MAS 305 **Algebraic Structures II**

Notes 4 **Autumn 2006**

Group actions

Definition Given a group G, an *action* of G on a set Ω is a homomorphism from G into the group of all permutations of Ω.

We usually write the homomorphism as π, and $g\pi$ as π_g, so π_g is a permutation of Ω for all g in G. It is usually easy to see that each π_g is a function from Ω to itself. Then being an action means that

$$\pi_g \text{ is a permutation} \qquad \text{for all } g \text{ in } G \tag{1}$$

and

$$\pi_g \pi_h = \pi_{gh} \qquad \text{for all } g, h \text{ in } G. \tag{2}$$

In particular, putting $h = 1_G$ in (2) gives

$$\pi_g \pi_{1_G} = \pi_g \qquad \text{for all } g \text{ in } G.$$

Since π_g is a permutation (by (1)), it is invertible, and so

$$\pi_{1_G} \text{ is the identity permutation of } \Omega. \tag{3}$$

Thus (1) and (2) imply (2) and (3). Conversely, if (2) and (3) hold and $g \in G$ then

$$\pi_g \pi_{g^{-1}} = \pi_{1_G} = \text{identity permutation of } \Omega,$$

so π_g is invertible and therefore is a permutation. (Incidentally, this also shows that $(\pi_g)^{-1} = \pi_{g^{-1}}$.) This shows that conditions (2) and (3) imply (1) and (2). It is usually easier to check condition (3) than condition (1).

The kernel of π is called the *kernel of the action*. We say that G acts *faithfully* on Ω if $\ker(\pi) = \{1_G\}$.

Example Put $\Omega = G$. For g in G, define π_g by

$$x\pi_g = xg \qquad \text{for } x \text{ in } \Omega.$$

Then

$$x\pi_{1_G} = x1_G = x \qquad \text{for all } x \text{ in } G,$$

so π_{1_G} is the identity permutation of Ω, and

$$x\pi_g\pi_h = xg\pi_h = xgh = x\pi_{gh},$$

for all x in Ω, so $\pi_g\pi_h = \pi_{gh}$ for all g, h in G, so this is an action. It is called the *right regular action* of G on itself. It is faithful because if π_g is the identity permutation then $x\pi_g = x$ so $xg = x$ so $g = 1_G$.

Cayley's Theorem Every group is isomorphic to a group of permutations.

Proof Given a group G, let π be its right regular action. Then $\mathrm{Im}(\pi)$ is a group of permutations. By the First Isomorphism Theorem, $G/\ker(\pi) \cong \mathrm{Im}(\pi)$. But $\ker(\pi) = \{1_G\}$ and $G/\{1_G\} \cong G$. □

Given an action π of G on Ω, write $\alpha \sim \beta$ (for α, β in Ω) if there is some g in G with $\alpha\pi_g = \beta$.

Lemma $\sim$ is an equivalence relation on Ω.

Proof
(a) π_{1_G} is the identity permutation, so $\alpha\pi_{1_G} = \alpha$ for all α in Ω, so $\alpha \sim \alpha$ for all α in Ω. Thus $\sim$ is reflexive.

(b) If $\alpha \sim \beta$ then there is some g in G with $\alpha\pi_g = \beta$. Now, $(\pi_g)^{-1} = \pi_{g^{-1}}$, so $\beta\pi_{g^{-1}} = \beta(\pi_g)^{-1} = \alpha\pi_g\pi_g^{-1} = \alpha$, so $\beta \sim \alpha$. Therefore $\sim$ is symmetric.

(c) If $\alpha \sim \beta$ and $\beta \sim \gamma$ then there are g, h in G with $\alpha\pi_g = \beta$ and $\beta\pi_h = \gamma$. Then $\gamma = \beta\pi_h = \alpha\pi_g\pi_h = \alpha\pi_{gh}$, because π is a homomorphism, so $\alpha \sim \gamma$. Therefore $\sim$ is transitive. □

Definition The equivalence classes of $\sim$ are called *orbits*. The orbit containing α is written α^G. If there is only one orbit then G is *transitive* on Ω.

Warning: note the two different meanings of the word *transitive*!

The right regular action is transitive because, given any x, y in G, we can put $g = x^{-1}y$ and then $x\pi_g = xg = xx^{-1}y = y$, so $x \sim y$.

Example Let $G = \mathrm{GL}(2,3) = \{$all invertible 2×2 matrices with entries in $\mathbb{F}_3\}$. Here $\mathbb{F}_3$ denotes the finite field with 3 elements, which is just the integers modulo 3. The first row of such a matrix can be any ordered pair of elements from $\mathbb{F}_3$ except $(0,0)$, so there are $3^2-1=8$ possibilities. The second row can be any ordered pair which is not a scalar multiple of the first row, so there are $3^2-3=6$ possibilities. Hence $|\mathrm{GL}(2,3)| = 8\times 6 = 48$.

Let $\Omega = \mathbb{F}^2$, which is the set of all row vectors with 2 coordinates in $\mathbb{F}_3$. For α in Ω and g in G, define $\alpha\pi_g = \alpha g$, which is interpreted as the product of the row vector α with the matrix g, and hence is another row vector. The matrix g is invertible, so π_g is a permutation. Moreover, $\alpha\pi_g\pi_h = (\alpha g)h = \alpha(gh)$ by the usual rules for matrix multiplication, so π is an action.

$|\Omega| = 3^2 = 9$. Label the nine row vectors as

$$\begin{array}{ccccccccc} (0,1) & (0,2) & (1,0) & (2,0) & (1,1) & (2,2) & (1,2) & (2,1) & (0,0) \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9. \end{array}$$

Suppose that $g = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. Then $(1,0)g = (1,0)\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = (1,2)$ so $3\pi_g = 7$. Similarly, $(0,0)g = (0,0)$ so $9\pi_g = 9$, and $(1,2)\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = (1,1)$ so $7\pi_g = 5$. In fact, $\pi_g = (3\,7\,5)(4\,8\,6)(1)(2)(9)$.

Note that $(0,0)g = (0,0)$ for all g in G, so $\{9\}$ is a whole orbit.

Definition Given an action π of a group G on Ω, and an element α of Ω, the *stabilizer* of α is $\left\{g \in G : \alpha\pi_g = \alpha\right\}$, written G_α.

Orbit-Stabilizer Theorem (a) G_α is a subgroup of G.

(b) There is a bijection between the orbit α^G containing α and the set of right cosets of G_α in G.

Proof (a) (i) π_{1_G} is the identity permutation of Ω so $\alpha\pi_{1_G} = \alpha$, so $1_G \in G_\alpha$, so G_α is not empty.

(ii) Suppose that g, h are in G_α. Then $\alpha\pi_g = \alpha$, so $\alpha = \alpha(\pi_g)^{-1} = \alpha\pi_{g^{-1}}$, because π is a homomorphism, so

$$\begin{aligned} \alpha\pi_{g^{-1}h} &= \alpha\pi_{g^{-1}}\pi_h, \qquad \text{because } \pi \text{ is a homomorphism,} \\ &= \alpha\pi_h = \alpha. \end{aligned}$$

Therefore $g^{-1}h \in G_\alpha$.

Hence $G_\alpha \leqslant G$.

(b) Suppose that $\beta \in \alpha^G$, so that there is some g in G with $\alpha\pi_g = \beta$. If $h \in G_\alpha$ then $\alpha\pi_{hg} = \alpha\pi_h\pi_g = \alpha\pi_g = \beta$, so everything in the right coset $G_\alpha g$ maps α to β. Put $C(\beta) = \{x \in G : \alpha\pi_x = \beta\}$. We have just shown that $G_\alpha g \subseteq C(\beta)$. Conversely, if $\alpha\pi_x = \beta$ for some x in G then $\alpha\pi_{xg^{-1}} = \alpha\pi_x\pi_{g^{-1}} = \alpha\pi_x\pi_g^{-1} = \beta\pi_g^{-1} = \alpha$ so $xg^{-1} \in G_\alpha$ so $x \in G_\alpha g$. This shows that $C(\beta) \subseteq G_\alpha g$. Hence $C(\beta) = G_\alpha g$. There is a bijection between the points β in the orbit α^G and the sets $C(\beta)$, because β defines $C(\beta)$ while any x in $C(\beta)$ defines β as $\alpha\pi_x$. $\square$

Corollary The size of the orbit α^G is equal to the index of G_α in G; in particular, if G is finite then $\left|\alpha^G\right| = |G| / |G_\alpha|$.

Example In $\mathrm{GL}(2,3)$, put $\alpha = (1,0)$ and $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then

$$\alpha\pi_g = (1,0)\begin{bmatrix} a & b \\ c & d \end{bmatrix} = (a,b),$$

so the orbit of α contains all the non-zero vectors, so $\left|\alpha^G\right| = 8$. Also

$$g \in G_\alpha \iff \alpha\pi_g = \alpha \iff (a,b) = (1,0)$$

and there are six matrices in $\mathrm{GL}(2,3)$ with first row $(1,0)$, so $|G_\alpha| = 6$. Then we have $\left|\alpha^G\right| \times |G_\alpha| = 8 \times 6 = 48 = |G|$, in accordance with the theorem.

Similarly, if $\beta = (0,1)$ then $\beta\pi_g = (c,d)$ so $g \in G_\beta \iff (c,d) = (0,1)$. If π_g is the identity then $\pi_g \in G_\alpha \cap G_\beta$: therefore $(a,b) = (1,0)$ and $(c,d) = (0,1)$ so $g = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_G$. This shows that $\ker(\pi) = \{1_G\}$, so this action π is faithful, so $\mathrm{GL}(2,3)$ is isomorphic to a subgroup of S_9.

Example Let G be the group of all 3-dimensional rotational symmetries of a cube. Consider elements of G as permutations of the 6 faces of the cube. Let α be one face. Then G_α consists of rotations about the axis perpendicular to the centre of α, through multiples of $2\pi/4$, so $|G_\alpha| = 4$. Also, G is transitive on the faces, so $\left|\alpha^G\right| = 6$. Hence $|G| = 6 \times 4 = 24$.

Cauchy's Theorem If H is a finite group and $|H|$ is divisible by a prime p, then H contains an element of order p.

Proof Let Ω be the set of p-tuples

$$\left\{(h_1, h_2, \ldots, h_p) : h_i \in H \text{ for } i = 1, \ldots, p \text{ and } h_1 h_2 \ldots h_p = 1_H\right\}.$$

In such a p-tuple, $h_p = (h_1 h_2 \ldots h_{p-1})^{-1}$, so $|\Omega| = |H|^{p-1}$.

Let g be the following permutation of Ω:

$$(h_1, h_2, \ldots, h_p)g = (h_2, h_3, \ldots, h_p, h_1).$$

Note that if $h_1 h_2 \ldots h_p = 1_H$ then $h_1^{-1} h_1 h_2 \ldots h_p h_1 = h_1^{-1} 1_H h_1 = 1_H$ so $h_2 h_3 \ldots h_p h_1 = 1_H$ and so g really is a permutation of Ω. Then g^p is the identity permutation but g is not the identity. Hence the order of g is not 1, and it divides p, which is prime, so the order of g is p.

Let $G = \langle g \rangle$, which has order p. By the Orbit-Stabilizer Theorem, every orbit of G on Ω has size dividing p, so size either 1 or p. Suppose that there are m_1 orbits of size 1 and m_2 orbits of size p. Then

$$m_1 + m_2 p = |\Omega| = |H|^{p-1},$$

which is divisible by p, because p divides $|H|$. Hence p divides m_1.

Any orbit of size 1 contains a single p-tuple of the form $(h, h, \ldots, h)$ with $h^p = 1_H$. There is at least one such orbit: $\{(1_H, 1_H, \ldots, 1_H)\}$. Therefore $m_1 \neq 0$. Hence $m_1 \geqslant p$. So there must be at least $p-1$ other orbits of size 1. If $\{(h, h, \ldots, h)\}$ is any one of these other orbits then h is an element of order p. □

Given an action π of a group G on a set Ω, an equivalence relation $\sim$ on Ω is called a *G-equivalence* if $\alpha \sim \beta \iff \alpha\pi_g \sim \beta\pi_g$ for all α, β in Ω and all g in G. Given such a G-equivalence, let Ω' be the set of equivalence classes of $\sim$, and define an action ρ of G on Ω' by $[\alpha]\rho_g = [\alpha\pi_g]$. We need to show that ρ really is an action. Now, $[\alpha] = [\beta] \Longrightarrow \alpha \sim \beta \Longrightarrow \alpha\pi_g = \beta\pi_g \Longrightarrow [\alpha\pi_g] = [\beta\pi_g] \Longrightarrow [\alpha]\rho_g = [\beta]\rho_g$, so ρ_g is well defined. Also $[\alpha]\rho_{1_G} = [\alpha\pi_{1_G}] = [\alpha]$ for all α in Ω, so ρ_{1_G} is the identity permutation of Ω'. Finally, for g, h in G:

$$\begin{aligned}
[\alpha]\rho_g\rho_h = [\alpha\pi_g]\rho_h &= [\alpha\pi_g\pi_h] \\
&= [\alpha\pi_{gh}], \qquad \text{because } \pi \text{ is an action,} \\
&= [\alpha]\rho_{gh},
\end{aligned}$$

so ρ is an action.

Example Let π be the right regular action of G on itself, and let $H \leqslant G$. For x, y in G, $x \sim_R y \iff yx^{-1} \in H$. Given g in G,

$$\begin{aligned}
x\pi_g \sim_R y\pi_g &\iff xg \sim_R yg \\
&\iff (yg)(xg)^{-1} \in H \\
&\iff ygg^{-1}x^{-1} \in H \\
&\iff yx^{-1} \in H \\
&\iff x \sim_R y,
\end{aligned}$$

so $\sim_R$ is a G-equivalence. The equivalence classes of $\sim_R$ are the right cosets of H in G, so there is an action ρ of G on these right cosets defined by

$$(Hx)\rho_g = [x]\rho_g = [x\pi_g] = [xg] = Hxg.$$

This action is transitive, because, given any two right cosets Hx and Hy, we have $Hy = (Hx)\rho_g$ with $g = x^{-1}y$.

Theorem If a group G has a subgroup H of index n then there is a normal subgroup K of G such that $K \leqslant H$ and G/K is isomorphic to a transitive subgroup of S_n.

Proof Let ρ be the above action of G on the right cosets of H in G. Then $\mathrm{Im}(\rho)$ is a transitive subgroup of S_n.

Let $K = \ker(\rho)$. By the First Isomorphism Theorem, $G/K \cong \mathrm{Im}(\rho)$.

If $k \in K$ then $Hx\rho_k = Hx$ for all x. In particular, $H\rho_k = H$, so $Hk = H$ so $k \in H$. Therefore $K \leqslant H$. $\square$

This prompts a remark about subsets of a subgroup. Suppose that H is a subgroup of a group G and $K \subseteq H$. If K is a subgroup of G then it is a subgroup of H. If K is a subgroup of H then it is a subgroup of G. If K is a normal subgroup of G then it is a normal subgroup of H. However, if K is a normal subgroup of H then it may not be a normal subgroup of G.

Example Let $G = \mathrm{GL}(2,3)$ and Ω consist of the eight non-zero vectors in $\mathbb{F}_3^2$. Let π be the action defined by $\alpha\pi_g = \alpha g$ for α in Ω and g in G.

Define $\alpha \sim \beta$ if there is a non-zero scalar λ in $\mathbb{F}_3$ (so $\lambda = 1$ or $\lambda = 2$) such that $\alpha = \lambda\beta$. This is a G-equivalence because

$$(\lambda\beta)\pi_g = (\lambda\beta)g = \lambda(\beta g) = \lambda(\beta\pi_g)$$

since λ is a scalar. There are four equivalence classes:

$$\begin{aligned} \{(1,0),\ (2,0)\} &= A \\ \{(0,1),\ (0,2)\} &= B \\ \{(1,1),\ (2,2)\} &= C \\ \{(1,2),\ (2,1)\} &= D. \end{aligned}$$

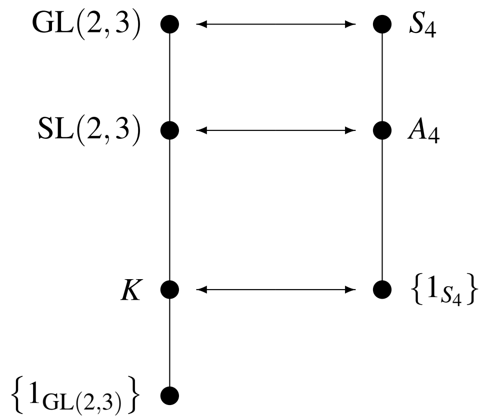
Let $K = \ker(\rho)$. If $\lambda = 1$ or $\lambda = 2$ then $\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \in K$. Conversely, suppose that $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in K$. Then $A\rho_g = A$ so $(a,b) = (1,0)$ or $(2,0)$ so $b = 0$. Similarly,

$B\rho_g = B$ so $(c,d) = (0,1)$ or $(0,2)$ so $c = 0$. Then $C\rho_g = [(a,d)] = C$ so $a = d$. Therefore

$$K = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \right\}$$

and $|K| = 2$. Then $|G/K| = |G|\,/\,|K| = 48/2 = 24 = |S_4|$, so $G/K \cong S_4$. In other words, we get all permutations of $\{A,B,C,D\}$.

We know that S_4 has a unique subgroup of index 2: it is A_4. By the Correspondence Theorem, $\mathrm{GL}(2,3)$ has a unique subgroup of index 2 which contains K. We also know that $\mathrm{GL}(2,3)$ has a subgroup $\mathrm{SL}(2,3)$, which is the kernel of the determinant homomorphism. The determinant of an element of $\mathrm{GL}(2,3)$ can be either of the two non-zero scalars in $\mathbb{F}_3$, so $\mathrm{SL}(2,3)$ has index 2 in $\mathrm{GL}(2,3)$, by the First Isomorphism Theorem. Inspection shows that both elements of K have determinant 1, so $K \leqslant \mathrm{SL}(2,3)$. Therefore $\mathrm{SL}(2,3)$ is this unique subgroup of $\mathrm{GL}(2,3)$ which contains K and has order 24.



Theorem (wrongly attributed to Burnside) Let π be an action of a finite group G on a set Ω. For g in G, put $f(g) = \left|\left\{\alpha \in \Omega : \alpha\pi_g = \alpha\right\}\right|$. Then the number of orbits of G on Ω is equal to

$$\frac{1}{|G|}\sum_{g\in G} f(g).$$

Proof Let $m = \left|\left\{(\alpha,g) : \alpha \in \Omega,\ g \in G,\ \alpha\pi_g = \alpha\right\}\right|$. Count m in two ways:

$$m = \sum_{g\in G} f(g) = \sum_{\alpha\in\Omega} |G_\alpha|\,.$$

Let $\Gamma \subseteq \Omega$ be any orbit. By the Orbit-Stabilizer Theorem, $|G_\alpha| = |G|\,/\,|\Gamma|$ for each α in Γ, and so

$$\sum_{\alpha\in\Gamma} |G_\alpha| = \sum_{\alpha\in\Gamma} \frac{|G|}{|\Gamma|} = |\Gamma| \times \frac{|G|}{|\Gamma|} = |G|\,.$$

Therefore

$$\sum_{\alpha\in\Omega} |G_\alpha| = |G| \times \text{number of orbits}$$

and so

$$\frac{1}{|G|}\sum_{g\in G} f(g) = \frac{1}{|G|}\sum_{\alpha\in\Omega} |G_\alpha| = \text{number of orbits.} \quad \square$$

Example Take $\Omega = \{1,2,3,4,5,6\}$ and let $G = \{1,a,b,c\}$ where $a = (1\,2)(3\,4)$, $b = (3\,4)(5\,6)$ and $c = (1\,2)(5\,6)$. Then $f(1) = 6$ and $f(a) = f(b) = f(c) = 2$, so

$$\text{the number of orbits} = \frac{1}{4}(6+2+2+2) = 3,$$

which is correct, because the orbits are $\{1,2\}$, $\{3,4\}$ and $\{5,6\}$.

Note: any group $\{1,a,b,c\}$ in which $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$ and $bc = cb = a$ is called a *Klein* group. Any two such groups are isomorphic to each other.