David Owen Horace Cutler | Math 146: Midterm | March 15, 2024

Exercise 1. Let R be the set of all functions $f : \mathbb{R} \to \mathbb{R}$. Given $f, g \in R$, let $f + g$ and $f \cdot g$ be the usual function addition and function multiplication.

(a) Prove that R is a commutative ring.

Proof. We need to verify the ring axioms and that multiplication is commutative.

Note of course we have closure under these operations, as the pointwise sum and product of two functions is nonetheless a function.

(i) *(Addition is commutative)* Consider $f, g \in R$ and let $x \in \mathbb{R}$. We note the following:

$$\begin{aligned}(f+g)(x) &= f(x) + g(x) \\ &= g(x) + f(x) && \text{(Commutativity in } \mathbb{R}\text{)} \\ &= (g+f)(x)\end{aligned}$$

Thus $(f + g)(x) = (g + f)(x)$ for all $x \in \mathbb{R}$, so $f + g = g + f$.

(ii) *(Addition is associative)* Consider $f, g, h \in R$ and let $x \in \mathbb{R}$. We have the following:

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x) + h(x) \\ &= (f(x) + g(x)) + h(x) \\ &= f(x) + (g(x) + h(x)) && \text{(Associativity in } \mathbb{R}\text{)} \\ &= f(x) + (g+h)(x) \\ &= (f + (g+h))(x)\end{aligned}$$

Consequently $((f + g) + h)(x) = (f + (g + h))(x)$ for all $x \in \mathbb{R}$, so $(f + g) + h = f + (g + h)$.

(iii) *(An additive identity exists)* We claim the additive identity is the zero function 0, defined by $0(x) = 0$. Clearly $0 \in R$.

Let $f \in R$, and $x \in \mathbb{R}$. We note the following:

$$\begin{aligned}(f+0)(x) &= f(x) + 0(x) \\ &= f(x) + 0 \\ &= f(x) && \text{(Identity in } \mathbb{R}\text{)}\end{aligned}$$

By reasoning similar to the previous parts then, we know $(f+0) = f$. As addition is commutative in R then, this is a proper additive identity.

(iv) *(Additive inverses exist)* Let $f \in R$. Define the function $-f$ by $(-f)(x) = -f(x)$, where the latter is the additive inverse of $f(x)$ in $\mathbb{R}$.

Clearly $-f$ is a function, so $-f \in R$. Let then $x \in \mathbb{R}$, we note:

$$\begin{aligned}(f + (-f))(x) &= f(x) + (-f)(x) \\ &= f(x) - f(x) \\ &= 0 && \text{(Additive inverse in } \mathbb{R}) \\ &= 0(x)\end{aligned}$$

Thus $(f + (-f)) = 0$. The commutativity of addition in R thus has this is a proper additive inverse.

(v) *(Multiplication is commutative)* Consider $f, g \in R$ and let $x \in \mathbb{R}$. We note the following:

$$\begin{aligned}(f \cdot g)(x) &= f(x) \cdot g(x) \\ &= g(x) \cdot f(x) && \text{(Commutativity in } \mathbb{R}) \\ &= (g \cdot f)(x)\end{aligned}$$

Thus $(f \cdot g)(x) = (g \cdot f)(x)$ for all $x \in \mathbb{R}$, so $f \cdot g = g \cdot f$.

(vi) *(Multiplication is associative)* Consider $f, g, h \in R$ and let $x \in R$. We note the following:

$$\begin{aligned}((f \cdot g) \cdot h)(x) &= (f \cdot g)(x) \cdot h(x) \\ &= (f(x) \cdot g(x)) \cdot h(x) \\ &= f(x) \cdot (g(x) \cdot h(x)) && \text{(Associativity in } \mathbb{R}) \\ &= f(x) \cdot (g \cdot h)(x) \\ &= (f \cdot (g \cdot h))(x)\end{aligned}$$

Consequently $((f \cdot g) \cdot h)(x) = (f \cdot (g \cdot h))(x)$ for all $x \in \mathbb{R}$, so $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

(vii) *(A multiplicative identity exists)* We claim the multiplicative identity is the constant function 1, defined by $1(x) = 1$. Clearly $1 \in R$.

Let $f \in R$, and $x \in \mathbb{R}$. We note the following:

$$\begin{aligned}(f \cdot 1)(x) &= f(x) \cdot 1(x) \\ &= f(x) \cdot 1 \\ &= f(x) && \text{(Identity in } \mathbb{R})\end{aligned}$$

By reasoning similar to the previous parts then, we know $(f \cdot 1) = f$. As multiplication is commutative in R then, this is a proper additive identity.

(viii) *(Multiplication distributes over addition)* Let $f, g, h \in R$ and consider $x \in \mathbb{R}$. We

get the following:

$$\begin{aligned}(f \cdot (g+h))(x) &= f(x) \cdot (g+h)(x) \\ &= f(x) \cdot (g(x) + h(x)) \\ &= (f(x) \cdot g(x)) + (f(x) \cdot h(x)) \qquad \text{(Distributivity in } \mathbb{R}\text{)} \\ &= (f \cdot g)(x) + (f \cdot h)(x) \\ &= ((f \cdot g) + (f \cdot h))(x)\end{aligned}$$

It follows $f \cdot (g+h) = (f \cdot g) + (f \cdot h)$. The commutativity of multiplication shows that distribution holds in the other direction.

With all these axioms verified, it follows R is a ring. □

(b) Prove that every non-zero element of R is either a unit or a zero-divisor.

Proof. To prove this, we establish a small lemma.

Lemma 1. If $f \in R$ is not a zero divisor, then for all $x \in \mathbb{R}$ we have $f(x) \neq 0$.

Proof. Assume for the sake of contradiction that f is not a zero divisor, but we have some $a \in \mathbb{R}$ for which $f(a) = 0$.

Define then the function g by stipulating

$$g(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{if } x \neq a \end{cases}$$

We note clearly $g \neq 0$, as $g(a) = 1$. However, we note for a and for $x \neq a$ that

$$\begin{aligned}(f \cdot g)(a) &= f(a) \cdot g(a) = 0 \cdot 1 = 0 \\ (f \cdot g)(x) &= f(x) \cdot g(x) = f(x) \cdot 0 = 0\end{aligned}$$

So the product $f \cdot g = 0$ where $g \neq 0$. But then this is exactly that f is a zero divisor, a contradiction. Thus the claimed result holds. □

With this lemma then, let $f \in R$ not a zero divisor. It follows for all $x \in \mathbb{R}$, $f(x) \neq 0$.

Define then the function f' by $f'(x) = f(x)^{-1}$, where $f(x)^{-1}$ refers to the multiplicative inverse of $f(x)$ in $\mathbb{R}$. Note these inverses exist as each $f(x) \neq 0$.

We claim then f' is the inverse of f, such that f is a unit. Recall as we established multiplication to be commutative we need only establish it is an inverse on one side.

Let $x \in \mathbb{R}$. It follows:

$$\begin{aligned}(f \cdot f')(x) &= f(x) \cdot f'(x) \\ &= f(x) \cdot f(x)^{-1} \\ &= 1 && \text{(Multiplicative inverse in } \mathbb{R}) \\ &= 1(x)\end{aligned}$$

Thus $f \cdot f' = 1$, i.e. f' is a right inverse. As noted earlier then, commutativity of multiplication also has it is a left inverse. Thus f is a unit.

As we only made the assumption f wasn't a zero divisor then, it follows all elements of R are either zero divisors or units. □

(c) Let $\mathcal{S}$ be any subset of $\mathbb{R}$. Prove that the set $V(\mathcal{S}) = \{f \in R \mid f(s) = 0 \text{ for all } s \in S\}$ is an ideal of R.

Proof. We need to show $V(\mathcal{S})$ is an additive subgroup and that it absorbs multiplication. Note $V(\mathcal{S})$ is of course a subset.

(1) *(Nonemptiness)* Remark that $V(\mathcal{S})$ always clearly always contains the zero function, even when $\mathcal{S} = \emptyset$ (in which case $V(\mathcal{S})$ is the whole ring).

(2) *(Closure under addition)* Let $f, g \in V(\mathcal{S})$, i.e. $f(s) = g(s) = 0$ for all $s \in \mathcal{S}$. Let $s \in \mathcal{S}$. Note the following:

$$\begin{aligned}(f + g)(s) &= f(s) + g(s) \\ &= 0 + 0 \\ &= 0\end{aligned}$$

It follows $(f + g)(s) = 0$ for all $s \in \mathcal{S}$. Thus $f + g \in V(\mathcal{S})$.

(3) *(Closure under inverses)* Let $f \in \mathcal{S}$, i.e. $f(s) = 0$ for all $s \in \mathcal{S}$. Let $-f$ denote the additive inverse of f as defined earlier, and let $s \in \mathcal{S}$. We note:

$$\begin{aligned}(-f)(s) &= -f(s) \\ &= -0 \\ &= 0\end{aligned}$$

Thus $(-f)(s) = 0$ for all $s \in \mathcal{S}$. It follows $-f \in V(\mathcal{S})$.

(4) *(Closure under outside multiplication)* Let $f \in V(\mathcal{S})$ and let $g \in R$. Moreover, consider $s \in \mathcal{S}$. We note the following:

$$\begin{aligned}(f \cdot g)(s) &= f(s) \cdot g(s) \\ &= 0 \cdot g(s) \\ &= 0\end{aligned}$$

Therefore $f \cdot g \in V(\mathcal{S})$ as s was arbitrary. Recall this is enough as multiplication is commutative.

It follows $V(\mathcal{S})$ is an ideal. □

(d) Prove that ${}^{R}\!/_{V(\{0\})} \cong \mathbb{R}$.

Proof. Consdider the evaluation homomorphism $\phi_0 : R \to \mathbb{R}$ defined by $f \mapsto f(0)$.

Clearly this is a homomorphism given our pointwise operations, but we quickly verify this:

$$\phi(f+g) = (f+g)(0) = f(0) + g(0) = \phi(f) + \phi(g)$$
$$\phi(f \cdot g) = (f \cdot g)(0) = f(0) \cdot g(0) = \phi(f) \cdot \phi(g)$$

Note then that clearly $\text{im}(\phi_0) = \mathbb{R}$, as for any given $x \in \mathbb{R}$, the function that is identically x is in R, and of course ϕ_0 maps this function to x.

We want to determine the kernel of ϕ_0 then. Let $f \in \ker(\phi_0)$ then, we have

$$0 = \phi_0(f) = f(0),$$

which by definition has $f \in V(\{0\})$. Considering a new $f \in V(\{0\})$ then, we have of course $f(0) = 0$. Thus

$$\phi_0(f) = f(0) = 0,$$

which in tandem with the previous fact clearly shows $\ker(\phi_0) = V(\{0\})$.

With this established then, as R and $\mathbb{R}$ are rings, we can appeal to the **First Isomorphism Theorem** to get:

$${}^{R}\!/_{V(\{0\})} = {}^{R}\!/_{\ker(\phi_0)} \cong \text{im}(\phi_0) = \mathbb{R},$$

which is of course

$${}^{R}\!/_{V(\{0\})} \cong \mathbb{R}.$$

□

Exercise 2. Let R be a commutative ring and define

$$I = \{r \in R \mid r^n = 0 \text{ for some } n \geq 0\}.$$

Prove that I is an ideal of R.

Proof. We need to show I is a additive subgroup and that it absorbs multiplication. Note I here is of course a subset.

(a) *(Additive subgroup)* We work first to show I is additive subgroup.

(i) *(Nonemptiness)* Remark that I clearly contains the additive identity.

(ii) *(Closure under addition)* Let $r, s \in I$, i.e. for some integers $n, m \geq 0$ we have

$$r^n = 0 = s^m.$$

We want to show that $r + s \in I$. For this consider the expansion of $(r+s)^{n+m}$ using the binomial formula, where $n + m \geq 0$:

$$(r+s)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} r^{n+m-k} s^k$$

Note then that in this expansion either the exponent of r is $\geq n$ or the exponent of s is $\geq m$. Of course, r raised to any exponent greater than n is zero; similar for s with an exponent greater than m.

It follows every term of this sequence vanishes, as the product $r^{n+m-k}s^k$ is consequently 0 for any k where $0 \leq k \leq n+m$. It follows $r+s \in I$ then as $(r+s)^{n+m} = 0$ where $n + m \geq 0$.

(iii) *(Closure under inverses)* Let $r \in I$. We want to show $-r \in I$.

In particular, take $n \geq 0$ such that $r^n = 0$. Then we note

$$(-r)^n = (-1 \cdot r)^n = (-1)^n r^n = (-1)^n \cdot 0 = 0,$$

and so $-r \in I$. Note $-r = -1 \cdot r$ holds in rings in general.

(b) *(Closure under outside multiplication)* Let $i \in I$ such that $i^n = 0$ for $n \geq 0$. Let $r \in R$. We want to show $ir = ri \in I$. For this note

$$(ir)^n = i^n r^n = 0 \cdot r^n = 0,$$

and so it follows $ri = ir \in I$.

With these two criteria verified, it follows I is an ideal. □

Exercise 3. Let $\phi : F \to K$ be a nonzero homomorphism of fields. Prove that the characteristics of F and K are equal.

Proof. Recall that the characteristic of a field F is the generator of the principal ideal that is the kernel of the unique ring homomorphism $\varphi : \mathbb{Z} \to F$ where $\varphi(1) = 1$ (ideals in $\mathbb{Z}$ are principal).

Consider this φ into our field F. Clearly then $\varphi(1) = 1$. Moreover, as K is a field, it is an integral domain, so as ϕ is nonzero we know $\phi(1) = 1$.

Note then as the composition of ring homomorphisms is a ring homomorphisms, $\phi \circ \varphi : \mathbb{Z} \to K$ is a homomorphism. By our previous observations then, we know

$$\phi \circ \varphi = \phi(\varphi(1)) = \phi(1) = 1,$$

and so it follows $\phi \circ \varphi$ is the unique homomorphism $\mathbb{Z} \to K$ that sends $1 \in \mathbb{Z}$ to the multiplicative identity of K.

We want to show the kernel of $\phi \circ \varphi$ is that of φ then. First we note as ϕ is a homomorphism, we know $\phi(0) = 0$. Naturally then

$$\ker(\varphi) \subseteq \ker(\phi \circ \varphi).$$

Consider then some $x \in \ker(\phi \circ \varphi)$, i.e.

$$\phi(\varphi(x)) = 0.$$

Note then that as $\phi : F \to K$ is a nonzero homomorphism and F is a field, it must be $\ker(\phi) = \{0\}$ as the kernel is an ideal and the online ideals of F are $F, \{0\}$, where the former is impossible given the nonzero assumption.

Thus is must be $\varphi(x) = 0$, but this is exactly $x \in \ker(\varphi)$, and so

$$\ker(\phi \circ \varphi) \subseteq \ker(\varphi),$$

which has $\ker(\phi \circ \varphi) = \ker(\varphi)$.

But of course $\ker(\varphi) = m\mathbb{Z}$, where m is the characteristic of K. Moreover, $\ker(\phi \circ \varphi) = n\mathbb{Z}$, where n is the characteristic of F.

As $\ker(\phi \circ \varphi) = \ker(\varphi)$ then, the only possibility is $n = m$, i.e. $\text{char}(K) = \text{char}(F)$. □

Exercise 4. Let F be a field and K an extension of F. Let $\alpha \in K$ algebraic over F. Prove that α^2 is also algebraic over F.

Proof. Let $\phi_\alpha : F[x] \to K$ be the homomorphism given by evaluation at α. Clearly ϕ_α is indeed a ring homomorphism as we have

$$(fg)(\alpha) = f(\alpha) \cdot g(\alpha) \text{ and } (f + g)(\alpha) = f(\alpha) + g(\alpha).$$

As α is algebraic over F, it has a miniminal polynomial $f \in F[x]$ with degree n. We claim then that $\ker(\phi_\alpha) = (f)$.

Note first clearly that $(f) \subseteq \ker(\phi_\alpha)$, as all elements of (f) are of the form fg and consequently

$$\phi_\alpha(fg) = \phi_\alpha(f)\phi_\alpha(g) = f(\alpha)\phi_\alpha(g) = 0 \cdot \phi_\alpha(g) = 0.$$

Consider the inclusion $\ker(\phi_\alpha) \subseteq (f)$. If $g \in \ker(\phi_\alpha)$ this is exactly that $g(\alpha) = 0$, i.e. α is a root of g.

As f is the minimal polynomial of α then, it must be $f|g$ (this is simply seen by appeling to the division algorithm). It follows

$$\ker(\phi_\alpha) \subseteq (f),$$

and thus $\ker(\phi_\alpha) = (f)$ in general. Let then $F[\alpha]$ defined as the following:

$$F[a] = \{f(\alpha) \mid f \in F[x]\}$$

By construction $\text{im}(\Phi) = F[\alpha]$. Appealing to the **First Isomorphism Theorem** then, we know

$$F[x]/(f) \cong F[\alpha]$$

As discussed in class, $F[x]/(f)$ is a field extension of F such that

$$[F[x]/(f) : F] = \deg(f) = n,$$

and so as $F[x]/(f) \cong F[\alpha]$, it is clear that $[F[x]/(f) : F] = [F[\alpha] : F]$.

Thus this has that $F[\alpha]$ is a finite extension of F, and so it is algebraic. Note then $\alpha^2 \in F[\alpha]$ as it is $x^2 \in F[x]$ evaluated at α. As $F[\alpha]$ is an algebraic extension then, it must be α^2 is algebraic over $F[x]$.

□

Exercise 5. Let $k \geq 2$ be an integer, and let $F = \mathbb{F}_{2^k}$ be the field with order 2^k. Define $\phi : F \to F$ by $\phi(a) = a^2$.

(a) Prove that ϕ is a nontrivial homomorphism from F to itself.

Proof. We first prove a small lemma.

Lemma 2. Let $k \in \mathbb{N}$. Then the field of order 2^k, i.e. $\mathbb{F}_{2^k}$, has characteristic 2.

Proof. We know, as discussed in class, that a field F either has $\text{char}(F) = p$ for prime p or $\text{char}(F) = 0$.

A simple pigeonhole argument shows that finite fields cannot have characteristic zero, so it follows $\text{char}(\mathbb{F}_{2^k}) = p$ for some prime p. Moreover, we know the order of $\mathbb{F}_{2^p}$, i.e. $|\mathbb{F}_{2^p}| = 2^p$.

We can consider the additive subgroup formed by repeated addition of 1 then. Clearly, the size of this subgroup should be p, by the definition of characteristic. By **Lagrange's Theorem** then, we know it should be

$$p \mid 2^k, \text{ i.e. } p \text{ divides } 2^k,$$

but of course then it must be that $p = 2$, appealing to the uniqueness of prime factorization, or even by **Euclid's Lemma**.

Thus it is that $\text{char}(\mathbb{F}_{2^k}) = 2$ □

With this lemma established then, we want to show ϕ is a nontrivial homomorphism. To do this, we need to show it cooperates with the additive and multiplicative structures on F.

To do this, we prove another *even quicker* lemma.

Lemma 3. Let $a, b \in F$. Then $(a+b)^2 = a^2 + b^2$.

Proof. We can expand $(a+b)^2$, i.e.

$$(a+b)^2 = a^2 + ba + ab + b^2,$$

which is precisely

$$a^2 + (1+1)ab + b^2,$$

but as F is characteristic 2, we know $1+1=0$. So the ab term vanishes, and we are just left with

$$(a+b)^2 = a^2 + b^2.$$

□

With this final lemma then, we establish ϕ is a homomorphism $F \to F$ very quickly, as

$$\begin{aligned} \phi(a+b) = (a+b)^2 = a^2 + b^2 = \phi(a) + \phi(b) \\ \phi(ab) = (ab)^2 = a^2 b^2 = \phi(a)\phi(b), \end{aligned}$$

where in the last part we are just using commutativity of multiplication.

Clearly this homomorphism is additionally "nontrivial", as it is assuredly nonzero by definition (consider $\phi(1)$).

Moreover, it is *not* the identity mapping, as for some nonzero element $a = \phi(a) = a^2$ quickly implies $a = 1$ by applying multiplicative inverses.

As $k \geq 2$ then, we know we are not working in $\mathbb{F}_2$, so there is an element which is neither 0 nor 1, and thus it will not be mapped to itself. □

(b) Prove that ϕ is an isomorphism.

Proof. It suffices to show ϕ is an injection, as F is of finite cardinality, and so injectivity implies surjectivity.

Note then as F is a field, it has as ideals only $\{0\}$ and F. As $\ker(\phi)$ an ideal then, and we showed that the mapping is not the zero homomorphism, it must be that

$$\ker \phi = \{0\},$$

as it cannot be the whole F. Thus the kernel is trivial, and so ϕ is an injection. As outlined earlier then, it is also a surjection.

Using this together with the fact that ϕ is a homomorphism shows it is an isomorphism. $\square$