20241119 MATH3301 Tutorial 10

1.(a) Proof: Recall that $\text{char}(R)$ is the unique nonnegative integer n such that $\text{Ker}(\phi_R) = n\mathbb{Z}$, where $\phi_R: \mathbb{Z} \to R, n \mapsto n1_R$ is a ring homomorphism.

Now $m1_R = 0_R \Rightarrow m \in \text{Ker}(\phi_1) \Rightarrow m \in n\mathbb{Z} \Rightarrow n|m$

(b) Proof: Assume that $\text{char}(R/I) = k$ and $\text{char}(R) = n$, want to show $k|n$.

It suffices to show $n1_{R/I} = 0_{R/I}$, i.e., to show $n(1_R + I) = I$.

Notice that $n(1_R + I) = (n1_R) + I = 0_R + I = I$, and we are done.

2.(a) Proof: For all $r \in R$:

$r \in [\text{All zero divisors}] \cap [\text{All units}]$

$\Rightarrow r$ is a zero divisor and r is a unit.

$\Rightarrow r \neq 0_R$, and for some $r' \neq 0_R$, $rr' = r'r = 0_R$

and for some $r'' \in R$, $rr'' = r''r = 1_R$

$\Rightarrow r' = 1_R r' = r''rr' = r''0_R = 0_R \Rightarrow$ contradiction.

Hence, $[\text{All zero divisors}] \cap [\text{All units}] = \emptyset$

(b) Proof: Define $G = R^\times = [\text{All units}]$ and $X = R$.

Take an arbitrary $x \in X$, and assume to the contrary that G_x contains a nontrivial element $g \in G \setminus \{e\}$, where $e = 1_R$

$g \in G_x \Rightarrow g * x = x$ in set X

$\Rightarrow gx = 1_R x$ in ring R

$\Rightarrow x(g - 1_R) = 0$

$\Rightarrow$ If $x = 0_R$, then the equation is satisfied.

If $x \neq 0_R$ then $x \neq 0_R, g - 1_R \neq 0_R, x(g - 1_R) = 0_R$ suggests that x is a zero-divisor.

Date

(c)(i). Solution:

$R^G = [\text{All } G\text{-fixed points}] \subseteq [\text{All } r \in R \text{ with a nontrivial stabilizer subgroup } G_r] \subseteq \{0_R\} \cup [\text{All zero divisors}]$

In $\mathbb{Z}_{2p}$, r is a zero divisor iff $\gcd(r, 2p) \neq 1$, so:

$\{0_R\} \cup [\text{All zero divisors}] = \underbrace{\{0, 2, 4, \cdots, 2p-2\}}_{1^{st} \text{ part}} \cup \underbrace{\{p\}}_{2^{nd} \text{ part}}$

This implies $R^G \subseteq \{0, 2, 4, \cdots, 2p-2\} \cup \{p\}$

Case1: Consider the first part $\{0, 2, 4, \cdots, 2p-2\}$.

On one hand, every $r \in R^\times$ fixes 0, so $0 \in R^G$.

On the other hand, the set $\{2, 4, \cdots, 2p-2\}$ contains no solution of the equation $(2p-1) * x = x$, where $2p-1 \in R^\times$, so $\{2, 4, \cdots, 2p-2\}$ contains no element in R^G.

Case2: Consider the second part $\{p\}$.

For all unit $r \in R^\times$, our argument in Case1 suggests that $r \notin \{0, 2, 4, \cdots, 2p-2\}$, so $r = [\text{Some even integer}] + 1_R$.

This implies the identity:

$$\begin{aligned} r * p &= ([\text{Some even integer}] + 1_R) * p \\ &= ([\text{Some even integer}] + 1)p \\ &= [\text{Some even integer}]p + 1p = 0 + p = p. \end{aligned}$$

Hence, $p \in R^G$

To conclude, $R^G = \{0, p\}$.

(ii) Solution: $\#(\text{Element } x \in R \text{ with } G_x < G)$

$= |R| - \#(\text{Element } x \in R \text{ with } G_x = G) = 2p - 2$

Date / /

3.(a): Proof: It suffices to prove that every ideal of R is $\{0_R\}$ or R, both of which are principal ($\{0_R\} = 0_R R = R 0_R$, $R = 1_R R = R 1_R$).

For all nonzero ideal I of R, take an nonzero element r from I. As R is a field, there exists $r' \in R$, such that $rr' = r'r = 1_R$. This implies $1_R = \underset{R}{r'}\,\underset{I}{r} \in I$, which gives $I = R$.

(b) Proof: R is an integral domain $\Leftrightarrow$ [$\forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$]

$\Leftrightarrow$ [$\forall a, b \in R$, $\{0\} \ni ab \Rightarrow \{0\} \ni a$ or $\{0\} \ni b$]

$\Leftrightarrow$ $\{0\}$ is prime in R

(c) Proof: R is a field $\Leftrightarrow$ [$\forall a \in R \setminus \{0\}$, $\exists b \in R$, $ab = ba = 1$]

$\Leftrightarrow$ [$\forall a \in R \setminus \{0\}$, $\{0\} + \langle a \rangle = \langle a \rangle + \{0\} \ni 1$]

$\Leftrightarrow$ [$\forall a \in R \setminus \{0\}$, $\{0\} + \langle a \rangle = \langle a \rangle + \{0\} = R$]

$\Leftrightarrow$ $\{0\}$ is maximal in R.

4. (a) Proof: We may divide our proof into two parts.

Part1: In this part, we prove that $\langle 2 \rangle \subsetneq \langle 2, t \rangle$.

Every $2r(t) \in \langle 2 \rangle$ can be written as $2r(t) + t \cdot 0 \in \langle 2, t \rangle$, so $\langle 2 \rangle \subseteq \langle 2, t \rangle$

Note that t has at least one odd coefficient 1, so $t \in \langle 2, t \rangle \setminus \langle 2 \rangle$, $\langle 2 \rangle \subsetneq \langle 2, t \rangle$

Part2: In this part, we prove that $\langle t \rangle \subsetneq \langle 2, t \rangle$.

Every $t r(t) \in \langle t \rangle$ can be written as $2 \cdot 0 + t r(t) \in \langle 2, t \rangle$, so $\langle t \rangle \subseteq \langle 2, t \rangle$

Note that 2 has order $0 \notin \{-\infty\} \cup \{1, 2, 3, \cdots\}$, so $2 \in \langle 2, t \rangle \setminus \langle t \rangle$, $\langle t \rangle \subsetneq \langle 2, t \rangle$

(b) Proof: For all principal ideal $\langle r(t) \rangle$, we wish to show that $\langle 2, t \rangle \subseteq \langle r(t) \rangle \Rightarrow r(t) = \pm 1$

On one hand, $\langle t \rangle \subseteq \langle r(t) \rangle \Rightarrow$ every polynomial with deg ≥ 1 is in $\langle r(t) \rangle$,

so $\deg r(t) \neq -\infty$ and $\deg r(t) \leq 1$.

On the other hand, if $\deg r(t) = 1$, then $2 \notin \langle r(t) \rangle$, which is a contradiction.

if $\deg r(t) = 0$ and $r(t) \neq \pm 1$, then $t \notin \langle r(t) \rangle$, another contradiction. Hence, $r(t) = \pm 1$ and we're done.

Date

(c) Proof: We may divide our proof into two parts.

Part1: In this part, we prove that $\mathbb{Z}[t]/\langle 2,t\rangle$ is a field.

Note that $r(t)\in\langle 2,t\rangle \Leftrightarrow \exists p(t),q(t)\in\mathbb{Z}[t],\ r(t)=2p(t)+tq(t)$

$\Leftrightarrow$ The constant term of $r(t)$ is even,

so $\mathbb{Z}[t]/\langle 2,t\rangle = \{[\text{All } r(t) \text{ with even constant term}],$

$[\text{All } r(t) \text{ with odd constant term}]\}\cong \mathbb{Z}_2=\{0,1\}$ is a field.

Part2: In this part, we prove that $\mathbb{Z}[t]/\langle 2\rangle$ is not a field.

~~Recall that (i) I is maximal in R iff R/I is a field.~~

~~(ii) I is prime in R iff R/I is an integral domain.~~

Note that $\langle 2\rangle+\langle t\rangle=\langle 2,t\rangle\subsetneq\mathbb{Z}[t]$ for some $t\notin\langle 2\rangle$,

so $\langle 2\rangle$ is not maximal in $\mathbb{Z}[t]$, $\mathbb{Z}[t]/\langle 2\rangle$ is not a field.

(d) Proof: The following arguments shows that $\forall a(t),b(t)\in\mathbb{Z}[t],\ a(t)b(t)\in\langle 2\rangle\Rightarrow a(t)\in\langle 2\rangle$ or $b(t)\in\langle 2\rangle$

$a(t)\notin\langle 2\rangle$ and $b(t)\notin\langle 2\rangle$

$\Rightarrow$ Some coefficient a_i of $a(t)$ is odd, now take a_i with largest index i

and some coefficient b_j of $b(t)$ is odd, now take b_j with largest index j

$$\Rightarrow a(t)b(t)=\sum_{(p,q)\in\mathbb{P}\times\mathbb{Q}} a_p b_q t^{p+q} = \cdots+\Big(\underbrace{a_0 b_{i+j}}_{\text{even}}+\underbrace{a_1 b_{i+j-1}}_{\text{even}}+\cdots+\underbrace{a_{i-1}b_{j+1}}_{\text{even}}+\underbrace{a_i b_j}_{\text{odd}}+\underbrace{a_{i+1}b_{j-1}}_{\text{even}}+\cdots\Big)t^{i+j}+\cdots$$

(? even ? even ? even odd odd even ?)

The coefficient $a_0b_{i+j}+a_1b_{i+j-1}+\cdots+a_{i-1}b_{j+1}+a_ib_j+a_{i+1}b_{j-1}+\cdots$ IS ODD

$\Rightarrow a(t)b(t)\notin\langle 2\rangle$, so $\langle 2\rangle$ is prime in $\mathbb{Z}[t]$, $\mathbb{Z}[t]/\langle 2\rangle$ is an integral domain.

(e) Proof: We've constructed an ideal $\langle 2\rangle$ of $\mathbb{Z}[t]$,

such that $\langle 2\rangle$ is nonzero, prime and not maximal.

Date / /