INTRO TO GROUP THEORY - MAR. 21, 2012
SOLUTION SET 7 - GT10/11. EXAMPLES OF NON-ISOMORPHIC GROUPS/AUTOMORPHISMS

1. First we show the four group properties.

(1) Closed under multiplication: $x \circ y$ is a real number.
(2) Identity: $e = -2$, $-2 + x = -2 + x + 2 = x$.
(3) Inverse: $x^{-1} = -x - 4$, $x \circ x^{-1} = x + (-x - 4) + 2 = -2 = e$.
(4) Associativity:

$$((x \circ y) \circ z) = (x + y + 2) \circ z = (x + y + 2) + z + 2 = x + y + z + 4 = (x \circ (y \circ z)).$$

Isomorphism: $\pi(x) = x + 2$. This is clearly a bijection. Homomorphism:

$$\pi(x \circ y) = \pi(x + y + 2) = x + y + 4 = \pi(x) + \pi(y).$$

2. (a) We saw that $\pi(H)$ is a subgroup of K if π is a homomorphism. If we restrict π to H, then π is a bijective homomorphism from H to $\pi(H)$.

To see that $[G : H] = [K : \pi(H)]$, consider the map $\pi' : G/H \to K/\pi(H)$ defined by

$$\pi'(gH) = \pi(gH) = \pi(g)\pi(H).$$

To see π' is onto, if we choose g in G such that $\pi(g) = k$, then

$$\pi(gH) = \pi(g)\pi(H) = k\pi(H).$$

To see π is one-one, suppose $\pi'(gH) = \pi'(g'H)$. Then $\pi(g)\pi(H) = \pi(g')\pi(H)$ or $\pi(g^{-1}g')$ is in $\pi(H)$. Thus $g^{-1}g'$ is in H or g' is in gH.

(b) If k is in K, then there is some g such that $\pi(g) = k$. Now

$$k\pi(N)k^{-1} = \pi(g)\pi(N)\pi(g^{-1}) = \pi(gNg^{-1}) = \pi(N).$$

So $\pi(N) \triangleleft K$. The isomorphism of quotient groups follows from (a). Also by (a), the cyclic groups generated by xN and $\pi(x)\pi(N)$ are isomorphic, so equal order.

3. (a) $D_8/Z(D_8)$ has four elements. Since $(1234)^2 = (1432)^2 = (13)(24)$ is in $Z(D_8)$, all elements of the quotient have order 2. So isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$.

$D_{12}/Z(D_{12})$ has six elements. Since $(123456)^3 = (165432)^3 = (13)(25)(36)$ is in $Z(D_{12})$, there are no elements of order 6 in the quotient. So isomorphic to S_3.

$D_{12}/\{e, r^2, r^4\}$ has 4 elements. Since D_{12} has no elements of order 4, the quotient group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Date: March 28, 2012.

(b) S_4/H has six elements. Since S_4 has no elements of order 6, the quotient is isomorphic to S_3.

4. The elements with order are:

(1) $(e, 0), 1$,
(2) $((123), 0), ((132), 0), 3$,
(3) $((123), 1), ((132), 1), 6$,
(4) $(e, 1), ((12), 0), ((12), 1), ((13), 0), ((13), 1), ((23), 0), ((23), 1), 2$.

G is isomorphic to D_{12}. In terms of generators of relations, let $x = ((123), 1)$ and $y = ((12), 0)$. Then $x^6 = e$, $y^2 = e$, and $yxy^{-1} = x^{-1}$. For an explicit isomorphism, let $\pi(x) = (123456)$ and $\pi(y) = (16)(25)(34)$.

5. (a) Suppose $x^2 = e$ for all x in G. We have allready shown that G is abelian. Choose $y \neq e$ in G. Let $H = \{e, y\}$, so that G/H also has all $(xH)^2 = H$. Using induction, we see that $|G| = 2^n$ and G has a minimal generating set $\{x_1, x_2, \ldots, x_n\}$. Define an isomorphism $\pi : G \to (\mathbb{Z}/2)^n$ by

$$\pi(x_1^{i_1} \ldots x_n^{i_n}) = (i_1, \ldots, i_n)$$

where each i is in $\{0, 1\}$.

(b) If we write the group multiplication as addition, then G will satisfy all the properties of vector space over the field $\mathbb{Z}/2$. Since G is finite, G is finite dimensional as a vector space over $\mathbb{Z}/2$. If we choose a basis, passing to coordinates gives an isomorphism with some $(\mathbb{Z}/2)^n$.

6. Each automorphism π is a bijection, but $\pi(e) = e$ means that we have at most $|G| - 1$ degrees of freedom. Hence $(|G| - 1)!$.

First $|Aut(\mathbb{Z}/2)| = (2-1)! = 1$, and the only automorphism is the identity element. Next $|Aut(\mathbb{Z}/3)| = (3 - 1)! = 2$. These are given by the identity and inverse automorphisms.

7. First G is generated by any element x of order 4 and any element y of order 2 such that $x^2 \neq y$. G has four elements of order 4 and three elements of order 2. Thus there are $4 \times 2 = 8$ elements in $Aut(G)$.

8. Here Q is the quaternion group, which we have not seen yet. There are only two non-abelian groups of order eight (up to isomorphism), Q and D_8.

(a) M_1 has order 4; $M_1^2 = -I$ and $M_1^{-1} = M_1^3 = -M_1$. M_2 also has order 4; $M_2^2 = -I$ and $M_2^3 = -M_2$. $M_3 = M_1 M_2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ again has order 4, $M_3 = -I$, and $M_3^3 = -M_3$.

Thus Q has eight elements, six of which have order 4. One sees immediately that $M_1 M_2 \neq M_2 M_1$, so Q is non-abelian, but not isomorphic to D_8, which has only two elements of order 4.

9. (a) Since $SL(2, \mathbb{Z}/p) \triangleleft GL(2, \mathbb{Z}/p)$ as the kernel of the homomorphism det (which is onto $(\mathbb{Z}/p)^*$), the number of cosets is

$$[G : H] = |(\mathbb{Z}/p)^*| = p - 1$$

by the Isomorphism Theorem. So

$$|H| = |G|/(p-1) = p^3 - p.$$

24, 120, 336.

(b) $|Z(G)| = p - 1$ and $|Inn(G)| = p^3 - p$. In this case of H, $det(A) = c^2 = 1$. Since $\mathbb{Z}/p$ is a field and $p > 2$, $(x^2 - 1) = (x + 1)(x - 1)$ has distinct roots $c = \pm 1$. So $|Z(H)| = 2$ and $|Inn(H)| = (p^3 - p)/2$.

12, 60, 168. (60 and 168 are simple group orders!)

10. The automorphism group is isomorphic to $SL(3, \mathbb{Z}/2)$. Using linear algebra, the columns of a non-singular matrix must form a basis of $(\mathbb{Z}/2)^3$. There are $2^3 - 1 = 7$ options for the first column (discard (0,0,0)). Then there are $2^3 - 2 = 6$ options for the second column (discard multiples of column 1). Finally there are $2^3 - 2^2 = 4$ options for the third column (discard all linear combinations of the first two columns). This gives $7 \times 6 \times 4 = 168$ elements in G.

$$\text{Order 2: } \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \qquad \text{Order 3: } \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \qquad \text{Order 7: } \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Verify and note that $x^7 - 1 = (x - 1)(x^3 + x^2 + 1)(x^3 + x + 1)$ over $\mathbb{Z}/2$. The element of order 7 is the companion matrix for $x^3 + x + 1$.