation. By (4.7), \(p\) divides \(|X_G|\) and \(1 \in X_G\).

(4.7b) If \(|G| = p^2\), then \(G \in \{Z_{p^2}, Z_p \times Z_p\}\).

Proof \(G/Z(G)\) is cyclic. By (1.4.9a), \(G\) is abelian. If \(G\) has an element or order \(p^2\), then \(G = Z_{p^2}\). Otherwise choose \(x \in G\) with \(|x| = p\) and \(y \in G - \langle x \rangle\). Show \(G = \langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle\).

(4.8) (Cauhy, Thm 5.2) If \(|G| < \infty\) and if \(p\) is a prime dividing \(|G|\), then there is some \(g \in G\) such that \(|g| = p\).

Proof Let \(X = \{(g_p, \cdots, g_2, g_1)| g_i \in G\) and \(g_p \cdots g_2 g_1 = 1\}\).

(Step 1) \(|X| = |G|^{p-1} (g_p = (g_{p-1} \cdots g_2 g_1)^{-1})\). Since \(p\) divides \(|G|\), \(p\) divides \(|X|\).

(Step 2) Let \(\sigma = (1, 2, \cdots, p)\) and \(H = \langle \sigma \rangle\). Let \(\sigma\) act on \(X\) by \(\sigma(g_p, \cdots, g_2, g_1) = (g_{\sigma(p)}, \cdots, g_{\sigma(2)}, g_{\sigma(1)}) = (g_1, g_p, \cdots, g_3, g_2) \in X\). By (4.7), \(|X| \equiv |X_H| \pmod{p}\). By (Step 1) and since \((1, 1, 1, \cdots, 1) \in X_H\), \(X_H\) has at least \(p\) elements. Note that \(\sigma(g_p, \cdots, g_2, g_1) = (g_p, \cdots, g_2, g_1)\) implies \(a = g_1 = g_2 = \cdots = g_p\) and so \(|a| = p\).