INTRO TO GROUP THEORY - FEB. 22, 2012
PROBLEM SET 3 - GT3. COSETS AND LAGRANGE'S THEOREM

1. (a) ($\rightarrow$) if $xH = yH$, then $x = xe$ is in yH.

($\leftarrow$) If x is in yH then $x = yh$ for some h in H. Thus if h' is in H, then $xh' = yhh'$ is in yH, and $xH \subseteq yH$. On the other hand, $y = xh^{-1}$ and a similar argument shows $yH \subseteq xH$. So $xH = yH$.

(b) $H = \{e, (123), (132)\}$.

(1) $(12)(34)H = \{(12)(34), (243), (143)\}$,
(2) $(243)H = \{(243), (143), (12)(34)\}$. and
(3) $(143)H = \{(143), (12)(34), (243)\}$.

2. Note that x is an element of xH and Hx. Also note the partitions of A_4.

(1) $H_1 = \{e, (123), (132)\}$,
(2) $(124)H_1 = \{(124), (14)(23), (134)\}$
(3) $(12)(34)H_1 = \{(12)(34), (243), (143)\}$, and
(4) $(142)H_1 = \{(142), (234), (13)(24)\}$.

(1) $H_1 = \{e, (123), (132)\}$,
(2) $H_1(124) = \{(124), (13)(24), (243)\}$,
(3) $H_1(12)(34) = \{(12)(34), (134), (234)\}$, and
(4) $H_1(142) = \{(142), (143), (14)(23)\}$.

(1) $H_2 = \{e, (12)(34), (13)(24), (14)(23)\}$,
(2) $(142)H_2 = \{(142), (243), (134), (123)\} = H_2(142)$, and
(3) $(124)H_2 = \{(124), (143), (132), (234)\} = H_2(124)$.

3. Suppose there exists a subgroup H of order 6. H must contain an element of order 3; the products of disjoint 2 cycles generate a subgroup of order 4. We may assume this element is (123), so $H_1 \subset H$. If x is in H but not in H_1, then xH_1 and H_1x are contained in H. The possibilities are listed in Problem 2, so $H_1 \cup xH_1 \cup H_1x$ has at least 8 elements. By Lagrange's Theorem, $H = A_4$. (If the cosets weren't readily available, we could use Cauchy's Theorem to get elements of order 2 and 3 and work from there.)

Date: February 16, 2012.

4. Note that x is an element of xH and Hx. Also note the partitions of D_8.

(1) $H_1 = \{e, (13)(24)\}$,
(2) $(1234)H_1 = \{(1234), (1432)\} = H_1(1234)$
(3) $(13)H_1 = \{(13), (24)\} = H_1(13)$,
(4) $(12)(34)H_1 = \{(14)(23), (12)(34)\} = H_1(12)(34)$.

(1) $H_2 = \{e, (13)\}$,
(2) $(24)H_2 = \{(24), (13)(24)\}$,
(3) $(1234)H_2 = \{(1234), (14)(23)\}$, and
(4) $(1432)H_2 = \{(1432), (12)(34)\}$.

(1) $H_2 = \{e, (13)\}$,
(2) $H_2(24) = \{(24), (13)(24)\}$,
(3) $H_2(1234) = \{(1234), (12)(34)\}$, and
(4) $H_2(1432) = \{(1432), (14)(23)\}$.

5. Well-defined: if x and y belong to the same coset, we show $\omega(x) = \omega(y)$. Since $x = y + n$ for some n in $\mathbb{Z}$,

$$\omega(x) = exp(2\pi i(y+n)) = exp(2\pi iy + 2\pi in) = exp(2\pi iy)exp(2\pi in) = exp(2\pi iy) = \omega(y).$$

This allows us to define ω' on cosets: $\omega'(x + H) = \omega(x)$.

One-one: suppose $\omega'(x + H) = \omega'(y + H)$. Then $\omega(x) = exp(2\pi ix) = exp(2\pi iy) = \omega(y)$, and $exp(2\pi i(x - y)) = 1$. Thus $x - y$ is in $\mathbb{Z}$, and x and y belong to the same coset. That is, $x + H = y + H$.

Onto: Fix α on the unit circle. Then $\alpha = exp(2\pi ix)$ for some x in $\mathbb{R}$. Then $\omega'(x+H) = \alpha$.

6. (a) $1 = det(I) = det(AA^T) = det(A)det(A^T) = [det(A)]^2$.

(b) Closed under multiplication: $(AB)^{-1} = B^{-1}A^{-1} = B^TA^T = (AB)^T$. So AB is in $O(2)$.

Closed under inverses: $(A^{-1})^{-1} = (A^T)^{-1} = (A^{-1})^T$. So A^{-1} is in $O(2)$.

Nonempty: $I = I^{-1} = I^T$, so I is in $O(2)$.

(c) $det(AB) = det(A)det(B) = 1$ (closed under multipication) and

$$det(A^{-1}) = 1/[det(A)] = 1$$

(closed under inverse). $det(I) = 1$ so nonempty.

$$I = AA^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{pmatrix}.$$

Thus

$$a^2 + b^2 = 1, \qquad c^2 + d^2 = 1, \qquad ac = -bd, \qquad \text{and} \qquad ad - bc = 1.$$

Since (d, c) corresponds to some point on the unit circle, we can choose $d = cos(\theta)$ and $c = sin(\theta)$, which forces $b = -sin(\theta), a = cos(\theta)$.

7. (a) Straightforward. Key points: $det(A) > 0$ so the inverse formula yields positive diagonal entries. I is in H, so nonempty.

(b) Note that $RR^T = R^TR = I$. Thus $A^TA = U^TR^TRU = U^TU$. Let $U = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$. Then

$$U^TU = \begin{pmatrix} x^2 & xy \\ xy & y^2 + z^2 \end{pmatrix}.$$

But $A^TA = U^TU$, so

$$\begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix} = \begin{pmatrix} x^2 & xy \\ xy & y^2 + z^2 \end{pmatrix}.$$

Thus

$$x = \sqrt{a^2 + c^2} > 0, \qquad y = \frac{ab + cd}{\sqrt{a^2 + c^2}}, \qquad z = \frac{det(A)}{\sqrt{a^2 + c^2}} > 0.$$

Now solve

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} C & -S \\ S & C \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$$

to get

$$C = \frac{a}{\sqrt{a^2 + c^2}}, \qquad S = \frac{c}{\sqrt{a^2 + c^2}}.$$

Uniqueness of the decomposition follows since $SO(2) \cap H = I$. Then $RU = R'U'$ imples $R^{-1}R' = U(U')^{-1} = I$. So $R = R'$ and $U = U'$.

(c) Well-defined: we show that if x and y belong to the same coset, then $\omega(x) = \omega(y)$. Then ω' is defined on the coset space by $\omega'(xH) = \omega(x)$. If $x = RU$ and $y = R'U'$ belong to the same coset, then $y = xh$ for some h in H. Then $R'U' = RUh$. By uniqueness of the decomposition, $R = R'$ and $U' = Uh$. Thus $\omega(x) = \omega(y)$.

One-one: If $\omega'(xH) = \omega'(yH)$, then $R = R'$ and $xH = RH = R'H = yH$.

Onto: If R is in S^1, then R is in RH, and $\omega'(RH) = R$.

8. (a) Same argument as in Problem 6, change $>$ to $\neq$.

(b) Order of G : there are p^4 2×2 matrices over $\mathbb{Z}/p$. We discard those with

$$det(A) = ad - bc = 0.$$

If b, d both not 0, this is equivalent to $a = bk, c = dk$ for some k in $\mathbb{Z}/p$. Otherwise there are p^2 remaining matrices with $b = d = 0$. Counting gives $p(p^2 - 1) + p^2 = p^3 + p^2 - p$ matrices with $det(A) = 0$. Thus G has $p^4 - p^3 - p^2 + p = (p^2 - 1)(p^2 - p)$. With more linear algebra, we confirm the answer by counting the number of bases.

For the order of H, each diagonal entry gives $p - 1$ choices and the off-diagonal entry has p choices. Thus $|H| = p(p - 1)^2$.

The coset space G/H has $|G|/|H|$ elements. Factoring gives $p+1$ elements. These elements correspond to the lines through the origin in $(\mathbb{Z}/p)^2$. More when we have group actions.

9. Order 2: the only possible orders of elements are 1 and 2, and only the identity element has order 1. So there must be an element of order 2, say x. $G = \{e, x\}$ with $x^2 = e$. Note that $x = x^{-1}$. G is abelian.

Order 3: the only possible orders of elements are 1 and 3, and only the identity element has order 1. So there must be an element of order 3, say x. Consider x^2. If $x^2 = e$, x is an element of order 2. If $x^2 = x$, then $x = e$. Thus the remaining element is x^2, and $x^{-1} = x^2$. Thus $G = \{e, x, x^2\}$ with $x^3 = e$. G is cyclic.

Order 4: the possible orders of elements are 1, 2, or 4. If there exists and element of order 4, say x, then we reason that $G = \{e, x, x^2, x^3\}$ with $x^4 = e$. Then G is cyclic. If no element of order 4, then there are three elements of order 2, each self-inverse since $x^2 = e$ implies $x = x^{-1}$. If we label two of these elements x and y, then the third element is xy. Because yx is not equal to e, x or y, we have $yx = xy$. G is abelian, but not cyclic. This is the Klein group $\mathbb{Z}/2 \times \mathbb{Z}/2$; we've seen it before as a subgroup of A_4.

Note that we can do the proofs without Lagrange's Theorem, but I'll leave that as another exercise.

10. By the Corollary to Lagrange's theorem, $|x|$ divides $|G|$. Thus $|G| = m|x|$, and $x^{|G|} = (x^{|x|})^m = e$.

Orders:

(1) S_3 : 1, 2, 3 divide 6,
(2) A_4 : 1, 2, 3 divide 12,
(3) D_8 : 1, 2, 4 divide 8, and
(4) $\mathbb{Z}/12$: 1, 2, 3, 4, 6, 12 divide 12.