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.

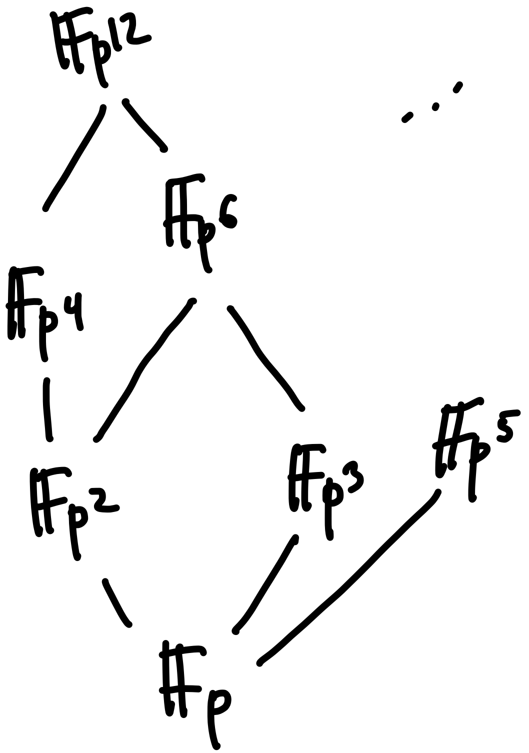
Finite fields

For all p a prime, n positive integer, there is exactly one finite field of order p^n up to isomorphism. These are all the finite fields that there are.

$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ iff $d \mid n$

these are the only containments

draw a lattice of subfields



We also saw that $\mathbb{F}_{p^n} / \mathbb{F}_p$ is Galois because splitting field of $X^{p^n} - X$ which is separable

Note: almost all of this is true with p replaced by $q = p^n$

- $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ iff $d \mid n$
- $\mathbb{F}_{q^n} / \mathbb{F}_q$ is Galois, it is the splitting field of $x^{q^n} - x$

$$
\begin{tikzcd}[arrows=-]
\mathbb{F}_{q^4} \arrow[dr] & & \mathbb{F}_{q^6} \arrow[dl] \arrow[dr] & & \\
& \mathbb{F}_{q^2} \arrow[dr] & & \mathbb{F}_{q^3} \arrow[dl] & \mathbb{F}_{q^5} \arrow[dll] \\
& & \mathbb{F}_q & &
\end{tikzcd}
$$

14.3 Galois theory

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \ni \sigma_p(\alpha) = \alpha^p$

① σ_p is a field automorphism of $\mathbb{F}_{p^n}$

② σ_p fixes $\mathbb{F}_p$ ✓

$\forall \alpha \in \mathbb{F}_{p^n},\ \alpha^{p^n} = \alpha$

$\forall \beta \in \mathbb{F}_p,\ \beta^p = \beta$

Let's show σ_p is a field automorphism

- field homomorphism $\leftarrow$ respect $+$, respect $\times$
- bijective $\leftarrow$ injective, surjective

- field homomorphism $\leftarrow$ respect $+$ ✓
  respect $\times$
- bijective $\leftarrow$ injective
  surjective

- $\sigma_p(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \sigma_p(\alpha)\sigma_p(\beta)$

- $\sigma_p(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p$

  true for any $\alpha, \beta \in K$, $\mathrm{char}(K) = p$

• σ_p is injective: Show the kernel is 1

Suppose that $\alpha \in \mathbb{F}_{p^n}$ $\quad \sigma_p(\alpha) = 1$

i.e. $\quad \alpha^p = 1$

i.e. $0 = \alpha^p - 1 = \alpha^p - 1^p = (\alpha - 1)^p$

$\Downarrow$

$\alpha = 1$

$\alpha = 1$ is the only element of $\mathbb{F}_{p^n}$ with $\alpha^p = 1$.

In a field, if $x^p = 0 \Rightarrow x = 0$

• $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ injective, $\mathbb{F}_{p^n}$ finite $\Rightarrow$ surjective

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \ni \sigma_p$ $\qquad$ $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

$\qquad\qquad\qquad\qquad\qquad\qquad \alpha \mapsto \alpha^p$

Notice that $\#\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$

j-fold composition

Claim: $\sigma_p \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ has order n

identity

Let $j>0$ be an integer, suppose that $\boxed{\sigma_p^j = 1 \text{ on } \mathbb{F}_{p^n}}$

this means that $\forall \alpha \in \mathbb{F}_{p^n}$ $\quad \sigma_p^j(\alpha) = \alpha$

$$((\alpha^p)^p)^{p\cdots} = \sigma_p^j(\alpha) = \alpha^{p^j}$$

Suppose that $j > 0$ is such that

$$\alpha^{p^j} = \alpha \qquad \forall\, \alpha \in \underbrace{\mathbb{F}_{p^n}}$$

$\alpha^{p^n} = \alpha$

$=$

$\sigma_p^n(\alpha)$

- $j = n$ ✓ $\Rightarrow$ the order of σ_p divides n

$\sigma_p^n = 1$

- if $j < n$, get a contradiction:

if $\alpha^{p^j} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$, for $j < n$

then the polynomial $x^{p^j}-x$ has p^n roots in $\mathbb{F}_{p^n}$, but this is impossible since $x^{p^j}-x$ has degree p^j and a polynomial of degree m has at most m distinct roots in any field

$\Rightarrow \sigma_p^n = 1$ in $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ but $\sigma_p^j \neq 1$ if $0<j<n$

So $\langle \sigma_p \rangle \leq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$

which has size n

$\Rightarrow \quad \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$

Note: • $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle \qquad \sigma_q(\alpha) = \alpha^q$

• We will use the notation σ_p for every field so

$\#\langle \sigma_p \rangle = d \leftarrow \sigma_p : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d} \qquad \sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \rightsquigarrow \#\langle \sigma_p \rangle = n$

- $$\begin{array}{cc} & \mathbb{F}_{p^n} \\ \frac{n}{d} & | \\ & \mathbb{F}_{p^d} \\ d & | \\ & \mathbb{F}_p \end{array}$$

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d}) = \langle \sigma_p^{\,d} \rangle$

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$

$$\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \big/ \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})$$

$$= \langle \sigma_p \rangle$$

this σ_p is the image of the other σ_p above in the quotient gp.

$\mathbb{F}_{p^n}/\mathbb{F}_p$ is finite and separable ($\Leftarrow$ Galois)

$q = p^r$

$\mathbb{F}_q$ = finite fld with q elem.

$\Rightarrow \exists\ \theta \in \mathbb{F}_{p^n}$ with $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$

θ is a primitive element

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \deg \underbrace{m_{\theta,\mathbb{F}_p}}$$

↳ irreducible polynomial of degree n over $\mathbb{F}_p$

Upshot: $\forall n \geq 1$ $\exists$ an irred. polynomial of deg n over $\mathbb{F}_q$

Note that $\theta^{p^n} = \theta$ since $\theta \in \mathbb{F}_{p^n}$

$\Rightarrow$ minimal polynomial of θ divides $x^{p^n} - x$

Note that if $d | n$ then $(x^{p^d} - x) \mid (x^{p^n} - x)$

if $\beta \in \mathbb{F}_{p^d}$, then $\beta \in \mathbb{F}_{p^n}$

Proposition 18

$$x^{p^n} - x = \prod_{d|n} \Big(\prod_{\substack{f \text{ irred of} \\ \deg d \text{ over } \mathbb{F}_p}} f \Big)$$

Example $p=2$, $n=2$ $d=1,2$

$$X^{p^n}-X = X^{2^2}-X = X^4-X = \begin{pmatrix}\text{product of}\\ \text{all irred}\\ \text{poly of deg } 1\end{pmatrix}\begin{pmatrix}\text{product of}\\ \text{all irred}\\ \text{poly of deg } 2\end{pmatrix}$$

$$= x(x-1)\boxed{\left(\text{all irred poly deg } 2\right)}$$

$$\frac{x^4-x}{x(x-1)} = \frac{x(x^3-1)}{x(x-1)} = \frac{\cancel{x}\,\cancel{(x-1)}\,\boxed{(x^2+x+1)}}{\cancel{x}\,\cancel{(x-1)}}$$

there is a unique irreducible polynomial of deg 2 over $\mathbb{F}_2$

To find irreducible polynomials of deg n over $\mathbb{F}_p$

factor

$$X^{p^n} - X$$

this is constructive

Plan:

Friday Nov 20: questions then Quiz 10

Monday Nov 23: lecture on separability
inseparability

Monday Nov 30: finish finite fields
HW 11 #4, 3

Wednesday Dec 2: Questions

Friday Dec 4: Questions + Quiz 11

Monday Dec 7 : final exam

That's all for today!

Math 331
373
395 A