Abstract Algebra III

This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat.

Finite fields

→ will change the problem that we do on Wednesday

we will do #4 then #3 if time

Sections 13.5 ← existence + uniqueness

14.3 ← Galois theory

We know that there are fields that are finite

the set of elements has finite cardinality.

because the quotient ring $\mathbb{Z}/p\mathbb{Z}$ p prime is a field.

$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$: rings/fields 2 operations

C_p: gp with one operation

$\# \mathbb{F}_p = p$

Are there more? Yes

Assume F is a finite field.

- We know that every field contains a prime subfield. Since F is finite, it cannot be $\mathbb{Q}$, because $\mathbb{Q}$ is infinite

  $\Rightarrow$ If F is finite, it has characteristic p for some prime p.

- F is then an extension of $\mathbb{F}_p$, which must be of finite degree.

(If the degree were infinite then F would be infinite)

So F has the structure of a finite-dimensional vector space over $\mathbb{F}_p$

$$\Rightarrow \quad \# F = p^n \qquad n = [F : \mathbb{F}_p]$$

so p^n choices for v

$v = (v_1, v_2, \ldots, v_n)$ $\quad v_i \in \mathbb{F}_p$ $\quad$ p choices

Now: Construct a field of size p^n for each p prime, n positive integer

Bonus: Construction will show such a field is unique.

Fix p a prime, consider the polynomial

$$x^{p^n} - x \in \mathbb{F}_p[x]$$

There exists K a splitting field for this polynomial over $\mathbb{F}_p$

$$\begin{array}{c} K \\ \Big| \\ \mathbb{F}_p \end{array}$$

$$\Omega = \{ \alpha \in K : \alpha^{p^n} - \alpha = 0 \}$$

i.e. the roots of $\boxed{X^{p^n} - X}$ in K

- how big is Ω?

  We know $\# \Omega \leq p^n$ since a polynomial of degree p^n has at most p^n distinct roots.

<u>Proposition</u> f has distinct roots iff $\gcd(f, f') = 1$.

$$\frac{d}{dx}\left(x^{p^n}-x\right) = \underbrace{p^n\, x^{p^n-1}}_{\underbrace{x^{p^n-1}+x^{p^n-1}+\dots+x^{p^n-1}}_{p^n \text{ times}}} - 1 = -1$$

because $p=0$ in K

$$\gcd\left(x^{p^n}-x, -1\right) = 1$$

$\Rightarrow$ $x^{p^n}-x$ has p^n distinct roots

$$\begin{array}{ccc} K & \supseteq & \Omega = \{\alpha \in K : \alpha^{p^n} - \alpha = 0\} \\ | & & \#\Omega = p^n \\ \mathbb{F}_p & & \end{array}$$

Claim Ω by itself is a field.

or Ω is a subfield of K

It suffices to show that if $\alpha, \beta \in \Omega$ then

1. $\alpha + \beta \in \Omega$
2. $\alpha\beta \in \Omega$
3. $\alpha^{-1} \in \Omega$
4. $-\alpha \in \Omega$
5. $0 \in \Omega$
6. $1 \in \Omega$

5 + 6 : $0^{p^n} - 0 = 0$ ✓ $1^{p^n} - 1 = 0$ ✓

2 : $\alpha, \beta \in \Omega \Rightarrow \alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$

then $\alpha\beta \in \Omega$ if $(\alpha\beta)^{p^n} = \alpha\beta$

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$$

3 : $\alpha \in \Omega$ $(\alpha^{-1})^{p^n} = \alpha^{-p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$

$\Rightarrow \alpha^{-1} \in \Omega$

④ $\alpha \in \Omega$ if $p=2$ then $-\alpha = \alpha$ so $-\alpha \in \Omega$

$\hookrightarrow \alpha + \alpha = 0$

if p is odd $(-\alpha)^{p^n} = -\alpha^{p^n} = -\alpha$

$\Rightarrow -\alpha \in \Omega$

$$\frac{p^n!}{k!(p^n-k)!} = \binom{p^n}{k} = 0 \quad 1 \le k \le p^n - 1$$

in any field of char p

⑤ $\alpha, \beta \in \Omega$ $$(\alpha+\beta)^{p^n} = \sum_{k=0}^{p^n} \binom{p^n}{k} \alpha^k \beta^{p^n-k}$$

$\Rightarrow \alpha + \beta \in \Omega$ $$= \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$$

K ← splitting field of $x^{p^n}-x$

$$\Omega = \{\alpha \in K : \alpha^{p^n} - \alpha = 0\}$$

$\mathbb{F}_p$

this is a field! it contains $\mathbb{F}_p$ and all the roots of $x^{p^n}-x$

I must have $\Omega = K$ since K was the smallest field containing $\mathbb{F}_p$ and the roots of $x^{p^n}-x$

$K = \Omega$ is a field of size p^n

$\Rightarrow$ there exists a field of size p^n for each p and n.

Observation: The identity $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ is true for all n, and for all $\alpha, \beta \in F$ if $\mathrm{Char}(F) = p$

" The freshman's dream"

Now suppose that F is another field of size p^n. From our earlier discussion, F is an extension of $\mathbb{F}_p$ of degree n.

Consider the multiplicative group $F^\times \overset{\text{as set}}{=} F - \{0\}$ (with operation multiplication)

Then $\# F^\times = p^n - 1$ and by a group theorem

$\Rightarrow \alpha \in F^\times, \quad \alpha^{p^n - 1} = 1$

Theorem I'm using:
If $\#G = n$ then $g^n = 1$ $\forall g \in G$

So $\forall \alpha \in F^{\times}$ i.e. $\forall \alpha \neq 0$ in F, $\alpha^{p^n - 1} = 1$

So $\alpha^{p^n} = \alpha$. Now this is true $\forall \alpha \in F$ since $0^{p^n} = 0$.

$\Rightarrow \forall \alpha \in F \quad \alpha^{p^n} - \alpha = 0$

$\forall \alpha \in F \quad \alpha^{p^n} - \alpha = 0$

so the polynomial $x^{p^n} - x$ splits completely in $F[x]$, which forces

$$\underbrace{\Omega}_{} = K \subseteq F$$

smallest field over which $x^{p^n} - x$ splits; inside any field where $x^{p^n} - x$ splits

$\Rightarrow K = F$ since both have size p^n

since the splitting field is unique up to isomorphism the field of size p^n is also

Separability vs Inseparability

- if $char(F)=0$ all extensions are separable
- if $F=\mathbb{F}_{p^n}$ any finite extension is separable

The polynomial x^5-1 over $\mathbb{F}_5$ is inseparable

$$x^5-1=(x-1)^5$$

To get inseparable extension need f irreducible and inseparable

That’s all for today!