UNIVERSITY OF PENNSYLVANIA DEPARTMENT OF MATHEMATICS
Math 370 Algebra Fall Semester 2006
Prof. Gerstenhaber, T.A. Asher Auel

Homework #4 Solutions (due 10/3/06)
Chapter 2 Groups

Recall: Let G be a group. For $x \in G$ let $\#x$ denote the order of x in G. The central mantra of orders (proved in the previous solution set) is:

$$\boxed{x^n = e \quad \Leftrightarrow \quad \#x \mid n}$$

and the order $\#x$ of x is the smallest such positive integer n.

Definitions/Facts: About $\gcd$ and lcm. For positive integers n and m define their *greatest common divisor* to be the positive integer $\gcd(n, m)$ characterized by the following equivalent conditions:

i) any common divisor of n and m is a divisor of $\gcd(n, m)$, i.e. $a|n$ and $a|m \Rightarrow a|\gcd(n, m)$,
ii) $\gcd(n, m)$ is the smallest positive integer that can be written in the form $kn+lm$ for $k, l \in \mathbb{Z}$,
iii) writing $n = p_1^{e_1} \cdots p_r^{e_r}$ and $m = p_1^{f_1} \cdots p_r^{f_r}$ as a product of powers of distinct prime numbers $p_1, \dots, p_r$ with nonnegative exponents $e_1, \dots, e_r, f_1, \dots, f_r \geq 0$, then we have that $\gcd(n, m) = p_1^{g_1} \cdots p_r^{g_r}$ where $g_i = \min\{e_i, f_i\}$ for $i = 1, \dots, r$.

For positive integers n and m define their *least common multiple* to be the positive integer $\operatorname{lcm}(n, m)$ characterized by the following equivalent conditions:

i) any common multiple of n and m is a multiple of $\operatorname{lcm}(n, m)$, i.e. $n|b$ and $m|b \Rightarrow \operatorname{lcm}(n, m)|b$,
ii) $\operatorname{lcm}(n, m)$ is the smallest positive integer that can be written simultaneously in the form kn and lm for $k, l \geq 1$, note that in this case $\frac{l}{k}$ is the "reduced fraction" of $\frac{n}{m}$,
iii) writing $n = p_1^{e_1} \cdots p_r^{e_r}$ and $m = p_1^{f_1} \cdots p_r^{f_r}$ as a product of powers of distinct prime numbers $p_1, \dots, p_r$ with nonnegative exponents $e_1, \dots, e_r, f_1, \dots, f_r \geq 0$, then we have that $\gcd(n, m) = p_1^{g_1} \cdots p_r^{g_r}$ where $g_i = \max\{e_i, f_i\}$ for $i = 1, \dots, r$.

The $\gcd$ and lcm have the following useful properties:

- $\gcd(n, m) \cdot \operatorname{lcm}(n, m) = n \cdot m$,
- n and m are *relatively prime* $\Leftrightarrow$ $\gcd(n, m) = 1$ $\Leftrightarrow$ $\operatorname{lcm}(n, m) = nm$,
- $n|m$ $\Leftrightarrow$ $\gcd(n, m) = n$ $\Leftrightarrow$ $\operatorname{lcm}(n, m) = m$

2.10 Let G be a group.

a) **Claim:** If $\#x = rs$ for some $r, s \geq 1$ then $\#x^r = s$.

Proof. First note that $(x^r)^s = x^{rs} = e$ since $\#x = rs$ so $\#x^r \mid s$. Furthermore, for $0 < k < |s|$ we have that $0 < rk < r|s|$, so that $(x^r)^k = x^{rk} \neq e$. So $\#x^r$ really is s. □

b) **Claim:** If $\#x = n$ then

$$\#x^r = \frac{n}{\gcd(n, r)} = \frac{\operatorname{lcm}(n, r)}{r}.$$

for any $r \geq 1$.

Proof. For $l \geq 1$ we have that

$$(x^r)^l = x^{rl} = e \;\Leftrightarrow\; n|rl \;\Leftrightarrow\; nk = rl \text{ for some } k \geq 1,$$

and if $l = \#x^r$, i.e. the least possible such l, then $nk = rl = \operatorname{lcm}(n, m)$ is then the least common multiple of n and m. But then

$$\#x^r = l = \frac{nk}{r} = \frac{\operatorname{lcm}(n, m)}{r} = \frac{n}{\gcd(n, m)},$$

where the final equality comes from the formula relating $\gcd$ and lcm. □

2.11 Let $a, b \in G$ be elements of a group, and suppose ab is of finite order n. Then

$$(ab)^n = e \;\Leftrightarrow\; a^{-1}(ab)^n a = a^{-1}a = e \;\Leftrightarrow\; (a^{-1}aba)^n = e \;\Leftrightarrow\; (ba)^n = e,$$

where the second equivalence is exercise 3.4. Thus ba has finite order and $\#ba|n$. Now similarly, for $0 < k < n$ we have

$$(ab)^k \neq e \;\Leftrightarrow\; a^{-1}(ab)^k a \neq a^{-1}a = e \;\Leftrightarrow\; (a^{-1}aba)^k \neq e \;\Leftrightarrow\; (ba)^k \neq e,$$

and so indeed the order of ba is n. This also proves that if ab has infinite order, then so does ba.

2.16 Let G be a cyclic group of order n. Then an element $x \in G$ generates G if and only if $\#x = n$. Now fixing a generator $x \in G$, we have $G = \{e, x, x^2, \ldots, x^{n-1}\}$, and so in view of the formula from exercise 2.10b, we see that

$$\begin{aligned} x^r \text{ also generates } G \quad &\Leftrightarrow \quad \#x^r = n \;\Leftrightarrow\; \frac{n}{\gcd(n,r)} = n \;\Leftrightarrow\; \gcd(n,r) = 1 \\ &\Leftrightarrow \quad r \text{ is relatively prime to } n. \end{aligned}$$

Thus in asking the question "how many of its elements generate G?" we are forced to deal with the following number

$$\begin{aligned} \varphi(n) &= |\{r : 0 < r < n \text{ and } \gcd(n,r) = 1\}| \\ &= \text{the number of numbers from } 1, 2, \ldots, n-1 \text{ that are relatively prime to } n, \end{aligned}$$

usually called the *Euler phi-function* of n.

a) For $n = 6$, we see that of the numbers $1, 2, 3, 4, 5$, only $1, 5$ are relatively prime to 6, so $\varphi(6) = 2$. For completeness I'll compute the cyclic subgroups generated by every element:

$$\begin{aligned} < e > &= \{e\} \\ < x > &= \{e, x, x^2, x^3, x^4, x^5\} \\ < x^2 > &= \{e, x^2, x^4\} \\ < x^3 > &= \{e, x^3\} \\ < x^4 > &= \{e, x^4, x^2\} \\ < x^5 > &= \{e, x^5, x^4, x^3, x^2, x\} \end{aligned}$$

and we see that only x and x^5 are generators.

b) Why don't we make a little table for $n = 2, \ldots, 12$:

n	numbers $1, \ldots, n-1$	relatively prime to n	$\varphi(n)$
2	1	1	1
3	$1, 2$	$1, 2$	2
4	$1, 2, 3$	$1, 3$	2
5	$1, 2, 3, 4$	$1, 2, 3, 4$	4
6	$1, 2, 3, 4, 5$	$1, 5$	2
7	$1, 2, 3, 4, 5, 6$	$1, 2, 3, 4, 5, 6$	6
8	$1, 2, 3, 4, 5, 6, 7$	$1, 3, 5, 7$	4
9	$1, 2, 3, 4, 5, 6, 7, 8$	$1, 2, 4, 5, 7, 8$	6
10	$1, 2, 3, 4, 5, 6, 7, 8, 9$	$1, 3, 7, 9$	4
11	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$	10
12	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$	$1, 5, 7, 11$	4

c) As already noted, the number of elements that generate a cyclic group of order n is $\varphi(n)$.

2.20a Claim: Let $x, y \in G$ be commuting elements of a group and let $\#x = n$ and $\#y = m$. Then all we can say is that

$$\#xy \mid \operatorname{lcm}(n, m).$$

Proof. First, note that since x and y commute, $(xy)^l = x^l y^l$ for all $l \in \mathbb{Z}$. Now let $l = \mathrm{lcm}(n, m)$. Then since $n \mid l$ and $m \mid l$, i.e. there exist $a, b \geq 1$ such that $l = an = bm$, we know that

$$(xy)^l = x^l y^l = (x^n)^a (y^m)^b = e^a e^b = e,$$

thus $\#xy \mid \mathrm{lcm}(n, m)$. $\square$

Note: The order $\#xy$ is difficult to relate exactly to the individual orders $\#x$ and $\#y$. For example, let $G =< a >$ be a cyclic group of order 6, then the following table displays the range of possible behavior:

x	y	xy	$\#x$	$\#y$	$\#xy$	$\mathrm{lcm}(\#x, \#y)$	"="?
a	a	a^2	6	6	3	6	no
a	a^2	a^3	6	3	2	6	no
a	a^3	a^4	6	2	3	6	no
a	a^4	a^5	6	3	6	6	yes
a	a^5	e	6	6	1	6	no
a^2	a^2	a^4	3	3	3	3	yes
a^2	a^3	a^5	3	2	6	6	yes
a^2	a^4	e	3	3	1	3	no
a^2	a^5	a	3	6	6	6	yes
a^3	a^3	e	2	2	1	2	no
a^3	a^4	a	2	3	6	6	yes
a^3	a^5	a^2	2	6	3	6	no
a^4	a^4	a^2	3	3	3	3	yes
a^4	a^5	a^3	3	6	2	6	no
a^5	a^5	a^4	6	6	3	6	no

3.11 Claim: Let G be a group. Then the set $\mathrm{Aut}(G)$ of group automorphisms of G forms a group under composition.

Proof. We need to verify the group axioms for the set $\mathrm{Aut}(G)$ under the operation of composition.

First, we show that $\mathrm{Aut}(G)$ is closed under composition. We'll need the following:

Lemma: Let $\varphi, \psi : G \to G$ be maps. Then

i) if φ and ψ are injective then so is $\varphi \circ \psi$,
ii) if φ and ψ are surjective then so is $\varphi \circ \psi$,
iii) if φ and ψ are bijective then so is $\varphi \circ \psi$,
iv) if φ and ψ are group homomorphisms then so is $\varphi \circ \psi$,
v) if φ and ψ are group isomorphisms then so is $\varphi \circ \psi$.

Proof. To *i)*, let $x, y \in G$, then

$$(\varphi \circ \psi)(x) = (\varphi \circ \psi)(y) \quad \Rightarrow \quad \varphi(\psi(x)) = \varphi(\psi(y)) \quad \Rightarrow \quad \psi(x) = \psi(y) \quad \Rightarrow \quad x = y,$$

where the second and third implications follow if φ and ψ are injective, respectively. Thus $\varphi \circ \phi$ is injective.

To *ii)*, let $x \in G$, then since ψ is surjective, there exists $x' \in G$ such that $\psi(x') = x$. Since φ is surjective, there exists $x'' \in G$ such that $\varphi(x'') = x'$. But then

$$(\varphi \circ \psi)(x'') = \varphi(\psi(x'')) = \varphi(x') = x,$$

so we see that $\varphi \circ \psi$ is surjective.

To *iii)*, combine *i)* and *ii)*.

To *iv)*, let $x, y \in G$, then

$$(\varphi \circ \psi)(xy) = \varphi(\psi(xy)) = \varphi(\psi(x)\psi(y)) = \varphi(\psi(x))\ \varphi(\psi(y)) = (\varphi \circ \psi)(x)\ (\varphi \circ \psi)(y),$$

if both φ and ψ are homomorphisms. So we indeed see that $\varphi \circ \psi$ is a homomorphism.

To *v)*, combine *iii)* and *iv)*. $\square$

Thus we see that for automorphisms $\varphi, \psi \in \mathrm{Aut}(G)$ the composition $\varphi \circ \psi \in \mathrm{Aut}(G)$ is again an automorphism, so $\mathrm{Aut}(G)$ is closed under composition.

Next we quickly verify that composition is associative. For $\varphi, \psi, \lambda \in \mathrm{Aut}(G)$ and for $x \in G$ we have

$$((\varphi \circ \psi) \circ \lambda)(x) = (\varphi \circ \psi)(\lambda(x)) = \varphi(\psi(\lambda(x))) = \varphi((\psi \circ \lambda)(x)) = (\varphi \circ (\psi \circ \lambda))(x),$$

so that indeed $(\varphi \circ \psi) \circ \lambda = \varphi \circ (\psi \circ \lambda)$, so composition is associative.

Next, we find an identity. Let $\mathrm{id} : G \to G$ be the identity function, which is clearly an automorphism. For $\varphi \in \mathrm{Aut}(G)$ and for $x \in G$ note that

$$(\varphi \circ \mathrm{id})(x) = \varphi(\mathrm{id}(x)) = \varphi(x), \quad \text{and} \quad (\mathrm{id} \circ \varphi)(x) = \mathrm{id}(\varphi(x)) = \varphi(x),$$

so that indeed $\varphi \circ \mathrm{id} = \varphi$ and $\mathrm{id} \circ \varphi = \varphi$. Thus $\mathrm{id} \in \mathrm{Aut}(G)$ is indeed an identity.

Finally, we check that inverses exist, but we already did this in exercise 3.5. For an isomorphism $\varphi : G \to G$, we previously showed that the inverse function $\varphi^{-1} : G \to G$ is again an isomorphism, and by definition satisfies $\varphi \circ \varphi^{-1} = \mathrm{id}$ and $\varphi^{-1} \circ \varphi = \mathrm{id}$, so φ^{-1} is an inverse of φ for composition. So indeed, $\mathrm{Aut}(G)$ has inverses. We've finished showing that $\mathrm{Aut}(G)$ is a group under composition. □

3.14 Determining some automorphism groups.

a) We're already show that $\mathrm{Aut}(\mathbb{Z}) = \{\pm \mathrm{id}\}$ in exercise 4.4.

b) Since $\mathbb{Z}/10\mathbb{Z}$ is a cyclic group generated by 1, any homomorphism $\varphi : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ is completely defined by the image of 1. Now we also know by exercise 3.6a that if φ is an isomorphism, then it preserves orders of elements, i.e. $\#\varphi(x) = \#x$ for all $x \in \mathbb{Z}/10\mathbb{Z}$. In particular, a generator must be sent to a generator. Now in exercise 2.16b, we already know that the only elements in $\mathbb{Z}/10\mathbb{Z}$ that generate are $1, 3, 7, 9$. It's also easy to see that each of the four choices of where to send 1 gives an automorphism of $\mathbb{Z}/10\mathbb{Z}$, so we'll label them accordingly:

$$\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z}) = \{\varphi_1, \varphi_3, \varphi_7, \varphi_9\}.$$

Note that $\varphi_1 = \mathrm{id}$. Now we compute the group structure on $\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$. For example, for $x \in \mathbb{Z}/10\mathbb{Z}$, we have

$$(\varphi_3 \circ \varphi_7)(x) = \varphi_3(\varphi_7(x)) = \varphi_3(7x) = 3(7x) = 21x = x,$$

so we find that $\varphi_3 \circ \varphi_7 = \mathrm{id} = \varphi_1$. Continuing like this we can calculate the multiplication table for $\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$:

$\circ$	φ_1	φ_3	φ_7	φ_9
φ_1	φ_1	φ_3	φ_7	φ_9
φ_3	φ_3	φ_9	φ_1	φ_7
φ_7	φ_7	φ_1	φ_9	φ_3
φ_9	φ_9	φ_7	φ_3	φ_1

Notice that we have a nice group isomorphism

$$\begin{array}{ccc} (\mathbb{Z}/10\mathbb{Z})^\times & \xrightarrow{\sim} & \mathrm{Aut}(\mathbb{Z}/10\mathbb{Z}) \\ a & \mapsto & \varphi_a \end{array}$$

We also see that both $\varphi_3, \varphi_7 \in \mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$ have order 4, i.e. they each generate. This shows that $\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$ is cyclic, and we can construct two different isomorphisms

$$\begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Aut}(\mathbb{Z}/10\mathbb{Z}) \\ 0 & \mapsto & \varphi_1 \\ 1 & \mapsto & \varphi_3 \\ 2 & \mapsto & \varphi_9 \\ 3 & \mapsto & \varphi_7 \end{array} \qquad \begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Aut}(\mathbb{Z}/10\mathbb{Z}) \\ 0 & \mapsto & \varphi_1 \\ 1 & \mapsto & \varphi_7 \\ 2 & \mapsto & \varphi_9 \\ 3 & \mapsto & \varphi_3 \end{array}$$

neither of which seems particularly appealing, but just illustrates the two ways we can force ourselves to think of $\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$ as a cyclic group of order 4.

c) Writing $S_3 =< s,t : s^2 = t^3 = e, ts = st^2 >$, we see that the symmetric group S_3 is generated by elements s, t or orders $2, 3$, respectively, subject to a further relation. Any automorphism $\varphi : S_3 \to S_3$ is determined by the images of s, t, and as before, must preserve the orders of elements. Now S_3 has three elements s, st, st^2 of order 2, and two elements t, t^2 of order 3. So any automorphism must take s to one of s, st, s^2 and t to one of t, t^2. There are only six conceivable ways of doing this:

$$\begin{array}{rcl} s & \to & s \\ t & \to & t \end{array} \qquad \begin{array}{rcl} s & \to & st \\ t & \to & t \end{array} \qquad \begin{array}{rcl} s & \to & st^2 \\ t & \to & t \end{array}$$

$$\begin{array}{rcl} s & \to & s \\ t & \to & t^2 \end{array} \qquad \begin{array}{rcl} s & \to & st \\ t & \to & t^2 \end{array} \qquad \begin{array}{rcl} s & \to & st^2 \\ t & \to & t^2 \end{array}$$

One now checks that each of these in fact does give an automorphism of S_3. Thus $\mathrm{Aut}(S_3)$ just consists of these six elements. We would further like to know the structure of $\mathrm{Aut}(S_3)$. One way to do this is to know that there are only two isomorphism classes of groups of order six, namely cyclic of order six and S_3. We then just need to check if two of these automorphisms don't commute. In fact $\mathrm{Aut}(S_3) \cong S_3$. Another way to see this is to note that the center $Z(S_3)$ is trivial, so that conjugation by each element of S_3 gives a different automorphism, since there are already six of these, these fill up all of $\mathrm{Aut}(S_3)$. Thus we have the nice isomorphism

$$\begin{array}{rcl} \mathrm{ad} : S_3 & \xrightarrow{\sim} & \mathrm{Aut}(S_3) \\ x & \mapsto & \mathrm{ad}_x : y \mapsto xyx^{-1}, \end{array}$$

in the notation from lab.

d) The analysis of $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ follows exactly the same way as for $\mathrm{Aut}(\mathbb{Z}/10\mathbb{Z})$ in part b). In the end, we find that $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) = \{\varphi_1, \varphi_3, \varphi_5, \varphi_7\}$ and we have the nice isomorphism

$$\begin{array}{rcl} (\mathbb{Z}/8\mathbb{Z})^\times & \xrightarrow{\sim} & \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \\ a & \mapsto & \varphi_a \end{array}$$

Incidentally, we check that each element of $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ has order two, so that $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

e) Is the automorphism group of a cyclic group necessarily cyclic? Well, no, see part d).

f) Is the automorphism group of an abelian group necessarily abelian? Well, no either. Take for example the abelian group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Each permutation of the entries gives a group automorphism, and as we know, permutations of three objects don't usually commute. In particular, we see that $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ has a subgroup isomorphic to the permutation group S_3. Do you think that is the whole automorphism group?

4.8 Subgroups of groups.

a) The subgroups of $S_3 =< s,t : s^2 = t^3 = e, ts = st^2 >$ are:

$$\{e\},\ \{e,s\},\ \{e,st\},\ \{e,st^2\},\ \{e,t,t^2\},\ S_3,$$

and $\{e\}, \{e,t,t^2\}, S_3$ are normal subgroups.

b) The subgroups of the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, and $ki = j$, are:

$$\{1\},\ \{\pm 1\},\ \{\pm 1, \pm i\},\ \{\pm 1, \pm j\},\ \{\pm 1, \pm k\},\ Q,$$

and every subgroup is normal.

4.9b Claim: Let $\psi : G \to G'$ and $\varphi : G' \to G''$ be homomorphisms of groups. Then

$$\ker(\varphi \circ \psi) = \psi^{-1}(\ker(\varphi)) \subset G.$$

Proof. Obvious. □