Algebra I Algebraic extensions: 13.2–13.3.

- OH shift
- HW situation
- Exam grading
- Exam: Cumulative

Finish Last Wks,

Ex: $\mathbb{Q}(\sqrt{d})$ $d>0$.

Can "embed" in $\mathbb{R}$ 2 ways: $\sqrt{d}$ = "usual $\sqrt{d}$"
(alg. # theory) $\sqrt{d} = -\sqrt{d}$.

- $\mathbb{Q}(\sqrt[3]{2})$ has one root of x^3-2, misses some;

say adjoin. pos $\sqrt[3]{2} \in \mathbb{R}$, misses ω. $\sqrt[3]{2}, \omega^2\sqrt[3]{2} \in \mathbb{C}$

Adjoining the diff. roots are ≅ situations..

Useful gen. (for Galois theory).

Th$^{\cong}$: $\varphi: F \xrightarrow{\sim} F'$ (field ≅)

$p \in F[x]$ irred, $p' = \varphi(p)$ (apply φ to coeffs.).

α a root of p in ext^{n}, β of p'. Then $\exists \sigma$:

$$\begin{array}{ccc} \sigma: F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ \cup & & \cup \\ F & \xrightarrow[\varphi]{\sim} & F' \end{array}$$

Pf: φ induces ~~from.~~ from: $F[x] \to F'[x]$

apply φ to coeffs.

check $(p) \longmapsto (p')$

quotient out by these (max$^{\text{l}}$) ideals

(gives) $\rightsquigarrow$ $F[x]/(p) \xrightarrow{\sim} F'[x]/(p')$

$\cong$ $F(\alpha)$ $\cong$ $F(\beta)$

restriction = φ: Clear.

(1)

Def^n : L/K. field ext^n

- $\alpha \in L$ is algebraic $/K$ if $\exists\ p(x) \in K[x]$ non-zero poly, $p(\alpha) = 0$.
  otherwise, α is called transcendental $/K$.
- L/K is algebraic if all $\alpha \in L$ are alg., else transc.

Ex : $\bar{\mathbb{Q}}/\mathbb{R}$ is alg.
- $\mathbb{R}/\mathbb{Q}$ is transc. (e.g. π isn't alg.)

If $\alpha \in L$ is alg $/K$,

$I_\alpha = \{ p(x) \in K[x] \mid p(\alpha) = 0 \}$ is an ideal in $K[x]$ (non-zero)

$\Rightarrow I_\alpha = (p_\alpha(x))$ some nonzero de poly $p_\alpha \in K[x]$.

$p_\alpha(x)$ is the minimal poly of α/K.

Prop : p_α is irred.

gen. of ideal in E.D. $K[x]$ is an elt. of minimal degree

Pf : If $p_\alpha = g \cdot h$, either $g(\alpha) = 0$ or $h(\alpha) = 0$.

(minimality) p_α here?

smaller degree $\Rightarrow$ not a gen. of (p_α)

$\Rightarrow (p_\alpha) \subsetneq (g)$ ~~$= (p_\alpha)$~~ $*$ ☒

deg p_α = degree of α

For $\alpha_1, \dots, \alpha_n \in L$, let

$K[\alpha_1, \dots, \alpha_n]$ = smallest subring of L cont. $K, \alpha_1, \dots, \alpha_n$

$K(\alpha_1, \dots, \alpha_n)$ = " subfield " " "

Th= If $\alpha \in L$ is alg/k, $k[\alpha] = k(\alpha)$.

If $\deg p_\alpha(x) = n$, every elt. of $k(\alpha)$ can be written uniquely as

$$c_{n-1}\alpha^{n-1} + \dots + c_1\alpha + c_0, \quad c_i \in k,$$] saw

and $k(\alpha) \cong k[x]/(p_\alpha)$.] saw

Pf: Define $\varphi_\alpha : k[x] \to k(\alpha)$ eval. at α.

$\ker(\varphi_\alpha) = (p_\alpha)$, by def^n, $\operatorname{im}(\varphi_\alpha) = k[\alpha]$

On the other hand, $\operatorname{im}(\varphi_\alpha) \cong k[x]/(p_\alpha)$ is a field

So $k[\alpha] = k(\alpha)$. [Reduce mod p_α $\Rightarrow 1, \dots, \alpha^{n-1}$ span. Subtracting two such expressions gives uniqueness (E-Z) (minimal deg)] clear

Cor: If $\alpha \in L$ is alg./k of deg. n, $k(\alpha)/k$ is n-dimensional ext^n, basis $1, \alpha, \dots, \alpha^{n-1}$!

Direct

Th Cor: If $\alpha \in L$,

α alg./$k \iff k(\alpha)/k$ $[k(\alpha):k] < \infty$.

Pf: α alg. $\Rightarrow n = [k(\alpha):k] < \infty$ by above

$\Rightarrow$ ~~every $\beta \in L$ sat. a poly of deg $< n$~~

since ~~$1, \beta, \dots, \beta^n$ lin. dep.~~

Conversely, $k(\alpha)/k$ finite $\Rightarrow \alpha$ sat. a poly of deg $< n$:

(if ext^n has deg n, the $n+1$ elts $1, \alpha, \dots, \alpha^n$ are lin. dep $\Rightarrow$ rel^n)

(powers of α are $1, \alpha, \dots, \alpha^n$, a lin. comb.)

Ex: $K = \mathbb{F}_2$. $g(x) = x^2 + x + 1$

$L = \mathbb{F}_2[x]/(g)$.

Let $\vartheta = \bar{x}$. Then $[L:K] = 2$, so $1, \vartheta$ a basis for L/K. Note that $g(\vartheta) = 0$.

$L = \{a + b\vartheta : a, b \in \mathbb{F}_2\}$ $\vartheta^2 = \vartheta + 1$

$(a + b\vartheta)(c + d\vartheta) = (ac + bd) + (ad + bc + bd)\vartheta$

To find $\vartheta(1+\vartheta)^{-1}$, e.g. use Euclidean alg. to find $A, B \in \mathbb{F}_2[x]$, $A \cdot (1+x) + B \cdot (x^2+x+1) = 1$

Then $A(\vartheta)(1+\vartheta) = 1$ in K

Rem: $x^2 + x + 1 = x(x+1) + 1$

$\Rightarrow A(x) = -x$, $B(x) = 1$, $\Rightarrow -\vartheta(1+\vartheta) = 1$ in L.

Thm: $F \subseteq K \subseteq L$ fields

$\{\alpha_i\}_{i \in I}$ basis L/K

$\{\beta_j\}_{j \in J}$ basis K/F

Then $\{\alpha_i \beta_j\}_{\substack{i \in I \\ j \in J}}$ basis L/F.

Cor: $[L:F] = [L:K] \cdot [K:F]$. (Even if $= \infty$ possibly)

Pf: Span: Can write $\gamma \in L$ as $a_1 \alpha_1 + \cdots + a_m \alpha_m$, $a_i \in K$

$a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n$, $b_{ij} \in F$.

Lin. indi: If $\sum_{i,j} b_{ij}\alpha_i\beta_j = 0$, $b_{ij} \in F$ (define by eq = as above)

2p terms then $a_1\alpha_1 + \cdots + a_m\alpha_m = 0$ with $a_i \in K$

$\Rightarrow$ all $a_i = 0$. But $a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n$

$\Rightarrow$ all $b_{ij} = 0$.

(α_i basis of L/K) (β_i basis of K/F)

Ex: $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$

$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$

Pf: $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ is divis. by 6.

$\mathbb{Q}(\sqrt{2})$ (a) | (n) $\mathbb{Q}(\sqrt[3]{2})$ (b)

$\mathbb{Q}(\sqrt{2})$ / 2 / $\mathbb{Q}$ (min poly x^2-2)

$\mathbb{Q}$ / 3 / $\mathbb{Q}(\sqrt[3]{2})$ (min poly x^3-2)

$n = a \cdot 2 = b \cdot 3$

$\Rightarrow 2, 3 \mid n \Rightarrow 6 \mid n$.

But $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2}) \Rightarrow \mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2})$ too small!!

Thm: If L/K is a field ext^n, $\alpha_1, \ldots, \alpha_n$ alg./K, then $K(\alpha_1, \ldots, \alpha_n)$ is a finite alg. ext^n of K.

pf: α_i alg./$K \Rightarrow \alpha_i$ alg/$K(\alpha_1, \ldots, \alpha_{i-1})$ (still sat. a poly. eq = are the biggest free 0)

$\Rightarrow [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})] < \infty$

By last cor: $[K[\alpha_1, \ldots, \alpha_n], K] < \infty$ &

$\Rightarrow K[\alpha_1, \ldots, \alpha_n]/K$ algebraic (as finite)

Cor: L/K. The set of elts of L which are alg/K (apply Thm to every ext.) is a field.

Pf: $\alpha, \beta \in L$ alg/$K \Rightarrow K(\alpha, \beta, \ldots)$ is alg. ext^n of K

This ext^n contains $\alpha \pm \beta$, $\alpha\beta$, α^{-1} are all alg. $\in L$.

So $\alpha \pm \beta$, $\alpha\beta$, α^{-1}

Ex: $\sqrt{2}+\sqrt[3]{2}$ is alg. $/\mathbb{Q}$.

$\exists$ subfield $\bar{\mathbb{Q}} \subseteq \mathbb{C}$ of all alg. complex nos.
$[\bar{\mathbb{Q}} : \mathbb{Q}]$ is countably ∞.

Cor: L/K finite $\Leftrightarrow$ L gen. by finitely many alg. elts.

Thm: $p(x) \in K[x]$ monic, irreducible, and $L = K(\alpha)$, $L' = K(\alpha')$ are two simple alg. extns with $p(\alpha) = p(\alpha') = 0$, then $\exists$ field $\cong$ $\varphi : L \to L'$, $\alpha \mapsto \alpha'$ fixing K. Now Galois theory...

Skip!

Pf: Suffices to prove $\exists$ isom. $\bar{\varphi} : K[x]/(p) \to L$ fixing K. (skip pf! we already know this!)
$\bar{x} \longrightarrow \alpha$.

Thm: alg/alg = alg. ie. L/K alg, K/F alg. $\Rightarrow L/F$ alg.

Pf: Let $\alpha \in L$. Write $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$, $c_i \in K$ (hence alg $/F$)

Then $F \subseteq F(c_0, \ldots, c_{n-1}) \subseteq F(c_0, \ldots, c_{n-1}, \alpha)$,

$[F(c_0, \ldots, c_{n-1}) : F] < \infty$? → See next pg

$\Rightarrow [F(\alpha, c_0, \ldots, c_{n-1}) : F] < \infty \Rightarrow \alpha$ alg. $/F$.

Ex: Every root of $x^3 + \sqrt{2}x - \sqrt[3]{7}$ in $\mathbb{C}$ is alg $/\mathbb{Q}$.

~~a few more ex next time from notes~~

Pf. (alg/alg = alg)

L
|
K
|
F

$x \in L$. alg./K

$\Rightarrow \exists\ a_0, \dots, a_n \in K$ s.t. $a_0 x + \dots + a_n x^n = 0$.

Let $E = F(a_0, \dots, a_n)$.

E/F is f.g. and alg ebraic.

we proved this $\Rightarrow [E : F] < \infty$.

$E(x)/E$ simple (primitive) + alg.

also fin. te.

$E(x)$

$| < \infty \Rightarrow E(x)/F$ finite

E

$| < \infty$

F

$\Rightarrow$ x contained in a fin. ext $/K$

$\Rightarrow E(x)/F$ alg.

$\Rightarrow$ x alg. /F.

Extra time alg integers

so $\exists$ monic poly/$\mathbb{Q}$.

$\mathcal{O}_K$ K = # field. fin. ext of $\mathbb{Q}$.

$\mathcal{O}_K$ = ring of mb. in K = alg in $\mathbb{Z} \cap K$.

$K = \mathbb{Q}(\sqrt{D})$, $\mathcal{O}_K = \mathbb{Z}[\omega]$ $\omega = \sqrt{D}$ $D \equiv 2,3$

$\frac{1+\sqrt{D}}{2}$ $D \equiv 1$

$K = \mathbb{Q} \to \mathcal{O}_K = \mathbb{Z}$.

$\zeta_n = e^{\frac{2\pi i}{n}}$ n^{th} rt of 1, O.U. $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$

not always so simple!

ring of mb. = Ded domain

UFD $\Leftrightarrow$ PID

class #5.