Midterm

October 23, 2019

The use of notes and electronic devices is forbidden. All answers have to be justified. You can use all results proved in lectures without proof. If you use a result seen in a homework or in recitation you need to prove it.

Exercise 1. Let G be the group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

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

   Solution. We have

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

   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. What is the order of G?

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

3. Is G cyclic?

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

4. Is G isomorphic to $\mathbf{Z}/8\mathbf{Z}$?

   Solution. No, since it is not cyclic.

5. Give an example of a proper subgroup of G.

   Solution. We can for example take the subgroup

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

6. 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 proves 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 2. Let G be a group.

1. What does it mean for G to be commutative?

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

3. Show that if G is cyclic, then G is commutative.

4. 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 3. 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. Show that G is a subset of $GL_2(\mathbf{R})$, the set of invertible 2×2 matrices with real coefficients. 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. 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 $\begin{pmatrix} a & -ab \\ 0 & 1 \end{pmatrix} \in G$.

3. 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.

4. 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.

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

1. 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.

2. Is it commutative?

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

3. 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. 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.

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

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

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

Exercise 6. 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 $\gcd(a, n) = \gcd(b, n)$.

Exercise 7. 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, $\gcd(a, bc) = 1$.