MATH4302, Algebra II, 2022

Jiang-Hua Lu

The University of Hong Kong

Monday April 4, 2022

Second Lecture

Today

1. §3.2.6 : Finite fields, I

What we already know about finite fields:

- Most basic example: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number.
- $|\mathbb{F}_p| = p$.
- Every finite field F is an extension of $\mathbb{F}_p$, where $p = \mathrm{char}(F)$.
- If F is a finite field and $\mathrm{char}(F) = p$, then

  $$F \cong \mathbb{F}_p^n = \{(a_1, \ldots, a_n) : a_j \in \mathbb{F}_p\} \qquad \text{as a vector space over } \mathbb{F}_p,$$

  where $n = [F : \mathbb{F}_p]$. In particular, $|F| = p^n$.
- There there are no fields with 35 elements.

Lemma. If $|F| = p^n$ and $K \subset F$ a subfield, then $|K| = p^d$ for some $1 \le d \le n$ and $d|n$.

Proof. Being a subfield of F, K also has characteristic p. Let $d = [K : \mathbb{F}_p]$. Then

$$n = [F : \mathbb{F}_p] = [F : K][K : \mathbb{F}_p] = d[F : K]. \quad \Rightarrow d|n$$

◇

Example. If $|F| = 7^6$, then possible cardinalities of subfields of F are

$$7, 7^2, 7^3, 7^6.$$

Question. If $|F| = 7^6$, are there subfields of F with 7^2 or 7^3 elements?

Theorems to be proved: Let p be a prime number.

1. For any $n \geq 1$, there is one field, and only one up to isomorphism, with p^n elements, which is denoted as $\mathbb{F}_{p^n}$.
2. For each $n \geq 1$ and for each $d|n$, there is exactly one subfield of $\mathbb{F}_{p^n}$ which is $\mathbb{F}_{p^d}$.
3. A description of all irreducible polynomials over $\mathbb{F}_p$. for every prime p.

Question: How to construct $\mathbb{F}_{p^n}$

Main tools:

1. The quotient $\mathbb{F}_p[x]/\langle f \rangle$ for irreducible $f \in \mathbb{F}_p[x]$.
2. Splitting fields.

$\cancel{p=2}$ $\quad x^n - 2 \in \mathbb{F}_p[x]$

$p=7$

Recall the quotient construciton:

If $f(x) \in \mathbb{F}_p[x]$ is irreducible and has degree n, then $\mathbb{F}_p[x]/\langle f \rangle$ is a field with p^n elements.

Easy for small n. & small p

Example. There are exactly 4 quadratic polynomials in $\mathbb{F}_2[x]$: $f(x) = x^2 + ax + b$ with $a, b \in \mathbb{F}_2$:

$$x^2, \quad \underbrace{x^2+1}_{=(x+1)(x+1)}, \quad x^2 + x, \quad \boxed{x^2 + x + 1.}$$

Let $f(x) = x^2 + x + 1$, so

$$\mathbb{F}_2[x]/\langle f \rangle = \mathbb{F}_4 = \{0, 1, a, a+1\}.$$

Multiplication table:

$n=3$

Exercise: There are exactly two cubic irreducible polynomials in $\mathbb{F}_2[x]$:

$$f = \underline{x^3 + x + 1} \quad \text{and} \quad g \underline{= x^3 + x^2 + 1.}$$

Write down the addition and multiplication tables of

$$\mathbb{F}_8 = \mathbb{F}_2[x]/\langle f\rangle \quad \text{and} \quad \mathbb{F}_8' = \mathbb{F}_2[x]/\langle f\rangle$$

and show that $\mathbb{F}_8 \cong \mathbb{F}_8'$.

A fundamental fact about characteristic p (Every student's dream)

Lemma. If F is a field with $\mathrm{char}(F) = p > 0$, then

$$(a+b)^p = a^p + b^p, \qquad \forall a, b \in F.$$

Proof: Exercise to prove that

$$p \mid \binom{p}{k} \qquad k = 2, \cdots p-1.$$

cardinality

Lemma. If F is a finite field of ~~order~~ q, then every element $a \in F$ satisfies

$$x^q - x = 0.$$

Proof.

- If $a = 0$, ok.
- Assume that $a \neq 0$. Then $\underline{a \in F \backslash \{0\}}$ which is an abelian group with $q - 1$ elements.
- By Lagrange's Theorem, $a^{q-1} = 1$, so $a^q = a$.

$\diamond$

We fix a prime number p throughout. Let $n \geq 1$ be an integer.

Theorem

A finite field F has order p^n if and only if it is isomorphic to the splitting field over $\mathbb{F}_p$ of

$$f(x) = x^{p^n} - x \in \mathbb{F}_p[x].$$

Proof. Assume first that F is a field of order p^n.

- The prime field of F is $\mathbb{F}_p$, so F is an extension of $\mathbb{F}_p$;
- By previous lemma, every $\alpha \in F$ is a root of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$;
- f can have at most p^n roots in F, so $F = R_f$, the set of all roots of f in F;
- Thus f completely splits in $F[x]$, and $F = \mathbb{F}_p(R_f)$ is a splitting field of f over $\mathbb{F}_p$.

Proof Cont'd:

Conversely, let F be a splitting field of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. Let R be the set of all roots of f on F. Then $F = \mathbb{F}_p(R)$

- Since $f'(x) = p^n x^{p^n - 1} - 1 = -1$ has no roots in F, f has no repeated roots in F.
- Since $\deg(f) = p^n$, f has exactly p^n roots in F, i.e. $|R| = p^n$.
- For any $a, b \in R$, $a^{p^n} = a$ $b^{p^n} = b$

$$\underline{(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b}, \quad (ab)^{p^n} = a^{p^n} b^{p^n} = ab,$$

and if $b \neq 0$, then $(1/b)^{p^n} = 1/b$. Thus R is a subfield of F.

- Moreover, $\mathbb{F}_p \subset R$. Thus $F = \mathbb{F}_p(R) = R$ because R is a subfield. Conclude that

$$|F| = |R| = p^n.$$

$\mathbb{F}_p(R)$ is the smallest subfield of F containing $\mathbb{F}_p$ & R

So $R \subset \mathbb{F}_p(R) \supseteq R$

Q.E.D.

Corollary

For any prime number p and any integer $n \geq 1$,

part 2 of Thm + existence of splitting

1. *there exist fields with p^n elements;*
2. *any two fields with p^n elements are isomorphic.* part 1 of Thm + uniqueness

Proof. Statements follow directly from existence and uniqueness of splitting fields.