Debra Griffin
Math 210A
HW #13 Ch 3.2 #17, Ch 3.4 #29, Ch 3.5 #46, 47, 48(i)

3.17 (i) Show that $F = \{a + bi\colon a, b \in \mathbb{Q}\}$ is a field.

Proof:
Since $F \subseteq \mathbb{C}$, and $\mathbb{C}$ is a field, then we know + and • are well-defined, associative and commutative and $1, 0 \in F$. We only need to show closure under + and • and the existence of • inverses for each element in F.
Let $w, z \in F$. Then $w = a + bi$ and $z = c + di$ for some $a, b, c, d \in \mathbb{Q}$.
Since $w + z = a + bi + c + di = a + c + (b + d)i$ where $a + c, b + d \in \mathbb{Q}$, and
$wz = (a + bi)(c + di) = ac - bd + (ad + bc)i$ where $ac - bd, ad + bc \in \mathbb{Q}$, then
$w + z, wz \in \mathbb{Q}$. Thus, F is closed under + and •.
Since $(a + bi)(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i) = 1 + 0i$, and $a^2 + b^2 \neq 0$, then each element of F has a multiplicative inverse.
$\therefore$ F is a field.

(ii) Show that F is the fraction field of the Gaussian integers.

Proof:
Let $x \in F$. Then for some $a, b \in \mathbb{Q}$ where $a = p/q$ and $b = r/s$ where $p, q, r, s \in \mathbb{Z}$ such that $q \neq 0$ and $s \neq 0$, we have $x = a + bi = \frac{p}{q} + \frac{r}{s}i = \frac{ps + rqi}{qs + 0i}$. Since $ps, rq, qs \in \mathbb{Z}$, then $ps + rqi, qs + 0i \in \text{Frac}(\mathbb{Z}[i])$. So $F \subseteq \text{Frac}(\mathbb{Z}[i])$.
Let $y \in \text{Frac}(\mathbb{Z}[i])$. Then for some $a, b, c, d \in \mathbb{Z}$, where c and d are not both 0, we have that $y = \frac{a + bi}{c + di} = \frac{ac - bd + (ad + bc)i}{c^2 + d^2} = \frac{ac - bd}{c^2 + d^2} + \frac{ad + bc}{c^2 + d^2}i$.
Since $c^2 + d^2 \neq 0$, then $y \in F$. So $\text{Frac}(\mathbb{Z}[i]) \subseteq F$.
$\therefore$ $F = \text{Frac}(\mathbb{Z}[i])$, as desired.

3.29 Let R be a domain. If $f(x) \in R[x]$ has degree n, prove that $f(x)$ has at most n roots in R. Hint. Use Frac (R).

Proof:

Let $f(x) \in R[x]$ with degree n, then $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_i \in R$.

Since Frac (R) is a field, then $g(x) = \sum_{i=0}^{n} [a_i, 1]x^i$, $a_i \in R$ has at most n roots in Frac (R).

Suppose $f(x)$ has $n + 1$ roots in R, say $\{\alpha_1, \alpha_2, \ldots, \alpha_{n+1}\}$.

Assume $[\alpha_{n+1}, 1]$ is not a root of $g(x)$. Since $f(\alpha_{n+1}) = \sum_{i=0}^{n} a_i \alpha_{n+1}^i = 0$,

then $g([\alpha_{n+1}, 1]) = \sum_{i=0}^{n} [a_i, 1][\alpha_{n+1}, 1]^i = \sum_{i=0}^{n} [a_i, 1][\alpha_{n+1}^i, 1] = \sum_{i=0}^{n} [a_i \alpha_{n+1}^i, 1] = [0, 1]$, a contradiction to our assumption that $[\alpha_{n+1}, 1]$ is not a root of $g(x)$.

$\therefore$ If $f(x) \in R[x]$ has degree n, prove that $f(x)$ has at most n roots in R.

3.46 If R is a field, show that $R \cong$ Frac (R). More precisely, show that the homomorphism $f: R \to$ Frac (R) in Example 3.45 (i), namely, $r \mapsto [r, 1]$, is an isomorphism.

Proof:

Define $f: R \to$ Frac (R) by $r \mapsto [r, 1]$.

To show f is injective, we note that $\forall\ a \in \ker f, f(a) = [a, 1] = [0, 1]$.

$\therefore$ $\ker f = \{0\}$, hence f is injective.

To show f is surjective, we let $y \in$ Frac (R) and note that

$y = [a, b]$ for some $a, b \in R, b \neq 0$. Since R is a field, then $ab^{-1} \in R$, thus

$[a, b] = [ab^{-1}, 1]$. So $f(ab^{-1}) = y$. $\therefore$ f is surjective.

To show f is a homomorphism, we note that

$f(a + b) = [a + b, 1] = [a, 1] + [b, 1] = f(a) + f(b)$ and

$f(ab) = [ab, 1] = [a, 1][b, 1] = f(a)f(b)$.

$\therefore$ $R \cong$ Frac (R).

3.47 (i) If A and R are domains and $\varphi: A \to R$ is a ring isomorphism, prove that $[a, b] \mapsto [\varphi(a), \varphi(b)]$ is a ring isomorphism Frac $(A) \to$ Frac (R).
Proof:
Define f : Frac $(A) \to$ Frac (R) by $[a, b] \mapsto [\varphi(a), \varphi(b)]$.

To show f is **injective**, we note that

$\forall\ [a, b] \in \ker f, f([a, b]) = [\varphi(a), \varphi(b)] = [0, \varphi(b)]$ where $\varphi(b) \neq 0_A$.

Since φ is an isomorphism, then $[a, b] = [0, b]$ $\therefore$ $\ker f = \{[0, b]\}$, hence f is injective.

To show f is **surjective**, we let $y \in$ Frac (R) and note that

$y = [u, v]$ for some $u, v \in R, v \neq 0$. Since φ is surjective, then $\exists\ a, b \in$ A such that

$\varphi(a) = u$ and $\varphi(b) = v$. So $f([a, b]) = [\varphi(a), \varphi(b)] = [u, v]$. $\therefore$ f is surjective.

To show f is a **homomorphism**, we note that since φ is an isomorphism, we have

$f([a, b] + [c, d]) = f([ad + bc, bd]) = [\varphi(ad + bc), \varphi(bd)] = [\varphi(ad) + \varphi(bc), \varphi(bd)] =$

$[\varphi(a)\varphi(d) + \varphi(b)\varphi(c), \varphi(b)\varphi(d)] = [\varphi(a), \varphi(b)] + [\varphi(c), \varphi(d)] = f([a, b]) + f([c, d])$.

And $f([a, b][c, d]) = f([ac, bd]) = [\varphi(ac), \varphi(bd)] = [\varphi(a)\varphi(c), \varphi(b)\varphi(d)] =$

$= [\varphi(a), \varphi(b)][\varphi(c), \varphi(d)] = f([a, b])\, f([c, d])$.

$\therefore f$ is a homomorphism.

In conclusion, we have that f is an isomorphism.

3.47 (ii) Prove that if a field k contains an isomorphic copy of $\mathbb{Z}$ as a subring, then k must contain an isomorphic copy of $\mathbb{Q}$.

Proof:
We have $\varphi: \mathbb{Z} \to \varphi(\mathbb{Z})$ where $\varphi(\mathbb{Z}) \subseteq$ k is an isomorphism.
Define $f : \mathbb{Q} \to k$ by $f(a/b) = \varphi(a)\varphi(b)^{-1}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$.

To show f is injective, we note that if $x \in \ker f$, then $x = p/q$ where $q \neq 0$ and
$f(p/q) = \varphi(p)\varphi(q)^{-1} = 0$. Since φ is an isomorphism and k is a field,
we have $\varphi(q)^{-1} \neq 0$, thus $\varphi(p) = 0$. And so $p = 0 = x$, hence $\ker f = \{0\}$.
$\therefore$ f is injective.
To show f is a homomorphism, we note that since φ is an isomorphism and k is a field, then for $a/b, c/d \in \mathbb{Q}$ $(a, b, c, d \in \mathbb{Z}, b \neq 0, d \neq 0)$, we have
$f(a/b + c/d) = f((ad + bc)/(bd)) = \varphi(ad + bc)\varphi(bd)^{-1} = [\varphi(ad) + \varphi(bc)]\varphi(bd)^{-1} =$
$\varphi(a)\varphi(d)\varphi(b^{-1})\varphi(d^{-1}) + \varphi(b)\varphi(c)\varphi(b^{-1})\varphi(d^{-1}) = \varphi(a)\varphi(b^{-1}) + \varphi(c)\varphi(d^{-1}) = f(a/b) + f(c/d)$.
And $f(a/b \bullet c/d) = f((ac)/(bd)) = \varphi(ac)\varphi(bd)^{-1} = \varphi(a)\varphi(c)\varphi(b^{-1})\varphi(d^{-1}) = f(a/b)\, f(c/d)$.
$\therefore f$ is a homomorphism.
So, since $f(\mathbb{Q}) \subseteq k$ and $f : \mathbb{Q} \to f(\mathbb{Q})$ is surjective, then $f : \mathbb{Q} \to f(\mathbb{Q})$ is an isomorphism.
$\therefore$ k contains an isomorphic copy of $\mathbb{Q}$.

3.47 (iii) Let R be a domain and let $\varphi: R \to k$ be an injective ring homomorphism, where k is a field. Prove that there exists a unique ring homomorphism Φ: Frac $(R) \to k$ extending φ; that is, $\Phi|R = \varphi$.

Proof:
We have that $\varphi: R \to k$ is an injective ring homomorphism.
Define Φ: Frac $(R) \to k$ by $\Phi([a, b]) = \varphi(a)\varphi(b)^{-1}$. Then

$\Phi([a, b] + [c, d]) = \Phi([ad + bc, bd]) = [\varphi(ad + bc)]\varphi(bd)^{-1} = [\varphi(ad) + \varphi(bc)]\varphi(bd)^{-1} =$

$[\varphi(a)\varphi(d) + \varphi(b)\varphi(c)]\varphi(b)^{-1}\varphi(d)^{-1} = \varphi(a), \varphi(b)^{-1} + \varphi(c), \varphi(d)^{-1} = \Phi([a, b]) + \Phi([c, d])$.

And $\Phi([a, b][c, d]) = \Phi([ac, bd]) = \varphi(ac), \varphi(bd)^{-1} = \varphi(a)\varphi(c), \varphi(b)^{-1}\varphi(d)^{-1} =$

$= [\varphi(a)\varphi(b)^{-1}][\varphi(c)\varphi(d)^{-1}] = \Phi([a, b])\ \Phi([c, d])$.

$\therefore$ Φ is a **homormophism**.

Since $\Phi([r, 1]) = \varphi(r)\varphi(1)^{-1} = \varphi(r)$, then $\Phi|R = \varphi$.

To show **uniqueness**, we suppose $\exists\ \Phi_2$: Frac $(R) \to k$ such that $\Phi_2|R = \varphi$.
Then $\Phi|R = \varphi = \Phi_2|R$.
Since $\Phi([a, b]) = \varphi(a)\varphi(b)^{-1} = \Phi([a, 1])\Phi([b, 1])^{-1} = \Phi([a, 1])\Phi([1, b]) =$
$\Phi_2([a, 1])\Phi_2([1, b]) = \Phi_2([a, 1][1, b]) = \Phi_2([a, b])$, then $\Phi = \Phi_2$.

3.48 R is a domain with fraction field $F =$ Frac (R).
(i) Prove that Frac $(R[x]) \cong F(x)$.

Proof:
Note that

$\forall f \in R[x], f(x) = \sum_{i=0}^{n} a_i x^i, a_i \in R, n \in \mathbb{N}$, and

$\forall\ h \in F[x], h(x) = \sum_{i=0}^{n} [a_i, b_i] x^i, a_i, b_i \in R, b_i \neq 0$.

Define φ : Frac $(R[x]) \to F(x)$ by

$\varphi([f(x), g(x)]) = \varphi([\sum_{i=0}^{n_1} a_i x^i, \sum_{i=0}^{n_2} b_i x^i]) = [\sum_{i=0}^{n_1} [a_i, 1] x^i, \sum_{i=0}^{n_2} [b_i, 1] x^i]$.

To show φ is **injective**, note that if $[f(x), g(x)] = [\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{n} b_i x^i] \in \ker \varphi$, then

$[\sum_{i=0}^{n} [a_i, 1] x^i, \sum_{i=0}^{n} [b_i, 1] x^i] = 0_{F(x)}$. Thus, $\sum_{i=0}^{n} [a_i, 1] x^i = 0_{F[x]}$. So $\sum_{i=0}^{n} a_i x^i = 0_{R[x]}$.

$\therefore \ker \varphi = \{0_{R[x]}\}$, hence φ is injective.

3.48 (i) (continued)

To show φ is **surjective**, let $[h(x), j(x)] = [\sum_{i=0}^{n}[a_i,b_i]x^i, \sum_{i=0}^{n}[c_i,d_i]x^i]$, and let

$r = \prod_{i=0}^{n_1} b_i$ where $b_i = 1$ if $a_i = 0$, and $s = \prod_{i=0}^{n_2} d_i$ where $d_i = 1$ if $c_i = 0$.

Then $[rs \bullet h(x), rs \bullet j(x)] \in \text{Frac}(R[x])$ and $\varphi([rs \bullet h(x), rs \bullet j(x)]) =$

$[rs \bullet \sum_{i=0}^{n}[a_i,b_i]x^i, rs \bullet \sum_{i=0}^{n}[c_i,d_i]x^i] = [\sum_{i=0}^{n}[a_i,b_i]x^i, \sum_{i=0}^{n}[c_i,d_i]x^i]$.

To show φ is a **homomorphism**, we will simplify our notation to

$\varphi([f, g]) = [f', g']$ where $\varphi([f, g]) = \varphi([f(x), g(x)]) = [\sum_{i=0}^{n}[a_i, 1]x^i, \sum_{i=0}^{n}[b_i, 1]x^i] = [f', g']$.

Note that $(fg)' = (\sum_{i=0}^{n_1} a_i x^i \bullet \sum_{i=0}^{n_2} b_i x^i)' = (\sum_{i=0}^{n_p} \sum_{i=j+k} a_j b_k x^i)' = \sum_{i=0}^{n_p} \sum_{i=j+k} [a_j b_k, 1]x^i =$

$\sum_{i=0}^{n_p} \sum_{i=j+k} [a_j, 1][b_k, 1]x^i = \sum_{i=0}^{n_1}[a_i, 1]x^i \bullet \sum_{i=0}^{n_2}[b_i, 1]x^i = f'g'$ (where $n_p = \max(n_1, n_2)$).

And $(f+g)' = (\sum_{i=0}^{n_1} a_i x^i + \sum_{i=0}^{n_2} b_i x^i)' = (\sum_{i=0}^{n_p}(a_i + b_i)x^i)' = \sum_{i=0}^{n_p}([a_i + b_i, 1])x^i =$

$\sum_{i=0}^{n_p}([a_i, 1] + [b_i, 1])x^i = = \sum_{i=0}^{n_1}[a_i, 1]x^i + \sum_{i=0}^{n_2}[b_i, 1]x^i = f' + g'$ (where $n_p = \max(n_1, n_2)$).

So $\varphi([f, g] + [h, j]) = \varphi[fj + hg, gj] = [(fj + hg)', (gj)'] = [f'j' + h'g', g'j'] =$
$[f', g'] + [h', j'] = \varphi([f, g]) + \varphi([h, j])$.
And $\varphi([f, g][h, j]) = \varphi[fh, gj] = [(fh)', (gj)'] = [f'h', g'j'] = [f', g'][h', j'] =$
$\varphi([f, g])\varphi([h, j])$.
∴ φ is a homomorphism.
In conclusion, $\text{Frac}(R[x]) \cong F(x)$.