

ALGEBRA HOMEWORK SET I SOLUTIONS

JAMES CUMMINGS

- (1) Let G be a group and let $H, K \leq G$. The *double cosets of H and K* are the subsets of G of the form HaK where $a \in G$. Prove that the double cosets form a partition of G . Is it true in general that all the double cosets have the same cardinality? (Either prove it or give a counterexample)

It is easy to check that the binary relation in which a is related to b iff $b = hak$ for $h \in H, k \in K$ is an equivalence relation.

For a slick analysis we can think of $H \times K$ acting on G by the action where (h, k) applied to g gives $h g k^{-1}$. The stabiliser of g is the set of (h, k) such that $h g k^{-1} = g$, that is $h g = g k$ or $g k g^{-1} = h$.

So for fixed g , every $h \in H \cap K^g$ is the first entry of a unique element $(h, h^{g^{-1}})$ of the stabiliser of g . Hence the order of the stabiliser is $|H \cap K^g|$.

Now it is easy to find an example where double cosets have different sizes. In S_3 let $H = \langle (12) \rangle$, $K = \langle (13) \rangle$. They are distinct conjugate subgroups, in particular $H^{(23)} = K$.

Then $HeK = HK = \{e, (12), (13), (12)(13) = (132)\}$. The other double coset here is $H(23)K = \{(23), (123)\}$.

- (2) Let G be a group and let $H, K \leq G$. Prove that if $h_1, h_2 \in H$ then $h_1K = h_2K \iff h_1(H \cap K) = h_2(H \cap K)$. Use this to prove that if H, K are both finite then the set of products HK has cardinality $|H| \times |K| / |H \cap K|$.

Since $h_1^{-1}h_2 \in H$,

$$h_1K = h_2K \iff h_1^{-1}h_2 \in K \iff h_1^{-1}h_2 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K).$$

HK is the union of cosets of form hK for $h \in H$, and by the calculation above there are exactly $[H : H \cap K]$ such cosets, each of which has size $|K|$.

- (3) Recall from class that for any group G
- (a) An *automorphism* (AM) of G is an isomorphism from G to G .
 - (b) For any $g \in G$, the map $h \mapsto h^g$ is an AM of G , where as usual $h^g = ghg^{-1}$.
 - (c) $N \triangleleft G$ iff $N^g = N$ for all $g \in G$.

A subgroup H of G is said to be *characteristic* iff $\alpha(H) = H$ for every AM α of G (so that clearly any characteristic subgroup is normal). In this case we write " $H \text{ char } G$ ".

- (a) Prove that $Z(G)$ is a characteristic subgroup of G .

This is routine. Any subgroup defined in terms of the group operation will be characteristic for similar reasons.

- (b) Give an example of a group G and a normal subgroup of G which is not characteristic. Hint: every subgroup of an abelian group is normal.

Let $G = C_2^2$ where C_2 is cyclic of order 2. Let $N = C_2 \times \{e\}$. Then $N \triangleleft G$ but N is not fixed by the AM $(a, b) \mapsto (b, a)$.

- (c) Let G be a group. Prove that if $A \text{ char } B$ and $B \text{ char } G$ then $A \text{ char } G$, and that if $A \text{ char } B$ and $B \triangleleft G$ then $A \triangleleft G$.

Let $A \text{ char } B$ and $B \text{ char } G$. If $\gamma \in \text{Aut}(G)$ then since $B \text{ char } G$ we have that the restriction $\gamma \upharpoonright B \in \text{Aut}(B)$, so in particular since $A \text{ char } B$ we have $\gamma(A) = A$.

Now let $A \text{ char } B$ and $B \triangleleft G$. Let $g \in G$. Since $B \triangleleft G$ we have $B^g = B$, which means that the restriction of the AM “conjugate by g ” to B is in $\text{Aut}(B)$. Since $A \text{ char } B$ we have $A^g = A$.

- (d) Give an example of a group G and subgroups $B \triangleleft G$ and $A \triangleleft B$ such that A is not normal in G .

Let $G = D_4$, the dihedral group of order 8 which can be represented as the symmetries of a square. Let s be rotation through $\pi/2$ and let t be reflection in a line joining opposite vertices. Then let $A = \{e, t\}$ and $B = \{e, t, s^2, ts^2\}$.

Note: By the following question we see $A \triangleleft B \triangleleft G$ without doing any work. Geometrically s^2 is rotation through π and s^2t is the other reflection in a line joining opposite vertices. A is not normal in G because $sts^{-1} = ts^2$.

Note: we knew we needed $A \triangleleft B$ with A not characteristic in B , so it's not surprising that the counterexample has this form.

- (4) Let G be a group and let $H \leq G$ with $[G : H] = 2$.
 (a) Prove that $H \triangleleft G$, and that if $h \in H$ then the G -conjugacy class of h is a subset of H .

There are just two cosets of H , namely H and $G \setminus H$. If $g \in H$ then $gH = H = Hg$, otherwise $gH = G \setminus H = Hg$. So $H \triangleleft G$. The other claim is immediate.

- (b) Prove that if $h \in H$ then *either* the G -conjugacy class of h equals the H -conjugacy class of h *or* the G -conjugacy class of h is the union of two disjoint H -conjugacy classes.

We do a more general analysis from which the required result follows easily.

Let G and $H \leq G$ be arbitrary, and let G act on some set X . Let $x \in X$ and let $\mathcal{O}_x^G, \mathcal{O}_x^H$ be its orbits under the actions of G and H . If $\mathcal{O}_x^G = \mathcal{O}_x^H$ then for every $g \in G$ there is $h \in H$ with $gx = hx$, so that $h^{-1}g \in G_x$ and $g \in HG_x$; arguing along these lines we see easily that $\mathcal{O}_x^G = \mathcal{O}_x^H$ if and only if $G = HG_x$.

Now specialise to the case where $[G : H] = 2$ but the action is still arbitrary. Since $H \triangleleft G$, $HG_x \leq G$ and so easily $G = HG_x$ if and only if $G_x \not\leq H$. If on the other hand $G_x \leq H$ then (letting H_x be the stabiliser of x in the H -action) we have $H_x = G_x \cap H = G_x$. In this case the G -orbit of x is in bijection with the left cosets of G_x in G , and under this bijection the points of the H -orbit correspond to the left cosets of G_x in H .

To finish we specialise even more, to the case where $X = H$ and G is acting on H by conjugation. We see that the stabiliser of h is $C_G(h)$, and that the conjugacy class splits into two if and only if $C_G(h) \leq H$.

- (5) Show that if G is a group such that $a^2 = e$ for all $a \in G$, then G is abelian. (Trickier) Produce an example of a non-abelian group G such that $a^3 = e$ for all $a \in G$.

$(ab)^2 = abab = e$, so multiplying from the left by a and the right by b we see $ba = ab$.

(Tricky bit) If G is finite then easily G must be a 3-group. All groups of order p and p^2 for p prime are abelian, so the smallest order that can work is order 27.

Looking at one of the useful online lists of groups of small order, you will find that there are two non-abelian groups of order 27. We check that one of the them works (and will see later how you could guess that this would be the right group and construct it for yourself).

The group is generated by elements x, y, z such that

$$x^3 = y^3 = z^3 = e, xy = yx, xz = zx, zy = xyz.$$

Every element can easily be written in the form $x^i y^j z^k$ for unique $i, j, k \in \{0, 1, 2\}$. It is also easy to check that $z^a y^b = x^{ab} y^b z^a$ (move all the z 's rightwards and all the x 's which are generated leftwards).

Since x commutes with everything $(x^i y^j z^k)^3 = x^{3i} (y^j z^k)^3$. Finally

$$y^j z^k y^j (z^k y^j) z^k = x^{jk} y^j z^k y^{2j} z^{2k} = x^{3jk} y^{3j} z^{3k} = e,$$

and we are done.

- (6) Prove that if $G/Z(G)$ is cyclic then G is abelian (so in fact $Z(G) = G$). Give an example of a non-abelian group such that $G/Z(G)$ is abelian.

Let $G/Z(G)$ be generated by a coset $aZ(G)$, so that every element of G has form $a^m z$ for $z \in Z(G)$. Then $a^m z a^n z' = a^{m+n} z z' = a^n z' a^m z$, so that G is abelian and in fact $Z(G) = G$.

Now let G be the dihedral group of order 8, that is the symmetries of the square. The centre $Z(G)$ consists of e and the rotation through π , and $G/Z(G)$ has order 4.

- (7) Find $Z(G)$ when G is the group of non-singular $n \times n$ real matrices under matrix multiplication (and $n \geq 2$).

(This is the quickest way I know. Brute force also works!)

Note that the set of matrices which commute with a fixed matrix A is closed under addition and scalar multiplication. So $A \in Z(G)$ iff A commutes with all matrices in the span of G (considering the set of matrices to be a real vector space of dimension n^2 in the obvious way).

Now for all i, j let $D_{i,j}$ be the matrix with a 1 in the (i, j) position and zeroes elsewhere. Then routinely $I_n + D_{i,j} \in G$. It follows that all the $D_{i,j}$ are in the span of G (so in fact all matrices are in the span).

It is now easy to check that $A \in Z(G)$ iff $A = \lambda I_n$ for some real λ .