Math 491, Thursday, April 2, Chapter 21 Fields

Fri – Chapter 21 Ruler / Compass

Mon – Problem session
Sage 21

Sun Project Proposal
11:59 PM

Tue – Exam 3
Chapter 20/21

Theorem E/K finite extension, K/F finite extension

$\Longrightarrow$ E/F is finite extension

$$[E:F] = [E:K][K:F]$$

E — $\beta_1, \beta_2, \beta_3 \ldots, \beta_m \in E$ basis

$[E:K]$

K — $\alpha_1, \alpha_2 \ldots \alpha_n \in K$ basis

$[K:F]$

F

$[E:F]$

Proof Outline

Show $\{\alpha_i \beta_j \mid 1 \le i \le n,\ 1 \le j \le m\} \subseteq E$
is a basis for E/F of size mn

Theorem E/F, $\alpha \in E$ algebraic over F w/ min poly $p(x)$
$\beta \in F(\alpha)$ w/ min poly $q(x)$. Then degree of q divides degree p.

Proof

$$\text{degree } p(x)\left[\begin{array}{c} F(\alpha) \\ | \\ F(\beta) \\ | \\ F \end{array}\right.\quad \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right] \text{degree } q(x)$$

$$\underbrace{[F(\alpha):F]}_{\text{degree } p(x)} = [F(\alpha): F(\beta)]\underbrace{[F(\beta):F]}_{\text{degree } q(x)}$$

Theorem E/F. The following are equivalent

1) E is a finite extension of F

2) There exists finite list $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ so that
$E = F(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n) = \Big(\big((F(\alpha_1))(\alpha_2)\big)(\alpha_3) \cdots (\alpha_n)\Big)$

3) tower of extensions

$$\begin{array}{c} E \\ \vdots \\ F(\alpha_1, \alpha_2) \\ | \\ F(\alpha_1) \\ | \\ F \end{array}$$

Algebraic Closure

Theorem E/F. Set of all algebraic elements in E that are algebraic over F form a field.

Question α algebraic $\Rightarrow$ $p(\alpha)=0$, $p(x)\in F[x]$

β algebraic $\Rightarrow$ $q(\alpha)=0$, $q(x)\in F[x]$

$\alpha+\beta$ algebraic ??? what polynomial?

Sage has QQbar ($\overline{\mathbb{Q}}$) all algebraic elements over $\mathbb{Q}$.

"$\sqrt{3}$" x^2-3

$\Rightarrow$ $\sqrt{2}+\sqrt{3}\in\overline{\mathbb{Q}}$ min poly of $\sqrt{2}+\sqrt{3}$?

"$\sqrt{2}$" x^2-2

$\mathbb{A}$ = algebraic real field = AA ← Sage

real roots of polynomials in $\mathbb{Q}[x]$.

Defn A field F is algebraically closed if every root of every polynomial in $F[x]$ is in F.

Ex $\mathbb{R}$ is not algebraically closed x^2+1 **Ex** $\mathbb{C}$ is algebraically closed

Theorem F algebraically closed if every nonconstant polynomial factors into linear factors.

Splitting Fields

Defn $p(x) \in F[x]$, then E is a splitting field for $p(x)$ if ① E extension of F ② $p(x)$ factors into linear factors over ~~in~~ E ("splits"), ③ no subfield of E has these properties.

Fact splitting field always exists, unique up to isomorphism. "the splitting field of $p(x)$"