Math 562/662 — Spring 2024
Homework 1 — Drew Armstrong

1. The Field of Fractions of a Domain. Let $(R, +, \cdot, 0, 1)$ be an integral domain (i.e., a commutative ring in which $ab = 0$ implies $a = 0$ or $b = 0$) and consider the set of "fractions":

$$\text{Frac}(R) = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\},$$

At first we will think of the fraction a/b as a formal symbol.

(a) Check that the following is an equivalence relation on the set of fractions:

$$\frac{a}{b} \sim \frac{c}{d} \quad \Longleftrightarrow \quad ad = bc.$$

(b) We define "addition" and "multiplication" of fractions as follows:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Check that these operations are well-defined with respect to the equivalence $\sim$. That is, for all $a, b, c, d, a', b', c', d' \in R$ with $b, d, b', d' \neq 0$, show that

$$\frac{a}{b} \sim \frac{a'}{b'} \text{ and } \frac{c}{d} \sim \frac{c'}{d'} \quad \Longrightarrow \quad \frac{a}{b} + \frac{c}{d} \sim \frac{a'}{b'} + \frac{c'}{d'} \text{ and } \frac{a}{b} \cdot \frac{c}{d} \sim \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

(c) One can check that the set of equivalence classes $\text{Frac}(R)/\sim$ from part (b) is a field.[1] We usually denote this field by $\text{Frac}(R)$, omitting mention of the equivalence relation. Show that the function $\varphi : R \to \text{Frac}(R)$ defined by $\varphi(a) := a/1$ is an injective ring homomorphism. Thus we can think of R as a subring of $\text{Frac}(R)$.

Remark: Assuming that we already have a definition of the integers $\mathbb{Z}$, we use this construction to define the rational numbers $\mathbb{Q} := \text{Frac}(\mathbb{Z})$. In this course we will **not** discuss the construction of the real numbers $\mathbb{R}$ from $\mathbb{Q}$. However, we **will** discuss the construction of the complex numbers $\mathbb{C}$ from $\mathbb{R}$. See Problem 4 below.

(a): *Reflexive.* For any $a, b \in R$ with $b \neq 0$ we have $ab = ba$ and hence $a/b \sim a/b$. *Symmetric.* Consider any $a, b, c, d \in R$ with $b, d \neq 0$ and suppose that $a/b \sim c/d$, so that $ad = bc$. Then we also have $cb = ad$, and hence $c/d \sim a/b$. *Transitive.* Consider any $a, b, c, d, e, f \in R$ with $b, d, f \neq 0$, such that $a/b \sim c/d$ and $c/d \sim e/f$, which means that $ad = bc$ and $cf = de$. Our goal is to show that $af = be$, and hence $a/b \sim e/f$. To see this, first note that

$$\begin{aligned} daf &= adf \\ &= bcf && \text{because } ad = bc \\ &= bde && \text{because } cf = de \\ &= dbe. \end{aligned}$$

Then since R is a domain and $d \neq 0$ we have $af = be$.[2]

[1] This is easy but tedious. You don't need to do it.

[2] Recall that multiplicative cancellation holds in a domain. Proof. If $ac = bc$ and $c \neq 0$ then since $(a-b)c = 0$ and $c \neq 0$ we must have $a - b = 0$ and hence $a = b$.

(b): Let $a/b \sim a'/b'$ and $c/d \sim c'/d'$, so that $ab' = a'b$ and $cd' = c'd$. Then we have

$$\begin{aligned}(ac)(b'd') &= (ab')(cd') \\ &= (a'b)(c'd) \\ &= (a'c')(bd),\end{aligned}$$

so that $(a/b)(c/d) \sim (a'/b')(c'/d')$, and

$$\begin{aligned}(ad+bd)(b'd') &= (ad)(b'd') + (bd)(b'd') \\ &= (ab')(dd') + (cd')(bb') \\ &= (a'b)(dd') + (c'd)(bb') \\ &= (a'd')(bd) + (b'c')(bd) \\ &= (a'd' + b'c')(bd),\end{aligned}$$

so that $(a/b + c/d) \sim (a'/b' + c'/d')$.

(c): Consider the function $\varphi : R \to \mathrm{Frac}(R)$ defined by $\varphi(a) := a/1$. This is an injective function since $a/1 \sim b/1$ implies $a1 = b1$ and hence $a = b$. And it is a ring homomorphism since $\varphi(1) = 1/1$ is the unit element of $\mathrm{Frac}(R)$ and since for all $a, b \in R$ we have

$$\varphi(a) + \varphi(b) = a/1 + b/1 = (a1 + 1b)/1 = (a+b)/1 = \varphi(a+b)$$

and

$$\varphi(a)\varphi(b) = (a/1)(b/1) = (ab)/(1 \cdot 1) = (ab)/1 = \varphi(ab).$$

2. Adjoining an Element to a Field. Given a field extension $\mathbb{E} \supseteq \mathbb{F}$ and an element $\alpha \in \mathbb{E}$, one can check that the following *evaluation function* is a ring homomorphism:[3]

$$\begin{array}{rcl}\varphi_\alpha : \mathbb{F}[x] & \to & \mathbb{E} \\ f(x) & \mapsto & f(\alpha).\end{array}$$

(a) We denote the image of φ_α by $\mathbb{F}[\alpha] := \operatorname{im}\varphi_\alpha = \{f(\alpha) : f(x) \in \mathbb{F}[x]\} \subseteq \mathbb{E}$. Prove that $\mathbb{F}[\alpha]$ is the **smallest subring of $\mathbb{E}$ that contains the set** $\mathbb{F} \cup \{\alpha\}$**.** [Hint: Let R be the smallest subring of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\alpha\}$. Show that $\mathbb{F}[\alpha] = R$.]

(b) Prove that $\mathbb{F}[\alpha]$ is a domain. [Hint: Show that any subring of a field is a domain.]

(c) We denote the field of fractions of $\mathbb{F}[\alpha]$ by

$$\mathbb{F}(\alpha) := \mathrm{Frac}(\mathbb{F}[\alpha]) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in \mathbb{F}[x], g(\alpha) \neq 0\} \subseteq \mathbb{E}.$$

Prove that $\mathbb{F}(\alpha)$ is the **smallest subfield of $\mathbb{E}$ that contains the set** $\mathbb{F} \cup \{\alpha\}$. [Hint: Let $\mathbb{K}$ be the smallest subfield of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\alpha\}$. Show that $\mathbb{F}(\alpha) = \mathbb{K}$.]

Warning: Using similar notation, we let $\mathbb{F}(x)$ denote the field of fractions of the ring of polynomials $\mathbb{F}[x]$, where x is an "indeterminate". This is the set of formal expressions $f(x)/g(x)$ with $f(x), g(x) \in \mathbb{F}[x]$ where $g(x)$ is not the zero polynomial. Given an element $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ in a field extension, it is tempting to try to define an "evaluation homomorphism" $\mathbb{F}(x) \to \mathbb{E}$ by $f(x)/g(x) \mapsto f(\alpha)/g(\alpha)$. However, this function doesn't exist when α is a root of $g(x)$. "Rational functions" are more subtle than "polynomial functions" and require more sophisticated ideas,[4] which we will not discuss in this class.

[3]This is easy and tedious. However, it does depend in a subtle way on the fact that multiplication in $\mathbb{E}$ is commutative. The idea of "evaluation" doesn't work over noncommutative rings.

[4]This the concept of "meromorphic functions" from complex analysis.

(a): Let $\mathbb{F}[\alpha] := \operatorname{im}\varphi_\alpha = \{f(\alpha) : f(x) \in \mathbb{F}[x]\}$, and let R be the smallest subring of $\mathbb{E}$ that contains $\mathbb{F}\cup\{\alpha\}$. Note that $\mathbb{F}[\alpha]$ is itself a subring of $\mathbb{E}$ that contains $\mathbb{F}\cup\{\alpha\}$.[5]. By minimality of R this implies that $R \subseteq \mathbb{F}[\alpha]$. On the other hand, consider any element $f(\alpha) \in \mathbb{F}[\alpha]$, which can be expressed as $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ for some $n \in \mathbb{N}$ and $a_0, \ldots, a_n \in \mathbb{F}$. Since R contains $\mathbb{F} \cup \{\alpha\}$ we must have

$$a_0, a_1, \ldots, a_n, \alpha \in R.$$

But then since R is closed under ring operations we must also have $f(\alpha) \in R$. Hence $\mathbb{F}[\alpha] \subseteq R$.

(b): Let $\mathbb{K}$ be any field and let $R \subseteq \mathbb{K}$ be any subring. For any $a, b \in R$ with $a \neq 0$ we also have $a \in \mathbb{K}$, which implies that $a^{-1} \in \mathbb{K}$. But then in $\mathbb{K}$ we have

$$\begin{aligned} ab &= 0 \\ a^{-1}ab &= a^{-1}0 \\ b &= 0, \end{aligned}$$

which must also hold in R.

(c): Consider the field of fractions[6]

$$\mathbb{F}(\alpha) := \operatorname{Frac}(\mathbb{F}[\alpha]) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in \mathbb{F}[x], g(\alpha) \neq 0\} \subseteq \mathbb{E}.$$

and let $\mathbb{K}$ be the smallest subfield of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\alpha\}$. Note that $\mathbb{F}(\alpha)$ is itself a subfield of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\alpha\}$, hence by minimality we have $\mathbb{K} \supseteq \mathbb{F}(\alpha)$. On the other hand, consider any element $f(\alpha)/g(\alpha) \in \mathbb{F}(\alpha)$, which can be expressed as

$$\frac{f(\alpha)}{g(\alpha)} = \frac{a_0 + a_1\alpha + \cdots + a_m\alpha^m}{b_0 + b_1\alpha + \cdots + b_n\alpha^n}$$

for some $a_0, \ldots, a_m, b_0, \ldots, b_n \in \mathbb{F}$. Since $\mathbb{K}$ contains $\mathbb{F} \cup \{\alpha\}$ we must have

$$a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n, \alpha \in \mathbb{K}.$$

Since $\mathbb{K}$ is closed under field operations, this implies that $f(\alpha)/g(\alpha) \in \mathbb{F}(\alpha)$. Hence $\mathbb{F}(\alpha) \subseteq \mathbb{K}$.

3. Square Roots are Irrational. Let $D \in \mathbb{N}$ be a positive integer and let $\sqrt{D} \in \mathbb{R}$ be one of its two square roots. In this problem you will show that

$$\sqrt{D} \notin \mathbb{Z} \quad\Longrightarrow\quad \sqrt{D} \notin \mathbb{Q}.$$

(a) Consider the set $S = \{n \in \mathbb{N} : n\sqrt{D} \in \mathbb{Z}\} \subseteq \mathbb{N}$. Show that

$$S = \emptyset \quad\Longleftrightarrow\quad \sqrt{D} \notin \mathbb{Q}.$$

(b) Assuming that $\sqrt{D} \notin \mathbb{Z}$, use the well-ordering principle to prove that there exists an integer $a \in \mathbb{Z}$ such that $a < \sqrt{D} < a + 1$.

(c) Continuing from part (b), suppose also that $\sqrt{D} \in \mathbb{Q}$. By part (a) and well-ordering, this means that the set S has a least element, say $m \in S$. Now use part (b) to get a contradiction. [Hint: Consider the number $m(\sqrt{D} - a)$.]

---

[5] The image of a ring homomorphism is always a subring.

[6] There is a small subtlety here. At first the field of fractions is just an abstractly constructed field. However, if R is a subring of a field $\mathbb{E}$ then there is an obvious way to view $\operatorname{Frac}(R)$ as a subfield of $\mathbb{E}$ by sending the abstract fraction a/b to the element $ab^{-1} \in \mathbb{E}$. I didn't bother to turn this into an exercise.

(a): Suppose that $\sqrt{D} \in \mathbb{Q}$, so that $\sqrt{D} = a/b$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Since $a/b = (-a)/(-b)$, we may assume that $b > 0$, and hence $b \in \mathbb{N}$.[7] But then since $b\sqrt{D} = a \in \mathbb{Z}$ we have $b \in S$, so that $S \neq \emptyset$. On the other hand, suppose that $S \neq \emptyset$, and choose some $b \in S$. By assumption this means that $b\sqrt{D} = a$ for some $a \in \mathbb{Z}$. But then $\sqrt{D} = a/b \in \mathbb{Q}$.

(b): Suppose that $\sqrt{D} \notin \mathbb{Z}$, and let $a \in \mathbb{Z}$ be the greatest integer satisfying $a < \sqrt{D}$ (which exists by the well-ordering principle). Since $a+1$ is greater than a we know that $a+1 \not< \sqrt{D}$, i.e., that $a+1 \geq \sqrt{D}$. And since $\sqrt{D} \notin \mathbb{Z}$ we know that $a+1 \neq \sqrt{D}$, hence $a+1 > \sqrt{D}$.

(c): Suppose that $\sqrt{D} \notin \mathbb{Z}$ and let $a \in \mathbb{Z}$ satisfy $a < \sqrt{D} < a+1$. In order to prove that $\sqrt{D} \notin \mathbb{Q}$, let us assume for contradiction that $\sqrt{D} \in \mathbb{Q}$. By part (a) this means that $S \neq \emptyset$, so by well-ordering there exists a least element $m \in S$. By definition of S we have $m\sqrt{D} \in \mathbb{Z}$, and hence $m(\sqrt{D} - a) = m\sqrt{D} - ma \in \mathbb{Z}$. On the other hand, we have

$$\begin{array}{ccccc} a & < & \sqrt{D} & < & a+1 \\ 0 & < & \sqrt{D} - a & < & 1 \\ 0 & < & m(\sqrt{D} - a) & < & m. \end{array}$$

Finally, since $m\sqrt{D} \in \mathbb{Z}$ we have $m(\sqrt{D} - a)\sqrt{D} = mD - am\sqrt{D} \in \mathbb{Z}$, and we see that $m(\sqrt{D} - a)$ is an element of S that is less than m. Contradiction. $\square$

Remark: This proof requires a minimum of technology, but it not very pretty. Later we will see a better proof using the theory of unique prime factorization.

4. Quadratic Field Extensions. Consider a field extension $\mathbb{E} \supseteq \mathbb{F}$ and an element $\alpha \in \mathbb{E}$ satisfying $\alpha \notin \mathbb{F}$ and $\alpha^2 \in \mathbb{F}$. As in Problem 2, consider the ring $\mathbb{F}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{F}[x]\}$, which is the smallest subring of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\alpha\}$. We can write this explicitly as

$$\mathbb{F}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n : a_0, \ldots, a_n \in \mathbb{F}, n \in \mathbb{N}\} \subseteq \mathbb{E}.$$

(a) Prove that every element $\beta \in \mathbb{F}[\alpha]$ can be expressed as $\beta = a + b\alpha$ for some $a, b \in \mathbb{F}$. [Hint: By assumption we have $\beta = f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Since $\alpha^2 \in \mathbb{F}$, there exist $q(x), r(x) \in \mathbb{F}[x]$ with $\deg(r) \leq 1$ such that $f(x) = q(x)(x^2 - \alpha^2) + r(x)$. Now substitute $x = \alpha$.]

(b) For any two elements $\beta = a + b\alpha$ and $\beta' = a' + b'\alpha$ in $\mathbb{F}[\alpha]$, show that

$$\beta = \beta' \iff a = a' \text{ and } b = b'.$$

Thus we obtain a bijection $\mathbb{F}[\alpha] \leftrightarrow \mathbb{F}^2$ defined by $a + b\alpha \leftrightarrow (a, b)$. [Hint: If $b = b'$ then we are done. Otherwise, show that $\alpha = (a - a')/(b' - b) \in \mathbb{F}$, which is a contradiction.]

(c) Multiplying an element $a + b\alpha \in \mathbb{F}[\alpha]$ by its "conjugate" gives $(a + b\alpha)(a - b\alpha) = a^2 - b^2\alpha^2 \in \mathbb{F}$. Use this to show that

$$a + b\alpha = 0 \iff a^2 - b^2\alpha^2 = 0.$$

(d) Prove that $\mathbb{F}[\alpha]$ is actually a field. [Hint: "Rationalize the denominator".]

(a): Consider any element $\beta \in \mathbb{F}[\alpha]$. By definition we can write $\beta = f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}[x]$ with coefficients in $\mathbb{F}$. Since $\alpha^2 \in \mathbb{F}$, the polynomial $x^2 - \alpha^2$ (of degree 2) is in $\mathbb{F}[x]$. Hence by the division algorithm in $\mathbb{F}[x]$ there exist (unique) $q(x), r(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = q(x)(x^2 - \alpha^2) + r(x), \\ r(x) = 0 \text{ or } \deg(r) < 2. \end{cases}$$

[7] For the purpose of this problem, I guess we will say that $0 \notin \mathbb{N}$.

Since $r(x) = 0$ or $\deg(r) < 2$ we can write $r(x) = a + bx$ for some $a, b \in \mathbb{F}$, possibly both zero. Finally, substituting $x = \alpha$ gives

$$\begin{aligned}\beta &= f(\alpha)\\ &= q(\alpha)(\alpha^2 - \alpha^2) + r(\alpha)\\ &= q(\alpha) \cdot 0 + r(\alpha)\\ &= r(\alpha)\\ &= a + b\alpha.\end{aligned}$$

(b): Consider any two elements $\beta = a + b\alpha$ and $\beta' = a' + b'\beta$ in $\mathbb{F}[\alpha]$, and suppose that $\beta = \beta'$, so that $a - a' = \alpha(b' - b)$. If $b = b'$ then we are done because $a - a' = \alpha \cdot 0 = 0$ implies $a = a'$. Otherwise we must have $b \neq b'$. But this implies that $\alpha = (a - a')/(b' - b) \in \mathbb{F}$, which contradicts our assumption that $\alpha \notin \mathbb{F}$.

(c): Given $\beta = a + b\alpha$, we define its *conjugate* $\beta^* := a - b\alpha$,[8] and we note that $\beta\beta^* = a^2 - b^2\alpha^2$. Our goal is show that $\beta = 0$ if and only if $\beta\beta^* = 0$. Well, if $\beta = 0$ then certainly $\beta\beta^* = 0$. On the other hand, suppose that $\beta\beta^* = 0$. Since $\mathbb{F}[\alpha]$ is a subring of a field, it is a domain, hence we must have $\beta = 0$ or $\beta^* = 0$. But from part (b) we know that

$$\beta = 0 \iff (a, b) = (0, 0) \iff (a, -b) = (0, 0) \iff \beta^* = 0.$$

Hence we must have $\beta = 0$.

(d): Consider any $\beta = a + b\alpha \in \mathbb{F}[\alpha]$. If $\beta \neq 0$ then from part (c) we know that $\beta\beta^* \neq 0$ and $\beta\beta^* \in \mathbb{F}$. Hence we have

$$\frac{1}{\beta} = \frac{\beta*}{\beta\beta^*} = \left(\frac{a}{a^2 - b^2\alpha^2}\right) + \left(\frac{-b}{a^2 - b^2\alpha^2}\right)\alpha,$$

which is an element of $\mathbb{F}[\alpha]$. $\square$

Remark: Thus we have shown that $\mathbb{F}[\alpha]$ is a field, which implies that $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$. Later we will show that the same holds for any element $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ that is *algebraic over* $\mathbb{F}$, which means that $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in \mathbb{F}[x]$. The proof will depend on the Euclidean algorithm in the ring $\mathbb{F}[x]$.

We say that α *is transcendental over* $\mathbb{F}$ if it is not algebraic. In this case I claim that $\mathbb{F}[\alpha] \neq \mathbb{F}(\alpha)$. Indeed, consider the ring homomorphism $\mathbb{F}[x] \to \mathbb{E}$ defined by $f(x) \mapsto f(\alpha)$. Note that α is transcendental over $\mathbb{F}$ precisely when the kernel is trivial:

$$\ker\varphi = \{f(x) \in \mathbb{F}[x] : f(\alpha) = 0\} = \{0\}.$$

If α is transcendental over $\mathbb{F}$ then the First Isomorphism Theorem for Rings shows that $\mathbb{F}[\alpha]$ is isomorphic to the ring of polynomials:

$$\mathbb{F}[x] \cong \frac{\mathbb{F}[x]}{\{0\}} = \frac{\mathbb{F}[x]}{\ker\varphi} \cong \operatorname{im}\varphi = \mathbb{F}[\alpha].$$

This isomorphism just sends $x \mapsto \alpha$. In other words, a number that is transcendental over $\mathbb{F}$ is basically the same thing as a "variable". Finally, since $\mathbb{F}[x]$ is not a field,[9] neither is $\mathbb{F}[\alpha]$.

[8] Note that this definition relies on the uniqueness of $a, b \in \mathbb{F}$ in the expression $\beta = a + b\alpha$.

[9] For example, the variable $x \in \mathbb{F}[x]$ has no multiplicative inverse.