Margaret Bilu
Office 604

bilu@cims.nyu.edu

Midterm

October 31, 2017

Exercise 1. 1. Let $f : G \to H$ be a group homomorphism. Define $\operatorname{Ker} f$ and show that it is a subgroup of G.

Solution. See lectures.

2. Let A be the subset of $M_2(\mathbf{R})$ given by

$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a + d = 0 \right\}.$$

Is it a subgroup of $M_2(\mathbf{R})$?

Solution. Yes, it is a subgroup. This can be seen by checking all axioms separately, or by checking that the map $\phi : M_2(\mathbf{R}) \to \mathbf{R}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$$

is a homomorphism and by noticing that $A = \operatorname{Ker} \phi$.

Exercise 2. 1. (a) Give the order of the class of 2 in the group $(\mathbf{Z}/10\mathbf{Z}, +)$. Is it a generator?

Solution. Recall that the group law here is addition. Since $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 6$, $4 \cdot 2 = 8$ and $5 \cdot 2 \equiv 0 \pmod{10}$, we see that 2 is of order 5. In particular, it is not a generator of $\mathbf{Z}/10\mathbf{Z}$, since the latter is of order 10.

(b) Show that the group $\mathbf{Z}/10\mathbf{Z}$ is cyclic and give the list of all its generators.

Solution. We have seen in lectures that $\mathbf{Z}/10\mathbf{Z}$ is cyclic, and that its generators are exactly the classes of elements coprime to 10, that is $\{1, 3, 7, 9\}$.

(c) Give an element of order 2 in $\mathbf{Z}/10\mathbf{Z}$.

Solution. The class of 5 is of order 2, since $2 \cdot 5 \equiv 0 \pmod{10}$.

(d) Give a subgroup of order 5 of $\mathbf{Z}/10\mathbf{Z}$.

Solution. Since 2 is of order 5 as we have seen in question 1.(a), the subgroup $\{[0], [2], [4], [6], [8]\}$ it generates is of order 5.

2. Let $\phi : \mathbf{Z}/10\mathbf{Z} \to \mathbf{Z}/10\mathbf{Z}$ be a group homomorphism.

(a) Can we have $\phi([0]) = [3]$?

Solution. No, we have seen in lectures that the image of the identity element by a homomorphism should be the identity element, so we must have $\phi([0]) = [0]$.

(b) If $\phi([2]) = [4]$, what is $\phi([8])$?

Solution. Since -2 and 8 have the same class in $\mathbf{Z}/10\mathbf{Z}$ and ϕ is a homomorphism, we have $\phi([8]) = \phi(-[2]) = -\phi([2]) = -[4] = [6]$.

(c) If $\phi([1]) = [2]$, can ϕ be an isomorphism?

Solution. No, we have seen in lectures that if ϕ is an isomorphism, then the order of $\phi([1])$ should be equal to the order of $[1]$, which is not the case here since $[1]$ is of order 10 whereas $[2]$ is of order 5.

(d) Show that ϕ is of the form $[n] \mapsto a[n]$ for some $a \in \mathbf{Z}/10\mathbf{Z}$.

Solution. For all $n \in \{0, \ldots, 9\}$, we have, since ϕ is a homomorphism,

$$\phi([n]) = \phi(\underbrace{[1] + \ldots + [1]}_{n \text{ terms}}) = \underbrace{\phi([1]) + \ldots + \phi([1])}_{n \text{ terms}} = \phi([1])[n].$$

Putting $a = \phi([1])$, we have the result.

(e) Check that any map of this type is indeed a homomorphism.

Solution. Let $f : [n] \mapsto a[n]$ be such a map. For all integers n, m we have

$$f([n]+[m]) = f([n+m]) = a([n+m]) = a([n]+[m]) = a[n] + a[m] = f([n]) + f([m]).$$

(f) For which values of a is the homomorphism $n \mapsto an$ an isomorphism?

Solution. Note that the image of $\phi : [n] \mapsto [a][n]$ consists of the multiples $[0], [a], [2a], \ldots, [9a]$ of the class of a. Thus, ϕ is surjective if and only if all elements of $\mathbf{Z}/10\mathbf{Z}$ are multiples of the class of a. This will happen if and only if a is a generator of $\mathbf{Z}/10\mathbf{Z}$, so if $a \in \{[1], [3], [7], [9]\}$, as we have seen in question 1.(b). Conversely, if a is one of these classes, then a is invertible in $\mathbf{Z}/10\mathbf{Z}$, and therefore

$$\operatorname{Ker}\phi = \{[n] \in \mathbf{Z}/10\mathbf{Z},\ a[n] = 0\} = \{[0]\},$$

so that in this case ϕ is automatically injective. As a conclusion, $[n] \mapsto a[n]$ is an isomorphism exactly when a is a unit in $\mathbf{Z}/10\mathbf{Z}$, that is, exactly if $a \in \{[1], [3], [7], [9]\}$.

3. (a) What is the order of the group $(\mathbf{Z}/10\mathbf{Z})^\times$? Give all its elements and compute their inverses.

Solution. As mentioned earlier, we have $(\mathbf{Z}/10\mathbf{Z})^\times = \{[1], [3], [7], [9]\}$ as seen in lectures. It is of order 4. The classes [1] and [9] are their own inverses since $[1] \cdot [1] = [1]$ and $[9] \cdot [9] = [81] = [1]$. On the other hand, [3] is the inverse of [7] since $[3] \cdot [7] = [21] = [1]$.

(b) Describe the group $(\mathbf{Z}/10\mathbf{Z})^\times$ by giving its Cayley table.

Solution. Here is the Cayley table (we omit square brackets to simplify notation).

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(c) Is $(\mathbf{Z}/10\mathbf{Z})^\times$ cyclic? If yes, give a generator.

Solution. Yes, and [3] is a generator, since $[3]^2 = [9]$, $[3]^3 = [7]$ and $[3]^4 = [1]$.

(d) Is there an element of order 3 in $(\mathbf{Z}/10\mathbf{Z})^\times$?

Solution. We see that [1] is of order 1, [3] and [7] are of order 4, and [9] is of order 2, so there is no element of order 3.

(e) Give an example of a proper subgroup of $(\mathbf{Z}/10\mathbf{Z})^\times$.

Solution. The class [9] is of order 2, as we can see from the Cayley table. Therefore, the subgroup generated by [9] is

$$\langle [9] \rangle = \{[1], [9]\}$$

which is a proper subgroup of $(\mathbf{Z}/10\mathbf{Z})^\times$.

Exercise 3. Let $f : \mathbf{R}^2 \to \mathbf{R}^2$ be the map defined by

$$(x, y) \mapsto (x + y, y)$$

1. Show that f is a group homomorphism.

Solution. Recall that the group law is $+$. Let $(x, y), (x', y') \in \mathbf{R}^2$. We have

$$f(x, y) + f(x', y') = (x + y, y) + (x' + y', y') = ((x + x') + (y + y'), y + y')$$
$$= f(x + x', y + y') = f((x, y) + (x', y')).$$

2. Determine its kernel and its image.

   Solution. We have

$$\begin{aligned}\operatorname{Ker} f &= \{(x,y) \in \mathbf{R}^2,\ (x+y,y) = (0,0)\} \\ &= \{(x,y) \in \mathbf{R}^2,\ x+y=0 \text{ and } y=0\} \\ &= \{(0,0)\}\end{aligned}$$

   The image of f is

$$\begin{aligned}\operatorname{Im} f &= \{(u,v) \in \mathbf{R}^2,\ \text{there exists } (x,y) \in \mathbf{R}^2,\ \text{such that } (x+y,y) = (u,v)\} \\ &= \{(u,v) \in \mathbf{R}^2,\ \text{there exists } (x,y) \in \mathbf{R}^2,\ \text{such that } x+y=u, y=v\}\end{aligned}$$

   Note that $x+y=u$ and $y=v$ if and only if $x=u-v$ and $y=v$. Thus, for all $(u,v) \in \mathbf{R}^2$, $f(u-v,v) = (u,v)$, so that $(u,v) \in \operatorname{Im} f$. We may conclude that $\operatorname{Im} f = \mathbf{R}^2$.

3. Is f an isomorphism?

   Solution. Yes, by the computation of kernel and image in the previous question.

Exercise 4. 1. Give a list of all groups of order at most 4 up to isomorphism.

   Solution. We proved in lectures that up to isomorphism, the only groups of order at most 4 are the trivial group, $\mathbf{Z}/2\mathbf{Z}$ (order 2), $\mathbf{Z}/3\mathbf{Z}$ (order 3) and $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (both of order 4).

2. Let G be a group of order 4 having at least two distinct elements of order 2. Determine which of the groups in the list from the previous question it is isomorphic to.

   Solution. The group $\mathbf{Z}/4\mathbf{Z}$ has only one element of order 2, namely the class of 2. Indeed, its other non-trivial elements 1 and 3 are both of order 4. Therefore, G is necessarily isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and we can in fact conclude that all the non-trivial elements of G are of order 2.

3. Give a list of all the subgroups of this group.

   Solution. Let G be a non-trivial subgroup of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. As we have noted in lectures, whenever it contains two of the non-trivial elements of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, it also contains the third one, and is therefore equal to all of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Therefore, if G is not $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, then G contains exactly one non-trivial element of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Conversely, for any non-trivial element a of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, a is of order 2, so $\{(0,0), a\}$ is a subgroup of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. This gives us the list of all the subgroups:

$$\{(0,0)\},\ \{(0,0),(1,0)\},\ \{(0,0),(0,1)\},\ \{(0,0),(1,1)\},\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$