§6.1 #5b, d, e Given the Cayley Table below for $*$ analyze if $*$ is unital (has identity), associative, commutative and for those elements with inverses find them.

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

Let $\{a, b, c, d\} = A$

← this says $c * d = d$

The identity e must satisfy $x * e = e * x = x \quad \forall x \in A$.
we need $e * e = e * e \Rightarrow \underline{e = c}$ if anything. Observe,

$$c * a = a = a * c$$
$$c * b = b = b * c$$
$$c * d = d = d * c$$

Thus $c * x = x * c = x \quad \forall x \in A$. We find $\boxed{e = c}$

Moreover, we can see from the symmetry of the table about the diagonal that $x * y = y * x$ $\forall x, y \in A$.

Inverses a^{-1} have $a * a^{-1} = a^{-1} * a = e = c$ for this example. Clearly $\boxed{c^{-1} = c}$ since $c * c = c$. Also

$a * a = e \Rightarrow \boxed{a = a^{-1}}$ note $d * b = e$ and $b * d = e$

thus $\boxed{d^{-1} = b}$ and $\boxed{b^{-1} = d}$

§6.1 #7 (Hint) When is $\mathbb{R}^{m\times n} = \mathcal{M} = \{A \mid A \text{ } m\times n \text{ real matrix}\}$ an algebraic structure under matrix multiplication?

Reminder: If A is $m\times n$ and B is $p\times q$ then AB is a $m\times q$ matrix iff $n = p$. We assume $m, n, p, q \in \mathbb{N}$. If you want to write details some nice notation is $A \in \mathbb{R}^{m\times n}$ is denoted $A = [A_{ij}]$ where $A_{ij} \in \mathbb{R}$ for $1 \le i \le m$ and $1 \le j \le n$. If $B \in \mathbb{R}^{n\times q}$ then $B = [B_{\ell k}]$ such that $1 \le \ell \le n$ and $1 \le k \le q$. We can define $AB \in \mathbb{R}^{m\times q}$ with $AB = [(AB)_{ik}]$ and

$$(AB)_{ik} = \sum_{\ell=1}^{m} A_{i\ell} B_{\ell k}$$

On the other hand, we can only add matrices of the same size. If $A, B \in \mathbb{R}^{m\times n}$ then

$$A + B = [(A+B)_{ij}]$$

$$(A+B)_{ij} = A_{ij} + B_{ij} \quad \text{for all } i, j \text{ with } 1 \le i \le m \text{ and } 1 \le j \le n.$$

Ok, enough hinting.

§6.1#8 Let $(A, \circ)$ be an algebraic structure. Prove that if e and f are identities for $\circ$ then $e = f$

Proof: Since e is an identity for $\circ$ then $e \circ x = x \circ e = x$ $\forall x \in A$. Likewise f is an identity for $\circ$ then $f \circ y = y \circ f = y$ $\forall y \in A$. In particular choose $x = f$ and $y = e$ then

$$\left.\begin{aligned} e \circ f &= f \circ e = f \\ f \circ e &= e \circ f = e \end{aligned}\right\} \rightarrow \boxed{f = e}$$

§6.1#9a Let $(A, \circ)$ be an algebraic structure, $a \in A$ and e the identity for $\circ$.

a.) Prove that if $\circ$ is associative and x and y are inverses of a then $x = y$

Assume $(A, \circ)$ is an associative algebraic structure and $a \in A$ and e is identity with respect to $\circ$. If x and y are inverses of a then

$$x \circ a = a \circ x = e \quad \text{and} \quad y \circ a = a \circ y = e$$

Thus, $x \circ a = y \circ a$. Operate by x on the right, $(x \circ a) \circ x = (y \circ a) \circ x$

$\Rightarrow x \circ (a \circ x) = y \circ (a \circ x)$ using associativity!

$\Rightarrow x \circ e = y \circ e$

$\Rightarrow x = y$. //

§6.1# 14a Construct Cayley Table for $(\mathbb{Z}_8, +_8)$.

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

add $\bar{\ }$ to all numbers here technically speaking.

§6.1# 15a Find zero-divisors in $\mathbb{Z}_6$

Def^n, a zero-divisor $a \in \mathbb{Z}_6$ is $a \neq 0$ such that $\exists\, b \in \mathbb{Z}_6$ with $b \neq 0$ and $ab = 0$.

$\bullet_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Mod(6), $\bar{2}(\bar{3}) = 0$ and $\bar{3}(\bar{4}) = 0$ thus $\bar{2}, \bar{3}, \bar{4}$ are zero divisors

In contrast, $\bar{1}$ and $\bar{5}$ have multiplicative inverses $\bar{1}^{-1} = \bar{1}$ and $\bar{5}^{-1} = \bar{5}$ where $e = \bar{1}$ w.r.t. $\bullet_6$.

Remark: there is a difference between 0 and $\bar{0}$ etc... but since there is little danger of confusion in many contexts you'll find the "$\bar{\ }$" is missing. I'll try to keep them most places.

§6.2#2 Given that $G = \{e, u, v, w\}$ is a group of order 4 with identity e and $u^2 = v$ and $v^2 = e$, construct the Cayley Table for the group.

Notice $u^4 = u^2 u^2 = vv = v^2 = e$. Let's see the group has order 4 thus the products $uv, vu, uw, wu, wv, vw, w^2$ all must be in $\{e, u, v, w\}$. Notice $v^2 = e \Rightarrow v = v^{-1}$

	e	u	v	w
e	e	u	v	w
u	u	v	w	e
v	v	w	e	u
w	w	e	u	v

Suppose $ww = v$ then $(wv)(vw) = wv^2w = w^2 = v$
This suggests $wv = vw = u$ to be consistent.
Then the rest of the table fills out by the rule that no elements is repeated in any particular row or column.

$u = wv \Rightarrow uv = wv^2 \Rightarrow uv = w$.

Remark: these sort of problems require a fair amount of guessing and tinkering. I think §6.2#3 is easier

§6.2#6c Construct Cayley Table for $(\mathbb{Z}_5 - \{0\}, \cdot_5)$

$\cdot_5$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Notice $(\bar{4})^{-1} = \bar{4}$
and $(\bar{2})^{-1} = \bar{3}$
while $(\bar{3})^{-1} = \bar{2}$
here $e = \bar{1}$

Remark: you don't have to use $\bar{1}$ etc... for #6 if you don't want to. I just wanted to emphasize that these objects are multiplied by modular arithmatic.

§6.2 #8b) Compute the following products in the group of permutations on 4 objects S_4:

$[1243] \circ [4213]$, $[4321] \circ [4321]$ and $[2143] \circ [1324]$

We calculate, (see pg. 270 - 271)

$$[1243] \circ [4213] = [3214]$$

$$[4321] \circ [4321] = [1234]$$

$$[2143] \circ [1324] = [2413]$$

§6.2 #11) Let G be a group. Prove that if $g^2 = e$ $\forall g \in G$ then G is Abelian.

Proof: If $a, b \in G$ then $ab \in G$ since G is a group which is closed under multiplication. Furthermore,

$$(ab)^2 = (ab)(ab) = e$$

Note $a^2 = e$ and $b^2 = e$ and multiply on right by ba to obtain:

$$(ab)(ab)(ba) = ba$$

$\Rightarrow abab^2a = ba$: used associativity in G.

$\Rightarrow abaea = ba$: $b^2 = e$

$\Rightarrow aba^2 = ba$: $aea = aa = a^2$

$\Rightarrow abe = ba$: $a^2 = e$

$\Rightarrow ab = ba$

Thus G is abelian since $ab = ba$ $\forall a, b \in G$. //

§6.2 #18c Solve $x \cdot x = 0$ in $\mathbb{Z}_{20}$. Make sure to find all sol^{n}'s

Notice that if x is a unit (meaning x^{-1} exists) then $xx^{-1} = 1 \Rightarrow xxx^{-1} = x \Rightarrow x^2x^{-1} = x$. If $x^2 = 0$ in this context then $x = 0$ but then x^{-1} d.n.e. Thus we can safely ignore units in $\mathbb{Z}_{20}$.

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

these numbers are relatively prime to 20

$\gcd(u, 20) = 1$ for $u \in U(20)$.

I guess brute-force isn't too hard here,

$0 \cdot 0 = 0$
$1 \cdot 1 = 1$
$2 \cdot 2 = 4$
$4^2 = 16$
$5^2 = 25 = 5$
$6^2 = 36 = 16$
$7^2 = 49 = 9$
$8^2 = 64 = 4$
$10^2 = 100 = 0$
$12^2 = 144$
$13^2 = 169$
$14^2 = 196 = 16$
$15^2 = 225 = 5$
$16^2 = 256 = 16$
$18^2 = 324 = 4$

thus $x = 0$ and $x = 10$ are the sol^{n}'s of $x^2 = 0$ in $\mathbb{Z}_{20}$

Remark: maybe you can see a better way to deal with such a question

§6.3#4 Show that if $H < G$ and $K < G$ then $H \cap K < G$ where $H < G$ denotes H being a subgroup of G

Proof: Suppose $H < G$ and $K < G$. Note $e \in H \cap K$ since $e \in H < G$ and $e \in K < G$. Suppose $a, b \in H \cap K$ then $a, b \in H$ and $a, b \in K$ thus $ab^{-1} \in H$ and $ab^{-1} \in K$ by Th^{m}(6.9). Hence $ab^{-1} \in H \cap K \Rightarrow H \cap K < G$ by Th^{m}(6.9).

§6.3#6 (Hint) Additive groups are easy to think about. For example $(\mathbb{R}^2, +)$ is a group under vector addition.

§6.3#9c Find the order of the elements in $(\mathbb{Z}_8, +_8)$

Let $x \in \mathbb{Z}_8$ the order of x is the smallest $n \in \mathbb{N}$ such that $nx \equiv \underbrace{x + x + \cdots + x}_{n\text{-times}} = 0 \mod(8)$. All calculations mod(8) below.

$1 \cdot 0 = 0$
$8 \cdot 1 = 0$
$4 \cdot 2 = 0$
$8 \cdot 3 = 0$
$2 \cdot 4 = 0$
$8 \cdot 5 = 0$
$4 \cdot 6 = 0$
$8 \cdot 7 = 0$

In $\mathbb{Z}_8$ we find,
0 has order 1.
1, 3, 5, 7 have order 8.
2, 6 have order 4
4 has order 2

§6.3#9d Find order of elements in $(\mathbb{Z}_7 - \{0\}, \cdot)$

Here the order of a is smallest $n \in \mathbb{N}$ such that $a^n = \underbrace{a \cdot a \cdots a}_{n\text{ factors}} = 1$.

$2 \cdot 2 \cdot 2 = 8 \cong 1 \Rightarrow$ 2 has order 3.

$4 \cdot 4 \cdot 4 = 64 \cong 1 \Rightarrow$ 4 has order 3.

Notice $5 \cdot 5 = 25 \cong 4 \Rightarrow 5^4 \cong 4^2 = 16 \cong 2$
$\Rightarrow 5^5 \cong 10 \cong 3$
$\Rightarrow 5^6 \cong 15 \cong 1 \quad \therefore$ 5 has order 6

I'll leave the rest for you to play with.

§6.4 #6a,b Let $f: (A, \cdot) \to (B, *)$ and $g: (B, *) \to (C, \times)$ be operation preserving maps. Prove $g \circ f$ is an OP map. Prove if f^{-1} is a function then f^{-1} is an OP map

(a) Proof: Let $a, b \in A$ then consider,

$$\begin{aligned}(g \circ f)(a \cdot b) &= g(f(a \cdot b)) && : \text{def}^{n} \text{ of } g \circ f \\ &= g(f(a) * f(b)) && : f \text{ is OP map.} \\ &= g(f(a)) \times g(f(b)) && : g \text{ is OP map.} \\ &= (g \circ f)(a) \times (g \circ f)(b) && : \text{def}^{n} \text{ of } g \circ f\end{aligned}$$

Thus $g \circ f$ is an OP map.

(b.) Proof: Suppose f^{-1} is a function. Then $f^{-1}(f(x)) = x$ for each $x \in A$ and $f(f^{-1}(y)) = y$ for each $y \in B$.

Let $y, z \in B$ and consider

$$\begin{aligned}f^{-1}(y * z) &= f^{-1}(f(a) * f(b)) && : \exists a, b \in A \text{ such that } f(a) = y \text{ and } f(b) = z \text{ as } f \text{ must be onto for } f^{-1} \text{ to be a function.} \\ &= f^{-1}(f(a \cdot b)) && \leftarrow \text{used } f \text{ is OP map} \\ &= a \cdot b \\ &= f^{-1}(y) \cdot f^{-1}(z)\end{aligned}$$

Thus f^{-1} is an OP map.

§6.4 #8a Show $\text{Conj}: (\mathbb{C}, +) \to (\mathbb{C}, +)$ is OP preserving where $a+ib \in \mathbb{C}$ and $\text{Conj}(a+ib) = a - ib$

Let $z, w \in \mathbb{C}$ then $\exists\ a, b, c, d \in \mathbb{R}$ such that $z = a+ib$, $w = c+id$.

$$\begin{aligned}\text{Conj}(z+w) &= \text{Conj}(a+ib+c+id) \\ &= \text{Conj}(a+c+i(b+d)) \\ &= a+c-i(b+d) \\ &= a-ib+c-id \\ &= \text{Conj}(z) + \text{Conj}(w).\end{aligned}$$

Thus $\text{Conj}: \mathbb{C} \to \mathbb{C}$ is OP map w.r.t. $(+)$.

§6.5 #1a Is $\mathbb{N}$ with it's usual operations a ring?

$\mathbb{N}$ is not a ring for the following reason:
0 is the additive identity for $\mathbb{N}$ yet $n \geq 1$ has additive inverse $-n$ $(n + (-n) = 0)$. Clearly $-n \leq -1 \Rightarrow -n \notin \mathbb{N}$. In other words, $\mathbb{N}$ is <u>not</u> an Abelian group w.r.t. addition.

(there's no problem with the multiplicative axioms here and it is the case that $\mathbb{Z}$ is a ring. In fact, the integers are the quintessential model for a ring)

§6.5 #1d Let $R = \{ bi \mid b \in \mathbb{Z} \}$ is this a ring under the natural operations? [$ai + bi \equiv (a+b)i$ and see ✱

R is an Abelian group since $\forall\, ai, bi, ci \in R$ $(a, b, c \in \mathbb{Z})$,

(a.) $0 = 0i \in R$ and $ai + 0i = 0i + ai = ai$.

(b.) for every $ai \in R$, $\exists\, -ai \in R$ and $ai - ai = 0 = -ai + ai$.

(c.) $ai + (bi + ci) = (a+b+c)i = (ai + bi) + ci$

(skipped some detail here, the reason c holds is because $\mathbb{Z}$ has $(a+b)+c = a+(b+c)$ $\forall\, a, b, c \in \mathbb{Z}$.

(d.) $ai + bi = bi + ai = (a+b)i$

✱ <u>Multiplication</u>: $(ai) \cdot (bi) = ab\, i^2 = -ab \notin R$ thus R is not a Ring if we use this as the multiplication.

However, if we define $(ai) * (bi) \equiv (ab)i$ then note:

$$ai * (bi * ci) = ai * (bc\, i) = (abc)i = ai * (bc\, i) = ai * (bi * ci)$$

Thus $*$ is associative. Then,

$$ai * (bi + ci) = ai * ((b+c)i) = a(b+c)i = (ab + ac)i = ai * bi + ai * ci$$

(The problem is ambiguous since the operations on R are not given!)
Clearly $(R, +, \cdot)$ not a ring YET $(R, +, *)$ is a ring.

§6.5 #3 Complete proof of Th^m 6.17 which says that $(\mathbb{Z}_m, +_m, \cdot_m)$ is a ring. Show that

$$(\bar{b} +_m \bar{c}) \cdot_m \bar{a} = (\bar{b} \cdot_m \bar{a}) +_m (\bar{c} \cdot_m \bar{a})$$

~~$\forall a, b, c \in \mathbb{Z}$~~. I disagree with text, $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$

Proof: Recall the definitions. $\bar{a} = \bar{b}$ iff $m \mid (a-b)$, and

$\bar{a} +_m \bar{b} \equiv \overline{a+b}$ whereas $\bar{a} \cdot_m \bar{b} = \overline{ab}$

($+_m$: addition in $\mathbb{Z}_m$; $+$: addition in $\mathbb{Z}$; $\cdot_m$: multiplication in $\mathbb{Z}_m$; $\cdot$: multiplication in $\mathbb{Z}$.)

Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$,

$$\begin{aligned}
(\bar{b} +_m \bar{c}) \cdot_m \bar{a} &= \overline{b+c} \cdot_m \bar{a} && : \text{def}^n \text{ of } +_m, \\
&= \overline{(b+c)a} && : \text{def}^n \text{ of } \cdot_m, \\
&= \overline{ba + ca} && : \text{properties of } \mathbb{Z}, \\
&= \overline{ba} +_m \overline{ca} && : \text{def}^n \text{ of } +_m, \\
&= (\bar{b} \cdot_m \bar{a}) +_m (\bar{c} \cdot_m \bar{a}) && : \text{def}^n \text{ of } \cdot_m.
\end{aligned}$$

§6.5 #4 Define $\oplus$ and $\otimes$ on $\mathbb{Z} \times \mathbb{Z}$ as follows: $\forall a, b, c, d \in \mathbb{Z}$

$(a,b) \oplus (c,d) \equiv (a+c, b+d)$ & $(a,b) \otimes (c,d) \equiv (ac, bd)$. Prove that $R = (\mathbb{Z}^2, \oplus, \otimes)$ forms a ring

Abelian Group w.r.t. $\oplus$: Let $a, b, c, d, f, g \in \mathbb{Z}$.

1.) $(0,0) \oplus (a,b) = (a,b) \oplus (0,0) = (a,b)$. We have $0 \in R$.

2.) for every $(a,b) \in \mathbb{Z}^2$, $(-a,-b) \in \mathbb{Z}^2$ and $-(a,b) = (-a,-b)$ has $(a,b) \oplus (-(a,b)) = (a,b) \oplus (-a,-b) = (0,0)$ and $(-(a,b)) \oplus (a,b) = (-a,-b) \oplus (a,b) = (0,0)$. Additive Inv.

3.) $(a,b) \oplus ((c,d) \oplus (f,g)) = (a,b) \oplus (c+f, d+g) = (a+c+f, b+d+g)$

$((a,b) \oplus (c,d)) \oplus (f,g) = (a+c, b+d) \oplus (f,g) = (a+c+f, b+d+g)$

thus $\oplus$ is associative

§6.5 #4 Continued

4.) $(a,b)\oplus(c,d) = (a+c, b+d) = (c+a, d+b) = (c,d)\oplus(a,b)$

thus $\oplus$ is commutative.

Multiplicative properties of R

1.) $(a,b)\otimes[(c,d)\otimes(f,g)] = (a,b)\otimes(cf, dg)$
$= (acf, bdg)$
$= (ac, bd)\otimes(f,g)$
$= [(a,b)\otimes(c,d)]\otimes(f,g)$

thus $\otimes$ is associative.

2.) $(a,b)\otimes[(c,d)\oplus(f,g)] = (a,b)\otimes(c+f, d+g)$
$= (a(c+f), b(d+g))$
$= (ac+af, bd+bg)$
$= (ac, bd)\oplus(af, bg)$
$= [(a,b)\otimes(c,d)]\oplus[(a,b)\otimes(f,g)]$

Likewise we can show
$[(a,b)\oplus(c,d)]\otimes(f,g) = [(a,b)\otimes(f,g)]\oplus[(c,d)\otimes(f,g)]$
thus $\oplus$ and $\otimes$ have the need distributive properties and we conclude $(\mathbb{Z}^2, \oplus, \otimes)$ is a RING.

Remark: Clearly $(a,b)\otimes(c,d) = (ac, bd) = (c,d)\otimes(a,b)$ $\forall (a,b),(c,d)\in\mathbb{Z}^2$ thus we can call $\mathbb{Z}^2$ a commutative ring (the "commutative" refers to the multiplication since it is assumed $\forall$ rings that addition is commutative)

Remark: $(1,1)\otimes(a,b) = (a,b) = (a,b)\otimes(1,1)$ $\forall (a,b)\in\mathbb{Z}^2$.
What does this mean? What can we say about $\mathbb{Z}^2$?

§6.5 # 7b Let $a, b, c \in R$ show $(-a)\cdot b = -(a\cdot b)$

We must be careful to use only the axioms of R. Each step should be justified. Consider, for all $a, b \in R$,

$$\begin{aligned} a\cdot b + (-a)\cdot b &= (a+(-a))\cdot b && : \text{ by dist. prop. of } R \\ &= 0\cdot b && : -a \text{ is additive inverse.} \\ &= 0 && : \text{part (a) of Th}^{m}(6.19) \end{aligned}$$

Likewise,

$$\begin{aligned} (-a)\cdot b + a\cdot b &= (-a+a)\cdot b && : \text{ dist. prop. of } R. \\ &= 0\cdot b && : -a+a = 0. \\ &= 0 && : \text{part (a) of Th}^{m}(6.19) \end{aligned}$$

Thus, $(-a)\cdot b = -(a\cdot b)$ since the calculations above demonstrate it is the additive inverse of $a\cdot b$.

Remark: I'd like to ask a few easy questions about integral domains and fields. However, ~~I~~ the questions I'd like in the text. I'll let lecture cover it.