Debra Griffin
Math 210A
HW #10
3.2 #3, 5, 6, 7, 8, 10, 12, 13 + Worksheet #3 – 8
Hand in #3.12

Textbook Problems:

1. Read and study section 3.2 on your own.

3.3 (i) If R is a domain and $a \in R$ satisfies $a^2 = a$, prove that either $a = 0$ or $a = 1$.

Proof:

Assume R is an integral domain $\forall\ a \in R, a^2 = a$. Then $a^2 - a = a(a-1) = 0$.

Since R is an integral domain, then either $a = 0$ or $a = 1$.

(ii) Show that the commutative ring $\mathcal{F}(\mathbb{R})$ in Example 3.7 (Let $\mathcal{F}(\mathbb{R})$ be the set of all the functions $\mathbb{R} \to \mathbb{R}$ equipped with the operations of pointwise addition and pointwise multiplication: Given $f, g \in \mathcal{F}(\mathbb{R})$, define functions $f+g$ and fg by $f+g : a \mapsto f(a) + g(a)$ and $fg : a \mapsto f(a)g(a)$.) contains infinitely many elements $f \neq 0, 1$ with $f^2 = f$.

Proof:

Let $f_n(a) = \begin{cases} 1 : a \in nZ \\ 0 : \text{otherwise} \end{cases}$.

Then $\forall n \in \mathbb{N}, f_n^2 = f$, $\{f_n\}_{n \in \mathbb{N}} \subseteq \mathcal{F}(\mathbb{R})$ and $\{f_n\}_{n \in \mathbb{N}}$ contains infinitely many elements.

3.5 Show that $U(\mathbb{Z}_m) = \{[k] \in \mathbb{Z}_m : (k, m) = 1\}$.

Proof:

Let $m \in \mathbb{Z}$. Let $T = \{[k] \in \mathbb{Z}_m : (k, m) = 1\}$.

Let $[x] \in U(\mathbb{Z}_m)$. Then $\exists\ [y] \in U(\mathbb{Z}_m)$ such that $[x] \bullet [y] = [xy] = [1]$.

$\therefore\ xy \equiv 1 \pmod{m}$, hence $xy - 1 = rm$ for some integer r.

$\therefore\ xy - rm = 1$.

Suppose $(x, m) = d$. Then $x = sd$ and $m = td$ for some integers s, t.

So then $xy - rm = sdy - rtd = d(sy - rt) = 1$. $\therefore\ d = 1$, hence $[x] \in T$.

And this gives us $U(\mathbb{Z}_m) \subseteq T$.

Let $[w] \in T$. Then $(w, m) = 1$.

$\therefore\ \exists\ s, t \in \mathbb{Z}$ such that $ws + tm = 1$,

$\Rightarrow ws - 1 = -tm$,

$\Rightarrow ws \equiv 1 \pmod{m}$,

$\Rightarrow [ws] = [1]$,

$\Rightarrow [w] \bullet [s] = [1]$.

$\therefore\ [w] \in U(\mathbb{Z}_m)$.

Hence $T \subseteq U(\mathbb{Z}_m)$.

So, finally, we have $U(\mathbb{Z}_m) = T$.

3.6 Find all the units in the commutative ring $\mathcal{F}(\mathbb{R})$ defined in Example 3.7.

$U\mathcal{F}(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) : \forall\, a \in \mathbb{R}, f(a) \neq 0\}$.

Proof:

Let $f \in U(\mathcal{F}(\mathbb{R}))$.

Then $\forall\, a \in \mathbb{R}, \exists\, (f(a))^{-1} \neq 0$, such that $f(a)(f(a))^{-1} = 1$.

$\therefore\ \forall\, a \in \mathbb{R}, f(a) \neq 0$, hence $f \in \{f \in \mathcal{F}(\mathbb{R}) : \forall\, a \in \mathbb{R}, f(a) \neq 0\}$.

Thus $U\mathcal{F}(\mathbb{R}) \subseteq \{f \in \mathcal{F}(\mathbb{R}) : \forall\, a \in \mathbb{R}, f(a) \neq 0\}$.

Let g $\in \{f \in \mathcal{F}(\mathbb{R}) : \forall\, a \in \mathbb{R}, f(a) \neq 0\}$.

Then since $g: \mathbb{R} \to \mathbb{R}$, then $\forall\, a \in \mathbb{R}, \exists\, (g(a))^{-1} \neq 0$, such that $g(a)(g(a))^{-1} = 1$.

Thus, $g \in U(\mathcal{F}(\mathbb{R}))$, hence $\{f \in \mathcal{F}(\mathbb{R}) : \forall\, a \in \mathbb{R}, f(a) \neq 0\} \subseteq U\mathcal{F}(\mathbb{R})$.

$\therefore\ U\mathcal{F}(\mathbb{R}) = \{f \in \mathcal{F}(\mathbb{R}) : \forall\, a \in \mathbb{R}, f(a) \neq 0\}$.

3.7 Generalize the construction of $\mathcal{F}(\mathbb{R})$ to arbitrary commutative rings R: Let $\mathcal{F}(R)$ be the set of all functions from R to R, with pointwise addition, $f + g : r \mapsto f(r) + g(r)$, and pointwise multiplication, $fg: r \mapsto f(r)g(r)$ for $r \in R$.

(i) Show that $\mathcal{F}(R)$ is a commutative ring.

Proof:

(1) The function $f = 0_{\mathcal{F}(R)}$ where $f(r) = 0_R\ \forall\, r \in R$, is the additive identity for $\mathcal{F}(R)$.

(2) Let $f, g \in \mathcal{F}(R)$. Since $f(r), g(r) \in R\ \forall\, r \in R$, then $f(r) + g(r) \in$ R.

Thus $f + g \in \mathcal{F}(R)$. And we have closure under addition.

(3) Let $f, g, h \in \mathcal{F}(R)$. Since R is associative under addition, then

$f(r) + (g(r) + h(r)) = (f(r) + g(r)) + h(r)\ \forall\, r \in R$, then $f + (g + h) = (f + g) + h$. Thus, $\mathcal{F}(R)$ is associative under addition.

(4) And since R is commutative under addition, then

$f(r) + g(r) = g(r) + f(r)\ \forall\, r \in R$, then $f + g = g + f$. Thus, $\mathcal{F}(R)$ is commutative under addition.

(5) Since $\forall\, r \in R, \exists\, -r$ such that $r + -r = 0_R$, then $\forall\, f \in \mathcal{F}(R)$,

$f(r) + -f(r) = 0_R\ \forall\, r \in R$, hence $f + -f = 0_{\mathcal{F}(R)}$. Thus, each element of $\mathcal{F}(R)$ has an additive inverse.

(6) Since $f(r), g(r) \in R\ \forall\, r \in R$, then $f(r)g(r) \in$ R.

Thus $fg \in \mathcal{F}(R)$. And we have closure under multiplication.

(7) Since R is associative under multiplication, then

$f(r)(g(r)h(r)) = (f(r)g(r))h(r)\ \forall\, r \in R$, then $f(gh) = (fg)h$. Thus, $\mathcal{F}(R)$ is associative under multiplication.

(8) Since R is commutative under multiplication, then

$f(r)g(r) = g(r)f(r)\ \forall\, r \in R$, then $fg = gf$. Thus, $\mathcal{F}(R)$ is commutative under multiplication.

(9) Since the distributive law holds in R, then
$f(r)(g(r)+h(r)) = f(r)g(r)+f(r)h(r)\ \forall\ r \in R$, then $f(g+h) = fg+fh$. Thus the distributive law holds in $\mathcal{F}(R)$.

$\therefore$ $\mathcal{F}(R)$ satisfies all the axioms of a commutative ring.

(ii) Show that $\mathcal{F}(R)$ is not a domain.

Proof:
Let $f(r) = \begin{cases} r : r \neq 0 \\ 0 : r = 0 \end{cases}$ and $g(r) = \begin{cases} r : r = 0 \\ 0 : r \neq 0 \end{cases}$. Then $f \neq 0_{\mathcal{F}(R)}$ and $g \neq 0_{\mathcal{F}(R)}$, but $fg = 0_{\mathcal{F}(R)}$.

$\therefore$ $\mathcal{F}(R)$ is not a domain.

(iii) Show that $\mathcal{F}(\mathbb{Z}_2)$ has exactly four elements, and that $f+f=0$ for every $f \in \mathcal{F}(\mathbb{Z}_2)$.

Proof:
$\mathbb{Z}_2 = \{[0], [1]\}$.
By the fundamental counting principle, there are $2 \bullet 2$ possible maps from $\mathbb{Z}_2$ to $\mathbb{Z}_2$.
Specifically, $\mathcal{F}(\mathbb{Z}_2) = \{f_1, f_2, f_3, f_4\}$ where
$f_1 = \{([0], [0]), ([1], [1])\}$
$f_2 = \{([0], [1]), ([1], [0])\}$
$f_3 = \{([0], [0]), ([1], [0])\}$
$f_4 = \{([0], [1]), ([1], [1])\}$

3.8 (i) If R is a domain and S is a subring of R, then S is a domain.

Proof:
Let R be a domain and S be a subring of R.
Let $a, b \in S$ such that $a \neq 0_S$ and $b \neq 0_S$. Since $a, b \in R$ then $ab \in R$ and $ab \neq 0_R$. Since S is a subring of R, then $0_S = 0_R$. $\therefore$ $ab \neq 0_S$. $\therefore$ S is a domain.

(ii) Prove that $\mathbb{C}$ is a domain, and conclude that the ring of Gaussian integers is a domain.

Proof:
We know $\mathbb{C}$ is a ring with the usual addition and multiplication (easily verified), so we only need to verify $\mathbb{C}$ is a domain.
Let $a + bi, c + di \in \mathbb{C}$ where $a, b, c, d \in \mathbb{R}$ and $(a + bi)(c + di) = 0$. Then
$ac - bd + (ad + bc)i = 0$. Thus,
$ac - bd = 0$ and $ad + bc = 0$, which gives us
$ac = bd$ and $ad = -bc$. So, by substitution, we have
$d^2 = -c^2$ or $a^2 = -b^2$.
Since $a, d \in \mathbb{R}$, then this can only be true if $d = c = 0$ or $a = b = 0$.

3.10 (i) Prove that $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a domain.

Proof:
It is easily verified that R is a ring under the usual addition and multiplication, so we will only show that R is a domain.
Let $a + b\sqrt{2}, c + d\sqrt{2} \in R$ such that
$(a + b\sqrt{2})(c + d\sqrt{2}) = 0$. Then
$ac + 2bd + (ad + bc)\sqrt{2} = 0$. Thus,
$ac + 2bd = 0$ and $ad + bc = 0$, which gives us
$ac = -2bd$ and $ad = -bc$. So, by substitution, we have
$c^2 = 2d^2$ or $a^2 = 2b^2$.
Since $a, b, c, d \in \mathbb{Z}$, then this can only be true if $d = c = 0$ or $a = b = 0$.
$\therefore a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$., hence R is a domain.

(ii) Prove that $R = \{\frac{1}{2}(a + b\sqrt{2}) : a, b \in \mathbb{Z}\}$ is not a domain.

Proof:
Let a, b, c, d be odd integers. Then
$\frac{1}{2}(a + b\sqrt{2})\frac{1}{2}(c + d\sqrt{2}) = \frac{1}{4}(ac + 2bd) + \frac{1}{4}(ad + bc)\sqrt{2}$.
Since a, c are odd, then by simple number theory, $ac + 2bd$ is odd.
Thus $\frac{1}{4}(ac + 2bd)$ cannot be written as $\frac{1}{2}k$ where k is an integer.
$\therefore$ R is not closed under multiplication, hence R is not a ring, and ergo R is not a domain.

(iii) Using the fact that $\alpha = \frac{1}{2}(1 + \sqrt{-19})$ is a root of $x^2 - x + 5$, prove that
$R = \{a + b\alpha : a, b \in \mathbb{Z}\}$ is a domain.

Proof:
The ring axioms for addition, multiplicative identity, closure under multiplication, and distributive law can be easily shown. So, we will only show R is a domain.
Let $a + b\alpha, c + d\alpha \in R$ such that $(a + b\alpha)(c + d\alpha) = 0$.
$(a + b\alpha)(c + d\alpha) = bd\alpha^2 + (ad + bc)\alpha + ac = 0$.
Since $\alpha = \frac{1}{2}(1 + \sqrt{-19})$ is a root of $x^2 - x + 5$, then $bd\alpha^2 + (ad + bc)\alpha + ac = 0 \Rightarrow$
$bd = 1$, $ad + bc = -1$, and $ac = 5$ or $bd = 0$, $ad + bc = 0$, and $ac = 0$.
Since a, b, c, d are integers, then if $bd = 1$ we have $b = d = 1$. Hence $ad + bc = a + c = -1$.
So then, $a(-a - 1) = 5$, a contradiction to $a \in \mathbb{Z}$.
$\therefore bd = 0$, $ad + bc = 0$, and $ac = 0$.
If $b \neq 0$, then $d = 0$, hence $ad + bc = bc = 0$, which implies that $c = 0$.
If $d \neq 0$, then $b = 0$, hence $ad + bc = ad = 0$, which implies that $a = 0$.
$\therefore a + b\alpha = 0$ or $c + d\alpha = 0$.
$\therefore R = \{a + b\alpha : a, b \in \mathbb{Z}\}$ is a domain.

3.12 (i) If R is a commutative ring, define the circle operation $a \circ b$ by

$$a \circ b = a + b - ab.$$

Prove that the circle operation is associative and that $0 \circ a = a$ for all $a \in R$.

Proof:

Let $a, b, c \in R$. Then, since R is a commutative ring where $(-1)a = -a \ \forall \ a \in R$, we have

$$\begin{aligned}(a \circ b) \circ c &= a \circ b + c - (a \circ b)c \\ &= a + b - ab + c - (a + b - ab)c \\ &= a + b + (-1)ab + c + (-1)(ac + bc + (-1)abc) \\ &= a + b + (-1)ab + c + (-1)(ac) + (-1)(bc) + (-1)(-1)(abc) \\ &= a + b + c + (-1)(bc) + (-1)ab + (-1)(ac) + (-1)(-1)(abc) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + (b \circ c) - a(b \circ c) \\ &= a \circ (b \circ c)\end{aligned}$$

$\therefore$ The circle operation is associative.

And since $0 \bullet a = a \bullet 0 = 0$ for each $a \in R$, we have

$0 \circ a = 0 + a - 0 \bullet a = a + (-1) \bullet 0 = a + 0 = a$.

(ii) Prove that a commutative ring R is a field if and only if $\{r \in R: r \neq 1\}$ is an Abelian group under the circle operation.

Hint. If $a \neq 0$, then $a + 1 \neq 1$.

Proof:

Let $T = \{r \in R: r \neq 1\}$.

$\Rightarrow$: Assume R is a field. We will show T is an Abelian group.

(1) To show closure under $\circ$, let $a, b \in T$, then $a \neq 1$ and $b \neq 1$.

Suppose $a \circ b = a + b - ab = 1$. Then $b - ab = 1 - a \Rightarrow b(1 - a) = 1 - a \Rightarrow b = \dfrac{1 - a}{1 - a} = 1$.

But this is clearly a contradiction as $b \neq 1$. $\therefore a \circ b \neq 1$. $\therefore a \circ b \in T$.

(2) To show associativity under $\circ$, note that since R is a field and $T \subseteq R$, we have by part (i), T is associative under $\circ$.

(3) To show commutativity under $\circ$, let $a, b \in T$.

Since R is commutative under $+$ and $\bullet$, then $a \circ b = a + b - ab = b + a - ba = b \circ a$, hence T is commutative under $\circ$.

(4) To show existence of an identity, 0 under $\circ$, note that by commutativity of T and by result of part (i), we have $0 \circ a = a \circ 0 = a, \forall \ a \in T$.

(5) To show existence of an inverse for each element of T under $\circ$, let $a \in T$.

If $a = 0$, then a is its own inverse. So, assume $a \neq 0$.

Since $a \in T$, then $a \neq 1$, hence $1 - a \neq 0$.

We have $(1 - a)^{-1} \in R$ (as R is a field) and $(-a)(1 - a)^{-1} \in T$ (as $(-a)(1 - a)^{-1} \neq 1$).

Since $a \circ \dfrac{-a}{1-a} = a + \dfrac{-a}{1-a} - a \bullet \dfrac{-a}{1-a} = a + \dfrac{-a + a^2}{1-a} = a + \dfrac{a(a-1)}{1-a} = a + \dfrac{-a(a-1)}{a-1} = 0$, then each element $a \in T$ has an inverse in T under $\circ$.

3.12 (ii) (continued)
⇐: Assume R is a commutative ring and $T = \{r \in R: r \neq 1\}$ is an Abelian group under the circle operation.
Let $x \in R$ such that $x \neq 0$. Then $x + 1 \neq 1$, hence $x + 1 \in T$.
Since T is an Abelian group under $\circ$, then $\exists\ y \in T$ such that $0 = (x + 1) \circ y$.
$\therefore\ 1 = (x + 1) \circ y + 1 = x + 1 + y - (xy + y) = x(y - 1)$.
Since $y \in T$, then $y \neq 1$, hence $y - 1 \neq 0$. $\therefore$ x is a unit in R.
$\therefore$ Every nonzero element of R is a unit, hence R is a field.

3.13 Find the inverses of the nonzero elements of $\mathbb{Z}_{11}$.

$\mathbb{Z}_{11} = \{[0]. [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]\}$.
$[1] \bullet [1] = [1]$, hence $[1]^{-1} = [1]$.
$[2] \bullet [6] = [12] = [1]$, hence $[2]^{-1} = [6]$ and $[6]^{-1} = [2]$.
$[3] \bullet [4] = [12] = [1]$, hence $[3]^{-1} = [4]$ and $[4]^{-1} = [3]$.
$[5] \bullet [9] = [45] = [1]$, hence $[5]^{-1} = [9]$ and $[9]^{-1} = [5]$.
$[7] \bullet [8] = [56] = [1]$, hence $[7]^{-1} = [8]$ and $[8]^{-1} = [7]$.
$[10] \bullet [10] = [100] = [1]$, hence $[10]^{-1} = [10]$.

Worksheet Problems:

---

3. Prove that in a ring with unity, $U(R) \cap ZD(R) = \varnothing$.

Proof:
We will prove the result by contradiction. Suppose $U(R) \cap ZD(R) \neq \varnothing$.
Then $\exists\ x \in U(R)$ such that $x \in ZD(R)$.
Thus, $\exists\ y \in R$ such that $xy = yx = 1$ and $\exists\ z \in R$ such that $z \neq 0$ but $xz = 0$.
From this we have $1 = xy = xy + 0 = xy + xz = x(y + z)$.
Therefore, $y = y \bullet 1 = y(x(y + z)) = (yx)(y + z) = 1 \bullet (y + z) = y + z$.
And since $z \neq 0$, then we have a contradiction.
$\therefore$ $U(R) \cap ZD(R) = \varnothing$.

---

4. Let R be a ring and let $a \in R$. Prove that if $a \neq 0$ and $a \notin ZD(R)$, then $ab = ac$ implies $b = c$ and $ba = ca$ for all $b, c \in R$.

Proof:
Let $a \in R$ such that $a \neq 0$ and $a \notin ZD(R)$.
Let $b, c \in R$ such that $ab = ac$. Then $0 = ab - ac = a(b - c)$.
Since $a \neq 0$ and $a \notin ZD(R)$, then $b - c = 0$.
This gives us that $b = c$, hence $ba = ca$.

---

5. Prove that every finite integral domain is a field.

Proof:
Let R be a finite integral domain.
Since R is a commutative ring with identity, we need only show that for each nonzero element, a, in R, a is a unit.
Since R is finite, then $R = \{a_1, a_2, \ldots, a_n\}$ for some natural number n.
Suppose $a_t \neq 0$ for some $t \in \{1, 2, \ldots, n\}$.
Consider the products $a_t a_1, a_t a_2, \ldots, a_t a_n$. If $a_i \neq a_j$, then $a_t a_i \neq a_t a_j$.
Thus, $a_t a_1, a_t a_2, \ldots, a_t a_n$ are distinct elements of R.
And since there are n of them, then they are all of the elements of R.
Since $1 \in \{a_t a_1, a_t a_2, \ldots, a_t a_n\}$, then for some $j \in \{1, 2, \ldots, n\}$, $a_t a_j = 1$.

---

6. Let R be a ring in which $x^2 = x$ for all $x \in R$. (Such a ring is called a Boolean ring.) Prove that R is a commutative ring.

Proof:
Let $x, y \in R$. Then $x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$
$\Rightarrow 0 = x + x$
$\Rightarrow x = -x$.
And $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$
$\Rightarrow 0 = xy + yx = -xy + yx$
$\Rightarrow xy = yx$.
$\therefore$ R is commutative.

---

7. Find all subrings of $\mathbb{Z}$. (Compare to problem # 9 in book.)

The subrings of $\mathbb{Z}$ are $\{0\}, \{n\mathbb{Z} : n \in \mathbb{N}\}$.

Proof:
We know $\{0\}$ is a subring of any ring, R, so we will show
(1) $n\mathbb{Z}$ is a subring of $\mathbb{Z}$, $\forall\ n \in \mathbb{N}$ and
(2) $\forall\ T \subseteq \mathbb{Z}$ such that $T \neq n\mathbb{Z}\ \forall\ n \geq 0$, T is not a subring of $\mathbb{Z}$.
(1) Let $n \in \mathbb{N}$. Let $a, b \in$ Z. Then $na - nb = n(a - b) \in n\mathbb{Z}$ (as $a - b \in \mathbb{Z}$).
And $na \bullet nb = n(anb) \in n\mathbb{Z}$ (as $anb \in \mathbb{Z}$). And since $0 \in n\mathbb{Z}$ then $n\mathbb{Z} \neq \varnothing$.
$\therefore$ $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.
(2) Let $T \subseteq \mathbb{Z}$ such that $T \neq n\mathbb{Z}\ \forall\ n \geq 0$.
Consider $Y = \{|a - b| : a, b \in T$, such that $a \neq b\}$.
Then by the well-ordering principle, Y has a least element h.

---

8. Find an example of a ring with elements a and b such that a and b are zero divisors, but $a + b \neq 0$ and $a + b$ is not a zero divisor.

In $\mathbb{Z}_6$, [2] and [3] are zero divisors, but [2] + [3] = [5] is not a zero divisor and [5] ≠ [0].
