Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Notes 4 **Autumn 2011**

---

4 More on group actions

We saw when we considered group actions before that any action of a group can be "decomposed" into orbits, so that the group has a transitive action on each orbit. In this section we look further at transitive actions, and show that all the different transitive actions of a group can be recognised in terms of the subgroup structure of the group. We define primitivity of an action, and examine how to recognise this in group-theoretic terms and its consequences for normal subgroups. We also look at the stronger notion of double transitivity. After some examples, we turn to *Iwasawa's Lemma*, which will enable us to show that certain groups are simple.

4.1 Coset actions

Let H be a subgroup of the group G. We will consider the set of right cosets of H in G:

$$\cos(H,G) = \{Hg : g \in G\}.$$

Sometimes this is written as $H\backslash G$, but this is too close to the notation $H \setminus G$ for set difference so I will avoid it. Sometimes it is written $[G{:}H]$.

Now G acts on $\cos(H,G)$ by right multiplication. Formally, using $\mu(x,g)$ for the action of the permutation corresponding to g on the element x, the action is given by

$$\mu(Hx,g) = H(xg).$$

Fortunately, we can write this in the briefer form $(Hx)g = H(xg)$ without risk of too much confusion.

Note that the action of G on $\cos(H,G)$ is transitive; for given any two cosets Hx and Hy, we have $(Hx)(x^{-1}y) = Hy$. The important thing is that every transitive action can be realised in this way, in a sense which we now explore.

Let G have actions on two sets Ω_1 and Ω_2. An *isomorphism* between these actions is a bijection $f : \Omega_1 \to \Omega_2$ such that $(\alpha g)f = (\alpha f)g$ for all $g \in G$. Here the left-hand side means "apply the group element g to α, in the given action on Ω_1, and then map across to Ω_2 using f", while the right-hand side means "map to Ω_2 using f, and then apply g using the action on Ω_2". Another way that this is commonly expressed is that the following diagram *commutes*, in the sense that all routes through the diagram following the arrows give the same result:

$$\begin{array}{ccc} \Omega_1 & \stackrel{f}{\to} & \Omega_2 \\ g\downarrow & & \downarrow g \\ \Omega_1 & \stackrel{f}{\to} & \Omega_2 \end{array}$$

The gs on left and right refer to the two actions.

Recall that, if G acts on Ω, then the *stabiliser* $\mathrm{Stab}(\alpha)$ of a point α is

$$\mathrm{Stab}(\alpha) = \{g \in G : \alpha g = \alpha\}.$$

Theorem 4.1 *(a) Any transitive action of a group G on a set Ω is isomorphic to the action of G on the coset space $\mathrm{cos}(H,G)$, where $H = \mathrm{Stab}(\alpha)$ for some $\alpha \in \Omega$.*

(b) The actions of G on the coset spaces $\mathrm{cos}(H,G)$ and $\mathrm{cos}(K,G)$ are isomorphic if and only if the subgroups H and K are conjugate (that is, $K = g^{-1}Hg$ for some $g \in G$).

Proof I will prove the first part; the second is a (non-trivial) exercise. The proof is just an adaptation of the proof of the Orbit-Stabiliser Theorem. If G acts transitively on Ω, we saw that there is a bijection between Ω and the set of subsets $X(\alpha,\beta)$ of G for fixed α (as β ranges over Ω), where

$$X(\alpha,\beta) = \{g \in G : \alpha g = \beta\}.$$

We saw, furthermore, that $X(\alpha,\beta)$ is a right coset of $\mathrm{Stab}(\alpha)$, and that every right coset arises in this way. Now it is a fairly routine exercise to check that the bijection from Ω to $\mathrm{cos}(\mathrm{Stab}(\alpha),G)$ taking β to $X(\alpha,\beta)$ is an isomorphism.

Example Let G be the dihedral group D_6 of symmetries of an equilateral triangle. Let Ω_1 be the set of three vertices of the triangle, and Ω_2 the set of three edges. Show that G acts transitively on both these sets, and that the map f which takes each vertex to the opposite edge is an isomorphism of actions.

4.2 Primitivity

Let G act transitively on a set Ω, with $|\Omega| > 1$. A *congruence*, or *G-congruence*, on Ω is an equivalence relation on Ω which is preserved by G (that is, if $\alpha \equiv \beta$, then $(\alpha g) \equiv (\beta g)$ for all $g \in G$). An equivalence class of a congruence is called a *block*. Note that, if B is a block, then so is Bg for any $g \in G$.

There are always two trivial congruences:

equality: $\alpha \equiv \beta$ if and only if $\alpha = \beta$;

the *universal* relation: $\alpha \equiv \beta$ for all $\alpha, \beta \in \Omega$.

The action is called *imprimitive* if there is a non-trivial congruence, and *primitive* if not.

Example Let G be the symmetry group of a square (the dihedral group of order 8), acting on Ω, the set of four vertices of the square. The relation $\equiv$ defined by $\alpha \equiv \beta$ if α and β are equal or opposite is a congruence, with two blocks of size 2.

Proposition 4.2 *Let G act transitively on Ω. A non-empty subset B of Ω is a block if and only if, for all $g \in G$, either $Bg = B$ or $B \cap Bg = \emptyset$.*

Proof If B is a block, then so is Bg; and equivalence classes are equal or disjoint.

Conversely, suppose that B is a non-empty set such that $B = Bg$ or $B \cap Bg = \emptyset$ for all g. Then for any $h, k \in G$, we have $Bh = Bk$ or $Bh \cap Bk = \emptyset$. (For $Bh \cap Bk = (B \cap Bkh^{-1})h$.) So the images of B are pairwise disjoint. By transitivity, every point of Ω is covered by these images. So they form a partition, which is the set of equivalence classes of a congruence.

We saw that every transitive action is isomorphic to a coset space: how do we recognise primitive actions? A subgroup H of G is *maximal* if $H < G$ but there is no subgroup K satisfying $H < K < G$.

Proposition 4.3 *Let H be a proper subgroup of G. Then the action of G on $\mathrm{cos}(H, G)$ is primitive if and only if H is a maximal subgroup of G.*

Proof Suppose that $H < K < G$, and let B be the set of cosets of H which are contained in K. Then B satisfies the conditions of the previous proposition. For take a coset Hk with $k \in K$. For any $g \in G$,

- if $g \in K$, then $Hkg \in B$, so $Bg = B$;
- if $g \notin K$, then $Hkg \notin B$, so $B \cap Bg = \emptyset$.

Conversely, suppose that G acts imprimitively on $\cos(H,G)$; let B be a block containing the coset H, and $K = \{g \in G : Bg = B\}$. Then K is a subgroup of G, and $H < K < G$.

One of the important properties of primitive actions is the following strong restriction on normal subgroups:

Proposition 4.4 *Let G act primitively on Ω, and let N be a normal subgroup of G. Then either N acts trivially on Ω (that is, N lies in the kernel of the action), or N acts transitively on Ω.*

Proof We show that, for any transitive action of G, the orbit relation of the normal subgroup N is a congruence. It follows that, if the action is primitive, then either all orbits have size 1, or there is a single orbit.

So let $\alpha \equiv \beta$ if $\alpha h = \beta$ for some $h \in N$. Then for any $g \in G$, $(\alpha g)(g^{-1}hg) = \beta g$, and $g^{-1}hg \in N$ by normality; so $\alpha g \equiv \beta g$. Thus $\equiv$ is indeed a congruence.

Example If G is the group of symmetries of a square, then the subgroup of order 2 generated by the 180° rotation is normal; its orbit relation is the congruence we found earlier.

Remark Let G act transitively on an n-element set. If $\equiv$ is a congruence with l classes, then each class has the same size k, and $kl = n$. If n is prime, then necessarily $k = 1$ or $k = n$. So:

A transitive action on a prime number of points is primitive.

Exercise Consider the regular action of G on itself by right multiplication. Show that there is a congruence $\equiv_H$ for each subgroup H of G, whose classes are the right cosets of H, and that these are all the congruences.

4.3 Digression: Minimal normal subgroups

A *minimal normal subgroup* of a group G is a normal subgroup $N \trianglelefteq G$ with $N \neq \{1\}$ such that, if $M \trianglelefteq G$ with $M \leq N$, then either $M = N$ or $M = \{1\}$.

There is an important result which says:

Theorem 4.5 *A minimal normal subgroup of a finite group is isomorphic to the direct product of a number of copies of a simple group.*

Since I haven't given in detail the result for recognising the direct product of more than two factors, I won't prove this theorem in general; but I will prove a special case as an illustration.

Let p be a prime number. An *elementary abelian p-group* is an abelian group in which every element different from the identity has order p. By the Fundamental Theorem of Abelian Groups, such a group is a direct product of cyclic groups of order p.

Proposition 4.6 *An abelian minimal normal subgroup of a finite group is elementary abelian.*

Proof Let N be such a subgroup, and let p be a prime dividing $|N|$. There is an element of order p in N. Let M be the set of elements of N with order dividing p. Then $M \neq \{1\}$, and M is a normal subgroup of G (since conjugation preserves both order and membership in N). So $M = N$.

Any minimal normal subgroup of a soluble group is abelian. For let G be soluble, and N a minimal normal subgroup. Then N is soluble, so its derived group N' satisfies $N' \neq N$; and $N' \trianglelefteq G$, since conjugation preserves both commutators and members of N. So $N' = \{1\}$, that is, N is abelian.

Here is a slightly unexpected corollary.

Proposition 4.7 *Let G be a finite soluble group. Then any maximal subgroup of G has prime power index.*

Proof Let H be a maximal subgroup, and consider the (primitive) action of G on $\mathrm{cos}(H,G)$. The image of this action is a quotient of G, hence is soluble. So we may assume that the action is faithful.

Let N be a minimal normal subgroup of G. Then N is abelian, and hence an elementary abelian p-group for some prime p; and N is transitive, since G is primitive and $N \neq \{1\}$. So by the Orbit-Stabiliser Theorem, $|\mathrm{cos}(H,G)|$ (the index of H in G) is a power of p.

4.4 Regular actions

In this section we consider only faithful actions.

An action of G on Ω is *regular* if it is transitive and the point stabiliser is trivial.

If H is the trivial subgroup, then each coset of H consists of a single element; so the set $\mathrm{cos}(H,G)$ is "essentially" just G. Thus, a regular action of G is isomorphic to the action on itself by right multiplication.

(If we did not require the action to be faithful, then we could say that an action is regular if it is transitive and the point stabiliser H is a normal subgroup of G; such an action is isomorphic to the action of G/H on itself by right multiplication. In particular, since every subgroup of an abelian group is normal, we see that every transitive action of an abelian group is regular.)

We need to look at a fairly technical situation. Let G be a group with a faithful action on Ω, and N a normal subgroup of G whose action on Ω is regular. Then we can "identify" Ω with N so that N acts by right multiplication. More precisely, we choose a fixed reference point $\alpha \in \Omega$; then there is a bijection between N and Ω, under which $h \in N$ corresponds to $\alpha h \in \Omega$; this is an isomorphism between the action of N on itself by right multiplication and the given action.

Can we describe the entire action of G on N? It turns out that there is a nice description of the subgroup $\mathrm{Stab}(\alpha)$ of G:

> Under the above bijection, the action of $\mathrm{Stab}(\alpha)$ on N by conjugation corresponds to the given action on Ω.

To show this, take $g \in \mathrm{Stab}(\alpha)$ and suppose that g maps β to γ. Let h and k be the elements of N corresponding to β and γ under the bijection: that is, $\alpha h = \beta$ and $\alpha k = \gamma$. Now

$$\alpha(g^{-1}hg) = \alpha hg = \beta g = \gamma,$$

since g^{-1} fixes α. Since there is a unique element of N mapping α to γ, namely k, we have $g^{-1}hg = k$, as required.

We will use this analysis when we come to showing the simplicity of the alternating group.

4.5 Double transitivity

Let G act on Ω, with $|\Omega| > 1$. We say that the action is *doubly transitive* if, given any two ordered pairs (α_1, α_2) and (β_1, β_2) of *distinct* elements of Ω, there is an element $g \in G$ satisfying $\alpha_1 g = \beta_1$ and $\alpha_2 g = \beta_2$.

Here "distinct" means that $\alpha_1 \neq \alpha_2$ and $\beta_1 \neq \beta_2$, but we don't say anything about the relation between α_1 and β_1, for example. (A permutation cannot map distinct points to equal points or *vice versa*.)

Examples 1. The symmetric group S_n acts doubly transitively on the set $\{1, 2, \ldots, n\}$ for $n \geq 2$.

2. The automorphism group of the Fano plane, the group of order 168 on Problem Sheet 1, acts doubly transitively on the seven points of the plane.

Proposition 4.8 *A doubly transitive action is primitive.*

Proof Let $\equiv$ be a congruence. By the reflexive property, $\alpha \equiv \alpha$ for all α. If $\alpha_1 \equiv \alpha_2$ for any single pair (α_1, α_2) of distinct elements, then $\beta_1 \equiv \beta_2$ for all distinct pairs, and $\equiv$ is the universal congruence; otherwise, it is the relation of equality.

Remark In a similar way, we can define t-transitivity of an action, for any $t \geq 1$.

4.6 Iwasawa's Lemma

Iwasawa's Lemma is a technique for proving the simplicity of a group. It looks rather technical, but we will use it to show that the group $\mathrm{PSL}(d,F)$ is simple in most cases. Though it is technical, fortunately the proof is quite straightforward.

Recall that the *derived group*, or *commutator subgroup*, of G is the subgroup G' generated by all *commutators* $[g,h] = g^{-1}h^{-1}gh$ for $g,h \in G$. It has the following properties:

- G' is a normal subgroup of G;
- G/G' is abelian;
- if N is a normal subgroup of G such that G/N is abelian, then $G' \leq N$.

Theorem 4.9 *Let G be a group with a faithful primitive action on Ω. Suppose that there is an abelian normal subgroup A of $\mathrm{Stab}(\alpha)$ with the property that the conjugates of A generate G. Then any non-trivial normal subgroup of G contains G'. In particular, if $G = G'$, then G is simple.*

Proof Suppose that N is a non-trivial normal subgroup of G. Then N is transitive, so $N \not\leq \mathrm{Stab}(\alpha)$. Since $\mathrm{Stab}(\alpha)$ is a maximal subgroup of G, we have $N\,\mathrm{Stab}(\alpha) = G$.

Let g be any element of G. Write $g = nh$, where $n \in N$ and $h \in \mathrm{Stab}(\alpha)$. Then

$$gAg^{-1} = nhAh^{-1}n^{-1} = nAn^{-1},$$

since A is normal in $\mathrm{Stab}(\alpha)$. Since N is normal in G we have $gAg^{-1} \leq NA$. Since the conjugates of A generate G we see that $G = NA$.

Hence

$$G/N = NA/N \cong A/(A \cap N)$$

is abelian, whence $N \geq G'$, and we are done.

4.7 Exercises

1. Let G be the symmetry group of the cube. Show that the action of G on the set of vertices of the cube is transitive but imprimitive, and describe all the congruences. Repeat for the action of G on the set of faces, and on the set of edges.

2. An *automorphism* of a group G is an isomorphism from G to itself. An *inner automorphism* of G is a conjugation map, one of the form $c_g : x \mapsto g^{-1}xg$.

(a) Show that the set of automorphisms, with the operation of conjugation, is a group $\mathrm{Aut}(G)$.

(b) Show that the set of inner automorphisms is a subgroup $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$.

(c) Show that $\mathrm{Inn}(G) \cong G/Z(G)$, where $Z(G)$ is the centre of G.

(d) Show that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. (The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is defined to be the *outer automorphism group* $\mathrm{Out}(G)$ of G.)

3. Let G be a group. Then there is in a natural way an action of the automorphism group $\mathrm{Aut}(G)$ of G on the set G. The identity is fixed by all automorphisms, so $\{1\}$ is an orbit of size 1 for this action.

(a) Suppose that $G \setminus \{1\}$ is an orbit for $\mathrm{Aut}(G)$. Show that all non-identity elements of G have the same order, and deduce that the order of G is a power of a prime p, and hence that G is an elementary abelian p-group.

(b) Suppose that $\mathrm{Aut}(G)$ acts doubly transitively on $G \setminus \{1\}$. Show that either $|G| = 2^d$ for some d, or $|G| = 3$.

(c) Suppose that $\mathrm{Aut}(G)$ acts triply transitively on $G \setminus \{1\}$. Show that $|G| = 4$.