Algebra: Chapter 0 Exercises

Chapter 3, Section 2

David Melendez

July 24, 2018

Problem 2.1. Prove that if there is a homomorphism from a zero ring to a ring R, then R is a zero ring.

Solution. Let Z denote the zero ring, and let $\varphi : Z \to R$ be a ring homomorphism. Since φ is a homomorphism, it must take the identity in Z to the identity in R, so $\varphi(0) = 1_R$. But 0 is also the *additive* identity in Z, meaning $\varphi(0) = 0$, and so $0 = 1$ in R.

If $r \in R$, we then have $1 \cdot r = 0 \cdot r = 0$, showing that R is the zero ring. ∎

Problem 2.2. Let R and S be rings, and let $\varphi : R \to S$ be a function preserving both operations $+, \cdot$.

1. Prove that if φ is surjective, then necessarily $\varphi(1_R) = 1_S$.

2. Prove that if $\varphi \neq 0$ and S is an integral domain, then $\varphi(1_R) = 1_S$.

Solution.

1. First suppose φ is surjective. Then, if $s \in S$, then there exists an $r \in R$ such that $\varphi(r) = s$. Note that

$$\begin{aligned}\varphi(1_R) \cdot s &= \varphi(1_R) \cdot \varphi(r) \\ &= \varphi(1_R \cdot r) \\ &= \varphi(r) \\ &= s.\end{aligned}$$

Since this is true for all $s \in S$ (as φ is surjective), this implies that $\varphi(1_R) = 1_S$, as desired.

2. Now, let $\varphi \neq 0$ and suppose $\varphi(1_R) \neq 1_S$. This implies that $\varphi(1_R) - 1_S \neq 0$. Since φ is nonzero, there exists an $r \in R$ with $\varphi(r) \neq 0$. Note, then, that we have:

$$\begin{aligned}\varphi(r) \cdot (\varphi(1_R) - 1_S) &= \varphi(r) \cdot \varphi(1_R) - \varphi(r) \cdot 1_S \\ &= \varphi(r \cdot 1_R) - \varphi(r) \\ &= \varphi(r) - \varphi(r) \\ &= 0,\end{aligned}$$

implying S is not an integral domain since both of the terms in the original product are nonzero. Therefore, if S is an integral domain and $\varphi \neq 0$, then $\varphi(1_R) = 1_S$.

$\blacksquare$

Problem 2.6. Verify the 'extension property' of polynomial rings, stated in Example 2.3.

Solution. I will instead do the more general case, stating and proving a universal property for *monoid* rings.

Proposition. Let R be a ring, and M a monoid. The monoid ring $R[M]$, as defined in the text, then satisfies the following universal property:

Let $\iota_M : (M, \cdot) \hookrightarrow (R[M], \cdot)$ be the monoid homomorphism $m \mapsto 1_R m$, and let $\iota_R : R \hookrightarrow R[M]$ be the ring homomorphism $r \mapsto r1_M$. If S is a ring, $\varphi : R \to S$ is a ring homomorphism, and $j : M \to S$ is a monoid homomorphism with respect to multiplication on S such that $a \in \operatorname{im} j$ and $b \in \operatorname{im} \varphi$ implies $ab = ba$, then there exists a unique ring homomorphism $\overline{\varphi} : R[M] \to S$ such that the following diagram commutes:

$$\begin{tikzcd}
R \arrow[d, "\iota_R"'] \arrow[dr, "\varphi"] & \\
R[M] \arrow[r, dashed, "\overline{\varphi}"] & S \\
M \arrow[u, "\iota_M"] \arrow[ur, "j"'] &
\end{tikzcd}$$

Proof. First, we show that $\overline{\varphi}$ is determined by the fact that it must be a ring homomorphism that makes the diagram above commute.

$$\begin{aligned}
\overline{\varphi}\left(\sum_{m\in M} r_m m\right) &= \sum_{m\in M} \overline{\varphi}(r_m m) \\
&= \sum_{m\in M} \overline{\varphi}(\iota_R(r_m) \cdot \iota_M(m)) \\
&= \sum_{m\in M} \overline{\varphi}(\iota_R(r_m)) \cdot \overline{\varphi}(\iota_M(m)) \\
&= \sum_{m\in M} \varphi(r_m) \cdot j(m)
\end{aligned}$$

Since this function $\overline{\varphi}$ is the only function making the diagram commute, we just have to prove that it is a ring homomorphism. The fact that $\overline{\varphi}$ preserves addition and the identity is clear enough, so we will just show that it preserves multiplication. If we let $p = \sum_{m\in M} a_m m$

and $q = \sum_{m \in M} b_m m$, we then have:

$$\begin{aligned}
\overline{\varphi}(p) \cdot \overline{\varphi}(q) &= \left(\sum_{m \in M} \varphi(a_m) \cdot j(m) \right) \left(\sum_{m \in M} \varphi(b_m) \cdot j(m) \right) \\
&= \sum_{m \in M} \sum_{n \in M} \varphi(a_m) \cdot j(m) \cdot \varphi(b_n) \cdot j(n) \\
&= \sum_{m \in M} \sum_{n \in M} \varphi(a_m) \cdot \varphi(b_n) \cdot j(m) \cdot j(n) \\
&= \sum_{m \in M} \sum_{n \in M} \varphi(a_m b_n) \cdot j(mn) \\
&= \sum_{\ell \in M} \sum_{mn = \ell} \varphi(a_m b_n) \cdot j(\ell) \\
&= \overline{\varphi}(pq).
\end{aligned}$$

Hence $\overline{\varphi}$ is a homomorphism, and thus it satisfies the universal property, as desired. □

This universal property is a generalization of the universal property for polynomial rings over one indeterminant mentioned in the text, which is really just the monoid ring $R[\mathbb{N}]$. Additionally, much to our pleasure, polynomial rings in n indeterminants (which commute with each other) can be thought of as monoid rings $R\left[\mathbb{N}^n\right]$. ■

Problem 2.8. Prove that every subring of a field is an integral domain.

Solution. Let k be a field and R a subring of k. If $a \in R$ and $b \in R$, then $ab = 0$ implies $a = 0$ or $b = 0$ since a, b are also in k. Hence R is an integral domain. Note that R might not be a field, since the multiplicative inverse of an element of R might not be in R. ■

Problem 2.9. The center of a ring R, denoted $Z(R)$, consists of the elements a such that $ar = ra$ for all $r \in R$.

Prove that $Z(R)$ is a subring of R.

Proof. Suppose $a, b \in Z(R)$, and $r \in R$. We then have:

$$\begin{aligned}
(a+b)r &= ar + br \\
&= ra + rb \\
&= r(a+b),
\end{aligned}$$

and

$$\begin{aligned}
(ab)r &= a(br) \\
&= a(rb) \\
&= (ar)b \\
&= (ra)b \\
&= r(ab).
\end{aligned}$$

Of course 1 commutes with every element of R, so $Z(R)$ is a subring of R. □

Prove that the center of a division ring is a field.

Proof. Suppose R is a division ring. Clearly $Z(R)$ is commutative, so we just need to show that $a \in R$ implies $a^{-1} \in R$. This is easy: If $r \in R$, then:

$$\begin{aligned} ar = ra &\implies a^{-1}ar = a^{-1}ra \\ &\implies r = a^{-1}ra \\ &\implies ra^{-1} = a^{-1}r \end{aligned}$$

Hence every element $a \in Z(R)$ has a multiplicative inverse in $Z(R)$, making $Z(R)$ a field. $\square$

Problem 2.10. The *centralizer* of an element a of a ring R consists of the elements $r \in R$ such that $ar = ra$.

Prove that the centralizer of a, denoted $C_R(a)$ is a subring of R, for every $a \in R$.

Proof. This follows from an argument identital to the one above for the center of a ring. $\square$

Prove that the center of R is the intersection of all its centralizers.

Proof. Suppose $a \in C_R(r)$ for all $r \in R$. Then, by definition, a commutes with every element of r, and so $a \in Z(R)$. Suppose conversely that $a \in Z(R)$. Then $r \in R$ implies a commutes with r, again by definition, so $a \in C_R(r)$. $\square$

Prove that every centralizer in a division ring is a division ring.

Proof. By the argument at the top of this page, an element a being in a centralizer implies its inverse a^{-1} is also in that centralizer. $\square$

Problem 2.15. For $m > 1$, the abelian groups $(\mathbb{Z}, +)$ and $(m\mathbb{Z}, +)$ are manifestly isomorphic: the fucntion $\varphi : \mathbb{Z} \to m\mathbb{Z},\ n \mapsto mn$ is a group homomorphism.