Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 12, 2020

Problems in Section 3.1-3.2.

1. If $a, b, c, d \in R$, evaluate $(a+b)(c+d)$.

Solution. Observe that

$$(a+b)(c+d) = a(c+d) + b(c+d) = ac + ad + bc + bd.$$

□

2. Prove that if $a, b \in R$, then $(a+b)^2 = a^2 + ab + ba + b^2$, where by x^2 we mean xx.

Proof. Observe that

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

□

3. Find the form of the binomial theorem in a general ring; in other words, find an expression for $(a+b)^n$, where n is a positive integer.

Solution. We define the notion of word by arbitrary products of a and b(with its order kept in consideration). Let $C_k(a, b)$ an equivalence class of words, with k a's and $n-k$ b's in the word of length n. It is clear that for each $C_k(a, b)$, its size is $\begin{pmatrix} n \\ k \end{pmatrix}$. Consequently,

$$(a+b)^n = \sum_{k=0}^{n} \left(\sum_{x \in C_k(a,b)} x \right)$$

is one of the form of binomial expansion in a general ring. □

4. If every $x \in R$ satisfies $x^2 = x$, prove that R must be commutative.(A ring in which $x^2 = x$ for all elements is called a Boolean ring.

Proof. Note that in a Boolean ring R, $x = -x$ for all $x \in R$ since $1 = (-1)^2 = -1$. Now we see that for $a, b \in R$,

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

so that R must be commutative. $\square$

5. If R is a ring, merely considering it as an abelian group under its addition, we have defined in Chapter 2, what is mean by na, where $a \in R$ and n is an integer. Prove that if $a, b \in R$ and n, m are integers, then $(na)(mb) = (nm)(ab)$.

Proof. Observe that

$$\begin{aligned}
(na)(mb) &= \underbrace{(a + a + \cdots + a)}_{n \text{ summands}}(mb) \\
&= \underbrace{a(mb) + a(mb) + \cdots + a(mb)}_{n \text{ summands}} \\
&= \underbrace{a(b + b + \cdots + b) + a(b + b + \cdots + b) + \cdots + a(b + b + \cdots + b)}_{n \text{ summands}} \\
&= \underbrace{(ab + ab + \cdots + ab) + (ab + ab + \cdots + ab) + \cdots + (ab + ab + \cdots + ab)}_{n \text{ summands}} \\
&= \underbrace{ab + ab + \cdots + ab}_{nm \text{ summands}} \\
&= (nm)(ab).
\end{aligned}$$

$\square$

6. If D is an integral domain and D is of finite characteristic, prove that the characteristic of D is a prime number.

Proof. Suppose we assume that the characteristic d is not a prime, that is, $d = mn$ for some integers $n, m > 1$. Note that $da^2 = 0 \iff (mn)a^2 = (ma)(na) = 0$. Since D is an integral domain, either $ma = 0$ or $na = 0$. But in either cases, we have a smaller characteristic than d, which is a contradiction. Hence, it is must that d is a prime. $\square$

7. Give an example of an integral domain which has a infinite number of elements, yet is of finite characteristic.

Solution. Consider the infinite product ring $\prod \mathbb{Z}_2$. This is an integral domain with infinite number of elements but has characteristic 2. $\square$

8. If D is an integral domain and if $na = 0$ for some $a \neq 0$ in D and some integer $n \neq 0$, prove that D is of finite characteristic.

Proof. Let n be the smallest positive integer satisfying $na = 0$. Suppose D is not of finite characteristic. Then, we have $b \neq 0$ in D such that $kb = 0$ if and only if $k = 0$. Let $k < n$ and $k > 0$. Then

$$0 = (na)(kb) = (nk)(ab) = (kn)(ab) = (ka)(nb).$$

Since $nb \neq 0$ and D is an integral domain, $ka = 0$, which is a contradiction. Hence, D must be of finite characteristic. $\square$

9. If R is a system satisfying all the conditions for a ring with unit element with the possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring.

Proof. We compute $(a + b)(1 + 1)$ in two ways;

$$(a + b)(1 + 1) = a(1 + 1) + b(1 + 1) = a + a + b + b,$$
$$(a + b)(1 + 1) = (a + b)1 + (a + b)1 = a + b + a + b,$$

which implies $a + a + b + b = a + b + a + b \iff a + b = b + a$. $\square$

10. Show that the commutative ring D is an integral domain if and only if for $a, b, c \in D$, with $a \neq 0$ the relation $ab = ac$ implies that $b = c$.

Proof. Suppose D is an integral domain. Then for $a \neq 0$, $ab = ac \iff a(b - c) = 0$ so that $(b - c) = 0 \iff b = c$. Conversely, if we assume that D is not an integral domain, there exists $a, b \neq 0 \in D$ such that $ab = 0$. But $0 = ab = a \cdot 0 \implies a(b - 0) \implies b - 0 = 0$, $b = 0$ which is a contradiction. Hence, D must be an integral domain. $\square$

11. Prove that Lemma 3.2.2 is false if we drop the assumption that the integral domain is finite.

Proof. $\mathbb{Z}$ is clearly an infinite integral domain, but not a field. $\square$

12. Prove that any field is an integral domain.

Proof. Suppose $a \neq 0$ and $ab = 0$ for some b. Since the inverse of a exists, $a^{-1}ab = 0 \iff b = 0$. So, there is no zero divisor in the field. Hence, every field is also an integral domain. $\square$

13. Using the pigeonhole principle, prove that if m and n are relatively prime integers and a and b are any integers, there exists an integer x such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

Proof. Consider the remainders of $a, a+m, a+2m, \cdots, a+(n-1)m$ on division by n. Since n and m are relatively prime, each of remainders of above yield distinct integers. Now by pigeonhole principle, for some $0 \leq b \leq n$, there corresponds one of remainders(under division of n) of $a + km$. That is, $a + km \equiv b \pmod{n}$. Moreover, $a + km \equiv a \pmod{m}$. By setting $x = a + km$, x is the desired integer satisfying the given relationship. $\square$

14. Using the pigeonhole principle, prove that the decimal expansion of a rational number must, after some point, become repeating.

Proof. Let p/q be a rational number where p, q are relatively prime. On reminding, for a decimal expansion of a rational number $p/q = a_0.a_1a_2a_3\cdots$, each $a_i, i > 1$, corresponds to the quotient of $a_{i-1} \cdot 10$ on divison by q. Note that there can be at most q distinct values of $a_{i-1} \cdot 10$. Thus, keep making such modular calculation consequently, at the time when calculation is made more than q times, the pigeonhole principle forces that there must exists a tuple (i, j) of positive integers $i < j$ such that $a_{i+j} = a_i$. Hence a_i is occuring at least twice in these calculations. Now from these, we can conclude that $(a_i, a_{i+1}, \cdots, a_{i+j-1}) = (a_{i+j}, a_{i+j+1}, \cdots, a_{i+2j-1})$ and so on, so that the decimal expansion of p/q, after a_{i-1}, becomes repeating. $\square$