20250213 MATH4302 Assignment 2

(1)

1) Proof: $\phi(I)\subseteq\phi(I)Q \Rightarrow I\subseteq\phi^{-1}(\phi(I)Q)=(I^e)^c$

2) Proof: $\phi(\phi^{-1}(J))\subseteq J \Rightarrow (J^c)^e=\phi(\phi^{-1}(J))Q\subseteq JQ=J$

(2)

1) Proof: It remains to prove $(J^c)^e\supseteq J$

$\underset{\substack{\psi\\ D^{-1}R}}{\ } \ \underset{\substack{\psi\\ J}}{\ }$ because $\phi(r)=d\left(\frac{r}{d}\right)$

For all $\frac{r}{d}\in J$, $\frac{r}{d}=\underset{D^{-1}R}{\left(\frac{1}{d}\right)}\underset{R}{r}=\underset{D^{-1}R}{\left(\frac{1}{d}\right)}\phi(\underset{R}{r})$, where $r\in\phi^{-1}(J)$, $\frac{1}{d}\in Q=D^{-1}R$

Hence, $\frac{r}{d}\in\phi(\phi^{-1}(J))Q=(J^c)^e$, which implies $J=(J^c)^e$

Ideal is closed under scalar multiplication

2) Proof: $I^e=\phi(I)Q=\left\{\left(\frac{r'}{d'}\right)r\in D^{-1}R:\frac{r'}{d'}\in D^{-1}R \text{ and } r\in I\right\}$.

$=\left\{\frac{r}{d}\in D^{-1}R: r\in I \text{ and } d\in D\right\}$.

$(I^e)^c=\phi^{-1}(I^e)=\left\{s\in R: s=\frac{r}{d} \text{ for some } r\in I \text{ and } d\in D\right\}$

$=\{s\in R: ds\in I \text{ for some } d\in D\}$.

Moreover, $I^e=D^{-1}R \Leftrightarrow 1\in D^{-1}R \Leftrightarrow$ Some $\frac{\overset{\in I}{r}}{\underset{\in D}{d}}=1 \Leftrightarrow I\cap D\neq\phi$

3) Proof: We may divide our proof into three parts.

Part 1: Assume that $I$ is a prime ideal of $R$, and $I\cap D=\phi$.

let's prove that $I^e$ is a prime ideal of $D^{-1}R$.

First, as $I\cap D=\phi$, $I^e$ is an proper ideal of $D^{-1}R$.

Second, for all $\frac{\overset{\in I^{\text{complement}}}{r_1}}{\underset{\in D}{d_1}}, \frac{\overset{\in I^{\text{complement}}}{r_2}}{\underset{\in D}{d_2}}\in(I^e)^{\text{complement}}$

as $I$ is prime, $\frac{\overset{\in I^{\text{complement}}}{r_1r_2}}{\underset{\in D}{d_1d_2}}\in(I^e)^{\text{complement}}$

This implies $I^e$ is a prime ideal of $D^{-1}R$.

Part2: Assume that $J$ is a prime ideal of $D^{-1}R$,

let's prove that $J^c$ is a prime ideal of $R$, and $J^c \cap D = \phi$.

First, as $1 \notin J$, $J^c \cap D = \phi$, and certainly $J^c \neq R$ as $D \neq \phi$.

$J$ complement

Second, for all $r_1, r_2 \in (J^c)^{\text{complement}}$, $\phi(r_1 r_2) = \underline{\phi(r_1)}\,\underline{\phi(r_2)} \in (J)^{\text{complement}}$

because $J$ is prime and preimage preserves complement, so $J^c$ is a prime ideal of $R$.

Part3: We prove that contraction and extension are inverses to each other.

First, we've already proven $J = (J^c)^e$ for all ideal $J$ of $D^{-1}R$.

Second, for all prime ideal $I$ of $R$ with $I \cap D = \phi$:

$(I^e)^c = \{r \in R : dr \in I \text{ for some } d \in D\}$

as $I$ is prime   as $D \cap I = \phi$, $d \notin I$

$= \{r \in R : d \in I \text{ or } r \in I\} = I$

Hence, contraction and extension are inverses to each other.

Above all, contraction and extension give a bijection between prime ideals $I$ of $R$ such that $I \cap D = \phi$ and prime ideals $J$ of $D^{-1}R$.

(3) Define $R = \mathbb{C}[x,y]$, and we would like to prove that $\mathbb{C}[x,y,z]/\langle z-2 \rangle$

$= R[z]/\langle z-2 \rangle \cong R$, and then, as $\mathbb{C}$ is a unique factorization domain,

so do $R = \mathbb{C}[x,y]$ and the ring $\mathbb{C}[x,y,z]/\langle z-2 \rangle$ isomorphic to it.

Define a map $\sigma: R[z] \to R$, $f(z) \mapsto f(2)$. This is a surjective ring homomorphism, and $\mathrm{Ker}(\sigma)$ = All $f(z)$ that vanishes at $z=2$ = All multiples of $z-2$ = $\langle z-2 \rangle$, so it follows from the first isomorphism theorem that $R[z]/\langle z-2 \rangle \cong R$

(4) Proof: Assume that $a, b$ are nonzero, nonunit elements of $R$, we wish to show that $\langle a\rangle \cap \langle b\rangle$ has a generator.

To do so, factorize $a, b$ as irreducibles respectively:

$$a = r_1^{\alpha_1} r_2^{\alpha_2} \cdots r_n^{\alpha_n}, \quad b = r_1^{\beta_1} r_2^{\beta_2} \cdots r_n^{\beta_n}$$

Define the following element:

$$c = r_1^{\max\{\alpha_1,\beta_1\}} r_2^{\max\{\alpha_2,\beta_2\}} \cdots r_n^{\max\{\alpha_n,\beta_n\}}$$

On one hand, $a, b$ are divisible by $c$, so $\langle a\rangle, \langle b\rangle \subseteq \langle c\rangle$, $\langle a\rangle \cap \langle b\rangle \subseteq \langle c\rangle$

On the other hand, for all nonzero, nonunit element $d \in \langle a\rangle \cap \langle b\rangle$, factorize it:

$$d = r_1^{\sigma_1} r_2^{\sigma_2} \cdots r_n^{\sigma_n} r_{n+1}^{\sigma_{n+1}} \cdots r_m^{\sigma_m}$$

As $d \in \langle a\rangle, \langle b\rangle$, $d$ is divisible by $a, b$, so $\sigma_1 \geq \max\{\alpha_1,\beta_1\}$, $\sigma_2 \geq \max\{\alpha_2,\beta_2\}$, $\dots$, $\sigma_n \geq \max\{\alpha_n,\beta_n\}$, which implies $d$ is divisible by $c$. Hence, $\langle a\rangle \cap \langle b\rangle = \langle c\rangle$

(5) 1) As $\mathbb{Q}[x]$ is an Euclidean domain, it is an integral domain.

As $R = \mathbb{Z} + x\mathbb{Q}[x]$ is a subring of $\mathbb{Q}[x]$, it is an integral domain.

2) Assume that $r$ is an irreducible element of $R$.

Case 1: If $\mathrm{Deg}(r) < 1$, then $r$ is not a unit implies $r \neq \pm 1$, and $\langle r\rangle^c$ is closed under multiplication implies $r$ has no nontrivial proper factor.

Hence, $r = \pm p$, where $p$ is a prime number.

Case 2: If $\mathrm{Deg}(r) \geq 1$, then and prime number $p$ fails to divide $r$, which implies the constant term of $r$ is $\pm 1$; As $\pm 1 + xf(x) = \underbrace{(r + xg(x))\left(\frac{\pm 1}{r} + xh(x)\right)}_{\text{reducible in } \mathbb{Q}[x]}$ implies $\pm 1 + xf(x) = \underbrace{(1 + xg(x))(\pm 1 + xh(x))}_{\text{reducible in } \mathbb{Z}+x\mathbb{Q}[x]}$, $r = \pm 1 + xf(x)$ is irreducible in $\mathbb{Q}[x]$.

3) The polynomial $x \in \mathbb{Z} + x\mathbb{Q}[x]$ has infinitely many nontrivial proper factors $p$, where $p$ is a prime number. Hence, the ascending chain criterion for principal ideals fails:

$$\underset{\substack{\text{first order}\\ \text{coefficient } \mathbb{Z}}}{\langle x \rangle} \subsetneq \underset{\substack{\text{first order}\\ \text{coefficient } \frac{\mathbb{Z}}{2}}}{\langle \tfrac{x}{2} \rangle} \subsetneq \underset{\substack{\text{first order}\\ \text{coefficient } \frac{\mathbb{Z}}{4}}}{\langle \tfrac{x}{4} \rangle} \subsetneq \cdots$$

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

Part 1: Assume that $f(x) = \sum_{i=0}^{n} f_i x^i \in R[x] \setminus \{0\}$

As $R$ is a unique factorization domain, $f_0, f_1, \cdots, f_n$ has a greatest common divisor $r$, which implies $f(x)$ can be decomposed as $r g(x)$ where $g(x) = \frac{f(x)}{r}$.

Part 2: Assume that $f(x) = r g(x) = \bar{r} \bar{g}(x)$, where $r, \bar{r}$ are greatest common divisors of $f_0, f_1, \cdots, f_n$. As $R$ is a unique factorization domain, $r, \tilde{r}$ are associated, so $g(x), \bar{g}(x)$ are associated.

(7) Proof: $0 \neq f(x) = \sum_{i=0}^{n} f_i x^i = \sum_{i=0}^{n} \frac{r_i}{s_i} x^i = \frac{\sum_{i=0}^{n} r_i \prod_{j \neq i} s_j x^i}{\prod_{j=0}^{n} s_j} = \overset{\in F}{\boxed{\frac{\text{content}}{\prod_{j=0}^{n} s_j}}} \overset{\in R[x]}{\text{primitive part}}$

$0 \neq f(x) = \frac{s}{t} \overset{\text{primitive}}{\sum_{i=0}^{n} r_i x^i} = \frac{\bar{s}}{\bar{t}} \overset{\text{primitive}}{\sum_{i=0}^{n} \bar{r}_i x^i} \Rightarrow \overset{\text{content}}{\underline{s\bar{t}}} \sum_{i=0}^{n} r_i x^i = \overset{\text{content}}{\underline{\bar{s}t}} \sum_{i=0}^{n} \bar{r}_i x^i \neq 0.$

Hence, $s\bar{t}, \bar{s}t$ are associated, which means $\exists u \in R^{\times}$, $\frac{s}{t} = \frac{\bar{s}}{\bar{t}} u$

(8) Proof: Treat this polynomial as an element in $R[y]$, where $R = \mathbb{R}[x]$, $x, x^2+1$ are coprime

so it suffices to show that this polynomial of degree 3 has no root in $R$.

As the evaluation of $xy^3 + x^2y^2 - x^5y + x^2 + 1$ at any $y = y_0(x)$ always has a nonzero constant term 1, this evaluation gives a nonzero element of $R = \mathbb{R}[x]$, and we've proven that $f(x,y) = xy^3 + x^2y^2 - x^5y + x^2 + 1$ is irreducible.

(9) Proof: As $|1+i|^2 = 2$ is prime in $\mathbb{Z}$, $1+i$ is prime in $\mathbb{Z}[i]$

Define $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[i]$, where:

$a_3 = 1$, $\frac{a_3}{1+i} = \frac{1-i}{2} \notin \mathbb{Z}[i]$, $1+i \nmid a_3$

$a_2 = -6$, $\frac{a_2}{1+i} = -3+3i \in \mathbb{Z}[i]$, $1+i \mid a_2$

$a_1 = 4i$, $\frac{a_1}{1+i} = 2+2i \in \mathbb{Z}[i]$, $1+i \mid a_1$

$a_0 = 1+3i$, $\frac{a_0}{1+i} = 2+i \in \mathbb{Z}[i]$, $1+i \mid a_0$

$\frac{a_0}{(1+i)^2} = \frac{3-i}{2} \notin \mathbb{Z}[i]$, $(1+i)^2 \nmid a_0$.

This implies $f(x)$ is irreducible over the Euclid domain $\mathbb{Z}[i]$

(10) (a) 3 is prime in $\mathbb{Z}$, and define $f(x) = 2x^9 + 12x^4 + 36x^3 + 27x + 6$.

As $3 \nmid 2$, $3 \mid 12$, $3 \mid 36$, $3 \mid 27$, (certainly $3 \mid 0$), $3 \mid 6$, $3^2 \nmid 6$,

$f(x)$ is irreducible over $\mathbb{Z}$, thus irreducible over $\mathbb{Q} = \mathrm{Frac}\,\mathbb{Z}$.

(b) Assume to the contrary that $f(x) = x^4 + 25x + 7$ is reducible over $\mathbb{Q}$,

which implies $f(x)$ has a proper factorization over $\mathbb{Z}$.

Step 1: We prove that $f(x)$ has no factor $qx - p$, where $q \neq 0$, $(p,q) = 1$

- If $f(x)$ has a factor $qx-p$ $(q \neq 0, (p,q)=1)$, then $f(\frac{p}{q}) = \frac{p^4 + 25pq^3 + 7q^4}{q^4} = 0$,

so $p^4 + 25pq^3 + 7q^4 = 0$ is divisible by $p$ and $q$, where $q \neq 0$, $(p,q) = 1$.

This gives $q \mid 1$ and $p \mid 7$, so $\frac{p}{q} \in \{\pm 1, \pm 7\}$, but:

| $x$ | $x^4+25x+7$ |
|---|---|
| 1 | 33 |
| $-1$ | $-17$ |
| 7 | 2583 |
| $-7$ | 2233 |

Hence, $f(x)$ has no factor $qx-p$, where $q \neq 0$, $(p,q) = 1$.

Step2: We prove that $f(x)$ has no factor $ax^2+bx+c$, where $a\neq 0$.

If $f(x)$ factors into $(a_1x^2+b_1x+c_1)(a_2x^2+b_2x+c_2)=x^4+25x+7$,

then we may assume WLOG that $a_1=a_2=1$.

Consider the third order term, we obtain $0=a_1b_2+a_2b_1=b_1+b_2$, so $b_2=-b_1$.

Consider the second order term, we obtain $0=a_1c_2+b_1b_2+a_2c_1=c_1+c_2-b_1^2$

Consider the constant term, we obtain $c_1c_2=7$ (prime), so:

$\{c_1,c_2\}\in\{\{1,7\},\{-1,-7\}\}$, $c_1+c_2=\pm 8$ is not a perfect square $b_1^2$

Hence, $f(x)$ has no factor $ax^2+bx+c$, where $a\neq 0$, so we obtain a contradiction, where $f(x)$ should but doesn't have a proper factorization over $\mathbb{Z}$.

(c) Similar to what we've done before:

The monic polynomial $f(x)=\prod_{k=1}^{n}(x-k)+1$ is reducible over $\mathbb{Q}$

$\Rightarrow$ $f(x)$ have an integal root, but $f(l)=0+1=1\neq 0$ when $k\leq l\leq n$,

and $|f(l)+1|\geq|f(l)|-1\geq n!-1>0$ when $k<l$ or $l>n$, contradiction!

Date / /