April27

Tuesday, April 27, 2021 12:34 PM

Extend properties from $\mathbb{Z}$ to more rings.

Example

Analogy between $\mathbb{Z}$ & $F[x]$

↑ F a field.

Today R - integral domain.

↑ commutative
unital
only zero divisor is 0.

First Goal: Long Division. ← remainder must be smaller. So need a notion of size.

Def^n

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

Def^n A Euclidean Domain is an integral domain R s.t. $\exists$ a norm on R and any $a, b \in R$ w/ $b \neq 0$, $\underbrace{\exists\, q, r \in R}_{\text{not unique in general.}}$ s.t.

1) $a = bq + r$

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

Rmk This is a very strong condition, as the following prop shows.

Prop

Let R be a Euclidean Domain. Then every ideal of R is principal. $I = (0)$ ✓

Proof $N : R \longrightarrow \mathbb{Z}_{\geq 0}$. I an $_{\wedge}$ ideal.
nonzero.

$d \in I$ $\overset{\text{nonzero}}{\text{s.t.}}$ $\forall\ e \in I,\ N(d) \leq N(e)$.

We will show $I = (d)$.

Fix $i \in I$. Do long division

$i = bd + r$ w/ $\underset{①}{r = 0}$ or $\underset{②}{N(r) < N(d)}$

① $\Rightarrow i = bd \Rightarrow i \in (d)$

② $r = i - bd \in I$ & $\underline{N(r) < N(d)}$ ↯

Must be in case ① & $I \subseteq (d)$. ✓ $\varnothing$

Examples

① Fields are Euclidean domains.

$N : F \longrightarrow \mathbb{Z}_{\geq 0}$

$N(a) = 0$.

Divide a by b, $b \neq 0$. $a = qb + 0$

$(q = ab^{-1})$.

② $\mathbb{Z}$ is a Euclidean w/ standard long division

③ Important

Prop

F a field. Then $F[x]$ is a Euclidean domain.

Proof

1) Need a norm.

$$N : F[x] \longrightarrow \mathbb{Z}_{\geq 0}$$

$$N(f(x)) = \deg(f(x))$$

2) Want long division of $f(x)$ by $g(x) \neq 0$

Proceed by induction on $n = \deg(f(x))$

Case 0 $f(x) = 0$. $q = r = 0$

$$f = gq + r.$$

General Case Let $m = \deg g(x)$.

i) If $m > n$. $\leftarrow$

$\rightsquigarrow q(x) = 0 \quad r(x) = f(x)$

$\rightsquigarrow$ i) $f(x) = g(x)q(x) + r(x)$

ii) $\deg(r(x)) = n < m$

ii) $m \leq n$.

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

Let $\hat{f}(x) = \underline{f(x)} - \underline{\frac{a_n}{b_m} g(x) x^{n-m}}$ (uses that F a field)

$\Longrightarrow \deg \hat{f}(x) < \deg f(x).$

Induction:

$$\hat{f}(x) = \hat{q}(x) \cdot g(x) + r(x)$$

either
$r(x) = 0$
or
$\deg r(x) < \deg g(x).$

Define $q(x) = \hat{q}(x) + \frac{a_n}{b_m} x^{n-m}$

$$\Longrightarrow f(x) = q(x) \cdot g(x) + r(x).$$

$$\underline{\hat{f}(x)} + \boxed{\frac{a_n}{b_m} g(x) x^{n-m}} \qquad \left(\hat{q}(x) + \frac{a_n}{b_m} x^{n-m}\right) g(x) + r(x)$$

$$\parallel$$

$$\underline{\hat{q}(x) g(x) + r(x)} + \boxed{\frac{a_n}{b_m} x^{n-m} g(x)}$$

$\varnothing$

Exercise q, r unique for $F[x]$.

Corollary Every ideal in $F[x]$ is principal.

Examples: Quadratic Integer Rings.

$\mathcal{O} = \mathbb{Z}[\sqrt{D}]$

$$N: \mathcal{O} \longrightarrow \mathbb{Z}_{\geq 0}$$

$$a+b\sqrt{D} \longmapsto \left|(a+b\sqrt{D})(a-b\sqrt{D})\right|$$

$$\|$$

$$|a-b^2D| \geq 0.$$

Question Does this make $\mathcal{O}$ into a Euclidean Domain?

A. Not in general.
Yes if $D=-1$.

Prop $\mathbb{Z}[i]$ is a Euclidean Domain.

Proof $N(a+bi) = a^2+b^2$

$$\beta^{-1} = \frac{c-di}{c^2+d^2}$$

$\alpha = a+bi$
$\beta = c+di$ $\rightsquigarrow$ in $\mathbb{Q}(i)$ $\quad \dfrac{\alpha}{\beta} = r+si$

Check.

$r = \dfrac{ac+bd}{c^2+d^2}$, $\quad s = \dfrac{bc-ad}{c^2+d^2}$

$p =$ int closest to r.

$q =$ int closest to s.

$$\alpha = \underline{(p+qi)}\beta + \gamma \leftarrow$$

$$\boxed{\theta = \frac{\alpha}{\beta} - (p+qi)}$$

difference b/w quotient in $\mathbb{Q}(i)$ & approximation.

$$\rightsquigarrow \alpha = (p+qi)\beta + \beta\theta$$

$$\theta = \underbrace{(r-p)}_{\substack{\leq 1/2 \\ \text{abs value}}} + \underbrace{(s-q)}_{\substack{\leq 1/2 \\ \text{abs value.}}} i \rightarrow N(\theta) \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2}$$

$$\longrightarrow N(\gamma) = N(\beta\theta) = N(\beta)N(\theta) \leq \frac{1}{2}N(\beta) < \underline{N(\beta)}$$

Corollary

Every ideal in $\mathbb{Z}[i]$ is principal.

Nonexamples

① $\mathbb{Z}[x]$ not a Euc. Domain.

bc $(2, x)$ not principal!!

② $\mathbb{Z}[\sqrt{-5}]$ not a Euc. Domain.

$I = (3, 2+\sqrt{-5})$

Exercise I not principal.

Greatest Common Divisors

Def^n

R a commutative ring w/ 1, $b \neq 0$.

a) a is a multiple of b if $\exists\ x \in R$ s.t. $a = xb$.

Also say b divides a $\quad b \mid a$

b) A greatest common divisor of $\overset{\text{nonzero}}{\vee}$ a & b is a $d \in R$ s.t.

1) $d \mid a$ & $d \mid b$

2) If $d' \mid a$ & $d' \mid b$.
$\implies d' \mid d$.

Rmks

1) These don't always exist.
2) If F a field, $a, b \neq 0$. Then any $d \in F$ is a gcd of a & b.

Translate into Ideal language

Fact

$$b \mid a \iff a \in (b) \iff (a) \subseteq (b)$$

Slogan

In rings divisibility $\iff$ Containment of ideals.

Let $I = (a, b)$.

Let d a coman divisor of a & b.

$(a) \subseteq (d)$, & $(b) \subseteq (d)$

$\Longleftrightarrow$ $I = (a,b) \subseteq (d)$.

We have therefor proved

Prop (Ideal theoretic def of gcd)
d is a gcd of a & b if & only if

i) $(a,b) \subseteq (d)$

ii) If $(a,b) \subseteq (d')$ $\Longrightarrow$ $(d) \subseteq (d')$.

i.e.
The ideal generated by d is the smallest principal ideal containing (a,b).
The ideal is therefore unique (if it exists).

Corollary $(*)$
If $a,b \in R$ & $(a,b) = (d)$, then
d is a gcd for a & b.

Corollary (Uniqueness of GCDs in integral Domains) $(*)$
R an integral domain.
Let d, d' be gcds of a, b. Then
$d' = ud$ for some $u \in R^\times$.

Proof

$(d) = (d')$. So done by

$\varnothing$

HW 11 5(b)

Corollary (*)

In Euclidean Domains, GCDs exist.

Proof

(a,b) is principal so $(a,b) = (d)$

so d a GCD. $\varnothing$

Theorem In Euc. Domains, GCDs can be computed algorithmically.

$a, b \in R$. $a, b \neq 0$. Run long div.

(0) $a = q_0 b + \underline{\underline{r_0}}$

(1) $\underline{b} = q_1 \underline{r_0} + r_1$

$\vdots$

(n-1) $r_{n-2} = q_n \underline{\underline{r_{n-1}}} + \underline{\underline{r_n}}$

(n) $r_{n-1} = q_{n+1} r_n$

$N(r_0) < N(b)$

$\vee$

$N(r_1)$

$\vee$

$N(r_2)$ until $r_n = 0$.

$\vee$

$\vdots$

decreasing sequence of ints.

Then 1) r_n a gcd of (a,b)

2) $(r_n) = (a,b)$.

Pf/ a) $\supseteq$ $r_n | a$ & $r_n | b$.

(n) $\Rightarrow r_n | r_{n-1}$

$(n-1) \longrightarrow r_n \mid r_{n-2}$

$\vdots$

$r_n \mid b$ & $r_n \mid a$. ✓

b) $\subseteq$

$(0)\quad r_0 \in (a,b)$

$(1)\quad r_1 \in (r_0, b) \subseteq (a,b)$

$\vdots$

$(n)\quad r_n \subseteq (r_{n-1}, r_{n-2}) \subseteq \dots \subseteq (a,b)$

The most useful theoretical peice of being a E.D. is all ideals being principal.

Principal Ideal Domains

Defn

An integral domain R is a Principal Ideal Domain (PID) if every ideal is principal.

Prop

A Euclidean Domain is a PID.

Examples

Yes: $\mathbb{Z}$, $\overset{\text{field}}{F}[x]$, $\mathbb{Z}[i]$ are PIDs.

No: $\mathbb{Z}[x]$, $\mathbb{Z}[\sqrt{-5}]$

There exist PIDs which are not Euclidean Domains $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

PIDs are similar to Euclidean Domains.

⇝ GCDs ∃ & are unique up to units.

Prop

R a PID. $a, b \in R$ nonzero.

Then $(a,b) = (d)$

1) d a GCD of a & b. (*)
2) ∃ $x, y \in R$ s.t. $d = ax + by$ (*)
3) d is unique up to mult by a unit. (*)

Recall

In $\mathbb{Z}$, all nonzero prime ideals are maximal.

Not true in every ring (E.g. $(x) \subseteq \mathbb{Z}[x]$)

It is for PIDs.

Theorem R a PID.

Let $I \subseteq R$ be nonzero & prime. Then

R is maximal.

Proof

$I = (p)$ some $p \in R$.

$$\begin{array}{ccccc} I & \subseteq & J & \subseteq & R \\ \| & & \| & & \cup\!| \\ (p) & \subseteq & (m) & & \end{array}$$

Show $J = R \leftarrow$ or $J = I \leftarrow$

$p \in (m) \Longrightarrow p = \underline{r} \cdot m \quad r \in R$

$\Longrightarrow r \cdot m \in (p)$

$\Longrightarrow r \in (p)$ ① or $m \in (p)$ ②

① $r \in (p) \rightsquigarrow r = ps = rms$

R a domain $\Longrightarrow$ has cancellation

$\rightsquigarrow 1 = ms$

$\rightsquigarrow m \in R^{\times}$

$\rightsquigarrow (m) = R$

$\uparrow$ HW 11 #5(a)

② $m \in (p) \Longrightarrow (m) \subseteq (p)$

$\Longrightarrow (m) = (p)$

Very Important Consequence

F a field.

$F[x]$ a PID

so Any prime ideal $(p) \leq F[x]$ nonzero is maximal

so $F[x]/(p)$ a field.

Uses F a field $\Longrightarrow$ $F[x]$ a PID.

Not true if F not a field. (e.g. $\underline{\underline{\mathbb{Z}[x]}}$)

Corollary

R a commutative unital ring.

$$R[x] \text{ a PID} \iff R \text{ a field.}$$

Pf/ $\Longleftarrow$ ok

$\Longrightarrow$ $R \leq R[x]$ ← a PID then

Integral domain (no 0 divisors).

$$\begin{tikzcd} R[x] \arrow[r, "\varepsilon_0"] & R \\ f(x) \arrow[r, mapsto] & f(0) \end{tikzcd}$$

$\ker(\varepsilon_0) = (x)$. ε_0 surjective.

So $\dfrac{R[x]}{(x)} \simeq R$ ← integral domain.

$\Longrightarrow$ (x) a nonzero prime ideal.

$\Longrightarrow$ $R[x]$ a PID so (x) is maximal.

$$\Longrightarrow \frac{R[x]}{(x)} \text{ a field}$$
$$\cong$$
$$R.$$

Another property of $\mathbb{Z}$ is unique factorization into prime numbers. $\longleftarrow$?? maybe 2 options to define in general?

Maybe PIDs have this too?

Def^n R an integral domain.

1) $r \in R$ nonzero & not a unit.
r is irreducible if whenever $r = ab$,
either $a \in R^\times$ or $b \in R^\times$.

2) $p \in R$ is prime if (p) is a prime ideal. } Euclid's Lemma.

In $\mathbb{Z}$ these are same. In a general ring they aren't.

Prop R an integral domain.

① Prime elts of R are irreducible

② If R is a PID, the converse holds.

Proof

① (P) a prime ideal.

$p = ab.$

Then $ab \in (p) \rightsquigarrow \underbrace{a \in (p)}_{\text{WLOG}}$ or $b \in (p)$

$\rightsquigarrow a = pr = abr$

Cancel a's $\rightsquigarrow 1 = br$

$\rightsquigarrow b \in R^{\times}.$

② p irreducible & R a PID

$\underline{\underline{(p) \subseteq M}} = (m)$ ✓ $\quad M$ prime ideal. (maximal).

So $p = rm$, but p irred so $\underset{①}{r}$ or $\underset{②}{m} \in R^{\times}$

① Then $(p) = (m)$ by HW11 #5(b)

so (p) prime.

② $(m) = R$ HW11 #5(a) ↯ bc

M is prime.