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 $c$ while $AE$ multiplies column 1 by $c$. If $EA = AE$, then the nondiagonal entries in row 1 and in column 1 must be zero, etc...

This takes care of the nondiagonal entries. Then one can use the elementary matrices that switch rows to show that the diagonal entries must be equal.

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:

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

There are 52 actual partitions, I think.

3. Chapter 2, Exercise 8.13 (b). (a partition of $\mathbb{Z}$)

Say that we are given a partition of $\mathbb{Z}$ such that if $\Pi_i$ and $\Pi_j$ are elements of the partition, $\Pi_i + \Pi_j \subseteq \Pi_k$ for some $\Pi_k$.

One of the subsets will contain the integer 0. Let’s call that subset $\Pi_0$. By hypothesis, $\Pi_0 + \Pi_0$ is contained in a single subset of the partition, say in $\Pi_1$. Therefore $0 = 0 + 0 \in \Pi_1$. Since $0 + 0 = 0 \in \Pi_0$, $\Pi_1 = \Pi_0$. Then if $a$ and $b$ are in $\Pi_0$, $a + b \in \Pi_0$.

Say that $(-a) \in \Pi_2$. Since $a + (-a) = 0 \in \Pi_0$, $\Pi_0 + \Pi_2 \subseteq \Pi_0$. Then since $0 \in \Pi_0$, $0 + \Pi_2 \subseteq \Pi_0$, and therefore $\Pi_2 = \Pi_0$. This shows that $\Pi_0$ is a subgroup of $\mathbb{Z}^+$.

So, such a partition is the set of cosets of a subgroup.

(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. If $g$ is an element of order 21, then $g^7$ will have order 3. We need to show that it is impossible for each of the 20 elements different from 1 to have order 7.

An element of order 7 will generate a cyclic subgroup $H$ that contains the identity and 6 elements of order 7. Because the intersection of two distinct subgroups $H_1, H_2$ of order 7 is a subgroup whose order divides 7, $H_1 \cap H_2$ must be the subgroup $\{1\}$. Therefore, the number of elements of order 7 is a multiple of 6. Since 20 isn’t a multiple of 6, there must be an element whose order is different from 1 and 7.
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.

As always, the method is 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

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

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 make one of the entries $a$ or $c$ of the first column positive. If $c \neq 0$, 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:** If $a > 0$, we divide $c$ by $a$, 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 $c > 0$, 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 $a > 0$, 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 nonzero entry of the first column must be $1$.

**Step 4:** If the entry 1 of the first column is the “$c$” entry, we add $(row2)$ to $(row1)$ to get $a = c = 1$. Then we subtract $(row1)$ from $(row2)$ to get $a = 1, c = 0$.

**Step 5:** The matrix is now $A = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$. Since $\det A = 1, d = 1$. We subtract $b(row2)$ from $(row1)$ to get the identity matrix.