$F \subset E$ field extension, $\alpha \in E$

2 cases:

α - transcendental, generates ring $F[\alpha] \simeq F[x] \subset E$. $\{1, \alpha, \alpha^2, \dots\}$ - lin indep.
all powers of α

α - algebraic, root of a polynomial $p(x) \in F[x]$, can take p irreducible/F

$$E \supset F(\alpha) = F[\alpha] \simeq F[x]/p(x) \qquad F \underset{n}{\subset} F(\alpha) \subset E$$

subfield of E, $[F(\alpha):F] = \deg p = n$

Examples: $\sqrt[n]{a}$, $a \in \mathbb{Q}$ $\qquad$ $\sqrt[n]{a}$ root of $x^n - a$ $\qquad$ $p(x) \mid x^n - a$
$\cap$ $\qquad$ $p(\alpha) = 0$
$\mathbb{C}$ $\qquad$ $\alpha = \sqrt[n]{a}$ $\qquad$ sometimes irreducible/$\mathbb{Q}$, sometimes reducible $\qquad$ $\operatorname{irr}(\alpha, \mathbb{Q})$.

algebraic/$\mathbb{Q}$

π, e transcendental/$\mathbb{Q}$ $\qquad$ $x^2 - 3$ (irr), $x^4 - 1$ (red), $x^3 + 1$ (red)

Def Let E/F field extension. E is <u>algebraic extension</u> of F if $\forall \alpha \in E$, α is algebraic/F.

lemma If E/F finite extension ($[E:F] < \infty$) then E is an algebraic extension

Proof $\qquad F \subset F(\alpha) \subset E \qquad [E:F] < \infty \Rightarrow [F(\alpha):F] < \infty$ degree formula.

$$[E:F] = [E:F(\alpha)][F(\alpha):F].$$

Prop E/F field extension. Let $\alpha, \beta \in E$ be algebraic over F.
Then $\alpha \pm \beta$, $\alpha\beta$, and α/β (if $\beta \neq 0$) are algebraic over F

Proof Consider extensions

smallest subfield of E that contains F, α, β.

$$F \subset F(\alpha) \subset F(\alpha)(\beta) = F(\alpha, \beta)$$

$[F(\alpha):F] = n < \infty$ since α is alg$/F$, root of $\operatorname{irr}(\alpha, F)$ of some degree n $\quad p(x)$

$[F(\beta):F] = m < \infty$ since β is alg$/F$, root of $\operatorname{irr}(\beta, F)$, deg $= m$ $\quad q(x)$

$\underset{r(x)}{\operatorname{irr}(\beta, F(\alpha))}$ is a divisor of $\underset{q(x)}{\operatorname{irr}(\beta, F)}$.

In the larger field $F(\alpha)$, $q(x)$ may stop being irreducible.
$r(x) \mid q(x)$ both have coefficients in $F(\alpha)$

$$\Rightarrow [F(\alpha,\beta):F] = \underbrace{[F(\alpha,\beta):F(\alpha)]}_{\deg r \leq m}\underbrace{[F(\alpha):F]}_{n} \leq$$

$$\leq nm = [F(\alpha):F][F(\beta):F]$$

$F[x] \subset F(\alpha)[x]$
$p(x), q(x) \in F[x]$, $\quad r(x) \in F(\alpha)[x]$

$q(x)$ may not be irreducible in $F(\alpha)[x]$

$\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha,\beta) \Rightarrow$ they are algebraic

Corollary/Examples: $\sqrt[n]{a} \in \mathbb{C}$, $a \in \mathbb{Q}$ algebraic $\Rightarrow$ their combinations are alg.

$\sqrt[3]{7} - 2\sqrt{5} + \sqrt[5]{10} + \sqrt{3}\, i \in \mathbb{C}$, algebraic$/\mathbb{Q}$ $\Rightarrow$ a root of some polynomial with coefficients in $\mathbb{Q}$
(not obvious without the theory we've developed)

Def Let $F \subset E$ field extension. The algebraic closure of F in E is $\overline{F}_E := \{\alpha \in E : \alpha \text{ is algebraic over } F\}$.

Prop $\overline{F}_E$ is a subfield of E and an algebraic extension of F

Proof: use last proposition. $\square$.

$\mathbb{Q}^{alg} \subset \mathbb{C}$ alg. closure of $\mathbb{Q}$ in $\mathbb{C}$. $\overline{\mathbb{Q}}_{\mathbb{C}}$

the field of algebraic numbers

$\mathbb{Q}^{alg}$ - countable, $\mathbb{C}$ - uncountable.

E/F finite ($[E:F] < \infty$) $\Rightarrow$ algebraic extension.

The opposite implication does not hold. $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5} \dots)$ algebraic; we'll see later that it has ∞-degree.

Prop E/F is a finite extension iff $\exists\, \alpha_1, \dots \alpha_n \in E$, algebraic over F, s.t. $E = F(\alpha_1, \dots, \alpha_n)$.

Proof: Straightforward or see Friedman, lemma 2.16, page 9 of "Extension Fields I" notes.

<u>Lemma</u> Let $F \subset E \subset K$ be field extensions and E/F algebraic. Let $\alpha \in K$. Then α is alg. over F iff α is algebraic over E.

<u>Proof</u> $\Rightarrow$ α is a root of $f \in F[x] \Rightarrow \alpha$ is a root of $f \in E[x]$.

$\Leftarrow$ Let $\operatorname{irr}(\alpha, E) = x^n + a_{n-1}x^{n-1} + \dots + a_0$, $a_i \in E \Rightarrow$ they are algebraic $/F$.

$F(a_0, a_1, \dots a_{n-1})$ is a finite extension of F;

α is algebraic over $F(a_0, \dots a_{n-1})$

$F(a_0, \dots a_{n-1})(\alpha) = F(a_0, \dots a_{n-1}, \alpha)$ is a finite extension of F.

$$\underset{\text{finite}}{F \subset} F(a_0, \dots a_{n-1}) \underset{\text{finite}}{\subset} F(a_0, \dots a_{n-1}, \alpha) \Rightarrow \begin{array}{c} F \subset F(a_0, \dots a_{n-1}, \alpha) \text{ finite} \\ \Downarrow \\ F \subset F(\alpha) \text{ finite.} \end{array}$$

<u>Corollary</u> Let $F \subset E \subset K$ be field extensions. Then K/F algebraic $\Leftrightarrow$ E/F algebraic and K/E algebraic.

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

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

(1) K is algebraically closed

(2) A nonconstant polynomial $f \in K[x]$ factors into linear polynomials

(only linear polynomials are irreducible over K)

(3) The only algebraic extension of K is K.

<u>Proof</u> (1) $\Rightarrow$ (2). Take any nonconstant f. Since K is algebraically closed, f has a root α. $\Rightarrow x-\alpha \mid f$, $f=(x-\alpha)g$. Next factor g ...

(2) $\Rightarrow$ (3) Suppose $K \subset E$ is an algebraic extension. Let $\alpha \in E$. $p=\operatorname{irr}(\alpha, K)$ is monic irreducible$/K$, has the form $x-\alpha$. $p \in K[x] \Rightarrow$ $\alpha \in K$

(3) $\Rightarrow$ (1) If $f \in K[x]$ is a nonconstant polynomial $\Rightarrow$ $\exists$ extension $K \subset E$, $\alpha \in E$ root of f. α is algebraic $/K$

$\Rightarrow$ $K(\alpha)$ algebraic extension of K. By assumption, $K(\alpha)=K$, $\alpha \in K$.

$\Rightarrow$ f has a root in K.

Theorem (Fund. Thm of algebra) $\mathbb{C}$ is algebraically closed

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

1) K is an algebraic extension of F

2) K is algebraically closed.

write $K=\overline{F}$

<u>Prop</u> Let K/F be field extension and suppose K is algebraically closed then the algebraic closure of F in K is an algebraic closure of F.

<u>Remark</u>: all algebraic closures of F are isomorphic.

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

$\uparrow$ algebraic closure of $\mathbb{Q}$.

<u>Thm</u> For any field F there exists an algebraic closure of F.

Any two algebraic closures are isomorphic: if K_1, K_2 are alg. closures of F,

$\exists$ an isomorphism $\rho: K_1 \to K_2$ such that $\rho(a) = a$ $\forall a \in F$.

$$\begin{array}{ccc} K_1 & \xrightarrow{\rho} & K_2 \\ \cup & & \cup \\ & F & \end{array}$$

Suppose $f(x) \in \mathbb{R}[x]$ or $\mathbb{C}[x]$ and $f(x)$ factors $f = (x-\alpha_1)\dots(x-\alpha_n)$. How do check if f has a multiple root?

$f = (x-\alpha)^2 g(x)$. $\quad \alpha$ has multiplicity ≥ 2

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)\underbrace{\left[2g(x) + (x-\alpha)g'(x)\right]}_{h(x)}$$

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

If $f = (x-\alpha_1)\dots(x-\alpha_n)$ all distinct

$$f'(x) = \sum_{i=1}^{n} (x-\alpha_1)\dots\widehat{(x-\alpha_i)}\dots(x-\alpha_n)$$

omit this term

In this sum, all terms but first are divisible by $x-\alpha_1$

first term is $(x-\alpha_2)\dots(x-\alpha_n)$.

$\Rightarrow f'(\alpha_1) = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\dots(\alpha_1-\alpha_n) \neq 0$

$\Rightarrow \alpha_1$ is not a root of $f'(x)$, $\quad x-\alpha_1 \nmid f'(x)$.

same for all α_i.

$x-\alpha_i \mid f(x)$, $\quad x-\alpha_i \nmid f'(x) \Rightarrow \gcd(f(x), f'(x)) = 1$.

Thm If $f(x)$ factors into linear terms in $\mathbb{R}$ or $\mathbb{C}$ then $f(x)$ has a multiple root $\Leftrightarrow \gcd(f, f') \neq 1$.

If does not factor. $(x^2+1)^2$ no roots in $\mathbb{R}$, multiple roots in $\mathbb{C}$

$\mathbb{R}[x]$ $\qquad (x-i)^2(x+i)^2$

$\gcd(f, f') \neq 1$.

Can extend this to any field F. Need notion of (formal) derivative D

$(x^n)' = n x^{n-1}$
derivative is linear

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

uniquely determined by

1) D is F-linear
2) $D(x^n) = n x^{n-1}$

An F-linear map between F-vector spaces $V \xrightarrow{L} W$ is determined by the image of a basis $\{v_i\}_{i \in I}$ of V.

$F[x]$ basis $\quad 1, x, x^2, x^3 \ldots$

$$\begin{array}{cccc} 1 & x & x^2 & x^3 \\ D\downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2x & 3x^2 \end{array}$$

$$D(ax^n) = an\, x^{n-1} \quad a \in F$$

$$D\left(\sum_{i=1}^{n} a_i x^i\right) = a_n \cdot n \cdot x^{n-1} + a_{n-1}(n-1)x^{n-2} + \ldots + a_2 \cdot 2x + a_1$$

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

$$D(f(x)g(x)) = D(f(x))\,g(x) + f(x)\,D(g(x))$$

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

<u>Proof</u>: Exercise. First check on monomials $f = x^n, g = x^m$

Then use that D is F-linear.

<u>Remark</u> if $\operatorname{char} F = p$ $\quad \mathbb{F}_p \subset F \quad D(x^p) = px^{p-1} = 0$

$D(x^{pn}) = 0$.

special feature of char p.

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

$$\ker D = \begin{cases} F & \text{if } \operatorname{char} F = 0 \quad \text{(constant functions)} \\ F[x^p] & \text{if } \operatorname{char} F = p \end{cases}$$

$F[x^p]$ ↑ subalgebra of $F[x]$.

$\square$

Prop (power Rule) $f \in F[x]$, $n \in \mathbb{N}$

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

Prop Let $f \in F[x]$ nonconstant, $F \subset E$ f. extension

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

$\left(x-\alpha \mid f(x),\ x-\alpha \mid Df(x) \text{ in } E[x] \right)$

Proof Repeat our arguments back couple of pages ago or see Friedman Lemma 3.7 p. 15 of EF II notes.

write $f = (x-\alpha)^m g$, $g(\alpha) \neq 0$. $\quad Df = m(x-\alpha)^{m-1} g + (x-\alpha)^m Dg$

Note that

$m = 1 \quad Df(\alpha) = g(\alpha) \neq 0$

$m \geq 2 \quad f(\alpha) = Df(\alpha) = 0.$

Prop $F \subset E$, $f, g \in F[x]$. 1) GCD of f, g in F is the same as GCD of f, g in E.

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

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

Proof Euclid algorithm (long division) happens in F, no difference if work over 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 $F[x]$.

Proof $\Rightarrow$ if α is a multiple root of f in $E \Rightarrow$

$x - \alpha \mid f, Df \Rightarrow x - \alpha \mid \underset{\substack{\uparrow \\ \text{same in } E \text{ and } F}}{\gcd(f, Df)} \Rightarrow \gcd(f, Df) \neq 1$.

$\Leftarrow$ then $p(x) \mid \gcd(f, Df)$, take irreducible $p(x)$, take E where $p(x)$ has a root $\alpha \Rightarrow x - \alpha$ is a multiple root of $f(x)$. $\square$.

Remark: $\deg f(x) = n \Rightarrow \deg Df(x) = n-1$ or char $F = p$ and $n = pk$ some k. $f(x) = a_{pk} x^{pk} + \dots$

$\downarrow D$

$0 + \dots$

<u>Prop</u> If $f(x) \in F[x]$ irreducible and char $F = 0$

then f does not have multiple roots in any extension E of F.

If f factors fully in E, $f = c(x-\alpha_1) \ldots (x-\alpha_n)$

$\alpha_1 \ldots \alpha_n$ distinct, $c \in F^*$.

If $\exists$ a multiple root $\Rightarrow$ $\gcd(f, Df) \neq 1$, but f is irreducible

& $\deg Df < \deg f$ $\Rightarrow$ need $Df = 0$, $\gcd(f, 0) = f$

$Df = 0 \Rightarrow$ char $F = p$, $f = a_{pk} x^{pk} +$ l.o.t

<u>Only possible in char p</u>

<u>Example</u> : $x^p - t$, $F = \mathbb{F}_p(t)$ ← rational functions in t

$f(x)$

$\frac{h(t)}{g(t)}$

$Df(x) = p x^{p-1} = 0$ $F \subset E$ $E = \mathbb{F}_p(\sqrt[p]{t}) =$

$= \mathbb{F}_p(t^{1/p})$

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

if expand, get $\binom{p}{i}$ terms $= 0$.

$(x-\alpha)^p = x^p - \alpha^p$

same sign, why?

<u>Exercise</u>* Not possible when F is a finite field

Note that $\mathbb{F}_p(t)$ is an infinite field