April 16

HW: $x^{p-1}+x^{p-2}+\cdots+x+1$ irred.

① $= \dfrac{x^p-1}{x-1}$

② translate $x \mapsto x+1$

③ $p \mid \binom{p}{i}$ $i=1,\dots,p-1$

$\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$

Plan

- recap
- algebraic field ext.
- tower of field ext.

Recap

We have notion of a field extension

$K \subset L$ $\qquad$ $K \xrightarrow{\varphi} L$ ← ring hom

$K \xrightarrow{\sim} \varphi(K) \subset L$

- <u>degree</u> $[L:K] = \dim_K L$
- say $K \subset L$ <u>simple</u> if $\exists\, \alpha \in L$ such that $L = K(\alpha)$

<u>Example</u> Let K any field & $f(x) \in K[x]$ irred. poly

$\rightsquigarrow L = K[x]/(f(x))$ field

$\rightsquigarrow K \longrightarrow L$ field ext

$\rightarrow [L:K] = \deg f$

<u>Defn</u> Given field ext $K \subset L$ we say <u>$\alpha \in L$ algebraic over K</u> if $\exists\, 0 \neq p(x) \in K[x]$ s.t. $p(\alpha) = 0$

- Say $\alpha \in L$ is <u>transcendental</u> if α not algebraic.

Ex: $\pi \in \mathbb{C}$ not alg./$\mathbb{Q}$

<u>Defn</u> If $\alpha \in L$ algebraic over K, then the <u>minimal polynomial of α over K</u> is a monic polynomial $p(x) \in K[x]$ such that

(a) $p(\alpha) = 0$

(b) if $g(x) \in K[x]$ w/ $g(\alpha) = 0$ then $p \mid g$.

<u>Prop</u>: The min poly $p(x)$ of α exists!

Moreover, it is irreducible & $\deg p(x) = [K(\alpha):K]$.

Picture

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$$

$i \in \overline{\mathbb{Q}}$, $\pi i \in \mathbb{C}$, $\pi, \pi i \notin \overline{\mathbb{Q}}$

$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \text{ algebraic}/\mathbb{Q}\}$

Ques: Why is $\overline{\mathbb{Q}}$ a field?

Ex: We've already seen that $\sqrt{2}+\sqrt{3}$ is algebraic.

$\to$ Given $f(x)$ w/ $f(\alpha)=0$
$g(x)$ w/ $g(\beta)=0$

Can you build another poly $h(x)$ s.t. $h(\alpha+\beta)=0$?

Towers of field exts

Suppose $F \subset K \subset L$

Prop: $[L:F] = [L:K][K:F]$

Ex: $\mathbb{Q} \underset{2}{\subset} \mathbb{Q}(\sqrt{2}) \underset{2}{\subset} \mathbb{Q}(\sqrt{2},\sqrt{3})$, with $\mathbb{Q} \xrightarrow{4} \mathbb{Q}(\sqrt{2},\sqrt{3})$

Pf: View L additive group (it is abelian)

$K/F \subset L/F$

Gp theory $\Rightarrow$ $\underbrace{(L/F)}/\underbrace{(K/F)} = \underbrace{L/K}$

all vector spaces $/F$

$$[L:F] = \dim_F L$$

Sketch another proof

- Let $n=[K:F] \Rightarrow \exists$ basis $x_1,\dots,x_n$ of F over K
- Let $m=[L:K] \Rightarrow \exists$ basis $y_1,\dots,y_m$ of L over K

Strategy: find basis of size $n \cdot m$ of L over F

Guess: basis is $\{x_i y_j\}$ $i=1,\dots,n$, $j=1,\dots,m$

Guess is correct! ✓

Sketch another proof

- Let $n = [K:F] \Rightarrow \exists$ basis $x_1, \dots, x_n$ of F over K
- Let $m = [L:K] \Rightarrow \exists$ basis $y_1, \dots, y_m$ of L over K

Strategy: find basis of size $n \cdot m$ of L over F

Guess: basis is $\{x_i y_j\}$ $i = 1, \dots, n$, $j = 1, \dots, m$

Guess is correct!

Need $\quad [F \subset K \subset L]$

- $\{x_i y_j\}$ spanning set
- $\{x_i y_j\}$ lin indep.

Let $\alpha \in L$.

- Know $\alpha = a_1 y_1 + \dots + a_m y_m$, $a_i \in K$

Write $a_i = b_{i1} x_1 + \dots + b_{in} x_n$

$\rightsquigarrow$ expand!

$\Rightarrow \alpha = (b_{11} x_1 + \dots + b_{1n} x_n) y_1 + \dots$
$(b_{m1} x_1 + \dots + b_{mn} x_n) y_m$
$= \sum b_{ji} x_i y_j$

Shows spanning.

Defn
- Say $K \subset L$ algebraic field ext if every $\alpha \in L$ is alg. over K.
- Say $K \subset L$ finite if $|L:K|$ finite
- Say $K \subset L$ trans. if not algebraic

Ex: $\mathbb{Q} \underset{\text{alg.}}{\subset} \overline{\mathbb{Q}} \underset{\text{trans}}{\subset} \mathbb{C}$

Lemma: $K \subset L$ finite $\Rightarrow K \subset L$ algebraic

Pf:
- Know L has a finite basis over K.
- Need to show: $\forall \alpha \in L$, $\exists$ poly $0 \neq f(x) \in K[x]$ s.t. $f(\alpha) = 0$

Comments
1. $\underset{\text{finite}}{\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})}$ $\quad \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$ is algebraic, but why?
2. Special case $K \subset L = K(\alpha)$ $\quad (L = K[x]/(f))$

Take powers!

Consider $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \dots\} \subset L$

Since $[L:K] = d$ finite

know $\underbrace{\{1, \alpha, \dots, \alpha^d\}}_{\text{d+1 elements}}$ lin. dependent

$\Rightarrow \exists\, a_0, \dots, a_d \in K$ not all zero such that

$a_d \alpha^d + \dots + a_0 = 0$

$\Rightarrow$ Define $f(x) = \underset{\neq 0}{a_d} x^d + \dots + a_0 \in K[x]$

$f(\alpha) = 0$ ✓