

**620-222: Linear and Abstract Algebra 2007**  
**Solutions to Assignment 2**

1. (a) Note that  $G$  is a non-empty subset of the group  $GL(3, \mathbb{Z}_p)$  so we just need to show that  $G$  is closed under multiplication and taking inverses. Let

$$A = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}, A' = \begin{bmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{bmatrix}$$

be arbitrary elements of  $G$ . Then

$$AA' = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & c+c'+ab' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{bmatrix} \in G,$$

since  $\mathbb{Z}_p$  is closed under addition and multiplication. Further, taking  $a' = -a$ ,  $b' = -b$  and  $c' = ab - c$  gives  $AA' = I$ , so

$$A^{-1} = \begin{bmatrix} 1 & -a & ab - c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix} \in G.$$

Hence  $G$  is a subgroup of  $GL(3, \mathbb{Z}_p)$ .

- (b) Since  $|\mathbb{Z}_p| = p$  there are  $p$  choices for  $a, b, c$  in the matrix  $A$  above, hence  $|G| = p^3$ .  
 Now

$$A'A = \begin{bmatrix} 1 & a+a' & c+c'+a'b \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & a+a' & c+c'+ab' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{bmatrix} = AA'$$

in general, e.g take  $a = 1, a' = 0, b = 0, b' = 1, c = c' = 0$ . So  $G$  is non-abelian.

- (c) For  $A, A'$  as above we have

$$f(AA') = f\left(\begin{bmatrix} 1 & a+a' & c+c'+ab' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{bmatrix}\right) = (a+a', b+b') = (a, b) + (a', b') = f(A) + f(A').$$

So  $f : G \rightarrow \mathbb{Z}_p \times \mathbb{Z}_p$  is a homomorphism.

- (d) We have

$$\ker f = \{A \in G : f(A) = (0, 0)\} = \left\{ \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : c \in \mathbb{Z}_p \right\}$$

and

$$\text{im } f = \{f(A) : A \in G\} = \{(a, b) : a, b \in \mathbb{Z}_p\} = \mathbb{Z}_p \times \mathbb{Z}_p.$$

- (e)  $A$  belongs to the centre  $Z$  of  $G$  iff  $AA' = A'A$  for all  $A' \in G$ . For  $A, A'$  as above, this means  $ab' = a'b$  for all  $a', b' \in \mathbb{Z}_p$ . Taking  $a' = 1, b' = 0$  shows  $a = 0$ ; taking  $a' = 0, b' = 1$  shows  $b = 0$ . Further  $a = b = 0$  implies  $ab' = a'b$  for all  $a', b'$ . Hence the centre of  $G$  is

$$Z = \left\{ \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : c \in \mathbb{Z}_p \right\} = \ker f.$$

- (f) By the isomorphism theorem and parts (d), (e),  $G/Z = G/\ker f \cong \text{im } f = \mathbb{Z}_p \times \mathbb{Z}_p$ .  
 (g) Consider the non-abelian group  $G$  of order 8 obtained when  $p = 2$ .

- (i) By Lagrange's theorem, each element has order 1, 2, 4 or 8 since the order must divide  $|G| = 8$ . There is 1 element of order 1 (the identity), and no elements of order 8 (otherwise  $G$  would be cyclic, hence abelian). Using  $\mathbb{Z}_2$  coefficients we have

$$\begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2a & 2c + ab \\ 0 & 1 & 2b \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & ab \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

So the elements of order 4 are those with  $ab = 1$ ; this gives 2 matrices with  $(a, b, c) = (1, 1, 0)$  or  $(1, 1, 1)$ . The remaining  $8 - 1 - 2 = 5$  elements have order 2; these are the non-identity matrices with  $ab = 0$ , i.e.  $(a, b, c) = (0, 0, 1), (1, 0, 0), (1, 0, 1), (0, 1, 0)$  or  $(0, 1, 1)$ .

- (ii) Since  $Q_8$  has only 1 element of order 2 (and 6 of order 4),  $G \not\cong Q_8$ . Hence  $G \cong D_4$  since this is the only other non-abelian group of order 8.

2. (a) Let  $h$  be a generator for the cyclic group  $H$ . Since  $K$  is a subgroup of a cyclic group,  $K$  is cyclic with a generator  $h^k$  for some integer  $k$  and  $K = \{h^{mk} : m \in \mathbb{Z}\}$ . Let  $g \in G$ . Then since  $H$  is normal in  $G$ ,  $ghg^{-1} \in H$  so  $ghg^{-1} = h^n$  for some integer  $n$ . Then  $gh^k g^{-1} = (ghg^{-1})^k = (h^n)^k = h^{nk} = (h^k)^n \in K$  and  $gh^{mk} g^{-1} = (h^k)^{nm} \in K$ . Hence  $K$  is closed under conjugation, so is normal in  $G$ .  
 (b) There are many possibilities. One example is:

$$G = GL(2, \mathbb{R}), H = SL(2, \mathbb{R}), \text{ and } K = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{R} \right\}.$$

Then  $H$  is a normal subgroup of  $H$  (from lectures), and it is easy to check that  $K$  is a subgroup of  $H$ . However

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in K \text{ but } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \notin K$$

so  $K$  is not a normal subgroup of  $G$ .

3. Let  $G$  be the group of all rotational symmetries of a cube  $X$ .

(b) (i) For a vertex, the stabilizer is the cyclic group of order 3 generated by a rotation by 120 degrees about an axis from the vertex to the opposite vertex, and the orbit is the set of all 8 vertices of  $X$ .

(ii) For the centre (midpoint) of a face, the stabilizer is the cyclic group of order 4 generated by the 90 degree rotation about the axis joining the centre of the face to the centre of the opposite face, and the orbit is the set of all 6 centres of faces of  $X$ .

(iii) For the midpoint of an edge, the stabilizer is the cyclic group of order 2 generated by the 180 degree rotation about the axis joining the midpoint to the midpoint of the opposite edge, and the orbit is the set of all 12 midpoints of edges of  $X$ .

(c)  $|G| = |\text{stabilizer}(x)| \cdot |\text{orbit}(x)|$  for any point  $x$ . Hence  $|G| = 3 \times 8 = 4 \times 6 = 2 \times 12 = 24$  using (i), (ii) or (iii).

(d) Consider the action of  $G$  on the set  $D$  consisting of the four “long diagonals” of the cube. This defines a homomorphism  $\sigma : G \rightarrow \text{Sym}(D) \cong S_4$ .

(i) Recall that a “symmetry” of  $X$  means an isometry of Euclidean space taking the cube  $X$  to itself. Any symmetry which maps each diagonal in  $D$  to itself must either fix or interchange the endpoints of each diagonal. But each endpoint is a vertex of the cube so the corresponding pairs of vertices must either be fixed or interchanged. If one vertex is fixed then its set of 3 neighbouring vertices must be permuted amongst themselves (since distances are preserved by an isometry). But this set of 3 neighbouring vertices does not contain any pair of opposite vertices and so each vertex must be fixed. Repeating the argument, we see that if one vertex is fixed then all vertices are fixed. Therefore, if one pair of opposite vertices is interchanged then all pairs are interchanged.

(ii) In the first case, each vertex is fixed. Hence every point of the cube is fixed and the symmetry is the identity. (e.g. Taking the centre of the cube as origin, we have a linear transformation fixing three linearly independent vectors in  $\mathbb{R}^3$ ; this must be the identity.) In the second case, each vertex is sent to its ‘antipodal point’. Thus, again, the symmetry must be the function that sends each point to its antipodal point. But this is not a rotation since it is represented by the

matrix  $\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$  with determinant  $-1$ .

(iii) Because we are considering only rotations, the first case above must hold and so only the identity fixes each element in  $D$ . Thus the kernel of  $\sigma$  is the identity and  $\sigma$  is an injection by Lemma 2.5.4 from the notes. (Proof: If  $\sigma(g_1) = \sigma(g_2)$  then  $\sigma(g_1 g_2^{-1}) = e$  and so  $g_1 g_2^{-1} = e$  and  $g_1 = g_2$ .)

(iv) Since  $|G| = 24$  and  $\sigma$  is injective, we have  $|\sigma(G)| = 24$ . But  $\sigma(G) \subset \text{Sym}(D)$  and  $|\text{Sym}(D)| = |S_4| = 4! = 24$ . Hence  $\sigma$  is also surjective and so is an isomorphism.