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.

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:[2]

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

(a) We denote the image of φ_α by $\mathbb{F}[\alpha] := \text{im}\,\varphi_\alpha = \{f(\alpha) : f(x) \in \mathbb{F}[x]\} \subseteq \mathbb{E}$. 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

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

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 $\mathbb{F}(\alpha) = \mathbb{K}$.]

---

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

[2] 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.

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,[3] which we will not discuss in this class.

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 $m(\sqrt{D} - a)$.]

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

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

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

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

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

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