Queen Mary University of London

MAS 305 Algebraic Structures II

Notes 5 **Autumn 2006**

Conjugacy

For x, g in a group G, put
$$x^g = g^{-1}xg,$$
which is called the *conjugate* of x by g.

Temporarily, write $x^g = x\pi_g$. Then $x\pi_{1_G} = 1_G x 1_G = x$ for all x in G, so π_{1_G} is the identity permutation of G. Also

$$x\pi_g\pi_h = (g^{-1}xg)\pi_h = h^{-1}g^{-1}xgh = (gh)^{-1}xgh = x\pi_{gh},$$

so conjugation is an action.

The orbit containing x is
$$x^G = \{x^g : g \in G\},$$
which is called the *conjugacy class* of x; so conjugacy is an equivalence relation.

The stabilizer of x is

$$G_x = \left\{g \in G : g^{-1}xg = x\right\} = \{g \in G : xg = gx\},$$

which is called the *centralizer* of x in G, written $C(x)$. So $C(x)$ is a subgroup of G and $\left|x^G\right| = |G : C(x)|$, by the Orbit-Stabilizer Theorem. In particular, if G is finite then $\left|x^G\right| \times |C(x)| = |G|$. Note that $\langle x \rangle \leqslant C(x)$ for all x.

The kernel of the action is

$$\{g \in G : x^g = x \text{ for all } x \text{ in } G\} = \{g \in G : xg = gx \text{ for all } x \text{ in } G\} = \bigcap_{x \in G} C(x).$$

This is called the *centre* of G, and written $Z(G)$. So $Z(G)$ is a normal subgroup of G.

Lemma Let H be a subgroup of a group G. Then H is a normal subgroup of G if and only if H consists of whole conjugacy classes.

Lemma In S_n, g is conjugate to h if and only if g and h have the same cycle structure.

Proof We have already seen that h and $x^{-1}hx$ have the same cycle structure. Conversely, if g and h have the same cycle structure then they can be matched up as

$$\begin{array}{rcl} h & = & (a_1 \;\; a_2 \;\; \dots \;\; a_m) \;\; (c_1 \;\; c_2 \;\; \dots \;\; c_r) \;\; \dots \\ g & = & (b_1 \;\; b_2 \;\; \dots \;\; b_m) \;\; (d_1 \;\; d_2 \;\; \dots \;\; d_r) \;\; \dots \end{array}$$

Put $a_i x = b_i$, $c_i x = d_i$ and so on: then $x^{-1}hx = g$. $\square$

Note that the order of any permutation is the least common multiple of the lengths of its cycles. For example, if $x = (1\ 2)(3\ 4\ 5)$ then $x^n = (3\ 4\ 5)^n$ if n is even and $x^n = (1\ 2)^n$ if n is divisible by 3:

$$\begin{array}{ll} x & = (1\,2)(3\,4\,5) \\ x^2 = & \qquad\;\, (3\,5\,4) \\ x^3 = & (1\,2) \\ x^4 = & \qquad\;\, (3\,4\,5) \\ x^5 = & (1\,2)(3\,5\,4) \\ x^6 = & (1). \end{array}$$

Example We calculate the conjugacy classes in S_5. For one permutation x in each conjugacy class, we calculate the order of its centralizer as $|C(x)| = 120/\left|x^{S_5}\right|$.

(a) The identity 1_{S_5} is conjugate only to itself, so $\{1_{S_5}\}$ is a whole conjugacy class. Evidently, $C(1_{S_5})$ is the whole of S_5, which has order $120 = 120/1$.

(b) Let $x = (1\,2)$. Then x^{S_5} consists of all the transpositions. The number of transpositions is ${}^5\mathrm{C}_2$, so $\left|x^{S_5}\right| = 10$ and $|C(x)| = 120/10 = 12$.

(c) Let $x = (1\,2\,3)$. Then x^{S_5} consists of all 3-cycles. There are $5 \times 4 \times 3$ ways of choosing the elements of the 3-cycle in order, but we can start the cycle at any point in it, so the number of 3-cycles is $(5 \times 4 \times 3)/3$. Hence $\left|x^{S_5}\right| = 20$ and $|C(x)| = 120/20 = 6$.

(d) Similarly, if $x = (1\,2\,3\,4)$ then $\left|x^{S_5}\right| = (5 \times 4 \times 3 \times 2)/4 = 30$ and $|C(x)| = 120/30 = 4$.

(e) Similarly, if $x = (1\,2\,3\,4\,5)$ then $\left|x^{S_5}\right| = (5 \times 4 \times 3 \times 2 \times 1)/5 = 24$ and $|C(x)| = 120/24 = 5$.

(f) Each 3-cycle is disjoint from exactly one transposition, so there are 20 permutations conjugate to $(1\,2\,3)(4\,5)$. The order of the centralizer of this permutation is $120/20 = 6$.

(g) Each transposition is disjoint from three other transpositions, so the number of conjugates of $(1\,2)(3\,4)$ is $(10\times 3)/2$ (why do we have to divide by 2?). The order of the centralizer of this permutation is $120/15 = 8$.

Check: $1+10+20+30+24+20+15 = 120$, so we have accounted for all the elements of S_5.

Before identifying the centralizers of elements of S_5, we introduce a useful construction. Suppose that a group G has subgroups H and K such that $hk = kh$ for all h in H and all k in K. Put

$$HK = \{hk : h \in H,\ k \in K\}.$$

Then $H \subseteq HK$ and $K \subseteq HK$, so HK is not empty. If $h_1, h_2 \in H$ and $k_1, k_2 \in K$ then

$$(h_1k_1)^{-1}(h_2k_2) = k_1^{-1}h_1^{-1}h_2k_2 = h_1^{-1}h_2k_1^{-1}k_2 \in HK$$

because $h_1^{-1}h_2 \in H$ and $k_1^{-1}k_2 \in K$. Therefore HK is a subgroup of G. Also

$$(h_1k_1)^{-1}h_2(h_1k_1) = k_1^{-1}h_1^{-1}h_2h_1k_1 = h_1^{-1}h_2h_1 \in H$$

and

$$(h_1k_1)^{-1}k_2(h_1k_1) = k_1^{-1}h_1^{-1}k_2h_1k_1 = k_1^{-1}k_2k_1 \in K,$$

so $H \trianglelefteq HK$ and $K \trianglelefteq HK$.

If $h_1k_1 = h_2k_2$ then $h_2^{-1}h_1 = k_2k_1^{-1}$, which is in $H \cap K$, so if $H \cap K = \{1_G\}$ then each element of HK has a *unique* expression as hk for some h in H and k in K.

Definition Let H and K be subgroups of a group G. If $hk = kh$ for all h in H and all k in K, and if $H \cap K = \{1_G\}$, then the subgroup HK is called the *internal direct product* of H and K, and may be written $H \times K$.

Example Now we shall find the centralizers of elements in S_5, finding $C(x)$ for one element x in each conjugacy class. We already know $|C(x)|$, so as soon as we find a subgroup H of $C(x)$ with $|H| = |C(x)|$ then we know that $H = C(x)$.

(a) If $x = 1_{S_5}$ then $C(x) = S_5$.

(b) If $x = (1\,2)$ then $|C(x)| = 12$. Of course, $C(x)$ contains $\langle x\rangle$, which has order 2. It also contains the subgroup H of all permutations of $\{3,4,5\}$, which is isomorphic to S_3. Now, $\langle x\rangle \cap H = \{1_{S_5}\}$, so $C(x)$ contains $\langle x\rangle \times H$, whose order is $2\times|S_3| = 12$. Therefore $C((1\,2))$ is precisely $\langle (1\,2)\rangle \times (S_3 \text{ on } \{3,4,5\})$.

(c) Similarly, if $x = (1\,2\,3)$ then $C(x)$ contains $\langle x\rangle$ and $\langle (4\,5)\rangle$ and these two subgroups have trivial intersection. Therefore $\langle x\rangle \times \langle (4\,5)\rangle$ has order 6 and so is the whole of $C(x)$. Alternatively, put $y = (1\ 2\ 3)(4\ 5)$ and note that $x \in \langle y\rangle$ so $\langle y\rangle \leqslant C(x)$. Again, $\langle y\rangle$ and $C(x)$ have the same order, so $C(x) = \langle y\rangle$.

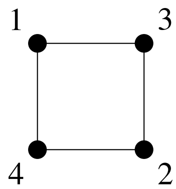
(d) When $x = (1\,2\,3\,4)$ then $|C(x)| = 4 = |\langle x\rangle|$, so $C(x) = \langle x\rangle$.

(e) Similarly, when $x = (1\,2\,3\,4\,5)$ then $|C(x)| = 5 = |\langle x\rangle|$, so $C(x) = \langle x\rangle$.

(f) If $x = (1\,2\,3)(4\,5)$ then the order of x is the lcm of the orders of $(1\,2\,3)$ and $(4\,5)$, which is 6. Since $|C(x)| = 6$, we again have $C(x) = \langle x\rangle$.

(g) Let $x = (1\,2)(3\,4)$. We know that $|C(x)| = 8$, and shall demonstrate a subgroup of S_5 which has order 8 and centralizes x.

We know that the group of symmetries of a square is the dihedral group D_8 of order 8. Label the square as in the following picture, so that one of the symmetries is $(1\,2)(3\,4)$.



$$D_8 = \{1,\ (1\,3\,2\,4),\ (1\,2)(3\,4),\ (1\,4\,2\,3),\ (1\,3)(2\,4),\ (1\,4)(2\,3),\ (1\,2),\ (3\,4)\}$$

Now, x is in the cyclic group of order 4 generated by $(1\,3\,2\,4)$, so its centralizer in D_8 contains $\langle x\rangle$, which has order 4. It is readily checked that $x(1\,2) = (1\,2)x = (3\,4)$, so the centralizer of x in D_8 is a subgroup of order strictly bigger than 4, so it must be the whole of D_8. But our labelling of the corners of the square shows D_8 as a subgroup of S_4, hence as a subgroup of S_5, so this is the group we seek.

The following table summarizes these results.

x	cycle structure	$\lvert x^{S_5} \rvert$	$\lvert C(x) \rvert$	$C(x)$
1_{S_5}	1, 1, 1, 1, 1	1	120	S_5
$(1\,2)$	1, 1, 1, 2	10	12	$\langle (1\,2) \rangle \times (S_3 \text{ on } \{3,4,5\})$
$(1\,2\,3)$	1, 1, 3	20	6	$\langle (1\,2\,3) \rangle \times \langle (4\,5) \rangle$
$(1\,2\,3\,4)$	1, 4	30	4	$\langle (1\,2\,3\,4) \rangle$
$(1\,2\,3\,4\,5)$	5	24	5	$\langle (1\,2\,3\,4\,5) \rangle$
$(1\,2\,3)(4\,5)$	2, 3	20	6	$\langle (1\,2\,3)(4\,5) \rangle$
$(1\,2)(3\,4)$	2, 2	15	8	D_8 on the labelled square above

Now we find all the normal subgroups of S_5. Each normal subgroup consists of some of the conjugacy classes, always including the class of size 1, and the sum n of the sizes of the relevant conjugacy classes must divide 120, by Lagrange's Theorem.

If we include the class of size 24 then (since we always include the class of size 1) 5 divides n, $25 \leqslant n$, and n divides 120. The only possibilities are $n = 40$, $n = 60$ and $n = 120$. For $n = 40$, the subgroup consists of the unique conjugacy classes of sizes 1, 24 and 15; but this is impossible, because $(1\ 2)(3\ 4)$ and $(1\ 2)(3\ 5)$ are in the conjugacy class of size 15 and their product $(1\ 2)(3\ 4)(1\ 2)(3\ 5) = (3\ 4\ 5)$, which is one of the conjugacy classes of size 20. Similarly, the only possibility for $n = 60$ is the union of the unique conjugacy classes of size 1, 24 and 15 together with the conjugacy class of size 20 consisting of the 3-cycles. These are precisely the even permutations, giving the normal subgroup A_5. Of course, $n = 120$ gives the normal subgroup S_5.

If we do not include the class of size 24 then 5 does not divide n, so n divides 24: the only possibility is $n = 1$, corresponding to the normal subgroup $\{1_{S_5}\}$.

Does S_5 have *any* subgroup of order 40? Suppose that H is such a subgroup. Then $|S_5 : H| = 3$, so S_5 has a normal subgroup K such that $K \leqslant H$ and S_5/K is isomorphic to a transitive subgroup of S_3. We have just seen that the only normal subgroup of S_5 with order less than or equal to 40 is just $\{1_{S_5}\}$, so $|S_5/K| = 120$, so S_5/K cannot be isomorphic to S_3, which has order 6. Therefore, S_5 has no subgroup of order 40.

A similar argument shows that S_5 has no subgroup of order 30.

Given a subgroup H of a group G, and an element g in G, define

$$H^g = \left\{g^{-1}hg : h \in H\right\},$$

which is called the *conjugate* of H by g. We also write $H^g = g^{-1}Hg$.

Theorem (a) H^g is a subgroup of G;

(b) H^g is isomorphic to H;

(c) The map $g \mapsto \pi_g$, where $\pi_g\colon H \mapsto H^g$ for g in G, is an action of G on the set of subgroups of G.

Proof Exercise.

The stabilizer of H in this action is

$$\left\{g \in G : g^{-1}Hg = H\right\} = \{g \in G : H^g = H\},$$

which is called the *normalizer* of H, written $N(H)$. Then $H \trianglelefteq N(H) \leqslant G$; in fact, $N(H)$ is the largest subgroup of G in which H is normal. If $H \trianglelefteq G$ then $N(H) = G$. By the Orbit-Stabilizer Theorem, the number of conjugates of H in G is equal to $|G : N(H)|$.

Theorem If α and β are in the same orbit of some action π of a group G, then G_β is conjugate to G_α. More precisely, if $\alpha\pi_g = \beta$ then $G_\beta = G_\alpha^g$.

Proof Suppose that $\alpha\pi_g = \beta$. Put $H = G_\alpha$. Then

$$\begin{aligned} x \in H^g &\Rightarrow x = g^{-1}hg \qquad \text{for some } h \text{ with } \alpha\pi_h = \alpha \\ &\Rightarrow \beta\pi_x = \beta\pi_{g^{-1}hg} = \beta\pi_g^{-1}\pi_h\pi_g = \alpha\pi_h\pi_g = \alpha\pi_g = \beta \\ &\Rightarrow x \in G_\beta. \end{aligned}$$

This shows that $H^g \subseteq G_\beta$. Conversely,

$$\begin{aligned} x \in G_\beta &\Rightarrow \beta\pi_x = \beta \\ &\Rightarrow \alpha\pi_g\pi_x = \alpha\pi_g \\ &\Rightarrow \alpha\pi_g\pi_x\pi_g^{-1} = \alpha \\ &\Rightarrow \alpha\pi_{gxg^{-1}} = \alpha \\ &\Rightarrow gxg^{-1} \in H \\ &\Rightarrow x = g^{-1}gxg^{-1}g \in H^g. \end{aligned}$$

This shows that $G_\beta \subseteq H^g$. Hence $G_\beta = H^g$. $\square$

Theorem Given a subgroup H of a finite group G, consider the action of H on the right cosets of H in G, acting by right multiplication. The coset Hg is a fixed point (that is, in an orbit of size 1) if and only if $g \in N(H)$.

Proof Write $\alpha = H$ and $\beta = Hg$. Then

$$G_\alpha = \{x \in G : Hx = H\} = H,$$

so $G_\beta = H^g$, by the preceding theorem. Then $H_\beta = \{x \in H : \beta h = \beta\} = G_\beta \cap H = H^g \cap H$. Therefore

$$\begin{aligned} \beta \text{ is a fixed point for the action of } H \quad &\iff \quad \left|H : H_\beta\right| = 1 \\ &\iff \quad H_\beta = H \\ &\iff \quad H^g \cap H = H \\ &\iff \quad H \subseteq H^g. \end{aligned}$$

If $g \in N(H)$ then $H^g = H$ so $H^g \cap H = H$ so β is a fixed point. Conversely, if β is a fixed point then $H \subseteq H^g$. Conjugating by g again gives $H^g \subseteq H^{g^2}$. Continuing like this gives $H^{g^m} \subseteq H^{g^{m+1}}$ for all positive integers m. If G is finite then there is some positive integer n such that $g^n = 1_G$, so $H^{g^{n-1}} \subseteq H^{1_G} = H$. This gives the chain

$$H \subseteq H^g \subseteq H^{g^2} \subseteq \cdots \subseteq H^{g^{n-1}} \subseteq H.$$

If a chain of inequalities begins and ends with the same thing then all the terms must be equal, so $H = H^g$, which implies that $g \in N(H)$. $\square$

There are some infinite groups for which there is a subgroup H and an element g such that

$$H \subsetneqq H^g \subsetneqq H^{g^2} \subsetneqq \cdots \subsetneqq H^{g^{n-1}} \subsetneqq H^{g^n} \subsetneqq \cdots.$$

In any such group, the "only if" part of the theorem is not true.