Margaret Bilu
Office 604
Fall 2019, Algebra MATH-UA.343-003
bilu@cims.nyu.edu

Midterm: solutions

October 23, 2019

Exercise 1. (12 points) Prove or disprove: for any of the following statements, say if it is true or false, by either proving it or providing a counterexample.

1. Let a, b, c be integers. If a divides bc then a divides b or c.

   Solution. This is false, e.g. for $a = 4$ and $b = c = 2$.

2. Let G and H be commutative groups. Then $G \times H$ is commutative.

   Solution. Let $(g, h), (g', h') \in G \times H$. Then

   $$(g, h) \cdot (g', h') = (gg', hh') = (g'g, h'h) = (g', h')(g, h),$$

   where we used that G and H are commutative. Thus, $G \times H$ is commutative.

3. Let G be a group and H a subgroup of G. If G is commutative, then so is H.

   Solution. Let $h, h' \in H$. Then h, h' are also elements of G, so $hh' = h'h$ by commutativity of G. Thus, H is commutative.

4. Let G be a group with identity element e and $x \in G$ an element of order 4. Then $x^{20} = e$.

   Solution. We have $x^4 = e$, so $x^{20} = (x^4)^5 = e^5 = e$.

Exercise 2. Let G be the group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

1. (5 points) Write out the list of the elements of G, and for each element, give its order.

   Solution. We have

   $$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}.$$

   Note that the group law on both $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$ is addition, and therefore, the group law on the product is also addition. Thus, the order of an element (x, y) here is the smallest positive integer n such that $n(x, y) = (0, 0)$.

   Checking orders by hand, we get:

   (a) The element $(0, 0)$ is of order 1.

   (b) The elements $(0, 2), (1, 2), (1, 0)$ are of order 2.

(c) The elements $(0,1),(0,3),(1,1),(1,3)$ are of order 4.

2. (2 points) What is the order of G?

   Solution. G has 8 elements, so its order is 8.

3. (2 points) Is G cyclic?

   Solution. There is no element of order 8, so G is not cyclic.

4. (2 points) Is G isomorphic to $\mathbf{Z}/8\mathbf{Z}$?

   Solution. No, since it is not cyclic.

5. (3 points) Give an example of a proper subgroup of G.

   Solution. We can for example take the subgroup

   $$H = \{0\} \times \mathbf{Z}/4\mathbf{Z} = \{(0,0),(0,1),(0,2),(0,3)\},$$

   which is the subgroup generated by the element $(0,1)$.

6. (4 points) We consider the map $p : G \to \mathbf{Z}/2\mathbf{Z}$ given by $p(x,y) = x$. Determine its kernel and image.

   Solution. The kernel is the subgroup H from the previous question. (In particular, this is another proof of the fact that H is indeed a subgroup!). The image is all $\mathbf{Z}/2\mathbf{Z}$, since e.g. $p(0,0) = 0$ and $p(1,0) = 1$.

Exercise 3. Let G be a group.

1. (2 points) What does it mean for G to be commutative?

2. (2 points) What does it mean for G to be cyclic?

3. (3 points) Show that if G is cyclic, then G is commutative.

4. (3 points) Give an example of a group which is commutative, but not cyclic.

Solution. See lecture notes. The group in Exercise 1 is commutative, but not cyclic. You can also take $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Exercise 4. Let $*$ be the law of composition of $\mathbf{Z}$ given by $x * y = 2x + 2y$.

1. (4 points) Is it associative?

   Solution. We have

   $$(x * y) * z = (2x + 2y) * z = 4x + 4y + 2z,$$

   and

   $$x * (y * z) = x * (2y + 2z) = 2x + 4y + 4z.$$

   These two expressions are not equal in general, as we can see by taking e.g. $x = y = 0$ and $z = 1$. Thus, $*$ is not associative.

   Remark: Note that you do need to prove that the expressions are not equal, for example by comparing them for some specific values. You get one point deducted if you simply assert they are different.

2. (2 points) Is it commutative?

   Solution. We have $x * y = 2x + 2y = 2y + 2x = y * x$. Thus, this law is commutative.

3. (3 points) Does it have an identity element?

   Solution. Assume that we have an identity element e. Then we should have

   $$x * e = 2x + 2e = x$$

   for all $x \in \mathbf{Z}$. Taking $x = 1$, we see that we must have $2e = 1$, which is impossible since e is an integer. So we have no identity element.

Exercise 5. 1. (2 points) State Bézout's theorem.

   Solution. Let $a, b \in \mathbf{Z}$ be not both zero. The integers a, b are relatively prime if and only if there exist $u, v \in \mathbf{Z}$ such that $ua + bv = 1$.

2. (5 points) Let a, b, c be integers such that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Show that $\gcd(a, bc) = 1$.

Solution. Because $\gcd(a, b) = 1$, we can find coefficients $s, t \in \mathbf{Z}$ such that

$$sa + tb = 1.$$

Multiply both sides of the equation by c to get

$$csa + tbc = c.$$

Now, let d be such that $d|a$ and $d|bc$. Then by the preceding equation, we have that $d|c$. Then, $d|a$ and $d|c$, so $d \leq \gcd(a, c) = 1$. Hence, $d = 1$. Therefore, $\gcd(a, bc) = 1$.

Exercise 6. Let G be the set given by

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbf{R}),\ a \in \{1, -1\}, b \in \mathbf{Z} \right\}.$$

1. (2 points) Show that G is a subset of $GL_2(\mathbf{R})$, the set of invertible 2×2 matrices with real coefficients.

   Solution. For this, it suffices to verify that all elements of G are invertible. This is the case since the determinant of a matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ is equal to a which is non-zero since it is equal to 1 or -1.

2. (8 points) Show that G is a subgroup of $(GL_2(\mathbf{R}), \cdot)$.

   Solution. We first verify that G is closed under matrix multiplication. For this, let $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \in G$. Then

   $$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix}.$$

   Since $a, a' \in \{1, -1\}$, we also have $aa' \in \{1, -1\}$. Moreover, since $a, b, b' \in \mathbf{Z}$, we have $ab' + b \in \mathbf{Z}$. Thus, the product matrix is indeed an element of G.

   Second, the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is the identity for matrix multiplication, is indeed an element of G.

   Finally, let us check that G is stable under taking inverses. For this, either you know how to compute the inverse of a two-by-two matrix, or you find the formula by hand. To do the latter, let $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$, and let us try to find conditions for a matrix $\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \in G$ to be its inverse:

   $$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

   We obtain that $aa' = 1$ and $ab' + b = 0$. The first equation, combined with the fact that $a, a' \in \{1, -1\}$,shows that either $a = a' = 1$ or $a = a' = -1$. The second equation then completely determines $b' = -ab$. After this computation,

we may check that indeed, the matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ has inverse $\begin{pmatrix} a & -ab \\ 0 & 1 \end{pmatrix} \in G$.

If you are more comfortable with matrices where most of the coefficients are numbers, you can also distinguish the two cases $a = 1$ and $a = -1$, and observe that for $a = 1$, the matrix $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G$ has inverse $\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in G$, whereas for $a = -1$, the matrix $\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix} \in G$ is its own inverse.

Remark: This approach is helpful for question 4, because an element of a group is of order 2 if and only if it is its own inverse. From this, you see directly that all the matrices in G with $a = -1$ are of order 2, and that they are the only ones (the identity being of order 1).

3. (3 points) Is G commutative?

   Solution. We have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix},$$

   and

$$\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & a'b + b' \\ 0 & 1 \end{pmatrix}.$$

   There are many ways of seeing that these two matrices are distinct in general. For example, when $a = a' = -1$ and $b \neq b'$. So this group is not commutative.

   Remark: Again, you need to justify that these two matrices are indeed not equal in general, otherwise you get one point deducted.

4. (5 points) Determine all elements of order 2 of G.

   Solution. Let $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ be an element of order 2. Then we have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

   that is,

$$\begin{pmatrix} a^2 & ab + b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This gives us two conditions $a^2 = 1$ and $ab + b = 0$. The first one is automatically satisfied since $a \in \{1, -1\}$. The second one is equivalent to $b(a + 1) = 0$, which is equivalent to $b = 0$ or $a = -1$. In the case $b = 0$, we get $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ (indeed, the other value of a gives us the identity matrix, which is of order 1). In the case $a = -1$, we get the matrices

$$\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$$

for all values of b (in particular, it includes the matrix we found in the previous case).

Thus, we may conclude that the set of elements of order 2 is

$$\left\{ \begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}, \quad b \in \mathbf{Z} \right\}.$$

Exercise 7. (6 points) If $a, b \in \mathbf{Z}$ are such that $a \equiv b \pmod{n}$, show that $\gcd(a, n) = \gcd(b, n)$.

Solution. $a \equiv b \pmod{n}$ means that there exists an integer k so that $a = b + kn$. Now, if $d|a$ and $d|n$, then $d|b$ by $b = a - kn$. Similarly, if $d|b$ and $d|n$, then $d|a$ because $a = b + kn$. So,

$$\{d \in \mathbf{Z} : d|a \text{ and } d|n\} = \{d \in \mathbf{Z} : d|b \text{ and } d|n\}$$

so that the greatest elements of each set are equal. Hence $\gcd(a, n) = \gcd(b, n)$.
Another way to prove this is to recall the following fact from lectures: $a \equiv b \pmod{n}$ if and only if a and b have the same remainder in the Euclidean division by n. Let r be this remainder. On the other hand, we also proved in lectures that when $a = nq + r$ is the Euclidean division of a by n, then $\gcd(a, n) = \gcd(n, r)$ (this was the starting point of the proof of the Euclidean algorithm!). Applying this to the Euclidean division $b = q'n + r$ of b by n as well, we get

$$\gcd(b, n) = \gcd(n, r) = \gcd(a, n).$$