MATH 375.9

Class 9: Selected Answers

1. The **Klein Four-Group** is the following set of 4 matrices. It is denoted by V_4.

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad b = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \qquad c = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

a) Fill in a Cayley Table for these matrices.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

b) Prove that V_4 is a subgroup of $GL(\mathbf{R}, 2)$. **Solution:** By the **Finite Subgrpoup Test**, since V_4 is closed (see table) it is a subgroup.

c) Normally matrix multiplication is not commutative. But is this subgroup commutative? **Solution:** Yes, the table is symmetric.

d) Is V_4 cyclic? Explain. **Solution:** No, every non-identity element has order 2 (note the the e's on the diagonal). To be cyclic, there would have to be an element of order 4.

2. a) Find $\gcd(624, 500)$. **Solution:** Using Katie's applet, I get $\gcd(624, 500) = 4$.

b) Express the gcd as a linear combination of 624 and 500. **Solution:** Again with her applet $4 = 5 \cdot 500 - 4 \cdot 624$.

c) Find $|a^{500}|$ if $|a| = 624$. **Solution:** From Sam's Theorem,

$$|a^{500}| = \frac{624}{\gcd(624, 500)} = \frac{624}{4} = 156.$$

d) Find $|500|$ in $\mathbf{Z}_{624}$. **Solution:** Same as above since $|1| = 624$.

3. Gallian page 79 #8 (a). **Solution:** From Sam's Theorem, $|a^3| = \frac{15}{\gcd(3,15)} = \frac{15}{3} = 5$. The others are the same: $|a^6| = |a^9| = |a^{12}| = 5$, since the gcd with 15 is 3 in each case.

4. Let G be a finite group. Let p be a prime. Show that if $x \neq e$ and $x^p = e$, then $|x| = p$. **Solution:** We have shown that if $|a| = n$ and $a^k = e$, then $n \mid k$. Here, if $|x| = n$, since $x^p = e$, so $n \mid p$. Since p is prime either $n = 1$ (this leads to a contadiction since we are given $x \neq e$) or $n = p$. Therefore, $|x| = p$.

5. a) List (describe) all the elements of $< \frac{1}{2} >$ in $(\mathbf{Q}, +)$. **Solution:** Remember to use both positive, 0, and negative multiples: $\{\ldots, -2, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, 2, \ldots\}$.

b) List (describe) all the elements of $< \frac{1}{2} >$ in $(\mathbf{Q}^*, \cdot)$. **Solution:** Remember to use both positive, 0, and negative powers: $\{\ldots, 8, 4, 2, 1, 0, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots\}$.

6. Without doing any computations, explain why both elements in each of the following pairs in $\mathbf{Z}_{30}$ have the same order: $\{2, 28\}$ and $\{8, 22\}$. **Solution:** Because each pair of elements are inverses of each other and inverses have the same order.

7. What is the order of $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $GL(\mathbf{Z}_3, 2)$? The $\mathbf{Z}_3$ means that you do the multiplcation mod 3. **Solution:** Just multiply and reduce mod 3.

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad A^3 = \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix} = I.$$

So $|A| = 3$.

8. D_4 has 7 distinct cyclic subgroups. What are they? Hint: Dig out your table and just see what each element generates! **Solution:** The cyclic subgroups are:

$$< r_0 > = \{r_0\}$$
$$< r_{180} > = \{r_0, r_{180}\}$$
$$< r_{90} > = \{r_0, r_{90}, r_{180}, r_{270}\} =< r_{270} >$$
$$< h > = \{r_0, h\}$$
$$< v > = \{r_0, v\}$$
$$< d > = \{r_0, d\}$$
$$< d' > = \{r_0, d'\}$$

9. If $G =< a >$ is a cyclic group of order p where p is prime, what is the order of a^k where $1 < k < p$? **Solution:** From Sam's Theorem, $|a^k| = \frac{p}{\gcd(k,p)} = \frac{p}{1} = p$. This means that any non-identity element generates G.

10. From the Fundamental Theorem on Cyclic Groups, we know that any subgroup of a cyclic group is also cyclic. We also know that $\mathbf{Z}_n$ is always cyclic since it is generated both by 1 and $n-1$. (Sam's Theorem may be helpful here.)

a) Find the generators and the corresponding elements of all the cyclic subgroups of $\mathbf{Z}_{18}$. **Solution:**

$$< 1 > = \mathbf{Z}_{18} =< 5 >=< 7 >=< 11 >=< 13 >=< 17 >$$
$$< 2 > = \{0, 2, 4, 6, 8, 10, 12, 14, 16\} =< 4 >=< 8 >=< 10 >=< 14 >=< 16 >$$
$$< 3 > = \{0, 3, 6, 9, 12, 15\} =< 9 >=< 15 >$$
$$< 6 > = \{0, 6, 12\} =< 12 >$$
$$< 9 > = \{0, 9\}$$
$$< 0 > = \{0\}$$

b) Find the generators and the corresponding elements of all the cyclic subgroups of $\mathbf{Z}_{25}$. **Solution:**

$$< 5 > = \{0, 5, 10, 15, 20\} =< 10 >=< 15 >=< 20 >$$
$$< 0 > = \{0\}$$

Every other element is relatively prime to 25 and generates all of $\mathbf{Z}_{25}$.

c) Find the generators and the corresponding elements of all the cyclic subgroups of $\mathbf{Z}_{19}$. **Solution:** Every element (other than 0) is relatively prime to 19 and so generates all of $\mathbf{Z}_{19}$.

d) From the exam, you know that U_5 is cyclic. Find the generators and the corresponding elements of all its cyclic subgroups. **Solution:** From the exam $< 2 >=< 3 >= U(5)$. Obiously $< 1 >= \{1\}$, and finally $< 4 >=< 1, 4 >$.