MATH 212 Assignment 1

Colton Broughton
Oliver Tonnesen
Ashley Van Spankeren
Selma Yazganoglu

February 25, 2019

1

$G := \mathbb{Z} \oplus \mathbb{Z} = \{(0,0), (0,1), (1,0), (1,1)\}$
$\langle (0,0) \rangle = \{(0,0)\}$
$\langle (0,1) \rangle = \{(0,0), (0,1)\}$
$\langle (1,0) \rangle = \{(0,0), (1,0)\}$
$\langle (1,1) \rangle = \{(0,0), (1,1)\}$
So there exists no $g \in G$ with $\langle g \rangle = G$, and G is therefore not cyclic. The following are the subgroups of G:
$\{(0,0)\}$
$\{(0,0), (0,1)\}$
$\{(0,0), (1,0)\}$
$\{(0,0), (1,1)\}$

Note that each subgroup can be constructed by taking the union of the set containing the identity – $(0,0)$ – and the set containing exactly one element of $\mathbb{Z} \oplus \mathbb{Z}$. Additionally, the group generated by $g \in G$ is exactly the vector space over $\{(x,y) \mid x, y \in GF(n)\}$ spanned by g.

2

*	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

<u>Nonempty</u>: True

Associative:

$$a(bd) = (ab)d = c$$
$$b(cd) = (bc)d = a$$
$$a(bc) = (ab)c = d$$
$$a(cd) = (ac)d = b$$

The table shows the group to be abelian, so this is true for all other permutations.

Inverse: Every element is its own inverse.

Binary operation: All pairs of elements map to an element in the set.

3

3.a

We know $h \neq e$ and $g \neq e$, so gh can be neither g nor h, and so has to be e. Thus $gh = e = gg^{-1}$ and $h = g^{-1}$. The same can be said for hg, and so $g = h^{-1}$. hh cannot be h since $h \neq e$, and hh cannot be e since $h^{-1} = g$, so $hh = g$. Similarly, $gg = h$. Thus we have completed the binary operation table for G:

	e	g	h
e	e	g	h
g	g	h	e
h	h	e	g

We can simply look at the table and see that it is symmetric about the diagonal, and so G is abelian.

3.b

Similarly to as in section 3.a, we can simply look at the binary operation table and see that $\langle g \rangle = G$, and so G is cyclic.

4

4.a

Recall *Thorem 3.7.6*: $H \subseteq G$ is a subgroup of G if and only if $H \neq \emptyset$ and for all $h_1, h_2 \in H$, $h_1^{-1}h_2 \in H$.

We have $0 \in H$, so $H \neq \emptyset$.
Suppose we have $h_1 = dk_1$, and $h_2 = dk_2$ where $h_1, h_2 \in d\mathbb{Z}$. We know that $h_1^{-1} = -dk_1$, since $dk_1 + (-dk_1) = e$. Thus, $h_1^{-1}h_2 = -dk_1 + dk_2 = d(k_2 - k_1)$. $k_2 - k_1 \in \mathbb{Z}$, and so $d(k_2 - k_1) \in d\mathbb{Z}$. Thus we have satisfied both conditions of the theorem, and so H is a subset of G.

4.b

Suppose $H \subseteq \mathbb{Z}$ is a non-trivial subgroup of $\mathbb{Z}$. Let $n \in H$ be the smallest positive element in H. H is a group, and is therefore closed under its binary operation. Thus $nk \in H$ for all $k \in \mathbb{Z}$, and $n\mathbb{Z} \subseteq H$. Suppose for a contradiction that there exists an element in H that is not of the form nk, $k \in \mathbb{Z}$. By the division algorithm, there exist disinct integers q and r, $0 \leq r < n$ such that $m = qn + r$. Since $m \neq nk$ for all $k \in \mathbb{Z}$, $r \neq 0$. From $m = qn + r$, we have $m + (-qn) = r \in H$ since $m, (-qn) \in H$. So $n > r \in H$, contradicting our initial supposition that n is the smallest positive element in H.

5

5.i

True. Let A be an abelian group. There exist $a, b \in A$ such that $ab = ba$. For a subgroup B of A, $a_B b_B = b_B a_B$, since all $a, b \in A$ commute.

5.ii

True. Let $\langle g \rangle = G$ for some $g \in G$. Then for any $g' \in G$, there exists some $k \in \mathbb{Z}$ such that $g' = g^k$. Similarly, if $H \subseteq G$ is a subgroup of G, then for any $h \in H$, there exists some $m \in \mathbb{Z}$ such that $h = g^m$.
Let n be the least positive integer such that $g^n \in H$. We wish to show that $n \mid m$. That is, we wish to show that every m can be written as nq for some $q \in \mathbb{Z}$, and by extension, every g^m can be written as $(g^n)^q$. If this is the case, then $\langle g^n \rangle = H$.
By the division algorithm, we know that there exist distinct integers q and r, $0 \leq r < n$, such that $m = nq + r$. So

$$\begin{aligned}
g^m &= (g^n)^q \cdot g^r \\
(g^n)^{-q} \cdot g^m &= (g^n)^{-q} \cdot (g^n)^q \cdot g^r \\
(g^n)^{-q} \cdot g^m &= g^r
\end{aligned}$$

By definition, $g^n, g^m \in H$, and so $(g^n)^q \cdot g^m = g^r \in H$. Recall that n was defined to be the smallest positive integer such that $g^n \in H$, but $0 \leq r < n$. So $r = 0$, and therefore it is the case that $n \mid m$, and so $\langle g^n \rangle = H$, and H is cyclic.

5.iii

False. The trivial subgroup containing only the identity is always abelian.

5.iv

False. The trivial subgroup containing only the identity is always cyclic.

5.v

True. Let $h, m \in G$, a cyclic group. We know there exists $g \in G$ such that $\langle g \rangle = G$, and so $h = g^k$ and $m = g^l$ for some $k, l \in \mathbb{Z}$. $hm = g^k g^l = g^{k+l} = g^{l+k} = g^l g^k = mh$.

5.vi

False. $(\mathbb{R}, +)$ is abelian but not cyclic.