INTRO TO GROUP THEORY - APR. 11, 2012
SOLUTION SET 10
GT15/16. GROUP ACTIONS/ CAYLEY'S THEOREM

1. (a) If x is the origin, then $O_0 = \{0\}$ and $Stab_G(0) = G$. Otherwise x is fixed by no rotation, and the possible stabilizers have order 1 or 2. If $Stab_G(x)$ has two elements, then x is on an axis of reflection, and the orbit is the vertex set of an equilateral triangle. Otherwise no reflection fixes x and the orbit is the vertex set of a possibly irregular hexagon. A sketch shows that the equilateral triangles form two families.

(b) Again only the origin has $Stab_G(x) = \{0\}$. Otherwise x is fixed by no rotation. Then x is either fixed by a reflection with orbit the vertex set of a regular hexagon, or the orbit of x is a possibly irregular 12-gon. Again the hexagons appear in two families.

2. (a) $G = \{\pm 1\}$: each orbit has two elements $O_x = \{\pm x\}$ except for $O_0 = \{0\}$. $Stab_G(0) = G$, otherwise $Stab_G(x) = \{1\}$.

$G = \{g > 0\}$: there are three orbits, $O_{-1} = \{x < 0\}$, $O_0 = \{0\}$, and $O_1 = \{x > 0\}$. $Stab_G(0) = G$, otherwise $Stab_G(x) = \{1\}$.

$G = \mathbb{R}^*$: there are two orbits, $O_0 = \{0\}$, and $\mathbb{R}^*$. $Stab_G(0) = G$, otherwise $Stab_G(x) = \{1\}$.

None of these actions are transitive, but all are faithful.

(b) Similar answer for $G = \{\pm 1\}$ or $\mathbb{C}^*$. For the second group, orbits are rays emanating from the origin and $\{0\}$. For the third, lines through the origin sans origin, and $\{0\}$. For $G = S^1$, the orbits are circles centered at the origin, and the origin.

None of these actions are transitive, but all are faithful.

3. (a) First $\pi(I)(z) = (z + 0)/(0 + 1) = z$.

Next if $g_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $g_2 = \begin{pmatrix} x & y \\ u & v \end{pmatrix}$, and $g_1 g_2 = \begin{pmatrix} ax + bu & ay + bv \\ cx + du & cy + dv \end{pmatrix}$,

$$\begin{aligned} \pi(g_1 g_2)(z) &= [(ax + bu)z + (ay + bv)]/[(cx + du)z + (cy + dv)], \\ \pi(g_1)[\pi(g_2)(z)] &= \pi(g_1)[(xz + y)/(uz + v)] \\ &= [a(xz + y)/(uz + v) + b]/[c(xz + y)/(uz + v) + d]. \end{aligned}$$

This action is not faithful as $\pi(cI)(z) = (cz)/z = z$. It is transitive as $O_1 = X$:

Date: July 27, 2012.

$$g = \begin{pmatrix} 1 & w-1 \\ 0 & 1 \end{pmatrix} : 1 \mapsto w \qquad \text{and} \qquad h = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} : 1 \mapsto 1/0 = \infty.$$

(b) T sends $z \mapsto z+1$; this shifts the complex plane to the right by 1. S sends $z \mapsto -1/z$; if $z = re^{i\theta}$, then $r \mapsto 1/r$ and $\theta \mapsto -\theta + \pi$ (reflection in the imaginary axis). So S interchanges the interior and exterior of the unit circle. This is the beginning of the story for modular forms. S and T generate $SL(2,\mathbb{Z})$, and one next considers the orbits in H under this group (in an advanced number theory class).

(c) Fixed points are solutions to $(az+b)/(cz+d) = z$. If $c \neq 0$, then $cz^2+(d-a)z-d = 0$ and there are at most two solutions in $\mathbb{C}$. If $c = 0$ then the action is by translation along the x-axis and the only fixed point is ∞.

(d) Let $z = x + yi$ with $y > 0$. Consider

$$\frac{(az+b)}{(cz+d)} = \frac{(az+b)\overline{(cz+d)}}{(cz+d)\overline{(cz+d)}} = \frac{(az+b)\overline{(cz+d)}}{|cz+d|^2}.$$

Since the denominator is real and positive, we need only check that the imaginary part of the numerator is positive:

$$\begin{aligned} (a(x+yi)+b) \qquad & (c(x-yi)+d) \\ = \; & ((ax+b)+ayi)((cx+d)-cyi) \\ = \; & [(ax+b)(cx+d)+acy^2] + [(ax+b)(-cy)+(cx+d)(ay)]i. \end{aligned}$$

The imaginary part simplifies to $(ad-bc)y = y > 0$. The action is transitive on H, but not faithful since $-I$ acts as the identity map.

Note that this argument also show that the lower half-plane is preserved by the action of $SL(2,\mathbb{R})$. There are three orbits on X; the third is the real axis (including ∞).

4. (a) If $g = [v_1\ v_2]$, then $\pi(g)e_1 = v_1$. So the orbits are $\{0\}$ and $\mathbb{R}^2\backslash\{0\}$.

First $Stab_G(0) = G$. Otherwise note that

$$Stab_G(e_1) = \begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix}.$$

For general nonzero v, find h such that $he_1 = v$. If $gv = v$, then $ghe_1 = he_1$ and $h^{-1}gh$ is in $Stab_G(e_1)$. So the stabilizer of v is all matrices in $hStab_G(e_1)h^{-1}$.

(b) Closed: $AB(AB)^T = ABB^TA^T = AIA^T = I$ and $det(AB) = det(A)det(B) = 1$. Associative: property of matrix multiplication. Identity: $e = I$, and $II^T = I$. Inverse: $A^{-1}(A^{-1})^T = A^{-1}(A^T)^{-1} = (A^TA)^{-1} = I$.

(c) If $g = [u_1\ u_2\ u_3]$ with $\{u_1, u_2, u_3\}$ an orthonormal basis of $\mathbb{R}^3$, then $\langle u_1, u_1\rangle = 1$. Thus $ge_1 = u_1$, and O_{e_1} is contained in S^2, the unit sphere centered at the origin. But every element of S^2 is u_1 for some g in $SO(3)$ by choosing u_2 and u_3 from the standard

basis. If we replace e_1 with re_1, then the orbit is $x^2+y^2+z^2 = r^2$. So the orbits are spheres centered at the origin, and the origin.

First $Stab_G(0) = G$. Next $Stab_G(e_1) = \{diag(1, r(\theta)\}$ where $r(\theta)$ runs through each plane rotation $\begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$. Then one can finish using the argument in (a).

(d) The same argument as in (a) shows there are two orbits: $\{0\}$ and $(\mathbb{Z}/p)^2\backslash\{0\}$. Thus $|G| = (p^2-1)\cdot|Stab_G(e_1)|$. These matrices have the same form as in (a) with d in $(\mathbb{Z}/p)^*$ and c in $\mathbb{Z}/p$. So $|G| = (p^2-1)(p^2-p)$.

5. (a) As seen in Problem 4, G will have two orbits: the origin and $(\mathbb{Z}/2)^3\backslash\{0\}$. Since the latter orbit has seven elements, the result follows if we show the action is faithful on the orbit. That is, if $gv = v$ for all v, then $g = I$. Note that $ge_i = e_i$ implies g has associated matrix I. So faithful.

(b) Every invertible matrix may be factored into a product of matrices associated to elementary row operations. Here we need only consider row sums and rows switches. These are generated by

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

6. Suppose g is in $Stab_G(y)$, so $\pi(g)y = y$. If $\pi(h)x = y$, then $\pi(h)\pi(h)x = \pi(h)x$, so $h^{-1}gh$ is in $Stab_G(x)$, or g is in $hStab_G(x)h^{-1}$.

7. (a) Closed: $\pi_{a,b}(\pi_{c,d}(x)) = \pi_{a,b}(cx+d) = a(cx+d)+b = acx+(ad+b) = \pi_{ac,ad+b}$. Associative: follows from associativity of composition of functions. Identity: $e = \pi_{1,0}$. Inverse: $\pi_{a,b}^{-1} = \pi_{1/a,-b/a}$.

We define the isomorphism by

$$\pi_{a,b} \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

noting that

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}.$$

(b) D_{2n} is the subgroup with $a = \pm 1$. Check for generators and relations. To see that G_n is isomorphic to $Aut(D_{2n})$, we first note that both groups have $n\phi(n)$ elements. The action by conjugation is faithful, so all automorphisms for D_{2n} arise from inner automorphisms of G_n restricted to D_{2n}. Finish by verifying that $D_{2n} \triangleleft G_n$ and $Z_{G_n}(D_{2n}) = \{e\}$.

(c) As with the dihedral groups, we identify G with the subgroup of G_7 where a is in $\{1, 2, 4\}$. One finds generators and checks relations for G. We have seen that $Aut(G)$ has 42

elements, as does G_7. We finish by noting that each automorphism of G is the restriction of an inner automorphism of G_7. For this, we need to show $G \triangleleft G_7$ and $Z_{G_7}(G) = \{e\}$, which we leave as an exercise.

(d) First if $p < q$, we have seen that non-trivial implies that $q = pk + 1$ and there exists a unique subgroup H_p of order p in $(\mathbb{Z}/q)^*$. To find subgroups in G_q, we consider the group G with relations

$$y^p = e, \qquad x^q = e, \qquad yxy^{-1} = x^s$$

for some fixed s in H_p. For the matrices, we restrict a to elements of H_p and find generators in G_q satisfying the relations for G. For instance,

$$y \mapsto \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}, \qquad x \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We have seen that $Aut(G)$ has $q(q-1)$ elements, as does G_q. Same finish as in part (c).

These generators and relations all describe the same subgroup of G_q, so there is only one isomorphism class.

8. (a) If the cycles of σ have length n_i, then $|\sigma| = lcm(n_i)$.

(b) We can always embed $\mathbb{Z}/n$ into S_n by sending 1 to $(1234\ldots n)$. To improve, we factor n into powers of prime $p_i^{i_k}$. Then use $m = \sum p_j^{i_j}$. By (a),

$$\sigma = (12\ldots p_1^{i_1})\ldots(1'2'\ldots p'^{i_k}_k),$$

has order n; here we reuse labels; that is, 1 is distinct from $1'$.

9. (a) Since there are no non-trivial, proper normal subgroups, the Corollary says $|G|$ must divide $[G : H]$. If $|H| = 15, 20$, or 30, then $[G : H]! = 24, 6$, or 2, none of which are divisible by 60.

(b) Same argument as part (a). If $|H| = 28, 42$, or 84, then $[G : H]! = 720, 24$, or 2, none of which are divisible by 168.

10. Two subgroups: these must be $\{e\}$ and G. If there is an element $g \neq e$, then $G = \langle g \rangle$ is cyclic. To have no proper subgroups, $|g| = p$, a prime. So $G \cong \mathbb{Z}/p$.

Three subgroups: since we must have $\{e\}$ and G, there is a unique proper, non-trivial subgroup H. This subgroup can have no subgroups except for $\{e\}$ and H. By the two-subgroup result, $H \cong \mathbb{Z}/p$ for some prime p. If g is not in H, then $G = \langle g \rangle$. Thus G is cyclic with subgroup $\mathbb{Z}/p$. If $|G| = pk$, then $k = p$ since each divisor of $|G|$ corresponds to a subgroup of G. That is, $G \cong \mathbb{Z}/p^2$.