Debra Griffin
Math 210A
HW #11 Ch 3.4 #41, 42, 44, 45, 49, 50 (i), (ii), 51

Textbook Problems:

3.40 Let R be a commutative ring and let $\mathcal{F}(R)$ be the subring consisting of all functions $f: R \to R$ with pointwise operations.

(i) Show that R is isomorphic to the subring of $\mathcal{F}(R)$ consisting of all the constant functions.

Proof:

Let T be the subring of $\mathcal{F}(R)$ consisting of all the constant functions.
Let $r \in R$ and let
$f_r : R \to R$ be defined by $f_r(x) = r \ \forall \ x \in R$. Let
$\varphi: R \to T$ be defined by $\varphi(r) = f_r$.
Since $\forall \ x \in R$, $\varphi(a + b) = f_{a+b}(x) = a + b = f_a(x) + f_b(x)$, and
$\varphi(ab) = f_b(x) = a + b = f_a(x) + f_b(x)$, then φ is a homomorphism under + and •.
To show φ is injective, let $a, b \in R$ such that $\varphi(a) = \varphi(b)$ and note that
$\forall \ x \in R$, $a = f_a(x) = f_b(x) = b$.
To show φ is surjective, let $y \in T$ and note that $y = f_y = \varphi(y)$ where y in R.

(ii) If $f(x) \in R[x]$, let
$\varphi_f: R \to R$ be defined by $r \mapsto f(r)$
[thus, φ_f is the polynomial function associated to $f(x)$]. Show that the function
$\varphi: R[x] \to \mathcal{F}(R)$, defined by
$\varphi(f(x)) = \varphi_f$, is a ring homomorphism.

Proof:

Let $f, g \in R[x]$. Then $\varphi(f + g) = \varphi_{f+g} = \{(r, (f + g)(r)) | \ r \in R\}$
$= \{(r, (f(r) + g(r)) | \ r \in R\} = \{(r, f(r)) + (r, g(r)) | \ r \in R\} = \varphi_f + \varphi_g = \varphi(f) + \varphi(g)$.
And, similarly, $\varphi(fg) = \varphi_{fg} = \varphi_f \varphi_g = \varphi(f)\varphi(g)$.
$\therefore$ φ is a ring homomorphism.

(iii) Show that φ is injective if R is an infinite field.

Proof:

Assume R is an infinite field. Let $f, g \in R[x]$ such that $\varphi(f) = \varphi(g)$. Then $\varphi_f = \varphi_g$. Thus $\forall \ r \in R, f(r) = g(r)$. Assume, without loss of generality, $\deg f(x) \geq \deg g(x)$ and let $h(x) = f(x) - g(x)$. If $h(x) \neq 0$, then $\deg h(x) = n$ for some integer $n \geq 0$. By Theorem 3.25 (If k is a field, $f(x) \in k[x]$, $\deg f(x) = n$, then $f(x)$ has at most n roots in k.), $h(x)$ has at most n roots. However, $\forall \ r \in R, h(r) = f(r) - g(r) = 0$. Thus every element of R is a root of h and R is an infinite field. But this contradicts that $h(x)$ has at most n roots.
$\therefore$ $h(x) = 0$. $\therefore f(x) = g(x)$, hence φ is injective.

3.41 Let I and J be nonzero ideals in a commutative ring R. If R is a domain, prove that $I \cap J \neq \{0\}$.

Proof:
Since I and J are nonzero ideals, then $\exists\ a \in I, a \neq 0$, and $b \in J, b \neq 0$.
Thus, $ab \neq 0$ as $a, b \in r$ and R is a domain.
Since $b \in R \Rightarrow ab \in I$ and $a \in R \Rightarrow ab \in J$, then $I \cap J \neq \{0\}$.

3.42 Let R be a commutative ring. Show that the function ε: $R[x] \to R$, defined by ε: $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mapsto a_0$, is a homomorphism. Describe ker ε in terms of roots of polynomials.

Proof:
We first show that ε is a ring homomorphism.
Let $f, g \in R[x]$. Then $f = f_0 + f_1x + f_2x^2 + \cdots + f_nx^n$ for some $f_0, f_1, \ldots, f_n \in R$, and $g = g_0 + g_1x + g_2x^2 + \cdots + g_nx^n$ for some $g_0, g_1, \ldots, g_n \in R$.
Since R is commutative, we have
$\varepsilon(f + g) = \varepsilon(f_0 + g_0 + (f_1 + g_1)x + \cdots + (f_n + g_n)x^n) = f_0 + g_0 = \varepsilon(f) + \varepsilon(g)$.
And $\varepsilon(fg) = \varepsilon\left(\sum_{i=0}^{n}\left(\sum_{j+k=i} f_j g_k\right)x^i\right) = f_0g_0 = \varepsilon(f)\varepsilon(g)$.
$\therefore$ ε is a ring homomorphism.
To describe ker ε in terms of roots of polynomials, we note that
ker $\varepsilon = \{f \in R[x]: \varepsilon(f) = f(0) = 0\}$. $\therefore$ $\forall\ f \in R[x]$ such that 0 is a root of $f, f \in \ker \varepsilon$.

3.44 (i) Prove that F, the field with 4 elements (see Exercise 3.14 on page 125: $\mathbb{F}_4 = \{\begin{bmatrix} a & b \\ b & a+b \end{bmatrix} | \ a, b \in \mathbb{Z}_2\}$), and $\mathbb{Z}_4$ are not isomorphic commutative rings.

Proof:
Suppose φ: $F \to \mathbb{Z}_4$ is an isomorphism.
Let $F = \{0_F, 1_F, a, b\}$. where $0_F = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $1_F = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $a = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.
By simple calculations we have $ab = 1_F$. $\therefore$ $\varphi(ab) = \varphi(1_F) = 1_{\mathbb{Z}4}$.
But only $1_{\mathbb{Z}4} \bullet 1_{\mathbb{Z}4} = 1_{\mathbb{Z}4}$ and $3 \bullet 3 = 1_{\mathbb{Z}4}$, contradicting that $a \neq b$.
$\therefore$ φ is not an isomorphism.

(ii) Prove that any two fields having exactly four elements are isomorphic.
Hint. First prove that $1 + 1 = 0$, and then show that the nonzero elements form a cyclic group of order 3 under multiplication.

Proof:
Let F be a field of order 4. Then $F = \{0, 1, a, b\}$ where 1, a, and b are units.
We have $ab = 1$ (otherwise $ab = a$ or $ab = b$, causing $b = 1$ or $a = 1$, a contradiction).
Thus, $a^2 = b$ and $b^2 = a$, as $ab = 1$ rules out $a^2 = 1$ or $b^2 = 1$ (inverses are unique).
So we can rewrite $F = \{0, 1, a, b\}$ as $F = \{0, 1, a, a^2\}$. This gives us that, under multiplication, $U(F) = \langle a \rangle$ where $\langle a \rangle$ is a cyclic group of order 3.
Since F is a group under addition, then there is a group isomorphism, $F \cong \mathbb{Z}_4$ or F $\cong \boldsymbol{V}_4$ by Proposition 2.89, (Every group G of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\boldsymbol{V}_4$. Moreover, $\mathbb{Z}_4$ and $\boldsymbol{V}_4$ are not isomorphic.)
However, by Proposition 3.12 (The commutative ring $\mathbb{Z}_m$ is a field if and only if m is prime.) $\therefore$ $\mathbb{Z}_4$ is not a field.
So, we shall assume that there is a group isomorphism, $F \cong \boldsymbol{V}_4 = \{e, a, b, c\}$ where e is the additive identity and $a + a = b + b = c + c = e$.
And, by simple calculations, we can see that the multiplication table for $\mathbb{F}_4 = \{\begin{bmatrix} a & b \\ b & a+b \end{bmatrix} \mid a, b \in \mathbb{Z}_2\}$ matches the multiplication for F as described above, and the addition table for $\mathbb{F}_4$ matches that of $\boldsymbol{V}_4$.
Thus, we can establish an isomorphism
$\varphi: F \to \mathbb{F}_4$ defined by $\varphi(0_F) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\varphi(1_F) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\varphi(a) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, and $\varphi(a^2) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.
$\therefore$ Any two fields having exactly four elements are isomorphic to $\mathbb{F}_4$with multiplication defined as above.

3.45 (i) Show that every element $a \in \mathbb{Z}_p$ has a p^{th} root (i.e. there is $b \in \mathbb{Z}_p$ with $a = b^p$).

Proof:
(I think we must assume p is prime. A quick check shows $2 \neq a^4$ for any $a \in \mathbb{Z}_4$.)
We first note that $0^p = 0$ and $1^p = 1$.
Assume p is prime. Then $U(\mathbb{Z}_p) = \mathbb{Z}_p - \{0\} = \{a_1, a_2, \ldots, a_{p-1}\}$, a multiplicative group of order $p - 1$.
By corollary to Lagrange's Theorem, $\forall\ a_i \in U(\mathbb{Z}_p)$, $(a_i)^{p-1} = 1$.
Thus, $(a_i)^{p-1}a_i = (a_i)^p = a_i$.
$\therefore$ Every element $a \in \mathbb{Z}_p$ has a p^{th} root.

3.45 (ii) Let k be a field that contains $\mathbb{Z}_p$ as a subfield [e.g. $k = \mathbb{Z}_p(x)$]. For every positive integer n, show that the function φ_n: $k \to k$, given by $\varphi(a) = a^{p^n}$, is a ring homomorphism.

Proof:
Let p be a prime.
We first note that the unity $1 \in \mathbb{Z}_p$ is the same as the unity of k (as $ab = 1_{Z_p}$ for some $a, b \in \mathbb{Z}_p$, and $ac = 1_k$ for some $c \in k \Rightarrow ac = (1_{Z_p} a)c = 1_{Z_p}(ac) = abac = 1_{Z_p} \bullet 1_k = 1_{Z_p}$).
Secondly, note that $\forall\ a \in \mathbb{Z}_p, pa = 0$ (by corollary to Lagrange's theorem).
Since p is prime, then p is the smallest positive integer such that $p \bullet 1 = 0$.
Thirdly, note that $\forall\ b \in k, pb = p \bullet 1 \bullet b = 0 \bullet b = 0$. Thus the characteristic of k is p.
Also, note that for $\forall\ n > 0,\ j \neq 0$ and $j \neq p^n, p \mid p^n! = \binom{p^n}{j} j!(p^n - j)!$. This gives us that

$\forall\ a, b \in k, \varphi(a + b) = (a + b)^{p^n} =$
$\sum_{j=0}^{p^n} \binom{p^n}{j} a^{p^n - j} b^j = (a + b)^{p^n} = a^{p^n} + 0 + \ldots + 0 + b^{p^n} = \varphi(a) + \varphi(b).$
as the only terms of which are not divisible by p^n are a^{p^n} and b^{p^n}.
Also, $\forall\ a, b \in k, \varphi(ab) = (ab)^{p^n} = (a)^{p^n}(b)^{p^n} = \varphi(a)\varphi(b)$. $\therefore$ φ_n is a ring.

3.49 (i) If R and S are commutative rings, show that their direct product $R \times S$ is also a commutative ring, where addition and multiplication in $R \times S$ are defined "coordinatewise": $(r, s) + (r', s') = (r + r', s + s')$ and $(r, s)(r', s') = (rr', ss')$.

Proof:
Let (r, s), (r', s'), and $(r'', s'') \in R \times S$.
(1) $(r, s) + (r', s') = (r + r', s + s') \in R \times S$ (since R and S are closed under addition).
(2) $(r, s) + [(r', s') + (r'', s'')] = (r, s) + (r' + r'', s' + s'') = (r + r' + r'', s + s' + s'')$ and
$[(r, s) + (r', s')] + (r'', s'') = (r + r', s + s') + (r'', s'') = (r + r' + r'', s + s' + s'')$
(since R and S are associative under addition).
(3) $(r, s) + (r', s') = (r + r', s + s') = (r' + r, s' + s) = (r', s') + (r, s)$
(since R and S are commutative under addition).
(4) $(r, s) + (0_R, 0_S) = (r + 0_R, s + 0_S) = (r, s). = (0_R + r, 0_S + s) = (0_R, 0_S) + (r, s)$.
(5) $(r, s) + (-r, -s) = (r + (-r), s + (-s)) = (0_R, 0_S) = ((-r) + r, (-s) + s) = (-r, -s) + (r, s)$
(since r and s have additive inverses, $-r$ and $-s$ in R and S respectively).
(6) $(r, s) \bullet (r', s') = (rr', ss') \in R \times S$ (since R and S are closed under multiplication).
(7) $(r, s) \bullet [(r', s') \bullet (r'', s'')] = (r, s) \bullet (r'r'', s's'') = (rr'r'', ss's'')$ and
$[(r, s) \bullet (r', s')] \bullet (r'', s'') = (rr', ss') \bullet (r'', s'') = (rr'r'', ss's'')$
(since R and S are associative under multiplication).
(8) $(r, s) \bullet [(r', s') + (r'', s'')] = (r, s) \bullet (r' + r'', s' + s'') = (rr' + rr'', ss' + ss'')$ and
$(r, s) \bullet (r', s') + (r, s) \bullet (r'', s'') = (rr', ss') + (rr'', ss'') = (rr' + rr'', ss' + ss'')$
(since the distributive law holds in both R and S).
(9) $(r, s) \bullet (r', s') = (rr', ss') = (rr', ss') = (r', s') \bullet (r, s)$
(since R and S are commutative under multiplication).
$\therefore$ $R \times S$ is a commutative ring.

(ii) Show that if m and n are relatively prime, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as rings.
Hint. See Theorem 2.81.

Proof:
By Theorem 2.81, we have that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as groups. Thus, we only need to show $\forall\, a, b \in \mathbb{Z}, f(ab) = f(a)f(b)$ where $f: \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $f(x) = ([x]_m, [x]_n)$.
$f(ab) = ([ab]_m, [ab]_n) = ([a]_m, [a]_n)([b]_m, [b]_n) = f(a)f(b)$.
$\therefore\ \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as rings.

(iii) Show that if neither R nor S is the zero ring, then $R \times S$ is not a domain.

Proof:
Since R $\neq \{0\}$ and S $\neq \{0\}$, then $\exists\ r \in R$ and $s \in S$ such that $r \neq 0$ and $s \neq 0$.
Thus $(r, 0) \in R \times S$, $(0, s) \in R \times S$, $(r, 0) \neq (0, 0)$ and $(0, s) \neq (0, 0)$.
However, $(r, 0)(0, s) = (0, 0)$. Thus $R \times S$ is not a domain.

(iv) Show that $R \times \{0\}$ is an ideal in $R \times S$.

Proof:
Let $(r, s) \in R \times S$, and $(a, 0) \in R \times \{0\}$, then $(r, s)(a, 0) = (ra, 0) \in R \times \{0\}$ (as $ra \in R$).

(v) Show that $R \times \{0\}$ is a ring isomorphic to R, but it is not a subring of $R \times S$.

Proof:
Define φ: $R \to R \times \{0\}$ by $\varphi(r) = (r, 0)$.
Then φ is a bijection and we have that
$\forall\, a, b \in$ R, $\varphi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \varphi(a) = \varphi(b)$
and $\varphi(ab) = (ab, 0) = (a, 0)(b, 0) = \varphi(a)\varphi(b)$.
$\therefore\ R \times \{0\}$ is a ring isomorphic to R,
However, if $0 \neq 0_S$, then $R \times \{0\}$ is not even a subset of $R \times S$, hence cannot be a subring of $R \times S$.

3.50 (i) If R and S are nonzero commutative rings, prove that $U(R \times S) = U(R) \times U(S)$, where $U(R)$ is the group of units of R.

Proof:
Let $(x, y) \in U(R \times S)$, then $\exists\ (w, z) \in R \times S$ such that $(x, y)(w, z) = (xw, yz) = (1_R, 1_S)$.
Thus, $xw = 1$ and $yz = 1$ where $w \in R$ and $z \in S$.
So x is a unit in R and y is a unit in S, hence $(x, y) \in U(R) \times U(S)$.
$\therefore\ U(R \times S) \subseteq U(R) \times U(S)$.
Let $(a, b) \in U(R) \times U(S)$, then $\exists\ c \in$ R and $d \in$ S such that $ac = 1_R$ and $bd = 1_S$.
So then $(a, b)(c, d) = (1_R, 1_S)$. Thus, (a, b) is a unit in $R \times S$,
hence $U(R) \times U(S) \subseteq U(R \times S)$.
$\therefore\ U(R \times S) = U(R) \times U(S)$.

3.50 (ii) Redo Exercise 2.65 on page 94 using part (i) (Prove $U(\mathbb{Z}_{15}) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$).

Proof:
By Theorem 2.81 (If m and n are relatively prime, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ as groups), thus $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$. By part (i), $U(\mathbb{Z}_3 \times \mathbb{Z}_5) = U(\mathbb{Z}_3) \times U(\mathbb{Z}_5)$.
Since $U(\mathbb{Z}_3) = \{1, 2\}$ is a multiplicative group of order 2, then $U(\mathbb{Z}_3) \cong \mathbb{Z}_2$.
And since $U(\mathbb{Z}_5) = \{1, 2, 3, 4\}$ is a multiplicative group of order 4 in which $\circ(3) = 4$ and V_4 has no element of order 4, then $U(\mathbb{Z}_5) \cong \mathbb{Z}_4$.
Thus, $U(\mathbb{Z}_{15}) \cong U(\mathbb{Z}_3 \times \mathbb{Z}_5) = U(\mathbb{Z}_3) \times U(\mathbb{Z}_5) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

3.51 Let F be the set of all 2×2 real matrices of the form $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. Prove that F is a field (with operations matrix addition and matrix multiplication), and prove that there is an isomorphism $\varphi: F \to \mathbb{C}$ with $\det(A) = \varphi(A)\overline{\varphi(A)}$.
Hint. Define $\varphi: F \to \mathbb{C}$ by $\varphi(A) = a + ib$.

Proof:
Let $A, C \in F$ such that $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $C = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$.
Then $A + C = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} = C + A \in F$. And $AC = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} = CA \in F$.
This gives us that F is closed under addition and multiplication and commutative.
The zero matrix, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in F$ and the identity matrix, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in F$.
If $A \neq 0_F$ and $X = \begin{bmatrix} a/(a^2+b^2) & -b/(a^2+b^2) \\ b/(a^2+b^2) & a/(a^2+b^2) \end{bmatrix}$, then $AX = 1_F$.
$\therefore$ F is a field.
Define $\varphi: F \to \mathbb{C}$ by $\varphi(A) = a + ib$.
To show φ is injective, let $A, C \in F$ (as defined above) such that $\varphi(A) = \varphi(C)$.
Then $a + ib = c + id$. $\Rightarrow$ $a = c$ and $b = d \Rightarrow A = C \Rightarrow \varphi$ is injective.
To show φ is surjective, let $y \in \mathbb{C}$. Then $y = w + iz$ for some real numbers w, z.
$\therefore$ $\exists\ W = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \in F$ such that $\varphi(W) = x + iy = y$.
To show φ is a homomorphism, define arbitrary elements A and C as above and note that
$\varphi(A + C) = a + c + i(b + d) = a + ib + c + id = \varphi(A) + \varphi(C)$ and
$\varphi(AC) = ac - bd + i(ad + bc) = (a + ib)(c + id) = \varphi(A)\varphi(C)$.
$\therefore$ φ is an isomorphism.
Lastly, we note that $\det(A) = a^2 + b^2 = (a + ib)(a - ib) = \varphi(A)\overline{\varphi(A)}$, as desired.

Worksheet Problems

2. Recall that an element in a ring is called idempotent if $a^2 = a$. Prove that in a commutative ring of characteristic 2, the set of idempotents forms a subring.

Proof:
Let R be a commutative ring of characteristic 2. Let $T = \{a \in R \mid a^2 = a\}$.
First, note that $0^2 = 0$, so $0 \in T$, hence $T \neq \varnothing$.
Let $a, b \in T$. Then $(a - b)^2 = a^2 - 2ab + b^2 = a^2 + b^2$, since char $(R) = 2$.
And $a^2 + b^2 = a + b = a - b + b + b = a - b + 2b = a - b \in T$.
Also $(ab)^2 = abab = a^2b^2 = ab \in T$.
$\therefore$ T is a subring of R.

---

3. Let F be a finite field with n elements. Prove that $x^{n-1} = 1$ for all nonzero x in F.

Proof:
First, note that $F - \{0\}$ is a multiplicative group with identity 1_F and $|F - \{0\}| = n - 1$.
By corollary to Lagrange's theorem, $\forall\, x \in F - \{0\}$, $x^{n-1} = 1$, as desired.

---

4. Let R be a ring with unity and let I be an ideal in R.
(a) Prove $I = R$ if and only if I contains an element of $U(R)$.

Proof:
Assume $I = R$. Let $r \in U(R)$. Since $U(R) \subseteq R = I$, then $r \in I$.
Conversely, assume I contains an element, x, of $U(R)$. Then $\exists\, y \in R$ such that $xy = 1$.
Since I is an ideal and $y \in R$, then $xy = 1 \in I$. $\therefore$ $\forall\, r \in R$, $1r = r \in R$. Thus, $R \subseteq I$.
By definition, $I \subseteq R$, thus $I = R$.

(b) Prove that if R is a field, then R has exactly two ideals.

Proof:
Let R be a field. We know $\{0\}$ is an ideal of R, so suppose $I \neq \{0\}$ is an ideal of R.
Let $a \in I$ where $a \neq 0$. Since R is a field, then a is a unit in R. By part (a), $I = R$.
$\therefore$ $\{0\}$ and R are the 2 and only 2 ideals of R.

---

4. (c) Show that a homomorphism from a field onto a ring with more than one element must be an isomorphism.

Proof:
Let F be a field. Let T be a ring with more than one element.
Let $\varphi : F \to T$ be an epimomorphism. By Proposition 3.50 (If $f : A \to R$ is a ring homomorphism, then $\ker f$ is an ideal in A…) we know $\ker \varphi$ is an ideal in F.
Since F is a field, then by part (b), $\ker \varphi = \{0\}$ or $\ker \varphi = F$.
If $\ker \varphi = \{0\}$, then φ is an injection and we are done.
If $\ker \varphi = F$, then $T = \{0\}$, a contradiction to our assumption that T is a ring with more than one element. $\therefore$ $\ker \varphi = \{0\}$, hence φ is a bijection.
