University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 6

Tom Winckelman (edited by Darij Grinberg)

May 15, 2019

Exercise 3: Entangled inverses

Let $\mathbb{K}$ be a ring.

A *left inverse* of an element $x \in \mathbb{K}$ is defined to be a $y \in \mathbb{K}$ such that $yx = 1$.

A *right inverse* of an element $x \in \mathbb{K}$ is defined to be a $y \in \mathbb{K}$ such that $xy = 1$.

Let a and b be two elements of $\mathbb{K}$. Prove the following:

(a) If c is a left inverse of $1 - ab$, then $1 + bca$ is a left inverse of $1 - ba$.

(b) If c is a right inverse of $1 - ab$, then $1 + bca$ is a right inverse of $1 - ba$.

(c) If c is an inverse of $1 - ab$, then $1 + bca$ is an inverse of $1 - ba$.

Here and in the following, the word "*inverse*" (unless qualified with an adjective) means "multiplicative inverse".

Solution

(a) Assume that c is a left inverse of $1-ab$. That is, $c(1-ab)=1$. It follows that:[1]

$$\begin{aligned}
&(1+bca)(1-ba)\\
&=(1-ba)+bca(1-ba) && \text{(by distributivity, since } \mathbb{K} \text{ is a ring)}\\
&=1-ba+bca-bcaba && \text{(by distributivity)}\\
&=1+(-b)(a-ca+caba) && \text{(by distributivity)}\\
&=1+(-b)(1-c+cab)a && \text{(by distributivity)}\\
&=1+(-b)(1-c(1-ab))a && \text{(by distributivity)}\\
&=1+(-b)(1-1)a && \text{(since } c(1-ab)=1\text{)}\\
&=1+(-b)(0)a && \text{(since } -1 \text{ is the additive inverse of } 1\text{)}\\
&=1+0 && \text{(since zero annihilates)}\\
&=1. && \text{(since zero is the neutral element of addition)}
\end{aligned}$$

In other words, $1+bca$ is a left inverse of $1-ba$. This solves part **(a)**.

(b) Assume that c is a right inverse of $1-ab$. That is, $(1-ab)c=1$. It follows that:

$$\begin{aligned}
&(1-ba)(1+bca)\\
&=(1+bca)-ba(1+bca) && \text{(by distributivity)}\\
&=1+bca-ba-babca && \text{(by distributivity)}\\
&=1+b(ca-a-abca) && \text{(by distributivity)}\\
&=1+b(c-1-abc)a && \text{(by distributivity)}\\
&=1+b(c-abc-1)a && \text{(by commutativity of addition, since } \mathbb{K} \text{ is a ring)}\\
&=1+b((1-ab)c-1)a && \text{(by distributivity)}\\
&=1+b(1-1)a && \text{(since } (1-ab)c=1\text{)}\\
&=1+b(0)a && \text{(since } -1 \text{ is the additive inverse of } 1\text{)}\\
&=1+0 && \text{(since zero annihilates)}\\
&=1. && \text{(since zero is the neutral element of addition)}
\end{aligned}$$

In other words, $1+bca$ is a right inverse of $1-ba$. This solves part **(b)**.

(c) Assume that c is an inverse of $1-ab$. In other words, $c\,(1-ab)=1$ and $(1-ab)\,c=1$. Hence, c is a left inverse of $1-ab$ and c is a right inverse of $1-ab$. Therefore, parts **(a)** and **(b)** imply that $1+bca$ is a left inverse of $1-ba$ and $1+bca$ is a right inverse of $1-ba$. In other words,

$$(1+bca)(1-ba)=1=(1-ba)(1+bca).$$

Therefore, by the definition of an inverse, $1+bca$ is an inverse of $1-ba$. This solves part **(c)**.

---

[1] Here and in the following, when we refer to "distributivity", we mean distributivity laws in the wide sense of this word. This includes identities like $u\,(x+y+z)=ux+uy+uz$ and $u\,(x-y+z)=ux-uy+uz$. All of these identities can easily be proven from the ring axioms and the definition of subtraction.

Exercise 4: Composition of ring homomorphisms

Problem

Let $\mathbb{K}$, $\mathbb{L}$ and $\mathbb{M}$ be three rings. Prove the following:

(a) If $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ are two ring homomorphisms, then $g \circ f : \mathbb{K} \to \mathbb{M}$ is a ring homomorphism.

(b) If $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ are two ring isomorphisms, then $g \circ f : \mathbb{K} \to \mathbb{M}$ is a ring isomorphism.

Solution

(a) Let $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ be two ring homomorphisms.
In order to prove that $g \circ f : \mathbb{K} \to \mathbb{M}$ is a ring homomorphism, we must prove four things:

(i) $(g \circ f)(a+b) = (g \circ f)(a) + (g \circ f)(b)$ for all $a, b \in \mathbb{K}$.
(ii) $(g \circ f)(0_{\mathbb{K}}) = 0_{\mathbb{M}}$.
(iii) $(g \circ f)(ab) = (g \circ f)(a) \cdot (g \circ f)(b)$ for all $a, b \in \mathbb{K}$.
(iv) $(g \circ f)(1_{\mathbb{K}}) = 1_{\mathbb{M}}$.

We begin by proving **(i)**. Fix arbitrary $a \in \mathbb{K}$ and $b \in \mathbb{K}$. Thus, we have

$$f(a+b) = f(a) + f(b),$$

since f is a ring homomorphism. Now, let us apply g to both sides, yielding:

$$g(f(a+b)) = g(f(a) + f(b)). \tag{1}$$

The left hand side of (1) is clearly equal to $(g \circ f)(a+b)$ by the definition of $g \circ f$. Since g is a ring homomorphism, we obtain:

$$g(f(a) + f(b)) = g(f(a)) + g(f(b)) = (g \circ f)(a) + (g \circ f)(b)$$

(by the definition of $g \circ f$). Hence, (1) rewrites as $(g \circ f)(a+b) = (g \circ f)(a) + (g \circ f)(b)$. Thus, **(i)** is proven. The proof of **(iii)** is similar.

To see that **(ii)** is true, observe that $f(0_{\mathbb{K}}) = 0_{\mathbb{L}}$ (since f is a ring homomorphism) and $g(0_{\mathbb{L}}) = 0_{\mathbb{M}}$ (likewise). Hence, $(g \circ f)(0_{\mathbb{K}}) = g\left(\underbrace{f(0_{\mathbb{K}})}_{=0_{\mathbb{L}}}\right) = g(0_{\mathbb{L}}) = 0_{\mathbb{M}}$. This proves **(ii)**. The proof of **(iv)** is similar.

Together, **(i)**, **(ii)**, **(iii)**, and **(iv)** imply that $g \circ f : \mathbb{K} \to \mathbb{M}$ is a ring homomorphism. This solves part **(a)**.

(b) Let $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ be two ring isomorphisms.
Thus, f and g are invertible, and f, g, f^{-1}, and g^{-1} are ring homomorphisms.

From the fact that f and g are ring homomorphisms, we conclude using part **(a)** of this exercise that $g \circ f : \mathbb{K} \to \mathbb{M}$ is a ring homomorphism.

As well, from the fact that f and g are invertible, we obtain that $g \circ f$ is invertible by well known properties of functions.

From the fact that g^{-1} and f^{-1} are ring homomorphisms, we conclude using part **(a)** of the exercise (applied to $\mathbb{M}$, $\mathbb{K}$, g^{-1} and f^{-1} instead of $\mathbb{K}$, $\mathbb{M}$, f and g) that $f^{-1} \circ g^{-1} : \mathbb{M} \to \mathbb{K}$ is a ring homomorphism. In other words, $(g \circ f)^{-1}$ is a ring homomorphism (since $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$). Thus, $g \circ f$ is an invertible ring homomorphism whose inverse $(g \circ f)^{-1}$ is a ring homomorphism as well. In other words, $g \circ f$ is a ring isomorphism. This proves part **(b)**.

Exercise 6: The characteristic of a field

Problem

Let $\mathbb{F}$ be a field. Recall that we have defined na to mean $\underbrace{a + a + \cdots + a}_{n \text{ times}}$ whenever $n \in \mathbb{N}$ and $a \in \mathbb{F}$.

Assume that there exists a positive integer n such that $n \cdot 1_{\mathbb{F}} = 0$. Let p be the **smallest** such n.

Prove that p is prime.

[**Hint:** $(a \cdot 1_{\mathbb{F}}) \cdot (b \cdot 1_{\mathbb{F}}) = ab \cdot 1_{\mathbb{F}}$ for all $a, b \in \mathbb{N}$.]

Remark

The p we just defined is called the *characteristic* of the field $\mathbb{F}$ when it exists. (Otherwise, the characteristic of the field $\mathbb{F}$ is defined to be 0.)

Thus, for each prime p, the finite field $\mathbb{Z}/p$, as well as the finite field of size p^2 that we constructed in class, have characteristic p.

Solution

In our definition of fields, we have required a field $\mathbb{K}$ to satisfy $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$. Thus, $0_{\mathbb{F}} \neq 1_{\mathbb{F}}$ (since $\mathbb{F}$ is a field).

We have assumed that there exists a positive integer n such that $n \cdot 1_{\mathbb{F}} = 0$. Hence, by the well ordering property, the minimum

$$\min\left\{n \in \mathbb{Z}^+ : n \cdot 1_{\mathbb{F}} = 0\right\} \quad \text{exists}$$

(where $\mathbb{Z}^+$ denotes the set $\{1, 2, 3, \ldots\}$). Let m be this minimum. In other words, $m := \min\{n \in \mathbb{Z}^+ : n \cdot 1_{\mathbb{F}} = 0\}$. Then, $m \cdot 1_{\mathbb{F}} = 0 = 0_{\mathbb{F}} \neq 1_{\mathbb{F}} = 1 \cdot 1_{\mathbb{F}}$, so that $m \neq 1$. Therefore, $m > 1$ (since $m \in \mathbb{Z}^+$).

Of course, our m is exactly the number that was denoted by p in the exercise. Hence, we need to prove that m is prime.

Suppose that $m = ab$ for some $a, b \in \{1, 2, \ldots, m-1\}$. We shall derive a contradiction. We have

$$(a \cdot 1_{\mathbb{F}}) \cdot (b \cdot 1_{\mathbb{F}}) = a \underbrace{(1_{\mathbb{F}} \cdot (b \cdot 1_{\mathbb{F}}))}_{= b \cdot 1_{\mathbb{F}}} = a\,(b \cdot 1_{\mathbb{F}}) = \underbrace{ab}_{=m} \cdot 1_{\mathbb{F}} = m \cdot 1_{\mathbb{F}} = 0.$$

This implies that either $a \cdot 1_{\mathbb{F}} = 0$ or $b \cdot 1_{\mathbb{F}} = 0$. [2] Assume WLOG that $a \cdot 1_{\mathbb{F}} = 0$. Thus, $a \in \{n \in \mathbb{Z}^+ : n \cdot 1_{\mathbb{F}} = 0\}$. However, $a < m$ (since $a \in \{1, 2, \ldots, m-1\}$), so this contradicts the fact that $m = \min\{n \in \mathbb{Z}^+ : n \cdot 1_{\mathbb{F}} = 0\}$. This contradiction shows that there **do not** exist $a, b \in \{1, 2, \ldots, m-1\}$ such that $m = ab$. Hence, the only positive divisors of m are 1 and m (since any other positive divisor of m would be some $a \in \{1, 2, \ldots, m-1\}$, and the corresponding "complementary" divisor $b := m/a$ would also belong to the set $\{1, 2, \ldots, m-1\}$, which would yield that a and b are two elemnets of $\{1, 2, \ldots, m-1\}$ satisfying $m = ab$). Hence, m is prime (since $m > 1$). This is precisely what we wanted to prove, only that we called it m rather than p. This solves the exercise.

[2] Why? Recall that $\mathbb{F}$ is a field. Thus, every nonzero element of $\mathbb{F}$ is invertible. Having $(a \cdot 1_{\mathbb{F}}) \cdot (b \cdot 1_{\mathbb{F}}) = 0$, let us suppose that $a \cdot 1_{\mathbb{F}}$ and $b \cdot 1_{\mathbb{F}}$ are both nonzero. Hence, they are both invertible, since $\mathbb{F}$ is a field. Hence, the following computation is valid:

$$(b \cdot 1_{\mathbb{F}})^{-1} \cdot (a \cdot 1_{\mathbb{F}})^{-1} \cdot \underbrace{(a \cdot 1_{\mathbb{F}}) \cdot (b \cdot 1_{\mathbb{F}})}_{=0} = (b \cdot 1_{\mathbb{F}})^{-1} \cdot (a \cdot 1_{\mathbb{F}})^{-1} \cdot 0,$$

which clearly simplifies to $1_{\mathbb{F}} = 0_{\mathbb{F}}$, which contradicts $0_{\mathbb{F}} \neq 1_{\mathbb{F}}$. This contradiction shows that our assumption was false. In other words, $(a \cdot 1_{\mathbb{F}})$ and $(b \cdot 1_{\mathbb{F}})$ are **not** both not equal to zero. In other words, either $(a \cdot 1_{\mathbb{F}}) = 0$ or $(b \cdot 1_{\mathbb{F}}) = 0$.