Tower theorem

Jiang-Hua Lu

The University of Hong Kong

MATH4302 Algebra II, HKU

Monday, March 24, 2025

In this file:

- §3.1.2: Degrees of field extensions and the Tower Theorem

§3.1.2: Degrees of field extensions.

Key idea: If $K \subset L$ is a field extension, then L as a vector space over K.

Definitions.

1. The degree of a field extension $K \subset L$ is the dimension of L as a vector space over K and is denoted as $[L : K]$.
2. If $[L : K] < +\infty$, call L a finite extension of K;
3. If $[L : K] = +\infty$, call L an infinite extension of K.

Example. For a field F,

$$F(x) = \left\{ \frac{f(x)}{g(x)} : \ f, g \in F[x], g \neq 0 \right\}$$

is the field of fractions of $F[x]$, and is an infinite extension of F.

The fundamental example again:

Lemma. If $\cancel{p}f(x) \in K[x]$ is irreducible and has degree n, the

$$L = K[x]/\langle \cancel{p}f(x)\rangle$$

is a field extension of K of degree n.

If $K = \mathbb{F}_p$ and if $f(x) \in K[x]$ is irreducible, then L is a finite field of order p^n

$\forall$ given p, $p \neq 2$, do we always have a quadratic irred. poly $f(x)$ over $\mathbb{F}_p$?

The Tower Theorem.

The Tower Theorem: If $K \subset L$ and $L \subset M$ are finite extensions, then $K \subset M$ is a finite extension and

$$[M : K] = [M : L][L : K].$$

Pf: let $a_1, \cdots, a_m$ be a basis of M over L

let $b_1, \cdots b_l$ be a basis of L over K

Let $x \in M$ be arbitrary. Then $\exists\, \lambda_1, \cdots, \lambda_m \in L$

s.t. $x = \lambda_1 a_1 + \cdots + \lambda_m a_m$

For each $j = 1, \cdots, m$, we have

$$\lambda_j = \mu_{j1} b_1 + \cdots + \mu_{jl} b_l$$

where $\mu_{j1}, \cdots, \mu_{jl} \in K$. Thus

$$x = \sum_{j=1}^{n} \lambda_j a_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{l} \mu_{ji} b_i \right) a_j = \sum_{i,j} \underset{\uparrow}{\underset{K}{\mu_{ji}}} \underbrace{b_i a_j}_{M}$$

Next, show that $\{ b_i a_j : i = 1, \dots l, j = 1, \dots m \}$ is linearly indep. over K.

Suppose $\sum_{i,j} \xi_{ij} b_i a_j = 0 \Rightarrow \dots$

//

Orders of finite fields

Theorem. If K is a finite field, then $|K| = p^n$ for some prime number p and some integer n.

Pf: Let p be the charateristic of K.

So K is a finite field extension of

$\mathbb{F}_p \stackrel{\text{def}}{=} \mathbb{Z}/p\mathbb{Z}$

If $[K:\mathbb{F}_p] = n$, then $K \underset{\text{bijection}}{\simeq} (\mathbb{F}_p)^n$

So $|K| = p^n$.