Answers to Exam I – Math 411

1. (a) False. $(2/1)/2 = 1$, $2/(1/2) = 4$
   (b) True, $\mathbb{Z}/n\mathbb{Z}$
   (c) False, $\{e\}$, $\mathbb{Z}/p\mathbb{Z}$ (p prime) are counterexamples
   (d) False $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ not cyclic
   (e) True

2. (a) associative:
$$\begin{aligned}(a*b)*c &= (a+b-1)+c-1 \\ &= a+b+c-2 \\ &= a+(b+c-1)-1 \checkmark \\ &= a*(b*c)\end{aligned}$$
   identity: $a * 1 = 1 * a = a$ ✓
   inverses: $a*(2-a) = (2-a)*a = 1$ ✓

   (b) yes it is, $2 * x = 2 + x - 1 = x+1$
   a generator is 2.

3. (a) $(1,2,3) * (-1,-2,-1) = (0, 0, 3-1+(-2))$
$= (0,0,0)$

   $(0,0,0)*(3,5,7) = (3,5,7)$

   (b) we know it's associative.
   identity: (a) suggests $(0,0,0)$, so check that
$$\begin{aligned}(a,b,c)*(0,0,0) &= (a+0, b+0, c+0+a\cdot 0) \\ &= (a,b,c) \checkmark \\ (0,0,0)*(a,b,c) &= (0+a, 0+b, 0+c+0\cdot b) \\ &= (a,b,c) \checkmark\end{aligned}$$

3 b (cont'd) 2

inverses: a gives a clue. $(a,b,c)^{-1}$ should have form $(-a,-b,d)$ for some d.
check it:

$$(a,b,c)*(-a,-b,d) \stackrel{?}{=} (0,0,0)$$

$$= (0,0,c+d-ba) \quad \text{so} \quad d = ba-c$$

and $(a,b,c)^{-1} = (-a,-b,ba-c)$

check it: $(a,b,c)*(-a,-b,ba-c) = (0,0,0)$ ✓
$(-a,-b,ba-c)*(a,b,c) = (0,0,0)$ ✓

Remark: This is really a subgroup of 3×3 matrices:

$$\left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a,b,c \in \mathbb{Z} \right\}$$

called the Heisenberg group.

4 a need divisors of 60:

$$\left.\begin{array}{ccc} 1 & \cdot & 60 \\ 2 & \cdot & 30 \\ 3 & \cdot & 20 \\ 4 & \cdot & 15 \\ 5 & \cdot & 12 \\ 6 & \cdot & 10 \end{array}\right\}$$

so 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

3

4 (b) In $\mathbb{Z}/n\mathbb{Z} = \langle g \rangle$, subgp of order $d | n$ has generator $g^{n/d}$.

subgp ords	1	2	3	4	5	6	10	12	15	20	30	60
generator $= g^k$ with $k=$	60	30	20	15	12	10	6	5	4	3	2	1

(c) $\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = \varphi(4)\varphi(3)\varphi(5)$
$= 2 \cdot 2 \cdot 4 = 16$

(d) g^k where k is one of
1, 7, 11, 13, 17, 19, 23, 29, 31,
37, 41, 43, 47, 49, Herbie, 59.

5 (a) Let $x, y \in G$ and consider $xy \in G$.
We have $(xy)(xy) = e$. But then

$$(xy)(xy) = e \Rightarrow xy = (xy)^{-1}$$

$$\Rightarrow xy = y^{-1}x^{-1}$$

But $x^{-1} = x$, $y^{-1} = y$ since $x^2 = y^2 = e$.
so

$$\boxed{xy = yx}$$ ✓

(4)

(T) (5) $\mathbb{Z}/n\mathbb{Z}$, $n \geq 3$ has elements of orders > 2.

(6) First suppose $o(x) = \infty$. Then $o(x^{-1})$ must also be $= \infty$. Otherwise we have

$(x^{-1})^n = e$ for some finite $n > 0$

and then $x^n = e$ (take inverse of

both sides). Now suppose $o(x) = n \neq \infty$.

Then by same argument $x^{-n} = (x^{-1})^n = e$

so $o(x^{-1})$ is at most n. If

$o(x^{-1}) = d < n$ then same argument

shows $x^d = e$ and $o(x) < n$. Thus

$o(x^{-1}) = n$ as well.

(7) $A \times B = \{(a,b) \in G \times H \mid a \in A, b \in B\}$

inverses: $(a,b)^{-1} = (a^{-1}, b^{-1})$, and

$a^{-1} \in A$, $b^{-1} \in B$

closed under mult: $(a,b)(a',b') = (aa', bb')$,
and $aa' \in A$, $bb' \in B$.
identity is (e_G, e_H) and $e_G \in A$, $e_H \in B$