Intro to Modern Algebra
Homework 3

Sam Cook

October 19th, 2017

1 Section 3.3 #8

Problem Let $\mathbb{Q}(\sqrt{2})$ be as in Exercise 39 of Section 3.1 Prove that the function $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ given by $f(a + b\sqrt{2}) = a - b\sqrt{2}$ is an isomorphism.

Solution In order for f to be an isomorphism, it must be a bijective homomorphism.

First, to be bijective, it must be both injective and surjective. Take $f(a), f(b)\epsilon\mathbb{Q}(\sqrt{2})$ such that $f(a) = f(b)$. Then, for some $k, l, m, n\epsilon\mathbb{Q}, f(k + l\sqrt{2}) = f(m + n\sqrt{2})$. This implies that $k - l\sqrt{2} = m - n\sqrt{2}$, by the definition of f. We can group the rational and irrational parts together to get $k - l\sqrt{2} = m - n\sqrt{2} \Rightarrow (k - m) = (l - n)\sqrt{2}$. But $(k - m)$ is rational, and $(l - n)\sqrt{2}$ is irrational. The only way this could be possible is if $(k - m) = 0$ and $(l - n) = 0$, since $(0 - 0) = (0 - 0)\sqrt{2}$. This implies that $k = m$ and $l = n$. Therefore, $k + l\sqrt{2} = m + n\sqrt{2}$, or $a = b$ and f is an injective function.

Now, consider $c + d\sqrt{2}\epsilon\mathbb{Q}(\sqrt{2})$ for any $c, d\epsilon\mathbb{Q}$. $c + d\sqrt{2}$ is mapped to from $c - d\sqrt{2}$, which can also be written as $c + (-d)\sqrt{2}$, since $f(c - d\sqrt{2}) = c + d\sqrt{2}$. Therefore, f is surjective, and as a result of that, bijective.

Now, we must prove that f is a homomorphism. Consider $f((k + l\sqrt{2}) * (m + n\sqrt{2}))$ with $(k + l\sqrt{2}), (m + n\sqrt{2})\epsilon\mathbb{Q}(\sqrt{2})$. We can multiply the terms to get $f(km + kn\sqrt{2} + ml\sqrt{2} + nl)$, which simplifies to $f((km + nl) + (kn + ml)\sqrt{2})$. By applying the function f and distributive laws, $f((km + nl) + (kn + ml)\sqrt{2}) = (km + nl) - (kn + ml)\sqrt{2}$. Now consider $f(k + l\sqrt{2}) * f(m + n\sqrt{2})$. By appliying f, we get $(k - l\sqrt{2}) * (m - n\sqrt{2})$. We can use distributive laws to get $km - kn\sqrt{2} - ml\sqrt{2} + 2nl = (km + 2nl) - (kn + ml)\sqrt{2} = f((k + l\sqrt{2}) * (m + l\sqrt{2}))$. Therefore, f preserves multiplication

Now consider $f((k + l\sqrt{2}) + (m + n\sqrt{2}))$ This simplifies to $f((k + m) + (n + l)\sqrt{2})$.Applying f, $f((k + m) + (n + l)\sqrt{2}) = (k + m) - (n + l)\sqrt{2}$. Next consider $f(k + l\sqrt{2}) + f(m + n\sqrt{2})$. Applying f, $f(k + l\sqrt{2}) + f(m + n\sqrt{2}) = (k - l\sqrt{2}) + (m - \sqrt{2}) = (k + m) - (n + l)\sqrt{2}$, by associativity. But $(k + m) - (n + l)\sqrt{2} = f((k + l\sqrt{2}) + (m + n\sqrt{2})$ and therefore f preserves addition. Since f preserves addition and multiplication, it is a homomorphism, and since it is a bijective homomorphism, it is an isomorphism.

2 Section 3.3# 12e

Problem Is the following function a homeomorphism or not?

$$f : \mathbb{Z}_{12} \to \mathbb{Z}_4 \tag{1}$$

defined by $f([x]_{12}) = [x]_4$, where $[u]_4$ denotes the class of the integer u in $\mathbb{Z}_n$

Solution First, we need to prove that this function is well defined. To do this, consider $[a]_{12}$ and $[a+k12]_{12}, k\epsilon\mathbb{Z}$ such that $a, a+12\ epsilon\mathbb{Z}_{12}$. It is clear that $[a]_{12} = [a+12]_{12}$, since these are equivalence classes in $\mathbb{Z}_{12}$. Now consider $f([a]_{12})$ and $f([a+12]_{12})$. Then applying f, $f([a]_{12}) = [a]_4$ and $f([a+12]_{12}) = [a+12]_4$. But $[a+12]_4 = [a]_4 + [12]_4 = [a]_4 + [0]_4 = [a]_4$, since it is an equivalence class. Then $f([a]_{12}) = f([a+12]_{12})$, and f is well defined.

Now, for f to be a homomorphism, it must preserve addition and multiplication. Consider $f([x]_{12} + [y]_{12})$, $x, y\epsilon\mathbb{Z}_{12}$. Then $f([x]_{12} + [y]_{12}) = f([x+y]_{12}) = [x+y]_4$, by the definitions of equivalence classes and f. Now consider $f([x]_{12}) + f([y]_{12}) = [x]_4 + [y]_4 = [x+y]_4 = f([x]_{12} + [y]_{12})$, by the same properties of equivalence classes. Since $f([x]_{12} + [y]_{12}) = f([x]_{12}) + f([y]_{12})$, f preserves addition.

To check if f preserves multiplication, consider $f([x]_{12} * [y]_{12})$. We can use rules of equivalence classes and apply the function f to get $f([x]_{12} * [y]_{12}) = f([xy]_{12}) = [xy]_4$. Now consider $f([x]_{12}) * f([y]_{12})$. By applying f, we get $f([x]_{12}) * f([y]_{12}) = [x]_4 * [y]_4 = [xy]_4 = f([x]_{12} * [y]_{12})$, and therefore f preserves multiplication.

Since f is well-defined and preserves multiplication and addition, it is homomorphism.

3 Section 3.3#30

Problem Let $f: R \to S$ be a homomorphism of rings and let $K = \{r\epsilon R | f(r) = 0_S\}$. Prove that K is a subring of R.

Solution Since f is a homomorphism of rings, $0_R\epsilon R$, $0_S\epsilon S$, and $f(0_R) = 0_S$. Therefore, $0_R\epsilon K$, and $K \neq \emptyset$.

Now take $a, b\epsilon K$. By the definition of K, $f(a) = 0_S$ and $f(b) = 0_S$. Subtracting one from the other, $f(a) - f(b) = 0_S - 0_S = 0_S$. Since f is a ring homomorphism, it preserves subtraction, and $f(a) - f(b) = f(a-b) = 0_S$. This implies that $a - b\epsilon K$, and therefore K is closed under subtraction.

To proved that K is closed under multiplication, consider the same a, b from above. Then $f(a) * f(b) = 0_S * 0_S = 0_S$. Again, since f is a ring homomorphism, it preserves multiplication and $f(a) * f(b) = f(a * b) = 0_S$. Therefore, $ab\epsilon K$ and K is closed under multiplication.

Since K is a nonempty subset closed under subtraction and multiplication, it is a subring of R.

4 Section 3.3 #38

Problem Let F be a field and $f: F \to R$ a homomorphism of rings.

(a) If there is a nonzero element c of F such that $f(c) = 0_R$, prove that f is the zero homomorphism (that is, $f(x) = 0_R$ for every $x\epsilon F$). [Hint: c^{-1} exists (Why?). If $x\epsilon F$, consider $F(xcc^{-1})$.]

(b) Prove that f is either injective or the zero homomorphism. [Hint: If f is not the zero homomorphism and $f(a) = f(b)$, then $f(a-b) = 0_R$.]

Solution

(a) Take $c\epsilon F, c \neq 0, f(c) = 0_R$ and take any $x\epsilon F$. Note that since F is a field, c^{-1} exists. Now consider the product$f(x) * f(c) * f(c^{-1}) = 0_R$. We know that the solution is 0_R, since $f(c) = 0_R$, and 0_R multiplied by anything is 0_R. Since f is a ring homomorphism,

$f(x) * f(c) * f(c^{-1}) = f(xcc^{-1}) = f(x * 1) = f(x) = 0_R$. This implies that for any element $x \epsilon F, f(x) = 0_R$, and therefore f is the zero homomorphism.

(b) If there is a nonzero element c of F such that $f(c) = 0_R$, then f is the zero homomorphism, from part (a) above. Assume that there there is no such element c of F. Now assume that for $a, b \epsilon F$, $f(a) = f(b)$. Then $f(a) - f(b) = f(a - b) = 0_R$, since f is a ring homomorphism. Since F is a field and f is a ring homomorphism, $f(a - b) = 0_R$ implies that $a - b = 0_F$, which can be simplified to $a - b = 0_F \Rightarrow a = b + 0_F \Rightarrow a = b$. Therefore, f is injective.

Now, if there is a nonzero element c of F such that $f(c) = 0_R$, then f is the zero homomorphism, and if there is not, f is injective.

5 Extra Problem

Problem Define an equivalence relation on the set of all rings by defining a ring R to be equivalent to a ring S if there is a ring isomorphism $f : R \to S$, i.e. R is isomorphic to S, $R \simeq S$. Show that this is an equivalence relation by showing

•$R \simeq R$ for all rings R

• If $R \simeq S$ for rings R and S, then $S \simeq R$

• If $R \simeq S$ and $S \simeq T$ for rings R, S, and T, then $R \simeq T$ (See problem #27)

Solution

• Let $f : R \to R$ be defined for $a \epsilon R$ as $f(a) = a$, the identity function.

The identity function is bijective, but this is easy to prove. To prove injectivity, assume that $f(x) = f(y)$ for some $x, y \epsilon R$. By the definition of f, $f(x) = f(y) \Rightarrow x = y$, and therefore f is injective. To prove surjectivity, take $f(z) \epsilon R$. $f(z)$ is mapped to by $z \epsilon R$, and thus f is surjective. Since f is surjective and injective, it is bijective.

Now to prove that f is a homomorphism, we must prove that it preserves addition and multiplication.

Consider $f(x + y)$ such that $x, y \epsilon R$. Then $f(x + y) = x + y$. Now consider $f(x)$ and $f(y)$. Well $f(x) = x$ and $f(y) = y$, so $f(x+y) = x+y = f(x)+f(y)$. Therefore f preserves addition.

Next, consider $f(xy) = xy$, $f(x) = x$, and $f(y) = y$. Then $f(xy) = xy = f(x)f(y)$, and therefore f preserves multiplication.

Thus, $f : R \to R$ is an isomorphism for all rings R.

• Assume there is some function $f : R \to S$ such that f is an isomorphism. Consider $g : S \to R$ such that g is the inverse of f, f^{-1}. We know that the inverse of a bijective function is bijective, so this means that g is bijective.

Now, we need to prove that g is a homomorphism. By the definition of inverse functions, g is f^{-1}, $g(f(x)) = x$, for some $x \epsilon R$.

Consider $g(c + d)$ for some $c, d \epsilon S$. We know that c and d are mapped to by f, since f is onto, so let $f(a) = c$ and $f(b) = d$ for some $a, b \epsilon R$. Then $g(c+d) = g(f(a)+f(b)) = g(f(a+b))$, since f is isomorphic. Applying g, $g(f(a + b)) = a + b = g(f(a)) + g(f(b)) = g(c) + g(d)$, by applying g and substituting. Therefore g preserves addition.

Next, consider $g(c * d)$ for some $c, d \epsilon S$. Similarly, we know that c and d are mapped to by f, since f is onto, so let $f(a) = c$ and $f(b) = d$ for some $a, b \epsilon R$. Then $g(c * d) = g(f(a) * f(b))$. Again, since f is isomorphic, it preserves multiplication and $g(f(a) * f(b)) = g(f(ab)) = ab = g(f(a)) * g(f(b)) = g(c) * g(d)$, by applying g and substituting. Thus, g preserves multiplication.

Since g is a bijection that preserves addition and multiplication, $g : S \to R$ is an isomorphism.

• Assume that $f : R \to S$ and $g : S \to T$ are isomorphisms. Then f and g are bijective, and we must show that $g \circ f$ is bijective.

Take some $a \epsilon T$. Since g is bijective, a is mapped to by an element of S, so let $g(b) = a, b \epsilon S$. But since f is bijective, there is an element $c \epsilon R$ such that $f(c) = b$. Then we can rewrite a as $g(f(c))$. Thus, for any element in T, there is some element in R that maps to it, and the $g \circ f$ is surjective.

Now, consider $g(f(x)) = g(f(y))$ for some $x, y \epsilon R$. Well, since g is bijective, $g(f(x)) = g(f(y))$ implies that $f(x) = f(y)$, and since f is injective, $f(x) = f(y)$ implies that $x = y$. Therefore, the composition $g \circ f$ is injective.

Since $g \circ f$ is injective and surjective, it is bijective.

Now, we must prove that $g \circ f$ is an homomorphism. Consider $g(f(x+y))$, for some $x, y \epsilon R$ and $f(x+y) \epsilon S$. Since f and g are isomorphisms, $g(f(x+y)) = g(f(x)+f(y)) = g(f(x))+g(f(y))$, so $g \circ f$ respects addition.

Now, consider $g(f(x * y))$. Again, since f and g are isomorphisms, they respect multiplication, $g(f(x * y)) = g(f(x) * f(y)) = g(f(x)) * g(f(y))$, and $g \circ f$ respects multiplication.

Therefore, since $g \circ f$ preserves multiplication and addition, and is a bijection from $R \to T$, R and T are isomorphic.