11/12/17

2nd lecture tomorrow: email requests for proofs/examples to go over.

Corollary 23.2 Let F be a field, and let $p(x)$ be an irreducible poly. in $F[x]$. Then $\exists$ field F_0 such that

1) $F \subseteq F_0$

2) F_0 contains a root of $p(x)$.

Pf. Take

$$F_0 = \frac{F[x]}{(p(x))}.$$

Then (1) follows from Prop 23.1(5), and (2) from 23.1(4). //

Eg. Some more finite fields:

1) Now x^3+x+1 is irreducible in $\mathbb{Z}_2[x]$, so

$$F_8 = \frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$$

is a field of order 8.

By 23.1(2), if $\alpha = I + x$ ($I = (x^3+x+1)$), then the elements of F_8 are

$$\{ a\alpha^2 + b\alpha + c : a, b, c \in \mathbb{Z}_2 \}$$

with mult. determined by

$$\alpha^3 + \alpha + 1 = 0$$

2) For any prime p, $\exists$ irred. polys in $\mathbb{Z}_p[x]$ of degrees 2 and 3 (Sheet 9 q4), so $\exists$ fields of order p^2 and p^3.

Fact: For any prime power p^n, $\exists$ field of order p^n.

Applications of finite fields

Let F_q be a finite field of order q (so $q = p^n$ for some prime p, by Sheet 9, q4).

- $\exists$ finite vector spaces $(F_q)^n$ over F_q of dim n — no. of vectors is q^n.

- Finite groups $GL(n, F_q)$,

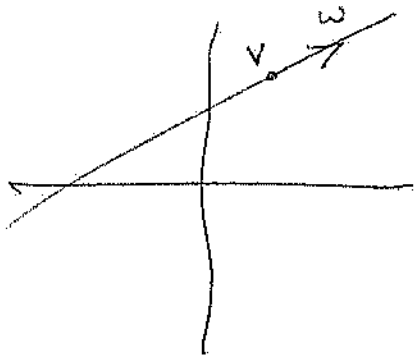
groups of invertible $n \times n$ matrices over F_q — leads to family of finite simple groups

$$PSL(n, q)$$

(projective special linear groups)

- Finite geometry

Eg. Finite plane $(F_q)^2$



Points = vectors in F_q^2

Lines = subsets $v + Sp(w)$

$(v, w \in F_q^2)$

Any 2 points are on a unique line.

Any line has q points.

- Number theory

"Riemann hypothesis over finite fields" is solved.

Now back to

Proof of Theorem 22.1:

$\frac{R}{I}$ is a field iff I is a maximal ideal

For proof we need

Lemma 22.2 A ring $(S, +, \times)$ (commutative with 1) is a field iff its only ideals are $\{0\}$ and S.

Pf ($\Rightarrow$) Space S is a field. Let I be an ideal of S, with $I \neq \{0\}$. Let $a \in I$, $a \neq 0$. Then as S is a field, $a^{-1} \in S$. As I is an ideal, $aa^{-1} = 1 \in I$, hence $I = S$.

($\Leftarrow$) Space the only ideals are $\{0\}$ & S.

Let $a \in S$, $a \neq 0$.

Then the principal ideal aS is nonzero (contains a), hence

$$aS = S.$$

So $\exists\, b \in S$ s.t. $ab = 1$.

Then $b = a^{-1}$. So S is a field. //

<u>Lemma 22.3</u> Every ideal of $\frac{R}{I}$ has the form $\frac{J}{I}$, where J is an ideal of R containing I.

Pf. Let K be an ideal of $\frac{R}{I}$. So K is a set of cosets $I+r$. Let

$$J = \bigcup_{I+r \in K} (I+r) \subseteq R.$$

Then

1) $I \subseteq J$, as the zero coset $I = I+0$ is in K.

2) J is an ideal of R:

· $(J,+)$ subgp of $(R,+)$:

$0 \in J$ (as $0 \in I \subseteq J$)

$x, y \in J \Rightarrow x \in I+r,\ y \in I+s$
(where $I+r, I+s \in K$)

$\Rightarrow x+y \in I+r+s \in K$
and $-x \in I-r \in K$

$\Rightarrow x+y, -x \in J$ ✓

· J ideal :

$x \in J,\ t \in R \Rightarrow x \in I+r\ (\in K)$

$\Rightarrow xt \in I+rt$
$= (I+r)(I+t)$
$\in K$ (ideal of $\frac{R}{I}$)

$\Rightarrow xt \in J$.

3) $K = \frac{J}{I}$:

· if $I+r \in K$ then $r \in J$
so $K \subseteq \frac{J}{I}$

· if $s \in J$, then $s \in I+r\ (\in K)$
so $I+s = I+r$, hence

$\frac{J}{I} \subseteq K$.

Therefore $K = \frac{J}{I}$. //

Ex. $R = \mathbb{Z}$, $I = 4\mathbb{Z}$

Ideals of $\mathbb{Z}$ containing $4\mathbb{Z}$ are

$$4\mathbb{Z},\ 2\mathbb{Z},\ \mathbb{Z}$$

Ideals of $\frac{\mathbb{Z}}{4\mathbb{Z}}$ are

$$\frac{4\mathbb{Z}}{4\mathbb{Z}} = \{0\},\ \frac{2\mathbb{Z}}{4\mathbb{Z}},\ \frac{\mathbb{Z}}{4\mathbb{Z}}$$

Know $\frac{\mathbb{Z}}{4\mathbb{Z}} \simeq \mathbb{Z}_4$: ideals of $\mathbb{Z}_4$:

$$\{0\},\ \{[0],[2]\},\ \mathbb{Z}_4.$$

12/12/17

Proof of Thm. 22.1

[$\frac{R}{I}$ field $\iff$ I max. ideal].

($\Rightarrow$) Spose $\frac{R}{I}$ is a field.

Let

$$I \subsetneq J \subseteq R$$

where J is an ideal.

By 22.3, $\frac{J}{I}$ is an ideal of $\frac{R}{I}$, and is not the zero ideal (as $I \neq J$).

So by 22.2,

$$\frac{J}{I} = \frac{R}{I}$$

hence $J = R$.

Therefore I is a max. ideal.

($\Leftarrow$) Spose I is a max. ideal of R.

Let K be an ideal of $\frac{R}{I}$. Then by 22.3,

$K = \frac{J}{I}$, where J

is an ideal and

$$I \subseteq J \subseteq R.$$

As I is maximal,

$$J = I \text{ or } R$$

hence

$$K = \frac{I}{I} (= 0) \text{ or } \frac{R}{I}$$

So the only ideals of $\frac{R}{I}$

are 0 and $\frac{R}{I}$.

Therefore $\frac{R}{I}$ is a field,

by Lemma 22.2. //.

Diophantine Equations

Eg. 1) Find all solns $x, y \in \mathbb{Z}$ to the eqn

$$y^2 = x^3 - 11$$

(example of Mordell's eqn $y^2 = x^3 + K$).

Soln Eqn is

$$x^3 = y^2 + 11$$
$$= (y + \sqrt{-11})(y - \sqrt{-11}),$$

factn in ring $\mathbb{Z}[\sqrt{-11}]$

FACT The ring

$$\mathbb{Z}\left[\tfrac{1}{2}(1+\sqrt{-11})\right]$$
$$= \left\{ \tfrac{a}{2} + \tfrac{b}{2}\sqrt{-11} : \begin{array}{l} a \equiv b \bmod 2 \\ a, b \in \mathbb{Z} \end{array} \right\}$$

is a UFD, units are ± 1.

Now

$$x^3 = y^2 + 11.$$

Space x is even.

Then y is odd, so

$$y^2 \equiv 1 \bmod 8$$

The $x^3 \equiv 0 \bmod 8$

but $y^2+11 \equiv 4 \bmod 8$ ✗

Therefore x is odd, y even

Also 11 does not divide x or y

Let

$$R = \mathbb{Z}\left[\tfrac{1}{2}(1+\sqrt{-11})\right].$$

In R,

$$\text{hcf}\left(y+\sqrt{-11},\ y-\sqrt{-11}\right)$$

divides $2\sqrt{-11}$.

As 2 and 11 don't divide x,

$$\text{hcf}\left(y+\sqrt{-11},\ y-\sqrt{-11}\right) = 1$$

As R is a UFD,

the eqn (M) implies

each factor $y \pm \sqrt{-11}$ is

a cube in R, so

$$y+\sqrt{-11} = \alpha^3, \quad \alpha \in R$$

Write

$$\alpha = a + \frac{b}{2}(1+\sqrt{-11})$$

where $a, b \in \mathbb{Z}$.

Equating coeffs of $\sqrt{-11}$,

$$8(y+\sqrt{-11}) = (2a+b+b\sqrt{-11})^3$$

so

$$8 = 3b(2a+b)^2 - 11b^3$$

$$= 4b(3a^2+3ab-2b^2)$$

Hence b divides, so

$$b = \pm 1, \text{ or } \pm 2.$$

Possibs:

$b=-1,\ a=1$ → $x=3, y=\pm 4$

$b=-1,\ a=0$ →

$b=2,\ a=1$ → $x=15, y=\pm 58$

$b=-2,\ a=3$ →

Cachude Sunhais of

$$y^2 = x^3 - 11$$

are

$$x=3,\ y=\pm 4$$

& $x=15,\ y=\pm 58$

Note Other values of k in Mordell's eqn $y^2 = x^3 + k$ are not so easy, eg

$$y^2 = x^3 - 5$$

Here $$x^3 = y^2 + 5 = (y+\sqrt{-5})(y-\sqrt{-5})$$

But the ring $\mathbb{Z}[\sqrt{-5}]$ (and also $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-5})]$ is not a UFD.

So this case is much harder.

2) Fermat's Last Thm

This says: if $n \geq 3$, the only sols to the Diophantine eqn

$$x^n + y^n = z^n \quad (x,y,z \in \mathbb{Z})$$

is $x = y = z = 0$.

Case $n = 3$

Eqn

$$x^3 + y^3 = z^3$$

1) Can factorize as

$$z^3 = x^3 + y^3$$

$$= (x+y)(x+wy)(x+w^2y)$$

where $w = e^{2\pi i/3}$.

Note $w^3 - 1 = 0$, so $w^2 + w + 1 = 0$

so

$$w = -\text{or} \ \tfrac{1}{2}(-1 + \sqrt{-3}).$$

So each is in the ring $R = \mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\}$.

This is a UFD. Units are

$\pm 1, \pm w, \pm w^2$.

2) Consider hcf's of the terms in factn.

Show

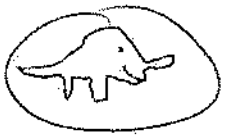
$$\text{hcf}(x+y, x+wy) = 1-w.$$

Let $\lambda = 1 - w$.

As R is UFD, get

$$x + y = u_1 \lambda^{3k-2} \alpha^3$$
$$x + wy = u_2 \lambda \beta^3$$
$$x + w^2 y = u_3 \lambda \gamma^3$$

where u_i are units in R, and $\alpha, \beta, \gamma \in R$.

Fiddling around with 

similarly to the previous eg. we get a ✳.

General case

✳
Need only consider $n = p$ (prime) > 2 or 4.

Main case

$$x^p + y^p = z^p \qquad (p \text{ prime}).$$

Factorizes as

$$z^p = (x+y)(x+\omega y)\cdots(x+\omega^{p-1}y)$$

Where $\omega = e^{2\pi i/p}$.

This fact. is in the ring

$$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1} : a_i \in \mathbb{Z}\}.$$

Problem ✳ Is this ring a UFD?

Ans No, usually not.

So previous method fails.

Revision topics:

1) JCF proof & examples

2) Examples of ring isomaphisms

---

1) JCF Proof

A) Direct sums $V = V_1 \oplus \dots \oplus V_k$.

(B) $T: V \to V$, char. poly $\prod_{i=1}^{k} (x-\lambda_i)^{a_i}$. Let

$$V_i = \ker (T - \lambda_i I)^{a_i}$$

Then

1) $V = V_1 \oplus \dots \oplus V_k$

2) Each V_i is T-invariant and restricted T_{V_i} has only one evalue, namely λ_i.

3) Case of 1 evalue

Each V_i has a Jordan basis:

Let $S = T_{V_i} - \lambda_i I$, so $S^m = 0$ for some m. Jordan basis of V_i is

$$S^{m_1-1}(v_1), \ldots, S(v_1), v_1,$$

$$\vdots$$

$$S^{m_r-1}(v_r), \ldots, S(v_r), v_r$$

where $S^{m_i}(v_i) = 0$.

If B is the union of all the Jordan bases for the V_i's, then

$$[T]_B = \text{JCF matrix}$$

How to compute JCF & Jordan basis of $T: V \to V$

1) Find each $V_i = \ker (T - \lambda_i I)^{a_i}$

2) Let $S = T_{V_i} - \lambda_i I$. ($S^m = 0$).

a) Compute

$$\text{null}(S) = \dim(\ker S).$$

(This is same as

$$\text{null}(T - \lambda_i I)\ ).$$

This is the no. of λ_i-blocks in the JCF

b) Compute

$$\min(m : S^m = 0).$$

This is the size of the largest λ_i-block.

(This value is

$$\min\left(m : \operatorname{rank}(T-\lambda_i I)^m = \sum_{j \neq i} \dim V_j\right).)$$

\$ Often a) & b) are enough to compute the JCF.

If not, the ranks of $S^{m-1}, S^{m-2}, \dots$ determine the λ_i-block sizes.

3) Jordan basis of V_i

If $\exists$ only one λ_i-block, just need to find $v \in V_i$ s.t. $S^{m-1}(v) \neq 0$. Then Jordan basis is

$$S^{m-1}(v), \dots, S(v), v.$$

If $\exists$ more than one λ_i-block, find the image $S(V_i)$, and (if possible) find a Jordan basis of sub:

$$S^{m_1-2}(u_1), \ldots, S(u_1), u_1,$$
$$\vdots$$
$$S^{m_r-2}(u_r) \ldots, S(u_r), u_r$$

Add further vectors v_i, w_i to this such that

$$u_i = S(v_i)$$

and

$$S^{m_1-2}(u_1), \ldots, S^{m_r-2}(u_r), w_1, \ldots, w_s$$

is a basis of $\ker(S)$.

Eg. 1) Find Jordan basis for $T: \mathbb{C}^{\#5} \to \mathbb{C}^{\#5}$, $T(v) = Av$,

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 0 & 1 \\ & & 1 & 0 & 1 \\ 0 & & & 1 & 1 \\ & & & & 1 \end{pmatrix}$$

Ans Char poly $(x-1)^5$, evalue 1.

Now

$$\text{null}(A - I) = 3$$

So $\exists$ 3 Jordan blocks

Next,

$$(A-I)^2 = \begin{pmatrix} & & 3 \\ & 0 & \\ & & \end{pmatrix}$$

& $(A-I)^3 = 0$.

∴ largest block has size 3.

Hence JCF is

$$\underline{J_3(1) \oplus J_1(1) \oplus J_1(1)}.$$

<u>Jordan basis</u>

Let

$$S = A - I = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 1 \\ & & 0 & 0 & 1 \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix}$$

Image

$$S(V) = Sp(e_1, e_1+e_2+e_3+e_4)$$

Jordan basis for this

$$3e_1, \quad e_1+e_2+e_3+e_4$$

$$[\; S(u_1), \quad u_1 \;].$$

Add vectors

v_1 : want $S(v_1) = u_1$

take $v_1 = e_5$.

Add w_1, w_2 so that

$$3e_1, w_1, w_2$$

is basis of $\ker(S)$. Take

$$w_1, w_2 = e_2 - e_3, \; e_3 - e_4$$

So final Jordan basis is

$$\beta = 3e_1, e_1+e_2+e_3+e_4, e_5, e_2-e_3, e_3-e_4.$$

Then

$$[T]_\beta = J_3(1) \oplus J_1(1) \oplus J_1(1).$$

(B) Ring isomorphisms

Example Four rings of order 9

$$\frac{\mathbb{Z}_3[x]}{(f(x))}, \text{ where}$$

$$f(x) = \underset{f_1}{x^2}, \underset{f_2}{x^2+1}, \underset{f_3}{x^2-1}, \underset{f_4}{x^2+x-1}.$$

Call these rings

$$R_i = \frac{\mathbb{Z}_3[x]}{(f_i(x))}$$

Q Which pairs of R_1, R_2, R_3, R_4 are isomorphic?

Note By Lecs. Theory,

each $R_i = \{a\alpha + b : a, b \in \mathbb{Z}_3\}$

where $\alpha = (f_i(x)) + x$,

& $|R_i| = 9$.

Step 1 f_2, f_4 are irreducible

f_1, f_3 are reducible.

Hence

R_2, R_4 are fields (22.1)

R_1, R_3 are not

So only qns are

Is $R_2 \cong R_4$? $R_1 \cong R_3$?

Claim 1 $R_1 \not\cong R_3$.

Pf Now

$$R_1 = \{a\alpha + b : a, b \in \mathbb{Z}_3\},\ \alpha^2 = 0$$

$(\alpha = I_1 + x)$

$$R_3 = \{a\beta + b : a, b \in \mathbb{Z}_3\},\ \beta^2 - 1 = 0$$

$(\beta = I_2 + x)$

Suppose $f : R_1 \to R_3$ isomorphism. Then

$$f(\alpha)^2 = f(\alpha^2) = 0.$$

But

$$(a\beta + b)^2 = 0 \implies a = b = 0,$$

since

$$(a\beta + b)^2 = 0$$

$$\implies (ax + b)^2 \in I_2 = (x^2 - 1)$$

$$\implies (ax + b)^2 \text{ divisible by } x+1 \text{ \& } x-1$$

hence by $(x+1)^2$ & $(x-1)^2$

$\times\!\!\times$

Claim 2 $R_2 \cong R_4$

[In fact: any two fields of same order are isomorphism.].

Pf. $R_2 = \{a\alpha + b\}$, $\alpha^2 + 1 = 0$

$R_3 = \{a\beta + b\}$, $\beta^2 + \beta - 1 = 0$.

So $f(\alpha) \in R_3$, and $f(\alpha)^2 + 1 = 0$.

(for any isom. f).

Now

$$(\beta - 1)^2 + 1 = 0.$$

Now check the map

$$\alpha \longrightarrow \beta - 1$$

and in general

$$a\alpha + b \longrightarrow a(\beta - 1) + b$$

is an isomorphism $R_2 \to R_4$.