4/2

comm. w/ 1.

— rings

$\mathbb{Z}, \mathbb{R}, \mathbb{C}$.

$\mathbb{Z}/n\mathbb{Z}$.

$R[x]$

R/I

ker gp hom.

$H \trianglelefteq G$

G/H group.

kern. ring hom. ←

I ideal. $0 \in I$

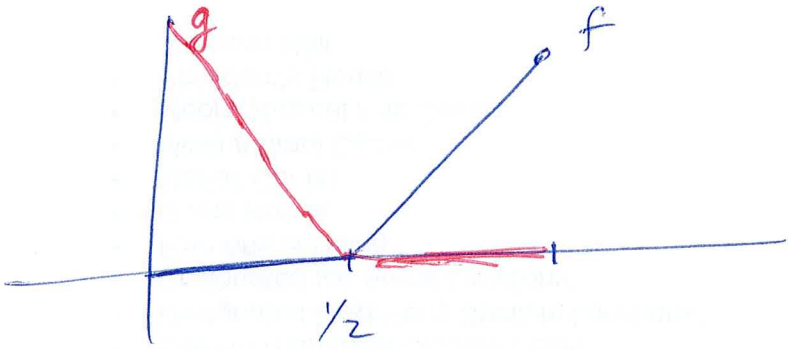
- subgp — closed under +
- abs. prop. $r \in R, x \in I \Rightarrow rx \in I$.

— Set of cont. functions on $[0,1]$.

ring. $C([0,1])$

constant funct
$\bar{0}$ is add id
$\bar{1}$ mult. identity

not an int. domain



$f \cdot g = 0$

trivial ideals $\{0\}, R$.

$I = aR$

— PID: principal ideal domain
every ideal is principally generated.

a fin. gen. $a_1, \ldots, a_n$
$I = a_1R + \ldots + a_nR$

— every ideal is fg. then R is called Noetherian.

fact
if $a \in I$, then $aR \subseteq I$

R[x] polynomial ring w/ coeff. in R.

Def. Euclidean Domains

A norm on a ring is a map $N: R \to \mathbb{N} \cup \{0\}$.

$N(0) = 0$.

a domain D is called a Euclidean domain if $\exists$ a norm $N: R \to \mathbb{N} \cup \{0\}$ s.t.

$\forall a, b \in D \ (b \neq 0) \quad \exists q, r \in D$

s.t. $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$

Division Algorithms say $\mathbb{Z}$ is a Euclidean domain w/ norm $N(a) = |a|$.

Thm Any Euclidean is a PID.

(3)

Recall Euclidean Algorithm

14, 7 $\quad 14 = 7 \cdot (2) + 0$. 7 divides 14.

$\gcd(14,7) = 7$.

51, 6

$$\begin{array}{r} 8 \\ 6 \overline{)\,51} \\ \underline{48} \end{array}$$

$51 = 6 \cdot (8) + 3$

$6 = 3 \cdot 2 + 0$

$\gcd(51,6) = 3$.

273, 143

$$\begin{array}{r} 273 \\ 143 \\ \hline 130 \end{array}$$

$273 = 143(1) + 130$

$143 = 130(1) + 13$

$130 = 13 \cdot 10 + 0$

$\gcd(273,143) = 13$.

$273 = 13 \cdot 3 \cdot 7$

$143 = 13 \cdot 11$

Bezout's Theorem on $\mathbb{Z}$.

$a, b \neq 0 \quad d = \gcd(a,b)$

~~If~~ "a divides b"

~~Def~~. $a \mid b$ if $\exists$ $k \in R$ s.t. $ak = b$.

R ring

in $\mathbb{Z}$

if $a \mid b$

$|a| \leq |b|$

So each int. has a finite # of divisors.

(4) $\mathbb{Z}$ $\{\text{div. of } a\} \cap \{\text{div of } b\}$

set of common divisors.

the largest is the $GCD(a,b)$.

Bezout's Identity Let $d = gcd(a,b)$. there exists $m,n \in \mathbb{Z}$ s.t. $d = ma+nb$.

the proof does not tell us how to find m,n

$a, b \quad b \neq 0$

Euclidean Algorith.

$a = bq_0 + r_0 \quad 0 < r_0 < b$ or $r_0 = 0$

$b = r_0 q_1 + r_1 \quad 0 < r_1 < r_0$ or $r_1 = 0$

$r_0 = r_1 q_2 + r_2$

$r_1 = r_2 q_3 + r_3$

process eventually stops

$\vdots$

~~$r_n = r_{n+1} q_{n+2} + 0$~~.

$r_{n-1} = r_n q_{n+1} + r_{n+1}$ ← gcd.

next is div.

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

(3)

$273 = 143 \cdot (1) + 130$

$143 = 130(1) + 13$

$13 = 143 + (-1)130$

$= 143 + (-1)(273 + (-1)143)$

$13 = 2 \cdot (143) + (-1)\,273.$ lin. comb. of 143, 273

Using Eucl. Alg. is a constructive way to find the m, n s.t.

$$d = ma + nb$$

Pf. that a Euclidean domain is a PID

Let R is a Eucl. domain and let I be an ideal of R.

Choose $d \in I$ $(d \neq 0)$ of least norm.

$dR \subseteq I$.

$\{N(a) \mid a \in I, a \neq 0\}$ natural #s.

WTS $I \subseteq dR$. take $x \in I$. Since R is Euclidean $x = dq + r$ $r = 0$ or $N(r) < N(d)$.

$r = x - dq \in I$. So $r \in I$.

by choice of d w/ least norm $r = 0$

so $x = dq \in dR$. ∎

(6)

$R[x]$ $f(x), g(x)$ two polynomials w/ real coeff.

$f(x) = x^2 + 1$

$g(x)$ $x - 1$

long Division

$$x-1 \;\overline{)\; x^2 + 1 \;}\;\; x+1$$

$$-x^2 + x$$

$$x + 1$$

$$-x + 1$$

$$2$$

~~$x^2 + 1 = x(x-1)$~~

$$x^2 + 1 = (x-1)(x+1) + 2$$

$\deg : R[x] \longrightarrow \mathbb{N} \cup \{0\}$.

~~$N(f(x))$~~

$\deg(f(x))$ is a norm

$\deg(0) = 0$

The deg is a norm.

Theorem TFAE

1) R is a field
2) R[x] is a Euclidean Domain
3) R[x] is a PID.

Corollay - $\mathbb{Z}[x]$ is not a PID. $\mathbb{Z}$ is not a field

(7) R a field $\Rightarrow R[x]$ is a Euc. dom w/ norm deg

Pf § R is a field & let $f(x), g(x) \in R[x]$, $g(x) \neq 0$.

WTS $\exists\, q(x), r(x) \in R[x]$ s.t.

$$f(x) = g(x)q(x) + r(x)$$ & either $r(x) = 0$ or $\deg r < \deg g$.

I. if $f(x) = 0$ $\quad 0 = 0 \cdot g(x) + 0$ ✓

II. ~~$f(x)$~~ $f(x) \neq 0$. if $\deg f < \deg g$.

$$f(x) = 0 \cdot g(x) + f(x) \quad \deg f < \deg g$$

III. $\deg f \geq \deg g(x)$.

write $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ $\quad \deg f = n$

$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$ $\quad \deg g = m$

monic means leading coeff. = 1

~~$n \geq 0$~~ $n \geq m$.

$$f(x) = -g(x) + r(x)$$

Aside $n = m$.

$$f(x) = a_n b_m^{-1} g(x)$$

$$\deg\left(f(x) - a_n b_m^{-1} g(x)\right)$$

$$a_n x^n + \dots + a_1 x + a_0 - a_n x^n - a_n b_m^{-1} b_{m-1} x^{m-1} + \dots - a_n b_m^{-1} b_0$$

(8)

$$f(x) = 3x^3 + 2x^2 + x + 1$$

$$g(x) = 5x^3 + \frac{10}{3}x^2 + 3x + 1$$

$f(x) - \frac{3}{5}g(x)$ $\qquad a_3 = 3$ $\quad b_3 = 5$ $\quad a_n b_m^{-1} = \frac{3}{5}$

$$3x^3 + 2x^2 + x + 1 - 3x^3 - 2x^2 - \frac{9}{5}x - \frac{3}{5}$$

$$(1 - \tfrac{9}{5})x + (1 - \tfrac{3}{5})$$

$n \geq m$ $\quad \deg\left(f(x) - a_n b_m^{-1} g(x)\right) < n.$

$$f(x) = \left(a_n b_m^{-1} x^{n-m} g(x)\right) + \left(f(x) - a_n b_m^{-1} x^{n-m} g(x)\right)$$

$\deg < n.$

R field $\Rightarrow$ R[x] Eucl. domain

$\Rightarrow$ R[x] PID

$\nexists$ R[x] PID WTS R field.

(9) $\S$ ~~R~~ $R[x]$ is PID $\Rightarrow$ WTS R field.

Let $a \in R$ $(a \neq 0)$.

~~$I = aR + xR$~~ $I = aR[x] + xR[x]$

$I = d(x)R[x]$

$r(x) = r_0 + \dots + r_t x^t$

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

$d(x) = a\,r(x) + x\,g(x)$

$d_0 = d(0) = a \cdot r_0$. WTS $= 1$

$a \in I$ so $a \in d(x)R[x]$

$a = d(x) \cdot s(x)$

$= d_0 + s_0$

~~d_0~~ $d(x) = d_0 + d_1 x + \dots + d_n x^n$

$s(x) = s_0 + s_1 x + \dots + s_j x^j$

$d(x)s(x)$ has leading coeff. $d_n s_j$.

$n = 0 = j$.

$d_0 = a r_0$

$a = d_0 s_0$

$d_0 = d_0 s_0 r_0$ $\quad 1 = s_0 r_0$

a is a unit

R field

I'll redo this part