MATH 375.6

Class 6: Selected Answers

1. Gallian page 52 #6. **Solution:** Look at a non-abelian group, say our old friend D_3. Notice that

$$a^{-1}ba \neq b \iff ba \neq ab.$$

In D_3, if a and b are any two reflections, then $ba \neq ab$.

$*$	r_0	r_{120}	r_{240}	a	b	c
r_0	r_0	r_{120}	r_{240}	a	b	c
r_{120}	r_{120}	r_{240}	r_0	b	c	a
r_{240}	r_{240}	r_0	r_{120}	c	a	b
a	a	c	b	r_0	r_{240}	r_{120}
b	b	a	c	r_{120}	r_0	r_{240}
c	c	b	a	r_{240}	r_{120}	r_0

2. Gallian page 52 #8. Prove that $(a^{-1}ba)^n = a^{-1}b^n a$. **Solution:** We will first show that this is true for the non-negative integers by induction. Base case: $n = 0$. Then $(a^{-1}ba)^0 = e$ and we compare this to $a^{-1}b^0a = a^{-1}ea = e$, so the the induction starts. Inductive step: Assume $(a^{-1}ba)^n = a^{-1}b^n a$ and now show $(a^{-1}ba)^{n+1} = a^{-1}b^{n+1}a$. But

$$(a^{-1}ba)^{n+1} = (a^{-1}ba)^n \cdot a^{-1}ba = a^{-1}b^n a \cdot a^{-1}ba = a^{-1}b^n eba = a^{-1}b^{n+1}a.$$

So the result is true for all non-negative integers. Now consider $-n$ where $n \in \mathbf{Z}^+$. Then using the fact that the inverse of a product is the product of the inverses in reverse order,

$$(a^{-1}ba)^{-n} = [a^{-1}ba)^n]^{-1} = [a^{-1}b^n a]^{-1} = a^{-1}(b^n)^{-1}(a^{-1})^{-1} = a^{-1}b^{-n}a.$$

This completes the proof.

3. Gallian page 53 #24. Prove that every Cayley table is a Latin square. **Solution:** Assume not. Assume that in there is an element $a \in G$ so that in the a-row of the table, the same element, say x, appears twice. This means that there are two distinct elements, say $s, t \in G$ such that $as = x$ and $at = x$. But then $as = at$ and by left cancellation, $s = t$. This contradicts that s and t are distinct. So the same element cannot appear twice in any row. A similar argument works for columns and uses right cancellation.

4. Gallian page 53 #26. Prove that if $(ab)^2 = a^2b^2$ in a group G, then $ab = ba$. **Solution:** Finally, an easy one. Just write it out.

$$(ab)^2 = a^2b^2 \iff abab = aabb \iff bab = abb \iff ba = ab$$

where we have used left and right cancellation in the last two steps.

5. Let $H(n)$ denote the set of $n \times n$ *symmetric matrices*. That is,

$$H(n) = \{A \in M_{nn} \mid A^T = A\},$$

where A^T denotes the *transpose* of A. Show that $H(n)$ is a subgroup of M_{nn}, the group of all $n \times n$ matrices under addition. **Solution:** Check closure and invervses. Closure: Let $A, B \in H(n)$. Then $A = A^T$ and $B = B^T$. Show $A + B$ is symmetric.

$$(A + B)^T = A^T + B^T = A + B.$$

So $A + B$ is symmetric. Inverses: Remember the group operation is addition. Then if A is symmetric, we must show $-A$ is symmetric. Now $A^T = A$ and one can pull scalars out of the transpose operation, so

$$(-A)^T = -(A^T) = -(A) = -A.$$

So $-A$ is symmetric and $H(n)$ is a subgroup of M_{nn}

6. **a)** The Heisenberg Group (Heisenberg was a Nobel prize winner in physics) is the set of 3×3 matrices defined by:

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbf{R} \right\}.$$

Show that H is an *subgroup* of $GL(3)$, the group of 3×3 matrices under multiplication. **Solution:** Closure: Let

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 1 & a+d & b+af+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that AB has the correct form to be in H. Inverses: From the product AB above, you can see what the inverse has to be. If we want B to be the inverse, then

$$AB = I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So comparing to the earlier calculation, we need $d = -a$, $f = -c$, and $e = -b + ac$. Alternately, you could get theinverse by the usual reduction process. In either case:

$$A^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that this matrix has the correct form to be in H.

b) In H, find the order of the element

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Solution: From the calculation of AB above, it follows that for any $n \in \mathbf{Z}^+$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So the order is ∞.

c) What is $|H|$? **Solution:** $|H| = \infty$ since it contains at least the infinite number of matrices from the previous part.

7. Find $|8|$ in $\mathbf{Z}_{10}$ and $|8|$ in $U(9)$. **Solution:** $|8| = 5$ in $\mathbf{Z}_{10}$ (since $5 \cdot 8 = 40 \equiv 0 \bmod 10$) and $|8| = 2$ in $U(9)$ (since $8^2 = 64 \equiv 1 \bmod 9$).

8. **a)** Gallian page 65 #4. Prove that any element a and its inverse a^{-1} have the same order. **Solution:** If both elements have infinite order then we are done. So assume that at least one of a or a^{-1} has finite order. Suppose a has order m. Then

$$a^m = e \Rightarrow (a^m)^{-1} = e^{-1} = e.$$

So a^{-1} has finite order. And similarly, if a^{-1} has finite order, so does a (just) reverse the arrow above).

Now we check to see if they are the same order. (The potential problem is that both could have finite order, say 4 and 8, but not the same order.) So assume $|a| = m$, so m is the smallest positive integer such that $a^m = e$. And assume $|a^{-1}| = n$, so n is the smallest positive integer such that $(a^{-1})^n = e$. However, we just saw that $a^m = e \Rightarrow (a^m)^{-1} = e$, so this means that $n \leq m$ since n is the smallest power of a^{-1} to produce e. Of course, $(a^{-1})^n = e \Rightarrow [(a^{-1})^n]^{-1} = a^n = e^{-1} = e$, so now $m \leq n$. Therefore $m = n$.

b) Prove that the number of elements x in a group G such that $x^3 = e$ is odd. **Solution:** Clearly $e^3 = e$. Now if $x \neq e$ then $x^2 = x^{-1}$ because $xx^2 = x^3 = e$. This also means that $x^2 \neq e$ otherwise we would have $x^2 = x^{-1} = e \Rightarrow x = e$. But from part a), both x and x^{-1} have the same order, namely 3. That is, the elements of order 3 come in pairs of the form x and $x^2 = x^{-1}$. So the the number of elements of order 3 is *even*. But we also have that $e^3 = e$, so the total number of elements satisfying the condition is odd.

9. **a)** Gallian page 68 #38 (a) and (c). **Solution:** $|U(3)| = 2$, $|U(4)| = 2$, $|U(12)| = 4$. $|U(4)| = 2$, $|U(5)| = 4$, $|U(12)| = 8$.

b) Conjecture: $|U(m)| \times |U(n)| = |U(mn)|$, at least if $\gcd(m, n) = 1$.

10. This problem combines linear algebra, trigonometry, and abstract algebra. Great! For any real number α, let

$$R_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

a) Show that $R_\alpha \in SL(2, \mathbf{R})$. **Solution:**

$$\det R_\alpha = \cos^2\alpha + \sin^2\alpha = 1 \Rightarrow R_\alpha \in SL(2, \mathbf{R}).$$

b) Show that $R_\alpha R_\beta = R_{\alpha+\beta}$. **Solution:**

$$\begin{aligned} R_\alpha R_\beta &= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \\ &= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \\ &= R_{\alpha+\beta} \end{aligned}$$

c) Show that $R_{-\alpha} = (R_\alpha)^{-1}$. **Solution:** From the last step

$$R_\alpha R_{-\alpha} = R_{\alpha-\alpha} = R_0 = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix} = I$$

d) Show that $\mathbf{Rot} = \{R_\alpha \mid \alpha \in \mathbf{R}\}$ is a subgroup of $SL(2, \mathbf{R})$. **Solution:** Part b) shows closure and part c) shows that the inverse has the right form, so $\mathbf{Rot}$ is a subgroup of $SL(2, \mathbf{R})$.

e) Let's assume that α measures an angle in *radians*. $|R_{\pi/4}| = 8$, since a rotation needs to be a multiple of 2π to be I. $|\mathbf{Rot}| = \infty$ since there are an infinite number of different angles between 0 and 2π.

f) Extra Credit: Go back to your linear algebra text (or use your head) and figure out what R_α represents geometrically. **Solution:** It represents a rotation of the plane of α radians with the origin as the center of rotation.

g) Extra Credit: What is $|R_1|$? Remember the angle is measred in radians! Justify your answer. $|R_1| = \infty$ since 2π is irrational, no integer multiple of 1 will ever be a multiple of 2π.

11. Extra Credit or may be substituted for any one problem in #1–5. Let G be an *abelian* group and let n be a fixed positive integer. Let $H = \{x \in G \mid x^n = e\}$. Is H a subgroup of G? **Solution:** Closure: Let $x, y \in H$. Show $xy \in H$. But $x^n = e$ and $y^n = e$, so since the G is abelian

$$(xy)^n = xy \cdot xy \cdots xy = x^n y^n = ee = e.$$

Inverses: We showed in problem #8 that $x^n = e \iff (x^{-1})^n = e$.

12. Extra Credit: Gallian page 54 #32. Done in class.