Math 561/661 **Fall 2021**
Homework 6 **Drew Armstrong**

---

1. Invariance of Quotient and Remainder. For every extension of fields $\mathbb{E} \supseteq \mathbb{F}$ we obtain an extension of rings $\mathbb{E}[x] \supseteq \mathbb{F}[x]$.

(a) Consider $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Since $\mathbb{F}[x] \subseteq \mathbb{E}[x]$ we also have $f(x), g(x) \in \mathbb{E}[x]$, hence there exist some $q(x), r(x) \in \mathbb{E}[x]$ satisfying

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

Prove that we must in fact have $q(x), r(x) \in \mathbb{F}[x]$. [Hint: Uniqueness.]

(b) Consider any $f(x), g(x) \in \mathbb{F}[x]$. We can also view $f(x), g(x)$ as elements of $\mathbb{E}[x]$. If $f(x)|g(x)$ in the ring $\mathbb{E}[x]$, use part (a) to prove that $f(x)|g(x)$ in the ring $\mathbb{F}[x]$.

(c) Now consider the field extension $\mathbb{C} \supseteq \mathbb{R}$. If $f(x) \in \mathbb{R}[x]$ and $f(i) = 0$, prove that there exists $q(x) \in \mathbb{R}[x]$ such that $f(x) = (x^2+1)q(x)$. [Hint: Use Descartes' Theorem to prove that $(x^2+1)|f(x)$ in the ring $\mathbb{C}[x]$. Then use part (b).]

(a): Given $f(x), g(x) \in \mathbb{E}[x]$ with $g(x) \neq 0$ there exist **unique** $q(x), r(x) \in \mathbb{E}[x]$ satisfying

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

Since we also have $f(x), g(x) \in \mathbb{F}[x]$ there also exist $q'(x), r'(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = g(x)q'(x) + r'(x), \\ r'(x) = 0 \text{ or } \deg(r') < \deg(g). \end{cases}$$

But then since $q'(x), r'(x) \in \mathbb{E}[x]$, it follows from uniqueness that $q(x) = q'(x)$ and $r(x) = r'(x)$, which implies that $q(x) \in \mathbb{F}[x]$ and $r(x) \in \mathbb{F}[x]$.

(b): Given $f(x), g(x) \in \mathbb{F}[x]$ we say that $f(x)|g(x)$ if $\mathbb{E}[x]$ if there exists $h(x) \in \mathbb{E}[x]$ such that $f(x)h(x) = g(x)$ and we say that $f(x)|g(x)$ in $\mathbb{F}[x]$ if there exists $h'(x) \in \mathbb{F}[x]$ such that $f(x)h'(x) = g(x)$. Clearly $f(x)|g(x)$ in $\mathbb{F}[x]$ implies $f(x)|g(x)$ in $\mathbb{E}[x]$ because $\mathbb{F}[x] \subseteq \mathbb{E}[x]$. (I did not ask you to prove this.) On the other hand, suppose that $f(x)|g(x)$ in $\mathbb{E}[x]$ so that $f(x)h(x) = g(x)$ for some $h(x) \in \mathbb{E}[x]$. We can view this $h(x)$ as the quotient of $g(x)$ mod $f(x)$. Since $f(x), g(x) \in \mathbb{F}[x]$, part (a) tells us that $h(x) \in \mathbb{F}[x]$, hence $f(x)|g(x)$ in $\mathbb{F}[x]$.

(c): Let $f(x) \in \mathbb{F}[x]$ and $f(i) = 0$. Then Descartes' Theorem in the ring $\mathbb{C}[x]$ tells us that $f(x) = (x-i)g(x)$ for some $g(x) \in \mathbb{C}[x]$. Since $f(x)$ has real coefficients we also know that $f(-i)$, so that

$$0 = f(-i) = (-i-i)g(-i) = -2ig(-i).$$

Applying Descartes again gives $g(x) = (x+i)h(x)$ for some $h(x) \in \mathbb{C}[x]$ and hence

$$\begin{aligned} f(x) &= (x-i)(x+i)h(x) \\ &= (x^2+1)h(x). \end{aligned}$$

Finally, since $f(x)$ and $x^2+1 \in \mathbb{R}[x]$, part (a) tells us that $h(x) \in \mathbb{R}[x]$, hence $(x^2+1)|f(x)$ in the ring $\mathbb{R}[x]$.

Remark: We have shown for $f(x) \in \mathbb{R}[x]$ that $f(i) = 0$ if and only if $(x^2+1)|f(x)$. Next semester we will say that x^2+1 is the *minimal polynomial for i over $\mathbb{R}$*.

2. Field of Fractions. Let R be an integral domain and consider the set of abstract fractions

$$\mathrm{Frac}(R) = \{a/b : a, b \in R, b \neq 0\}.$$

We declare that $a/b = a'/b'$ if and only if $ab' = a'b$ and we define the following operations:

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

Note that the fractions on the right exist because $b \neq 0$ and $d \neq 0$ imply $bd \neq 0$. One can check that these operations make $\mathrm{Frac}(R)$ in a field with identity elements $0/1$ and $1/1$.

(a) If $a/b = a'/b'$ and $c/d = c'/d'$, prove that

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

(b) Prove that the function $\varphi : R \to \mathrm{Frac}(R)$ defined by $\varphi(a) := a/1$ is an injective ring homomorphism.

(c) Let $\mathbb{F}$ be a field containing R as a subring. Prove that the function $\mu : \mathrm{Frac}(R) \to \mathbb{F}$ defined by $\mu(a/b) := ab^{-1}$ is an injective ring homomorphism. [Hint: In addition to the usual properties of an injective ring homomorphism, you must also show that $a/b = a'/b'$ implies $\mu(a/b) = \mu(a'/b')$. That is, you must show that μ is "well-defined".]

Remark: Given rings R and S, a *ring homomorphism* is a function $\varphi : R \to S$ satisfying

- $\varphi(1) = 1$,
- $\varphi(a + b) = \varphi(a) + \varphi(b)$,
- $\varphi(ab) = \varphi(a)\varphi(b)$.

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

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

and

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

(b): First we observe that φ preserves the multiplicative identity:

$$\varphi(1) = 1/1.$$

Next we observe that φ is injective:

$$\begin{aligned}\varphi(a) = \varphi(b) &\Rightarrow a/1 = b/1 \\ &\Rightarrow a \cdot 1 = b \cdot 1 \\ &\Rightarrow a = b.\end{aligned}$$

Finally, we observe that φ preserves addition and multiplication:

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

and

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

(c): First we observe that μ is well-defined:

$$\begin{aligned} a/b = a'/b' &\Rightarrow ab' = a'b \\ &\Rightarrow ab'b^{-1}(b')^{-1} = a'bb^{-1}(b')^{-1} \\ &\Rightarrow ab^{-1} = a'(b')^{-1} \\ &\Rightarrow \mu(a/b) = \mu(a'/b'). \end{aligned}$$

Next we observe that μ preserves the multiplicative identity:

$$\mu(1/1) = 1 \cdot 1^{-1} = 1.$$

Next we observe that μ is injective:

$$\begin{aligned} \mu(a/b) = \mu(a'/b') &\Rightarrow ab^{-1} = a'(b')^{-1} \\ &\Rightarrow ab^{-1}bb' = a'(b')^{-1}bb' \\ &\Rightarrow ab' = a'b \\ &\Rightarrow a/b = a'/b'. \end{aligned}$$

Finally, we observe that μ preserves addition and multiplication:

$$\begin{aligned} \mu(a/b + c/d) &= \mu((ad + bc)/(bd)) \\ &= (ad + bc)(bd)^{-1} \\ &= adb^{-1}d^{-1} + bcb^{-1}d^{-1} \\ &= ab^{-1} + cd^{-1} \\ &= \mu(a/b) + \mu(c/d) \end{aligned}$$

and

$$\mu(a/b)\mu(c/d) = (ab^{-1})(cd^{-1}) = (ab)(bd)^{-1} = \mu((ab)/(cd)) = \mu(a/b \cdot c/d).$$

Remark: Now we have earned the right to use fractional notation. This problem was intended as an introduction to the concept of ring homomorphisms. We will have much more to say about this next semester.