MATH 436 Notes: Group Actions.

Jonathan Pakianathan

September 30, 2003

1 Group Actions

Definition 1.1. *We say that a group G acts on a set X (on the left) if there is an action $G \times X \stackrel{\cdot}{\to} X$ such that:*
[A1:] *$e \cdot x = x$ for all $x \in X$.*
[A2:] *$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $g_1, g_2 \in G, x \in X$.*

Proposition 1.2. *Given a group G acting on a set X, we define $\rho : G \to \Sigma(X)$ via $\rho(g)(x) = g \cdot x$ for all $x \in X, g \in G$. Then ρ is a homomorphism called the* **action homomorphism** *associated to the action of G on X.*

Furthermore every homomorphism $\lambda : G \to \Sigma(X)$ is the action homomorphism for a unique (left) action of G on X.

Proof. First note that $\rho(g) : X \to X$ is a well-defined function so is in the monoid $M(X) = \{f : X \to X\}$.

We then compute:

$$(\rho(g) \circ \rho(h))(x) = g \cdot (h \cdot x) \stackrel{A2}{=} (gh) \cdot x = \rho(gh)(x)$$
$$\rho(e)(x) = e \cdot x \stackrel{A1}{=} x = 1_X(x)$$

for all $g, h \in G$ and $x \in X$. Thus $\rho(gh) = \rho(g) \circ \rho(h), \rho(e) = 1_X$ and ρ is hence a homomorphism of monoids $G \to M(X)$.

Then we note $1_X = \rho(e) = \rho(gg^{-1}) = \rho(g) \circ \rho(g^{-1})$ and similarly $1_X = \rho(g^{-1}) \circ \rho(g)$ and so the $\rho(g)$ are bijections $G \to G$ for all $g \in G$. Thus ρ is a homomorphism $G \to \Sigma(X)$.

Given a homomorphism $\lambda : G \to \Sigma(X)$, in order for it to be the action homomorphism of an action of G on X, we must define the action via

$$g \cdot x = \lambda(g)(x).$$

We leave it to the reader to check that this indeed defines an action of G on X. Thus every homomorphism $\lambda : G \to \Sigma(X)$ is the action homomorphism of a unique action of G on X. $\square$

Definition 1.3 (Orbits). *Given an action of G on X, and $x \in X$ we define the orbit of x, denoted $\mathcal{O}_x$ by*

$$\mathcal{O}_x = \{g \cdot x | g \in G\}.$$

We say that G acts transitively on X if $X = \mathcal{O}_x$ for some $x \in X$, i.e., if X consists of a single orbit.

If $\mathcal{O}_x = \{x\}$, i.e., $g \cdot x = x$ for all $g \in G$, we call x a fixed point of the action. We let $X^G = \{x \in X | g \cdot x = x \text{ for all } g \in G\}$ denote the set of all fixed points of the action.

Now we look at some examples:

Example 1.4 (Canonical Symmetric Group Action). *Σ_n acts on $X = \{1, 2, \ldots, n\}$ via $\sigma \cdot j = \sigma(j)$ for all $\sigma \in \Sigma_n, j \in X$. We check:*
[A1]: $e \cdot j = 1_X \cdot j = 1_X(j) = j$,
[A2]: $(\sigma \circ \mu) \cdot j = \sigma(\mu(j)) = \sigma \cdot (\mu \cdot j)$
for all $j \in X$, $\sigma, \mu \in \Sigma_n$. Thus this is indeed an action of Σ_n on X. It is easily verified that the action homomorphism $\rho : \Sigma_n \to \Sigma(X) = \Sigma_n$ is the identity map.

Since $(1i) \cdot 1 = i$ for all $i \in X$, we see that $\mathcal{O}_1 = X$ and so the action is transitive.

Since $(ij) \cdot i = j$ for all $i, j \in X$, we see that $X^{\Sigma_n} = \emptyset$ when $n > 1$.

Example 1.5 (Canonical General Linear Action). *$GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ via $\mathbb{A} \cdot \hat{x} = \mathbb{A}\hat{x}$. Here we view $\hat{x} \in \mathbb{R}^n$ as a n-dimensional column vector. We check:*
[A1]: $\mathbb{I} \cdot \hat{x} = \mathbb{I}\hat{x} = \hat{x}$,
[A2]: $(\mathbb{AB}) \cdot \hat{x} = (\mathbb{AB})\hat{x} = \mathbb{A}(\mathbb{B}\hat{x}) = \mathbb{A} \cdot (\mathbb{B} \cdot \hat{x})$
for all $\mathbb{A}, \mathbb{B} \in GL_n(\mathbb{R})$ and $\hat{x} \in \mathbb{R}^n$.

Thus this is an action of $GL_n(\mathbb{R})$ on $\mathbb{R}^n$. Note that $\mathbb{A}\hat{0} = \hat{0}$ for all $\mathbb{A} \in GL_n(\mathbb{R})$ and so the zero vector, $\hat{0}$ is a fixed point of the action.

Fix $\hat{x}, \hat{y} \neq \hat{0}$ then $\hat{x}$ is the first element of some basis B_x of $\mathbb{R}^n$ and $\hat{y}$ is the first element of some basis B_y of $\mathbb{R}^n$. From linear algebra, we know there is an invertible change of basis matrix $\mathbb{P}$ which takes one basis to the other and so in particular, $\mathbb{P} \cdot \hat{x} = \hat{y}$.

Thus we conclude $\mathcal{O}_{\hat{x}} = \mathbb{R} - \{\hat{0}\}$ for all $\hat{x} \neq \hat{0}$. Thus $\mathbb{R}^n = \mathcal{O}_{\hat{x}} \cup \mathcal{O}_{\hat{0}}$ is the union of two orbits.

Example 1.6 (Conjugation Action). *We have previously studied the homomorphism $\Theta : G \to Aut(G) \subseteq \Sigma(G)$ given by $\Theta(g)(h) = ghg^{-1}$ for all $g, h \in G$. This is the action homomorphism for an action of G on G given by $g \cdot h = ghg^{-1}$. This action is called the action of G on itself by conjugation.*

If we consider the power set $P(G) = \{A \subseteq G\}$ then the conjugation action induces an action of G on $P(G)$ via $g \cdot A = gAg^{-1}$ for all $g \in G, A \in P(G)$.

Note if $A \leq G$ then $gAg^{-1} = \gamma_g(A)$ is also a subgroup of G as it is the image of A under a homomorphism. Thus the action also induces an action of G on the set $Subgrp(G) = \{H | H \leq G\}$ given by $g \cdot H = gHg^{-1}$ for all $g \in G, H \leq G$.

It is easy to see that $Subgrp(G)^G = \{N | N \trianglelefteq G\}$ under this action.

Example 1.7 (Left Translation Action). *G also acts on itself by left translation. This is given precisely by $g \cdot h = gh$ for all $g, h \in G$. The action homomorphism $L : G \to \Sigma(G)$ is injective. This is because*

$$\begin{aligned} g \in ker(L) &\leftrightarrow L(g) = 1_G \\ &\leftrightarrow gh = h \text{ for all } h \in G \\ &\leftrightarrow g = e. \end{aligned}$$

Thus G is isomorphic to $Im(L) \leq \Sigma(G)$ which proves Cayley's Theorem that every finite group is isomorphic to a subgroup of Σ_n for some integer $n \geq 1$.

The action of left translation is transitive as given $h, h' \in G$ we have $(h'h^{-1}) \cdot h = h'$.

We are now ready to prove our fundamental theorem regarding group actions:

Theorem 1.8 (Fundamental Theorem of Group Actions). *Suppose a group G is acting on a set X. Let $x_0 \in X$, then:*
(1) $G_{x_0} = \{g \in G | g \cdot x_0 = x_0\}$ is a subgroup of G called the isotropy subgroup of x_0.
(2) There is a bijection $G/G_{x_0} \to \mathcal{O}_{x_0}$ for all $x_0 \in X$. Thus $|\mathcal{O}_{x_0}| = |G : G_{x_0}|$.
(3) Any two orbits $\mathcal{O}_x, \mathcal{O}_y$ are either disjoint or equal. Thus the set of orbits

partition X. If $|X| < \infty$ and I is a set of orbit representatives for the distinct orbits of G on X, then

$$|X| = \sum_{x \in I} |\mathcal{O}_x| = \sum_{x \in I} |G : G_x|.$$

Among the orbits, are the orbits of size 1, i.e., the fixed points which we may separate out in the sum. Thus if J is a set of orbit representatives for the distinct orbits of size > 1 then:

$$|X| = |X^G| + \sum_{x \in J} |G : G_x|.$$

(4) If x and y lie in the same orbit then the isotropy subgroups G_y and G_x are conjugate, i.e. $G_y = gG_xg^{-1}$ for some $g \in G$.

Proof. **Proof of (1):** $e \in G_{x_0}$ as $e \cdot x_0 = x_0$. If $g \in G_{x_0}$ then $x_0 = g \cdot x_0$. Acting on both sides with g^{-1} we find $g^{-1} \cdot x_0 = g^{-1} \cdot (g \cdot x_0) = (g^{-1}g) \cdot x_0 = e \cdot x_0 = x_0$ so $g^{-1} \in G_{x_0}$. Finally if $g, h \in G_{x_0}$ then $(gh) \cdot x_0 = g \cdot (h \cdot x_0) = g \cdot x_0 = x_0$ and so $gh \in G_{x_0}$. Thus $G_{x_0} \leq G$.
Proof of (2): Define $f : G/G_{x_0} \to \mathcal{O}_{x_0}$ via $f(gG_{x_0}) = g \cdot x_0$. To check that f is a well-defined function, suppose $gG_{x_0} = hG_{x_0}$ then $g = hw$ where $w \in G_{x_0}$. Thus

$$f(gG_{x_0}) = g \cdot x_0 = (hw) \cdot x_0 \overset{A2}{=} h \cdot (w \cdot x_0) = h \cdot x_0 = f(hG_{x_0}).$$

Thus f is well-defined. It is obvious that f is onto. To show injectivity, suppose $f(gG_{x_0}) = f(hG_{x_0})$. Then $g \cdot x_0 = h \cdot x_0$ and hence $h^{-1}g \in G_{x_0}$. Then $gG_{x_0} = h(h^{-1}g)G_{x_0} = hG_{x_0}$ and so f is injective. So we see that f gives a well-defined bijection between G/G_{x_0} and $\mathcal{O}_{x_0}$.
Proof of (3): Let $\mathcal{O}_x, \mathcal{O}_y$ be two orbits and assume $\mathcal{O}_x \cap \mathcal{O}_y \neq \emptyset$. Take α from the intersection then:

$$g \cdot x = \alpha = h \cdot y$$

for some $g, h \in G$. This gives $y = h^{-1} \cdot (g \cdot x) = (h^{-1}g) \cdot x$. Then

$$\mathcal{O}_y = \{w \cdot y | w \in G\} = \{(wh^{-1}g) \cdot x | w \in G\} = \{t \cdot x | t \in Gh^{-1}g = G\} = \mathcal{O}_x.$$

Thus two orbits are either disjoint or equal and hence the set of distinct orbits partition X. The rest of (3) follows immediately.

Proof of (4): If y and x lie in the same orbit then $y = g \cdot x$. Then:

$$\begin{aligned}\alpha \in G_y &\leftrightarrow \alpha \cdot y = y \\ &\leftrightarrow (\alpha g) \cdot x = g \cdot x \\ &\leftrightarrow (g^{-1}\alpha g) \cdot x = x \\ &\leftrightarrow g^{-1}\alpha g \in G_x \\ &\leftrightarrow \alpha \in gG_xg^{-1}\end{aligned}$$

Thus $G_y = gG_xg^{-1}$ and the two isotropy subgroups are conjugate. □

We now return to our previous examples of actions and apply the fundamental theorem of group actions!

Example 1.9 (Conjugacy classes and Centralizers). *By Example 1.6, G acts on itself via conjugation. If $x \in G$, we compute the isotropy subgroup:*

$$G_x = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}.$$

This is called the centralizer subgroup of x, and is denoted $C_G(x)$. It consists of all the elements of G which commute with x.

Thus the set of fixed points G^G is the center of G, $Z(G)$.

The orbit of x, $\mathcal{O}_x$ is called the conjugacy class of x. The elements y in this orbit are of the form gxg^{-1} and are called the conjugates of x.

It follows that the number of distinct conjugates of x is equal to the index $|G : C_G(x)|$ by (2) of Theorem 1.8.

If I is a set of conjugacy class representatives and J is a set of noncentral conjugacy class representatives, then (3) of Theorem 1.8 gives:

$$|G| = \sum_{x \in I} |G : C_G(x)| = |Z(G)| + \sum_{x \in J} |G : C_G(x)|.$$

This is called the **class equation** *of G.*

Example 1.10 (Conjugate subgroups and Normalizers). *By Example 1.6, G acts on $Subgrp(G)$ via $g \cdot H = gHg^{-1}$. If $H \leq G$ we compute the isotropy subgroup:*

$$G_H = \{g \in G | gHg^{-1} = H\} = \{g \in G | gH = Hg\}.$$

This is called the normalizer subgroup of H and is denoted $N_G(H)$.

Notice as $hH = H = Hh$ for all $h \in H$, $H \leq N_G(H)$ in general and furthermore $H \trianglelefteq N_G(H)$ by the definition of $N_G(H)$. It is easy to check that in fact $N_G(H)$ is the largest subgroup of G in which H is normal, hence the name normalizer. It follows then that $H \trianglelefteq G \leftrightarrow G = N_G(H)$.

$\mathcal{O}_H = \{gHg^{-1} | g \in G\}$ is the set of conjugate subgroups of H. By (2) in Theorem 1.8, the number of distinct conjugates of a subgroup H is equal to the index $|G : N_G(H)|$.

As an application of the class formula, let us prove some basic facts about p-groups which we define next.

Definition 1.11. *Let p be a prime number. A group P is called a p-group if $|P| = p^n$ for some $n \in \mathbb{N}$.*

Theorem 1.12 (Nontrivial p-groups have nontrivial center). *Let P be a p-group with $|P| > 1$. Then $|Z(P)| > 1$.*

Proof. $|P| = p^n$ for some integer $n \geq 1$. From the class equation we have:

$$|P| = |Z(P)| + \sum_{x \in J} |P : C_P(x)|$$

where J is a set of noncentral conjugacy class representatives.

For $x \in J$, $|P : C_P(x)| > 1$ and so is of the form p^k for some $1 \leq k \leq n$ as indices must divide the order of the group.

Thus modulo p, the class equation becomes $0 \equiv |Z(P)| \bmod p$. Thus $|Z(P)| = mp$ for some $m \in \mathbb{N}$. Since $e \in Z(P)$, $m > 0$ and $|Z(P)| \geq p > 1$. □

Before we prove the next theorem on p-groups, we record a lemma which is interesting of its own right.

Lemma 1.13 ($Inn(G)$ cannot be a nontrivial cyclic group). *For any group G, if $G/Z(G)$ is cyclic then $G = Z(G)$. Thus the only time $Inn(G)$ is cyclic is when G is Abelian and $Inn(G) = 1$.*

Proof. Suppose $G/Z(G)$ is cyclic generated by $\alpha Z(G)$ say.

For $x, y \in G$ we then have $xZ(G) = \alpha^n Z(G)$ and so $x = \alpha^n z$ for some $n \in \mathbb{Z}, z \in Z(G)$. Similarly $y = \alpha^m z'$ for some $m \in \mathbb{Z}, z' \in Z(G)$.

Then we compute $xy = \alpha^n z \alpha^m z' = \alpha^{n+m} z z'$ where we have used that z, z' are central and so can be commuted with any element.

Similarly $yx = \alpha^m z' \alpha^n z = \alpha^{n+m} zz'$. Hence $xy = yx$ for all $x, y \in G$ and G is Abelian. Thus $G = Z(G)$ and $G/Z(G) = 1$.

The statements about $Inn(G)$ follow as $Inn(G) \cong G/Z(G)$ in general.

□

Theorem 1.14 (Groups of order p and p^2). *Let p be a prime then every group of order p is cyclic and hence isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Every group of order p^2 is Abelian.*

Proof. Suppose $|G| = p$, p a prime. Let $x \neq e, x \in G$. Then $o(x) = p$ as orders of elements must divide the order of the group. Hence $G =< x >$ is cyclic and so is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Suppose $|G| = p^2$ and consider $Z(G)$. Since $Z(G)$ is a subgroup of G, and by Theorem 1.12, it follows that either $|Z(G)|$ is p or it is p^2. In the latter case $G = Z(G)$ is Abelian and we are done so we only have to consider the case that $|Z(G)| = p$.

Assume $|Z(G)| = p$ then $|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$ and so $G/Z(G)$ is cyclic of order p. This is impossible by Lemma 1.13 and so this case does not exist.

□