MATH 430, MODERN ALGEBRA, SPRING 2011

SOLUTIONS TO THE SELECTED PROBLEMS, PROBLEM SETS 1-3

1. Exercises from the book:

- **4. 32**: If $a \in G$, then since $a * a = e$, $a = a^{-1}$. Now for $a, b \in G$, we have $(a * b) * (a * b) = e$, so $a * (b * a) * b = e$, so $(b * a) * b = a^{-1}$, so $b * a = a^{-1} * b^{-1} = a * b$.

- **5. 46**: If G is an arbitrary group and $a \in G$, then the subgroup generated by a is equal to the subgroup generated by a^{-1}:

$$< a >= \{a^n |\ n \in \mathbf{Z}\} = \{a^{-n} |\ n \in \mathbf{Z}\} =< a^{-1} > .$$

In particular if $< a >= G$, then $< a^{-1} >= G$, so the inverse of a generator of a cyclic group is also a generator.

Now if a cyclic group G has only one generator a, then since a^{-1} is also a generator, $a = a^{-1}$, so $a^2 = e$, so a has order at most 2. If it has order 2, then $G = \{e, a\}$. If it has order 1, then $a = e$ and $G = \{e\}$.

- **6. 53**: Let $G = \{e, a, \ldots, a^{n-1}\}$. Let m be a positive divisors of n. If $0 \leq i \leq n-1$, then

$$(a^i)^m = e \Longleftrightarrow a^{im} = e \Longleftrightarrow im \text{ is a multiple of } n.$$

Write $n = mq$. Then

$$im \text{ is a multiple of } n \Longleftrightarrow i \text{ is a multiple of } q.$$

So $i = 0, q, 2q, \ldots, (m-1)q$, and therefore there are m possibilities for i.

- **9. 39**: Let $\sigma = (1\ 2\ \ldots\ n)$. We show that

$$\sigma^r\ (1\ 2)\ \sigma^{n-r} = \begin{cases} (r+1\ \ r+2) & \text{if} \quad 0 \leq r \leq n-2 \\ (n\ \ 1) & \text{if} \quad r = n-1. \end{cases}$$

First notice that σ^n is the identity permutation, and also

$$\sigma^{n-1} = \sigma^{-1} = (n\ \ n-1\ \ \ldots\ \ 2\ \ 1).$$

We consider the two cases separately:

(a) Assume first that $0 \leq r \leq n-2$. Then there are 4 possibilities:

* If $1 \leq i \leq r$, then $3 \leq n - r + i \leq n$. So σ^{n-r} sends i to $i + n - r$, and $n - r + i \neq 1, 2$, so $\sigma^r(1\ 2)\sigma^{n-r}$ sends i to i.
* If $i = r + 1$, then σ^{n-r} sends $r + 1$ to 1, and $(1\ 2)$ sends 1 to 2, and σ^r sends 2 to $r + 2$.
* If $i = r + 2$, then σ^{n-r} sends $r + 2$ to 2, and $(1\ 2)$ sends 2 to 1, and σ^r sends 1 to $r + 1$.
* If $r + 3 \leq i \leq n$, then σ^{n-r} sends i to $i - r$, and $i - 2 \geq 3$, and σ^r sends $i - r$ to i, so $\sigma^r(1\ 2)\sigma^{n-r}$ sends i to i.

(b) Now assume that $r = n - 1$. Then $\sigma^r(1\ 2)\sigma^{n-r} = \sigma^{n-1}(1\ \ 2)\sigma =$

$$(n\ \ n-1\ \ \ldots\ \ 2\ \ 1)(1\ \ 2)(1\ \ 2\ \ \ldots\ \ n)$$

and it is easy to show that this permutation is simply $(n\ \ 1)$.

To prove the statement of the problem, notice that if $1 \leq a, b, c \leq n$, then

$$(a\ c) = (a\ b)\ (b\ c)\ (a\ b)$$

So if $1 \leq i < j \leq n$, we have

$$(i\ \ j) = (i\ \ i+1)\ldots(j-2\ j-1)(j-1\ j)(j-2\ j-1)\ldots(i\ i+1).$$

Therefore, every transposition is in subgroup generated by σ and (12). Since every permutation can be written as a product of transpositions, we conclude that the subgroup generated by σ and (12) is the whole group.

- **10. 38**: Suppose that there are n distinct cosets of H in G: $a_1H, \ldots, a_nH$. So for every $a \in G$, there is a_i such that $aH = a_iH$, and $a_iH \neq a_jH$ if $i \neq j$. And suppose that there are m distinct cosets for K in H: $b_1K, \ldots b_mK$ where $b_1, \ldots, b_m \in H$ (Here we are considering H itself as a group, and K is a subgroup of H.)

  We show that the cosets

$$a_ib_jK \quad 1 \leq i \leq n, 1 \leq j \leq m$$

are distinct and that every coset of K in G is equal to one of them. First, if $a_ib_jK = a_kb_lK$, then $(a_ib_j)^{-1}a_kb_l \in K$, so $b_j^{-1}a_i^{-1}a_kb_l \in K$, but $b_j, b_l \in K$, so $a_i^{-1}a_k \in K \subset H$. So $a_i^{-1}a_k \in H$, so $a_iH = a_kH$, so $i = k$. Since $a_ib_jK = a_kb_lK$ and $a_i = a_k$, we cancel a_i and a_k to get $b_jK = b_lK$, so $j = l$.

  Now we show for $c \in G$, there are a_i and b_j such that

$$cK = a_ib_jK.$$

There is $1 \leq i \leq n$ such that $cH = a_iH$, so $c^{-1}a_i \in H$, so $(a_i)^{-1}c \in H$. Therefore, there is $1 \leq j \leq m$ such that $(a_i)^{-1}cK = b_jK$. Multiplying both sides by a_i, we get $cK = a_ib_jK$.

- **10. 46**: Let G be a cyclic group of order n,
$$G = \{e, a, \ldots, a^{n-1}\}.$$
(you can take G to be $\mathbf{Z}_n$.) We count the set S of all pairs (H, a^i) such that $0 \leq i \leq n-1$, and $H =< a^i >$, the subgroup of G generated by a^i. The set S has clearly n elements: we have n choices for the second component, and the first component is uniquely determined once we have the second component.

  Now we count the elements of S in a difference way. We first choose H and then the second component. Since H is a subgroup of G, $|H|$ is factor of n. We know that G has exactly one subgroup for every positive divisor of n. So let d be a divisor of n, and let H be the subgroup of order d. How many elements of G generate H?, that is to ask how many generators does H have? Since H itself is cyclic of order d, the number of its generators is exactly $\phi(d)$ (this is what proved in class). So the number of elements of S is exactly
$$\sum_{1 \leq d \text{ a divisor of } n} \phi(d).$$

2. Give an example of a finite group G and two elements $a, b \in G$ such that $(ab)^2$ is not equal to $(a^2)(b^2)$.

- **Solution:** In S_3, let $\tau_1 = (1\ 3), \tau_2 = (1\ 2)$. Then $\tau_1^2 = \tau_2^2 = e$, but $\tau_1\ \tau_2 = (1\ 2\ 3)$ and $(\tau_1\ \tau_2)^2 = (1\ 3\ 2)$

3. Show that the greatest common divisor (gcd) of any two integers a and b can be written as a linear combination of a and b
$$\gcd(a, b) = xa + yb, \qquad x, y \in \mathbf{Z}.$$

- **Solution:** Let S be the set of *positive* integers which are of the form $xa+yb$ for some $x, y \in \mathbf{Z}$. Since $a = 1*a+0*b$ and $-a = (-1)*a+0*b$, and since one of a or $-a$ is positive, S is non-empty. Let c be the smallest element of S. We show $c = \gcd(a, b)$. To show this, we show (1): c divides both a and b, (2) c divides every common divisor of a and b. Since there are integers x and y such that
$$c = xa + yb$$
the second assertion is clear. To prove the first assertion, we use the division algorithm to write
$$a = q\ c + r \quad 0 \leq r \leq c.$$

Then

$$r = a - qc = a - q(xa + yb) = (1 - qx)a + (-qy)b.$$

If $r \neq 0$, then it would be an element of S smaller than c which is not possible, so $r = 0$. Similarly, the remainder of b divided by c is zero.

4. The *order* of an element g in a group G is the smallest positive integer m such that $g^m = e$. If there is no such m, then g is said to be *of infinite order*.

(a) Show that for any two elements $a, b \in G$, ab and ba have the same order.
(b) Gives an example of a group G and two elements a and b of finite order such that ab has infinite order. (Hint: you can find an example using matrices with multiplication)

- **Solution:** (a): It is enough to show that if $(ab)^n = e$ for an integer $n \geq 1$, then $(ba)^n = e$ (This shows in particular that ba is of infinite order if and only if ab has infinite order) Assume $(ab)^n = e$. Then

$$(ab)^{n-1} = (ab)^{-1} = b^{-1}a^{-1}$$

So

$$(ba)^n = (ba)\dots(ba) = b(ab)^{n-1}a = b(b^{-1}a^{-1})a = e.$$

(b) Let $A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ and $B = A^t = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$. Then $A^2 = B^2 = I$, so they both have order 2 in $\mathrm{GL}(2, \mathbf{R})$. We have

$$AB = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}.$$

You can now use linear algebra to find powers of AB and show it is never identity. You can also argue as follows: Induction shows that $(AB)^k$ if of the form

$$(AB)^k = \begin{pmatrix} a_k + b_k & -a_k \\ -a_k & b_k \end{pmatrix}, \quad \text{for some} \quad a_k, b_k \geq 1.$$

So the first entry of every positive power of AB is at least 2.
(I found the two matrices by trial and error. If you have other methods, let me know)

2. Prove that A_4 (the alternating group on 4 letters) does not have a subgroup of order 6.

- **Solution**: Assume to the contrary that there is a subgroup H in A_4 whose order is 6. Then H has two left cosets in A_4. Let $\sigma \in A_4$.

  If $\sigma \in H$, then $\sigma^2 \in H$.

  If $\sigma \notin H$, then σH and H are not equal, and hence there are disjoint, and they are the two left cosets of H in A_4. So any left cosets should be equal to one of them. In particular, $\sigma^2 H = H$ or $\sigma^2 H = \sigma H$. The second case is not possible, since then $(\sigma^2)^{-1}\sigma \in H$, so $\sigma \in H$. Therefore the first case happens, and so $\sigma^2 \in H$.

  We have shown that if σ is an arbitrary element of A_4, then $\sigma^2 \in H$. Now if you compute the set

  $$S = \{\sigma^2 | \sigma \in A_4\}$$

  you see that it has more than 6 elements and so it cannot be a subset of H.