Homework 1

David Cardozo

February 3, 2015

1. (a) Can you write a surjective homomorphism $\frac{\mathbb{Z}}{24\mathbb{Z}} \to S_3$?
Solution

For this problem we assume $\left(\frac{\mathbb{Z}}{24\mathbb{Z}}, +\right)$ and $(S_3, \circ)$, so suppose that there exist a function that have the following properties:

$$f(\bar{a} + \bar{b}) = f(\bar{a}) \circ f(\bar{b})$$

where $\bar{a}$ is any set of representatives in $\frac{\mathbb{Z}}{24\mathbb{Z}}$ and $\bar{b} \neq \bar{a}$ is also other set of representatives in $\frac{\mathbb{Z}}{24\mathbb{Z}}$ and f is surjective and $f(\bar{a}) \in S_3$. Let us observe that any function, by the property described above, should hold the following:

$$f(\bar{a} + \bar{b}) = f(\bar{a} + \bar{a})$$

but observe that:

$$f(\bar{a})\ circ f(\bar{b}) \neq f(\bar{b}) \circ f(\bar{a})$$

and this in general is not true in s_3 since this group is not abelian, so we conclude that our assumption must be false, respectively that there exist a surjective homomorphism between these two structures. ■

1. (b) How many homomorphism can you write from S_3 to S_4? At least show one or prove that there are none. **Solution**

There are $25 = 1 + 4 \times 3!$, the reason is that, we have one homomorphism mapping everything to the identity, and then we have 4 options to fix a number in the cycle and in the same way of thought there are 3! options to choose any of the permutations of s_3 and s_4 so that the mapping respect the concatenation property.

1. (c) Without doing calculation, explain why there are no elements of order 24 in S_4.

As shown in the book, and in class, For any permutation on S_n the maximum order of any of the elements in s_n is n, so for this particular case we have $n = 4$. The proof is done on the fact that the order depends in the least common multiple of the lengths of the cycles written in disjoint form, so the possible ways to write this are $e, (ab), (ab)(cd), (abc), (abcd)$ a, b, c, d are all different numbers from 1 to 4, thus the orders of these elements are $1, 2, 2$ and 4 so that 4 is the maximum order of s_4

1. (d.) What are the possible orders of elements of S_4 ?

$1, 2, 3, 4$ see previous discussion.

e Show an element of every possible order.

$$\begin{aligned} (1)(2)(3)(4) &\quad \text{Order } 1 \\ (12)(3)(4) &\quad \text{Order } 2 \\ (123)(4) &\quad \text{Order } 3 \\ (1234) &\quad \text{Order } 4 \end{aligned}$$

2. Let F be a field. The Heisenberg group is $H(F) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} |a, b, c \in F \right\}$

2. (a) & (c) Show this is a nonabelian group. And deduce the order of the group.

Let $a, b, c, d, e, f \in F$ and let's take:

$$A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

and:

$$B = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix}$$

and the multiplication of these two matrices is:

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

and:

$$BA = \begin{bmatrix} 1 & a+d & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{bmatrix}$$

and we observe clearly that, in general, the multiplication of these two matrices depends in the order, this also shows that the elements of H are closed under matrix multiplication.

Also, observe that since the determinant of any element in H is one, then there exist a inverse matrix, $i.e$ it has a matrix inverse, more explicitly:

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

Now for association, let us observe that

$$\begin{aligned}
\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \left(\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \right) &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d+g & h+di+e \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d+g & h+di+e+af+ai+b \\ 0 & 1 & f+i+c \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\
&= \left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \right) \cdot \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

So that we observe the associative law holds with the matrix multiplication, and we conclude two things: The Heisenberg group is a group, and that the order of the group depends on the field we are working on, that is, we have shown above that $|H(F)| = |F|^3$.

2. (c) Find the order of each element when $F = \mathbb{F}_2$

Let us denote the matrices as:

$$I = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A_5 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_6 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A_7 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad A_8 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

To avoid this tedious calculation, we use Wolfram Alpha (we know how to multiply matrices but is boring), and we find that: $A_2^2 = A_3^2 = A_4^2 = A_5^2 = A_7^2 = I$, i.e, these are elements of order two. Now for A_6 we have:

$$A_6^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_6^4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and we conclude A_6 is of order 4. And similarly for A_8 we have:

$$A_8^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad A_8^4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and we conclude A_8 is of order 4.