4 Applications of Fraction Rings

Throughout this assignment, R will denote a *commutative* ring.

2/1: **4.1.** Let R be a ring, and let $f \in R$ be an element which is not a zero divisor. Recall that we defined $R_f = D^{-1}R$ for $D = \{1, f, f^2, \dots\}$. Prove that

$$R_f \cong R[X]/(fX - 1)$$

using the universal property of the ring of fractions.

Proof. Herein, let $\bar{g}$ denote $g + (fX - 1)$ for any $g \in R[X]$, and let S denote $R[X]/(fX - 1)$.

To prove that $R_f \cong R[X]/(fX-1)$, i.e., that $D^{-1}R \cong S$, it will suffice to construct an isomorphism $\tilde{\varphi} : D^{-1}R \to S$. Per Lecture 2.2, we may define a canonical injection $i : R \to R[X]$ and a canonical surjection $\pi : R[X] \to S$.

We now prove that the restriction $\pi|_R$ of π to $R \cong i(R) \subset R[X]$ is injective. Suppose $\pi|_R(a) = \pi|_R(b)$ for $a, b \in R$. Then $\bar{a} = \bar{b}$, so $a \in \bar{b}$. But since $\deg(a) = 0$ and b is the only element of $\bar{b}$ of degree 0, we must have $a = b$, as desired.

It follows that we may define an injective ring homomorphism $\varphi : R \to S$ by $\varphi = \pi|_R \circ i$. More explicitly, for any $a \in R$, we have that

$$\varphi(a) = (\pi|_R \circ i)(a) = \pi(i(a)) = \pi(a) = \bar{a}$$

We now wish to demonstrate that $\varphi(D) \subset S^\times$. We divide into two cases ($1 \in D$ and $f^n \in D$). Naturally $1 \in D$, which maps to $\bar{1} \in S$ since φ is a ring homomorphism, is a unit. To prove that every f^n maps to a unit in $S^\times$, we induct on n. For the base case $n = 1$, we have that

$$\begin{aligned}
\overline{fX - 1} &= \bar{0} \\
\bar{f}\bar{X} - \bar{1} &= \bar{0} \\
\bar{f}\bar{X} &= \bar{1} \\
\varphi(f) \cdot \bar{X} &= \bar{1}
\end{aligned}$$

Thus, $\varphi(f) \in S^\times$ by definition, as desired. Now suppose inductively that $\varphi(f^{n-1}) \in S^\times$; we wish to demonstrate that $\varphi(f^n) \in S^\times$. By the induction hypothesis, there exists $\bar{b} \in S$ such that $\varphi(f^{n-1}) \cdot \bar{b} = \bar{1}$. Therefore,

$$\begin{aligned}
\varphi(f^n) \cdot \overline{bX} &= \varphi(f)\varphi(f^{n-1})\bar{b}\bar{X} \\
&= \varphi(f)\bar{1}\bar{X} \\
&= \varphi(f)\bar{X} \\
&= \bar{1}
\end{aligned}$$

as desired, where we use the base case to get from the next-to-last line to the last line above.

At this point, we have proven that $\varphi : R \to S$ is an injective ring homomorphism such that $\phi(D) \subset S^\times$. Thus, we have by the universal property of rings of fractions that there exists a unique injective ring homomorphism $\tilde{\varphi} : D^{-1}R \to S$ such that $\tilde{\varphi} \circ \iota = \varphi$.

To verify that $\tilde{\varphi}$ is surjective, let $\bar{g} \in S$ be arbitrary, where $g \in R[X]$. Since R is a subring of $D^{-1}R$, we may consider $g \in D^{-1}R[X]$. In particular, we will be interested in $(1/f)g \in D^{-1}R[X]$ and $X - 1/f \in D^{-1}R[X]$. Applying the Euclidean algorithm to the latter monic polynomial generates $q, r \in D^{-1}R[X]$ such that $(1/f)g = q(X - 1/f) + r$ and, since $\deg(r) < \deg(X - 1/f) = 1$, $r \in D^{-1}R$. It follows that $g = q(fX - 1) + rf$, so $\tilde{\varphi}(rf) = \overline{rf} = \bar{g}$ for $rf \in D^{-1}R$.

Let d be the denominator of rf. Then $drf \in R$. It follows that $\tilde{\varphi}(drf) = \tilde{\varphi}(\iota(drf)) = \varphi(drf) = \overline{drf}$ so

$$\begin{aligned}
\bar{d} \cdot \overline{rf} &= \tilde{\varphi}(d)\tilde{\varphi}(rf) \\
&= \varphi(d)\tilde{\varphi}(rf) \\
&= \bar{d}\tilde{\varphi}(rf) \\
\overline{rf} &= \tilde{\varphi}(rf) \\
\tilde{\varphi}(rf) &= \bar{g}
\end{aligned}$$

as desired. □

4.2. Let $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$ denote the ring of **Gaussian integers**. Recall from class that $\mathbb{Z}[i]$ is a Euclidean domain with norm $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ defined by $N(a+bi) = a^2 + b^2$.

(a) Let R be a Euclidean domain with norm N which satisfies $N(xy) = N(x)N(y)$ for all $x, y \in R$. Prove that $a \in R$ is a unit iff $N(a) = 1$. (Hint: Start by computing $N(1)$.)

Proof. Taking the hint, we will begin by computing $N(1)$. Since $1 \neq 0$ and N is a positive norm by assumption, $N(1) > 0$. Additionally, since $\mathbb{Z}$ is an integral domain, we can use the cancellation law between the following equations.

$$\begin{aligned}
N(1 \cdot 1) &= N(1) \\
N(1)N(1) &= N(1) \cdot 1 \\
N(1) &= 1
\end{aligned}$$

Having computed $N(1)$, we now begin the argument in earnest.

Suppose first that $a \in R$ is a unit. Then there exists $b \in R$ such that $ab = 1$. It follows that

$$\begin{aligned}
N(ab) &= N(1) \\
N(a)N(b) &= 1
\end{aligned}$$

Thus, $N(a) = \pm 1$, but since $N(a) \in \mathbb{Z}_{\geq 0}$, we must have

$$N(a) = 1$$

as desired.

Now suppose that $N(a) = 1$. Since R is an ED and $a \neq 0$, we know that there exist $q, r \in R$ such that $1 = qa + r$ and $N(a) > N(r)$. But since $N(1) = 1$, we must have $N(r) = 0$ or $r = 0$. Therefore, $1 = qa$, so a is a unit, as desired. □

(b) Using part (a), find the units in $\mathbb{Z}[i]$.

Proof. Let $a + bi \in \mathbb{Z}[i]$ be a unit. Then $1 = N(a+bi) = a^2 + b^2$. The four possible solutions over $\mathbb{Z}$ are $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$. Therefore, the units of $\mathbb{Z}[i]$ are

$$\boxed{\pm 1, \pm i}$$

□

(c) Prove that $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i]$.

Proof. To prove that $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i]$, it will suffice to use a bidirectional inclusion argument. Suppose first that

$$\frac{a+bi}{c+di} \in \mathrm{Frac}(\mathbb{Z}[i])$$

Then by the laws of multiplication on the field of fractions and on $\mathbb{Z}[i]$, we have that

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Since $a+bi, c+di \in \mathbb{Z}[i] = \{\alpha+\beta i \mid \alpha, \beta \in \mathbb{Z}\}$ by the definition of $\text{Frac}(\mathbb{Z}[i])$, we know that $a, b, c, d \in \mathbb{Z}$. Thus,

$$\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$$

and hence

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \in \{\alpha+\beta i \mid \alpha, \beta \in \mathbb{Q}\} = \mathbb{Q}[i]$$

as desired.

Now suppose that

$$\frac{a}{b} + \frac{c}{d}i \in \mathbb{Q}[i]$$

Then by the laws of addition and multiplication on $\mathbb{Q}[i]$ and on $\mathbb{Z}[i]$, we have that

$$\frac{a}{b} + \frac{c}{d}i = \frac{a}{b} + \frac{c}{d}\frac{i}{1} = \frac{a}{b} + \frac{ci}{d1} = \frac{a}{b} + \frac{ci}{d} = \frac{ad+bci}{bd} = \frac{ad+bci}{bd+0i}$$

Since $a/b, c/d \in \mathbb{Q}$, $a, b, c, d \in \mathbb{Z}$. Thus, $ad, bc, bd, 0 \in \mathbb{Z}$ so $ad+bci, bd+0i \in \mathbb{Z}[i]$. Additionally, since $b, d \in \mathbb{Z} \setminus \{0\}$ by hypothesis, $bd+0i \neq 0$ as well. Therefore,

$$\frac{a}{b} + \frac{c}{d}i = \frac{ad+bci}{bd+0i} \in \text{Frac}(\mathbb{Z}[i])$$

as desired. ☐

4.3. (a) For $a, b \in \mathbb{Z}$, prove that $a^2 - 2b^2 = 0$ iff $a = b = 0$.

Proof. For the forward direction, let that $a, b \in \mathbb{Z}$ satisfy $a^2 - 2b^2 = 0$. Suppose for the sake of contradiction that either a or b is nonzero. It follows by the derived equality $a^2 = 2b^2$ that they are both nonzero. Thus, a/b is a well-defined element of $\mathbb{Q}$. However, we have that

$$\begin{aligned} a^2 - 2b^2 &= 0 \\ a^2 &= 2b^2 \\ \frac{a^2}{b^2} &= 2 \\ \frac{a}{b} &= \sqrt{2} \end{aligned}$$

i.e., that a rational number equals an irrational number, a contradiction. Therefore, $a = b = 0$.

For the reverse direction, let $a = b = 0$. Then

$$a^2 - 2b^2 = 0^2 - 2 \cdot 0^2 = 0$$

as desired. ☐

(b) Prove that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[X]/(X^2-2)$ is a field.

Proof. To prove that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[X]/(X^2-2)$ is a field, it will suffice to show that its additive and multiplicative identites are distinct and that every element is a unit. Let's begin.

$\mathbb{Q}[X]/(X^2-2)$ inherits addition and multiplication from $\mathbb{Q}[X]$, except now modulo X^2-1. Thus, the additive and multiplicative identities of $\mathbb{Q}[X]/(X^2-2)$ are the (distinct) images of those in $\mathbb{Q}[X]$ under the relevant canonical surjection.

Now let $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ be arbitrary and nonzero. Then a or b is nonzero. It follows by part (a) that $a^2 - 2b^2 \neq 0$, and hence

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

is well-defined. By the law of multiplication in $\mathbb{Q}[\sqrt{2}]$, it follows that

$$\left(a + b\sqrt{2}\right)\left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right) = \frac{\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)}{a^2 - 2b^2} = \frac{a^2 - b^2\sqrt{2}^2}{a^2 - 2b^2} = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1$$

as desired. Note that as in Q4.1, we can prove that $\sqrt{2}$ is the solution to $X^2 - 2 = 0$, i.e., an object X such that $X^2 = 2$. This is what rigorously allows us to simplify the above equation, not any intuitive or notationally implied notion of $\sqrt{2}$. $\square$

4.4. Let D be a multiplicative subset of an integral domain R. Now R is a subring of $D^{-1}R$. Let J be an ideal of $D^{-1}R$. Put $I = R \cap J$.

(a) Is I an ideal of R?

Proof. $\boxed{\text{Yes}}$ I is an ideal of R.
Since R, J are both additive subgroups of $D^{-1}R$, $R \cap J$ is an additive subgroup of $D^{-1}R$. Additionally, since $R \cap J \subset R$, $R \cap J$ must be an additive subgroup of R.
Now let $x \in I$ and $r \in R$ be arbitrary. Since $x \in I$, $x \in R$ and $x \in J$. It follows from the former statement and the fact that R is an ideal of R that $rx \in R$. It follows from the latter statement and the fact that J is an ideal of $D^{-1}R$ that $rx \in J$. Therefore, $rx \in R \cap J = I$, as desired. $\square$

(b) Prove that if $I \neq R$, then $I \cap D = \emptyset$.

Proof. Suppose for the sake of contradiction that there exists $x \in I \cap D$. Then $x \in I$ and $x \in D$. It follows from the latter statement that $1/x \in D^{-1}R$. It follows from the former statement that $x \in R$ and $x \in J$. Since J is an ideal of $D^{-1}R$ (hence is closed under multiplication by elements of $D^{-1}R$) and $x \in J$, we have in particular that

$$\frac{1}{x} \cdot x = \frac{x}{x} = 1 \in J$$

It follows that $J = D^{-1}R$. Consequently, since $R \subset D^{-1}R$, we have that $I = R \cap D^{-1}R = R$. This contradicts the hypothesis that $I \neq R$. $\square$

(c) Let $b \in J$. Is it true that $b = d^{-1}a$ for some $d \in D$ and $a \in I$?

Proof. $\boxed{\text{Yes}}$ it is true.
Since $b \in J$, we know that $b \in D^{-1}R$. It follows that we may write $b = a/d$ for some $a \in R$ and $d \in D$. Since J is an ideal and $d \in D \subset R \subset D^{-1}R$, we know that $a = db \in J$. Combining the facts that $a \in R$ and $a \in J$, we can determine that $a \in R \cap J = I$, as desired. $\square$

(d) Prove that if I is an ideal in R, then $I^e = \{s^{-1}x \in D^{-1}R \mid s \in D,\ x \in I\}$ is an ideal in $D^{-1}R$.

Proof. To prove that I^e is an ideal, it will suffice to show that $(I^e, +) \leq (D^{-1}R, +)$ and $a/b \cdot x/s \in I^e$ for all $a/b \in D^{-1}R$ and $x/s \in I^e$.
First, we will show that $(I^e, +)$ is a subgroup. By definition, it is a subset of $D^{-1}R$. Since $0 \in I$ and D is nonempty, the identity $0/d \in I^e$. Associativity follows from the containing group. And closure follows from that of I (under multiplication by elements of R and addition) and that of D (under multiplication by elements of D): If $x_1/s_1, x_2/s_2 \in I^e$, then

$$\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{x_1 s_2 + x_2 s_1}{s_1 s_2} \in I^e$$

as desired.

Now we show closure under multiplication. Let $x/s \in I^e$ and $a/b \in D^{-1}R$ be arbitrary. Since $x \in I$ and $a \in R$, $xa \in I$. Since $s, b \in D$, $sb \in D$. Therefore,

$$\frac{x}{s} \cdot \frac{a}{b} = \frac{xa}{sb} \in I^e$$

as desired. ☐

(e) Using part (c), prove that if J is an ideal of $D^{-1}R$, then $J = (R \cap J)^e$. Therefore, we have a surjective map of sets

$$\{\text{Ideals in } R\} \to \{\text{Ideals in } D^{-1}R\}$$

given by $I \mapsto I^e$. Note that the right inverse is given by $J \mapsto R \cap J$. Is this map a bijection?

Proof. To prove that $J = (R \cap J)^e$, we will use a bidirectional inclusion proof. Suppose first that $b \in J$. Then by part (c), $b = d^{-1}a$ for some $d \in D$ and $a \in I$. Therefore, by the definition of $(R \cap J)^e$, $b \in (R \cap J)^e$. Now suppose that $d^{-1}a \in (R \cap J)^e$ Then $a \in R \cap J$, so $a \in J$. It follows since J is an ideal of $D^{-1}R$ and $1/d \in D^{-1}R$ that $a/d = d^{-1}a \in J$, as desired.

$\boxed{\text{No}}$ this map is not a bijection. Counterexample: Let R, D be defined as in Q5. Consider (3). Since $3 \in D$, $1 = 3/3 \in (3)^e$. Thus, $(3)^e = D^{-1}R$. It follows that $\mathbb{Z}^e = (3)^e$ even though $\mathbb{Z} \neq (3)$. ☐

(f) If R is a PID, is $D^{-1}R$ a PID?

Proof. $\boxed{\text{Yes.}}$

Let $J \in D^{-1}R$ be an arbitrary ideal. Per part (e), there exists an ideal $I \subset R$ such that $J = I^e$. Since R is a PID, $I = Ra$ for some $a \in I$. Additionally, as per the definition of the extension map, $a = a/1 \in I^e = J$. We will now prove that $I^e = D^{-1}Ra$. By definition, $D^{-1}Ra \subset I^e$. In the other direction, let $x/s \in I^e$ be arbitrary. Since $x \in I$, $x = ab$ for some $b \in R$. Moreover, $b/s \in D^{-1}R$, so $x/s = (b/s) \cdot a \in D^{-1}Ra$, as desired. ☐

4.5. (a) Let $D = \{n \in \mathbb{Z} : 2 \nmid n\}$. Recall that we defined

$$\mathbb{Z}_{(2)} = D^{-1}R = \{a/b \in \mathbb{Q} : 2 \nmid b\}$$

Write down all of the ideals in $\mathbb{Z}_{(2)}$. You can use the fact that the ideals in $\mathbb{Z}$ are $(n) = n\mathbb{Z}$ for $n \in \mathbb{Z}$, and the previous question. Which of these ideals are maximal? For each maximal ideal $M \in \mathbb{Z}_{(2)}$, what is the field $\mathbb{Z}_{(2)}/M$?

Proof. Since the ideals in $\mathbb{Z}$ are $(n) = n\mathbb{Z}$ for all $n \in \mathbb{Z}$, Q4.4e implies that the set of ideals of $\mathbb{Z}_{(2)}$ is the image of $\{(n) \mid n \in \mathbb{Z}\}$ under $I \mapsto I^e$. However, many of these are equivalent. In particular, if n is divisible by any numbers other than 2, you will be able to multiply n by the product of those numbers to reduce the magnitude of the generator down to a power of 2. Therefore, the set of all ideals in $\mathbb{Z}_{(2)}$ is

$$\boxed{\{(2^n)^e \mid n \in \mathbb{Z}_{\geq 0}\} \cup \{0\}}$$

Among these ideals,

$$\boxed{\text{Only } (2)^e \text{ is maximal.}}$$

To prove this, we will show that every ideal $(n)^e \in \mathbb{Z}_{(2)}$ is either equal to $\mathbb{Z}_{(2)}$ or is contained in $(2)^e$. Let's begin. Let $(n)^e \subset \mathbb{Z}_{(2)}$ be arbitrary. We divide into two cases ($2 \nmid n$ and $2 \mid n$). If $2 \nmid n$, then $n \in D$. It follows by its definition that $1 = n/n \in (n)^e$. Therefore, $(n)^e = R$. If $2 \mid n$, then $n = 2^m \cdot r$ for some $m \geq 1$ and r coprime to 2. Let $a/d \in (n)^e$ be arbitrary. Then $a \in (n)$ and $d \in D$. It follows that $n \mid a$, i.e., that $2 \mid a$. Thus, $a = 2b \in (2)$. Therefore, $a/d \in (2)^e$, so $(n)^e \subset (2)^e$, as desired.

Finally, we will prove that

$$\boxed{\mathbb{Z}_{(2)}/(2)^e \cong \mathbb{Z}/2\mathbb{Z}}$$

To do so, it will suffice to show that for any $a/d \in \mathbb{Z}_{(2)}$, we either have

$$\frac{a}{d} + (2)^e = 0 + (2)^e \qquad\qquad \frac{a}{d} + (2)^e = 1 + (2)^e$$

Since $\mathbb{Z}$ is an ED and $2 \neq 0$, we know that there exist $b, c \in \mathbb{Z}$ such that $a = 2b + c$ and $|c| < |2| = 2$ (i.e., $c \in \{0, \pm 1\}$). We now divide into three cases. If $c = 0$, then $a = 2b$ and hence

$$\frac{a}{d} = \frac{2b}{d} \in (2)^e$$

so $a/d + (2)^e = 0 + (2)^e$. If $c = 1$, then

$$\frac{a}{d} = \frac{1}{d} + \frac{2b}{d}$$

so $a/d \in 1/d + (2)^e$. Additinally, since $2 \nmid d$ by hypothesis, $2 \mid d - 1$ and hence $\pm(d-1)/d \in (2)^e$. It follows that

$$\frac{1}{d} = \frac{1}{d} + \frac{d-1}{d} - \frac{d-1}{d} = 1 + -\frac{d-1}{d} \in 1 + (2)^e$$

Therefore, $a/d \in 1 + (2)^e$, as desired. The case $c = -1$ is analogous to the case $c = 1$. ☐

(b) Let $D = \{2^n \mid n \in \mathbb{Z}_{\geq 0}\}$ and let $R = D^{-1}\mathbb{Z}$. Write down the ideals in R. Which of these ideals are maximal?

Proof. The set of all ideals in R is

$$\boxed{\{(n) : (n, 2) \leq 1\}}$$

By definition, (n) is an ideal in R. Now suppose that I is an arbitrary ideal in R. By Q4.4e and the fact that the ideals of $\mathbb{Z}$ are of the form (n) for some $n \in \mathbb{Z}$, $I = (n)^e$. To verify that $(n)^e = D^{-1}\mathbb{Z}n = (n)$, first let $a/2^m \in (n)^e$. Then since $1/2^m \in R$, $a/2^m = a \cdot (1/2^m) \in (n)$. Now let $na/2^m \in (n)$. Then since $na \in (n)$, $na/2^m \in (n)^e$. Now suppose $(n, 2) > 1$. Then $2 \mid n$ and hence $(n/2)/1 \in (n)$, contradicting the assumption that the generator n is the smallest element of (n).

The maximal ideals in R are the subset of the above consisting of all prime ideals, i.e.,

$$\boxed{\{(n) : n \text{ is prime}\}}$$

We know that every maximal ideal is prime. In the other direction, suppose (n) is a prime ideal. Now suppose for the sake of contradiction that $(n) \subsetneq (m) \subsetneq R$. It follows that $n \in (m)$. Thus, $n = (a/b)m$ for some $a/b \in R$. Consequently, since (n) is a prime ideal, $m \in (n)$ or $a/b \in (n)$. We now divide into two cases. If $m \in (n)$, then $(m) \subset (n)$, a contradiction. If $a/b \in (n)$, then $a/b = n \cdot (c/d)$. Combining this with the result that $n = (a/b)m$, we have that

$$\begin{aligned} n &= \frac{a}{b} \cdot m \\ &= \frac{nc}{d} \cdot m \\ 1 &= \frac{c}{d} \cdot m \end{aligned}$$

But then $1 \in (m)$, and hence $(m) = R$, a contradiction. ☐

4.6. (a) Define $M_2 : \{\text{commutative rings}\} \to \{\text{sets}\}$ by

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \right\}$$

Show that for any R, there is a natural bijection between the set $M_2(R)$ and the set S_1 of ring homomorphisms between $\mathbb{Z}[X, Y, Z, W]$ and R. Note that notationally,

$$S_1 = \mathrm{Hom}_{\mathrm{ring}}(\mathbb{Z}[X, Y, Z, W], R)$$

One sometimes says that $\mathbb{Z}[X, Y, Z, W]$ represents the function M_2.

Proof. Define $\psi : M_2(R) \to S_1$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \mathrm{ev}_{(a,b,c,d)}$$

We know from class that every evaluation function is a ring homomorphism. Thus, $\mathrm{ev}_{(a,b,c,d)}$ does lie in the correct set.

Injectivity: Suppose

$$\psi \left[\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \right] = \psi \left[\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right]$$

Then $\mathrm{ev}_{(a_1,b_1,c_1,d_1)} = \mathrm{ev}_{(a_2,b_2,c_2,d_2)}$. It follows that

$$a_1 = \mathrm{ev}_{(a_1,b_1,c_1,d_1)}(X) = \mathrm{ev}_{(a_2,b_2,c_2,d_2)}(X) = a_2$$

Similar statements hold for b, c, d. Thus, since $x_1 = x_2$ ($x \in \{a, b, c, d\}$), we have that

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

as desired.

Surjectivity: Let $\varphi \in S_1$ be arbitrary. Suppose $\varphi(X) = a$, $\varphi(Y) = b$, $\varphi(Z) = c$, and $\varphi(W) = d$. Since any polynomial in $\mathbb{Z}[X, Y, Z, W]$ is a $\mathbb{Z}$-linear combination of X, Y, Z, W and φ respects these addition and multiplication operations, we have that for any $f \in \mathbb{Z}[X, Y, Z, W]$,

$$\varphi(f) = f(a, b, c, d) = \mathrm{ev}_{(a,b,c,d)}(f)$$

Therefore,

$$\psi \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] = \mathrm{ev}_{(a,b,c,d)} = \varphi$$

as desired. □

(b) (**You do not need to turn in part (b)**, but you are encouraged to think about it.)

Actually, $M_2(R)$ can be naturally given a ring structure: Addition and multiplication are defined using the same procedure as $M_2(\mathbb{R})$ (or with any other field you may have seen). Hence, it makes sense to talk about the units of $M_2(R)$.

Define the set $GL_2(R)$ to be the units of $M_2(R)$, i.e.,

$$GL_2(R) = M_2(R)^\times$$

Show that for any R, there is a natural bijection between $GL_2(R)$ and the set S_2 defined by

$$S_2 = \mathrm{Hom}_{\mathrm{ring}}(\mathbb{Z}[X, Y, Z, W]_{XW-YZ}, R)$$

Note that $\mathbb{Z}[X, Y, Z, W]_{XW-YZ}$ denotes the **localization** of $\mathbb{Z}[X, Y, Z, W]$ by the multiplicative set generated by $XW - YZ$ (that is, the multiplicative set $(1, XW - YZ, (XW - YZ)^2, \dots)$). (Hint: Use the universal property.)

One sometimes says $\mathbb{Z}[X, Y, Z, W]_{XW-YZ}$ represents the function GL_2.

4.7. Let $\mathbb{Q}(X)$ denote the field of fractions of $\mathbb{Q}[X]$. By the universal property of a polynomial ring, we know that giving a ring homomorphism $\varphi : \mathbb{Q}[X] \to \mathbb{R}$ is equivalent to choosing an element $r \in \mathbb{R}$ and setting $\varphi(X) = r$. Which ring homomorphisms $\varphi : \mathbb{Q}[X] \to \mathbb{R}$ extend to ring homomorphisms $\tilde{\varphi} : \mathbb{Q}(X) \to \mathbb{R}$? These ring homomorphisms should satisfy the following commutative diagram.

$$\begin{tikzcd} \mathbb{Q}[X] \arrow[r, "\varphi"] \arrow[d, "X \mapsto X/1"'] & \mathbb{R} \\ \mathbb{Q}(X) \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

Proof. We can prove that the set of ring homomorphisms φ which extend to the field of rational functions over $\mathbb{Q}$ is equal to

$$\boxed{\{\varphi : \varphi(X) \text{ is a real transcendental number}\}}$$

Let φ be an element of the above set. Since $\varphi(X) = r$ is transcendental, $\varphi(f) = \mathrm{ev}_r(f) \neq 0$ for any $f \in \mathbb{Q}[X]$. (Note that a similar argument to the surjectivity one used in Q4.6a can justify that $\varphi = \mathrm{ev}_r$.) It follows that if we extend φ to $\mathbb{Q}(X)$ by keeping the evaluation definition (recall that evaluation is always a ring homomorphism), then for any rational function $f/g \in \mathbb{Q}(X)$,

$$\tilde{\varphi}\left(\frac{f}{g}\right) = \left(\frac{f}{g}\right)(r) = \frac{f(r)}{g(r)}$$

where, as established, $g(r)$ is nonzero and hence $\tilde{\varphi}(f/g)$ is well-defined.

Now suppose that $\varphi : \mathbb{Q}[X] \to \mathbb{R}$ is a ring homomorphism that extends to a ring homomorphism $\tilde{\varphi} : \mathbb{Q}(X) \to \mathbb{R}$. Let $\tilde{\varphi}(X) = \varphi(X) = r$. Then as per Q4.6a, $\tilde{\varphi} = \mathrm{ev}_r$. Since $\tilde{\varphi}$ is a ring homomorphism, $\tilde{\varphi}(f/g)$ is well-defined for every $f \in \mathbb{Q}[X]$ and $g \in \mathbb{Q}[X] - \{0\}$. In particular, we must have $0 \neq \tilde{\varphi}(g) = \mathrm{ev}_r(g) = g(r)$ for all such g. It follows by definition that r is a real transcendental number. □

4.8. F is a field. Let R be the smallest subring of $F[X]$ such that (a) $F \subset R$ and (b) both X^2 and X^3 belong to R.

(a) Use the identity $(X^2)^3 = (X^3)^2$ to deduce that R is *not* a UFD.

Proof. Suppose for the sake of contradiction that X^2 is reducible. Then $X^2 = ab$ where $a, b \notin R^\times = F^\times$. It follows since they aren't units that $\deg(a), \deg(b) \geq 1$. But since $\deg(a) + \deg(b) = \deg(ab) = 2$, it must be that $\deg(a) = \deg(b) = 1$. Thus, $a = c_1X + d_1$ and $b = c_2X + d_2$. It follows that

$$\begin{aligned} X^2 &= ab \\ 1X^2 + 0X + 0 &= c_1c_2X^2 + (c_1d_2 + c_2d_1)X + d_1d_2 \end{aligned}$$

so

$$c_1c_2 = 1 \qquad\qquad d_1d_2 = 0$$

Then $c_1, c_2 \in R^\times = F^\times$ and $d_1 = d_2 = 0$. It follows that $X = c_1c_2X \in R$, and hence $R = F[X]$ by the construction from Lecture 1.2. However, this contradicts the hypothesis that R is the smallest subring of $F[X]$ containing F, X^2, X^3 since $F + (X^2, X^3)$ is an example of a smaller subring of $F[X]$ containing F, X^2, X^3. Therefore, X^2 is irreducible in R.

A similar argument can show that X^3 is irreducible in R.

It follows that two factorizations of X^6 are $(X^2)^3$ and $(X^3)^2$. But since these factorizations have different lengths, they are not equivalent. Therefore, R is not a UFD, as desired. □

(b) Exhibit an ideal I of R that is not a principal ideal.

Proof. Take

$$\boxed{I = (X^2, X^3)}$$

Since both generators are irreducible by part (a), their greatest common divisor is necessarily a unit. Thus, since (X^2, X^3) only consists of polynomials of degree greater than or equal to 2 (i.e., objects that are not units), no element of it can generate both extant generators. Therefore, $(2, X)$ is not principal. □

4.9. Mimic Euclid's proof of the infinitude of primes in $\mathbb{Z}$ to show that $F[X]$ has infinitely many primes for every field F.

Proof. Suppose for the sake of contradiction that $\{f_1, \dots, f_r\}$ is the set of all primes in $F[X]$. Since $F[X]$ is an ED, it is a PID. Thus, the primes and irreducibles coincide. Likewise, $F[X]$ being an ED makes it a UFD. Thus, the element $f_1 \cdots f_r + 1$ (for example) has a unique factorization in terms of $f_1, \dots, f_r$. In particular, since each f_i irreducible and hence not a unit, $\deg(f_i) \geq 1$ ($i = 1, \dots, r$). This means that $\deg(f_1 \cdots f_r + 1) \geq r$ so $f_1 \cdots f_r + 1$ is not a unit. It follows that there exists at least one f_i such that $f_i \mid f_1 \cdots f_r + 1$. Additionally, $f_i \mid f_1 \cdots f_r$. Thus, $f_i \mid f_1 \cdots f_r + 1 - f_1 \cdots f_r = 1$. Therefore, f_i is a unit, a contradiction. □

4.10. Let R be an integral domain and let d be the degree of a nonzero $f \in R[X]$. Prove that $\{a \in R \mid f(a) = 0\}$ is finite. *Hint*: Case 1 — first prove this when R is a field. Case 2 — reduce to case 1 by looking at the fraction field of R.

Proof. Let $A = \{a \in R \mid f(a) = 0\}$. We induct on d. For the base case $d = 0$, let $f \in R[X]$ be an arbitrary nonzero polynomial having $\deg(f) = d = 0$. It follows that $f(X) = a$ for some nonzero $a \in R$. Thus, since $f(X) \neq 0$ for any X, $|A| = 0$ and we have the desired result. Now suppose inductively that we have proven the claim for $d - 1$; we now wish to prove it for degree d. Once again, let $f \in R[X]$ be an arbitrary nonzero polynomial having $\deg(f) = d$. If f has no roots, then we are done. Otherwise, pick $a \in A$. By the Euclidean algorithm, $f(X) = q(X) \cdot (X - a) + r$ for some $q, r \in R[X]$ with $\deg r < \deg(X - a)$. It follows from the latter constraint that $r \in R$ is a constant. In particular,

$$r = f(a) - q(a) \cdot (a - a) = 0 - q(a) \cdot 0 = 0$$

Thus, $f = q \cdot (X - a)$. It follows that

$$\begin{aligned} \deg(f) &= \deg(q) + \deg(X - a) \\ d &= \deg(q) + 1 \\ \deg(q) &= d - 1 \end{aligned}$$

Thus, by the induction hypothesis, q has finitely many roots. This combined with the fact that $X - a$ has only one root (additive inverses are unique in rings, so only $a + (-a) = 0$) implies that f has at most one more root than q, i.e., f has finitely many roots, as desired. □