10/12/19

 Last lecture

 ~~Good~~ axe!

 Class on Thursday!

∃ wonderful project

Last time: Construction of finite fields:

$$\frac{\mathbb{Z}_p[x]}{(p(x))}$$

$p(x)$ irreducible poly.

Point of finite fields

1) ∃ finite vector spaces F^n (F finite), of order $|F|^n$.

2) ∃ finite general linear groups

$$GL(n, F)$$

—much studied— eg. they lead to families of finite simple groups

$$PSL(n,F) = SL(n,F) / \{\lambda I_n : \lambda^n = 1\}$$

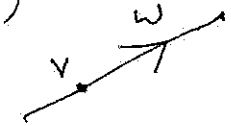
$$\left(SL = \{g \in GL : \det(g) = 1\}\right)$$

3) Finite geometry

e.g. plane F^2

points = vectors in F^2

lines = $v + \mathrm{Sp}(w)$



If $|F| = q$, every line has q points, and 2 points lie on a unique line, ~~and~~ any 2 lines meet in 0 or 1 points.

4) Number theory

"Riemann hypothesis over finite fields" was proved by Deligne....

28 Proof of Theorem 26.1

This says: for R an ID,

$\frac{R}{I}$ is a field $\Leftrightarrow$ I is a maxl. ideal.

Need two lemmas:

Lemma 28.1 Let S be a ring (commutative with 1). Then S is a field iff the only ideals of S are $\{0\}$, S.

Pf. ($\Rightarrow$) Suppose S is a field, and $I \neq \{0\}$ is an ideal. Let $0 \neq a \in I$. As S is a field, $\exists\, a^{-1} \in S$.
As I is an ideal

$$a a^{-1} = 1 \in I$$

$\therefore I = S$.

($\Leftarrow$) Suppose the only ideals of S are $\{0\}$, S.
Let $0 \neq a \in S$. The ideal aS is not $\{0\}$, hence is S.
Therefore $1 \in S = aS$
so $\exists\, b \in S$ s.t. $ab = 1$, i.e. $b = a^{-1}$.
Hence S is a field. //.

Lemma 28.2 Let R be an ID with an ideal I.
Then every ideal of $\frac{R}{I}$ is of the form $\frac{J}{I}$ where J is an ideal of R containing I.

Pf: Let K be an ideal of $\frac{R}{I}$.

Define $f: R \to \frac{R}{I}$ by (canonical homomorphism)

$$f(r) = I + r \quad (r \in R).$$

Let

$$J = f^{-1}(K)$$

$$= \{r \in R : f(r) \in K\}.$$

We claim J satisfies the conclusions of the lemma.

a) J contains I since

$$i \in I \Rightarrow f(i) = I + i = I \quad (\text{zero elt of } R/I)$$

$$\Rightarrow f(i) \in K$$

b) J an ideal

$(J, +)$ subgp:

$$0 \in J \text{ as } f(0) \in K$$

$$x, y \in J \Rightarrow f(x), f(y) \in K$$

$$\Rightarrow f(x+y) = f(x) + f(y) \in K$$

$$\Rightarrow x + y \in J$$

$$x \in J \Rightarrow \cdots\cdots \Rightarrow -x \in J.$$

$JR \subseteq J$

$$j \in J, r \in R \Rightarrow f(jr) = f(j) f(r)$$

$\in K\left(\frac{R}{I}\right) \subseteq K$ (ideal)

$\Rightarrow jr \in J$.

Finally, $K = \frac{J}{I}$ by defn

of $J = f^{-1}(K)$. //.

Proof Thm 26.1

[$\frac{R}{I}$ field $\Leftrightarrow$ I maxl ideal].

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

Let

$$I \subseteq J \subseteq R$$

where J is an ideal.

Then $\frac{J}{I}$ is an ideal

of the field $\frac{R}{I}$.

Hence by Lemma 28.1,

$$\frac{J}{I} = \{0\} \text{ or } \frac{R}{I}$$

& $J = I$ or R.

Therefore I is a maxl. ideal.

($\Leftarrow$) Spse I is a max. ideal.

Let K be an ideal of $\frac{R}{I}$.

By 28.2, $K = \frac{J}{I}$, where

$I \subseteq J \subseteq R$, J an ideal.

As I is maximal, $J = I$ or R,

hence

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

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

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

is a field, by Lemma 28.1. //

29. Applications to Diophantine equations

Recall: Diophantine eqn

is an algebraic eqn in

several variables, where solutions

are required to be integers.

Eg. Mordell's eqn

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

Solve for $x, y \in \mathbb{Z}$.

Sketch.

1) x, y are odd

Pf If not, both x & y are even,

but then

$$\text{LHS} \equiv 0 \bmod 4$$

$$\text{RHS} \equiv 2 \bmod 4 \quad \not\equiv$$

2) Factorize in the ring $\mathbb{Z}[\sqrt{-2}]$:

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

$R =$

Fact $\mathbb{Z}[\sqrt{-2}]$ is a UFD.

3) Claim $\gcd(x+\sqrt{-2}, x-\sqrt{-2}) = 1.$

Pf. Let

$$d = \gcd(x+\sqrt{-2}, x-\sqrt{-2}).$$

Then in R, d divides

the difference $2\sqrt{-2}$.

Taking absolute values,

$|d|^2$ divide 8

$(\in \mathbb{Z})$

Also $|d|^2$ divides y^3, an odd

number. Hence

$$|d|^2 = 1.$$

Hence the Claim.

4) Now $R = \mathbb{Z}[\sqrt{-2}]$ is a UFD and

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

This implies each factor $x \pm \sqrt{-2}$ is of the form ur^3, where u is a unit and $r \in R$.

Units of R are ± 1, hence can write

$$x+\sqrt{-2} = \text{unit} \cdot \text{cube}$$
$$= (a+b\sqrt{-2})^3 \quad (a,b \in \mathbb{Z})$$

Equating imaginary parts,

$$1 = 3a^2b - 2b^3$$
$$= b(3a^2 - 2b^2)$$

This implies

$$b = \pm 1, \quad 3a^2 - 2b^2 = \pm 1$$

$$\longrightarrow (a,b) = (\pm 1, \pm 1)$$

Then

$$x = a^3 - 6ab^2$$

hence $x = \pm 5$. So the only soln are

$$x = \pm 5, \quad y = 3$$