MATH 417, HOMEWORK 9

CHARLES ANCEL

Chapter IV.19

Exercise 3. Find all solutions of the equation $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$.

Alright, to solve the equation $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$, we need to test all possible values of x in $\mathbb{Z}_6$ (which are $0, 1, 2, 3, 4,$ and 5) and see which ones satisfy the equation.

First, let's rewrite the equation:

$$x^2 + 2x + 2 \equiv 0 \mod 6$$

Now, let's plug in each possible value of x and see if it satisfies the equation:

(1) $x = 0$: $0^2 + 2(0) + 2 = 2 \equiv 0 \mod 6$
(2) $x = 1$: $1^2 + 2(1) + 2 = 5 \equiv 0 \mod 6$
(3) $x = 2$: $2^2 + 2(2) + 2 = 10 = 4 \equiv 0 \mod 6$
(4) $x = 3$: $3^2 + 2(3) + 2 = 17 = 5 \equiv 0 \mod 6$
(5) $x = 4$: $4^2 + 2(4) + 2 = 26 = 2 \equiv 0 \mod 6$
(6) $x = 5$: $5^2 + 2(5) + 2 = 37 = 1 \equiv 0 \mod 6$

Proof. To show this, we substitute each element of $\mathbb{Z}_6$ into the equation and find that none of them satisfy the equation:

(1) $x = 0$: $0^2 + 2(0) + 2 \not\equiv 0 \mod 6$
(2) $x = 1$: $1^2 + 2(1) + 2 \not\equiv 0 \mod 6$
(3) $x = 2$: $2^2 + 2(2) + 2 \not\equiv 0 \mod 6$
(4) $x = 3$: $3^2 + 2(3) + 2 \not\equiv 0 \mod 6$
(5) $x = 4$: $4^2 + 2(4) + 2 \not\equiv 0 \mod 6$
(6) $x = 5$: $5^2 + 2(5) + 2 \not\equiv 0 \mod 6$

Hence, there are no solutions of the equation $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$. □

Exercise 9. Find the characteristic of the given ring.

$$\mathbb{Z}_3 \times \mathbb{Z}_4$$

Given the ring $\mathbb{Z}_3 \times \mathbb{Z}_4$, the elements are ordered pairs of the form (a, b) where a is an element of $\mathbb{Z}_3$ and b is an element of $\mathbb{Z}_4$. The multiplicative identity in this ring is $(1, 1)$.

To find the characteristic, we need to find the smallest positive integer n such that:

$$n \cdot (1, 1) = (n \mod 3, n \mod 4) = (0, 0)$$

This will occur when n is a multiple of both 3 and 4, which is the least common multiple (LCM) of 3 and 4. The least common multiple (LCM) of 3 and 4 is 12.

Proof. To find the characteristic of the ring $\mathbb{Z}_3 \times \mathbb{Z}_4$, we need to find the smallest positive integer n such that:

$$n \cdot (1, 1) = (n \mod 3, n \mod 4) = (0, 0)$$

Given that n needs to be a multiple of both 3 and 4, the smallest such value is the LCM of 3 and 4, which is 12.

Thus, the characteristic of the ring $\mathbb{Z}_3 \times \mathbb{Z}_4$ is 12. □

Exercise 17f. True or false:

f. Every integral domain of characteristic 0 is infinite.

Proof. Recall that the characteristic of a ring is the smallest positive integer n such that $n \cdot 1 = 0$ in that ring. If no such n exists, then the ring has characteristic 0.

If an integral domain has characteristic 0, then no positive integer n exists such that $n \cdot 1 = 0$. This means that for every positive integer n, the element $n \cdot 1$ is distinct from zero and from any other integer $m \cdot 1$ where $m \neq n$. Therefore, there are infinitely many distinct elements in the ring, making the ring infinite.

Thus, the statement is **True**. □

Exercise 17g. True or false:

g. The direct product of two integral domains is again an integral domain.

Proof. Recall the definition of an integral domain: An integral domain is a commutative ring with unity (1) and no zero divisors.

Let's consider two integral domains, D_1 and D_2. Their direct product, $D_1 \times D_2$, consists of ordered pairs (a, b) where a is from D_1 and b is from D_2.

Now, let's take two non-zero elements from $D_1 \times D_2$: (a_1, b_1) and (a_2, b_2). The product of these elements is:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

For this product to be the zero element of $D_1 \times D_2$, i.e., $(0, 0)$, both $a_1 \cdot a_2$ and $b_1 \cdot b_2$ must be zero. However, since D_1 and D_2 are integral domains, this can only happen if $a_1 = 0$ or $a_2 = 0$ and $b_1 = 0$ or $b_2 = 0$. But this contradicts our assumption that both elements are non-zero.

Therefore, $D_1 \times D_2$ does have zero divisors and is not an integral domain.

Thus, the statement is **False**. □

Exercise 23. An element a of a ring R is **idempotent** if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

Proof. Recall that a division ring is a ring in which every non-zero element has a multiplicative inverse.

Firstly, the element 0 is trivially idempotent because $0^2 = 0$.

Now, let's consider a non-zero idempotent element a in the division ring. Since $a^2 = a$, we can factor out a to get:

$$a(a - 1) = 0$$

Now, since our ring is a division ring, no non-zero element is a zero divisor. This means that if $ab = 0$, then either $a = 0$ or $b = 0$.

From the above equation $a(a - 1) = 0$, it follows that either $a = 0$ or $a - 1 = 0$. We already know that a is non-zero, so the only possibility is $a - 1 = 0$, or $a = 1$.

Thus, the element 1 is also idempotent because $1^2 = 1$.

No other element in the division ring can be idempotent because if there was another idempotent element b, such that $b^2 = b$, by the same reasoning as above, b would either have to be 0 or 1, which are the idempotents we already found.

Therefore, a division ring contains exactly two idempotent elements: 0 and 1.

□

Exercise 29. Show that the characteristic of an integral domain D must be either 0 or a prime p. [Hint: If the characteristic of D is mn, consider $(m \cdot 1)(n \cdot 1)$ in D.]

Proof. Let's denote the characteristic of D as n.

If $n = 0$, then the statement holds, and we are done.

If $n \neq 0$, then it's either prime or composite. Let's consider the case where n is composite. This means n can be expressed as the product of two smaller positive integers m and n (neither being 1).

Consider the product:

$$(m \cdot 1)(n \cdot 1)$$

Since the characteristic of D is n, we have:

$$m \cdot 1 = m \bmod n$$

$$n \cdot 1 = n \bmod n$$

Thus, the product becomes:

$$(m \cdot 1)(n \cdot 1) = mn \bmod n = 0$$

But since $m, n < n$ and neither m nor n are 1, neither $m \cdot 1$ nor $n \cdot 1$ are zero in the ring.

So, we have two non-zero elements in D whose product is zero. This means that D has zero divisors, which is a contradiction because an integral domain cannot have zero divisors.

Thus, n cannot be composite. The only positive integers that are not composite and not equal to 1 are prime numbers.

Therefore, the characteristic of an integral domain D must be either 0 or a prime p.

□

Chapter IV.21

Exercise 2. Describe (in the sense of Exercise 1) the field F of quotients of the integral subdomain $D = \{n + m\sqrt(2) | n, m \in \mathbb{Z}\}$ of R.

Proof. Firstly, recall the context from Exercise 1 for the Gaussian integers. The field of quotients for the subdomain $D' = \{n + mi \mid n, m \in \mathbb{Z}\}$ in $\mathbb{C}$ consists of all ratios of the form:

$$\frac{n_1 + m_1 i}{n_2 + m_2 i}$$

where n_1, m_1, n_2, m_2 are integers and $n_2 + m_2 i \neq 0$.

Similarly, the field F of quotients for our given integral subdomain D will consist of all ratios of the form:

$$\frac{n_1 + m_1\sqrt{2}}{n_2 + m_2\sqrt{2}}$$

where n_1, m_1, n_2, m_2 are integers and $n_2 + m_2\sqrt{2} \neq 0$.

This ratio can be simplified by multiplying both the numerator and the denominator by the conjugate of the denominator:

$$\frac{n_1 + m_1\sqrt{2}}{n_2 + m_2\sqrt{2}} \cdot \frac{n_2 - m_2\sqrt{2}}{n_2 - m_2\sqrt{2}}$$

This simplification results in a ratio where the denominator no longer contains $\sqrt{2}$. The simplified form represents the elements of the field of quotients F for the integral domain D.

Thus, F is the set of all numbers of the form $\frac{a+b\sqrt{2}}{c}$ where a, b, and c are integers, and $c \neq 0$. □

Exercise 4. Mark each of the following true or false.

(a.) $\mathbb{Q}$ is a field of quotients of $\mathbb{Z}$.

(b.) $\mathbb{R}$ is a field of quotients of $\mathbb{Z}$.

(c.) $\mathbb{R}$ is a field of quotients of $\mathbb{R}$.

(d.) $\mathbb{C}$ is a field of quotients of $\mathbb{R}$.

(e.) If D is a field, then any field of quotients of D is isomorphic to D.

(f.) The fact that D has no divisors of 0 was used strongly several times in the construction of a field F of quotients of the integral domain D.

(g.) Every element of an integral domain D is a unit in a field F of quotients of D.

(h.) Every nonzero element of an integral domain D is a unit in a field F of quotients of D.

(i.) A field of quotients F of a subdomain $D\prime$ of an integral domain $D\prime$ can be regarded as a subfield of some field of quotients of D.

(j.) Every field of quotients of $\mathbb{Z}$ is isomorphic to $\mathbb{Q}$.

Proof. (a) $\mathbb{Q}$ is a field of quotients of $\mathbb{Z}$.
True. The rational numbers $\mathbb{Q}$ are indeed constructed as quotients of integers. Every element in $\mathbb{Q}$ can be expressed as a ratio of two integers.

(b) $\mathbb{R}$ is a field of quotients of $\mathbb{Z}$.
False. While $\mathbb{Q}$ (the field of quotients of $\mathbb{Z}$) is a subset of $\mathbb{R}$, not all real numbers can be expressed as a ratio of two integers.

(c) $\mathbb{R}$ is a field of quotients of $\mathbb{R}$.
True. Any field is a field of quotients of itself.

(d) $\mathbb{C}$ is a field of quotients of $\mathbb{R}$.
False. The complex numbers extend the real numbers by including imaginary numbers, which cannot be constructed merely as quotients of real numbers.

(e) If D is a field, then any field of quotients of D is isomorphic to D.
True. A field is already a field of quotients of itself, so any field of quotients constructed from it would be isomorphic to the original field.

(f) The fact that D has no divisors of 0 was used strongly several times in the construction of a field F of quotients of the integral domain D.
True. The absence of zero divisors is a crucial property of integral domains, and this property is essential when constructing a field of quotients.

(g) Every element of an integral domain D is a unit in a field F of quotients of D.
False. Not every element of D is a unit in F. Only the non-zero elements of D become units in F, since they will have multiplicative inverses in F.

(h) Every nonzero element of an integral domain D is a unit in a field F of quotients of D.
True. This is because in the field of quotients, every non-zero element of D can be expressed as a ratio, and thus will have a multiplicative inverse.

(i) A field of quotients F of a subdomain D' of an integral domain D' can be regarded as a subfield of some field of quotients of D.
True. If D' is a subdomain of D, then the field of quotients of D' will naturally be a subfield of the field of quotients of D.

(j) Every field of quotients of $\mathbb{Z}$ is isomorphic to $\mathbb{Q}$.
True. The field of quotients of $\mathbb{Z}$ is, by definition, the set of rational numbers $\mathbb{Q}$. Any other field of quotients constructed from $\mathbb{Z}$ would be isomorphic to $\mathbb{Q}$.

$\square$