Upload to Canvas before Feb/16, 6:00pm

MA503: Homework 4

Exercise 4.1. [20pts] Consider a Cartesian product $G = \mathbb{Z}\times\mathbb{Z} = \{\,(\alpha, x) \mid \alpha, x \in \mathbb{Z}\,\}$ and a binary operation $\cdot$ on G defined as follows:

$$(\alpha_1, x_1)\cdot(\alpha_2, x_2) = (\alpha_1+\alpha_2, (-1)^{\alpha_2}x_1 + x_2)$$

(1) [8pts] Prove that $(G,\cdot)$ is a group.
(2) [2pts] Is $(G,\cdot)$ abelian?
(3) [2pts] Is $(G,\cdot)$ finite?
(4) [2pts] Prove that every cyclic group is abelian. Then use (2) to prove that $(G,\cdot)$ is not cyclic.
(5) [2pts] Does $(G,\cdot)$ have torsion?
(6) [2pts] Is $\pi_1 : G\to\mathbb{Z}$ defined by $(\alpha, x)\overset{\pi_1}{\mapsto}\alpha$ a homomorphism?
[I want to emphasize that G is not the direct product of $\mathbb{Z}$ and $\mathbb{Z}$.]
(7) [2pts] Is $\pi_2 : G\to\mathbb{Z}$ defined by $(\alpha, x)\overset{\pi_2}{\mapsto}x$ a homomorphism?

Solution: (1) $(G,\cdot)$ is a group because

(G1) $(0,0)$ is the identity element:

$$(\alpha, x)(0,0) = (\alpha, x) = (0,0)(\alpha, x)$$

(G2) $\cdot$ is associative because for any elements $((\alpha_1, x_1), (\alpha_2, x_2)), (\alpha_3, x_3)$ we have

$$\begin{aligned}((\alpha_1,x_1)\cdot(\alpha_2,x_2))\cdot(\alpha_3,x_3) &= (\alpha_1+\alpha_2, (-1)^{\alpha_2}x_1+x_2)\cdot(\alpha_3,x_3)\\ &= (\alpha_1+\alpha_2+\alpha_3, (-1)^{\alpha_2+\alpha_3}x_1 + (-1)^{\alpha_3}x_2 + x_3)\\ (\alpha_1,x_1)\cdot((\alpha_2,x_2)\cdot(\alpha_3,x_3)) &= (\alpha_1,x_1)\cdot(\alpha_2+\alpha_3, (-1)^{\alpha_3}x_2+x_3)\\ &= (\alpha_1+\alpha_2+\alpha_3, (-1)^{\alpha_2+\alpha_3}x_1 + (-1)^{\alpha_3}x_2 + x_3).\end{aligned}$$

(G3) $(\alpha, x)^{-1} = (-\alpha, -(-1)^{-\alpha}x)$ because

$$(\alpha, x)\cdot(-\alpha, -(-1)^{-\alpha}x) = (0, (-1)^{-\alpha}x - (-1)^{-\alpha}x) = (0,0).$$

(2) To show that G is not abelian it is sufficient to find a counterexample, like

$$\begin{aligned}(1,1)\cdot(1,2) &= (2, -1+2) = (2,1),\\ (1,2)\cdot(1,1) &= (2,-2+1) = (2,-1).\end{aligned}$$

(3) G is infinite, it contains infinitely many elements.
(4) If G is cyclic, then $G = \langle g\rangle = \{g^n \mid n\in\mathbb{Z}\}$ for some $g\in G$. Then for any $a, b\in G$ we have $a = g^k$ and $b = g^m$. Hence,

$$ab = g^k g^m = g^{k+m} = g^m g^k = ba$$

and G is abelian. Therefore, if G is not abelian, then it is not cyclic. The given group is not abelian, hence, it is not cyclic.
(5) No, G is has no torsion because it has no nontrivial element of finite order. Indeed, for any $(\alpha, x)\in G$

$$\begin{aligned}(\alpha, x)^n = (0,0) \text{ for some } n>1 \quad &\Rightarrow\quad (n\cdot\alpha, \ldots) = (0,0)\\ &\Rightarrow\quad n\cdot\alpha = 0\\ &\Rightarrow\quad \alpha = 0\\ &\Rightarrow\quad (0,x)^n = (0, n\cdot x) = (0,0)\\ &\Rightarrow\quad x = 0.\end{aligned}$$

Thus, only $(0,0)$ gives the trivial element $(0,0)$ when raised to power $n>1$.
(6) π_1 is a homomorphism because for any $(\alpha_1, x_1), (\alpha_2, x_2)\in G$ we have

$$\begin{aligned}\pi_1((\alpha_1,x_1)\cdot(\alpha_2,x_2)) &= \pi_1((\alpha_1+\alpha_2, (-1)^{\alpha_2}x_1+x_2)) = \alpha_1+\alpha_2\\ \pi_1((\alpha_1,x_1)) + \pi_1((\alpha_2,x_2)) &= \alpha_1+\alpha_2.\end{aligned}$$

(7) To show that π_2 is not a homomorphism we find a counterexample

$$\pi_2((1,1)\cdot(1,1)) = \pi_2((2,0)) = 0$$
$$\pi_2((1,1)) + \pi_2((1,1)) = 1+1 = 2.$$

□

Exercise 4.2. [5pts] Find $|2|$ in U_{67}.

Solution: 2 is a unit in U_{67} and by Lagrange theorem its order divides $|U_{67}| = 66 = 2\cdot 3\cdot 11$. We can directly check all divisors starting from greater ones

$$2^{33} \equiv_{67} 66 \qquad 2^{22} \equiv_{67} 37 \qquad 2^{6} \equiv_{67} 64.$$

Now it is obvious that $|2| = 66$. □

Exercise 4.3. [5pts] Is 2 a primitive root modulo 31?

Solution: 2 is a unit in U_{31} and by Lagrange theorem its order divides $|U_{31}| = 30 = 2\cdot 3\cdot 5$. We can directly check all divisors starting from greater ones

$$2^{15} \equiv_{31} 1$$

and make a conclusion that 2 is not a primitive root of 31. □

Exercise 4.4. [10pts] Consider a set $G = \{x_1, x_2, \dots, x_8\}$ of eight elements equipped with a binary operation $\cdot$ defined by the multiplication table shown below. $(G,\cdot)$ is a group.

$\cdot$	x_4	x_3	x_7	x_1	x_2	x_6	x_5	x_8
x_4	x_2	x_6	x_5	x_8	x_4	x_3	x_7	x_1
x_3	x_6	x_4	x_8	x_7	x_3	x_2	x_1	x_5
x_7	x_5	x_1	x_4	x_6	x_7	x_8	x_2	x_3
x_1	x_8	x_5	x_3	x_4	x_1	x_7	x_6	x_2
x_2	x_4	x_3	x_7	x_1	x_2	x_6	x_5	x_8
x_6	x_3	x_2	x_1	x_5	x_6	x_4	x_8	x_7
x_5	x_7	x_8	x_2	x_3	x_5	x_1	x_4	x_6
x_8	x_1	x_7	x_6	x_2	x_8	x_5	x_3	x_4

(1) Which element is the identity of G?
(2) Is G abelian? Why?
(3) Find $|x_3|$.
(4) Find $\langle x_4\rangle$.
(5) Find the coset $x_6\cdot\langle x_4\rangle$.
(6) Find x_5^{-1}.
(7) Is x_7 a primitive element?
(8) [3pts] Is G cyclic?

Solution:

(1) x_2 is the identity of G, because $x_2x_i = x_i$ for every $i = 1,\dots,8$.
(2) G is not abelian. For instance, $x_7x_3 = x_1 \neq x_8 = x_3x_7$.
(3) $x_3^2 = x_4$, $x_3^3 = x_6$, $x_3^4 = x_2$. Hence, $|x_3| = 4$.
(4) $\langle x_4\rangle = \{x_2, x_4\}$.
(5) $x_6\cdot\langle x_4\rangle = \{x_6, x_3\}$.
(6) $x_5^{-1} = x_7$.
(7) $|x_7| = 4$ and, hence, x_7 is not a primitive element.
(8) [3pts] G is not cyclic because

$$|x_4| = 2 \qquad |x_3| = 4 \qquad |x_7| = 4 \qquad |x_1| = 4$$
$$|x_2| = 1 \qquad |x_6| = 4 \qquad |x_5| = 4 \qquad |x_8| = 4.$$

□