Math 453—Fall 2011
Exam I
Solution

Show *all* work. Justify all your answers. Do the problems in an order which will maximize *your* score.

1. (8 points) Use the Euclidean algorithm to find $\gcd(3648, 1752)$.

Solution.
We use the division algorithm, repeatedly:

$$3648 = 1752 \cdot 2 + 144;$$
$$1752 = 144 \cdot 12 + 24;$$
$$144 = 24 \cdot 6 + 0.$$

Since 24 is th last non-zero remainder in the process, the Euclidean algorithm says $\gcd(3648, 1752) = 24$. $\square$

2. (12 points) Let G be a group. Prove,**using some form of induction,** that if a and b are elements of a group G, then $(aba^{-1})^n = ab^na^{-1}$, for all $n \in \mathbb{Z}$.

Proof. Note that if $n = 1$, then we have $(a^{-1}ba)^1 = a^{-1}b^1a,$, i.e. the statement holds trivially for $n = 1$. Note that for $n = 2$, $(a^{-1}ba)^2 = (a^{-1}ba)(a^{-1}ba) = a^{-1}b(aa^{-1})ba = a^{-1}b^2a$. Thus the claim holds for $n = 2$. Suppose the claim holds for n. That is, assume that $(a^{-1}ba)^n = a^{-1}b^na$. Note that $(a^{-1}ba)^{n+1} = (a^{-1}ba)^n(a^{-1}ba)$. Now, by assumption, $(a^{-1}ba)^n = a^{-1}b^na$. Thus,

$$(a^{-1}ba)^{n+1} = (a^{-1}b^na)(a^{-1}ba) = a^{-1}b^n(aa^{-1})ba = a^{-1}b^neba = a^{-1}b^{n+1}a.$$

Thus, by induction, the claim holds for $n \geq 1$.

For $n = 0$, we have $a^{-1}b^0a = a^{-1}ea = e = (a^{-1}ba)^0$. Suppose $n < 0$. Then $-n > 0$, so, by what we showed above, $(a^{-1}ba)^{-n} = a^{-1}b^{-n}a$. Now,

$$(a^{-1}ba)^n = \left(\left(a^{-1}ba\right)^{-n}\right)^{-1} = (a^{-1}b^{-n}a)^{-1}.$$

Now show that $(a^{-1}b^{-n}a)^{-1} = a^{-1}b^na$, and you're done. $\square$

3. (20 points) Show that there is only one way to complete the following Cayley table to form a group:

$\cdot$	a	b	c	d
a	b		d	
b				
c		c	a	
d	c			

(**Hint: Decide which element must be the identity first.**) Is this group abelian, cyclic, neither, or both??

Solution. Let $G = \{a, b, c, d\}$. Let e be the identity of this group. Since $cb = b = ce$, we must have $b = e$. This allows us to fill in the 2nd row and 2nd column:

$\cdot$	a	b	c	d
a	b	a	d	
b	a	b	c	d
c		c	a	
d	c	d		

Now, recall, each of the symbols a, b, c, and d must appear in each row and column (this is because, for a fixed x and y in G there must be a z so tht $xz = y$, namely $z = x^{-1}y$, and similarly a w so that $wx = y$, namely $w = yx^{-1}$). Thus, from the first row, we must have $ad = c$, and in the first column $ca = d$. So now we have

$\cdot$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	a	
d	c	d		

Now, this same reasoning tells us $dc = b = cd$, and finally that $a^2 = d$. Thus, the only way to fill in the table to get a group is

$\cdot$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	a	b
d	c	d	b	a

Now note, from the table $d^2 = a$, and $d^3 = d^2d = ad = c$, and $d^4 = dc = b$, so $G = \{a, b, c, d\} =< d >$ is cyclic, and hence also abelian. $\square$

4. (7 points each) For each of the following groups G, determine whether the given subset H is a subgroup.

(a) $G = U(24)$, and $H = \{1, 5, 7, 11\}$.

(b) $G = GL(2, \mathbb{R})$ and $H = \{A \in G | \det A < 0\}$.

(c) $G = GL(2, \mathbb{R})$ and $H = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} |ac \neq 0 \right\}$.

Solution.

(a) We can apply the finite subgroup test. Note $1 \cdot x = x \cdot 1 = x$, for any x. Also, $U(24)$ is abelian. So $5 \cdot 5 = 1, 5 \cdot 7 = 7 \cdot 5 = 11, 7 \cdot 7 = 1, 7 \cdot 11 = 11 \cdot 7 = 5$, and $11 \cdot 11 = 1$. Since $xy \in H$ for any $x, y \in H$, we have H is a subgroup of G.

(b) Note, the identity I of G is not an element of H, (since $\det I = 1 > 0$). So H is not a subgroup. Alternatively, if $g = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $h = \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}$, then $\det g = -1 < 0$, and $\det h = -2 < 0$, so $g, h, \in H$. But $gh = \begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}$ has determinant 2, so $gh \notin H$. Thus, H is not closed under matrix multiplication, and hence not a subgroup by the two step subgroup test.

(c) Note the identity I is in H so $H \neq \emptyset$, and thus, the subgroup tests apply. Note, if $g = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$, and $h = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix}$, then $gh = \begin{pmatrix} ax & 0 \\ bx + cy & cz \end{pmatrix} \in H$, since $(ac)(xz) \neq 0$. Thus $gh \in H$. Also, $g^{-1} = \frac{1}{ac} \begin{pmatrix} c & 0 \\ -b & a \end{pmatrix} \in H$. Thus, by the two step test, H is a subgroup of G. $\square$

5. (10 points) Let G be a group and H a subgroup of G. Let

$$C(H) = \{x \in G | xh = hx, \text{ for all } h \in H\}.$$

Show $C(H)$ is a subgroup of G.

Proof. If e is the identity of th group G, then, for any $h \in H$, we have $eh = h = he$, so $e \in C(H)$. Thus $C(H) \neq \emptyset$. Now, if $a, b \in C(H)$, then for any $h \in H$, we have $ah = ha$, and $bh = hb$. Thus, $(ab)h = a(bh) = a(hb) = (ah)b = (ha)b = h(ab)$. Thus $ab \in C(H)$. So, $C(H)$ is closed under the group operation in G. Also note since $ah = ha$, we have $a^{-1}(ah)a^{-1} = a^{-1}(ha)a^{-1}$, or $ha^{-1} = a^{-1}h$, so $a^{-1} \in C(H)$. Therefore, $C(H)$ is closed under inversion. Thus, by the two step subgroup test, we have $C(H)$ is a subgroup of G. $\square$

6. (9 points) Let D_n be the dihedral group of order $2n$, and suppose $F, R \in D_n$ with F a reflection and R a rotation. Prove $RFR = F$.

Proof. We know that RF is a reflection, and hence its own inverse, i.e., $(RF)^{-1} = RF$. On the other hand, $(RF)^{-1} = F^{-1}R^{-1} = FR^{-1}$. Thus, $RF = FR^{-1}$, and so $RFR = F$. $\square$

7. True/False (5 points each) Determine wheteher each of the follwoing statements is true or false. If true, give a proof. If false, give a concrete counterexample.

(a) If G is a group and $ab = ba$ for some $a, b \in G$ then G is abelian.
(b) If $a = b \bmod n$ and $a = c \bmod n$, then $b = c \bmod n$.
(c) If G is a group for which $x^2 = e$ for all $x \in G$, then G is abelian.
(d) $U(20)$ is a cyclic group.

Solution.

(a) **False.** For example, $G = D_4$ is non-abelian. Bust some elements commute, e.g., $R_0 D = D = DR_0$.

(b) **True.** Recall $x = y \bmod n$ if and only if $n|(y-x)$. So if $n|(a-b)$ and $n|(a-c)$, we have $(a-b) = kn$ and $(a-c) = mn$, so $(b-c) = (a-c) - (a-b) = mn - kn = (m-k)n$. So $n|(b-c)$, and $b = c \bmod n$.

(c) **True.** We note since $x^2 = e$ for all $x \in G$, we have $x = x^{-1}$, for all $x \in G$. Now, if $x, y \in G$, we have $(xy)^{-1} = xy$,or $y^{-1}x^{-1} = yx = xy$, so G is abelian.

(d) The cyclic subgroups of $U(20)$ are $< 1 >= \{1\}, < 3 >= \{1, 3, 9, 7\} =< 7 >$, $< 9 >= \{1, 9\}, < 11 >= \{1, 11\}, < 13 >= \{1, 13, 9, 17\} =< 17 >$, and $< 19 >= \{1, 19\}$, none of which are $U(20)$, so $U(20)$ is not cyclic. $\square$