HW 10 - MATH403

Danesh Sivakumar

April 24th, 2022

Problem 1 (Chapter 13, Exercise 52)

Give an example of an infinite integral domain that has characteristic 3.

Proof. $\mathbb{Z}_3[x]$ is an example; notice that $\mathbb{Z}_3$ is an integral domain, so that $\mathbb{Z}_3[x]$ is also an integral domain. It follows from Theorem 13.3 that this integral domain has characteristic 3. $\square$

Problem 2 (Chapter 13, Exercise 56)

Find all solutions of $x^2 - x + 2 = 0$ over $\mathbb{Z}_3[i]$

Proof. Note that the elements of $\mathbb{Z}_3[i]$ are $\{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$. Testing each of these with our polynomial yields:
$(0)^2 - (0) + 2 = 2 \neq 0$
$(1)^2 - (1) + 2 = 2 \neq 0$
$(2)^2 - (2) + 2 = 1 \neq 0$
$(i)^2 - (i) + 2 = 1 + 2i \neq 0$
$(1+i)^2 - (1+i) + 2 = 1 + i \neq 0$
$(2+i)^2 - (2+i) + 2 = 0$
$(2i)^2 - (2i) + 2 = 1 + i \neq 0$
$(1+2i)^2 - (1+2i) + 2 = 1 + 2i \neq 0$
$(2+2i)^2 - (2+2i) + 2 = 0$
Thus the solutions are $x = 2 + i$ and $x = 2 + 2i$ $\square$

Problem 3 (Chapter 13, Exercise 64)

Suppose that a and b belong to a field of order 8 and that $a^2 + ab + b^2 = 0$. Prove that $a = 0$ and $b = 0$. Do the same when the field has order 2^n with n odd.

Proof. Suppose that $a = b$; then $a^2 + ab + b^2 = 3a^2 = a^2 = 0$. This implies that $a = 0$ and $b = 0$. Now, toward a contradiction suppose that $a \neq b$ and without loss of generality $a \neq 0$. Observe that $0 = (a-b)(a^2 + ab + b^2) = a^3 - b^3$ by the difference of powers formula. Thus $a^3 = b^3$. Now observe that the order of the field $F \setminus \{0\}$ is $2^n - 1$; the fact that $a^3 = b^3$ implies that $a^{-3}b^3 = 1$, meaning that $(a^{-1}b)^3 = 1$. But 3 never divides $2^n - 1$ for n odd. To prove this, we will show that 3 always divides $2^n + 1$ for n odd; then because $2^n - 1$ and $2^n + 1$ have a difference of 2, both cannot be divisible by 3. We prove this by induction; observe that $2^1 + 1 = 3$ is divisible by 3. Now suppose $2^{2n+1} + 1 = 3k$; it follows that $4(3k) - 3 = 3(4k - 1) = 3j = 2^{2n+1} + 1$. Thus, we have that the order of $a^{-1}b$ is 1, and so $a^{-1}b = 1$, meaning $a = b$, which is a contradiction; thus $a = b$ and $a = 0$ and $b = 0$. □

Problem 4 (Chapter 14, Exercise 16)

If A and B are ideals of a commutative ring R with unity and $A + B = R$, show that $A \cap B = AB$

Proof. Take $x \in A \cap B$. Because $R = A + B$, it follows that $1 = a + b$ for $a \in A$ and $b \in B$. This means that $x = 1 \cdot x = (a + b) \cdot x = ax + bx = ax + xb \in AB$ because $a \in A$, $x \in A$, $x \in B$ and $b \in B$. Now take $x \in AB$. It follows that $x = \sum_{i=1}^{n} a_i b_i$ for $a_i \in A$ and $b_i \in B$ and some n. Because A is an ideal, $a_i b_i \in A$. Because B is an ideal, $a_i b_i \in B$. Because $a_i b_i \in A$ and $a_i b_i \in B$ for all i, it follows that $x \in A \cap B$. □

Problem 5 (Chapter 14, Exercise 32)

Show that $A = \{(3x, y) \mid x, y \in \mathbb{Z}\}$ is a maximal ideal of $\mathbb{Z} \oplus \mathbb{Z}$. Generalize. What happens if $3x$ is replaced by $4x$? Generalize.

Proof. Suppose B is an ideal such that $A \subset B$. We claim that $B = \mathbb{Z} \oplus \mathbb{Z}$. To this end, suppose there exists an element $(m, n) \in B$ such that $(m, n) \notin A$. It follows that m is not a multiple of 3, so that $\gcd(m, 3) = 1$ because 3 is prime. Then by Bezout's lemma, we can find integers a, b such that $3a + mb = 1$, meaning that $(1, 1) \in B$ so that $B = \mathbb{Z} \oplus \mathbb{Z}$. This reasoning extends to any prime p. However, this does not work with $4x$ because $A \subset \{(2x, y) \mid x, y \in \mathbb{Z}\} \subset \mathbb{Z} \oplus \mathbb{Z}$. In general, this does not work with composite numbers. □

Problem 6 (Chapter 14, Exercise 34)

Let $R = \mathbb{Z}_8 \oplus \mathbb{Z}_{30}$. Find all maximal ideals of R, and for each maximal ideal I, identify the size of the field R/I.

Proof. We proceed by taking the direct product of the ideal of one component and the other component.
$I_1 = 2\mathbb{Z}_8 \oplus \mathbb{Z}_{30}$
$I_2 = 2\mathbb{Z}_8 \oplus 2\mathbb{Z}_{30}$
$I_3 = \mathbb{Z}_8 \oplus 3\mathbb{Z}_{30}$
$I_4 = \mathbb{Z}_8 \oplus 5\mathbb{Z}_{30}$
By calculating the orders of the fields, we deduce that $|I_1| = 2$, $|I_2| = 2$, $|I_3| = 3$ and $|I_4| = 5$ □

Problem 7 (Chapter 14, Exercise 54)

List the elements of the field $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$, and make an addition and multiplication table for the field.

Proof. Note that the only possibilities are $0, 1, x, x+1, x^2, x^2+1, x^2+x$ because $\langle x^2+x+1\rangle$ has degree 2. But the fact that $x^2+x+1=0$ implies that some of these elements go away; namely $x^2+x = x^2+x-(x^2+x+1) = -1 = 1$, $x^2+1 = x^2+1-(x^2+x+1) = -x = x$, and $x^2 = x^2-(x^2+x+1) = -(x+1) = x+1$. This means that the only elements of the field are $0, 1, x, x+1$. The tables are listed below:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

□

Problem 8 (Chapter 14, Exercise 58)

Show that $\mathbb{Z}[i]/\langle 1-i\rangle$ is a field. How many elements does this field have?

Proof. Note that because $1-i=0$, it follows that $1=i$, so that $1=-1$ and thus $2=0$. We then have that for any $x+yi \in \mathbb{Z}[i]$, that $x+yi+\langle 1-i\rangle = ki+\langle 1-i\rangle$ for $k=1$ or $k=0$. This means that $\mathbb{Z}[i]/\langle 1-i\rangle$ is a field with two distinct elements, namely $\langle 1-i\rangle$ and $i+\langle 1-i\rangle$ □

Problem 9 (Chapter 14, Exercise 66)

Let $R = \mathbb{Z}[\sqrt{-5}]$ and let $I = \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}, a-b \text{ is even}\}$. Show that I is a maximal ideal of R.

Proof. Suppose J is an ideal such that $I \subset J \subset R$. We have that J contains an element $a+b\sqrt{-5}$ such that the parity of a and b is different. Case 1: a odd and b even; $(2m+1)+2n\sqrt{-1}$. Case 2: a even and b odd; $2m+(2n+1)\sqrt{-1}$. Note that adding 1 to both elements yields an element in I. Thus, it follows that $1 = [(2m+1)+2n\sqrt{-5}]-[2m+2n\sqrt{-5}] = [(2m+1)+(2n+1)\sqrt{-5}]-[2m+(2n+1)\sqrt{-5}] \in J$, meaning that $J=R$; this means that I is a maximal ideal of R. □

Problem 10 (Chapter 14, Exercise 70)

Let $R = \{(a_1, a_2, a_3, \cdots\}$, where each $a_i \in \mathbb{Z}$. Let $I = \{(a_1, a_2, a_3, \cdots\}$, where only a finite number of terms are nonzero. Prove that I is not a principal ideal of R.

Proof. Suppose for the sake of contradiction that there is exists a sequence $a = \{(a_1, a_2, a_3, \cdots\}$ such that $I = \langle a \rangle$. Because there are only a finite number of nonzero terms, there exists an index m such that $a_n = 0$ for all $n \geq m$. Now consider the sequence $b = \{(a_1, a_2, a_3, \cdots a_m, 1, 0, 0, \cdots\}$. It follows that this sequence is an element of I, but there cannot exist an $r \in R$ such that $b = ar$ because this implies $1 = a_{m+1}r_{m+1}$, which cannot happen because $a_{m+1} = 0$. Thus I cannot be a principal ideal of R. $\square$

Problem 11 (Chapter 15, Exercise 56)

Let $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Show that these two rings are not ring-isomorphic.

Proof. Suppose such an isomorphism $\phi\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$ exists. Then $\phi(\sqrt{2}) = a + b\sqrt{5} \implies \phi(2) = a^2 + 2ab\sqrt{5} + 5b^2$. However, $phi(2) = 2\phi(1) = 2$. This is a contradiction, because 2 is rational but $a^2 + 2ab\sqrt{5} + 5b^2$ cannot be rational because of the additional $\sqrt{5}$ term. Thus, no such isomorphism exists. $\square$

Problem 12 (Chapter 15, Exercise 66)

Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| \ a, b \in \mathbb{Z} \right\}$, and let ϕ be the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to $a - b$.

(a) Show that ϕ is a homomorphism.

(b) Determine the kernel of ϕ.

(c) Show that $R/\text{Ker}\phi$ is isomorphic to $\mathbb{Z}$

(d) Is $\text{Ker}\phi$ a prime ideal?

(e) Is $\text{Ker}\phi$ a maximal ideal?

Proof. (a)

$$\phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix}\right) = a+c-b-d = a-b+c-d$$

$$= \phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) + \phi\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$$

$$\phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right) = \phi\left(\begin{bmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{bmatrix}\right) = (ac+bd)-(ad+bc) = (a-b)(c-d) =$$

$$= \phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right)\phi\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$$

so that ϕ is operation preserving in multiplication and addition.

(b) Observe that the kernel is the set of matrices such that $a - b = 0$, which occurs only when $a = b$; thus $\text{Ker}\phi = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| \ a \in \mathbb{Z} \right\}$

(c) Because ϕ is an onto homomorphism (it can take any value in $\mathbb{Z}$), it follows by the First Isomorphism Theorem that $R/\text{Ker}\phi \cong \mathbb{Z}$.

(d) Yes, because $\mathbb{Z}$ is an integral domain.

(e) No, because $\mathbb{Z}$ is not a field.

□