April22

Thursday, April 22, 2021 5:28 PM

TH3 Releases Tomorrow Due Monday.

Error HW #2(c)

$R \leq S$ a subring. and $1_R = 1_S$

Then $R^\times \leq S^\times$

Proof

$a \in R^\times$. $\exists\, b \in R$ s.t.

$$ab = ba = 1_R = 1_S$$

✓

Example

$$\mathbb{Z} \simeq \underset{R}{\underset{\shortparallel}{\mathbb{Z} \times \{0\}}} \leq \underset{S}{\underset{\shortparallel}{\mathbb{Z} \times \mathbb{Z}}}$$

$1_R = (1,0) \longleftarrow$ not even a unit in S bc it's a 0-divisor

$1_S = (1,1)$

$(1,0) \cdot (0,1) = (0,0)$.

Rmk: Many authors require

1) All rings unital
2) $R \leq S$ then $1_S \in R$. subring
3) $\phi : R \longrightarrow S$ then $\phi(1_R) = 1_S$.

Rmk On TH3 all rings will be unital!!

Recall

Def^{n} If R a ring. $S \subseteq R$ is a good multiplicative subset if

1) nonempty
2) Contains no zero divisors
3) Closed under $\times$.

Theorem

R is a commutative ring. $S \subseteq R$ a good multiplicative subset. The $\exists$ a commutative unital ring $Q = S^{-1}R$ s.t.

1) $R \subseteq Q$ is a subring.
2) $\forall\ s \in S \subseteq R \subseteq Q$, $s \in Q^{\times}$.
3) $\forall$ elts of Q are $\underset{\frac{r}{s}}{rs^{-1}}$, $r \in R$, $s \in S$

Furthermore, Q is the smallest ring satisfying 1) & 2).

$$\begin{tikzcd} R \arrow[r, hook, "\phi"] \arrow[d, phantom, sloped, "\subseteq"] & Q' \\ Q \arrow[ur, dashed, "\exists!\Phi"'] & \end{tikzcd}$$

ϕ inj ring hom w/ $\phi(s) \in Q'^{\times}$ $\forall\ s \in S$

Then $\exists!$ injective ring hom Φ w/ $\Phi|_R = \phi$.

Remark R unital, one can weaken S being a good mult subset to S being a mult subset

1) $1 \in S$
2) Closed under ×.

} maybe contains 0 divisors.

Then $R \longrightarrow S^{-1}R$ not necessarily injective.

Studied on TH3

Proof

① $Q = \{ \frac{a}{b},\ a \in R,\ b \in S \}$ w/

$$\frac{a}{b} = \frac{a'}{b'} \iff ab = a'b'$$

Proved well defined last time.

} If S contains 0 divisors adjust equiv relation.

② Make Q into a commutative unital ring. ✓

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

i) +, × well defined ←
ii) (Q, +) ab group.
iii) × associative & distributive.
iv) Q has identity
v) Q commutative.

③ Construct injective ring map ①

$$R \longrightarrow Q.$$

④ $s \in S \subseteq R \subseteq Q$ then $s \in Q^{\times}$ ←

⑤ $\forall\ q \in Q$, $q = rs^{-1}$ $r \in R$, $s \in S$.

⑥ Q is smallest such ring.

---

②i) + well defined.

$\frac{a}{b} = \frac{\tilde a}{\tilde b}$ & $\frac{c}{d} = \frac{\tilde c}{\tilde d}$ $c\tilde d = \tilde c d$

$a\tilde b = \tilde a b$

Show $\frac{a}{b} + \frac{c}{d} \overset{?}{=} \frac{\tilde a}{\tilde b} + \frac{\tilde c}{\tilde d}$

do this again on TH3 b/c new equiv reln when S contains 0 divs

$$\frac{ad+bc}{bd} \overset{?}{=} \frac{\tilde a \tilde d + \tilde b \tilde c}{\tilde b \tilde d}$$

$$(ad+bc)\tilde b \tilde d \overset{?}{=} (\tilde a \tilde d + \tilde b \tilde c)bd$$

$$\underline{a\tilde b}\,\underline{d\tilde d} + \underline{b\tilde b}\,\underline{c\tilde d} \underset{!!}{\overset{?}{=}} \underline{\tilde a b}\,\underline{d\tilde d} + \underline{b\tilde b}\,\underline{\tilde c d}$$

well defined ☺

× well defined easier.

---

②(ii) $(Q,+)$ ab group.

$\frac{0}{d}$ $d \in S$ is + identity (prove)

$-\left(\frac{a}{b}\right) = \frac{-a}{b}$ $b \in S$ (prove).

---

②(iv)

Want any $\underline{s \in S}$, $\frac{s}{\underline{s}} = 1_Q$

$\frac{sa}{sb} = \frac{s}{s} \cdot \frac{a}{b} \overset{!}{=} \frac{a}{b} \xrightarrow{\times \text{ mult}} sab = sba$ ✓

Have a multiplicative identity.

② v. Commutativity is easy.

---

③ $R \xrightarrow{i} Q \leftarrow$

$r \longmapsto \cancel{\frac{r}{1}}$ $\frac{rd}{d}$ any $d \in S$.

is $1 \in R$

$\underline{1} \in S$?

Check $\frac{rd}{d} = \frac{re}{e}$ for other $e \in S$.

✓ ok

Check ring hom directly.

Injectivity

$i(r) = 0 \iff \frac{rd}{d} = \frac{0}{d}$

$\iff rd^2 = 0$

d not 0 divisor.

$\implies r = 0$

so $\ker i = 0$ & i injects!

④ $\underline{s \in S}$. show $\underline{i(s) \in Q^\times}$

$\quad \| $

$\frac{sd}{d}$.

$$\frac{sd}{d} \cdot \frac{d}{ds} = \frac{sdd}{dds} \overset{!}{=} \frac{d}{d}$$

cross

$sd^3 = d^3 s$

✓

$\uparrow = 1_Q$

$\uparrow$

$d, s \in S$

so $ds \in S$ b/c mult closed.

⑤ $\frac{r}{s} = r \cdot s^{-1}$

✓

~~pf~~

$s^{-1} = \frac{d}{ds}$

$$\frac{rd}{d} \cdot \frac{d}{ds} \overset{\times}{=} \frac{r}{s}$$

$rd^2 s = d^2 s r$.

$ⓡ = \frac{rd}{d}$

Easier on TH b/c $1 \in S$.

⑥

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "i"] & Q' \\ Q \arrow[ur, dashed, "\exists ! \Phi"'] & \end{tikzcd}$$

s.t. $\phi(s) \in Q'^{\times}$ $\forall s \in S$

By ⑤ $z = rs^{-1}$

$\Phi(z) = \Phi(rs^{-1})$

$= \Phi(r)\Phi(s)^{-1}$

$\boxed{= \phi(r)\phi(s)^{-1}}$

← uniquenss.

Well defined

$rs^{-1} = \tilde{r}\tilde{s}^{-1} \iff r\tilde{s} = \tilde{r}s$

$\implies \phi(r)\phi(\tilde{s}) = \phi(\tilde{r})\phi(s)$

$\implies \phi(r)\phi(s)^{-1} = \phi(\tilde{r})\phi(\tilde{s})^{-1}$

so well defined.

Check it's a homomorphism. ✓

Injectivity

$z = rs^{-1} \in \ker \Phi$

$\phi(r)\underbrace{\phi(s)^{-1}}_{\text{a unit}} = 0$ in Q'

$\implies$ not 0-divisor

$\Longrightarrow \phi(r)=0 \quad \Longrightarrow r=0 \Longrightarrow z=0$

$\{$ ϕ injects

so $\ker \Phi = 0$.

Defⁿ/Prop

Let R be an integral domain. $(1 \neq 0)$

$S = R \setminus \{0\}$. Then S a good multiplicative subset. ①

$S^{-1}R$ is called the field of fractions ② of R.

Often write $\mathrm{Fract}(R)$ or $K(R)$.

Proof

① S contains no 0 divisors.

$S \neq \emptyset$ bc $1 \in S$

$a, b \in S \Longrightarrow ab \neq 0$ so $ab \in S$.

② $\frac{a}{b} \in S^{-1}R$. $b \neq 0$.

Show every nonzero elt of $S^{-1}R$ has an inverse.

if $\frac{a}{b} \neq 0 \Longrightarrow a \neq 0$

$\frac{b}{a} \in S^{-1}R$.

& $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = 1_{S^{-1}R}$.

Corollary

Let R be a ring. R is an integral domain $\iff$ it is a subring of a field.

Examples

- $\text{Fract}(\mathbb{Z}) = \mathbb{Q}$.
- $\text{Fract}(\mathbb{Z}[\sqrt{D}]) = \mathbb{Q}(\sqrt{D})$ ✓

Pf/ 1) $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{Q}(\sqrt{D}) \leftarrow$ a field

$\implies \text{Fract}(\mathbb{Z}[\sqrt{D}]) \subseteq \mathbb{Q}(\sqrt{D})$

$\uparrow$ smallest one.

given $\frac{a}{b} + \frac{c}{d}\sqrt{D} \in \mathbb{Q}(\sqrt{D})$

$$\frac{a}{b} + \frac{c}{d}\sqrt{D} = \frac{ad + bc\sqrt{D}}{bd} \in \text{Fract}(\mathbb{Z}[\sqrt{D}])$$

So $\mathbb{Q}(\sqrt{D}) \subseteq \text{Fract}(\mathbb{Z}[\sqrt{D}])$

- $\text{Fract}(2\mathbb{Z}) = \mathbb{Q}$

  Identity appears as $\frac{2}{2}$.

- R an integral domain.

  Then so is $R[x]$.

$$\operatorname{Fract}(R[x]) = \left\{ \frac{p(x)}{q(x)} : q, p \in R[x], \quad q \neq 0 \right\}.$$

Let $F = \operatorname{Fract}(R)$.

Then $F \subseteq \operatorname{Fract}(R[x])$

$$\frac{a}{b} \longmapsto \frac{a}{b}$$

Therefore $F[x] \subseteq \operatorname{Fract}(R[x])$

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d] & R[x] \arrow[d] \arrow[dl] \\
F[x] \arrow[r, hook] \arrow[r, dashed, bend right] \arrow[dr, hook, bend right] \arrow[dr, dashed] & \operatorname{Fract} R[x] \arrow[d, bend left] \\
& \operatorname{Fract}(F[x]) \arrow[u] \arrow[u, bend left]
\end{tikzcd}$$

$\rightsquigarrow \operatorname{Fract} R[x] = \operatorname{Fract} F[x]$

Def^n F a field then

$$F(X) := \operatorname{Fract}(F[x])$$
$$= \text{field of rational functions.}$$

- $R = \mathbb{Z}$ $\quad F = \mathbb{Q}$.

$$\mathrm{Fract}(\mathbb{Z}[x]) \underset{\textcircled{?}}{=} \mathbb{Q}(x)$$

$$\frac{p(x)}{q(x)} \in \mathbb{Q}(x)$$

polys w/ $\mathbb{Q}$ coeffs. $\exists\, N$

s.t. $Np(x) \in \mathbb{Z}[x]$

$Nq(x) \in$

$$\frac{p(x)}{q(x)} = \frac{Np(x)}{Nq(x)} \in \mathrm{Fract}(\mathbb{Z}[x]).$$

- R commutative w/ 1. $d \in R$ nonzero divisor.

$S = \{1, d, d^2, d^3, \ldots\}$ is a good mult subset.

$R[1/d] = S^{-1}R$. "formally invert d"

$\mathbb{Z}[1/2]$ = fractions whose denominators are powers of 2.

Sun Tzu's Theorem

A number is

2 more than a mult of 3 $\equiv 2 \bmod 3$

3 more than a mult of 5 $\equiv 3 \mod 5$

2 more than a mult of 7. $\equiv 2 \mod 7$

Does such a number exist?

Bc 3, 5, 7 coprime, yes

$x = 23$

x unique   (mod $105 = 3 \cdot 5 \cdot 7$).

$$\mathbb{Z}/105\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$$

$$23 \longleftrightarrow (2, 3, 2).$$

This generalizes to a ring theoretic statement.

HW 4 #5 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$

if $\gcd(m,n) = 1$.

↑ uses prime factorization & ring theory/arithmetic of $\mathbb{Z}$.

Extend these notions to rings. (in language of ideals).

$$\gcd(n,m) = 1 \Longleftrightarrow \exists\, u, v \text{ s.t. } nu + mv = 1$$

HW 11 $\Longleftrightarrow n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}.$

Def^n R be a commutative ring w/ $1 \neq 0$.

Let $I, J \subseteq R$ be ideals.

I & J are comaximal if

$$I + J = R$$

Def^n R, S 2 rings. Their direct product is

$$R \times S = \{ (r, s) \mid r \in R, \ s \in S \}$$

w/
$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2).$$

Exercise $R \times S$ a ring.

If R, S unital $\Longrightarrow$ $R \times S$ is

comm $\Longrightarrow$ " " "

Sun Tzu's Theorem

R commutative w/ $1 \neq 0$.

$A_1, A_2, \ldots, A_k \subseteq R$ ideals.

Consider
$$\phi : R \longrightarrow \frac{R}{\underline{A_1}} \times \frac{R}{\underline{A_2}} \times \cdots \times \frac{R}{\underline{A_k}}$$
$$r \longmapsto (r \bmod A_1, r \bmod A_2, \ldots, r \bmod A_k)$$
$$" = (\bar{r}, \bar{r}, \bar{r}, \ldots, \bar{r})$$

Then

① ϕ is a ring hom.

② $\ker\phi$ is $A_1 \cap A_2 \cap \cdots \cap A_k$

③ If A_i, A_j comaximal $\forall\, i \neq j$

then ϕ is surjective &

$A_1 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$.

So $\dfrac{R}{A_1 \cdots A_k} \simeq \dfrac{R}{A_1} \times \cdots \times \dfrac{R}{A_k}$

Proof

① $\phi(r * s) = (\overline{r*s}, \ldots, \overline{r*s})$ $\quad * = +$ or $\times$.

$= (\bar{r}, \ldots, \bar{r}) * (\bar{s}, \ldots, \bar{s})$

$= \phi(r) * \phi(s)$ $\quad$ ✓

② $r \in \ker\phi \iff r \equiv 0 \mod A_i \quad \forall i$

$\iff r \in A_1 \cap \cdots \cap A_k$

③ Induction

Base Case $k = 2$. $\quad \boxed{A_1 + A_2 = R}$

$R \longrightarrow \dfrac{R}{A_1} \times \dfrac{R}{A_2}$ $\quad$ surj by HW6 #1

$A_1 \cap A_2 = A_1 A_2$ $\quad$ by HW11 #4(d)

General Case

Let $A = A_1$ $\quad B = A_2 \cdots A_k$.

If $\boxed{A + B = R} \Longrightarrow$ base case + ind

$$\frac{R}{AB} = \frac{R}{A} \times \frac{R}{B} \underset{\uparrow\,\text{ind}}{=} \frac{R}{A_1} \times \cdots \times \frac{R}{A_k}$$

A_1, A_j are comax $\forall\, j = 2, \dots, k$.

So $\exists\, x_j \in A_1$, $y_j \in A_j$ w/ $x_j + y_j = 1$.

So $(x_2 + y_2) \cdots (x_n + y_n) = 1$

Reduce mod A_1 $\quad (x_i \in A_1)$

$$(x_2 + y_2) \cdots (x_n + y_n) \equiv y_2 \cdots y_n \quad \underline{\text{mod } A_1}$$

So $1 = (x_2 + y_2) \cdots (x_n + y_n) = \underset{A_1}{\underset{\in}{a_1}} + \underset{A_2 A_3 \cdots A_n = B}{\underset{\in}{y_2 \cdots y_n}}$

So $A + B \ni 1$ so $A + B = R$ $\emptyset$

Remains: Study nice integral domains.

Saw we can generalize gcds to an ideal theoretic context.

Finish

How to generalize nice properties of $\mathbb{Z}$ to other rings.

Euclidean Domains ⟵ division algorithm.

Principle Ideal Domains $\leftsquigarrow$ All ideals generated by 1 elt.

Unique Factorization

Euclidean Domains

(R = integral domain).

Want long division

$\forall\ a, b \in R$ w/ $b \neq 0$. want $q, r \in R$ s.t.

i) $a = bq + r$

2) $r = 0$ or $\boxed{r < b}$

↑ what does this mean

Do it abstractly

↙

Def^n A function $N: R \longrightarrow \mathbb{Z}_+ \cup \{0\}$ w/ $N(0) = 0$ is called a norm.

Def^n

An integral domain R is called a Euclitean domain if $\exists$ a norm on R s.t. all $a, b \in R$, w/ $b \neq 0$, $\exists$ $q, r \in R$ s.t.

1) $a = qb + r$

2) $r = 0$ or $N(r) < N(b)$.

Prop/ Let R be a Euclidean Domain. Then ideal of R is principle.

Pf/ $I = (0)$ nothing to prove.

Else fix $N : R \longrightarrow \mathbb{Z}_+ \cup \{0\}$ a Euclidean Norm. Let $d \in I$, have minimal norm in I

$$(d) \underline{\underline{\subseteq}} I.$$

Conversely, let $i \underline{\underline{\in}} I$, By long division

$i = dq + r$ for $\underset{*}{\underline{r=0}}$ or $\underline{N(r) < N(d)}$

$r = 0 \Rightarrow i = dq \in (d)$ we win

---

else $N(r) < N(d)$

But $r = i - dq \in I$ ↯

bc d minimal norm.