Math 417
HW2 Sols
2/4/19

Ungraded

§1.2-7 $a*b = a-b$. $b*a = b-a = -(a-b)$ so not commutative *see below

§1.2-9 $a*b = \frac{ab}{2}$ $b*a = \frac{ba}{2} = \frac{ab}{2}$ so yes commutative *see below

§1.3-3 $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ via $\phi(n) = 2n$. Well... $\phi(n_1+n_2) = \phi(n_1)+\phi(n_2)$ but ϕ is not onto so it's not a bijection. (There is no x so that $\phi(x) = 1, 3$, etc.)

§1.3-5 $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Q}, + \rangle$ $\phi(x) = \frac{x}{2}$. Well, ϕ is 1-1 and $\phi(2x) = x$, so ϕ is onto and $\phi(x+y) = \frac{x+y}{2} = \frac{x}{2} + \frac{y}{2}$, so the answer is "yes", it's an isa

§1.4-3 $a*b = \sqrt{ab}$ on $\mathbb{R}^+$.

Is it associative? $(a*b)*c$
$= \sqrt{(a*b)c} = \sqrt{\sqrt{ab}c} = a^{1/4} b^{1/4} c^{1/2}$
Similarly $a*(b*c) = a^{1/2} b^{1/4} c^{1/4}$
not equal, so not associative

§1.4-5 $a*b = a/b$ on $\mathbb{R}^+$
Again $(a*b)*c = (a/b)/c = \frac{a}{bc}$
$a*(b*c) = a/(b/c) = \frac{ac}{b}$
not associative.

§1.4-31 - Suppose G has an idempotent elem x, $x*x = x$ Note that $x = e$ is idempotent $e*e = e$ (because $e*y = y$ for every y). Suppose $x*x = x$. Apply x^{-1} to both sides
$x^{-1}*(x*x) = x^{-1}*x = e$
$(x^{-1}*x)*x = e*x = x$, so $x = e$

§1.2-7 associative? No
$(a*b)*c = (a-b)-c = a-b-c$
$a*(b*c) = a-(b-c) = a-b+c$

§1.2-9 associative? Yes
$(a*b)*c = \frac{ab}{2}*c = \frac{\frac{ab}{2}\cdot c}{2} = \frac{abc}{4}$
$a*(b*c) = a*\frac{bc}{2} = \frac{a\cdot\frac{bc}{2}}{2} = \frac{abc}{4}$.

1a §1.3-6
$\langle \mathbb{Q}, \cdot \rangle$ onto $\langle \mathbb{Q}, \cdot \rangle$, $\phi(x) = x^2$.
Since $\sqrt{2} \notin \mathbb{Q}$, there is no x so that $\phi(x) = 2$ and ϕ is not onto, so it isn't a bijection

1b. §1.4-4
$*$ defined on $\mathbb{Q}$ by $a*b = ab$.
It is associative (§1.1)
There is an identity $a*1 = a \cdot 1 = 1$ for all $a \in \mathbb{Q}$.
Alas, it doesn't always have an inverse. There is no b so that $0*b = 1$
(However, if we define $*$ on $\mathbb{Q} - \{0\}$ we will get a group - question not asked.)

2. $S = \mathbb{R}$ §1.3.
$a*b = a+b-ab$.
1. Check associativity
$(a*b)*c = (a+b-ab)*c$
$= a+b-ab+c-c(a+b-ab)$
$= a+b+c-ab-ac-bc+abc$
$a*(b*c) = a*(b+c-bc)$
$= a+b+c-bc-a(b+c-bc)$
$= a+b+c-bc-ab-ac+abc)$
Whew! But the answer is yes

2.b Identity. Given a, find b s.t. $a*b = a$.

$a + b - ab = a$

$\Leftrightarrow b(1-a) = 0$, so $b = 0$ will always work.

c. Inverse $a * b = 0$ (the identity)

$a + b - ab = 0$

$\Rightarrow b(1-a) = -a \to b = \frac{a}{a-1}$

Since $a \neq 1$, this is a^{-1} and yes, this is a group!

3a $n = 168 = 2^3 \cdot 3 \cdot 7$

$\nu_2(168) = 3$, $\nu_3(168) = 1$

$\nu_5(168) = 0$ (not asked: $\nu_7(168) = 1$.)

3b. $p^3 | n^2$ so $\nu_p(n^2) \geq 3$

That is, $2\nu_p(n) \geq 3$, $\nu_p(n) \geq \frac{3}{2}$

But $\nu_p(n)$ is an integer, so $\nu_p(n) \geq 2$; that is, $p^2 | n$.

3c. Following the hint, let $a = 4$ and $n = 8$. Then $a^3 = 64 = n^2$ so $a^3 | n^2$. but $a^2 = 16$ and $16 \nmid 8$.

4,5 $[a]_5 \times [b]_5 = [3ab]_5$

table reproduced for your convenience

	[1]	[2]	[3]	[4]
[1]	3	1	4	2
[2]	1	2	3	4
[3]	4	3	2	1
[4]	2	4	1	3

a. $(a*b)*c = a*(b*c)$ is what associativeness is

$a * b = 3ab$, so

$(a*b)*c = 3 \cdot (3ab) \cdot c = 9abc$

(also $= 4abc = -abc$).

(All equalities are in $\mathbb{Z}/5\mathbb{Z}$ (mod 5)).

$a*(b*c) = 3 \cdot a(3bc) = 9abc$

So yes, associative.

b. Looking at the table

$a * 2 = a$ for every a,

so $[2]_5$ is the identity elt.

c. $[1]*[4] = [2]$, $[2]*[2] = [2]$

$[3]*[3] = [2]$, so $[1]^{-1} = [4]$

$[2]^{-1} = 2$, $[3]^{-1} = 3$, $[4]^{-1} = 4$.

d. As corrected, additive group

Let $\phi: G \to (\mathbb{Z}/4\mathbb{Z}, +)$ be defined by: $\phi([2]_5) = [0]_4$

$\phi([1]_5) = [1]_4$, $\phi([3]_5) = [2]_4$,

$\phi([4]_5) = [3]_4$.

If I write the table out in the same order, I get

	$[1]_4$	$[0]_4$	$[2]_4$	$[3]_4$
$[1]_4$	2	1	3	0
$[0]_4$	1	0	2	3
$[2]_4$	3	2	0	1
$[3]_4$	0	3	1	2

It's a scrambled order, but this is the addition table mod 4.

In general, an isomorphism will map the identity to the identity

*Here it is also ok to say $\phi([1]_5) = [3]$ and $\phi([4]_5) = [1]_4$ also an isomorphism

6. $(\mathbb{Z}/12\mathbb{Z})^*$, $\cdot$

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(because, eg. $5 \cdot 7 = 35 \equiv 11 \bmod 12$

V.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

So the "obvious" choice

is $\phi([1]_{12}) = e$
$\phi([5]_{12}) = a$
$\phi([7]_{12}) = b$
$\phi([11]_{12}) = c$

but actually, any of the 3! ways of choosing $\{\phi([5]_{12}), \phi([7]_{12}), \phi([11]_{12})\} = \{a, b, c\}$ will work

HW1 redone with ν.

$\gcd(a,b) = 4$
means $\min(\nu_2(a), \nu_2(b)) = 2$
$\min(\nu_3(a), \nu_3(b)) = 0$
$\min(\nu_5(a), \nu_5(b)) = 0$

$\gcd(a,c) = 6$
means $\min(\nu_2(a), \nu_2(c)) = 1$
$\min(\nu_3(a), \nu_3(c)) = 1$
$\min(\nu_5(a), \nu_5(c)) = 0$.

because $4 = 2^2 \cdot 3^0 \cdot 5^0$
$6 = 2^1 \cdot 3^1 \cdot 5^0$.

So

a). $\nu_2(a) \geq 2$, $\nu_2(b) \geq 2$ (one of them equals 2) and $\min(\nu_2(a), \nu_2(c)) = 1$
So $\nu_2(c) = 1$
$g = \gcd(b,c)$.
$\nu_2(g) = \min(\nu_2(b), \nu_2(c))$
$\nu_2(b) \geq 2$, $\nu_2(c) = 1$ so
$\nu_2(g)$ has to equal 1.

b). $\nu_3(a) \geq 1$, $\nu_3(c) \geq 1$ (one of them =)
$\min(\nu_3(b), \nu_3(a)) = 0$, so $\nu_3(b) = 0$
$\nu_3(g) = \min(\nu_3(b), \nu_3(c))$
so $\nu_3(g)$ has to equal 0

c). Can't say anything! If $\nu_5(a) = 0$
$\nu_5(b)$ and $\nu_5(c)$ can be anything
$a = 12$, $b = 4 \cdot 5^m$, $c = 6 \cdot 5^m$
will satisfy the problem, and
$g = 2 \cdot 5^m$ for any m.