David Owen Horace Cutler **Math 146: Homework 2** February 9, 2024

Exercise 1. Let $F = \mathbb{Q}(i)$. Consider a non-zero ring homomorphism $\phi : F \to F$.

(a) Prove that ϕ must be an isomorphism.

Proof. Let 0 and 1 denote the additive identity and multiplicative identity in F respectively.

We will show injectivity first. For this, we want to show that $\ker(\phi)$ is trivial, i.e. $\ker(\phi) = \{0\}$. For this, we assume for the sake of contradiction that there is some $a \neq 0$ such that $\phi(a) = 0$.

Note as F is a field, it is an integral domain, as if we have $ab = 0$ with $a, b \neq 0$, we get a contradiction as then they both admits inverses, which has i.e. $a^{-1}ab = a^{-1}(0) \to b = 0$.

As F is an integral domain and ϕ is non-zero then, we have $\phi(1) = 1$, as proven in class. Moreover, as $a \neq 0$, we have that a^{-1} exists. Stitching these facts together yields the following:

$$1 = \phi(1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = (0)\phi(a^{-1}) = 0 \tag{1}$$

But F is a field, so it should be $1 \neq 0$. Thus (1) yields a contradiction, and so $\ker(\phi)$ is trivial, which furthermore has that ϕ is an injection.

(Note by convention it is that $1 \neq 0$ in fields, however, if we do not adopt this convention, we just note that this forces F to be the trivial ring, in which any function $F \to F$ is a bijection).

To show surjectivity, we need to use some aspects of the structure of $\mathbb{Q}(i)$ (as unlike the injectivity proof, surjectivity need not hold in arbitrary homomorphisms between fields).

In part (b), I prove that at least ϕ is onto the rationals as they lay in $\mathbb{Q}(i)$, in particular we have $\phi(a) = a$ for $a \in \mathbb{Q}$. Note then the following as $i^2 = -1$:

$$-1 = -\phi(1) = \phi(-1) = \phi(i^2) = \phi(i)^2 \tag{2}$$

Thus $\phi(i) = i$ or $-i$. In particular then, for $b \in \mathbb{Q}$, we have that either:

$$\phi(bi) = \phi(b)\phi(i) = bi \text{ or } -bi \tag{3}$$

One observes this has that bi is either mapped to by bi or by $-bi$, depending on how ϕ handles i. Moreover, in the later case, $\phi(-bi) = -\phi(bi) = -(-bi) = bi$. Thus:

$$a + bi = \phi(a) + \phi(bi) \text{ or } \phi(a) + \phi(-bi) = \phi(a + bi) \text{ or } \phi(a - bi) \tag{4}$$

But this of course has that ϕ is surjective, and so ϕ is an isomorphism. $\square$

(b) Prove that $\phi(a) = a$ for $a \in \mathbb{Q}$.

Proof. Let some $a \in \mathbb{Q}$. We express $a = \frac{p}{q}$, where $p \in \mathbb{Z}, q \in \mathbb{N}$. We moreover assume $a \neq 0$, as we already noted $\phi(0) = 0$.

We consider then two cases, the first being $p > 0$. Here, we get the following argument utilizing the fact that ϕ is a homomorphism:

$$\phi\Big(\frac{p}{q}\Big) = \phi\Big(p\frac{1}{q}\Big) = \phi\Big(\sum_{i=1}^{p}\frac{1}{q}\Big) = \sum_{i=1}^{p}\phi\Big(\frac{1}{q}\Big) = p\phi\Big(\frac{1}{q}\Big) \tag{5}$$

If instead $p < 0$, we make a slight modification:

$$\phi\Big(\frac{p}{q}\Big) = \phi\Big(p\frac{1}{q}\Big) = \phi\Big(\sum_{i=1}^{|p|}\frac{-1}{q}\Big) = \sum_{i=1}^{|p|}\phi\Big(\frac{-1}{q}\Big) = \sum_{i=1}^{|p|}-\phi\Big(\frac{1}{q}\Big) = p\phi\Big(\frac{1}{q}\Big) \tag{6}$$

So regardless $\phi(\frac{p}{q}) = q\phi(\frac{1}{q})$. An obvious corollary of this is that for a given $q \in \mathbb{N}$, we have $1 = \phi(1) = q\phi(\frac{1}{q})$. Thus $\phi(\frac{1}{q}) = \frac{1}{q}$. Putting this together with (5) and (6) thus gets $\phi(\frac{p}{q}) = \frac{p}{q}$ in general. $\square$

(c) Suppose $\alpha \in F$ is such that $\phi(\alpha) = i$. Find a complete list of possibilities for α.

Proof. We want to find all possibilities for α. For this, note we have the following:

$$\begin{aligned} \phi(\alpha) = i \longrightarrow \phi(\alpha)^2 = -1 \\ \longrightarrow \phi(\alpha^2) = -1 \longrightarrow \phi(\alpha^2) + 1 = 0 \\ \longrightarrow \phi(\alpha^2) + \phi(1) = 0 \longrightarrow \phi(\alpha^2 + 1) = 0 \end{aligned} \tag{7}$$

But ϕ is injective, so this has $\alpha^2 + 1 = 0$. Thus it must be $\alpha = i$ or $\alpha = -i$. Our earlier work in (b) verifies this, as we have either i or $-i$ maps to i as a corrolary of our surjectivity proof. $\square$

(d) Determine all non-zero homomorphisms $\phi : F \to F$.

Proof. In part (b), assuming that ϕ is a non-zero homomorphism gets us $\phi(1) = 1$ (as F is a field $\to$ F is an integral domain), which allowed us to prove that in part (a) a small lemma that either $\phi(i) = i$ or $-i$.

It's not hard to show then that the value of $\phi(i)$ determines whether or not ϕ is one of two possible automorphisms; in particular, we see ϕ is either the identity map or the conjugation map by considering $a, b \in \mathbb{Q}$:

$$\begin{aligned} \phi(i) = i \to \phi(a + bi) = \phi(a) + \phi(b)\phi(i) = a + bi \\ \phi(i) = -i \to \phi(a + bi) = \phi(a) + \phi(b)\phi(i) = a - bi \end{aligned} \tag{8}$$

As these are the only options for $\phi(i)$ then, these are the only only possible mappings. $\square$

Exercise 2. Let $\mathbb{F}_5 = \mathbb{Z}_5$.

(a) Prove that there is no element $\alpha \in \mathbb{F}_5$ such that $\alpha^2 = [2]_5$.

Proof. We explicitly verify this:

$$[0]_5^2 = [0]_5, [1]_5^2 = [1]_5, [2]_5^2 = [4]_5, [3]_5^2 = [4]_5, [4]_5^2 = [1]_5 \tag{9}$$

So there is no "square root of 2" here. □

(b) Now let $R = \{[a]_5 + [b]_5 x : [a]_5, [b]_5 \in \mathbb{F}_5\}$. Consider the normal operations with the added rule that $x^2 = [2]_5$; show that R is a ring under these operations.

Proof. Let some $f, g \in R$ such that $f = [a_0]_5 + [a_1]_5 x$, $g = [b_0]_5 + [b_1]_5 x$. Then we have:

$$\begin{aligned} f \cdot g = \sum_{l=0}^{2} \Big(\sum_{\substack{i+j=l \\ i,j \in \mathbb{N}}} [a_i]_5 [b_j]_5 \Big) &= [a_0]_5[b_0]_5 + [a_1]_5[b_0]_5 x + [a_0]_5[b_1]_5 x + [a_1][b_1]x^2 \\ = [a_0 b_0]_5 + [a_1 b_0 + a_0 b_1]x + [2a_1 b_1]_5 &= [2a_1 b_1 + a_0 b_0]_5 + [a_1 b_0 + a_0 b_1]_5 x \end{aligned} \tag{10}$$

This gives us a useful identity for $f \cdot g$, which will allow us to streamline the process of verifying R to be a ring, which we will do now.

Note also the fact that R is clearly closed under these operations given (9) (where closure under addition is trivial).

(a) *(Commutativity of Addition)* We use the commutativity of addition in $\mathbb{F}_5$:

$$\begin{aligned} f + g &= ([a_0]_5 + [a_1]_5 x) + ([b_0]_5 + [b_1]_5 x) \\ &= [a_0 + b_0]_5 + [a_1 + b_1]_5 x = [b_0 + a_0]_5 + [b_1 + a_1]_5 x \\ &= ([b_0]_5 + [b_1]_5 x) + ([a_0]_5 + [a_1]_5 x) = g + f \end{aligned} \tag{11}$$

(b) *(Associativity of Addition)* Consider in addition some $h = [c_0]_5 + [c_1]_5 x$, we utilize associativity in $\mathbb{F}_5$:

$$\begin{aligned} (f + g) + h &= (([a_0]_5 + [a_1]_5 x) + ([b_0]_5 + [b_1]_5 x)) + ([c_0]_5 + [c_1]_5 x) \\ &= ([a_0 + b_0]_5 + [a_1 + b_1]_5 x) + ([c_0]_5 + [c_1]_5 x) \\ &= ([(a_0 + b_0) + c_0]_5 + [(a_1 + b_1) + c_1]_5 x) \\ &= ([a_0 + (b_0 + c_0)]_5 + [a_1 + (b_1 + c_1)]_5 x) \\ &= ([a_0]_5 + [a_1]_5 x) + ([b_0 + c_0]_5 + [b_1 + c_1]_5 x) \\ &= ([a_0]_5 + [a_1]_5 x) + (([b_0]_5 + [b_1]_5 x) + ([c_0]_5 + [c_1]_5 x)) = f + (g + h) \end{aligned} \tag{12}$$

(c) *(Existence of an Additive Identity)* We claim the additive identity is just the zero polynomial $[0]_5$ (technically $[0]_5 + [0]_5 x$). We verify this quickly, needing only one side as our addition is commutative:

$$\begin{aligned} f + ([0]_5 + [0]_5 x) &= ([a_0]_5 + [a_1]_5 x) + ([0]_5 + [0]_5 x) \\ &= ([a_0 + 0]_5 + [a_1 + 0]_5 x) = ([a_0]_5 + [a_1]_5 x) = f \end{aligned} \tag{13}$$

(d) *(Existence of Additive Inverses)* We just levee the additive inverses from $\mathbb{F}_5$, again only needing one side as our addition is commutative:

$$\begin{aligned} f + ([-a_0]_5 + [-a_1]_5 x) &= ([a_0]_5 + [a_1]_5 x) + ([-a_0]_5 + [-a_1]_5 x) \\ &= [a_0 - a_0]_5 + [a_1 - a_1]_5 x = [0]_5 \end{aligned} \tag{14}$$

(e) *(Associativity of Multiplication)* We use a couple of facts, including distributivity in $\mathbb{F}_5$, as well as commutativity and associaivity of multiplication:

$$\begin{aligned} (f \cdot g) \cdot h &= ([2a_1b_1 + a_0b_0]_5 + [a_1b_0 + a_0b_1]x) \cdot ([c_0]_5 + [c_1]_5 x) \\ &= [2a_1b_1c_0 + 2a_1b_1c_0 + 2a_0b_1c_1 + a_0b_0c_0] + [2a_1b_1c_1 + a_0b_0c_1 + a_1b_0c_0 + a_0b_1c_0]x \\ &= ([a_0]_5 + [a_1]_5 x) \cdot ([2b_1c_1 + b_0c_0]_5 + [b_1c_0 + b_0c_1]_5 x) = f \cdot (g \cdot h) \end{aligned} \tag{15}$$

(f) *(Existence of a Multiplicative Identity)* We again quickly verify the multiplicative identity is just the polynomial $[1]_5$, needing only one direction as we later prove the multiplication is commutative:

$$\begin{aligned} f \cdot [1]_5 = ([a_0]_5 + [a_1]_5 x) \cdot [1]_5 = \\ ([a_0(1)]_5 + [a_1(1)]_5 x) = ([a_0]_5 + [a_1]_5 x) = f \end{aligned} \tag{16}$$

(g) *(Distributivity of Multiplication over Addition)* We use distributivity and commutativity largely to get the following:

$$\begin{aligned} f \cdot (g + h) &= ([a_0]_5 + [a_1]_5 x) \cdot ([b_0 + c_0]_5 + [b_1 + c_1]_5 x) \\ &= [a_0b_0 + a_0c_0]_5 + [a_0b_1 + a_0c_1]_5 x + [a_1b_0 + a_1c_0]x + [2a_1b_1 + 2a_1c_1] \\ &= ([2a_1b_1 + a_0b_0]_5 + [a_1b_0 + a_0b_1]_5 x) + ([2a_1c_1 + a_0c_0]_5 + [a_1c_0 + a_0c_1]x) \\ &= (f \cdot g) + (f \cdot h) \end{aligned} \tag{17}$$

These facts taken together verify R is a ring. □

(c) Prove that $([a]_5 + [b]_5 x)([a]_5 - [b]_5 x) = [a^2 - 2b^2] \neq [0]_5$ unless $[a]_5 = [b]_5 = [0]_5$.

Proof. Obviously, this expression is zero when a and b are such. Thus we just need to prove $([a]_5 + [b]_5 x)([a]_5 - [b]_5 x) = [a^2 - 2b^2] = [0]_5$ implies $[a]_5 = [b]_5 = [0]_5$.

For this, we consider the following argument, assuming $b \neq 0$ (so that it has an inverse).

$$\begin{aligned} [a^2 - 2b^2]_5 = [0]_5 &\to [a^2]_5 = [2b^2]_5 \\ \to [a]_5^2 = [2]_5[b]_5^2 &\to [a]^2[b]_5^{-2} = [2]_5 \\ &\to ([a][b]_5^{-1})^2 = [2]_5 \end{aligned} \tag{18}$$

But then this is a contradiction as $[a][b]_5^{-1} \in \mathbb{F}_5$ and we showed there is no element that has $[2]_5$ as its square.

So it must be $[b]_5 = 0$. It follows then $[a^2 - 2b^2] = [a^2] = [a]^2 = [0]_5$, but we trivially verify the only element in $\mathbb{F}_5$ with its square as $[0]_5$ is just $[0]_5$.

Thus here $[a]_5 = [b]_5 = 0$ as desired. □

(d) Prove that R is a field.

Proof. We need to verify now, in addition, commutativity of multiplication and the existence of multiplicative inverses for nonzero elements. Note we already have $1 \neq 0$ here.

(a) *(Commutativity of Multiplication)* We just use commutativity in $\mathbb{F}_5$:

$$\begin{aligned} f \cdot g = ([a_0]_5 + [a_1]_5 x) \cdot ([b_0]_5 + [b_1]_5) \\ = [2a_1b_1 + a_0b_0]_5 + [a_1b_0 + a_0b_1]_5 x = [2b_1a_1 + b_0a_0]_5 + [b_1a_0 + b_0a_1]_5 x \\ = g \cdot f \end{aligned} \tag{19}$$

(b) *(Existence of Multiplicative Inverses)* We claim that for nonzero polynomial $[a]_5 + [b]_5 x$, its inverse is $[a]_5[a^2 - 2b^2]_5^{-1} + [-b]_5[a^2 - 2b^2]_5^{-1} x$.

Note this is where we are using part (c), as we know as long as our polynomial isn't zero (i.e. $[a]_5 \neq [0]_5$ or $[b]_5 \neq [0]_5$) that $[a^2 - 2b^2]_5$ is nonzero, and thus it has an inverse.

$$\begin{aligned} f \cdot ([a]_5[a^2 - 2b^2]_5^{-1} + [-b]_5[a^2 - 2b^2]_5^{-1} x) = \\ ([a]_5 + [b_5]x) \cdot ([a]_5[a^2 - 2b^2]_5^{-1} + [-b]_5[a^2 - 2b^2]_5^{-1} x) \\ = [a^2][a^2 - 2b^2]_5^{-1} + [-2b^2][a^2 - 2b^2]_5^{-1} = \\ ([a^2 - 2b^2]_5)[a^2 - 2b^2]_5^{-1} = [1]_5 \end{aligned} \tag{20}$$

And so R is a field. □

Exercise 3. Let R be a commutative ring and let $I, J \subseteq R$ be ideals. We define a set $I + J$ as the set of all possibles sums of elements in I and J, i.e. $I + J = \{i + j : i \in I, j \in J\}$.

(a) Prove that $I + J$ is an ideal.

Proof. We first show that $I + J$ is an additive subgroup of R. For this, first note $I + J$ is nonempty, as all ideals include the additive identity (and so the sum $0 + 0 = 0 \in I + J$).

Let then $(i_1 + j_1), (i_2 + j_2) \in I + J$. To show that $I + J$ is an additive subgroup, we want that the following holds:

$$(i_1 + j_1) - (i_2 + j_2) \in I + J \tag{21}$$

Note then that $-(i_2 + j_2) = -i_2 - j_2$. Thus we reorganize the expression to get $(i_1 - i_2) + (j_1 - j_2)$.

But this of course must be in $I + J$, as we have $i_1 - i_2 \in I$ and $j_1 - j_2 \in J$, given that they are ideals.

That $I + J$ is closed under multiplication with outside elements is even simpler, we just note for all $r \in R$:

$$(i_1 + j_1)r = i_1 r + j_1 r \tag{22}$$

But then again, as I and J are ideals, the terms on the right are in I and J respectively, so the left term is in $I + J$ (as R is commutative, we only need to check one side of multiplication).

It follows $I + J$ is an ideal. □

(b) Suppose $K \subseteq R$ is any ideal containing both I and J. Show that $I + J \subseteq K$.

Proof. Consider some element $i_1 + j_1 \in I + J$. We know $i_1 \in I \subseteq K$ and $j_1 \in J \subseteq K$. Then, as K is an ideal (and thus an additive subgroup), we must have $i_1 + j_1 \in K$, but this proves it. □

(c) Prove that $I \cap J$ is an ideal.

Proof. First note $I \cap J$ is nonempty as all ideals must contain the additive identity (i.e. it contains the additive identity). Consider then some $k_1, k_2 \in I \cap J$.

Of course then, $k_1, k_2 \in I$ and $k_1, k_2 \in J$. Thus $k_1 - k_2 \in I$ and $k_1 - k_2 \in J$ (using additive subgroup properties), so we have $k_1 - k_2 \in I \cap J$.

Thus $I \cap J$ is an additive subgroup. Similarly, we have for all $r \in R$ that $k_1 r \in I$ given $k_1 \in I$ and and $k_1 r \in J$ given $k_1 \in J$.

Thus $k_1 r \in I \cap J$, so $I \cap J$ is an ideal. □