Combinatorics

Lecture 1

→ Art of counting things - Combinatorics.

→ Discrete Mathematematics.
(non-continuous) finite maths.

Linear Algebra. + cleverness!
(Finite) Field Theory.

—x—x—x—

Review - Finite fields.

Field Theory. Simplest possible ring.
Ring has + & ·. commutative w.r.t. ·
& has 1 mult. identity.

$0 \cdot a = 0 \quad \forall a \in R.$
unless $0 = 1$ (in that case $R = \{0\}$)
∴ 0 will never have mult. inverse in R.

Field is a ring where every elt. that is invertible has an inverse.

Fact. ⇒ the only ideals of a field F are generated by 0 & 1.

What is interesting from ring theory point of view is the poly. rings with coeff. from F and also the way two diff. fields interact with each other.

"units & primes" — in general ring theory.

If $F[x]$ is the poly. ring over F, then we can construct ~~a~~ many a new fields L such that $\underline{\underline{F \subseteq L}}$.

'interacting $\cong$ having functions.

Since a field has no ideals, any "$\underline{\text{function}}$" (ring homomorphism) $\underline{\text{bet}^n}$ two fields has to be injective.

($\because$ $\ker\theta \subset F$ ideal $\Rightarrow \ker\theta = \{0\}$, ~~F~~ as $1 \to 1$ in any ring homo.)

$f: G \to H$.

$f: R \to S$ $\quad f(xy) = f(x)f(y) \Rightarrow f(1_G) = 1_H$

$f(x+y) = f(x) + f(y)$ & $f(1_R) = 1_S$

$$\frac{R}{\ker\theta} \cong \mathrm{Im}(R) \quad \text{first homo. theorem.}$$

$$\Rightarrow R \simeq \mathrm{Im}(R).$$

——— x ——x——x——

$\underline{\text{Maximal}}$ ideals always exist in a Ring (comm. + 1)

(w.r.t. inclusion)

$$\begin{array}{ccc} R/\text{max.} & = & \text{Field.} \\ \uparrow \pi & & \cup \\ & & J. \\ R & \supseteq & \pi^{-1}(J) \end{array}$$

$$\Rightarrow \quad f \hookrightarrow F[x] \to \frac{F[x]}{m} = L.$$

$\underline{\underline{Q}}$. What are the max. ideals of $F[x]$? $F[x] = \text{PID}$

$\underline{\underline{\text{Ans}}}$. They are $\underline{\text{pricipal}}$. ie gen. by single element.

single elt. generates a max. ideal iff it is $\underline{\text{irreducible}}$ ($=$ prime) ($p \mid ab \Rightarrow p \mid a$ or $p \mid b$ is the def. prime in a general ring)

$f \neq g.h$ unless $\deg g$ or $\deg h = \deg f$. PID

Field is simplest ring ?

Finite field is "simplest" field !!

↳ a field having only finitely many elements.

$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, etc are not part of our course !

but $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ or any of their finite extensions are

Reference: Introduction to the theory of Error-Correcting Codes - Vera Pless (Second Edition)

(Chapter 4 :- Finite field.)

Q. Are there finite fields at all (if so can one list them all ?)

Thm: ① For any prime $p \in \mathbb{Z}$ & for any $n \in \mathbb{N}$, $\exists$ a finite field of order p^n.

② Any finite field must have order p^m with p, m as above.

③ $\forall$ p prime, $n \in \mathbb{N}$, $\exists!$ (up to isomorphism) field of order p^n; we will denote it by

$$GF(p^n) = \mathbb{F}_{p^n} \quad \text{(algebra notation)}$$

Galois field.

proof: ⓪ For any field F, $\exists$ $\bar{F}$ alg. closure of F.

Assuming ⓪, we prove ①.

(1a) Clearly $\mathbb{Z}/p\mathbb{Z}$ is a field. $(x, p) = 1 \Rightarrow \exists\, m, n$ s.t. $mx + np = 1$.

$\Rightarrow$ every non-zero elt in $\mathbb{Z}/p\mathbb{Z}$ has inverse.

$\Rightarrow \exists \ \overline{\mathbb{Z}/p\mathbb{Z}}$. the alg. closure of $\mathbb{Z}/p\mathbb{Z}$.

↳ infinite field (No finite field can be alg. closed)

$$f(X) = \prod_{a_i \in F}(X - a_i) + 1. \text{ has no root in } F.$$

$\forall n$, look at the roots of

$$X(X^{p^n}-1) = g(X) = X^{p^n} - X \in \mathbb{Z}/p[X] \text{ in } \overline{\mathbb{Z}_p}$$

<u>Claim</u> :- ① no root of $g(X)$ is repeated.

<u>Fact</u> A root of f is repeated iff it is a common root of $f(X)$ & $f'(X)$

$$f = \sum_{i=0}^{n} a_i X^i$$

$$f' = \sum_{i=0}^{n} i a_i X^{i-1}$$

$$g'(X) = \cancel{p^n X^{p^n-1}} - 1. \quad (p^n = 0)$$

$\overline{\mathbb{Z}/p}$, $p.a = 0 \ \forall a \in \overline{\mathbb{Z}/p}$.

$$\Rightarrow \left|\{\alpha \mid \alpha \in \overline{\mathbb{Z}_p} \ \& \ \alpha^{p^n} = \alpha\}\right| = p^n \rightarrow \text{Because } \mathbb{Z}/p \text{ is a domain.}$$

$$\| \\ GF(p^n)$$

clearly $0 \ \& \ 1 \in GF(p^n)$ Let $\alpha_0, \beta_0 \in GF(p^n)$

$$(\alpha_0\beta_0)^{p^n} = \alpha_0^{p^n} \cdot \beta_0^{p^n} = \alpha_0\beta_0 \Rightarrow \text{closed under mult.}$$

$$(\alpha_0 + \beta_0)^{p^n} = \alpha_0^{p^n} + \beta_0^{p^n} + \sum_{i=1}^{p^n-1} \binom{p^n}{i} \alpha_0^i \beta_0^{p^n-i}$$

↳ Binomial expansion.

$\binom{p^n}{i}$ is divisible by p $\forall 0 \neq i \neq p^n \rightarrow$ (Exercise)

$$\binom{p^2}{p} \qquad \frac{p(p-1)\cdots p-i+1}{i(i-1)\cdots 3.2.1}$$

$= \alpha_0 + \beta_0$ as $\alpha_0, \beta_0 \in GF(p^n)$

$\Rightarrow$ $GF(p^n)$ = roots of $x^{p^n} - x$ in $\overline{\mathbb{Z}_p}$ is a subring.

(Aside : $x^2 = x$ has 8 roots in $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$)

$\Rightarrow$ $GF(p^n)$ is a finite domain

(Fact (Exercise) – Any finite domain is a field)

$\Rightarrow$ $\exists$ a field of order p^n $\forall$ primes p & $n \in \mathbb{N}$.

(2) Given any finite field F, its characteristic must be a prime number.

$1 \in F \Rightarrow 1 \neq 0 \Rightarrow \underset{\text{order}}{O(1)}$ in $(F,+)$ is finite.

$\Rightarrow \exists$ least n s.t. $n \cdot 1 := \underbrace{1 + 1 + \cdots + 1}_{n\text{-times}} = 0$.

$n = m \cdot k$

$\Rightarrow \underset{\text{mult in field}}{(m \cdot 1) \cdot (k \cdot 1)} \overset{\text{notation}}{=} \underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$.

n has to be a prime.

$\mathbb{Z}$ - "Initial Object" in the cat. of comm. rings with 1.

$\exists! \, \theta$ from $\mathbb{Z} \xrightarrow{\theta} R$. ring homo. & it is unique.

$1_{\mathbb{Z}} \longrightarrow 1_R$

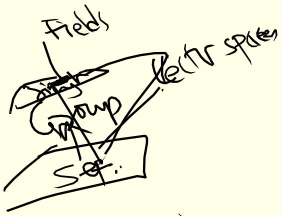
$n \rightarrow \underset{\text{notation}}{n \cdot 1_R} = \underbrace{(1_R + \cdots + 1_R)}_{n\text{-times}}$

$\Rightarrow$ $\forall R \; \exists! \, n$ s.t. $\mathbb{Z}/n\mathbb{Z} \subset R$. by 1st homo. thm.

$\Rightarrow$ Given F $\exists$ p a prime s.t. $\mathbb{Z}/p\mathbb{Z} \subset F$.

RCS

$\Rightarrow$ F is vector space on $\mathbb{Z}/p\mathbb{Z}$ of dim. n (say) $n < \infty$.



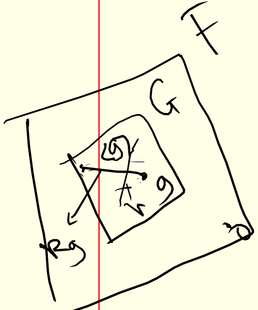
$\therefore \underbrace{\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p}_{n\text{-times}} \simeq F$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$

$\therefore |F| = p^n$ as a vector space & hence as a field !!

(Fact/Exercise/Thm/Prop)

→ ③ For any finite subgroup of F^* is cyclic.
where F is a field.

proof :- Let $G \subset F^* = F \setminus \{0\}$ be a finite subgroup
then any $g \in G$, its order is finite say k_g.



$\Rightarrow$ $\langle g \rangle$ the cyclic group gen by g has k_g elts
& each one of them satisfies $x^{k_g} = 1$.
$\Rightarrow$ G has at most one subgroup of order d $\forall\, d \mid |G|$
$\Rightarrow$ G is cyclic.

(Let $d \mid |G| \Rightarrow \exists$ at most $\phi(d)$ elts of order d in G
But every elt of G has some order.

$$|G| = \sum_{d \mid |G|} \#(\text{elts of order } d) \leq \sum_{d \mid |G|} \phi(d) = |G|$$

→ But. $\forall n$, $\sum_{d \mid n} \phi(d) = n$. elementary number theory Fact)

Given any field of order p^n, its characteristic is p.
& every non-zero elt must satisfy
$x^{p^n - 1} = 1$ (order of an elt divides order of the group)

$\Rightarrow$ every elt of F must satisfy
$x^{p^n} = x$

$\Rightarrow$ F is the collection of roots of $X^{p^n} - X$. as in (1).

$\therefore$ F is isomorphic to the field we constructed in (1).

Next level of natural questions.

(1) Given two finite fields $GF(p^n)$ & $GF(q^r)$ when do $GF(p^n) \subset GF(q^r)$?

if only if

Thm: Ans. (1) $q = p$ (2) $n \mid r$.

{ Remark:

$$\begin{array}{ccl} & F_2 & \\ d_2 & \mid & \\ & F_1 & \quad d_1 d_2 \\ d_1 & \mid & \\ & F = \mathbb{Z}/p & \end{array}$$

multi. property of deg }

$$\boxed{(X^n - 1) \text{ divides } (X^m - 1) \text{ iff } n \mid m}$$

(1) if $n \mid m$ then $X^m - 1 = X^{kn} - 1$

$$= (\underbrace{X^n}_{Y})^k - 1$$

$X^l - 1 = (X-1)(1 + X \cdots + X^{l-1})$

$$= (Y-1)(1 + Y + \cdots + Y^{k-1})$$

$$= (X^n - 1)(1 + X^n + X^{2n} + \cdots + X^{(k-1)n})$$

(2) conversely if $(X^n - 1)$ divides $(X^m - 1)$

Then $m = nq + r$. & continue $\to$ (Exercise)

we know that

Use this to prove the result.

• If $GF(p^n) \subset GF(q^r)$ clearly $q = p$ since
$ch(GF(p^n)) = p = ch\,GF(q^r) = q$.

• $\therefore$ $GF(p^n)$ is the ~~set~~ of roots of $x(x^{p^n-1}-1)$

$\cap$

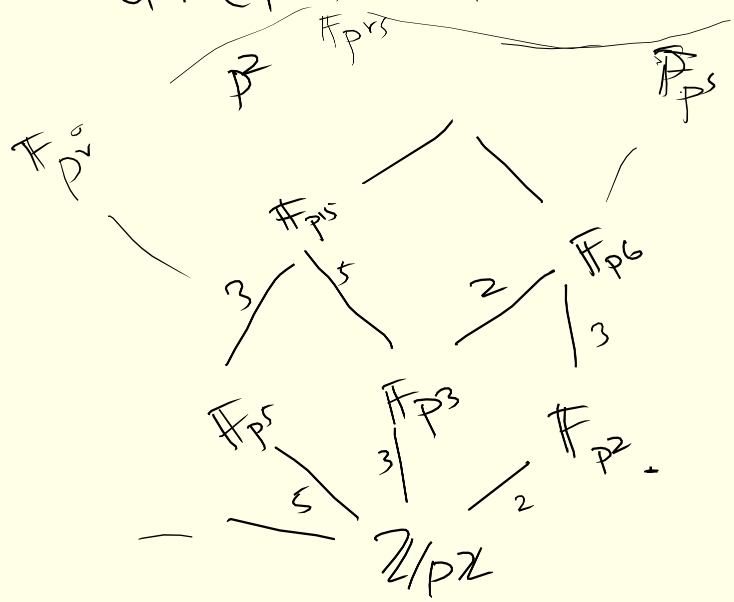
$GF(p^r)$ —— " —— $x(x^{p^r-1}-1)$

$\Rightarrow$ p^n-1 divides p^r-1.

$\Rightarrow$ $n \mid r$. QED.

—x—x—

$\mathbb{Z}/p$
$\|$
$GF(p) \subset GF(p^2) \subset GF(p^{\cancel{5}\ \text{odd no.}})$



$\mathbb{F}_{p^2} \not\subset \mathbb{F}_{p^{odd}}$

—x—x—x—

Counting over finite fields. next time!