Lecture 22   30   mean 32

Mon Dec 21 1–4pm

Plan: take-home final by 4pm Mon

Post Sun. morning.

Review session Saturday ✓ Dec 19 Morning/afternoon.

F - field at most n nth roots of unity.

$x^n - 1 = 0$

Ring $x^n = 1$ $\mathbb{Z}/8$ (not ID) $\{1,3,5,7\}$ $a^2 = 1$

$R_1 \times R_2$ $\{\pm 1\} \times \{\pm 1\}$ $-1 \neq 1$

$(\pm 1, \pm 1)$ ← 2nd roots of unity

Fields - rigid, rings - flexibility.

$\mathbb{Z}/n$ field iff n prime

$F[x]/(f)$ field iff f irreducible.

In general.

Thm (Chinese remainder theorem).

If $(n,m)=1$ $\mathbb{Z}/nm \simeq \mathbb{Z}/n \times \mathbb{Z}/m$

Reminder $e \in R$ an idempotent, R commutative

$e^2 = e$ Re ← ring e identity

$a\underbrace{ebe} = abe$.

$Re \subset R$

not a unital inclusion ring hom in a weak sense

$e \mapsto e$

$e \rightsquigarrow 1-e$ idemp. $\qquad e(1-e)=0 \qquad e-e^2=0$.

zero divisor

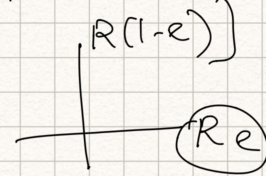
$Re, R(1-e) \subset R \qquad \boxed{R = Re \times R(1-e)}$

$Re \cap R(1-e) = 0 \qquad$ direct product of rings

$R_1 \times R_2 \longleftrightarrow Re \times R(1-e)$

$(1,0) \longleftrightarrow e$

$(0,1) \longleftrightarrow 1-e$



$a \in R \qquad a = a\cdot 1 = a(e+(1-e)) = \underset{\in Re}{ae} + \underset{\in R(1-e)}{a(1-e)}$.

$\mathbb{Z}/nm \simeq \mathbb{Z}/n \times \mathbb{Z}/m \qquad (n,m)=1 \quad (n),(m)$

I, J ideals

$\mathbb{Z}/nm \longrightarrow \mathbb{Z}/n\,,\ \mathbb{Z}/m \qquad R/_{IJ} \longrightarrow R/_{I}$

$x + nm\mathbb{Z} \longrightarrow x + n\mathbb{Z} \qquad \underline{IJ} \subset \underline{I}$

__Proof__ $\exists\, a, b \in \mathbb{Z} \quad \underbrace{an}_{e} + \underbrace{bm}_{1-e} = 1$

$an = 1 - bm \qquad \underline{\mathbb{Z}/nm}$

$e^2 = (an)^2 = an \cdot an = an(1-bm) = \qquad an\,,\ bm$

$= an - ab\underbrace{nm} = \underset{e}{an} \pmod{nm}$

$e^2 = e$ in $\mathbb{Z}/nm \qquad e = an \qquad 1-e = bm \qquad \underline{(a,m)=1}$

$(bm)^2 = bm$

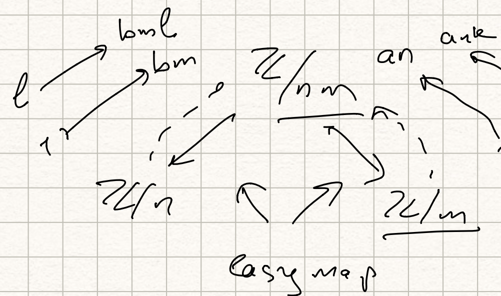
$(e) = (\underline{an}) = (n) \leftarrow$ ideals + contain idempotents

$(1-e) = (bm) = (m)$.

$\mathbb{Z}/m \quad \{0, 1, 2, \dots, m-1\} \qquad k \mapsto kan$

$(n) = \{0, n, 2n, 3n, \dots, an, \dots 2an, \dots (m-1)n\} \leftarrow m$ elements

$\{0, 1, \dots, m-1\} \bmod m \qquad$ idemp. in the middle $\qquad$ as ab. group



$\mathbb{Z}/nm \simeq \mathbb{Z}/n \times \mathbb{Z}/m$

idempotents.

$1 = an + bm$

div. with remainder to find a and b.

<u>Example</u> $n = 13,\ m = 5$ $\quad 13 \cdot 5 = 65$

$\mathbb{Z}/65 \simeq \mathbb{Z}/13 \times \mathbb{Z}/5$.

$a \cdot 13 + b \cdot 5 = 1 \qquad a = 2 \quad b = -5 \qquad \underline{2 \cdot 23} + \underline{(-5) \cdot 5} = 1$

idempotents $26,\ -25$.

$26^2 = 26(1+25) = 26 + \underbrace{\overset{2\cdot 13}{26} \cdot \overset{5\cdot 5}{25}}_{} = 26 \pmod{65}$.

$\mathbb{Z}/5 \to \mathbb{Z}/65$

$1 \mapsto 26$

$k \mapsto 26k$

$\mathbb{Z}/13 \to \mathbb{Z}/65$

$1 \mapsto -25$

$k \mapsto -25k$.

$\mathbb{Z}/m \to \mathbb{Z}/nm$

$1 \mapsto an$

$k \mapsto ank$

$1 = an + bm$

$\mathbb{Z}/n \to \mathbb{Z}/mn$

$1 \mapsto bm$

$k \mapsto bmk$.

$\mathbb{Z}/n$ - ?

$n = p_1^{r_1} \cdots p_k^{r_k}$

<u>Thm</u> $n = p_1^{r_1} \cdots p_k^{r_k}$ have

$$\mathbb{Z}/n \simeq \mathbb{Z}/p_1^{r_1} \times \mathbb{Z}/p_2^{r_2} \times \cdots \times \mathbb{Z}/p_k^{r_k}.$$

Proof: Hint: use induction $(p_1^{r_1})(p_2^{r_2} \dots p_k^{r_k})$

coprime.

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{r_1} \times \boxed{\mathbb{Z}/p_2^{r_2} \dots p_k^{r_k}}$$

use induction

$$= \mathbb{Z}/p_1^{r_1} \times \dots \times \mathbb{Z}/p_k^{r_k}.$$

$\mathbb{Z}/p^r$ p^r $\mathbb{Z}/p^r$ - field iff $r=1$ $\mathbb{Z}/p$

$\mathbb{Z}/p^2$, $\mathbb{Z}/p^3 \dots$ not a field, not an integral domain

$p^r = 0$.

p^{r-1} elements.

Ex $\mathbb{Z}/p^r$ has a unique maximal ideal (p)

$\forall$ elt of this ideal is nilpotent $a \in (p)$, $a = p \cdot m$

$a^r = (pm)^r = 0$.

Remark if a nilp. $1-a$, $1+a$ easy to find the inverse

$$(1-a)(1+a+a^2+\dots+a^{r-1}) = 1 - a^r = 1.$$

$\mathbb{Z} \longleftrightarrow F[x]$ both PID

$p \longleftrightarrow$ monic irr $f(x)$.

$F[x]/(f)$ - field $\mathbb{Z}/p$.

f - any pol.

$F[x]/(f)$ $\leftarrow$ not a field, in general.

$f = f_1 \cdot f_2$ $(f_1, f_2) = 1$ coprime.

$$\underline{a(x) f_1(x)} + \underline{b(x) f_2(x)} = 1.$$

$R = F[x]/(f_1(x) f_2(x))$ $\quad$ af_1 – idempotent

bf_2 – idempotent.

$R \longrightarrow \underline{F(x]}/(f_1)$, $R \to \underline{F[x]/(f_2)}$

Thm (Chinese remainder theorem) if $(f_1, f_2) = 1$

$$F[x]/\underline{\underline{(f_1 f_2)}} \simeq \underline{F[x]/(f_1)} \times \underline{F[x]/(f_2)}$$

$$F[x]/(f_2) \longrightarrow F(x]/(f_1 f_2)$$

$$1 \longmapsto af_1$$

$\underline{(n)}, \underline{(m)} \subset \mathbb{Z}$ $\quad$ (nm) $\quad$ $F[x]$ $\quad$ $(f_1), (f_2)$

$I_1, I_2 \subset R$ coprime or comaximal if

$\underline{\underset{\substack{\cap \\ \text{ideal}}}{I_1}} + \underline{I_2} = R \iff 1 \in I_1 + I_2$ $\quad$ $1 = a + b$ $\quad$ $a \in I_1$, $b \in I_2$.

$I_1 + I_2 = R$

Rem For $\underline{\text{coprime}}$ I_1, I_2 : $I_1 I_2 = I_1 \cap I_2$.

$$\underline{R \xrightarrow{\varphi} R/I_1 \times R/I_2}$$

This map is $\underline{\text{surjective}}$ and $\underline{\underline{\ker \varphi}} = I_1 I_2 = I_1 \cap I_2$.

$$\boxed{R/\underline{I_1 \cap I_2} \longrightarrow R/\underline{\underline{I_1}} \times R/\underline{\underline{I_2}} \text{ is an isomorphism}}$$

$\underline{1} = x + y$ $\quad$ $\underline{x \in I_1}, y \in I_2$. $\quad$ $1 \longrightarrow 1 \times 1$

$x \longmapsto (0, x)$

$\varphi(x)$ $\quad$ $x \in I_2$

$y \longmapsto (y, 0)$

$x+y=1 \longrightarrow (1,1)$ $\qquad (1,1) = (0,x)+(y,0)$

$x \mapsto (0,x)$, $y \mapsto (y,0)$

$(0,x) = (0,1)$, $(y,0) = (1,0)$

$x + I_2 = 1 + I_2 \qquad y + I_1 = 1 + I_1$

$(0,c) \qquad cx \mapsto (0, cx) = (0,c)$

Friedman why $I_1 I_2 = I_1 \cap I_2$. $\qquad \forall I, J \quad IJ \subset I \cap J$.

$F[x] \qquad f = f_1^{r_1} \cdot f_2^{r_2} \cdots f_k^{r_k} \qquad (f_i, f_j) = 1 \quad i \neq j$

Thm $F[x]/(f) \cong F[x]/(f_1^{r_1}) \times F[x]/(f_2^{r_2}) \times \cdots \times F[x]/(f_k^{r_k})$.

$g = f_i \leftarrow$ irreducible $/F$

$R = F[x]/(g^r)$ − field iff $r=1$. $\quad F[x]/(g)$.

otherwise $r>1$ has zero divisors.

R has a unique maximal ideal (local ring − a ring with a unique maximal ideal, $\mathbb{Z}/(p^r)$).

$(g) \leftarrow$ zero divisors

$g \cdot g^{r-1} = 0$.

$\mathbb{Z}/n$, $F[x]/(f)$

$1 = an + bm$

$R \cong R_1 \times R_2$

$(1, 0) = e$

$(0, 1) = 1-e$

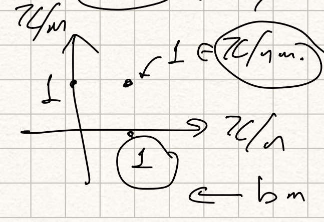
$(n,m)=1$

$\mathbb{Z}/nm \cong \mathbb{Z}/n \times \mathbb{Z}/m$.

$(1, 0)$

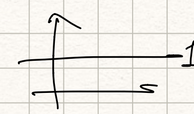
max. ideal $\leftrightarrow$ "points"

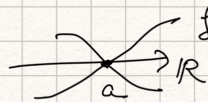
alg. geom



$\mathbb{R}$ Very large ring : continuous functions

Fun : $\mathbb{R} \xrightarrow{f} \mathbb{R}$ $f+g$, fg, 1





$I_a = \{ f \mid f(a) = 0 \}$ Fun /

ideal

$f, g \in I_a$ $f+g \in I_a$. $f \in I_a$, $g \in \mathrm{Fun}$ $fg \in I_a$

$f(a)g(a) = 0\, g(a) = 0$.

Rm $I_a \subset \mathrm{Fun}$ is a max ideal.

point a in $\mathbb{R} \longrightarrow$ max ideal I_a $\boxed{\mathrm{Fun}/I_a \simeq \mathbb{R}}$

$f \longmapsto f(a)$.

Rm This is a bijection between points and max. ideals.

use smaller rings, $F[x_1 \dots x_n]$, treat max ideals as points

(prime ideal).

Correspondence

Spaces $\longleftrightarrow$ commutative rings

$X \rightsquigarrow \mathrm{Fun}(X)$

space ring of functions

space, $\longleftarrow$ R

points are maximal/prime ideal

topology $\longleftrightarrow$ Commutative algebra.

geometry

field F — (0) max, prime

Local rings $\mathbb{Z}/p^r$ $\quad \mathbb{Z}/4, \mathbb{Z}/8,$

'unique max.' ideal

$\mathbb{Z}/27 \dots$

point + extra info. $\quad (p) \subset \mathbb{Z}/p^n$

$\to$ alg. geom

field theory $\subset$ comm. alg. (Atiyah–MacDonald)

Making, breaking codes.

$\mathbb{Z}/n$, f. field $\to$ applications

$\mathbb{Z}/$ $\quad n = pq$ $\quad p, q$ – distinct primes

$$\mathbb{Z}/n \simeq \mathbb{Z}/pq = \mathbb{Z}/p \times \mathbb{Z}/q.$$

If only known n and p, q are large enough (100+ digits each)

hard to compute p, q.

know n only

Quick ways to tell if m is prime.

Hack $\quad a^{p} = a \pmod{p} \Leftarrow$ prime.

$a^{m} = a \pmod{m}$ decent chance that m is prime

$$a^{\varphi(m)} = 1 \pmod{m} \quad \text{always}$$

$(a, m) = 1$

$\to (\mathbb{Z}/m)^*$ $\quad \varphi(m)$ $\quad \varphi(p) = p-1$ $\quad a^{p-1} = 1 \pmod{p}$ $\quad (a,p) = 1$

fin. ab. group, order $\varphi(m)$. $\quad a^{\varphi}$ $\quad a^{\varphi(m)} = 1.$ $\quad a^{\varphi(m)+1} = 1 \cdot a = a \pmod{m}$

$m = pq \quad \varphi(m) = \varphi(p)\varphi(q) =$

$= (p-1)(q-1)$

find a $\quad a^m \not\equiv a \pmod m \rightarrow m$ is composite

works for most non-prime m, use random a

Carmichael #'s: composite, $a^m \equiv a \pmod m$

$m = 561 = 3 \cdot 11 \cdot 17$

$\varphi(n)$? $\quad n = pq$ $\quad \varphi(n) = (p-1)(q-1)$

$\hookrightarrow$ RSA algorithm & public key cryptography.

n $\quad A, B \quad AB$ $\quad x \in (\mathbb{Z}/n)^\times$

A known $(x^A)^B = x$ $\quad x^{AB} = x \pmod n$.

$AB = \varphi(n) + 1 = (p-1)(q-1) + 1 = pq - p - q + 2$

$M \mapsto M^A \xrightarrow{\text{send}} M^A \quad (M^A)^B = M$.

$\mathbb{Z}/n \quad n = pq$. find idempotents