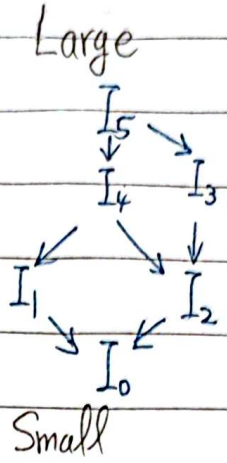
2024/12/0 MATH3301 Assignment 5

1. Solution:

Step1: List all principal ideals of $\mathbb{Z}_3\times\mathbb{Z}_4$.



$\langle(0,0)\rangle = \{(0,0)\} = I_0$

$\langle(1,0)\rangle = \{(0,0),(1,0),(2,0)\} = I_1$

$\langle(2,0)\rangle = \{(0,0),(1,0),(2,0)\} = I_1$

$\langle(0,1)\rangle = \{(0,0),(0,1),(0,2),(0,3)\} = I_3$

$\langle(1,1)\rangle = \mathbb{Z}_3\times\mathbb{Z}_4 = I_5$

$\langle(2,1)\rangle = \mathbb{Z}_3\times\mathbb{Z}_4 = I_5$

$\langle(0,2)\rangle = \{(0,0),(0,2)\} = I_2$

$\langle(1,2)\rangle = \{(0,0),(1,0),(2,0),(0,2),(1,2),(2,2)\} = I_4$

$\langle(2,2)\rangle = \{(0,0),(1,0),(2,0),(0,2),(1,2),(2,2)\} = I_4$

$\langle(0,3)\rangle = \{(0,0),(0,1),(0,2),(0,3)\} = I_3$

$\langle(1,3)\rangle = \mathbb{Z}_3\times\mathbb{Z}_4 = I_5$

$\langle(2,3)\rangle = \mathbb{Z}_3\times\mathbb{Z}_4 = I_5$

There are exactly 6 distinct principal ideals $I_0, I_1, I_2, I_3, I_4, I_5$

Step2: As $|\mathbb{Z}_3\times\mathbb{Z}_4| = 12 < +\infty$, every nonzero ideal I of $\mathbb{Z}_3\times\mathbb{Z}_4$ can be obtained by appending principal ideals, i.e., there exists a sequence $J_1, J_2, \cdots, J_n$ of nonzero principal ideals, such that $I = \sum_{k=1}^{n} J_k$.

If we can prove that $I_0, I_1, I_2, I_3, I_4, I_5$ is closed under addition, then every ideal is principal, and we've found every ideal of $\mathbb{Z}_3\times\mathbb{Z}_4$.

+	I_0	I_1	I_2	I_3	I_4	I_5
I_0	I_0	I_1	I_2	I_3	I_4	I_5
I_1	I_1	I_1	I_4	I_5	I_4	I_5
I_2	I_2	I_4	I_2	I_3	I_4	I_5
I_3	I_3	I_5	I_3	I_3	I_5	I_5
I_4	I_4	I_4	I_4	I_5	I_4	I_5
I_5	I_5	I_5	I_5	I_5	I_5	I_5

Date / /

Step3: We test whether each I_k is prime.

$\cdot$	I_0	I_1	I_2	I_3	I_4	I_5
I_0	I_0	I_0	I_0	I_0	I_0	I_0
I_1	I_0	I_1	I_0	I_0	I_1	I_1
I_2	I_0	I_0	I_0	I_2	I_0	I_2
I_3	I_0	I_0	I_2	I_3	I_2	I_3
I_4	I_0	I_1	I_0	I_2	I_1	I_4
I_5	I_0	I_1	I_2	I_3	I_4	I_5

For the ideal $I_0=\{(0,0)\}$, $I_0 \supseteq I_1 \cdot I_2$ but $I_0 \neq I_1$ and $I_0 \neq I_2$, so I_0 is not prime.

For the ideal $I_1=\{(0,0),(1,0),(2,0)\}$,

$I_1 \supseteq I_2 \cdot I_2$ but $I_1 \nsubseteq I_2$ and $I_1 \neq I_2$, so I_1 is not prime.

For the ideal $I_2=\{(0,0),(0,2)\}$,

$I_2 \supseteq I_1 \cdot I_3$ but $I_2 \nsubseteq I_1$ and $I_2 \neq I_3$, so I_2 is not prime.

For the ideal $I_3=\{(0,0),(0,1),(0,2),(0,3)\}$,

$I_3 \neq \mathbb{Z}_3 \times \mathbb{Z}_4$, and $A_3=\{I_k : I_3 \neq I_k\}=\{I_1, I_4, I_5\}$

is closed under multiplication, so I_3 is prime.

$\cdot$	I_1	I_4	I_5
I_1	I_1	I_1	I_1
I_4	I_1	I_1	I_4
I_5	I_1	I_4	I_5

For the ideal $I_4=\{(0,0),(1,0),(2,0),(0,2),(1,2),(2,2)\}$,

$I_4 \neq \mathbb{Z}_3 \times \mathbb{Z}_4$, and $A_4=\{I_k : I_4 \neq I_k\}=\{I_3, I_5\}$

is closed under multiplication, so I_4 is prime.

$\cdot$	I_3	I_5
I_3	I_3	I_3
I_5	I_3	I_5

Date / /

For the ideal $I_5 = \mathbb{Z}_3 \times \mathbb{Z}_4$, it is not prime.

Hence, we've obtained all prime ideals I_3, I_4 of $\mathbb{Z}_3 \times \mathbb{Z}_4$.

Step4: We test whether each I_k is maximal.

For the ideal $I_0 = \{(0,0)\}$, there is an ideal I_1 such that $I_0 \subsetneq I_1 \subsetneq I_5$, so I_0 is not maximal.

For the ideal $I_1 = \{(0,0), (1,0), (2,0)\}$,

there is an ideal I_4 such that $I_1 \subsetneq I_4 \subsetneq I_5$, so I_1 is not maximal.

For the ideal $I_2 = \{(0,0), (0,2)\}$,

there is an ideal I_4 such that $I_2 \subsetneq I_4 \subsetneq I_5$, so I_2 is not maximal.

For the ideal $I_3 = \{(0,0), (0,1), (0,2), (0,3)\}$,

$B_3 = \{I_k : I_3 \subseteq I_k\} = \{I_3, I_5\}$ has cardinality 2, so I_3 is maximal.

For the ideal $I_4 = \{(0,0), (1,0), (2,0), (0,2), (1,2), (2,2)\}$,

$B_4 = \{I_k : I_4 \subseteq I_k\} = \{I_4, I_5\}$ has cardinality 2, so I_4 is maximal.

For the ideal $I_5 = \mathbb{Z}_3 \times \mathbb{Z}_4$, it is not maximal.

Hence, we've obtained all maximal ideals I_3, I_4 of $\mathbb{Z}_3 \times \mathbb{Z}_4$.

2.(a) Solution: We may divide our proof into eight parts.

Part1: We prove that $A \triangle B = \{x \in S : x \in A \text{ or } x \in B\}$ is commutative.

$x \in A$	$x \in B$	$x \in A$ or $x \in B$	$x \in B$ or $x \in A$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	F	F

$\forall A, B \in P(S), A \triangle B = \{x \in S : x \in A \text{ or } x \in B\} = \{x \in S : x \in B \text{ or } x \in A\} = B \triangle A$.

Date / /

Part2: We prove that $A\Delta B = \{x \in S : x \in A \text{ xor } x \in B\}$ is associative.

$x\in A$	$x\in B$	$x\in C$	$x\in A$ xor $x\in B$	$x\in B$ xor $x\in C$	$x\in A$ xor ($x\in B$ xor $x\in C$)		$(x\in A$ xor $x\in B)$ xor $x\in C$
T	T	T	F	F	T	⇔	T
T	T	F	F	T	F	⇔	F
T	F	T	T	T	F	⇔	F
T	F	F	T	F	T	⇔	T
F	T	T	T	F	F	⇔	F
F	T	F	T	T	T	⇔	T
F	F	T	F	T	T	⇔	T
F	F	F	F	F	F	⇔	F

$\forall A,B,C \in \mathcal{P}(S)$, $A\Delta(B\Delta C) = \{x \in S : x \in A \text{ xor } (x \in B \text{ xor } x \in C)\}$

$= \{x \in S : (x \in A \text{ xor } x \in B) \text{ xor } x \in C\} = (A\Delta B)\Delta C$

Part3: We prove that ϕ is a zero element

$x\in\phi$	$x\in A$		$x\in\phi$ xor $x\in A$		$x\in A$ xor $x\in\phi$
F	T	⇔	T	⇔	T
F	F	⇔	F	⇔	F

$\exists \phi \in \mathcal{P}(S), \forall A \in \mathcal{P}(S), A = \{x \in S : x \in A\}$

$= \phi\Delta A = \{x \in S : x \in \phi \text{ xor } x \in A\}$

$= A\Delta\phi = \{x \in S : x \in A \text{ xor } x \in \phi\}$.

Part4: We prove that every A has an additive inverse A

	$x\in A$	$x\in A$	$x\in A$ xor $x\in A$		$x\in A$ xor $x\in A$		$x\in\phi$
	T	T	F	⇔	F	⇔	F
	F	F	F	⇔	F	⇔	F

Date / /

$\forall A \in \mathcal{P}(S), \exists A \in \mathcal{P}(S), A \triangle A = \{x \in S : x \in A \text{ or } x \in A\}$

$= A \triangle A = \{x \in S : x \in A \text{ or } x \in A\}$

$= \emptyset = \{x \in S : x \in \emptyset\}$

Part5: We prove that $A \cap B = \{x \in S : x \in A \text{ and } x \in B\}$ is commutative.

$x \in A$	$x \in B$	$x \in A$ and $x \in B$		$x \in B$ and $x \in A$
T	T	T	$\Leftrightarrow$	T
T	F	F	$\Leftrightarrow$	F
F	T	F	$\Leftrightarrow$	F
F	F	F	$\Leftrightarrow$	F

$\forall A, B \in \mathcal{P}(S), A \cap B = \{x \in S : x \in A \text{ and } x \in B\} = \{x \in S : x \in B \text{ and } x \in A\} = B \cap A.$

Part6: We prove that $A \cap B = \{x \in S : x \in A \text{ and } x \in B\}$ is associative.

$x \in A$	$x \in B$	$x \in C$	$x \in A$ and $x \in B$	$x \in B$ and $x \in C$	$x \in A$ and ($x \in B$ and $x \in C$)		($x \in A$ and $x \in B$) and $x \in C$
T	T	T	T	T	T	$\Leftrightarrow$	T
T	T	F	T	F	F	$\Leftrightarrow$	F
T	F	T	F	F	F	$\Leftrightarrow$	F
T	F	F	F	F	F	$\Leftrightarrow$	F
F	T	T	F	T	F	$\Leftrightarrow$	F
F	T	F	F	F	F	$\Leftrightarrow$	F
F	F	T	F	F	F	$\Leftrightarrow$	F
F	F	F	F	F	F	$\Leftrightarrow$	F

$\forall A, B, C \in \mathcal{P}(S), A \cap (B \cap C) = \{x \in S : x \in A \text{ and } (x \in B \text{ and } x \in C)\}$

$= \{x \in S : (x \in A \text{ and } x \in B) \text{ and } x \in C\} = (A \cap B) \cap C$

Date / /

Part 7: We prove that S is a unity.

$x \in S$	$x \in A$	$x \in S$ and $x \in A$	$x \in A$ and $x \in S$
T	T $\iff$	T $\iff$	T
T	F $\iff$	F $\iff$	F

$\exists S \in \mathcal{P}(S),\ \forall A \in \mathcal{P}(S),\ A = \{x \in S : x \in A\}$

$= S \cap A = \{x \in S : x \in S \text{ and } x \in A\}$

$= A \cap S = \{x \in S : x \in A \text{ and } x \in S\}$

Part 8: We prove that $\cap$ distributes over Δ on the left,

as $\cap$ is commutative, it automatically distributes over Δ on the right.

$x \in A$	$x \in B$	$x \in C$	$x \in B$ xor $x \in C$	$x \in A$ and $x \in B$	$x \in A$ and $x \in C$	$x \in A$ and ($x \in B$ xor $x \in C$)	($x \in A$ and $x \in B$) xor ($x \in A$ and $x \in C$)
T	T	T	F	T	T	F $\iff$	F
T	T	F	T	T	F	T $\iff$	T
T	F	T	T	F	T	T $\iff$	T
T	F	F	F	F	F	F $\iff$	F
F	T	T	F	F	F	F $\iff$	F
F	T	F	T	F	F	F $\iff$	F
F	F	T	T	F	F	F $\iff$	F
F	F	F	F	F	F	F $\iff$	F

$\forall A, B, C \in \mathcal{P}(S),\ A \cap (B \Delta C) = \{x \in S : x \in A \text{ and } (x \in B \text{ xor } x \in C)\}$

$= \{x \in S : (x \in A \text{ and } x \in B) \text{ xor } (x \in A \text{ and } x \in C)\} = (A \cap B) \Delta (A \cap C)$

To conclude, $\mathcal{P}(S)$ is a commutative ring with unity.

Date / /

(b) Solution:

On one hand, $0 1_{\mathcal{P}(S)} = 0_{\mathcal{P}(S)} = \phi$

$1 1_{\mathcal{P}(S)} = 1_{\mathcal{P}(S)} = S$

$(-1) 1_{\mathcal{P}(S)} = -1_{\mathcal{P}(S)} = -S = S$

On the other hand, for all $n \geq 0$:

$(2n) 1_{\mathcal{P}(S)} = \phi$ and $[\pm(2n+1)] 1_{\mathcal{P}(S)} = S$

$\Rightarrow [\pm(2n+2)] 1_{\mathcal{P}(S)} = [\pm(2n+1)] 1_{\mathcal{P}(S)} \pm 1_{\mathcal{P}(S)}$

$= S \pm S = \phi$

and $[\pm(2n+3)] 1_{\mathcal{P}(S)} = [\pm(2n+2)] 1_{\mathcal{P}(S)} \pm 1_{\mathcal{P}(S)}$

$= \phi \pm S = S$

Hence, $\ker(\phi_{\mathcal{P}(S)}) = \{n \in \mathbb{Z} : n 1_{\mathcal{P}(S)} = 0_{\mathcal{P}(S)}\}$

$= 2\mathbb{Z}$, $\mathrm{Char}(\mathcal{P}(S)) = 2$.

(c) Solution: It suffices to show the following:

$\forall A \in \mathcal{P}(S), A \notin P \Rightarrow P + \langle A \rangle = \mathcal{P}(S)$

Step1: Show that $A^c \in P$.

As P is prime in $\mathcal{P}(S)$, $P \ni \phi = A \cdot A^c \Rightarrow P \ni A$ or $P \ni A^c \Rightarrow P \ni A^c$

Step2: For all $B \in \mathcal{P}(S)$, show that $B = A^c \triangle (A \cap B) = A^c + (A \cdot B)$.

$x \in A$	$x \notin A$	$x \in B$	$x \in A$ and $x \in B$	$x \notin A$ xor $(x \in A$ and $x \in B)$
T	F	T	T	T
T	F	F	F	F
F	T	T	F	T
F	T	F	F	F

Hence, $B = \{x \in S : x \in B\} = \{x \in S : x \notin A$ xor $(x \in A$ and $x \in B)\} = A^c + (A \cdot B)$

Step3: As the arbitrary element $B = A^c + (A \cdot B) \in P + \langle A \rangle$, we have $P + \langle A \rangle = \mathcal{P}(S)$

($A^c \in P$, $A \cdot B \in \langle A \rangle$)

3.(a) Solution: We may divide our proof into eight parts.

Part1: $\forall \alpha\mapsto\phi(\alpha), \alpha\mapsto\psi(\alpha) \in Map(R,R)$,

$$\alpha\mapsto\phi(\alpha)+\alpha\mapsto\psi(\alpha) = \alpha\mapsto\phi(\alpha)+\psi(\alpha)$$
$$= \alpha\mapsto\psi(\alpha)+\phi(\alpha)$$
$$= \alpha\mapsto\psi(\alpha)+\alpha\mapsto\phi(\alpha)$$

Part2: $\forall \alpha\mapsto\phi(\alpha), \alpha\mapsto\psi(\alpha), \alpha\mapsto\theta(\alpha) \in Map(R,R)$,

$$\alpha\mapsto\phi(\alpha)+[\alpha\mapsto\psi(\alpha)+\alpha\mapsto\theta(\alpha)]$$
$$= \alpha\mapsto\phi(\alpha)+\alpha\mapsto\psi(\alpha)+\theta(\alpha)$$
$$= \alpha\mapsto\phi(\alpha)+[\psi(\alpha)+\theta(\alpha)]$$
$$= \alpha\mapsto[\phi(\alpha)+\psi(\alpha)]+\theta(\alpha)$$
$$= \alpha\mapsto\phi(\alpha)+\psi(\alpha)+\alpha\mapsto\theta(\alpha)$$
$$= [\alpha\mapsto\phi(\alpha)+\alpha\mapsto\psi(\alpha)]+\alpha\mapsto\theta(\alpha)$$

Part3: $\exists \alpha\mapsto 0 \in Map(R,R)$, $\forall \alpha\mapsto\phi(\alpha) \in Map(R,R)$,

$$\alpha\mapsto 0+\alpha\mapsto\phi(\alpha) = \alpha\mapsto 0+\phi(\alpha) = \alpha\mapsto\phi(\alpha)$$
$$\alpha\mapsto\phi(\alpha)+\alpha\mapsto 0 = \alpha\mapsto\phi(\alpha)+0 = \alpha\mapsto\phi(\alpha)$$

Part4: $\forall \alpha\mapsto\phi(\alpha) \in Map(R,R)$, $\exists \alpha\mapsto[-\phi(\alpha)] \in Map(R,R)$,

$$\alpha\mapsto[-\phi(\alpha)]+\alpha\mapsto\phi(\alpha) = \alpha\mapsto[-\phi(\alpha)]+\phi(\alpha) = \alpha\mapsto 0$$
$$\alpha\mapsto\phi(\alpha)+\alpha\mapsto[-\phi(\alpha)] = \alpha\mapsto\phi(\alpha)+[-\phi(\alpha)] = \alpha\mapsto 0$$

Part5: $\forall \alpha\mapsto\phi(\alpha), \alpha\mapsto\psi(\alpha) \in Map(R,R)$,

$$\alpha\mapsto\phi(\alpha)\cdot\alpha\mapsto\psi(\alpha) = \alpha\mapsto\phi(\alpha)\cdot\psi(\alpha)$$
$$= \alpha\mapsto\psi(\alpha)\cdot\phi(\alpha)$$
$$= \alpha\mapsto\psi(\alpha)\cdot\alpha\mapsto\phi(\alpha)$$

Date / /

Part 6: $\forall \alpha\mapsto\phi(\alpha), \alpha\mapsto\psi(\alpha), \alpha\mapsto\theta(\alpha)\in Map(R,R)$,

$\alpha\mapsto\phi(\alpha)\cdot[\alpha\mapsto\psi(\alpha)\cdot\alpha\mapsto\theta(\alpha)]$

$=\alpha\mapsto\phi(\alpha)\cdot\alpha\mapsto\psi(\alpha)\cdot\theta(\alpha)$

$=\alpha\mapsto\phi(\alpha)\cdot[\psi(\alpha)\cdot\theta(\alpha)]$

$=\alpha\mapsto[\phi(\alpha)\cdot\psi(\alpha)]\cdot\theta(\alpha)$

$=\alpha\mapsto\phi(\alpha)\cdot\psi(\alpha)\cdot\alpha\mapsto\theta(\alpha)$

$=[\alpha\mapsto\phi(\alpha)\cdot\alpha\mapsto\psi(\alpha)]\cdot\alpha\mapsto\theta(\alpha)$

Part 7: $\exists\,\alpha\mapsto 1\in Map(R,R), \forall\alpha\mapsto\phi(\alpha)\in Map(R,R)$,

$\alpha\mapsto 1\cdot\alpha\mapsto\phi(\alpha)=\alpha\mapsto 1\cdot\phi(\alpha)=\alpha\mapsto\phi(\alpha)$

$\alpha\mapsto\phi(\alpha)\cdot\alpha\mapsto 1=\alpha\mapsto\phi(\alpha)\cdot 1=\alpha\mapsto\phi(\alpha)$

Part 8: $\forall\alpha\mapsto\phi(\alpha),\alpha\mapsto\psi(\alpha),\alpha\mapsto\theta(\alpha)\in Map(R,R)$,

$\alpha\mapsto\phi(\alpha)\cdot[\alpha\mapsto\psi(\alpha)+\alpha\mapsto\theta(\alpha)]$

$=\alpha\mapsto\phi(\alpha)\cdot\alpha\mapsto\psi(\alpha)+\theta(\alpha)$

$=\alpha\mapsto\phi(\alpha)\cdot[\psi(\alpha)+\theta(\alpha)]$

$=\alpha\mapsto[\phi(\alpha)\cdot\psi(\alpha)]+[\phi(\alpha)\cdot\theta(\alpha)]$

$=\alpha\mapsto\phi(\alpha)\cdot\psi(\alpha)+\alpha\mapsto\phi(\alpha)\cdot\theta(\alpha)$

$=[\alpha\mapsto\phi(\alpha)\cdot\alpha\mapsto\psi(\alpha)]+[\alpha\mapsto\phi(\alpha)\cdot\alpha\mapsto\theta(\alpha)]$

As $\cdot$ is commutative, it automatically distributes over $+$ on the right.

To conclude, $Map(R,R)$ is a commutative ring with unity.

Date / /

(b)(i) Solution: We may divide our solution into three parts.

Part1: F(The polynomial with degree 0 and constant term 1)

$=$(The function on R with constant image 1), so F preserves unity.

Part2: For all $\sum_{k\in K} a_k t^k, \sum_{\ell\in L} b_\ell t^\ell \in R[t]$,

$$F\left(\sum_{k\in K} a_k t^k + \sum_{\ell\in L} b_\ell t^\ell\right) = F\left(\sum_{s\in K\cup L} (a_s+b_s)t^s\right)$$

$$= \alpha \mapsto \sum_{s\in K\cup L} (a_s+b_s)\alpha^s = \alpha\mapsto \sum_{k\in K} a_k\alpha^k + \alpha\mapsto \sum_{\ell\in L} b_\ell\alpha^\ell$$

$$= F\left(\sum_{k\in K} a_k t^k\right) + F\left(\sum_{\ell\in L} b_\ell t^\ell\right), \text{ so } F \text{ preserves addition.}$$

Part3: For all $\sum_{k\in K} a_k t^k, \sum_{\ell\in L} b_\ell t^\ell \in R[t]$,

$$F\left(\sum_{k\in K} a_k t^k \cdot \sum_{\ell\in L} b_\ell t^\ell\right) = F\left(\sum_{(k,\ell)\in K\times L} a_k b_\ell t^{k+\ell}\right)$$

$$= \alpha \mapsto \sum_{(k,\ell)\in K\times L} a_k b_\ell \alpha^{k+\ell} = \alpha\mapsto \sum_{k\in K} a_k\alpha^k \cdot \alpha\mapsto \sum_{\ell\in L} b_\ell\alpha^\ell$$

$$= F\left(\sum_{k\in K} a_k t^k\right)\cdot F\left(\sum_{\ell\in L} b_\ell t^\ell\right), \text{ so } F \text{ preserves multiplication.}$$

To conclude, F is a ring homomorphism.

(ii) Solution: Assume that $R=\{\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n\}$, where $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n$ are pairwisely distinct elements. As R is a field, the finite product $(\alpha_k-\alpha_0)(\alpha_k-\alpha_1)(\alpha_k-\alpha_2)\cdots(\alpha_k-\alpha_{k-1})(\alpha_k-\alpha_{k+1})\cdots(\alpha_k-\alpha_n)$ is nonzero, thus invertible. Hence, the following polynomial is well-defined.

Date / /

$$f(x)=\frac{(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_n)}f_R(x_0)+\frac{(x-x_0)(x-x_2)\cdots(x-x_n)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_n)}f_R(x_1)$$

$$+\cdots+\frac{(x-x_0)(x-x_1)(x-x_2)\cdots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)(x_n-x_2)\cdots(x_n-x_{n-1})}f_R(x_n)\in R[x]$$

No matter which $f_R\in Map(R,R)$ we choose, such $f(x)$ is always well-defined. Note further that forall $x_k\in R$:

[The evaluation of $f(x)$ at $x=x_k$]

$$=\frac{(x_k-x_1)(x_k-x_2)\cdots\boxed{(x_k-x_k)}\cdots(x_k-x_n)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_k)\cdots(x_0-x_n)}f_R(x_0)\quad(\boxed{(x_k-x_k)}\to 0)$$

$$+\frac{(x_k-x_0)(x_k-x_2)\cdots\boxed{(x_k-x_k)}\cdots(x_k-x_n)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_k)\cdots(x_1-x_n)}f_R(x_1)\quad(\boxed{(x_k-x_k)}\to 0)$$

$$+\cdots+\frac{\boxed{(x_k-x_0)(x_k-x_1)(x_k-x_2)\cdots(x_k-x_{k-1})(x_k-x_{k+1})\cdots(x_k-x_n)}}{(x_k-x_0)(x_k-x_1)(x_k-x_2)\cdots(x_k-x_{k-1})(x_k-x_{k+1})\cdots(x_k-x_n)}f_R(x_k)\quad(\boxed{\cdots}\to 1)$$

$$+\cdots+\frac{(x_k-x_0)(x_k-x_1)(x_k-x_2)\cdots\boxed{(x_k-x_k)}\cdots(x_k-x_{n-1})}{(x_n-x_0)(x_n-x_1)(x_n-x_2)\cdots(x_n-x_k)\cdots(x_n-x_{n-1})}f_R(x_n)\quad(\boxed{(x_k-x_k)}\to 0)$$

$$=0f_R(x_0)+0f_R(x_1)+\cdots+1f_R(x_k)+\cdots+0f_R(x_n)=f_R(x_k)$$

This implies $F(f(x))=f_R(x)$, F is surjective.

(iii) Solution: We wish to show that F has a trivial kernel.

Forall $\sum_{k=0}^{n}a_kx^k\in R[x]$, assume that $F(\sum_{k=0}^{n}a_kx^k)=\alpha\mapsto 0$.

Take $n+1$ distinct elements $x_0,x_1,\cdots,x_n$ from the infinite field R.

Evaluate $\sum_{k=0}^{n}a_kx^k$ at $x_0,x_1,\cdots,x_n$ respectively, and we get a linear system:

$$\begin{cases}a_0+a_1x_0+a_2x_0^2+\cdots+a_nx_0^n=0\\ a_0+a_1x_1+a_2x_1^2+\cdots+a_nx_1^n=0\\ a_0+a_1x_2+a_2x_2^2+\cdots+a_nx_2^n=0\\ \vdots\quad\vdots\quad\vdots\quad\vdots\\ a_0+a_1x_n+a_2x_n^2+\cdots+a_nx_n^n=0\end{cases}$$

Date / /

As the following coefficient determinant is nonzero:

$$\text{Det}\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} = \overrightarrow{\prod_{0\le i<j\le n}} (x_j - x_i) \neq 0$$

The above-mentioned linear system only has the trivial solution $a_0 = a_1 = a_2 = \cdots = a_n = 0$

This implies $\sum_{k=0}^{n} a_k x^k = 0$, $\text{Ker}(F) = \{0\}$, F is injective.

4. Proof: Assume to the contrary that a field $\mathbb{F}$ is finite.

According to Lemma 9.5.3, $\mathbb{F}$ is a field $\Rightarrow$ $\mathbb{F}$ is the zero field or $\text{Char}(\mathbb{F}) = p$ is prime.

If $\mathbb{F}$ is the zero field, then every polynomial in $\mathbb{F}[t]$ is the zero polynomial.

It doesn't make sense to discuss whether $\mathbb{F}$ is algebraically closed or not.

If $\text{Char}(\mathbb{F}) = p$ is prime, then $\mathbb{F}$ contains at least two elements and $|\mathbb{F}| < +\infty$.

Now $\left[\prod_{\text{All Element } x_k \in \mathbb{F}} (x - x_k)\right] + 1$ is well-defined, nonconstant and has no root in $\mathbb{F}$,

thus $\mathbb{F}$ is not algebraically closed. Hence, we are done.

5. Solution:

For the polynomial t^2+1 in $\mathbb{Q}[t]$, it has no root in $\mathbb{Q}$, thus irreducible in $\mathbb{Q}[t]$. Now theorem 11.2.16 suggests that $\mathbb{Q}[t]/\langle t^2+1 \rangle$ is a field.

For the polynomial t^2+1 in $\mathbb{Z}_3[t]$, the following table suggests that t^2+1 has no root in $\mathbb{Z}_3$:

The congruence class of t to	The evaluation of t^2+1
0	1
1	2
2	$5 \equiv 2$

Date / /

Hence, t^2+1 is irreducible in $\mathbb{Z}_3[t]$. Now theorem 11.2.16 suggests that $\mathbb{Z}_3[t]/\langle t^2+1\rangle$ a field.

For the polynomial t^2+1 in $\mathbb{Z}_5[t]$, note that $t^2+1 = t^2-4 = (t+2)(t-2)$ is reducible. (deg=2, deg=1, deg=1, 1<2)

Now theorem 11.2.16 suggests that $\mathbb{Z}_5[t]/\langle t^2+1\rangle$ is not a field.

For the polynomial t^3+t^2+1 (deg=3) in $\mathbb{Z}_2[t]$, the following table suggests that t^3+t^2+1 (deg=3) has no root in $\mathbb{Z}_2$

The congruence class of t	The evaluation of t^3+t^2+1
0	1
1	$3\equiv 1$

Hence, t^3+t^2+1 (deg=3) is irreducible in $\mathbb{Z}_2[t]$. Now theorem 11.2.16. suggests that $\mathbb{Z}_2[t]/\langle t^3+t^2+1\rangle$ is a field.

6. Proof: For the polynomial t^2+4t+1 (deg=2) in $\mathbb{Z}_5[t]$, the following table suggests that t^2+4t+1 (deg=2) has no root in $\mathbb{Z}_5$

The congruence class of t	The evaluation of t^2+4t+1
0	1
1	$6\equiv 1$
2	$13\equiv 3$
3	$22\equiv 2$
4	$33\equiv 3$

Hence, t^2+4t+1 (deg=2) is irreducible in $\mathbb{Z}_5$.

Now theorem 11.2.16. suggests that $\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle$ is a field.

Regard the field $\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle = \mathbb{F}_{25}$ as a vector space over $\mathbb{Z}_5$.

The Division Algorithm in $\mathbb{Z}_5[t]$ suggests that:

(1) Every $f(t)+\langle t^2+4t+1\rangle$ is equal to some $a_1t+a_0+\langle t^2+4t+1\rangle$

(2) For all $a_1t+a_0+\langle t^2+4t+1\rangle$, $a_1t+a_0+\langle t^2+4t+1\rangle = \langle t^2+4t+1\rangle$

$\Rightarrow a_1t+a_0 \in \langle t^2+4t+1\rangle \Rightarrow t^2+4t+1 \mid a_1t+a_0 \Rightarrow a_1=a_0=0$.

Hence, $(t, 1)$ is a basis of the vector space $|\mathbb{F}_{25}|$, $|\mathbb{F}_{25}| = |\mathbb{Z}_5|^{\dim|\mathbb{F}_{25}|} = 5^2 = 25$

Date / /

Now let's proceed to prove that t^2+4t+1 has a root in $\mathbb{F}_{25}=\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle$

Take the coset $\tilde{c} = t+\langle t^2+4t+1\rangle$,

we have $\tilde{c}^2 = t^2+\langle t^2+4t+1\rangle = (t^2+4t+1-4t-1)+\langle t^2+4t+1\rangle$

$= [t^2+4t+1+\langle t^2+4t+1\rangle] - 4[t+\langle t^2+4t+1\rangle] - [1+\langle t^2+4t+1\rangle]$

$= \tilde{0} - 4\tilde{c} - \tilde{1}$, $\tilde{c}^2+4\tilde{c}+\tilde{1}=\tilde{0}$

Hence, the evaluation of t^2+4t+1 at $t=\tilde{c}$ is $\tilde{0}$, t^2+4t+1 has a root in $\mathbb{F}_{25}$

7. Solution:

Define G as the multiplicative group $\mathbb{F}_q^\times$,

and X as the multiplicative group $\mathbb{F}_q^\times$, but we treat it as a set.

G acts on X by left multiplication.

Now $\prod_{\text{All element } \alpha\in X} \alpha \xrightarrow{\text{The left translation map } l_g:\alpha\mapsto g*\alpha \text{ is bijective}} \prod_{\text{All element } \alpha\in X} (g*\alpha)$

$= \prod_{\text{All } \alpha\in\mathbb{F}_q^\times} (g\alpha) \xrightarrow{\mathbb{F}_q^\times \text{ is Abelian}} \prod_{\text{All } \alpha\in\mathbb{F}_q^\times} g \prod_{\text{All } \alpha\in\mathbb{F}_q^\times} \alpha$

$= g^{|\mathbb{F}_q^\times|} \prod_{\text{All } \alpha\in\mathbb{F}_q^\times} \alpha$, $e = g^{|\mathbb{F}_q^\times|} = g^{q-1}$

As the identity element $e\in\mathbb{F}_q^\times$ is the unity 1,

we end up with an analogous version of Fermat's Little Theorem:

$$\forall g\in\mathbb{F}_q^\times,\ g^{q-1}=1$$

Date / /