Algebra: Chapter 0 Exercises
Chapter 3, Section 1

David Melendez

July 8, 2018

Problem 1. Prove that is $0 = 1$ in a ring R, then R is a zero-ring.

Proof. If $x \in R$, then $x = 1x = 0x = 0$. $\square$

Problem 2. Let S be a set, and define operations on the power set $\mathscr{P}(S)$ of S by setting $\forall A, B \in \mathscr{P}(S)$:

$$A + B := (A \cup B) \setminus (A \cap B)$$
$$A \cdot B := A \cap B$$

Prove that $(\mathscr{P}(S), +, \cdot)$ is a commutative ring.

Solution. We will establish a bijection between $\mathscr{P}(S)$ and another ring that preserves the given operations. Let $(\mathbb{Z}/2\mathbb{Z})^S$ be a ring as defined in problem 1.3, and define a function $\varphi : \mathscr{P}(S) \to (\mathbb{Z}/2Z)^S$ by

$$\varphi(A)(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

Case work shows that φ preserves $+$ and $\cdot$, and further investigation reveals a natural inverse for φ, showing that it is a bijection, and hence that $\mathscr{P}(S)$ is a ring (isomorphic to $(\mathbb{Z}/2\mathbb{Z})^S$, in fact). $\blacksquare$

Problem 1.3. Let R be a ring, and let S be any set. Explain how to endow the set R^S of set functions $S \to R$ of two operations $+, \cdot$ so as to make R^S into a ring, such that R^S is just a copy of R if S is a singleton.

Solution. Define $+$ on R^S by $(f_1 + f_2)(s) = f_1(s) + f_2(s)$ (making R^S into an abelian group, as R is an abelian group under $+$), and define $\cdot$ by $(f_1 \cdot f_2)(s) = f_1(s) \cdot f_2(s)$. Each of the ring axioms are clearly satisfies by this. If S is a singleton, then each $f : S \to R$ is uniquely identified by an element of R, and the operations coincide in the obvious way. $\blacksquare$

Problem 1.5. Let R be a ring. If a, b are zero-divisors in R, is $a + b$ necessarily a zero-divisor?

Solution. No. For example, $[2]_6$ and $[3]_6$ are zero-divisors in $\mathbb{Z}/6\mathbb{Z}$, but their sum $[5]_6$ is a unit in this ring, and hence is not a zero-divisor. ■

Problem 1.6. An element a of a ring R is *nilpotent* if $a^n = 0$ for some n.

1. Prove that if a and b are nilpotent in R and $ab = ba$, then $a + b$ is nilpotent.
2. Is the hypothesis $ab = ba$ in the previous statement necessary for its conclusion to hold?

Solution.

1. Suppose a and b are (nonzero, as this makes the conclusion obvious) nilpotent elements of R, so that $a^m = b^n = 0$ for positive integers m, n. Note, then, that, by the binomial theorem (as R is commutative):

$$(a+b)^{2mn} = \sum_{k=1}^{2mn} \binom{2mn}{k} a^{2mn-k} b^k$$

Notice that in each term of this sum, either $k \geq mn$ or $k \leq mn$, in which case $2mn - k \geq mn$. Since $mn \geq m$ and $mn \geq n$, this implies that in each term, either b^k or a^{2mn-k} is zero, meaning each term is zero, whence $a + b$ is nilpotent.

2. The hypothesis that a and b is indeed necessary. In the ring $\mathfrak{gl}_2(\mathbb{R})$, take the following matrices:

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \ ; \ B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

We have $A^2 = B^2 = 0$, but $A + B$ is of course not nilpotent.

■

Problem 1.7. Prove that $[m]$ is nilpotent in $\mathbb{Z}/nZ$ is and only if m is divisible by all prime factors of n.

Proof. First suppose $[m]$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$, so that $[m]^k \equiv a \bmod n$ for some positive integer k. This means that $n|m^k$, implying each prime factor of n is also a prime factor of m^k, and so is a prime factor of m since m^k and m have the same prime factors.

Conversely, suppose m is divisible by all prime factors of n. Let k be the largest exponent in the prime factorization of n. Then $n|m^k$, and so $[m]^k = [0]$. □

Problem 1.8. Prove that $x = \pm 1$ are the only solutions to $x^2 = 1$ in an integral domain. Find a ring in which the equation $x^2 = 1$ has more than two solutions.

Solution. Note that:

$$\begin{aligned} x^2 = 1 &\Leftrightarrow x^2 - 1 = 0 \\ &\Leftrightarrow (x+1)(x-1) = 0 \\ &\Leftrightarrow x + 1 = 0 \text{ or } x - 1 = 0 \\ &\Leftrightarrow x = \pm 1 \end{aligned}$$

where implications 1, 2, and 4 follow from the properties of rings, and the third implication follows from our ring being an integral domain.

In the ring $\mathbb{Z}/3Z$, the equation $x^2 = 1$ has solutions $\pm 1, \pm 2$. ■

Problem 10. Let R be a ring. Prove that if $a \in R$ is a right-unit and has two or more left-zero-divisors, then a is *not* a left-zero-divisor and *is* a right-zero-divisor.

Solution. Let u_1, u_2 be distinct left inverses of a, so that $u_1 a = u_2 a = 1$. We then have, for all $b \in R$,

$$\begin{aligned} ab = 0 &\implies u_1 ab = u_1 0 \\ &\implies b = 0, \end{aligned}$$

and so a is not a left-zero-divisor. Note, however, that

$$\begin{aligned} (u_1 - u_2)a &= u_1 a - u_2 a \\ &= 1 - 1 \\ &= 0, \end{aligned}$$

and so a is a right-zero-divisor since $u_1 \neq u_2$. ■

Problem 1.14. Let R be a ring, and let $f(x), g(x) \in R[x]$ be nonzero polynomials. Prove that

$$\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x))).$$

Assuming that R is an integral domain, prove that

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$$

Solution. Let $f(x) = \sum_i a_i x^i$ and $g(x) = \sum_i b_i x^i$. If $\deg(f(x)) = \deg(g(x)) = n$, then $i > n$ implies $a_i + b_i = 0$, and so the largest i for which the coefficient $a_i + b_i$ is potentially nonzero coefficient is $i = n$. Hence $\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x)))$.

If $\deg(f(x)) \neq \deg(g(x))$, then assume without loss of generality that $n = \deg(g(x)) > \deg(f(x))$. Of course $i > n$ then implies $a_i + b_i = 0$ and $a_n + b_n = a_n$, so the result holds.

Now, assume R is an integral domain, and let $\deg(f(x)) = m$, $\deg(g(x)) = n$. Since no $i \leq m, j \leq n$ implies $i + j \leq m + n$, we know then that the coefficient of x^k in the product of f and g for $k > m + n$ is zero. Furthermore, this also implies that the coefficient of x^{m+n} is $a_m b_n$ by the definition of the product of polynomials, which is nonzero since a_m, b_n are nonzero and R is an integral domain. ■

Problem 1.15. Prove that $R[x]$ is an integral domain if and only if R is an integral domain.

Solution. First suppose that $R[x]$ is an integral domain. Then every two constant polynomials $p = r_1, q = r_2$ in $R[x]$ satisfy $pq = 0$ if and only if $p = 0$ or $q = 0$ as polynomials. But this is true if and only if $r_1 = 0$ or $r_2 = 0$ as elements of R, hence R is an integral domain.

Conversely, suppose $R[x]$ is not an integral domain, that is, there exist nonzero polynomials

$$p = \sum_i p_i x_i$$
$$q = \sum_i q_i x_i;$$

(where p_i and q_i are elements of R) such that the polynomial $pq = 0$. Let m be the smallest positive integer such that p_m is nonzero, and let n be the smallest positive integer such that q_n is nonzero. Then $0 = (pq)_{m+n} = p_m q_n$ by the definition of the product of polynomials and the fact that $pq = 0$, so R is not an integral domain. ∎

¡++¿