Field ext'n: can add elts & their inverses

Thm (Nullstellensatz): Let k be a field, $k \subseteq E$, E a f.g. k-alg & E a field. Then E is a finite algebraic extension of k.
[if you a finitely many elts & get field, then elts you added were algebraic]

Pf: Let $x_1, \dots, x_n$ be generators of E as a k-alg. Assume some are not algebraic. We can renumber $x_1, \dots, x_n$ so that $x_1, \dots, x_r$ are algebraically independent over k & $x_{r+1}, \dots, x_n$ are algebraic over $k(x_1, \dots, x_r) = F$.
$k \subseteq F \subseteq E$ fields, F a purely transcendental ext'n (ie, can regard $x_1, \dots, x_r$ as abstract variables - they don't satisfy any rel's), E alg./F.

$$\overbrace{k \subseteq \underbrace{F \subseteq E}_{\text{f.g. } F\text{-mod}}}^{\text{f.g. } k\text{-alg}} \quad \Rightarrow F \text{ a f.g. } k\text{-alg. by prev. prop.}$$

WTS $k(x_1, \dots, x_r)$ is not a f.g. k-alg. This gives contradiction. Assume $\{f_i/g_i\}$ gen. $k(x_1, \dots, x_r)$ as a k-alg. Take $h = (\prod g_i) + 1$. Then h cannot appear as a denom. in any alg. comb. of $\{f_i/g_i\}$. $\Rightarrow 1/h \in k(x_1, \dots, x_r)$ is not an alg. comb. of $\{f_i/g_i\}$ $\Rightarrow k(x_1, \dots, x_r)$ cannot be f.g. as a k-alg. □.

FIELD THEORY

4/3 J.S. Milne - online notes on field theory & Galois theory

Def: The characteristic of a field k is $\min_{\substack{n \geq 0 \\ n \in \mathbb{Z}}} \{ n \mid n \cdot 1 = \overbrace{1 + \dots + 1}^{n} = 0 \}$ $= \text{Char } k$.

Char $k = 0 \iff n \cdot 1 \neq 0 \;\; \forall n \neq 0$.

map $\mathbb{Z} \xrightarrow{f} k$, $1 \mapsto 1$ $\ker f = 0$ if char $k = 0$

but $\ker f$ = prime ideal (preimage of prime is prime)

so char $k = p$, a prime

Binomial Thm: $(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + b^n$

true in any ring. $\{$ image of $\binom{n}{2}$ under f into field

- If $n = p^m$, $p = \text{char } k > 0$, then $p \mid \binom{p^m}{i}$ $\forall\, i \neq p^m, 0$.

$\Rightarrow (a+b)^{p^m} = a^{p^m} + b^{p^m}$

and $(ab)^{p^m} = a^{p^m} b^{p^m}$

$\Rightarrow$ If char $k = p$, then $F: k \to k$, $F(x) = x^p$ is a field homomorphism. $\rightarrow$ takes 1 to 1 & is additive & mult.

F is called the Frobenius homomorphism

Ex: $k = \mathbb{Z}/p\mathbb{Z}$, F = id. hom. b/c of Fermat's little thm.

- fixed pts of F are the images of $\mathbb{Z}$ under f

Claim: If char $k = p$, then $\text{Fix}(F) = \{x \in k \mid F(x) = x\}$ is $\text{Im}(\mathbb{Z}/p\mathbb{Z} \to k)$.

Why are there no other fixed pts? Look at eqn $X^p = X$ in k, a polynomial eqn, so cannot have more than p roots, those we found above. □

Weyl Conjecture)

Polynomial Rings: $k[x]$, k a field.

(1) Division algorithm – division w/ remainder

(2) $k[x]$ is a PID

- take a poly of min. degree – that will be generator
- or use Euclid's Alg to find gcd

(3) Only prime ideals are (0), (f) w/ f irred.

Prop: If $f(x) = a_m x^m + \cdots + a_0$, w/ $a_i \in \mathbb{Z}$, & $r = \frac{c}{d}$ is a root of f, $r \in \mathbb{Q}$. Assume $\gcd(c,d) = 1$. Then $c | a_0$ & $d | a_m$.

Pf: $\underbrace{a_m c^m + a_{m-1} c^{m-1} d + \cdots}_{\text{div. by } c} + a_0 d^m = 0$ (plug in & clear denoms)

$\Rightarrow c | a_0 d^m$, but $c \nmid d^m$, so $c | a_0$.

Similarly for $d | a_m$.

Ex: $x^3 - 3x - 1$ is irred. in $\mathbb{Q}[x]$.

If $\frac{c}{d}$ were a root, $c = \pm 1$, $d = 1 \Rightarrow \frac{c}{d} = \pm 1$. But these are not roots, therefore irreducible (b/c degree 3 – one factor must be linear)

(If it were deg. 4, would have to rule out 2 deg 2 factors)

Prop (Gauss' Lemma): If $f \in \mathbb{Z}[x]$ has a nontrivial decomp. in $\mathbb{Q}[x]$, then it has a nontrivial decomp in $\mathbb{Z}[x]$.

Pf: Write $f = g \cdot h$, $g, h \in \mathbb{Q}[x]$. Find m, n s.t. $mg = g_1 \in \mathbb{Z}[x]$, $nh = h_1 \in \mathbb{Z}[x]$.

$\Rightarrow mnf = g_1 h_1 \; (*)$ Pick any prime p, $p | mn$.

Reduce $(*)$ mod $p \Rightarrow 0 = \bar{g}_1 \bar{h}_1$, where $\bar{g}_1, \bar{h}_1 \in \mathbb{F}_p[x]$, an int. dom., so one of $\bar{g}_1, \bar{h}_1$ must be 0. Wlog, assume $\bar{g}_1 = 0 \Rightarrow g_1 = p g_2$, $g_2 \in \mathbb{Z}[x]$. So write $\underbrace{\left(\frac{mn}{p}\right)}_{\in \mathbb{Z}} f = g_2 \cdot h_1$ in $\mathbb{Z}[x]$. Repeat until mn has no more prime factors, ie, until $mn = 1$. □

Prop: Let $f \in \mathbb{Z}[x]$ be monic. Then any monic factor of f in $\mathbb{Q}[x]$ is in $\mathbb{Z}[x]$.

Pf: $f = gh$, $g, h \in \mathbb{Q}[x]$, g monic ($\Rightarrow h$ monic)

As before, pick m, n s.t. $mg = g_1 \in \mathbb{Z}[x]$ & $nh = h_1 \in \mathbb{Z}[x]$ with least total # of prime factors.

If $mn \neq 1$, $\exists\, p$ prime s.t. $p \mid mn$. But as before, p must divide g_1 or h_1. But the leading coeff of g_1 is m, so $p \mid m$ or $p \mid n$.

$\Rightarrow$ replace m by $\frac{m}{p}$ or n by $\frac{n}{p}$, a contradiction on minimality of m & n. □

Pf #2: Let $\xi_1, \dots, \xi_n$ be the roots in $\mathbb{C}$ of f. They are integral over $\mathbb{Z}$, so they are algebraic integers. Algebraic ints form a ring $R \subseteq \mathbb{C}$. If g is a monic factor of f in $\mathbb{Q}[x]$, then the roots of g are a subset of the roots of $f \Rightarrow$ the coeff's of g are combinations of these roots, so they are algebraic integers. By assumption, they are also rational. But $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, so coeffs of g are in $\mathbb{Z}$. □

Prop: (Eisenstein's Criterion): If $f \in \mathbb{Z}[x]$, $f(x) = a_m x^m + \dots + a_0$ & if $\exists\, p$ prime s.t.:

(1) $p \nmid a_m$

(2) $p \mid a_i$, $i \neq m$

(3) $p^2 \nmid a_0$

then f is irreducible.

Pf: Assume $f = g \cdot h$, & write

$a_m x^m + \dots + a_0 = (b_r x^r + \dots + b_0)(c_s x^s + \dots + c_0)$

(1) $a_0 = b_0 c_0$. Since $p \mid a_0$ & $p^2 \nmid a_0$, then (wlog) $p \mid b_0$ & $p \nmid c_0$.

(2) $a_1 = b_1 c_0 + b_0 c_1$. $p \mid a_1$ & $p \mid b_0 c_1 \Rightarrow p \mid b_1 c_0$ & $p \nmid c_0 \Rightarrow p \mid b_1$. Repeat $\Rightarrow p \mid b_i \; \forall i$.

$\Rightarrow a_m = b_r c_s$ is div. by p, contradiction. □

4/5 Field extensions

$K \subseteq L$ both fields, in other words, a map of fields, since such a map must be injective.

Note: L is always a vector sp. / K.

Ex: ① $\mathbb{R} \subseteq \mathbb{C}$ 2-dim

② $\mathbb{Q} \subseteq \mathbb{R}$ not f.dim → size of a basis will be uncountable

③ $\mathbb{Q} \subseteq \mathbb{Q}(i) = \mathbb{Q}[i] = \{a+bi \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$

↑ deg-2 ext'n.

Def: The deg. of an ext'n $K \subseteq L$, denoted $[L:K]$, is $\dim_K L$ (which could be ∞).

Prop: If $F \subseteq K \subseteq L$, then $[K:F] < \infty$ & $[L:K] < \infty \Leftrightarrow [L:F] < \infty$. If this is the case, then $[L:F] = [L:K] \cdot [K:F]$.

Pf: $[L:F] < \infty \Rightarrow [K:F] < \infty$ & $[L:F] < \infty$ clear.

Pick a basis $e_1, \dots, e_n$ of K/F & a basis $f_1, \dots, f_n$ of L/K. Claim: $\{e_i f_j\}_{\substack{i=\overline{1,n} \\ j=\overline{1,m}}}$ form a basis for L/F

(can multiply elts b/c L a field)

Pf: Let $x \in L$. We can write it as

$x = \sum_{j=1}^{m} a_j f_j$, $a_j \in K$. Each $a_j = \sum_{i=1}^{n} b_{ji} e_i$, $b_{ji} \in F$.

$\Rightarrow x = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{ji} e_i f_j \Rightarrow \{e_i f_j\}$ gen. over F.

If $x = 0$, $\sum_{j=1}^{n} \left(\sum_i b_{ji} e_i\right) f_i = 0 \Rightarrow \sum_i b_{ji} e_i = 0$

$\Rightarrow b_{ji} = 0$ ← ↑ basis ↗ ↑ basis ⇒

□

Let F be a field, $f \in F[x]$. look at $F[x]/(f) \doteq K$. (f. dim over F: dim = deg. f) If f reducible, not a field ($f = gh$, $g \neq 0, h \neq 0$ but $gh = 0$). If f is irreducible, $\Rightarrow (f)$ max'l $\Rightarrow F[x]/(f)$ a field & a f. dim ext'n/F. $[K:F] = \deg f$

Ex: ① $\mathbb{Q}[x]/(x^3-3x-1)$ a deg 3 ext'n of $\mathbb{Q}$.

$\Big\}$ irred.

② $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$ a deg 2 ext'n of $\mathbb{R}$

Def: A stem field (over F) for $f \in F[x]$ is a pair $K \supseteq F$ & $\alpha \in K$ s.t.

① $K = F(\alpha)$

② $f(\alpha) = 0$ in K.

Thm: If f irred, a stem field for f exists & is unique up to unique iso, ie $(K,\alpha), (K',\alpha') \Rightarrow \exists !$ iso $K \xrightarrow{\phi} K'$ s.t. $\phi(\alpha) = \alpha'$.

Pf: $(F[x]/(f), x)$ is a stem field. If (K,α) is a stem field for f,

$$F[x] \xrightarrow{\exists ! \phi} K$$

$$\text{s.t. } \begin{matrix} F \subseteq F \\ x \longmapsto \alpha \end{matrix} \Big\} \text{ univ. prop. of poly rings}$$

$\operatorname{Ker}\phi \ni f$ ∴ Since (f) max, $\operatorname{Ker}\phi = F[x]$ (↯ $x \to \alpha$ & $F \subseteq K$)

$\Rightarrow \operatorname{Ker}\phi = (f)$.

$F[x]/(f) \overset{\bar{\phi}}{\hookrightarrow} K$

↑ image contains $\alpha \Rightarrow$ image is $F(\alpha) \Rightarrow \bar{\phi}$ an iso. (by ①)

Ex: $\mathbb{Q}[x]/(x^3-3x-1)$ has basis $\{1, x, x^2\}$ / $\mathbb{Q}$.

$\cdot$: $(x^2+1)(x^2+2x+1)$ $\quad \langle 1,0,1\rangle \cdot \langle 1,2,1\rangle = \langle 5,9,3\rangle$

$x^4+2x^3+2x^2+2x+1$

$$= \underbrace{x^4-3x^2-x}_{x(x^3-3x-1)} + \underbrace{2x^3-6x-2}_{2(x^3-3x-1)} + \underbrace{5x^2+9x+3}_{\text{remainder}} \equiv 5x^2+9x+3 \pmod{x^3-3x-1}$$

$^{-1}$: $(x^2+1)^{-1}$ Euclid's alg.

(x^3+3x-1) irred & $\deg(x^2+1) < 3$ ⇐ no common factors

$\Rightarrow \gcd = 1 \overset{\text{Euclid}}{\Longrightarrow} \exists$ f, g s.t. $\underbrace{f(x^3-3x-1)}_{=0 \text{ in field}} + g(x^2+1) = 1$ $\Rightarrow g = $ inverse

(need rat'l coeffs for this!)

__Lemma__: $F \subseteq R$, F field, R an int. dom. If $\dim_F R < \infty$, then R is a field. (ie. f.d. ring ext'ns of field = field)

__Pf__: Let $x \neq 0$, $x \in R$ look at $\cdot x : R \to R$. It is F-linear & injective (b/c int dom: $xa = xb \Rightarrow x(a-b) = 0 \Rightarrow a = b$)

R f.d $\Rightarrow$ $\cdot x$ also surj (dim ker = dim coker)

$\Rightarrow \exists y \in R$ s.t. $(\cdot x)(y) = 1 \Rightarrow xy = 1$ □.

Let $F \subseteq K$ be an ext'n, $\alpha \in F$. $F(\alpha)$ = smallest subfield of K which contains F & α.

(ie, take all subfields containing α & intersect them.

OR look at subring of polys in α & take its field of fracs).

Two things can happen:

① $[F(\alpha) : F] < \infty$. We say α is __algebraic__ over F

② $[F(\alpha) : F] = \infty$. We say α is __transcendental__ /F

Look at $F[x] \xrightarrow{\phi} K$. Let $I \subseteq F[x]$, $I = \ker \phi$, a prime ideal b/c $\phi^{-1}((0))$ $^{\subseteq K}$ prime.
$\underset{x \mapsto \alpha}{F \subseteq K}$ & is principal.

So $I = (0)$ or $I = (f)$, f irred.

① If $I = (f)$, f irred, then $\operatorname{Im} \phi = F[x]/(f)$ is a subfield of K containing F, f. $\Rightarrow F[x]/(f) = F(\alpha)$

$\underset{\deg f}{\overset{\parallel}{[F(\alpha):F]}} < \infty$. Then α is algebraic.

The unique monic f is called the __minimal polynomial__ of α. (ie ! monic poly that α satisfies)

② If $I = (0) \Rightarrow F[x] \hookrightarrow K \Rightarrow \underset{F(\alpha)}{\overset{\parallel}{F(x)}} \hookrightarrow K$. $F(x)$ ∞-dim over F,

so α transcendental. (ie, α does not satisfy any polynomial)

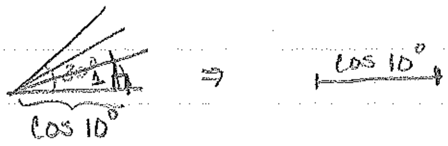
4/8 ## Constructions w/ Straight-Edge & Compass

$\overset{1}{\longleftrightarrow}$

Doubling Cube: $\overset{\sqrt[3]{2}}{\longleftrightarrow}$

Squaring the Circle: $\overset{\sqrt{\pi}}{\longmapsto}$

Trisecting the ∡:



Def: If $F \subseteq \mathbb{R}$ subfield, define the F-plane as $F^2 \subseteq \mathbb{R}^2$. An F-Line is a line s.t. two of its pts are F-points. An F-circle is a circle in $\mathbb{R}^2$ s.t. center & a pt on the circumference are F-pts.

Lemma: (1) The intersection of 2 F-lines is an F-pt

(2) The intersection of an F-Line & an F-circle is an $F[\sqrt{a}]$-pt for some $a \in F$, $a > 0$.

(3) The intersection of 2 F-circles is an $F[\sqrt{a}]$-pt.

Pf: (1) solution to sys of lin. eqns a quotient of a determ. of #'s in F ✓

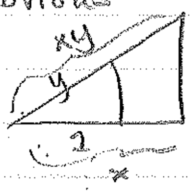
(2) Solve quadratic eqn w/ coeff's in F ✓

(3) — " — ✓

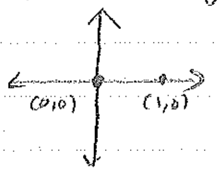
Claim: If 2 distances given, can +, −, ×, ÷ them.

+: obvious

×:



Def: Consider the set of pts in the plane which are constructible.



} given.

A distance is constructible if it is the dist. btwn 2 constructible pts.

Thm: A dist α constructible $\Leftrightarrow$ $\alpha \in \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$ s.t.
$\forall i$, $a_i \in \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_{i-1}})$
(ie, basic operations are $+, -, \times, \div, \sqrt{\ }$)
Pf: ($\Rightarrow$): Clear from lemma w/ $F = \mathbb{Q}$.
($\Leftarrow$): Can construct sq. roots (see geom. textbook)

Cor: α is constructible $\Rightarrow$ $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^d$ for some $d \geq 0$.
Pf: $\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})}_{2^n}$, & $[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid 2^n$.

Cor: Cannot double the cube: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$
Cor: Cannot square the circle: $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$ b/c
π transcendental
Cor: Cannot trisect the $\measuredangle$: $[\mathbb{Q}(\cos 10) : \mathbb{Q}] = 6$
write $\cos(3x)$ in $\sin x$, $\cos x$, so $\cos 10$ satisfies
cubic eqn w/ $\cos 30 = \sqrt{3}/2$ $\Rightarrow$ deg 6. (check)

What regular polygons can be constructed?
For even #'s can use smaller figures: ie 12-gon from square & triangle.
Thm (Gauss): If a regular p-gon can be constructed w/ ruler & compass, then
$p = 2^{2^n} + 1$.
$\left(\begin{array}{l} n=0, \text{ equil. } \Delta;\ n=1, \text{ pentagon (non-trivial)} \\ n=2, \text{ 17-gon (Gauss) } \dots \end{array} \right)$

Lemma: If p prime, then $x^{p-1} + x^{p-2} + \dots + 1$ is irreducible. (called a cyclotomic polynomial)

$$f(x) = \frac{x^p - 1}{x - 1}, \quad f(x+1) = \frac{(x-1)^p - 1}{x} = x^{p-1} + \underbrace{\binom{p}{1} x^{p-2} + \dots +}_{\div \text{ by } p} \underbrace{\binom{p}{p-1}}_{= p}$$

By Eisenstein, f is irreducible
($f(x+1)$ irred $\Rightarrow$ $f(x)$ irred)

Cor: $[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p-1$ (p^{th} roots of unity)

Cor: $[\mathbb{Q}(\cos(2\pi/p)) : \mathbb{Q}] = \frac{p-1}{2}$

Pf: $\mathbb{Q} \subseteq \mathbb{Q}(\cos\frac{2\pi i}{p}) \subseteq \mathbb{Q}(\underbrace{e^{2\pi i/p}}_{\zeta})$

$$\frac{\zeta + \zeta^{-1}}{2} = \frac{(\cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}) + (\cos\frac{2\pi}{p} - i\sin\frac{2\pi}{p})}{2} = \cos\frac{2\pi}{p}$$

$$\Rightarrow \cos 2\pi/p \in \mathbb{Q}(e^{2\pi i/p})$$

But $[\mathbb{Q}(\underset{\alpha}{\underset{\shortparallel}{e^{2\pi i/p}}}) : \mathbb{Q}(\cos\frac{2\pi}{p})] = 2.$

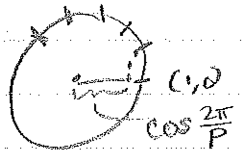
≤ 2: $\alpha^2 - 2\cos\frac{2\pi}{p}\alpha + 1 = 0$

> 1: LHS $\not\subseteq \mathbb{R}$, RHS $\subseteq \mathbb{R}$

$\Rightarrow = 2.$

Pf of Thm:

To construct p-gon, need to construct $\cos\frac{2\pi}{p}$.



$\Rightarrow p-1 = 2^d$ for some d, b/c deg. of ext'n a power of 2.

But $2^d + 1$ can be prime only if $d = 2^n$: If d has an odd factor, can find a factor of 2^d+1. □

4/10 Def: A field Ω is said to be alg. closed iff every polynomial in $\Omega[x]$ has a root in Ω.

Ex: Fundamental Thm of Alg: $\mathbb{C}$ is alg. closed

Prop: TFAE:

(1) Ω is alg. closed

(2) $\forall f \in \Omega[x]$, f splits in Ω (ie, f is a product of degree 1 factors)

(3) the only irred. polys in $\Omega[x]$ are degree 1

(4) If F is an alg. ext'n of Ω, then $F = \Omega$.

Def: If F is a field, Ω alg. closed, $F \subseteq \Omega$, Ω is algebraic over F, then Ω is an algebraic closure of F.

↳ unique only up to isomorphism (but not a ! isom.)

$\mathbb{C}$: conjugation is an $\cong$ of $\mathbb{C}$ that preserves $\mathbb{R}$.

Prop: Let $F \subseteq \Omega$ w/ Ω algebraically closed, let $G = \{x \in \Omega \mid x \text{ alg}/F\}$. Then G is an alg. closure of F.

Pf: WTS: (1) G a field, (2) G alg. closed.

(1): If $\alpha, \beta \in G$, then $[F[\alpha] : F] < \infty$ b/c α alg/F

$[F[\alpha,\beta] : F[\alpha]] < \infty$ b/c β alg/F

$\Rightarrow [F[\alpha,\beta] : F] < \infty \Rightarrow \forall \gamma \in F[\alpha,\beta]$ alg. over F

$\Rightarrow \alpha\beta$ alg/F, $\alpha+\beta$ alg/F. $\Rightarrow G$ a field.

(2): Let $f \in G[x] \subseteq \Omega[x]$. Let α be a root of f in Ω. Write $f = a_0x^n + \cdots + a_n$ w/ $a_i \in G$. Look at $[F[a_0, \ldots, a_n, \alpha] : F] < \infty \Rightarrow [F[\alpha] : F] < \infty$ $\Rightarrow \alpha \in G$. □

Ex: ① p prime, $f(x) = x^{p-1} + \cdots + 1 \in \mathbb{Q}[x]$

$\mathbb{Q}[\zeta] = \mathbb{Q}[x]/(f)$ (ie, add one root of f)

All roots of unity except 1 are primitive

Actually added all roots, b/c they're just powers of e/o:

In $\mathbb{Q}[\zeta]$, f will split completely b/c once you add one p^{th} root, & you add all p^{th} roots. of 1.

② $f(x) = x^3 - 2 \in \mathbb{Q}[x]$

roots are $\sqrt[3]{2}\cdot 1$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2$, $\zeta = e^{2\pi i/3}$

adding 1st root won't add last 2 (1st $\mathbb{R}$, last 2 $\mathbb{C}$)

In $\mathbb{Q}[\sqrt[3]{2}]$, $x^3 - 2 = (x - \sqrt[3]{2})(\underbrace{x^2 + \sqrt[3]{2}x + \sqrt[3]{4}})$

g is irred in $\mathbb{Q}[\sqrt[3]{2}]$

Def: Let F be a fixed field, $f \in F[x]$. We say f splits in $E \supseteq F$ if f is a product of deg 1 polys in $E[x]$.

Def: If E is gen./F by the roots of f, & f splits over E, then E is a splitting field of f. (pick an alg. closure, then it's the spl. field)

Def: If E, E' are fields containing F, then an F-homomorphism $E \xrightarrow{\phi} E'$ is a field hom. s.t. $\phi(x) = x$ $\forall x \in F$. (ie, an F-alg. hom.)

Similarly for F-isomorphism

Ex: conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

Def: A simple ext'n is one obtained by adjoining exactly one elt.

<u>Prop</u>: Let F be a field, $F(\alpha)$ a simple ext'n of f; Ω some other field containg F.

(a) If α is transcendental/F, $\forall\, \phi: F(\alpha) \to \Omega$ an F-hom, we have $\phi(\alpha)$ is trancendental /F & $\{\phi\} \overset{1-1}{\longleftrightarrow} \{F\text{-transcendental } x \in \Omega\}$

(b) If α alg. over F w/ min. poly $f \in F[x]$, then $\forall$ $\phi: F(\alpha) \to \Omega$ an F-hom, we have $\phi(\alpha)$ is a root of f and

$$\{\phi\} \overset{1-1}{\longleftrightarrow} \{\text{roots of } f \text{ in } \Omega\}$$

In particular, # of ϕ's = # of distinct roots of f in Ω. (if char $F=0$, # dist. roots = deg f, else, not nec.)

<u>Pf</u>: (a) If $\phi(\alpha)$ satis. eqn in Ω w/ coeff in F. Then α satis. eqn in F w/ same coeff.

$\phi \longmapsto \phi(\alpha)$
$\quad | \, x$

$F[\alpha] \to \Omega$ injective, so will descend to frac. field
$\alpha \longmapsto x$

(b) $\phi(f(\alpha)) = \phi(0) = 0$, but $\phi \circ f$ has coeffs in F b/c ϕ fixes F.

($\leftarrow$) Let β be root of f in Ω. look at map

$$\begin{tikzcd} F[x] \arrow[r, "\phi"] & \Omega \\ x \arrow[r, mapsto] & \beta \end{tikzcd}$$

$\ker \phi = (f)$ $\Rightarrow$ get map $F[x]/(f) \longrightarrow \Omega$

$$\begin{tikzcd} F[x]/(f) \arrow[r] \arrow[d, equal] & \Omega \\ F[\alpha] & \alpha \arrow[r, mapsto] & \beta \end{tikzcd}$$

($\leftrightarrow$): $\phi \longmapsto \phi(\alpha)$

□

4/12 F a field, $f \in F[x]$. Add one root canonically by $F[x]/(f)$

<u>Prop</u>: A splitting field E for f always exists & $[E:F] \leq n!$ where $n = \deg(f)$.

<u>Pf</u>; $F_1 = F[x]/(f)$ has at least one root. Factor F_1. Repeat for irred. factors of $\deg > 1$. deg of irred. factors decreases, so process terminates. Worst case: only add 1 root at a time; best case add all in F_1 $\Rightarrow$ $n \leq [E:F] \leq n!$

<u>Ex</u> ① $\mathbb{Q}[\zeta]$, $\zeta = e^{2\pi i/p}$ p prime is a spl. field for $x^{p-1} + \cdots + 1 = f(x)$. $f(x) = \prod_{i=1}^{p-1} (x - \zeta^i)$

② $x^p - x - a = f(x)$ for $a \in \mathbb{F}_p$, $f \in \mathbb{F}_p[x]$, $a \neq 0$

$\forall x \in \mathbb{F}_p$, Fermat's little thm says $x^p = x \pmod p$

$\Rightarrow x^p - x = 0$, $a \neq 0$.

If $\lambda \in E$ is a root of $f(x)$, then for $i \in \mathbb{F}_p$

$(\lambda + i)^p = \lambda^p + i^p = \lambda^p + i$

$\Rightarrow (\lambda+i)^p - (\lambda+i) - a = \lambda^p + i - \lambda - i - a = \lambda^p - \lambda - a = 0$.

$\Rightarrow$ in $\mathbb{F}_p[\lambda]$, $\{\lambda + i\}_{i \in \mathbb{F}_p}$ are all roots of f.

$\Rightarrow$ splitting field of f has deg $p/\mathbb{F}_p$.

③ $x^p - a = f(x) \in F[x]$, F has all n^{th} roots of unity.
ie cyclotomic poly splits.

but a has no n-th root in F.

Ex: $f(x) = x^3 - 2$ in $\mathbb{Q}[\zeta]$, $\zeta = e^{2\pi i/3}$ f irred, but adding $\sqrt[3]{2}$ gives all roots.

$f \in \mathbb{Q}$, need to do 2 splittings - add $\sqrt[3]{2}$ (deg 3) & then ζ (deg 2 - b/c solving quadratic)

Prop: Let F a field, $f \in F[x]$, & $E \supseteq F$ is gen. by some roots of f (ie $E = F[\alpha_1, \dots, \alpha_k]$, $f(\alpha_i) = 0 \ \forall \ 1 \le i \le k$) and let $\Omega^{\supseteq F}$ be a big field in which f splits.

(1) There exist F-homs $E \to \Omega$ & the # of such is $\le [E:F]$ w/ equality if f has distinct roots in Ω.

(2) Any 2 splitting fields of F are F-isomorphic (but not nec. uniquely isom.)

Pf: (1) Write $E = F[\alpha_1, \dots, \alpha_k]$, α_i are some roots of f.

Look at $F_1 = F[\alpha_1]$. Let g be min poly of α_1.

$\{F\text{-homs } F[\alpha_1] \to \Omega\} \overset{1-1}{\longleftrightarrow} \{\text{roots of } g \text{ in } \Omega\}$

$(g \mid f$ & g irred.)

g splits in Ω b/c g a factor of f. If f has distinct roots in Ω, then so does g.

Look at $F \subset F[\alpha_1] \subset E$.

$$\begin{tikzcd}
F \arrow[r, phantom, "\subset"] \arrow[dr] & F[\alpha_1] \arrow[r, phantom, "\subset"] \arrow[d, dashed, "\exists"] & E \\
 & \Omega &
\end{tikzcd}$$

Bootstrap until no more elts to add to get to E.

Note: (# of maps $\phi : E \to \Omega$ which are $F[\alpha_1]$-homs)
$\cdot$ (# of maps $\phi' : F[\alpha_1] \to \Omega$ which are F-homs) $\leftarrow \le \deg g$
$=$ (# of maps $E \to \Omega$ which are F-homs)

$\uparrow$ = if roots distinct

By induction $\le [E : F[\alpha_1]] = [E:F] / \deg g$

$\Rightarrow \ \le [E:F]$.

$\Rightarrow$ equality if roots of are distinct

Given map $E \to \Omega$ (map of fields $\Rightarrow$ injective)

$\Rightarrow E \subseteq \Omega$ b/c $F(\alpha_1) \subseteq E$, get F-lin map $F(\alpha_1) \to \Omega$.

Given map $F[\alpha_1]$, can extend to E by $\to$ again embed $F[\alpha_1] \to \Omega$ then need $F[\alpha_1]$-hom.

Given $\phi : E \to \Omega$ an F-hom, restricting $\phi|_{F[\alpha_1]}$

$\phi|_{F[\alpha_1]} : F[\alpha_1] \to \Omega$ an F-hom. using $\phi|_{F[\alpha_1]}$ to embed $F[\alpha_1] \subseteq \Omega$, now ϕ gives a $F[\alpha_1]$-hom of $E \to \Omega$.

(2) Let E, E' be splitting fields of f; ie
$E \supseteq F$ & $E' \supseteq F$ (or have fixed embedding of F into them), F splits in them, & they are gen./F by roots of f.
By (1), $\exists$ F-homs $E \to E'$ and $E' \to E$ (take 1st $E' = \Omega$ & 2nd $E = \Omega$)
$\Rightarrow$ $[E:F] = [E':F]$ (then done b/c regard them as f.d. F-vect. sp's) $\Rightarrow$ ϕ an iso.

$\left\{\begin{array}{l} E \to E' \Rightarrow [E:F] \le [E':F] \\ E' \to E \Rightarrow [E':F] \le [E:F] \end{array}\right\}$

<u>Cor</u>: E, L are ext'ns of F w/ $[E:F] < \infty$, then

$$\begin{tikzcd}
 & \Omega \arrow[dr, dash, "?"] & \\
E \arrow[ur] & & L \\
 & F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

(1) (# of F-homs $E \to L$) $\le [E:F]$
(2) $\exists$ an ext'n Ω of L and a hom $E \to \Omega$

Note $[\ ] = (\ )$ if ext are alg.

<u>Pf</u>: Let $E = F(\alpha_1, \dots, \alpha_k)$, let $f = \prod_{i=1}^{k} \min_F(\alpha_i)$ ← min polys over F.

Pick any sp. field of f/L, then $\exists\ \Phi : E \to \Omega \Rightarrow$ (b) ✓
(# of such) $\le [E:F] \Rightarrow$ (# F-hom's $E \to L$) $\le$ (# F-homs $E \to \Omega$) $\le [E:F] \Rightarrow$ (a) ✓ □

b/c $L \subseteq \Omega$ $\Downarrow$ a map to L is a map to Ω.

4/15 <u>Prop</u>: Let F be a field, $f, g \in F[x]$ & Let Ω be an ext'n field of F. Then $\gcd_F(f,g) = \gcd_\Omega(f,g)$.
↑ computed in $F[x]$

<u>Pf</u>: Let $A = \gcd_F(f,g) \in F[x]$ &
$B = \gcd_\Omega(f,g) \in \Omega[x]$. A is a common divisor of f & g in $\Omega[x] \Rightarrow A \mid B$.
Write $A = fM + gN$ for $M, N \in F[x]$ using Euclid's algorithm. $\Rightarrow B \mid A$ (b/c $B \mid f$ & $B \mid g$)
$\Rightarrow A = B$ (if take A & B to be monic) □

In particular, if $\gcd_F(f,g) = 1$, f & g cannot have a common root in Ω.

Def: We say an irreducible polynomial in $F[x]$ is separable if it does not have multiple roots in a splitting field. An arbitrary poly. in $F[x]$ is separable if its irred. factors are.
(can have mult. roots, but they must occur in diff. irred. factors, like x^3.)

Prop: TFAE for an irred. poly. $f \in F[x]$; $f \neq 0$,

(1) f is not separable (ie. f has a multiple root)

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

(3) char $F = p > 0$ & $f(x) = g(x^p)$ for some $g \in f(x)$

(4) all roots of f are multiple.

Ex: $x^p - x - a$, separable ; $x^p - a$, say $\lambda^p = a$, then $x^p - a = x^p - \lambda^p = (x-\lambda)^p$ in field of char p, so $x^p - a$ not separable.

Pf: (1) $\Leftrightarrow$ (2) does not require f irred.

Pf: f has a mult root $\Leftrightarrow$ $f = \prod_{i=1}^{n} (x-\alpha_i)^{\beta_i}$ & $\beta_1 > 1$, in some ext'n field Ω / F $\Leftrightarrow$ $f'(\alpha_1) = 0$.
(If $\beta_1 = 1$, then $f'(x) = \prod_{i=2}^{n} (x-\alpha_i)^{\beta_i} + (x-\alpha_1)\left(\prod_{i=2}^{n} (x-\alpha_i)^{\beta_i}\right)'$
But then $f(\alpha_1) \neq 0$)
$\Rightarrow \gcd(f, f') \neq 1$ (from cor.)

(2) $\Rightarrow$ (3): Assume $\gcd(f, f') \neq 1$. f irred $\Rightarrow f \mid f'$.
(b/c $\gcd = f$ since f irred & $\gcd \mid f$). But $\deg f' < \deg f \Rightarrow f' = 0$ $(\Rightarrow \text{char } F > 0)$. But if $f = \sum a_i x^i$, then $f' = \sum i a_i x^{i-1} = 0 \Rightarrow i a_i = 0 \; \forall i \Rightarrow i$ is a multiple of p (if $a_i \neq 0$)
$\Rightarrow f = a_0 + a_p x^p + a_{2p} x^{2p} + \dots = g(x^p)$ where
$g(x) = a_0 + a_p x + a_{2p} x^2 + \dots$

(3) $\Rightarrow$ (4): If $f = g(x^p)$ & Ω is a splitting field of g, $\Rightarrow g(x) = \prod (x - \alpha_i) \Rightarrow f(x) = \prod (x^p - \alpha_i)$
and adjoin p^{th} roots of α_i's.
$f(x) = \prod (x^p - \alpha_i) = \prod (x^p - (\sqrt[p]{\alpha_i})^p) = \prod (x - \sqrt[p]{\alpha_i})^p$.

(4) $\Rightarrow$ (1) obvious $\square$

Def: A field f is *perfect* if any $f \in F[x]$ is separable.

Ex: ① If char $F=0 \Rightarrow F$ is perfect

Prop: A field F is perfect iff either char $F=0$ or $\forall x \in F$, it has a p^{th} root in F, where $p=$char F.

Pf: If char $F=0$, obvious.

If char $F=p$ & a does not have a p^{th} root, then the poly x^p-a is not separable.

If all elts have p^{th} roots, assume f is irred & inseparable. Then $f=g(x^p)=a_0+a_1x^p+\dots+a_nx^{pn}$
$=(b_0+b_1x+\dots+b_nx^n)^p$ where $b_i^p=a_i$. ↯ b/c f was irred. $\Rightarrow$ f separable. □

Cor: $\mathbb{F}_p$ is perfect.

- everything is its own p^{th} root

Cor: If F is an alg. ext'n of $\mathbb{F}_p$, then F is perfect. (In particular, $\overline{\mathbb{F}_p}$ is perfect)

Pf: Let $x \in F$ & consider $G=\mathbb{F}_p[x]$, a finite ext'n of $\mathbb{F}_p$. Look at Frobenius map $\phi: G \to G$. This map is $\mathbb{F}_p$-linear & injective $(\phi(x)=x^p)$
b/c $\phi(x)=\phi(y) \Leftrightarrow x^p=y^p \Leftrightarrow (x-y)^p=0 \Leftrightarrow x=y$ b/c G has no 0-divisors. ϕ is an injective map of $\mathbb{F}_p$-vect. sp's of same dim $\Rightarrow \phi$ is surj $\Rightarrow$ every elt has a p^{th} root □

4/17 Ex: $\mathbb{F}_p(x)$ has char p but is not perfect, b/c x does not have a p^{th} root.

Note: $\mathbb{F}_p(x)$ not a finite field.

$\{ F \subset \underbrace{\text{intermediate field extns}}_{\text{what fields can go here?}} \subset E \} \xleftrightarrow{1-1} \{ \text{Subgps of } Gal(E/F) = Aut(E/F) \}$

^ alg ext'ns

under some conditions on E/F

Start w/ an ext'n E/F finite. (Gal extn → separable & normal)

Def: $Aut(E/F) := \{ \phi : E \to E \mid \phi \text{ is an } F\text{-isomorphism} \}$

ie, ϕ fixes F but can shuffle elts of E.

Ex: ① $Aut(\mathbb{C}/\mathbb{R}) = \{ id, \bar{\ } \} \simeq \mathbb{Z}/2\mathbb{Z}$

If $\phi \in Aut(\mathbb{C}/\mathbb{R})$, $\phi(a+bi) = \phi(a) + \phi(i)\phi(b) = a + b\phi(i)$

so ϕ completely determined by where it sends i.

Can only send i to another root of min poly:

$\phi(i) = i \Rightarrow \phi = id$ or $\phi(i) = -i \Rightarrow \phi =$ conjugation

② $Aut(\mathbb{C}(x)/\mathbb{C}) \cong GL_2(\mathbb{C})/\mathbb{C}^* = PGL_2(\mathbb{C})$

^ transcendental ext'n, so $x \mapsto$ any elt transc. / $\mathbb{C}$

but if send $x \mapsto x^2$, not an iso

As before, ϕ det. by where it sends x, & $\phi(x)$ has to be transc. / $\mathbb{C}$ & a generator of $\mathbb{C}(x)/\mathbb{C}$.

The set of gen of $\mathbb{C}(x)/\mathbb{C}$ are of form $\frac{ax+b}{cx+d}$, where $ad-bc \neq 0$. (2×2 matrix w/ nonzero det)

Composition equiv. to mult the 2×2 matrices

But $\neq GL_2(\mathbb{C})$ b/c if mult num. & denom by constant, get same elt

Geometrically, automorphisms of $\mathbb{P}^1 = Aut(\mathbb{P}^1)$

b/c thinking of $\mathbb{C}(x)$ as meromorphic fcns - compactify line by adding ∞, get $\mathbb{C}(x)$ are holomorphic fcns to $\mathbb{P}^1$.

Thm: Let F be a field, $f \in F[x]$ separable, & E a splitting field of f. Then $|\mathrm{Aut}(E/F)| = [E:F]$

Pf: Write $f = \prod f_i^{\alpha_i}$, $f_i \in F[x]$, $\alpha_i \geq 1$, f_i irred. Then wlog, we can replace f by $\prod f_i$ b/c have same splitting field. Then f has exactly $\deg f$ distinct roots in E. (no common roots btwn f_i's b/c $\gcd(f_i, f_j) = 1$ since they're irred). But then $|\mathrm{Aut}(E/F)| = [E:F]$ b/c we had a prop: If E gen by some roots of f & Ω contains all roots of F, then # of F-homs $E \to \Omega$ is $\leq [E:F]$, w/ equality if f has all distinct roots in Ω.

Our E a spl. field so gen by roots of f, take $\Omega = E$. □

Ex: ① $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = |\{1\}| < [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$

only added one root of of $x^3 - 2 = 0$, so $\sqrt[3]{2} \mapsto \sqrt[3]{2}$

Let F = spl. field of $x^3 - 2 / \mathbb{Q}$.

$|\mathrm{Aut}(F/\mathbb{Q})| = [F:\mathbb{Q}] = 6$, $\mathrm{Aut}(F/\mathbb{Q}) \simeq S_3$

$x^3 - 2 = (x - \sqrt[3]{2})(\text{quadratic})$

↑ 1st ext'n ↑ sol'n to this gives 2nd ext'n

Can permute the 3 roots of 2 any way & get an F-iso, so $\mathrm{Aut}(F/\mathbb{Q}) \simeq S_3$ (needs rigorous pf, b/c could be relations btwn 3 cube roots & so not all $\sigma \in S_3$ give different automorphisms)

Reminder: If E spl. field of f/F, $[E:F] \leq n!$ where $n = \deg f$.

ex: for cyclotomic poly $[E:F] = p$ b/c only where send ζ_p, since all other roots are powers of ζ.

Cor: If $[E:F] = n!$, then $\mathrm{Aut}(E/F) \simeq S_n$.

b/c always injective hom. to S_n, & if 2 gps have same order, then iso.

→ so can always look at $\mathrm{Aut}(E/F)$, E a spl. field, as a subgp of S_n.

Let G be a finite gp of automorphisms of a field E.
Define $E^G = \text{Fix}(G) = \{x \in E \mid \phi(x) = x \ \forall \phi \in G\}$.
$E^G \subseteq E$ is a subfield (sums & prods fixed)

Thm: If E is the spl. field of a separable poly. over F, then $E^{\text{Aut}(E/F)} = F$.

Ex: ⓐ Let char F = p & let $f = x^p - a$, a not a p^{th} root in F. Let E be the spl. field of f.
$\text{Aut}(E/F) = \{1\}$ b/c when add $\sqrt[p]{a}$ (unique b/c char. p)
then $f = x^p - b^p = (x-b)^p$, so poly. splits. Thus
$E = F[\sqrt[p]{a}]$, & $\phi(\sqrt[p]{a}) = \sqrt[p]{a}$ only F-iso.
* In field w/ char. p, only one p^{th} root *
but $[E:F] = p$.

4/19 (*) E/E^G, $G \subseteq \text{Aut}(E)$ finite. (not all field extn's are (ie, base field is fixed field of gp of autos) of this form)
ex: $\mathbb{Q}[\sqrt[3]{2}]$ all automorphisms fix $\mathbb{Q}$ (b/c $1 \to 1$)
$\Rightarrow \text{Aut}(\mathbb{Q}[\sqrt[3]{2}]) = \{1\}$
So $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not of the type E/E^G

(**) E/F, E = splitting field of some separable poly $f \in F[x]$.
ex: $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not of this type, either

We proved:
1. If E/F is of type (**), then $[E:F] = |\text{Aut}(E/F)|$

Thm (E. Artin): If E/F is type (*), ie $\exists\, G \subseteq \text{Aut}(E)$ finite s.t. $F = E^G$. Then $[E:F] \leq |G|$.
Pf: $G = \{\sigma_1, \dots, \sigma_m\}$, label them s.t. $\sigma_1 = \text{id}$.
WTS any set of elts of E bigger than m: $\{\alpha_1, \dots, \alpha_n\}$ $(n > m)$ is linearly dependent / F. Then dim. of vector sp E over F $\leq m$. →

Look at the system of eqns:

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_n)x_n = 0 \\ \vdots \\ \sigma_m(\alpha_1)x_1 + \cdots + \sigma_m(\alpha_n)x_n = 0 \end{cases}$$

$\leftarrow$ recall, $\sigma_1 = id$, so this eqn gives the lin. dependence condition

This systems admits a nonzero solution b/c # of vars > # of eqns. Want a minimal solution in the sense that want sol'n w/ most 0's – ie find a minimal linear dependence:

Look for such a solution $(c_1, \dots, c_n)$ which has the largest # of zeros among the c_i's. Wlog, assume $c_1 \neq 0$ (relabel α's & x's) & $c_1 \in F$. (can mult by sol'n by scalars, so could $\div$ by c_1 to get $c_1 \in F$)

<u>Claim</u>: $c_i \in F$ $\forall i$, hence $\{\alpha_i\}$ are linearly dependent /F.

<u>Pf</u>: Assume not. Then $\exists k > 1$ s.t. $c_k \notin F$, ie $\exists \ell$ s.t. $\sigma_\ell(c_k) \neq c_k$. Look at $(\sigma_\ell(c_1), \dots, \sigma_\ell(c_n))$. This is a new sol'n of the system, b/c hitting each eqn w/ σ_ℓ just permutes them, since $\sigma_\ell \circ \sigma_i = \sigma_j$ for some j, so i^{th} eqn becomes j^{th} eqn.

But now, $(c_1 - \sigma_\ell(c_1), \dots, c_n - \sigma_\ell(c_n))$ is also a sol'n. This is nonzero, b/c nonzero in k^{th} position. It has more zeros – all old zeros are preserved, but $c_1 - \sigma_\ell(c_1) = 0$ $(c_1 \in F)$ but $c_1 \neq 0$. ↯ □

<u>Cor</u>: If $G \leq Aut(E)$ finite, then $G = Aut(E/E^G)$.

((Given ext'n E/F of type $(*)$, so F is fixed field of some gp of autos & then can recover the gp – find all autos w/ fixed field F)

<u>Pf</u>: Note that $G \leq Aut(E/E^G)$

$$[E:E^G] \underset{\substack{\uparrow \\ \text{prev. thm}}}{\leq} |G| \leq |Aut(E/E^G)| \leq [E:E^G]$$

$\uparrow$ $E/F, \Omega/F \Rightarrow |F\text{-homs}(E,\Omega)| \leq [E:F]$

$\Rightarrow |G| = |Aut(E/E^G)|$

$\Rightarrow [E:E^G] = |G|$ ($\leq$ from Artin's thm actually an $=$)

Def: Let E/F be an algebraic ext'n. We say:

(1) E/F is separable if $\forall \alpha \in E$, the min. poly of α / F is separable.

(2) E/F is normal if $\forall \alpha \in E$, the min. poly of α / F is normal

(3) E/F is Galois iff E/F is separable & normal

Equivalently: E/F is (separable/normal/Galois) iff $\forall f \in F[x]$ irred, if f has a root in E, then (this root is simple / all roots of f in G / f has $\deg f$ distinct roots in E).

Geometric Picture:

$f \in F[x]$

$\text{Spec}\, F[x] = \mathbb{A}^1_F$ (affine line over F)

$\underset{\text{Spec}\left(F[x]/(f) = F'\right)}{\overset{\shortparallel}{Z(f)}} \subseteq \mathbb{A}^1_F$ zeros of poly. - none in $\mathbb{A}^1_F$ - if look at $Z(f) \subseteq \mathbb{A}^1_E$, see some zeros

- to be Galois, when look at $Z(f) \subseteq \mathbb{A}^1_E$, must see all zeros.

Ex: ① $\mathbb{Q}[\sqrt[3]{2}] / \mathbb{Q}$ is separable but not normal.

b/c $x^3 - 2$ does not split in $\mathbb{Q}[\sqrt[3]{2}]$

(* in char. 0, all polys are separables)

② $\mathbb{F}_p(t) / \mathbb{F}_p(t^p)$ is normal but not separable.

b/c $\underset{\mathbb{F}_p(t^p)}{\min}(t) = x^p - t^p$, but t is a root of order p.

③ $\mathbb{C}/\mathbb{R}$ is Gal.

④ $\mathbb{Q}[\sqrt[3]{2}, \zeta_3] / \mathbb{Q}$ is Galois.

Main Thm: Let E/F be a finite ext'n. TFAE:

(1) $F = E^G$ for some $\underset{\substack{\uparrow \\ \text{take any subgp} \\ \text{of } Aut(E)}}{G} \subseteq Aut(E)$ finite. (fix E, can find all F's)

(2) E is a splitting field of a separable poly $f \in F[x]$

↑ (fix F, can find all E's)

(take any separable poly

4/22 <u>Thm</u>: Let E/F be a finite ext'n. Then TFAE:

(1) E is the splitting field of a separable poly $f \in F[x]$.

(2) $F = E^G$ for $G \leq \mathrm{Aut}(E)$, G finite.

(3) E/F is normal & separable (= Galois)

(4) $F = E^{\mathrm{Aut}(E/F)}$ (= book's def of Galois)

<u>Def</u>: If E/F satisfies any of (1)-(4), we say E is a <u>Galois ext'n of F</u>, & we call $\mathrm{Aut}(E/F)$ the <u>Galois gp</u> of E/F, denoted $\mathrm{Gal}(E/F)$.

<u>Pf</u>: (1)⇒(4): Let $G = \mathrm{Aut}(E/F)$, $F' = E^G$. A priori we only know $F' \supseteq F$

Note that we can regard $f \in F'[x]$, & E is a splitting field of f over F' also (f splits in E <u>automatically</u> & E gen. over F by roots of poly, so E gen over F' by roots of poly). f is still separable. $\Rightarrow [E:F] = |\mathrm{Aut}(E/F)|$ and $[E:F'] = |\mathrm{Aut}(E/F')|$. Since $F' = E^G \Rightarrow \mathrm{Aut}(E/F') = G$ $= \mathrm{Aut}(E/F) \Rightarrow [E:F] = [E:F'] \Rightarrow F = F'$. ✓ Cor. to Artin

by def

(4)⇒(2): $\mathrm{Aut}(E/F)$ must be finite b/c $\leq [E:F] < \infty$ & 2 follows.

(2)⇒(3): Take $\alpha \in E$, WTS $\min(\alpha)$ splits into distinct linear factors in E (ie is normal & sep)

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_m\} = G \cdot \{\alpha\}$ (ie the orbit of α under action of G) as a set - no repetitions.

Take $g(x) = \prod_{i=1}^{n} (x - \alpha_i) \in E[x]$. We'll show $g = \min_F(\alpha)$ $\Rightarrow \min(\alpha)$ splits into distinct roots.

(a) $g \in F[x]$: Look at $\sigma \cdot g$ for some $\sigma \in G$.

for $\sigma \cdot g = \prod(\sigma(x) - \sigma(\alpha_i)) = \prod(x - \alpha_j) = g$

(ie, $\sigma \cdot \{\alpha_1, \ldots, \alpha_m\} = \{\alpha_1, \ldots, \alpha_m\}$). But if expand & act by σ on coeffs, they are fixed $\forall \sigma \in G$.

$\Rightarrow$ coeffs $\in F$, ie $g \in E[x]^G = F[x]$

$\Rightarrow$ Let $f = \min(\alpha)$. Then $f | g$. (g = some monic poly w/ coeff in f w/ α as a root). On the other hand, α_i is a root of f $\forall i$, b/c if $\alpha_i = \sigma \cdot \alpha$, then $f(\alpha_i) = f(\sigma \cdot \alpha) = \sum a_i (\sigma \cdot \alpha)^i = \sum a_i \sigma \cdot (\alpha^i) = \sigma \sum (\sigma^{-1} a_i) \alpha^i$
$= \sigma f(\alpha) = \sigma \cdot 0 = 0 \Rightarrow g | f \Rightarrow g = f$, & so $\min(\alpha)$ splits. ✓

<u>Ex</u>: $\mathbb{R} = \mathbb{C}^G$; $G = \{id, \text{conjugation}\}$

$z = 2+3i$ can find $\min_{\mathbb{R}}(z) = (x-(2+3i))(x-(2-3i))$
$= x^2 - 4x + 13 \in \mathbb{R}[x]$

orbit of z under G.
ie, $G \cdot \{2+3i\} = \{2+3i, 2-3i\}$

Easy to find $\min_F(\alpha)$ if know G.

(3) $\Rightarrow$ (1): E/F is f.g., so pick $\alpha_1, \ldots, \alpha_m \in E$ s.t. $E = F[\alpha_1, \ldots, \alpha_m]$. $f_i = \min(\alpha_i)$ are irred, separable polys in $f(x)$. (sep b/c E is a sep. ext'n). Take $f = \prod_{i=1}^{m} f_i \in F[x]$, f is sep (b/c all its irred factors are sep). Then E = splitting field of f b/c E/F normal & so each f_i splits completely in E. (ie, didn't add any new roots by taking the spl. field) ✓ □

<u>Cor</u>: Every finite separable ext'n is contained in a Galois ext'n.

<u>Pf</u>: Let $\alpha_1, \ldots, \alpha_m$ generate E/F. Let $f_i = \min_F(\alpha_i)$ separable in $F[x]$. Take E' = splitting field of $\prod_{i=1}^{m} f_i$. Then E'/F is Galois & contains E b/c contains $\{\alpha_1, \ldots, \alpha_m\}$.

<u>Cor</u>: If E/F is Galois & $E \supseteq M \supseteq F$ an intermediate field, then E/M is Galois.

<u>Pf</u>: E spl. field of $f \in F[x]$. Regard $f \in M[x]$, then E still spl. field of f, so E/M Gal. □

$$\begin{tikzcd}
 & E \arrow[d, dash] & \\
\text{Gal. gp } H \leq G & M \arrow[d, dash] & \text{Gal. gp } G = \mathrm{Gal}(E/F) \\
\text{need not be Gal.} & F &
\end{tikzcd}$$

b/c Gal. gp "wants to be" G/H, but can't quotient by any subgp. M/F will be Gal. iff $H \trianglelefteq G$, & then $\mathrm{Gal}(H/F) = G/H$.

*Any sep. ext'n can be put into a Gal ext'n, but what if we start w/ a non-sep ext'n?

Observation: If E/F is any algebraic ext'n. Let $E^{sep} = \{x \in E \mid \min_F(x) \text{ is sep}\}$. Then

$\underbrace{F \subseteq E^{sep}}_{\text{sep ext'n}} \subseteq E$ ↖ a field. E^{sep} is called the maximal Sep. ext'n of F in E.

[$\alpha, \beta \in E^{sep}$, then $F[\alpha,\beta]$ sep ext'n $\Rightarrow$ $\alpha+\beta, \alpha\beta, \alpha/\beta \in F[\alpha,\beta]$]

E/E^{sep} is purely inseparable

$\mathrm{Aut}(E/F) = \mathrm{Aut}(E^{sep}/F)$, ie Gal theory doesn't see anything that not sep.

4/24 Fundamental Thm of Galois Theory: Let E/F be a Gal. field ext'n, $G = \mathrm{Gal}(E/F)$. Then there exists a bijective correspondence

$$\{H \leq G\} \longleftrightarrow \{\text{intermediate fields } M,\ F \subset M \subset E\}.$$

$$H \longmapsto E^H$$

$$\mathrm{Gal}(E/M) \longmapsfrom M$$

Moreover, this correspondence satisfies:

(a) It is inclusion reversing: If $H_1 \leftrightarrow M_1$ & $H_2 \leftrightarrow M_2$, then $H_1 \leq H_2 \Leftrightarrow M_1 \supseteq M_2$

(b) relative indices correspond to degrees.

$$(H_2 : H_1) = [M_1 : M_2]$$

(c) If $\sigma \in G$ & $H \leq G$, & $M \leftrightarrow H$, then $\sigma H \sigma^{-1} \longleftrightarrow \sigma M$
$\sigma M = \{\sigma m \mid m \in M\} \subseteq E$.

(d) $H \triangleleft G \Leftrightarrow M$ is a normal ext'n of F, and then
$Gal(M/F) \simeq G/H$

all gend extns are normal

<u>Ex</u>: $F = \mathbb{Q}$, E = splitting field of $x^3 - 2$
$= \mathbb{Q}[\sqrt[3]{2} = \alpha, \beta]$, β is a root of $x^2 + \sqrt[3]{2} + \sqrt[3]{4}$ / $\mathbb{Q}[\sqrt[3]{2}]$

$Gal(E/F) = S_3$

$\left(\alpha_i = \text{cube roots of } 2 \text{ in } E \right)$

$$\begin{tikzcd}
 & F \arrow[dl, dash, "\deg_{\mathbb{Q}} \gamma = 2"'] \arrow[dr, dash, "3"] \arrow[dl, bend left, dash, "\mathbb{Z}/2\mathbb{Z} = S_3/\mathbb{Z}_3"] & \\
\text{normal } \mathbb{Q}[\zeta] \arrow[dr, dash, "\deg_{\mathbb{Q}[\zeta]} \alpha \quad 3"'] & & \mathbb{Q}[\alpha_i] \text{ not normal} \arrow[dl, dash, "2"] \\
 & E = \mathbb{Q}[\zeta, \alpha) &
\end{tikzcd}$$

$$\begin{tikzcd}
S_3 \arrow[d, dash, "2 \mid \triangleleft"'] \arrow[dr, dash, "3"] & \\
A_3 \simeq \mathbb{Z}_3 \arrow[d, dash, "3"'] & \mathbb{Z}_2 \times 3 \arrow[dl, dash, "2"] \\
(1) &
\end{tikzcd}$$

adjoin $\sqrt[3]{1}$ $\Leftarrow \left\{ \begin{array}{l} \exists \text{ normal extn btwn } \\ E \text{ \& } F;\ \deg/\mathbb{Q} = 2 \end{array} \right\} \Leftarrow$ A_3 gen by any 3 cycle $\triangleleft S_3$
$\mathbb{Z}_2$: gen by an 2 cycle, all conjugate to e/o

$M = \mathbb{Q}[\zeta]$, ζ a root of $x^2 + x + 1$.
Then M is the field of a poly / $\mathbb{Q}$ $\Rightarrow$ M/F is Gal, &
$Gal(M/F) = \mathbb{Z}/2\mathbb{Z}$.

S_3 gen by 3-cycle & any transp $\Rightarrow$ 3-cycle permutes α_i's
& 2-cycle sends ζ to ζ^2 (this is how S_3 acts on
$E = \mathbb{Q}[\zeta, \alpha]$

Let $\sigma = (1\,2\,3)$ & $\tau = (1\,2)$. Let σ act on $E = \mathbb{Q}[\gamma, \alpha]$ by
$\alpha \mapsto \alpha\zeta$, $\gamma \mapsto \gamma$ & let τ act by $\alpha \mapsto \alpha$, $\zeta \mapsto \zeta^2$
$\uparrow$ also a root of min poly of α $\qquad$ $\uparrow$ also a root of min poly of ζ

$Fix(\sigma) = \mathbb{Q}[\zeta]$, $\mathbb{Z}_3$ gen by σ
$Fix(\tau) = \mathbb{Q}[\alpha]$, $\mathbb{Z}_2$ gen by τ,
$Fix(\sigma\tau) = \mathbb{Q}[\alpha^2\zeta]$, $\mathbb{Z}_2$ gen by $\sigma\tau$
$Fix(\sigma^2\tau) = \mathbb{Q}[\alpha\zeta]$, $\mathbb{Z}_2$ gen by $\sigma^2\tau$

Pf of thm: If $H \leq G$, then let $M = E^H$. We proved

$\underset{\overset{\|}{\mathrm{Gal}(E/E^H)}}{\mathrm{Aut}(E/E^H)} = H$ (so
$$\begin{tikzcd} H \arrow[r, mapsto] & E^H \arrow[dl, bend left] \\ H & \end{tikzcd}$$
)

In the other direction, let M be an intermediate field. Look at $H = \mathrm{Gal}(E/M)$.

Aside: An ext'n E/F was Gal if F was the fixed locus of $\mathrm{Aut}(E/F)$ — $F = E^{\mathrm{Aut}(E/F)}$

$\Rightarrow M = E^H$ (so
$$\begin{tikzcd} H & M \arrow[l, mapsto] \arrow[from=1-1, to=1-2, bend right] \end{tikzcd}$$
)

Therefore the corresp. is a bijection.

(a) If $H_1 \subseteq H_2 \Rightarrow E^{H_1} \supseteq E^{H_2} \Rightarrow \mathrm{Aut}(E/E^{H_1}) \subseteq \mathrm{Aut}(E/E^{H_2})$

$\Rightarrow H_1 \subseteq H_2$. (so all statements equiv.)

(b) For $H \leq G$, we know $[E:E^H] = |H| = (H:1)$. This solves the problem when $H_1 = \{1\}$. If $H_1 \subseteq H_2$, then

$|H_2| = (H_2 : H_1) \cdot |H_1|$ $\qquad E \supseteq E^{H_1} \supseteq E^{H_2}$

$\underset{\overset{\|}{|H_2|}}{[E:E^{H_2}]} = \underset{\overset{\|}{|H_1|}}{[E:E^{H_1}]} \cdot [E^{H_1}:E^{H_2}]$ $\Rightarrow [E^{H_1}:E^{H_2}] = (H_2 : H_1)$

4/26 (c) Given H, σ, we need to identify $E^{\sigma H \sigma^{-1}} = \{x \in E \mid \sigma h \sigma^{-1} x = x \ \forall h \in H\}$

Note: $\sigma h \sigma^{-1}(x) = \sigma h \sigma^{-1}(\sigma y)$ $(y = \sigma^{-1} x)$

So $\sigma h \sigma^{-1}(x) = x \Leftrightarrow \sigma h(y) = \sigma y \Leftrightarrow$ (σ auto) $hy = y$. Therefore $x \in E^{\sigma H \sigma^{-1}}$ iff $\sigma^{-1} x = y \in E^H$ $\Leftrightarrow x \in \sigma E^H$. Therefore, $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$.

(d) ($\Rightarrow$): Assume $H \trianglelefteq G$. By (c), $\forall \sigma \in G$, $\sigma M = M$. ($M = E^H$)

So get map
$$\begin{aligned} G &\longrightarrow \mathrm{Aut}(M/F). \\ \sigma &\longmapsto \sigma|_M \end{aligned}$$

This map has kernel $\mathrm{Gal}(E/M)$ (ie, those σ that act trivially on M) $\overset{\text{b}}{=} H$. So we get an induced map $G/H \hookrightarrow \mathrm{Aut}(M/F)$.

$M^{G/H} \underset{\uparrow \text{ b/c } H \text{ acts trivially on } M}{=} M^G = F$. (b/c $M^G \subseteq E^G = F$, but $F \subseteq M^G$)

$\Rightarrow M/F$ is Galois ($\overset{\text{is}}{F}$ fixed locus of gp action on M)

↑ & ∴ normal

Then $\mathrm{Gal}(M/F) = G/H$ $\quad (F = M^{(G/H)})$

$(\Leftarrow)$: Let M be an intermediate field s.t. M/F is normal, $H = \mathrm{Aut}(E/M)$. <u>WTS</u> $H \trianglelefteq G$.

Write $M = F[\alpha_1, \ldots, \alpha_m]$.

$\min_F(\alpha_i) \in F[x]$. If $\sigma \in G$, $\sigma \cdot \alpha_i$ is also a root of $\min(\alpha_i)$. M/F normal $\overset{\leftarrow \text{all roots are in } M.}{\Rightarrow}$ $\sigma \cdot \alpha_i \in M \Rightarrow$ $\sigma \cdot M = M$ $\forall \sigma \in G \Rightarrow \sigma H \sigma^{-1} = H$ $\forall \sigma \Rightarrow H \trianglelefteq G$. □

<u>Application</u>: If M_1, M_2 are subfields, & H_1, H_2 are the corresp. subgps of G, then look at $M_1 \cdot M_2$ (smallest subfield of E containing M_1 & M_2). $M_1 \cdot M_2 \longleftrightarrow H_1 \cap H_2$

B/c $M_1 \cdot M_2$ smallest subfield of E containing M_1 & M_2 so $M_1 \cdot M_2 \longleftrightarrow$ the largest subgp of G contained in H_1 & H_2, which is $H_1 \cap H_2$.

- In particular, if $H_1 \cap H_2 = \{1\}$, then $M_1 \cdot M_2 = E$.

<u>Calculations of Gal. Gps</u>

① Cyclotomic field = $\mathbb{Q}[\zeta] =: E$ ζ a primitive 7th root of unity

a) $\mathbb{Q}[\zeta]/\mathbb{Q}$ is Galois: $\min_{\mathbb{Q}}(\zeta) = x^6 + x^5 + \cdots + 1$, & all powers of ζ are in the field & roots of $\min(\zeta)$

b) $[E:\mathbb{Q}] = 6 \Rightarrow |\mathrm{Gal}(E/\mathbb{Q})| = 6$

could be S_3 (non-comm) or $\mathbb{Z}/6\mathbb{Z}$ (comm).

Here are 6 auto. of $E/\mathbb{Q}$: $\phi_i : \zeta \mapsto \zeta^i$, $i = 1, \ldots, 6$

then $\{\phi_i\}$ as a gp wrt $\circ$ $\simeq (\mathbb{Z}/7\mathbb{Z})^{\times}$ ← units here wrt $\times$.

so $\mathrm{Gal}(E/\mathbb{Q})$ cyclic (mult. gp of finite field is cyclic)

So $\mathrm{Gal}(E/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$.

$\Rightarrow$

$$\begin{tikzcd}
 & \mathbb{Z}/6\mathbb{Z} \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\mathbb{Z}/3\mathbb{Z} \arrow[dr, "3"'] & & \mathbb{Z}/2\mathbb{Z} \arrow[dl, dash, "2"] \\
 & (1) &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
\mathbb{Q} \arrow[dr, dash, "3"] & \\
 & M \arrow[dl, dash, "2"] \\
E &
\end{tikzcd}$$

all normal b/c comm.
$\Rightarrow$ should be 2 normal intermed subfields, one of order $2/\mathbb{Q}$, one of order $3/\mathbb{Q}$.

$M = (E)^{\mathbb{Z}/2\mathbb{Z}} = \mathbb{Q}[\cos {}^{2\pi i}/_{7}]$

$[\mathbb{Q}[\cos {}^{2\pi i}/_{p}] : \mathbb{Q}] = \frac{p-1}{2}$

Let's find M explicitly: Write $(\mathbb{Z}/7\mathbb{Z})^{\times} \simeq \mathbb{Z}/6\mathbb{Z}$

$$\begin{tikzcd}[row sep=tiny] \overset{\psi}{3} & \arrow[l] 1 \end{tikzcd}$$
$\uparrow$ generator

Let $\sigma = \phi_3 : \zeta \to \zeta^3$

$\mathbb{Z}/2\mathbb{Z} = \langle \sigma^3 \rangle$ b/c $\mathbb{Z}/2\mathbb{Z} = \{0, 3\} \leq \mathbb{Z}/6\mathbb{Z}$.

Take $H = \langle e, \sigma^3 \rangle \leq Gal(E/\mathbb{Q})$. Want to find $M = E^H$

- only need to find invariants of σ^3

$\sigma^3 : \zeta \longmapsto \zeta^{27} = \zeta^6 = \bar{\zeta}$

so $\zeta + \bar{\zeta}$ is invariant under H.

look at $\mathbb{Q}[\zeta + \bar{\zeta}] \subseteq E^H$. (if order is correct, done)

$\zeta + \bar{\zeta} = 2\cos\frac{2\pi}{7} \notin \mathbb{Q}$, so nontrivial extn, so must be either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$, but not $\mathbb{Z}/6\mathbb{Z}$.

$\Rightarrow \mathbb{Q}[\zeta + \bar{\zeta}] = E^H = \min_{\mathbb{Q}}(2\cos\frac{2\pi}{7})$

What is $\min_{\mathbb{Q}}(\zeta + \bar{\zeta})$? Take all conjugates of $\zeta + \bar{\zeta}$ & mult (x - conj).

Conjugates of $\zeta + \bar{\zeta} = \alpha_1$ are $\alpha_1, \alpha_2, \alpha_3$

$\alpha_2 = \sigma(\alpha_1)$, $\alpha_3 = \sigma^2(\alpha_1)$ (then they repeat)
$= \zeta^3 + \bar{\zeta}^3$ $\quad = \zeta^2 + \bar{\zeta}^2$ $(= \zeta^9 + \bar{\zeta}^9 \pmod 7)$

so $\min_{\mathbb{Q}}(\zeta + \bar{\zeta}) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

need to compute $\alpha_1 + \alpha_2 + \alpha_3 = -1$

$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -2$

$\alpha_1\alpha_2\alpha_3 = 1$

$\Rightarrow \min_{\mathbb{Q}}(\zeta + \bar{\zeta}) = x^3 + x^2 - 2x - 1$

so $\min_{\mathbb{Q}}(\overset{\gamma}{\cos^{2\pi/7}}) = x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - 1/8$

b/c $(2\gamma)^3 + (2\gamma)^2 - 2(2\gamma) - 1 = 8\gamma^2 + 4\gamma - 4\gamma - 1$ ← not monic, ÷ 8.

4/29 ② Let E be the splitting field of $x^5 - 2 \;/\mathbb{Q}$.

$E = \mathbb{Q}[\zeta, \alpha]$, $\zeta = e^{2\pi i/5}$, $\alpha = \sqrt[5]{2}$

$$\begin{tikzcd}
 & E \arrow[dl, dash, "{}^{N}/5"'] \arrow[dr, dash, "\overset{H}{4}"] & \\
\mathbb{Q}[\zeta] \arrow[dr, dash, "4", "G/N"'] & & \mathbb{Q}[\alpha] \arrow[dl, dash, "5"] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & (1) \arrow[dl, dash, "5"'] \arrow[dr, dash, "4"] & \\
N \arrow[dr, dash] & & H \simeq \mathbb{Z}/4\mathbb{Z} \arrow[dl, dash] \\
 & G &
\end{tikzcd}$$

- $N \trianglelefteq G$, $|G| = 20$, $|N| = 5$, $H \leq G$, $|H| = 4$

  $H \simeq G/N \simeq (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$

  $\bar{2} \longleftarrow 1$

  $N \cap H = 1$ b/c $\mathbb{Q}[\alpha] \cdot \mathbb{Q}[\zeta] = \mathbb{Q}[\alpha, \zeta]$

  $\Rightarrow \underset{\text{(a s.e.s)}}{1 \to N \to G \to H \to 1}$, ie $G = N \rtimes H$

- Pick generators σ, τ of $\mathrm{Gal}(E/\mathbb{Q})$: $\quad \tau \mapsto \tau$, $\sigma \mapsto \bar{2}$

  $\sigma: \zeta \mapsto \zeta^2$, $\alpha \mapsto \alpha$ (corresp. to $1 \mapsto 2$) $\quad \tau: \zeta \mapsto \zeta$, $\alpha \mapsto \zeta\alpha$

  $\sigma^4 = 1$ (b/c $2^4 = 1$), $\tau^5 = 1$ (mult by ζ 5 times to get α)

  To describe G as a semidir. prod of N & H, need to see how τ conj. under σ ← must be power of τ b/c N normal

  $\sigma\tau\sigma^{-1}(\alpha) = \sigma\tau(\alpha) = \sigma(\zeta\alpha) = \zeta^2\alpha = \tau^2(\alpha)$ * check def of α

  $G = \langle \sigma, \tau \rangle / \langle \sigma^4 = 1, \tau^5 = 1, \sigma\tau\sigma^{-1} = \tau^2 \rangle$

Let $f \in F[x]$ separable, let E = spl. field of f. Let $\alpha_1, \dots, \alpha_n$ be the roots of f in E. Then $\exists$ map: $\mathrm{Gal}(E/F) \longrightarrow S_n$

$\phi \longmapsto$ permutation of $\{\alpha_1, \dots, \alpha_n\}$ given by ϕ.

This map is injective b/c E gen/F by $\{\alpha_i\}$'s, so if α_i fixed $\forall i$, E is fixed.

$\Rightarrow \mathrm{Gal}(E/F) \leq S_n$. How can we tell if $\mathrm{Gal}(E/F) \leq A_n$?

Write $D = \prod_{1\le i<j\le n} (\alpha_i-\alpha_j)^2$, $\Delta = \prod_{1\le i<j\le n} (\alpha_i-\alpha_j)$

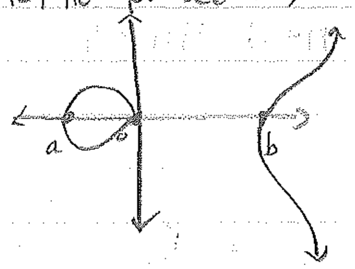
D is called the discriminant of f. $D \neq 0 \Leftrightarrow$ no mult. roots

· If $f(x) = x^2+bx+c$, then $\alpha_{1,2} = \frac{-b\pm\sqrt{b^2-4c}}{2}$

$\alpha_1-\alpha_2 = \frac{\pm 2\sqrt{b^2-4c}}{2} = \sqrt{b^2-4c} \Rightarrow D = b^2-4c$

· If $f(x) = x^3+bx+c$, $D = -4b^3-27c^2$

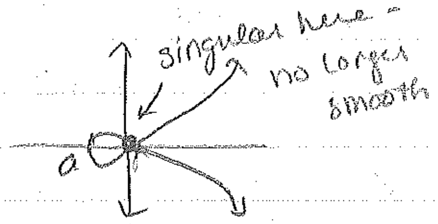
For elliptic curves: $\{y = x(x-a)(x-b)\} \subseteq \mathbb{A}^2$ is the affine part (ie, no pt at ∞)



$y = \pm\sqrt{x(x-a)(x-b)}$

(torus in $\mathbb{C}^2$ sliced by plane - 2 circles)

· If $b=0$, $y^2 = x^2(x-1)$



Let $G = Gal(E/F)$. Note: G acts on D & Δ. How?

G fixes D, ie $\sigma\cdot D = D$ $\forall \sigma\in G$. $\Rightarrow D\in F$

$\sigma\cdot\Delta = (-1)^{\varepsilon(\sigma)}\cdot\Delta$ $\forall\sigma\in G$.

$\Rightarrow \Delta\in F \Leftrightarrow G\le A_n$

But Δ is a root of $X^2-D=0$ in $F[X]$

$\Rightarrow G\le A_n$ iff D has a square root in F.

Ex: $f = x^3-2$

$D = -27(4) = -108$. D has no sq. root in $\mathbb{Q}$

$\Rightarrow G \not\le A_3$.

Note $|G|\ge 3$, but $G\not\le A_3 \Rightarrow G = S_3$.

(for cubics, only possibilities are S_3 & A_3)

Def: $f \in F[x]$ is called solvable if $\exists$ tower of fields $F_0 = F \subseteq F_1 \subseteq \cdots \subseteq F_n$ s.t. $F_i = F_{i-1}[\alpha_i]$, $\alpha_i^k = \beta_i \in F_{i-1}$ (add a k-th root of an elt in F_{i-1}) and F_n contains a splitting field of f.

Thm: f is solvable iff $Gal(E/F)$ is solvable, where E is the spl. field of f/F.
(we won't prove)
→ for each ext'n the Gal. gp will be abel.

Thm: The general degree-n polynomial has Gal. gp S_n.
("general" is well-defined)

Cor: Since S_5 is not solvable, $\exists$ degree 5 polys which are not solvable.

5/1 Thm: Let $f \in \mathbb{Q}[x]$, deg $f = p$ prime, f irred. Assume f has exactly 2 complex roots. If E is a spl. field of $f/\mathbb{Q}$, then $Gal(E/\mathbb{Q}) \simeq S_p$

Pf: Idea: Show that $Gal(E/\mathbb{Q}) \ni \{$p-cycle, transposition$\}$, which gen. S_p.
$\uparrow \Leftrightarrow$ elt of order p
b/c p prime

Transposition comes from conjugation
p-cycle: Note that adding one root of f, ζ_1, to $\mathbb{Q}$ gives $\mathbb{Q}(\zeta_1)$ whose deg/$\mathbb{Q}$ is p.
$E \supseteq \mathbb{Q}(\zeta_1) \supseteq \mathbb{Q} \Rightarrow p \mid [E:\mathbb{Q}] \Rightarrow p \mid |Gal(E/\mathbb{Q})|$
$\Rightarrow Gal(E/\mathbb{Q})$ has an elt of order p (by Cauchy). $\square$

Fact: If $f(x) = x^n - a$, a not an n^{th} root in F, f irred. $\overset{\text{\& separable}}{,}$ then $\mathrm{Gal}(E_f/F)$ is solvable, where E_f is the spl. field of f.

- need to add n^{th} root of a which gives cycl. gp of order n inside Gal & add n^{th} roots of unity, which is $\cong (\mathbb{Z}/m\mathbb{Z})^{\times}$, which is abel. Extn of 2 abel. gps is solvable.

(Revisit $x^5 - 2$)

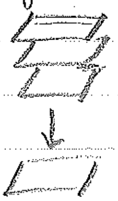
Grothendieck Galois Theory

$$\begin{tikzcd} Y \arrow[d, "\pi"', "\text{cts}"] \\ X \end{tikzcd}$$

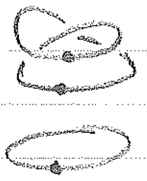
X, Y top. sp's. We say this is a covering (map) if $\forall x \in X$ $\exists$ nbhd $U \ni x$ open s.t. $\pi^{-1}(U) \underset{\uparrow \text{homeomorphic}}{\cong} U \times S$, S a set w/ discrete top.

ie, locally, Y looks locally like a bunch of copies of X.

Ex:



Ex:

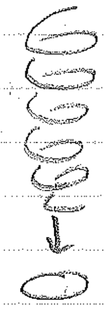


map $z \mapsto z^2$ for

$$\begin{array}{ccc} S^1 & \to & S^1 \\ \cap & & \cap \\ \mathbb{C} & & \mathbb{C} \end{array}$$

b/c $\sqrt{\ }$ exists locally, locally homeo.

Ex:



$\mathbb{R} \to S^1$

$t \mapsto e^{2\pi i t}$

Homotopy Lifting Prop: If $\pi: Y \to X$ is a covering map & $f: I = [0,1] \to X$ is a path starting at $x_0 = f(0)$ & if $y_0 \in \pi^{-1}(x_0)$, $\exists!$ path $\bar{f}: I \to Y$ s.t. $f(t) = \pi(\bar{f}(t))$ & $\bar{f}(0) = y_0$

Fact: There always exists a space $\bar{X}$ which is ctd & simply ctd. & a map $\bar{X} \to X$ (X assumed to be ctd)

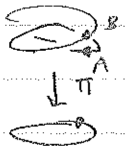
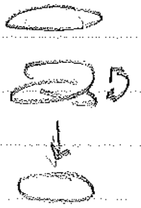
Ex: S^1 not s.ctd, but is simply ctd.

$\bar{X}$ is the <u>universal covering space</u>.

Dictionary

Grothendieck top on schemes (like $X = \mathrm{Spec}(k)$)

- open sets are certain maps from other top. sp's

Field Theory	Topology
F a field (char 0)	X a top. sp, ctd
• $\bar{F}$ an algebraic closure	• $\bar{X}$ a universal covering sp
• $E \supseteq F$ a field ext'n (sep.)	• $Y \xrightarrow{\pi} X$ a ctd covering "‖" Spec E "‖" Spec F
• $\mathrm{Aut}(E/F) = G$ $H \leq G$	• $G = \mathrm{Aut}(\pi)$ ~ deck transf. $\supseteq H$ Ex:  $\circlearrowleft \phi$ · ϕ can only map $A \to B$ "deck" $\pi \circ \phi = \pi$ Here, $G = \mathbb{Z}/2\mathbb{Z}$
• $E^H \supseteq F$	• Y/H " $\to X$, where
• E/F is Galois $\Leftrightarrow E^G = F$	• Y/X " is Galois (regular) iff $Y/G \cong X$ ($\Leftrightarrow$ $\mathrm{Aut}(\pi)$ acts transitively on each fiber $\pi^{-1}(x)$) Ex:  $\leftarrow \phi \Rightarrow \mathrm{Aut}\,\pi = \mathbb{Z}/2\mathbb{Z}$ but fiber has 3 pts, so can't act transitively
• $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \oplus \mathbb{C}$	

for Spec to be disctd, iff idempotents

tensor prod of fields not nec. a field

5/3

$\mathrm{Gal}(\bar{F}/F) =$ absolute Galois gp of F

Fields

• {set S w/ action of $\mathrm{Gal}(\bar{F}/F)$}

$\updownarrow$ 1-1

{sep. ~~extension~~ algebra E/F}

$E \longmapsto \mathrm{Maps}_F(E, \bar{F})$ = embedds of E into $\bar{F}$ which preserve the given embedding of F in $\bar{F}$

$S \longmapsto S \times_{\mathrm{Aut}(\bar{F}/F)} \bar{F}$

Claim: This establishes a 1-1 bij. correspondence.

Problem - b/c Y may not be ctd, E may have 0-divisors, so need sep. alg, not ext'n.

The corresp. interchanges $\otimes_F$ and $\times$ of sets w/ action

Ex: $\{\mathbb{C}/\mathbb{R}\} \longleftrightarrow$ {set w/ action of $\mathrm{Gal}(\bar{\mathbb{R}}/\mathbb{R}) = \mathbb{Z}/2$}

$S = 2$ pts

$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$

$\{0,1,0',1'\}$ w/ action of $\mathbb{Z}/2\mathbb{Z}$

$0 \leftrightarrow 1$, $0' \leftrightarrow 1'$ $= \{0,1\} \sqcup \{0,1\}$

(idempotents: $i \otimes 1 + 1 \otimes i$ & $i \otimes 1 - 1 \otimes i$ X

↑ need 2 idempotents to have this iso.)

Top. Sp.

• {set S w/ action of $\mathrm{Aut}(\bar{X}/X)$}

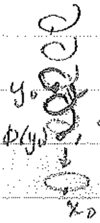
$\updownarrow$ 1-1

{covering sp. Y of X} ← possibly discntd

Let $y_0 \in \bar{X}$, $x_0 = \pi(y_0)$, $\pi : \bar{X} \to X$.

Then $\mathrm{Aut}(\bar{X}/X) = \pi_1(X)$ (fundamental gp)

$\phi \in \mathrm{Aut}(\pi)$



← proj. of path $y_0 \to y_1$ (f):

$\pi \circ f : I \to X$, is a loop at x_0 that wraps around twice $\rightsquigarrow \pi \circ f \in \pi_1(X, x_0)$.

This is the bijection: S = set of fiber of x_0.

$S \longmapsto S \times_{\mathrm{Aut}(\bar{X}/X)} \bar{X} = \{(s,x) \mid s \in S, x \in \bar{X}\} / (\phi \cdot s, x$ $\cong$ $(s, \phi$ $\forall \phi \in \mathrm{Aut}(\bar{X}$

(If $S = \mathrm{Aut}(\bar{X}/X)$, prod $= \bar{X}$

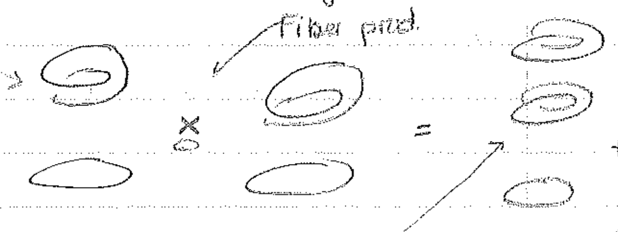
If $S =$ pt, prod $= X$)

$\mathrm{maps}_X(\bar{X}, Y) \longleftarrow\!\shortmid\, Y$

$= \{f : \bar{X} \to Y \mid f \circ \pi_Y = \pi_{\bar{X}}\}$

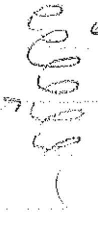
$Y \xrightarrow{\pi_Y} X$, $\bar{X} \xrightarrow{\pi_{\bar{X}}} X$

$y_0 \in \bar{X}$. What is $\mathrm{Maps}_X(\bar{X}, Y) = \pi_Y^{-1}(x_0)$ where $x_0 = \pi_{\bar{X}}(y_0)$



action fac thru $\mathbb{Z}/2$ · ↙ 2 loops to get back to beginn

action ↙ fac thru $\mathbb{Z}/6$ (6 lo to g back begi



$\overset{2}{\{0,1\}} \times \overset{2}{\{0',1'\}} =$ 4

$\overset{2}{\{0,1\}} \times \overset{3}{\{0',1',2'\}} = \{0,1,2,3,4,5\}$ 6

w/ action of $\mathbb{Z}$

5/6 Def: Let k be a field. An f.d. algebra A over k is separable iff for every ext'n $L \supseteq k$, we have $L \otimes_k A$ is semisimple.

Thm: A is separable iff $A = \prod_{i=1}^{n} M_{n_i}(D_i)$ where $n_i > 0$, D_i's are division alg's & $Z(D_i)$ is a finite sep. ext'n of k.
↳ f.d over center

$\Rightarrow$ A is sep. & comm. $\Rightarrow$ $A = \prod_{i=1}^{n} k_i$, k_i / k a fin. sep. ext'n.

(this is closed under tensor prod's & contains all sep. ext'ns)

Fact: If A & B are f.d. separable k-alg's, so is $A \otimes_k B$.
(if they are field ext'ns, then $i=1$ only) if tensor 2 field ext'ns, get ring that's prod of fields.
(field ext'n $\Leftrightarrow$ ctd cover, sep alg $\Leftrightarrow$ not nec. ctd cover)
tensor $\Leftrightarrow$ fiber prod

Traces in finite field ext'ns or sep. alg's

Let A/k be a f.d. alg$/k$. Define $\mathrm{Tr}: A \to k$ w/
$\mathrm{Tr}(x) = \mathrm{Tr}(\cdot x : A \to A)$
↳ operator "mult by x"; k-linear b/c $k \subseteq Z(A)$.
think of A as a f.d. v. sp $/k$.

Ex: ① $\mathbb{C}/\mathbb{R}$

$\mathrm{Tr}: \mathbb{C} \to \mathbb{R}$? Pick a basis $\{1, i\}$ of $\mathbb{C}$. If $x \in \mathbb{C}$, $x = a + bi$

$(a+bi)(1) = a+bi$
$(a+bi)(i) = -b + ai$ $\Rightarrow$ $(\cdot x): \mathbb{C} \to \mathbb{C}$ has basis $\begin{pmatrix} a & -b \\ +b & a \end{pmatrix}$

so $\mathrm{Tr}: \mathbb{C} \to \mathbb{R}$
$z \mapsto 2\mathrm{Re}(z)$

② $F(T^p) \subseteq F(T)$, char $F = p$. (a purely insep. field ext'n)

Basis: $\{1, T, T^2, \dots, T^{p-1}\}$ dim of ext'n is p

What is $Tr: F(T) \to F(T^p)$? zero map: $Tr(z) = 0\ \forall z$.

$Tr(1) = p = 0$ (b/c $1 = I$)

$\uparrow$ b/c $= \dim_{F(T^p)} F(T)$

$Tr(T) = 0$ • mult by T shifts basis one to right, so matrix is off diagonal $\begin{pmatrix} 0 & * & & \\ & 0 & \ddots & \\ & & \ddots & * \\ * & & & 0 \end{pmatrix}$

$Tr(T^2) = 0$ $\longrightarrow$ • shifts basis 2 to right

$Tr(T^i) = 0$ b/c permutes all basis elts, so get no zeros on diagonal.

Fact: If E/F is Galois, then $Tr(x) = \sum_i \sigma_i(x)$ where $\sigma_i \in Gal(E/F)$

$\in F$ b/c if act by elt of Gal(E/F), elts just get permuted:

$\sigma \cdot \sum \sigma_i(x) = \sum \sigma \cdot \sigma_i(x) = \sum \sigma_i(x)$

$\Rightarrow Tr(x) \in E^{Gal(E/F)} = F$

Note for ex #1 $\sum \sigma_i(z) = z + \bar{z} = 2\,Re(z)$, so works.

Fact: If E/F is separable, then $\langle -,- \rangle : E \times E \longrightarrow F$

$\langle x, y \rangle = Tr(x \cdot y)$

is a nondegenerate, invariant, F-bilinear pairing on E.

$\hookrightarrow \langle x \cdot y, z \rangle = \langle x, y \cdot z \rangle$

$\hookrightarrow \langle x, y \rangle = 0\ \forall y \Rightarrow x = 0$.

- This characterizes separable alg's (ie, the pairing is nondegen iff alg. sep)

ex 2: clearly not degen b/c $\langle x, y \rangle = 0\ \forall x, y$.

ex 1: $\langle x, y \rangle = 2\,Re(x \cdot y) = 2(ac - bd) \neq 0$ for $x, y \neq 0$.

if a, b fixed & $= 0\ \forall$ b, c, then $a = b = 0$.

There exists a 1-1 bij. corresp. which commutes w/ "correct" products

$\{\text{finite sets } S \text{ w/ action of } Gal(\bar{F}/F)\} = A$, $\times$, $\amalg$

$\updownarrow$

$\{\text{f.g. separable comm. } F\text{-alg's}\} = B$, $\otimes$, $\oplus$ (analogue of result for covering sp's)

$E \in B \longmapsto Hom_F(E, \bar{F}) \in A$

$S \times_{Gal(\bar{F}/F)} \bar{F} \longleftarrow\!\shortmid S \in A$

$= \{(s,f) \in S \times \bar{F}\} / \langle (s\sigma, f) = (s, \sigma f) \rangle$

$\times$: $g\cdot(a,b) = (ga, gb)$

$\oplus$: $g(a,b) = \underbrace{(ga, b) \amalg (a, gb)}_{\text{Not?}}$

<u>Ex</u>: $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \oplus \mathbb{C}$ ($\simeq$ as comm rings) $Gal(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$

$\mathbb{C} \longmapsto \{\mathbb{Z}/2\mathbb{Z}\}$ w/ action of Gal

$\mathbb{C} \otimes \mathbb{C} \longmapsto \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \amalg \mathbb{Z}/2\mathbb{Z}$ b/c Gal acts on 2 sets separately

$\mathbb{C} \oplus \mathbb{C} \longleftarrow\!\shortmid \mathbb{Z}/2\mathbb{Z} \amalg \mathbb{Z}/2\mathbb{Z}$

$\mathbb{C} \otimes \mathbb{C} \longmapsto \mathbb{Z}/2\mathbb{Z}$ acting on $S \times S$ by digonal action

$\Rightarrow$ $\mathbb{C} \otimes \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C} \longleftarrow\!\shortmid S \amalg S \cong S \times S$ as sets w/ G action

$S_1 = \{0, 1\}$ $S_2 = \{a, b\}$ $G = \{e, f\}$ $e = id$, $f(0) = 1$ $f(1) = 0$ $f(a) = b$ $f(b) = a$

$S_1 \times S_2 = \{(0,a), (0,b), (1,a), (1,b)\}$

w/ action

$f: (0,a) \longmapsto (1,b)$

$(0,b) \longmapsto (1,a)$

$(1,a) \longmapsto (0,b)$

$(1,b) \longmapsto (0,a)$

$S_1 \amalg S_2 = \{0, 1, a, b\}$

$f: 0 \leftrightarrow 1$

$a \leftrightarrow b$

Isomorphism: $S_1 \times S_2 \cong S_1 \amalg S_2$

$h: S_1 \amalg S_2 \longrightarrow S_1 \times S_2$

$0 \longmapsto (0,a)$, $1 \longmapsto (1,b)$ } b/c needs to be equivariant under f.

$a \longmapsto (1,a)$

$b \longmapsto (0,b)$

(there are 8 possible such iso's)

4 choices for 0, none for 1

2 for a, none for b

8 iso's btwn $\mathbb{C} \otimes \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$

Find them by finding idempotents

5/8 $F \subseteq E = F[\alpha_1, \dots, \alpha_n]$. We'd like to write $E = F[\gamma]$. This is not always possible:

Ex: $F = k[X^p, Y^p] \subseteq E = k(X,Y)$, k alg. closed & char $k = p$.
(a double purely inseparable ext'n – $t^p - X^p = 0$, in $k(X,Y) \Rightarrow (t-X)^p$, so one root w/ mult. p). → deg p^2

Fact: There exist infinitely many intermediate fields btwn E & F, $F \subseteq M \subseteq E$.

Pf: Take $M = F[X + cY]$, $c \in k$.

$\underbrace{F \subset M}_{p}\underbrace{\subset E}_{p}$, so $M \neq F$ & $M \neq E$

If $F[X+cY] = F[X+c'Y]^{=M}$, $c \neq c'$, then X is a lin comb $X = a(X+cY) + b(X+c'Y) \Rightarrow X \in M \Rightarrow Y \in M$
$\Rightarrow M = F[X,Y]$, a contradiction.

Claim: If $E = F[\gamma]$ for some γ (ie, E is primitively gen'), then $\exists$ only finitely many $F \subseteq M \subseteq E$.

Pf: (If γ sep, then $F[\gamma]$ contained in a Gal. ext'n, so clear)

(*) Claim: $\forall M$, let $g(x) = \min_M \gamma$. Then $M = F[\text{coeff's } \overset{\in M}{\text{of}}\ g]$
$\Rightarrow$ big claim: Let $f = \min_F \gamma$. Then $g | f$. $\Rightarrow$ finitely many g's b/c get g by looking at roots of f in a splitting field, & choosing some subset.
$\Rightarrow$ finitely many M.

Pf of (*): Let $M' = F[\text{coeff's of } g]$. $\Rightarrow M' \subseteq M$.
$[E:M] = \deg g = [E:M'] \Rightarrow M = M'$.
Note $E = M[\gamma]$ & $M'[\gamma]$, because these fields already contain F.
$\min_{M'} \gamma = g'$: so $g' | g$. but if $\deg g' < \deg g$, then g is not the min poly $/M'$ $\Rightarrow g = g'$

□

These 2 facts prove that the example is not a simple ext'n → if it were, there would be fin many subfields, but there are ∞ many. Happens b/c X & Y are both purely inseparable.

Primitive Element Thm: Let $E = F[\alpha_1, \dots, \alpha_n]$, w/ $\alpha_2, \alpha_3, \dots, \alpha_n$ separable $/F$ (ie, can have at most 1 insep. elt). Then $\exists \gamma \in E$ s.t. $E = F[\gamma]$.
(γ is actually just a lin. comb. of α_i's $/F$).

Pf #1: If F is finite. (& so E is finite, b/c a f.d. v. sp over finite field). Then $E^* = E \setminus \{0\}$ is cyclic, say gen by γ. Then clearly $E = F[\gamma]$.
(b/c can get all powers of γ, which is everything but 0, which is in F).

Pf #2: If F is infinite. By induction, can reduce to case $n=2$. $E = [\alpha, \beta]$, β is sep $/F$. Let f, g be min. polys of α & β $/F$. Want to find $c \in F$ s.t.

(*) β is the only common root of $g(x)$ & $f(\alpha + c\beta - cx)$.
(ie, if $\gamma = \alpha + c\beta$.)

Claim: $E = F[\gamma] = F'$

Pf: $E \supseteq F[\gamma]$ (b/c γ a lin. comb. of $\alpha, \beta \in E$).
Note that $g(x)$ & $f(\gamma - cx)$ are in $F'(x)$
Then $\gcd(g(x), f(\gamma - cx)) = x - \beta \Rightarrow \beta \in F'$
$\gamma \in F' \Rightarrow \alpha \in F' \Rightarrow F' = E$

Pf of (*): Fix a random $c \in F$, set $\gamma = \alpha + c\beta$. β is a root of $f(\gamma + cx)$ (b/c $= f(\gamma - c\beta) = f(\alpha) = 0$). $\Rightarrow \beta$ is a common root of $g(x), f(\gamma - cx)$. But the roots of $f(\gamma - cX)$ are of the for $\gamma - cX = \alpha_i$, where α_i is a root of $f(X)$. $\Rightarrow X = \frac{\gamma - \alpha_i}{c} = \frac{\alpha + c\beta - \alpha_i}{c} \Rightarrow$ $X = \frac{\alpha - \alpha_i}{c} + \beta$. As long as these x's never match roots of g other than β will be ok. As long as $\beta' \neq \beta$ c is uniquely determined. if we want to get $\beta' = \frac{\alpha - \alpha_i}{c} + \beta \Rightarrow c = \frac{\alpha - \alpha_i}{\beta' - \beta}$.

Want to take $c \neq$ any value $\frac{\alpha-\alpha_i}{\beta'-\beta}$ for $\beta \neq \beta'$ (β', $\overset{\text{runs through}}{\wedge}$ roots of g)

Choose any other $c \in F$ & then (*) holds. (Can do this b/c F is ∞).

<u>Ex</u>: $F = \mathbb{Q}$, $E = \mathbb{Q}(\overset{\alpha}{\sqrt{2}}, \overset{\beta}{\sqrt{3}})$

$f(x) = x^2 - 2$, $g(x) = x^2 - 3$

roots of f : $\pm\sqrt{2}$, roots of g : $\pm\sqrt{3}$

The excluded values of c are: $\frac{\alpha-\alpha}{\beta'-\beta} = 0$, $\frac{2\sqrt{2}}{2\sqrt{3}} = \frac{\sqrt{2}}{\sqrt{3}} \notin \mathbb{Q}$

(only 2 b/c $\beta' \neq \beta$)

Pick any $c \in \mathbb{Q}$, $c \neq 0$ (eg, $c = 1$). The proof claims that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\underset{\overset{\shortparallel}{x}}{\sqrt{2}+\sqrt{3}})$

$x^2 - 5 = 2\sqrt{6} \Rightarrow (x^2-5)^2 = 24$ → monic min. poly of x.

<u>Pf</u>: $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \underset{\sigma}{\mathbb{Z}/2\mathbb{Z}} \oplus \underset{\tau}{\mathbb{Z}/2\mathbb{Z}}$ (Klein 4-gp)

$\sigma: \sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$ $\tau: \sqrt{2} \to \sqrt{2}$, $\sqrt{3} \to -\sqrt{3}$ (& $\sigma\tau: \sqrt{2} \to -\sqrt{2}$, $\sqrt{3} \to -\sqrt{3}$)

$\Rightarrow \{\sigma \in \mathrm{Gal} \mid \sigma x = x\} = \{e\}$

$$\mathbb{Q} \leq \underbrace{\mathbb{Q}(\sqrt{2}+\sqrt{3}) \leq \mathbb{Q}(\sqrt{2},\sqrt{3})}$$

$\leftrightarrow H \leq \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

But only $\{e\}$ fixes $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \Rightarrow H = \{e\}$

$\Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. ✓

$$\begin{tikzcd} H = \{e\} \arrow[d, leftrightarrow] \\ \mathbb{Q}(\sqrt{2},\sqrt{3}) \end{tikzcd}$$

5/10 {finite sets w/ a transitive action of $\overset{G}{\overset{\shortparallel}{\mathrm{Gal}}}(\overline{F}/F)$}

G/H (set of cosets)

↕ 1:1

{finite$\underset{\text{sep.}}{\wedge}$field ext'ns E of F}

H {subgp $H \le \overset{G}{\overset{\shortparallel}{\mathrm{Gal}}}(\overline{F}/F)$} of finite index

get an action on G/H, that is trasitive, so go from subgp → fin. set. w/ trans. action. But do we get all fin sets w/ trans action? ie, can we go back? [Aside, given trans action, # of elts in set will ÷ order of Gp]

$$\begin{array}{r}\mathbb{Z}/6\mathbb{Z} = G\\ \vee\!\mid\\ \mathbb{Z}/3\mathbb{Z} = H\end{array}$$

$\hookrightarrow \{0,2,4\} \le \mathbb{Z}/6\mathbb{Z}$

$G/H = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}+H, \bar{1}+H\}$

Stab of $\bar{0}+H$ will recover H.

- If G acts on a set S, $e \in S$, $\mathrm{Stab}(e) \le G$, If action is transitive, thus $S \cong G/H$

But G/H has a distinguished pt (the identity), & S doesn't. So if had set w/ distinguished pt, S, then could recover H

So:

$$\begin{tikzcd}
\left\{\begin{array}{l}\text{finite sets, } S, \text{ w/ a trans}\\ \text{action of } G \text{ w/ a base pt}\end{array}\right\} \arrow[r, leftrightarrow] & \left\{\begin{array}{c}\text{subgps } H \le G \text{ of}\\ \text{fin. index}\end{array}\right\} \\
(G/H, e+H) & H \arrow[l, mapsto] \\
(S, s) \arrow[r, mapsto] \arrow[d, leftrightarrow] & \mathrm{Stab}_G(s) \le G \\
\left\{\text{fin. sep. field ext'ns } E \text{ of } F \ \&\ \text{a map} /F \ \ E \to \overline{F}\right\} &
\end{tikzcd}$$

(ie, get an embedding into alg. closure)

Recall:

$$\begin{tikzcd}
 & \{\text{sets w/ action of } \mathrm{Aut}(\bar{X}/X)\} \arrow[ddd, leftrightarrow] & \\
\mathrm{Maps}_X(Y, \bar{X}) & & S \arrow[d, mapsto] \\
Y \xrightarrow{\pi} X \arrow[u, mapsto] & & S \times_{\mathrm{Aut}(\bar{X}/X)} \bar{X} \\
 & \{\text{covers } Y \xrightarrow{\pi} X \text{ of } X\} &
\end{tikzcd}$$

- think what a distinguished pt of set would be.

So we have:

$$\begin{tikzcd}
\{H \leq G = \mathrm{Gal}(\bar{F}/F)\} \arrow[d, leftrightarrow] \\
\{F \subseteq E \subseteq \bar{F}\}
\end{tikzcd}$$

(ie, intermediate fields w/ embedding into alg. closure}

$\Rightarrow$ Begins to look like Galois correspondence.

Start w/ $F \subseteq E \subseteq \bar{F}$. This fixes $H_2 \leq \mathrm{Gal}(\bar{F}/F)$

$$\begin{tikzcd}
\{H_2' \text{ fixed}, \ H_2 \leq H_1 \leq G\} \arrow[d, leftrightarrow] \\
\{F \subseteq M \subseteq E \subseteq \bar{F}\}
\end{tikzcd}$$

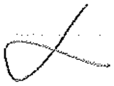
Precisely: For a fixed field ext'n E/F, w/ a fixed embedding $E \hookrightarrow \bar{F}$, get a gp inclusion $H \leq G$.

$$\begin{tikzcd}
\{\text{Intermediate gps } H \leq H' \leq G\} \arrow[d, leftrightarrow, "1:1"] \\
\{\text{intermediate fields } F \subseteq M \subseteq E\}
\end{tikzcd}$$

If add: fixed Gal. field ext'n $\Rightarrow H \trianglelefteq G$

$$\begin{tikzcd}
\{\text{Intermed. } H \leq H' \leq G\} \arrow[r, leftrightarrow, "1:1"] \arrow[d, leftrightarrow, "1:1"] & \{\text{Subgps of } G/H\} \\
\{\text{Intermed. fields } F \subseteq M \subseteq E\} &
\end{tikzcd}$$

(the quotient is the rel. Gal. gp.)

Given alg. variety :  , How can we discuss the tangent space?

Zariski : can define it alg, & it will make sense even if pt not smooth, ie, here , unlike in geom.

Let $(A, \underline{m})$ be a local ring w/ residue field $k = A/\underline{m}$.
Define $T = (\underline{m}/\underline{m}^2)^{\vee}$, where $\vee$ means dual wrt k.
Called the <u>Zariski tangent space</u>.

<u>Ex</u> : Tangent to line at pt 0. <u>line</u> : $A = k[x]_{(x)}$ ← corresp. to pt 0

Spec ↑ max ideals here corresp. to pts on line, & (x) corresp to 0.

$A = k[x]_{(x)} = \{ \frac{f}{g} \mid f, g \in k[x], g(0) \neq 0 \}$ ← has nontrivial const term.

(if $g = 1$)

$\underline{m} = (x)$, $\underline{m}/\underline{m}^2$ is 1-dim : $f \longleftrightarrow$ coeff of $x = \frac{\partial f}{\partial x}\Big|_{x=0}$

$\frac{x^3+x^2+2x+1}{x^2+x}$

Tangent vector e.g. $\partial/\partial x \longleftrightarrow$ map $\{$functions which are zero at x$\} \to k$

$\underline{m}$" $f \longmapsto \partial f/\partial x \big|_{x=0}$

$f, g \in \underline{m}$, $\partial/\partial x (fg)\big|_{x=0} = 0$ (b/c both zero at x)
so get map $\underline{m} \xrightarrow{\phi} k$ s.t. $\phi|_{\underline{m}^2} = 0$, ie get map $\underline{m}/\underline{m}^2 \to k$.

$\Updownarrow$

an element of $(\underline{m}/\underline{m}^2)^{\vee}$

<u>Def</u> : We say $(A, \underline{m})$ is <u>regular</u> if $\dim_k \underline{m}/\underline{m}^2 = \dim A$
(alg. notion that parallels "smooth")

↑ dim of a ring is length of longest chain of ideals.

We say Spec A <u>smooth</u> at a pt $\underline{p}$
$\Leftrightarrow (A_{\underline{p}}, \underline{p}A_{\underline{p}})$ is regular.