2024/11/01 MATH3301 Tutorial 9

1.(a) Proof: We may divide our proof into 9 parts.

Part 1: $\forall \sum_{k\in K} a_k t^k, \sum_{l\in L} b_l t^l \in R[t]$

$$\sum_{k\in K} a_k t^k + \sum_{l\in L} b_l t^l = \sum_{s\in K\cup L}(a_s+b_s)t^s = \sum_{s\in K\cup L}(b_s+a_s)t^s = \sum_{l\in L} b_l t^l + \sum_{k\in K} a_k t^k$$

Hence, $+$ is commutative on $R[t]$

Part 2: $\forall \sum_{k\in K} a_k t^k, \sum_{l\in L} b_l t^l, \sum_{s\in S} c_s t^s \in R[t]$

$$\left(\sum_{k\in K} a_k t^k + \sum_{l\in L} b_l t^l\right) + \sum_{s\in S} c_s t^s = \sum_{m\in K\cup L}(a_m+b_m)t^m + \sum_{s\in S} c_s t^s$$

$$= \sum_{u\in(K\cup L)\cup S}[(a_u+b_u)+c_u]t^u = \sum_{u\in K\cup(L\cup S)}[a_u+(b_u+c_u)]t^u$$

$$= \sum_{k\in K} a_k t^k + \sum_{n\in L\cup S}(b_n+c_n)t^n = \sum_{k\in K} a_k t^k + \left(\sum_{l\in L} b_l t^l + \sum_{s\in S} c_s t^s\right)$$

Hence, $+$ is associative on $R[t]$

Part 3: $\exists 0\in R[t]$, $\forall \sum_{k\in K} a_k t^k \in R[t]$, $0 + \sum_{k\in K} a_k t^k = \sum_{k\in K} a_k t^k + 0 = \sum_{k\in K} a_k t^k$

Part 4: $\forall \sum_{k\in K} a_k t^k \in R[t]$, $\exists \sum_{k\in K}(-a_k)t^k \in R[t]$,

$$\sum_{k\in K} a_k t^k + \sum_{k\in K}(-a_k)t^k = \sum_{k\in K}(-a_k)t^k + \sum_{k\in K} a_k t^k = 0$$

Part 5: $\forall \sum_{k\in K} a_k t^k, \sum_{l\in L} b_l t^l \in R[t]$,

$$\sum_{k\in K} a_k t^k \sum_{l\in L} b_l t^l = \sum_{(k,l)\in K\times L} a_k b_l t^{k+l} = \sum_{(l,k)\in L\times K} b_l a_k t^{l+k} = \sum_{l\in L} b_l t^l \sum_{k\in K} a_k t^k$$

Hence, $\cdot$ is commutative on $R[t]$

Part 6: $\forall \sum_{k\in K} a_k t^k, \sum_{l\in L} b_l t^l, \sum_{s\in S} c_s t^s \in R[t]$,

$$\left(\sum_{k\in K} a_k t^k \sum_{l\in L} b_l t^l\right)\sum_{s\in S} c_s t^s = \sum_{(k,l)\in K\times L} a_k b_l t^{k+l} \sum_{s\in S} c_s t^s$$

$$= \sum_{((k,l),s)\in(K\times L)\times S}(a_k b_l)c_s t^{(k+l)+s} = \sum_{(k,(l,s))\in K\times(L\times S)} a_k(b_l c_s)t^{k+(l+s)}$$

$$= \sum_{k\in K} a_k t^k \sum_{(l,s)\in L\times S} b_l c_s t^{l+s} = \sum_{k\in K} a_k t^k\left(\sum_{l\in L} b_l t^l \sum_{s\in S} c_s t^s\right)$$

Hence, $\cdot$ is associative on $R[t]$

Part 7: $\exists 1 \in R[t], \forall \sum_{k\in K} a_k t^k \in R[t],\ 1 \sum_{k\in K} a_k t^k = \sum_{k\in K} a_k t^k\, 1 = \sum_{k\in K} a_k t^k$.

Part 8: $\forall \sum_{i\in I} \lambda_i t^i, \sum_{k\in K} a_k t^k, \sum_{\ell\in L} b_\ell t^\ell \in R[t]$,

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

$$= \sum_{(i,s)\in I\times(K\cup L)} \lambda_i (a_s+b_s) t^{i+s} = \sum_{(i,s)\in(I\times K)\cup(I\times L)} (\lambda_i a_s + \lambda_i b_s) t^{i+s}$$

$$= \sum_{(i,k)\in I\times K} \lambda_i a_k t^{i+k} + \sum_{(i,\ell)\in I\times L} \lambda_i b_\ell t^{i+\ell} = \sum_{i\in I} \lambda_i t^i \sum_{k\in K} a_k t^k + \sum_{i\in I} \lambda_i t^i \sum_{\ell\in L} b_\ell t^\ell$$

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

$$= \sum_{(s,i)\in(K\cup L)\times I} (a_s+b_s)\lambda_i t^{s+i} = \sum_{(s,i)\in(K\times I)\cup(L\times I)} (a_s\lambda_i + b_s\lambda_i) t^{s+i}$$

$$= \sum_{(k,i)\in K\times I} a_k \lambda_i t^{k+i} + \sum_{(\ell,i)\in L\times I} b_\ell \lambda_i t^{\ell+i} = \sum_{k\in K} a_k t^k \sum_{i\in I} \lambda_i t^i + \sum_{\ell\in L} b_\ell t^\ell \sum_{i\in I} \lambda_i t^i$$

Hence, $\cdot$ is distributive over $+$ on $R[t]$.

Part 9: For all $r \in R^\times$, there exists $r' \in R$, such that $rr' = 1$.

Hence, for this $r \in R[t]$, there exists $r' \in R[t]$, such that $rr' = 1$

This implies $r \in R[t]^\times$, so $R^\times \subseteq R[t]^\times$

But Consider $\mathbb{Z}_4[t]$,

$\mathbb{Z}_4[t]^\times$ contains units $1 \pm 2t$ which are not in $\mathbb{Z}_4^\times$

(b) In the ring $\mathbb{Z}_4$, multiplication is commutative, and a unity 1 exists.

Note that $\operatorname{ord}(2)=0$, $\operatorname{ord}(2)+\operatorname{ord}(2)=0$, $\operatorname{ord}(2\cdot 2)=\operatorname{ord}(0)=-\infty$

so $\forall f(t), g(t)\in\mathbb{Z}_4[t]$, $\operatorname{ord}[f(t)]+\operatorname{ord}[g(t)]=\operatorname{ord}[f(t)g(t)]$ is not true.

(c)(i) Assume to the contrary that $R[t]$ is not an integral domain,

so for some $\sum_{k\in K} a_k t^k, \sum_{\ell\in L} b_\ell t^\ell$ with degrees n, m respectively,

$\sum_{k\in K} a_k t^k \sum_{\ell\in L} b_\ell t^\ell = \sum_{(k,\ell)\in K\times L} a_k b_\ell t^{k+\ell} = 0$

Take the highest order terms $a_n t^n, b_m t^m$, their product $a_n b_m t^{n+m}=0$,

so $a_n b_m = 0$. As R is an integral domain, $a_n=0$ or $b_m=0$, contradicting to a_n, b_m are the leading coefficients.

Hence, our assumption is false, and we've proven $R[t]$ is an integral domain.

(ii) For all $\sum_{k\in K} a_k t^k, \sum_{\ell\in L} b_\ell t^\ell$ with degrees n, m respectively,

$a_n\neq 0, b_m\neq 0$ are their leading coefficients.

As R is an integral domain, $a_n b_m\neq 0$, so $\sum_{k\in K} a_k t^k \sum_{\ell\in L} b_\ell t^\ell = \sum_{(k,\ell)\in K\times L} a_k b_\ell t^{k+\ell}$

has degree $n+m$.

(d) In $\mathbb{Z}[t]$, choose $a(t)=t$, $b(t)=2t$, assume to the contrary that:

$$\exists q(t), r(t)\in\mathbb{Z}[t],\ a(t)=q(t)b(t)+r(t) \text{ and } \deg r(t)<\deg b(t)$$

i.e. $\exists \sum_{k\in K} q_k t^k, \sum_{\ell\in L} r_\ell t^\ell \in\mathbb{Z}[t]$, $t = 2t\sum_{k\in K} q_k t^k + \sum_{\ell\in L} r_\ell t^\ell$ and $\deg \sum_{\ell\in L} r_\ell t^\ell < 1$

From $\deg\sum_{\ell\in L} r_\ell t^\ell<1$, we have $\sum_{\ell\in L} r_\ell t^\ell = r_0$.

Now the equality of the first order terms suggests $1=2q_0$.

However, the equation $1=2q_0$ has no solution in $\mathbb{Z}$,

contradicting to the existence of $q(t)$.

Hence, our assumption is wrong, and we've proven that the division algorithm doesn't hold in $\mathbb{Z}[t]$.

2.(a) Proof: According to a similar argument in (a),

$$R[a]=\{\sum_{k\in K} r_k a^k \in S : \text{Each } r_k\in R\}$$

is a commutative ring with unity containing $R\cup\{a\}$.

~~Now, it suffices to show that every commutative ring T with unity containing $R\cup\{a\}$ must contain $R[a]$.~~

For all $\sum_{k\in K} r_k a^k \in R[a]$:

Step1: T is closed under multiplication,

so $r_1 a^1 = r_1 a \in T$, $r_2 a^2 = r_2 a a \in T, \cdots,$

$r_k a^k = r_k \overbrace{a a \cdots a}^{k \text{ copies}} \in T, \cdots$

Step2: T is closed under addition,

so $\sum_{k\in K} r_k a^k = r_0 + r_1 a^1 + r_2 a^2 + \cdots + r_k a^k + \cdots \in T$

Hence, $\sum_{k\in K} r_k a^k \in T$, T contains $R[a]$.

Combine the two parts above, we've shown that $R[a]$ is the smallest subring of S that contains $R\cup\{a\}$.

(b) (i) Note that $\sqrt{2}$ is a root of some order 2 polynomial $x^2-2\in\mathbb{Z}[x]$,

so $\mathbb{Z}[\sqrt{2}]=\{a_0+a_1\sqrt{2}\in\mathbb{C} : a_0, a_1\in\mathbb{Z}\}$.

(ii) Note that ω is a root of some order 2 polynomial $x^2+x+1\in\mathbb{Z}[x]$,

so $\mathbb{Z}[\omega]=\{a_0+a_1\omega\in\mathbb{C} : a_0, a_1\in\mathbb{Z}\}$

(iii) Note that $\sqrt[3]{2}$ is a root of some order 3 polynomial $x^3-2\in\mathbb{Z}[x]$,

so $\mathbb{Z}[\sqrt[3]{2}]=\{a_0+a_1\sqrt[3]{2}+a_2\sqrt[3]{4}\in\mathbb{C} : a_0, a_1, a_2\in\mathbb{Z}\}$

Note further that $\sqrt{3}$ is a root of some order 2 polynomial $x^2-3\in(\mathbb{Z}[\sqrt[3]{2}])[x]$,

so $\mathbb{Z}[\sqrt[3]{2},\sqrt{3}]=(\mathbb{Z}[\sqrt[3]{2}])[\sqrt{3}]=\{(a_0+a_1\sqrt[3]{2}+a_2\sqrt[3]{4})+(b_0+b_1\sqrt[3]{2}+b_2\sqrt[3]{4})\sqrt{3}\in\mathbb{C} :$
$a_0, a_1, a_2, b_0, b_1, b_2\in\mathbb{Z}\}$.

(iv) π is transcendental, so no simplification is needed,

$$\mathbb{Z}[\pi]=\{\sum_{k\in K} r_k\pi^k\in\mathbb{C} : \text{Each } r_k\in\mathbb{Z}\}.$$

(c) Note that the transcendental element π is "very similar to" an indeterminate t.

$\forall \sum\limits_{k\in K} a_k t^k, \sum\limits_{\ell\in L} b_\ell t^\ell \in \mathbb{Z}[t]$, $\sum\limits_{k\in K} a_k t^k = \sum\limits_{\ell\in L} b_\ell t^\ell \Leftrightarrow$ Each $a_s = b_s$

$\forall \sum\limits_{k\in K} a_k \pi^k, \sum\limits_{\ell\in L} b_\ell \pi^\ell \in \mathbb{Z}[t]$, $\sum\limits_{k\in K} a_k \pi^k = \sum\limits_{\ell\in L} b_\ell \pi^\ell \Leftrightarrow$ Each $a_s = b_s$

Hence, the evaluation map $\sigma : \sum\limits_{k\in K} a_k t^k \mapsto \sum\limits_{k\in K} a_k \pi^k$ is injective.

Notice further that:

- $\mathbb{Z}[t]$ is a polynomial ring, every $\sum\limits_{k\in K} a_k t^k$ has a unique representation in $\mathbb{Z}[t]$, so σ is well-defined;
- σ is clearly surjective
- $\sigma\left(\sum\limits_{k\in K} a_k t^k + \sum\limits_{\ell\in L} b_\ell t^\ell\right) = \sigma\left(\sum\limits_{s\in K\cup L} (a_s + b_s) t^s\right)$

  $= \sum\limits_{s\in K\cup L} (a_s+b_s)\pi^s = \sum\limits_{k\in K} a_k \pi^k + \sum\limits_{\ell\in L} b_\ell \pi^\ell = \sigma\left(\sum\limits_{k\in K} a_k t^k\right) + \sigma\left(\sum\limits_{\ell\in L} b_\ell t^\ell\right)$

  σ preserves addition.
- $\sigma\left(\sum\limits_{k\in K} a_k t^k \sum\limits_{\ell\in L} b_\ell t^\ell\right) = \sigma\left(\sum\limits_{(k,\ell)\in K\times L} a_k b_\ell t^{k+\ell}\right)$

  $= \sum\limits_{(k,\ell)\in K\times L} a_k b_\ell \pi^{k+\ell} = \sum\limits_{k\in K} a_k \pi^k \sum\limits_{\ell\in L} b_\ell \pi^\ell = \sigma\left(\sum\limits_{k\in K} a_k t^k\right)\sigma\left(\sum\limits_{\ell\in L} b_\ell t^\ell\right)$

  σ preserves multiplication.
- $\sigma(1) = 1$, σ preserves the multiplicative identity.

Hence, the evaluation map σ is a ring isomorphism, $\mathbb{Z}[t] \cong \mathbb{Z}[\pi]$.

But if we take $\mathbb{Z}[1] = \mathbb{Z}$, then $\mathbb{Z}$ is countable but $\mathbb{Z}[t]$ is not countable, so $\mathbb{Z}[t] \ncong \mathbb{Z}[1] = \mathbb{Z}$.

Date / /

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

$r \in LM \Rightarrow$ There exist $l_k \in L$ and $m_k \in M$, such that $r = \sum_{k \in K} l_k m_k$

$\Rightarrow$ There exist $\lambda_k = m_k \in R$ and $l_k \in L$, such that $r = \sum_{k \in K} \lambda_k l_k$

and there exist $\mu_k = l_k \in R$ and $m_k \in M$, such that $r = \sum_{k \in K} \mu_k m_k$

$\Rightarrow r \in \langle L \rangle = L$ and $r \in \langle M \rangle = M \Rightarrow r \in L \cap M$

Take $R = \mathbb{Z}$, $L = M = 2\mathbb{Z}$.

Now $4\mathbb{Z} = LM < L \cap M = 2\mathbb{Z}$.

(b)(i) Proof: Assume that $L + M = R$, it suffice to show $L \cap M \subseteq LM$.

For all $r \in R$, there exist $l \in L$ and $m \in M$, such that $r = l + m$.

$r \in L \cap M \Rightarrow \exists\, l' \in L$ and $m' \in M$; $1 = l' + m'$ and $\exists\, l \in L$ and $m \in M$; $r = l + m$

$\Rightarrow l = r - m \in L \cap M$. and $m = r - l \in L \cap M$

$\Rightarrow \underset{M}{\underset{\Uparrow}{l}}\,\underset{L}{\underset{\Uparrow}{l'}} \in ML$ and $\underset{L}{\underset{\Uparrow}{l}}\,\underset{M}{\underset{\Uparrow}{m'}} \in ML$ and $\underset{M}{\underset{\Uparrow}{m}}\,\underset{L}{\underset{\Uparrow}{l'}} \in ML$ and $\underset{L}{\underset{\Uparrow}{m}}\,\underset{M}{\underset{\Uparrow}{m'}} \in ML$

$\Rightarrow r = 1r = (l' + m')(l + m) = ll' + lm' + ml' + mm' \in ML$.

Hence, $L \cap M \subseteq LM$ in this commutative ring with unity.

(ii) Proof: Assume that $L + M = R$.

For all $a, b \in R$, note that $a - b \in R = L + M$,

so there exist $l \in L$ and $m \in M$, such that $a - b = -l + m$

Hence, $a + l = b + m \in (a + L) \cap (b + M) \neq \phi$

4. Proof: Consider the following map:

$$f: R \to (R/J_1)\times(R/J_2),\ r \mapsto (r+J_1, r+J_2)$$

Step 1: $\forall r, r' \in R$, $f(r+r') = (r+r'+J_1, r+r'+J_2)$
$= (r+J_1, r+J_2) + (r'+J_1, r'+J_2) = f(r)+f(r')$

Hence, f preserves addition.

Step 2: $\forall r, r' \in R$, $f(rr') = (rr'+J_1, rr'+J_2)$
$= (r+J_1, r+J_2)(r'+J_1, r'+J_2) = f(r)f(r')$

Hence, f preserves multiplication.

Step 3: $f(1) = (1+J_1, 1+J_2)$.

Hence, f preserves the multiplicative identity.

Step 4: For all $(r_1+J_1, r_2+J_2) \in (R/J_1)\times(R/J_2)$,
as $J_1+J_2 = R$, $(r_1+J_1)\cap(r_2+J_2) \neq \emptyset$.
Choose $r \in (r_1+J_1)\cap(r_2+J_2)$, so $f(r) = (r+J_1, r+J_2) = (r_1+J_1, r_2+J_2)$

Hence, f is surjective.

Combine the four steps above, we've proven that:

$$(R/J_1)\times(R/J_2) = \mathrm{Im}(f) \cong R/\mathrm{Ker}(f) = R/(J_1\cap J_2),$$

where $\mathrm{Ker}(f) = f^{-1}(J_1, J_2) = J_1\cap J_2$ is obvious.

5 Proof: Take $R = \mathbb{Z}$, $J_1 = 3\mathbb{Z}$, $J_2 = 5\mathbb{Z}$, $J_3 = 7\mathbb{Z}$

$\mathbb{Z}/15\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/5\mathbb{Z})$, where $3\mathbb{Z}+5\mathbb{Z} = \mathbb{Z}$;

$\mathbb{Z}/105\mathbb{Z} \cong (\mathbb{Z}/15\mathbb{Z})\times(\mathbb{Z}/7\mathbb{Z})$, where $15\mathbb{Z}+7\mathbb{Z} = \mathbb{Z}$;

Hence, $\mathbb{Z}/105\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/5\mathbb{Z})\times(\mathbb{Z}/7\mathbb{Z})$

$$2\cdot 35\cdot 35_3^{-1} + 3\cdot 21\cdot 21_5^{-1} + 2\cdot 15\cdot 15_7^{-1} + 105\mathbb{Z} \mapsto (2+3\mathbb{Z}, 3+5\mathbb{Z}, 2+7\mathbb{Z})$$

As it is natural to assume $\#(\text{soldier}) < 105$, $\#(\text{soldier}) = \text{remainder} = 23$