lecture 10, mostly following Friedman's notes on Extensions of fields.

$F \subset E$ $\quad E/F$ $\quad \alpha \in E$

$\alpha \nearrow$ transcendental $/F$ $\quad [F(\alpha):F]$ ∞ degree

$F[\alpha]$ $\quad 1, \alpha, \alpha^2, \ldots$

$F(\alpha)$ $\quad$ lin. indep $/F$

$\searrow$ algebraic $/F$ $\quad \alpha$ root of $p(x) \in F[x]$

$p(\alpha) = 0$ in E, take irred

$$F \subset F(\alpha) = F[x]/(p(x))$$

$$F(\alpha) \subset E.$$

$F = \mathbb{Q}$ $\quad \underline{x^n - a}$ $\quad \underline{\sqrt[n]{a}} \in \overset{E}{\overset{\parallel}{\mathbb{C}}}$ $\quad a \in \mathbb{Q}$

root $\Leftarrow$ algebraic $/\mathbb{Q}$.

$F(\sqrt[n]{a})$

most $\mathbb{C}$ are transcendental

π, e.

__Def__ E/F $\quad E$ - alg. extension of F if $\forall \alpha \in E$

α is algebraic $/F$.

If E/F is finite $\quad [E:F] < \infty$ $\Rightarrow$ E is alg $/F$

$= n$

$\Leftarrow$ not necessarily $\quad \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$

∞ deg. extension of $\mathbb{Q}$

$[E:F] = [E:F(\alpha)][F(\alpha):F]$ $\qquad \alpha \in E$

fin

$F \subset F(\alpha) \subset E$

int. field

<u>Prop</u> E/F. Let $\alpha, \beta \in E$ algebraic $/F$.

Then $\alpha \pm \beta$, $\alpha\beta$, α/β $(\beta \neq 0)$ are algebraic over F.

smallest field in E contains F, α, β.

<u>Proof</u> $\underbrace{F \subset F(\alpha)}_{n} \subset \underbrace{F(\alpha)(\beta)}_{k} = F(\alpha, \beta)$

$n = \deg(\operatorname{irr}(\alpha, F))$ $\qquad [F(\alpha):F] = n$

$[F(\beta):F] = m$ $\qquad q(x) = \operatorname{irr}(\beta, F)$.

$\deg q(x) = m$

β $\qquad F(\alpha)$

$r(x) = \operatorname{irr}(\beta, F(\alpha))$

$r(x) \mid q(x)$ $\qquad \deg r \leq \deg q$

coeff in $F(\alpha)$ $\qquad$ coeff in F

$k = \deg r \leq m = \deg q$.

$[F(\alpha,\beta):F] = \underbrace{[F(\alpha,\beta):F(\alpha)]}_{k}\underbrace{[F(\alpha):F]}_{n} \leq$

$\leq nm$ $\qquad k \leq m$

γ - expression from α, β $\qquad \gamma \in F(\alpha, \beta)$.

$$[F(\gamma):F] \le \underset{\deg\alpha}{n}\,\underset{\deg\beta}{m}$$ □

$$\frac{h(\alpha,\beta)}{g(\alpha,\beta)\neq 0} \in F(\alpha,\beta) \quad \deg \le nm$$

$\mathbb{Q}\subset\mathbb{R}\subset\underline{\mathbb{C}}$

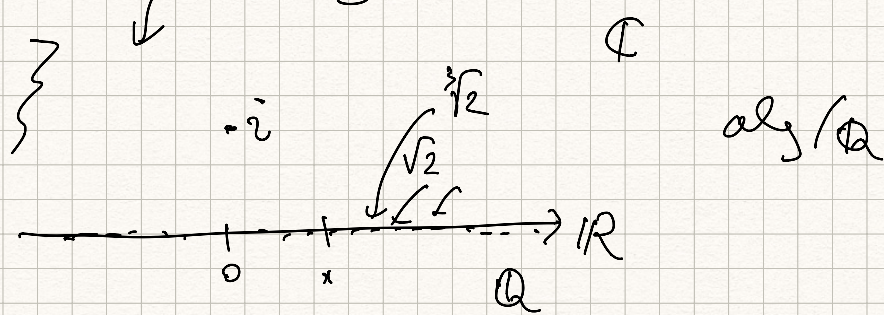
$\sqrt[n]{a},\ a\in\mathbb{Q}$ — alg/$\mathbb{Q}$.

$\sqrt[3]{4}+\sqrt{7}-5\sqrt{11}-\frac{7}{2}\sqrt[7]{9}\dots$ alg/$\mathbb{Q}$.

$\sqrt{2}+\sqrt{3}$ $\quad x^4-10x^2+1$ $\quad$ high deg irr.

$\sqrt{2}-\sqrt{3}\,i+(3-2i)\sqrt[4]{7}\in\mathbb{C}$

alg/$\mathbb{Q}$.



$\mathbb{Q}^{alg}\subset\mathbb{C}$ $\quad \overline{\mathbb{Q}}$ $\quad$ all complex #s alg/$\mathbb{Q}$.

subfield. $\quad \mathbb{Q}^{alg}$ has countably many elements. $\mathbb{C}\setminus\mathbb{Q}^{alg}$ has uncountably many.

$F \subset E$ alg. closure of F in E.

$\overline{F}_E = \{ \alpha \in E : \alpha \text{ is alg} / F \}$

Prop $\overline{F}_E$ is a subfield of E.

$\mathbb{Q}^{alg} \subset \mathbb{C}$

Prop E/F is finite $\Leftrightarrow$ $\exists\, \alpha_1 \ldots \alpha_n \in E$, alg $/F$
such that $\underline{E = F(\alpha_1, \ldots, \alpha_n)}$.

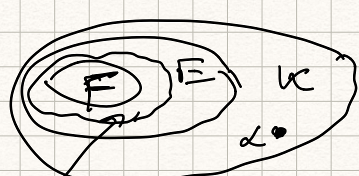
$$[F(\alpha_1, \alpha_2) : F] = [F(\alpha_1, \alpha_2) : F(\alpha_1)]\,[F(\alpha_1) : F]$$

$$\wedge\!\!|$$

$[F(\alpha_2) : F] \leftarrow$ fin. because α_2 is alg $/F$

Lemma $F \subset E \subset K$, Suppose $\underline{E/F \text{ is algebraic}}$, $\alpha \in K$. Then

α is alg $/F$ $\Leftrightarrow$ α is alg over E.



$\Rightarrow$ obvious.

$\Leftarrow$

$$\operatorname{Irr}(\alpha, E) = x^n + \underline{a_{n-1}}\, x^{n-1} + \cdots + a_0$$

$\Uparrow \Uparrow$

$E E$

$F(a_0, a_1 \ldots a_{n-1})$

$a_i \in E$, alg $/F$

α alg $/ F(a_0, \ldots a_{n-1})$

$F(a_0, a_1, \ldots a_{n-1}) \subset E$

$[F(a_0, \ldots a_{n-1}) : F] < \infty$ finite degree

$F \subset F(a_0, \ldots a_{n-1}) \subset E \subset K.$

$F(a_0, \ldots a_{n-1})(\alpha) = F(a_0, \ldots a_{n-1}, \alpha)$

a finite extension of F.

$$\underbrace{F \subset \underset{\text{finite}}{F(a_0, \ldots a_{n-1})} \overset{n}{\subset} \underset{\text{finite}}{F(a_0, \ldots a_{n-1}, \alpha)}}_{\text{finite}} \subset K.$$

α is algebraic $/F$ possibly of high degree

$[F(\alpha) : F]$ may be large.

<u>Corollary</u> $F \subset E \subset K.$

K/F algebraic $\Leftrightarrow$ E/F algebraic & K/E algebraic.

Concrete examples

$\sqrt[3]{\sqrt{2} + \sqrt{3}}$ $\quad \mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\alpha)$

α $\quad \mathbb{Q}(\sqrt{2}, \sqrt{3})$ $\quad x^3 - \sqrt{2} - \sqrt{3}$

$\sqrt[10]{\sqrt[7]{\sqrt{5} + \sqrt{2}} + 3\sqrt[3]{1 + \sqrt{3 + \sqrt[3]{2}}} - 5} \in \mathbb{C}$ alg $/\mathbb{Q}$.

Iterated expressions (iterated radicals) are alg $/\mathbb{Q}$.

<u>Def</u> K is <u>algebraically closed</u> if every nonconstant polynomial $f \in K[x]$ has a root in K.

<u>Example</u> $\mathbb{C}$ is algebraically closed.
$\mathbb{R}$ x^2+1

<u>Prop</u> Let K be a field. TFAE.

(1) K is alg. closed
(2) $\forall$ nonconstant polynomial $f \in K[x]$ factors into linear polynomials.
(only lin polyn. are irreducible $/K$)
(3) The only algebraic extension <u>of K is K</u>

$(1) \Rightarrow (2)$ $f = (x-\alpha)g(x)$.

$(2) \Rightarrow (3)$. $K \subset E$ $\alpha \in E$. $\mathrm{irr}(\alpha, K)$

$p(x)$ - factors $\Rightarrow$ not irreducible if $\deg p > 1$.
$\shortparallel$
$x-\alpha \Rightarrow \alpha \in K$.

$(3) \Rightarrow (1)$ take nonconstant polyn w/o roots
$p(x)$ $K[x]/(p(x))$ - alg $\neq K$

$\mathbb{C} \subset E$ no finite extensions except trivial

$\mathbb{C} \underset{1}{\subseteq} \mathbb{C}$

<u>Def</u> K/F is an algebraic closure of F if

(1) K is an alg. extension of F.

(2) K is alg. closed.

$$\mathbb{Q} \subset \underset{\substack{\uparrow \\ \text{alg. closed.}}}{\mathbb{Q}^{alg.}} \subset \mathbb{C}$$

(please read end of page 5, & page 6 for more alg. closure results).

$\overline{\mathbb{Q}}$ $\qquad \overline{F}$ algebraic closure of F.

$\overline{\mathbb{F}_p}$

Friedman II.

$f(x) \in F(x)$ has a multiple root

over $\mathbb{R}$ or $\mathbb{C}$ first

$f(x) = \underline{(x-\alpha)^2 g(x)}$ $\qquad \alpha$ a mult. root.

$f(x) = (x-\alpha)^m g(x)$ s.t. $g(\alpha) \neq 0$

α is a root of f of mult. m.

$$f'(x) = 2(x-\alpha)\, g(x) + (x-\alpha)^2 g'(x) =$$

$$= (x-\alpha)\big(2g(x) + (x-\alpha)\, g'(x)\big)$$

$$= (x-\alpha)\, h(x).$$

$x-\alpha \mid f(x), f'(x) \Rightarrow x-\alpha \mid \gcd(f(x), f'(x))$.

if $\underbrace{\gcd(f(x), f'(x)) = 1}$ then

all roots of f are simple (not multiple).

$f = (x^2+1)^2$ no roots in $\mathbb{R}$.

$$\gcd(f, f') = x^2+1 \neq 1$$

but in $\mathbb{C}$ multiple roots $f = (x+i)^2(x-i)^2$.

F (formal) derivative D

$D: F[x] \longrightarrow F[x]$

1) D is F-linear

2) $D(x^n) = n\, x^{n-1}$

$a, b, c \in F$

$$\underline{D(}\, ax + bx^4 + cx^5) = a + \overset{\in F}{4b}\, x^3 + \overset{\in F}{5c}\, x^4$$

Any F-linear map L between F-vect spaces

$\underline{V} \xrightarrow{L} W$ is determined by the image

of a basis $\{v_i\}_{i \in \underline{I}}$ of V.

$F[x]$ basis $1, x, x^2, x^3, \dots\dots x^n$

$$\begin{array}{ccccccc} 1, & x, & x^2, & x^3, & \dots & x^n \\ \downarrow D & & & & & \downarrow \\ 0, & 1, & 2x, & 3x^2 & & nx^{n-1} \end{array}$$

$D(ax^n) = a \cdot n \cdot x^{n-1}$

$D\left(\sum_{i=1}^{n} a_i x^i\right) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots$

$+ \dots + a_1$

<u>Prop</u> (Leibniz rule)

$$D(fg) = D(f)g + fD(g).$$

<u>Ex</u> $f = x^n, g = x^m$ use F-linearity to extend to all f and g.

$\operatorname{char} F = p \qquad \mathbb{F}_p \subset F$

$D(x^p) = \underline{p}\, x^{p-1} = 0$ $\qquad$ x^p like a constant function

$D(x^{pn}) = pn\, x^{pn-1} = 0$

<u>Prop</u> $D : F[x] \to F[x]$

$\ker D = \begin{cases} F & \text{constant polynomials if } \underline{\operatorname{char} F = 0}. \\ F[x^p] & \text{if } \operatorname{char} F = p \end{cases}$

$p \mid n$ $\qquad$ subring of $F[x]$.

$a_n x^n + \dots + a_0 \xrightarrow{D} \underline{n a_n x^{n-1}} + \dots$

$\underline{\deg(Df) = \deg f - 1}$, f not $\underline{\text{constant}}$

in char 0,

$p = 2 \qquad a_0 + a_2 x^2 + a_4 x^4 + a_6 x^6 + \dots \xrightarrow{D} 0$

$D(f^n) = n f^{n-1} D(f)$ exercise.

<u>Prop</u> Let $f \in F[x]$ nonconstant, $F \subset E$

$\alpha \in E$ is a multiple root of f $\Leftrightarrow$ $f(\alpha) = Df(\alpha) = 0$.

$(x-\alpha)^2 \mid f \iff x-\alpha \mid f,\ x-\alpha \mid Df$

<u>Proof</u> Complete the argument by analogy $F = \mathbb{R}, \mathbb{C}$ or see Friedman.

$f = (x-\alpha)^2 g$

$f = x^p - t$ in F char $F = p$. $F \subset E$ ↑ root α multiple root

$f' = p x^{p-1} = 0$.

<u>Prop</u> $F \subset E$ $f, g \in F[x]$

$\mathbb{F}_q$ - unique field $q = p^m$ elements.

1) gcd of f, g in F is the same as gcd of f, g in E.

$\underline{\underline{x^q}} - x$

der $= q x^{q-1} - 1 = -1$

"fake" linear polyn.

Same answer whether in E or F.

2) $g \mid f$ in $F[x] \iff g \mid f$ in $E[x]$

3) f, g coprime in $F \iff$ coprime in E

Prop $f \in F[x]$ nonconstant. Then f has a multiple root in some extension E/F iff $\gcd(f, Df) \neq 1$ in $F[x]$
$\Rightarrow$ F or E

Proof $\Rightarrow$ If α is a mult. root of f in E $\Rightarrow$ $x-\alpha \mid f, Df$ $\Rightarrow$ $x-\alpha \mid \underbrace{\gcd(f, Df)}_{\neq 1}$.

$\Leftarrow$ $\underset{\text{irred.}}{p(x)} \mid \gcd(f, Df)$.

Take E where $p(x)$ has a root α.

$\Rightarrow$ $x-\alpha$ is a multiple root of $f(x)$ $\square$.

Prop If $f(x) \in F[x]$ irreducible and char $F = 0$ then f does not have mult. roots in any extension E/F

If $\exists$ a multiple root in E
$\gcd(f, Df) \neq 1$ $x-\alpha$.

f irreducible, $\deg f \geq 2$

$\deg f = n$

$\deg Df = \deg f - 1$.
$n-1$

$\gcd(f, Df)$ divisor of f.
can compute in E or F.

only divisors of f in F are 1 and f.

if $\gcd(f, Df) \to 1 \leftarrow$ no mult. roots

$\to f \leftarrow$ possi

$Df = 0$. in char p.

$f(x) = x^p - t$ $\qquad$ $F = \mathbb{F}_p(t)$

$Df = 0. = px^{p-1}$ $\qquad$ rat. functions in t.

$F \subset E$. $\qquad \sqrt[p]{t}$

$E = \mathbb{F}_p(\sqrt[p]{t}) = \mathbb{F}_p(t^{1/p})$

$x^p - t = (x-\alpha)^p$ $\qquad \alpha = t^{1/p}$.

$(x-\alpha)^p = x^p - \binom{p}{1} x^{p-1}\alpha \ldots \binom{p}{i} x^{p-i}\alpha^i$

$-\alpha^p = x^p - t$ $\qquad$ 0 mod p.