(Zorn's lemma) Let $(P, \leq)$ be a POSET. If for every chain $C \subseteq P$ there exists $b \in P$ s.t. $(\forall a \in C)[a \leq b]$, then $\exists m \in P$ maximal. 3/14/2022

Theorem. Let R be a ring with 1. If $I \subsetneq R$ is ideal, then there exists $J \subsetneq R$, $J \supseteq I$ such that J is a maximal ideal.

Proof: Consider $P := \{J \text{ ideal} \mid J \subseteq R, 1 \notin J, J \supseteq I\}$ (to show)

Think of the poset $(P, \subseteq)$ (subset). Clearly if $M \in P$ is maximal, then $M \supseteq I$, $1 \notin M$ (so $M \subsetneq R$) and M is an ideal. So M is a maximal ideal as required.

"Let $C \subseteq P$ be a chain. $b := \bigcup C$. Clearly $J \in C \Rightarrow J \subseteq b$ (def union).

Since $J \in C \Rightarrow J \supseteq I$, we have $b \supseteq I$

Since $J \in C \Rightarrow 1 \notin J$, " $1 \notin b$.

(to show b is an ideal)

1) Given $\alpha, \beta \in b$, there are ideals $J_\alpha, J_\beta \in C$ s.t. $\alpha \in J_\alpha$, $\beta \in J_\beta$. Since C is a chain, either $J_\alpha \subseteq J_\beta$ or $J_\beta \subseteq J_\alpha$. WLOG let $J_\alpha \subseteq J_\beta$. $\alpha \in J_\alpha$ by choice of J_α, so $\alpha \in J_\beta$ by inclusion. Since J_β is an ideal $\alpha - \beta \in J_\beta \subseteq b$. So b is a subgroup w.r.t addition.

2) [Closure under left multiplication] Let $\alpha \in b$, $r \in R$ be given. Take $J_\alpha \in C$ s.t. $\alpha \in J_\alpha$. As J_α ideal, $r\alpha \in J_\alpha \subseteq b$. "

* An application of ZL proves existence of the maximal ideal.

Goal: "Given F there exists $E \supseteq F$ s.t. E is alg closed".

We deal with rings of polynomials in several variables.

$R[x]$ $R[x,y]$, natural definition for $R[x_1, x_2, \ldots x_n]$
$y + x^2 + 7 \ldots$

Fact $R[x_1, \ldots x_{n+1}] = R[x_1, \ldots x_n][x_{n+1}]$

($\subseteq$) 'Factorization'
($\supseteq$) 'Easy'

Def. let I (possibly infinite) be a set, R be a rng.

$$R^I = R[\{x_i \mid i \in I\}] := \bigcup_{\substack{I_0 \subseteq I \\ \text{finite}}} R[\{x_i \mid i \in I_0\}] \quad \left(\simeq R[x_1, \dots, x_n]\right)$$

Given $p(\bar{x}), q(\bar{y}) \in R^I$ (vector), let $I_0 \subseteq I$ finite s.t. $\bar{x} \cup \bar{y} \subseteq \{x_i \mid i \in I_0\}$

($I_0 = I_p \cup I_q$, where $p(\bar{x}) \in R[\{x_i \mid i \in I_p\}]$, $q(\bar{y}) \in R[\{x_i \mid i \in I_q\}]$

clearly $p, q \in R[\{x_i \mid i \in I_p \cup I_q\}]$ so we can define

I_0 finite $\quad p +_{R^I} q := p +_{R_{I_0}} q$ valid in finite rng

$p \cdot_{R^I} q := p \cdot_{R_{I_0}} q$ similarly)

So we have proved that R^I is a rng (R comm $\Rightarrow R^I$ comm)

Also R has $1 \Rightarrow R^I$ has 1

R int domain $\Rightarrow R^I$ int domain

(later (7L))

Key lemma: For every field K, there exists a field $K^* \supseteq K$ s.t. $\forall p \in K[x]$, $\exists a_p \in K^*$ root of p.

(Here p comes from $K[x]$, not $K^*[x]$, so this is a bit weaker.)

Proof of Theorem using KL. Given F, by induction on $n \in \mathbb{N}$ define $\{K_n \mid n \in \mathbb{N}\}$ fields s.t. $K_0 \subseteq K_1 \subseteq K_2$ "tower" $K_0 = F$, $K_{n+1} = K_n^*$ (using the key lemma repeatedly). Let $E := \bigcup_{n \in \mathbb{N}} K_n$.

Claim: E is an algebraically closed field extending F.

Pf. (E is a field) $\alpha, \beta \in E \Rightarrow \exists n_\alpha, n_\beta$ s.t. $\alpha \in K_{n_\alpha}$, $\beta \in K_{n_\beta}$. Since $K_n \subseteq K_{n+1}$, WLOG $K_{n_\alpha} \subseteq K_{n_\beta} \Rightarrow \alpha, \beta \in K_{n_\beta} \Rightarrow \alpha - \beta \in K_{n_\beta} \subseteq E$. Same proof for multiplication in $E \setminus \{0\}$.

(E is alg closed) Given $p \in E[x]$, write $p = \sum_{k=0}^{n} a_k x^k$, $a_k \in E$. So there is $\{n_k \mid k \le n\} \subseteq \mathbb{N}$ (indexing), $a_k \in K_{n_k}$. Let $m = \{n_k \mid k \le n\}$. Since $K_i \subseteq K_{i+1}$ $\forall i$, $K_m \supseteq K_{n_k}$ $\forall k \le n$. So $p \in K_m[x]$. By the lemma $K_{m+1} = K_m^*$, so $\exists \alpha_p \in K_{m+1} \subseteq E$ root of p. 45

3/16/22

Proof of Key Lemma: $\forall k, \exists k^* \supseteq k$ s.t. $\forall p \in k[x]$, $\exists \alpha \in k^*$, $p(\alpha) = 0$

(Fact: ZL) R commutative with 1, $I \subsetneq R$ ideal $\Rightarrow \exists J \subsetneq R$ maximal ideal containing I.

For any index set I, R ring, recall $R[\{x_i \mid i \in I\}]$ is a ring of polynomials.

Let $R = k[\{x_p \mid p \in k[x]\}]$. This is a commutative ring with $1_R = 1_k$.

($k[x]$ is the index set)

Consider $A = \{p(x_p) \mid p \in k[x]\}$, $A \subseteq R$. Let $J = (A)$, i.e. J is the ideal generated by A.

But we can write explicitly $(A) = \{\sum_{i=1}^{n} r_i \cdot a_i \mid n \in \mathbb{N}, a_i \in A, r_i \in R\}$

- Claim: $1 \notin R$ (i.e. $1 \notin J$) - see later.

By ZL, there exists $J \subsetneq R$ maximal s.t. $J \supseteq I$. Let $k^* := R/J$. Since J is maximal and k is commutative, k^* is a field. Given $p \in k[x]$, we show $\alpha := x + J$ is a root of p. Suppose $p = \sum_{\ell=0}^{n} a_\ell x^\ell$, we compute $p(\alpha)$ in k^*: $p(\alpha) = \sum_{\ell=0}^{n} a_\ell (x+J)^\ell$ $(\in k^*)$

$(x+J)(y+J) = xy + J \ldots$

$$= \sum_{\ell=0}^{n} a_\ell x_p^\ell + J$$

$$= p(x_p) + J \quad \text{but } p(x_p) \in A \subseteq I \subseteq J$$

$$\text{so} = J = 0_{k^*}.$$

$k \to R \to k^* = k/J$, so $k \subseteq k^*$.

(identity: $k \to R$; hom: $R \to k^*$)

(there is a ring homomorphism $\sigma : k \to k^*$. But k and k^* are both fields so σ is injective. Here $k \cong \sigma(k)$.)

Suppose otherwise that $1 \in I$. This means $\exists r_1, \ldots r_n \in R, a_1 \ldots a_n \in A$ s.t. $1 = \sum r_i a_i$ ($= 1_R = 1_k$). Take $p_1(x) \ldots p_n(x) \in k[x]$ s.t. $1 = \sum_{i=1}^{n} r_i p_i(x_{p_i})$. This holds in $R = k[\{x_p \mid p \in k[x]\}]$.

Fact (field extension): $\forall F, \forall f \in F[x]$, $\exists E \supseteq F$, $\exists \alpha \in E$ $f(\alpha) = 0$. Define now $k_0 \subseteq k_1 \subseteq \ldots k_n$ s.t. $k_0 = k$, k_1 has root α_1 of $p_1(x)$, k_2 has root α_2 of $p_2 \ldots k_n$ has root α_n of $p_n(x)$.

$K = K[\{x_p \mid p \in K[x]\}]$ we have
$p_i(x_{p_i}) \in R$, $1 \le i \le n$. $\alpha_i \in K_i$ root of $p_i(x)$.
$K_0 \le K_1 \le \cdots K_n$
$\alpha_0 \quad \alpha_1 \quad \alpha_n$

21-374 ($\mathbb{C} \supseteq \mathbb{Z} \ldots$) Still true! 3/16/22

Consider the same statement but in $K_n[\{x_p \mid p \in K[x]\}]$ (K_n larger than K). Substituting $x_{p_i} \mapsto \alpha_i$, we get

$$0 = \sum_{i=1}^{n} r_i p_i(\alpha_i) = \sum_{i=0}^{n} r_i \cdot 0 = 0. \quad \text{Contradiction!}$$

Def. Let $F \le E$. We say E is alg closure of F provided (1) E alg closed
(2) $\forall \alpha \in E$, α is alg over F.
('minimum')

↳ 'splitting' definition in textbook is equivalent over poly in F splits over E

Fact. $\forall K, \exists K^* \supsetneq K$.

Pf. Consider $K^* = K(x) = \left\{ \frac{p(x)}{q(x)} \mid p, q \in K[x], q \neq 0 \right\}$
'field of fractions of ring $K[x]$'

(corollary. $\forall K$ alg closed, $\exists K^* \supsetneq K$ alg closed (main theorem)

Theorem. $\forall F, \exists E \supseteq F$ alg closure.

Pf. By the main theorem, $\exists E^* \supseteq F$ algebraically closed. Consider

$$E := \{\alpha \in E^* \mid \alpha \text{ is alg}/F\}.$$

Claim. E is an algebraic closure of F.

Pf. We proved that $F \le E \le E^*$ (Show $[F(\alpha):F], [F(\beta):F] < \aleph_0 \Rightarrow [F(\alpha,\beta):F] < \aleph_0$)
Fact: $E \supseteq F$, $\alpha \in E$, α alg/$F \iff [F(\alpha):F] < \aleph_0$

- E by definition is algebraic.

- Why is E alg closed? Given $\sum a_k x^k \in E[x] \le E^*[x]$. As E^* is algebraically closed, there is $\alpha \in E^*$, $\sum a_k \alpha^k = 0$, namely α is alg/$F(a_0 \ldots a_n)$. By transitivity, given $F \le K \le E$, [if $\alpha \in E$ alg/K and $\forall \beta \in K$, β alg/$F \Rightarrow \alpha$ alg/F] $\Rightarrow \alpha \in E$.

Define $K = F(a_0, \ldots a_n)$ here, $[F(a_0 \ldots a_n):F] < \aleph_0$

$p \in F(a_0 \ldots a_n)[x]$, α is alg/$F(a_0 \ldots a_n)$

Recall that $\forall F$, $\exists E$ alg closure of F.

3/18/2022

① Remark $\mathbb{C}$ is alg closed, but not algebraic closure of $\mathbb{Q}$; $\pi \in \mathbb{C}$ but π is not alg/$\mathbb{Q}$.

$|\{z \in \mathbb{C} \mid z \text{ is alg}/\mathbb{Q}\}| \leq \aleph_0$ but $|\mathbb{C}| > \aleph_0$. so they are not the same

② $\mathbb{C}$ is alg closure of $\mathbb{R}$: since $\mathbb{C} = \{a+ib \mid a,b \in \mathbb{R}\}$, this is equivalent to

$\forall a,b \in \mathbb{R} \Rightarrow a+bi$ is alg/$\mathbb{R}$

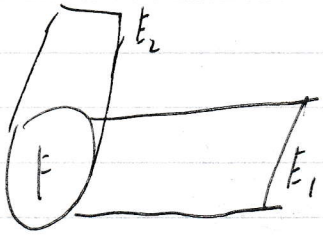
$\mathbb{C} = \mathbb{R}(i)$, $[\mathbb{C}:\mathbb{R}] = 2 \Rightarrow \forall \alpha \in \mathbb{C}$, $[\mathbb{R}(\alpha):\mathbb{R}] \leq 2 \Rightarrow \alpha$ alg/$\mathbb{R}$.

③ In the pf, we showed the following:

Lemma If $E^* \supseteq F$ s.t. E^* is alg closed, then $E := \{\alpha \in E^* \mid \alpha \text{ alg}/F\}$ is an alg closed field. $E \supseteq F$, since $\forall a \in F$, a is a root of $x-a \Rightarrow a$ alg/F

By ③ applied to $\mathbb{C} \supseteq \mathbb{Q}$: we set is algebraically closed field.

Question: Suppose

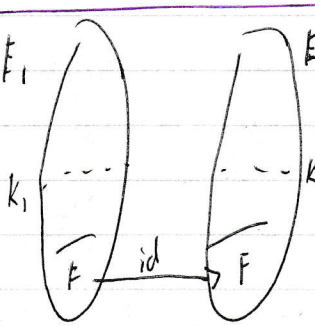


s.t. $F \subseteq E_\ell$, $\ell = 1,2$

Both E_1 and E_2 algebraic closures of F.
From E_1 we can construct E_2, but what if they are separately given?

Theorem. (Uniqueness of Algebraic Closure) $\forall F$, If $E_\ell \supseteq F$, $\ell = 1,2$ are both algebraic closures, then $\exists \varphi: E_1 \cong E_2$ s.t. $\varphi \restriction F = id_F$.

Proof.



Consider $P = \{\psi: K_1 \cong K_2 \mid F \subseteq k_\ell \subseteq E_\ell, \psi \supseteq \varphi, \psi \restriction F = id_F\}$

Clearly P is not empty since we can take $K_1 = K_2 = F$, $\psi = id_F$. Consider $(P, \subseteq)$ poset, where $\psi_1 \subseteq \psi_2 \Leftrightarrow \forall a \in dom\, \psi_1$, $a \in dom\, \psi_2$ and $\psi_1(a) = \psi_2(a)$.

21-374 3/18/2022

Use Zorn's lemma to show $\exists\ \psi \in \mathcal{P}$ maximal.

Given $\mathcal{C} \subseteq \mathcal{P}$ chain, let $\psi^* = \bigcup \mathcal{C}$. We claim that ψ^* is an upper bound of $\mathcal{C}$, $\psi^* \in \mathcal{P}$.

Proof: let $A_1 = \{\operatorname{dom} \psi \mid \psi \in \mathcal{C}\}$, $A_2 = \{\operatorname{range}(\psi) \mid \psi \in \mathcal{C}\}$.
$\subseteq E_1$

Since $\mathcal{C}$ is a chain, also A_1, A_2 are chains.

Suppose $A = \{F \mid F \text{ is a field}\}$, $\mathcal{C} \subseteq A$ chain, want $\bigcup \mathcal{C} \in A$.
(Same idea, union of ideals is ideals)
since $\mathcal{C}$ is a chain, $\exists F_\alpha \subseteq F_\beta$ (wlog) $\alpha \in F_\alpha$, $\beta \in F_\beta$
$\alpha, \beta \in F_\beta \Rightarrow \alpha+\beta$, $\alpha \cdot \beta$, ...

let $K_1 = \bigcup A_1$, $K_2 = \bigcup A_2$, both are fields s.t. $K_\ell \subseteq E_\ell$, $\ell = 1, 2$.

$K_1 = \operatorname{dom} \psi^*$, $K_2 = \operatorname{range} \psi^*$. As $\psi \in \mathcal{C} \Rightarrow \psi$ is injective,

we have ψ^* is injective. Range of ψ^* is K_2, so $\psi^* : K_1 \cong K_2 \Rightarrow \psi^* \in \mathcal{P}$.

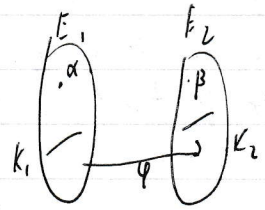
ψ^* is upper bound because given $\psi \in \mathcal{C} \Rightarrow \psi \subseteq \bigcup \mathcal{C} = \psi^*$.

Denote by $\psi \in \mathcal{P}$ a maximal element given by Zorn's lemma. We have to verify:

Lemma: $\operatorname{dom}(\psi) = E_1$, $\operatorname{range}(\psi) = E_2$

$K_2 := \operatorname{range} \psi$.

Exercise (3/25) Pf. ~~Assume~~ Otherwise let $K_1 := \operatorname{Dom} \psi \subsetneq E_1$. Take $\alpha \in E_1 \setminus K_1$. Since E_1 is an
verify (more range $\psi = E_2$.
Hint: Otherwise $K_2 \subsetneq E_2$. Algebraic closure of F, α must be $\overline{K_1}$. Since $F \subseteq K_1$, α is $\overline{K_1}$. Recall there
Take $\beta \in E_2 - K_2$, β $\overline{K_2}$.
$m_\beta \in K_2[x]$ monic irred poly is a (unique monic) irreducible $m_\alpha \in K_1[x]$ such that $m_\alpha(\alpha) = 0$. As $\psi : K_1 \cong K_2$,
$\psi^{-1} : K_2 \cong K_1$, consider $\psi^{-1}(m_\beta)$ $\psi(m_\alpha) \in K_2[x]$ irreducible.
$\in K_1[x]$



$\exists\ \alpha \in E_1$ not of $\psi^{-1}(m_\beta)$
use Kronecker's lemma
to find $\psi_2 \supsetneq \psi$, $\psi_2 \in \mathcal{P}$ cont.

Since E_2 is $\overline{K_2}$ closed, $\exists \beta \in E_2$ root of $\psi(m_\alpha)$.

Theorem (Kronecker) If $\psi : K_1 \cong K_2$, $P \in K_1[x]$ irreducible
$E_\ell \supseteq K_\ell$, $\alpha \in E_1$ root of P and $\beta \in E_2$ root of $\psi(P)$, then
$\exists\ \psi : K_1(\alpha) \cong K_2(\beta)$, $\psi(\alpha) = \beta$, $\psi \supseteq \psi$

By Kronecker, $\exists \psi \supseteq \psi$, $\psi : K_1(\alpha) \cong K_2(\beta)$. Since $\alpha \in K_1 = \operatorname{dom} \psi$ and $K_2(\beta) \subseteq E_2$, we have $\psi \in \mathcal{P}$.
So $\psi \supsetneq \psi$, contradicting the maximality of ψ.

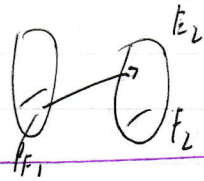
47

21-374 3/21/22

'Variations on a theme' - Notation: $\overline{F}$ is the alg closure of F.

Theorem. Given field F and $E_1, E_2 \geq F$ both algebraic closures of F, then $\exists \varphi: E_1 \cong E_2$, $\varphi \upharpoonright F = id_F$.

Th 1. Suppose F_1, F_2 s.t. $\operatorname{char} F_1 = \operatorname{char} F_2$, $E_2 \geq F_2$ algebraically closed and $\forall \alpha \in F_1$ is algebraic. Then $\exists \varphi: F_1 \to E_2$ (injective) field homomorphism (embedding). (necessity is obvious, sufficiency is not)



Remark: Even some E_2 alg closed, $\forall F_1$ s.t. $\operatorname{char} F_1 = \operatorname{char} E_2$, if $\forall \alpha \in F_1$ alg, then F_1 is an isomorphic to a subfield of E_2.

↳ Cayley's Theorem. Group with n groups is isomorphic to some subgroup of S_n.

Corollary. Let p be prime or zero, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Q}$. Take $E := \overline{\mathbb{F}_p}$. For every F of char p s.t. $\forall \alpha \in F$ alg, then $\exists \varphi: F \to E$.

Major applications: (Algebraic) number theory. Main object of study is solving diophantine equations: $p \in \mathbb{Q}[x_1, \dots x_n]$, $p(\bar{x}) = 0$. This involves field extensions $\mathbb{Q}(\alpha, \beta \dots)$, α, β alg. What is $F \geq \mathbb{Q}$ when $[F:\mathbb{Q}] < \aleph_0$?

By the last corollary, such F is isomorphic to a subfield of $\overline{\mathbb{Q}} \leq \mathbb{C}$

(analysis, diff eq, integral...)

Proof of Th 1. Consider $\mathcal{P} = \{\psi : k_1 \cong k_2 \mid \mathbb{F}_p \leq k_1 \leq F_1, F_2 \leq k_2 \leq E_2\}$.

Since $(\mathcal{P}, \subseteq)$ is POSET, we use Zorn's Lemma to show $\mathcal{P}$ has a maximal element: Given $C \subseteq \mathcal{P}$ chain, $h := \bigcup C$. Show $h \in \mathcal{P}$, $h \geq \psi$ $\forall \psi \in C$. Then there is $\varphi^* \in \mathcal{P}$ maximal.

we have to show: $\operatorname{dom} \varphi^* = F_1$

→ otherwise suppose $K_1 = \operatorname{dom} \varphi^* \subsetneq F_1$. Let $\alpha \in F_1 - K_1$. As α is alg/$\mathbb{F}_p$, also α is alg/K_1. Let $m_\alpha \in K_1[x]$ be irreducible s.t. $m_\alpha(\alpha) = 0$.

$q = \varphi^*(m_\alpha)$ is irreducible over $\varphi^*[K_1]$.

Apply Kronecker's lemma by substituting $F_1 \leftarrow K_1$, φ^* is given as $\varphi^*: K_1 \cong \underbrace{\varphi^*[K_1]}_{K_2}$

$p \leftarrow m_\alpha$.

As E_2 is alg closed, $\exists \beta \in E_2$ root of $q (= \varphi^*(p))$.

So there is $\psi: K_1(\alpha) \cong \varphi^*[K_1](\beta)$.

$\psi \supseteq \varphi^*$, $\psi(\alpha) = \beta$. So $\psi \neq \varphi^*$. Since $\alpha \notin \text{dom } \varphi^*$, but $\alpha \in \text{dom } \psi$,

$\psi \neq \varphi^* \in L$ contrary to maximality of φ^*.

GALOIS CORRESPONDENCE THEOREM

Consider $G = \text{Aut}_F(E) = \text{Aut}(E/F) = \text{Gal}(E/F)$.

Consider $\mathcal{F}_1 = \{K \leq E \mid K \supseteq F\}$ - all subfields between E and F (endpoints inclusive)

$\mathcal{F}_2 = \{H \mid H \leq G\}$ - subgroups $(\text{Aut}(E/F))$

The Galois Theorem states approximately that there is a bijection between $\mathcal{F}_1$ and $\mathcal{F}_2$. This is false in general, but true under some extra NATURAL assumptions.

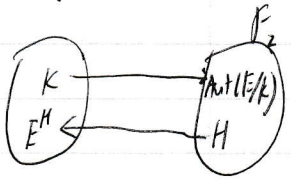
Fact: (1) Given $F \leq E$, $G := \text{Aut}(E/F)$.

(2) If $F \leq K \leq E$ then $\text{Aut}(E/K) \leq G$ (fixing $K \Rightarrow$ fixing F)

(3) If $H \leq G$, $E^H = \{\alpha \in E \mid (\forall \sigma \in H), \sigma(\alpha) = \alpha\}$ 'fixed field' (pg 50).

$\in \mathcal{F}_1$ $\in \mathcal{F}_2$ $\quad$ $\in \mathcal{F}_2$ $\in \mathcal{F}_1$

So we have $K \longmapsto \text{Aut}(E/K)$ $\quad$ $H \longmapsto E^H$



Idea: Under "reasonable assumptions", both functions are bijections and one is the inverse of the other.

Recalling some definitions...

Suppose $E \supseteq F$, we say that E is a Galois extension of F provided:

① $[E:F] < \aleph_0$, ② $[E:F] = |\mathrm{Aut}(E/F)|$.

Theorem. Suppose $p \in F[x]$ separable ($=$ no multiple roots). If E is the splitting field of p/F, then E/F is Galois. (① follows from iteration) pf.

Facts ① Suppose $\mathrm{char} F = p$ (prime). Then $x^{p^n} - x$ is separable

② $q \in F[x]$ is separable $\Leftrightarrow \gcd(q, q') = 1$.

All discussed on p 34. ③ $q \in \mathbb{Q}[x]$, q irreducible $\Rightarrow q$ separable.

(since $\deg q' = \deg q - 1$, and derivative cannot have zero coefficient)

Cor. ① let $q \in \mathbb{Q}[x]$ irreducible, E the splitting field of q. Then $E/\mathbb{Q}$ is Galois

② If p is prime, then $\forall n$ $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois

(splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$)

21-374 3/23/2022

Galois Extension Theorem (cont).

Recall: E/F Galois provided $[E:F]<\aleph_0$ and $[E:F] = |\mathrm{Aut}(E/F)|$.

Remark: It is possible to generalize this definition to the case where $[E:F]$ is infinite, but it requires knowledge of "topological groups".

↳ use $F \le K \le H \Rightarrow [H:F] = [H:K][K:F]$

Let $E \supseteq F$, there is $G = \mathrm{Aut}(E/F)$.

$\forall K$, $F \le K \le E \mapsto \mathrm{Aut}(E/K) \le G$

$E^H = \{a \in E \mid \forall \sigma \in H \ \sigma(a) = a\} \longleftrightarrow H \le G$

* $E^H \le E$, containing F.

Both are bijections (if E/F is Galois) one inverse of the other, s.t.

(1) $[E:E^H] = |H|$.

(2) F/E^H Galois? Always ✓

(3) E^H/F Galois $\Leftrightarrow \mathrm{Aut}(E/E^H) \trianglelefteq G$. ('normal subgroup')

(4) $\mathrm{Aut}(E^H/F) \cong \mathrm{Aut}(E/F) / \mathrm{Aut}(E/E^H)$

Applications: (A) Primitive Element Theorem. If $E \supseteq \mathbb{Q}$ s.t. $[E:\mathbb{Q}]<\aleph_0$, then $\exists \alpha \in E$ s.t. $E = \mathbb{Q}(\alpha)$.

(B) Fundamental Theorem of Algebra. $\mathbb{C}$ is alg closed. Use ECT + Sylow's Theorems

Proof ~1750 (Artin)

($|G| = m \cdot p^k$, p prime, $(p,m)=1$
Then $\exists P \le G$, $|P| = p^k$, $\forall \ell < k$
$\exists H_\ell \le P$, $|H_\ell| = p^\ell$.)

□

History of Galois Theory : Edwards (Harold M.), 'Galois Theory'

① Galois
② Cauchy clarified/simplified exposition } Group = 'set of permutations'
③ ~15-5-1830 E. Noether, E. Artin, B.L van der Waerden (Artin and vdW were postdocs to Noether)

Noether developed 'Abstract Algebra'
married to Jewish woman...
2-vol book 'Modern Algebra'

Modern notions: Groups, ring, field, vector spaces, φ homo, $N \triangleleft G$

④ Fled to United States, Jewish but liberal conception

Algebraic Number Theory

Artin: Notre Dame, book "Galois Theory" contained new proof of GT based on linear algebra. Most modern textbooks are based on that.

Def. Let G be a group, and L a field. Define $\chi: G \to \underbrace{L^\times}_{\text{multiplicative group of } L, \text{ excl. } 0}$ is called a character from G to L iff χ is a group homomorphism.

Remark. If $\varphi \in Aut(E)$ then $\varphi \restriction E^\times$ is a character from $E^\times$ to $E^\times$.

Def. Suppose $\chi_1, \chi_2, \dots \chi_n$ are characters from G to L. We say $\{\chi_1, \dots \chi_n\}$ are linearly independent iff $(\forall a_1, a_2 \dots a_n \in L)\left[\left((\forall g \in G)\left(\sum_{i=1}^{n} a_i \chi_i(g) = 0\right)\right) \Rightarrow a_1, a_2 \dots a_n = 0\right]$

The key technical theorem for GT [Th 9, 14.2 D&F]:
Given E, $G \leq Aut(E)$ finite, denote $F := E^G$. Then $[E:F] = |G|$.

Theorem 1. If $\{\chi_1, \chi_2, \dots \chi_n\}$ are distinct characters from G to L (a set), then they are linearly independent over L.

Pf. Suppose otherwise: $[\exists a_1, a_2 \dots a_n \in L]$ [Not all $a_1 \dots a_n$ are 0 and $(\forall g \in G)\sum_{i=1}^{n} a_i \chi_i(g) = 0$]

PMI $\Leftrightarrow$ WOP. (smallest counter-example)

Let $M := \min\{m \in \mathbb{N} \mid \exists\, i_1 < i_2 < \dots < i_m$ and $a_{i_\ell} \in L^\times$ (not zero) s.t. $(\forall g \in G)\sum_{k=1}^{m} a_{i_k} \chi_{i_k}(g) = 0\}$

By renaming, we may assume $m \leq n$, and $a_1, \dots a_m \in L^*$ s.t. $(\forall g \in G)\sum_{i=1}^{m} a_i \chi_i(g) = 0$. (*)

21-374 3/23/2022

[1) is prove by minimality (minimal counterexample)] As $\chi_1 \neq \chi_m$ $\exists\, g_0 \in G$, $\chi_1(g_0) \neq \chi_m(g_0)$.

Substituting $g \leftarrow g \cdot g_0$, $\sum_{i=1}^{m} a_i \chi_i(g \cdot g_0) = 0$ $\forall g \in G$. As χ homo, $\sum_{i=1}^{m} a_i \chi_i(g)\chi_i(g_0) = 0$.

No class on 3/25/2022

(Rami was sick...)

(1) $(\forall g \in G)$ $\sum_{i=1}^{m} a_i \chi_i(g)\, \chi_1(g_0) = 0$

But from before, (*) gives

(2) $(\forall g \in G)$ $\sum_{i=1}^{m} a_i \chi_i(g) \cdot \chi_m(g_0) = 0$

Then (1) − (2) = (3): $(\forall g \in G)$ $\sum_{i=1}^{m-1} a_i \chi_i(g) [\chi_i(g_0) - \chi_m(g_0)]$ $\left(\chi_m(g_0) - \chi_m(g_0) = 0\right)$

$\Downarrow$ Let $b_i = a_i [\chi_i(g_0) - \chi_m(g_0)]$.

(4) $(\forall g \in G)$ $\sum_{i=1}^{m-1} b_i \chi_i(g) = 0$.

But $b_1 = \chi_1(g_0) - \chi_m(g_0) \neq 0$ by choice of g_0. So we found $b_1, \ldots b_{m-1} \in L$ not all zero such that (4) holds. This contradicts the minimality of m.

3/28/2012

Fact from Linear Algebra: Given n linear homogeneous equations with m many unknowns, if $m > n$ then the system has a non-trivial solution (in fact infinitely many, by Gaussian Elimination)
(all constant terms are zero)

Thm of 14.2.9. Let E be a field, $G \leq_{\text{finite}} \mathrm{Aut}(E)$. We want to show $[E : E^G] = |G|$.

Two steps. (A) $[E : E^G] \leq |G|$ (B) $|G| \leq [E : E^G]$

(p154-58)

Proof of (B): Let $n \in \mathbb{N}$ s.t. $\{\sigma_1, \sigma_2, \ldots \sigma_n\} = G$. AFSOC $|G| > [E : E^G]$, i.e. $n > [E : E^G] =: m$. Pick $\alpha_1, \ldots \alpha_m$ basis of E/E^G. Consider the following system:

$$(\ast)\quad \begin{cases} \sigma_1(\alpha_1)X_1 + \sigma_2(\alpha_1)X_2 + \sigma_3(\alpha_1)X_3 + \ldots + \sigma_n(\alpha_1)X_n = 0 \\ \sigma_1(\alpha_2)X_1 + \sigma_2(\alpha_2)X_2 + \ldots + \sigma_n(\alpha_2)X_n = 0 \\ \vdots \\ \sigma_1(\alpha_m)X_1 + \sigma_2(\alpha_m)X_2 + \ldots + \sigma_n(\alpha_m)X_n = 0. \end{cases}$$

($\alpha_1 \downarrow \alpha_m$)

Since $n > m$, there exists $\beta_1, \ldots \beta_n \in E$ not all zero, solving $(\ast)$.

Idea: Since $\{\sigma_1, \ldots \sigma_n\}$ are characters from $E^\times$ to $E^\times$, as they are all distinct, by the previous lemma, $\{\sigma_1, \ldots \sigma_n\}$ should be linearly independent.

To derive a contradiction, we show they are actually not.

(note for later)
For any given $a_1, \ldots a_m \in E^G$, since $\sigma_i \upharpoonright E^G = \mathrm{id}_{E^G}$, $\forall i,j\ \sigma_i(a_j) = a_j$.

Substituting β_i's into $(\ast)$, we get

$$(\ast)_1\quad \begin{cases} \sigma_1(\alpha_1)\beta_1 + \ldots + \sigma_n(\alpha_1)\beta_n = 0 & \leftarrow \text{multiply by } a_1 \\ \sigma_1(\alpha_2)\beta_1 + \ldots + \sigma_n(\alpha_2)\beta_n = 0 & \text{"} \quad a_2 \\ \vdots \\ \sigma_1(\alpha_m)\beta_1 + \ldots + \sigma_n(\alpha_m)\beta_n = 0. & a_m \end{cases}$$

After multiplication,

$$(*)_2 \quad \begin{cases} \sigma_1(\alpha_1)a_1\beta_1 + \dots + \sigma_n(\alpha_1)a_1\beta_n = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{arbitrary elements of } E^G \\ \sigma_1(\alpha_m)a_m\beta_1 + \dots + \sigma_n(\alpha_m)a_m\beta_n = 0 \quad \text{. Since } \sigma_i(a_j) = a_j, \end{cases}$$

$$(*)_3 \quad \sigma_1(a_1\alpha_1)\beta_1 + \dots + \sigma_n(a_1\alpha_1)\beta_n = 0$$

$$\vdots$$

$$\sigma_1(a_m\alpha_m)\beta_1 + \dots + \sigma_n(a_m\alpha_m)\beta_n = 0.$$

sum by columns

$$\beta_1\sigma_1\Big(\sum_{k=1}^{m} a_k\alpha_k\Big) + \dots \quad \beta_n\sigma_n\Big(\sum_{k=1}^{m} a_k\alpha_k\Big)$$

We have therefore shown that $\forall a_1 \dots a_m \in E^G$, $\sum_{i=1}^{n} \beta_i \cdot \sigma_i\big(\sum_{k=1}^{m} a_k\alpha_k\big) = 0$. But since $\{\alpha_1, \dots \alpha_m\}$ is a basis of E/E^G, we have that $\forall\, g \in F^X$, g can be written as $\sum_{k=1}^{m} a_k\alpha_k$, so

$$\sum_{i=1}^{n} \beta_i \sigma_i(g) = 0, \text{ for some non-trivial } \{\beta_1 \dots \beta_n\} \ (\equiv \text{not all zero})$$

This contradicts (B) the lemma that $\{\sigma_1 \dots \sigma_n\}$ are linearly independent characters from E^X to E^X.

So we have completed the proof that $|G| \le [E:E^G]$. It remains to prove (A).

note: the contradiction comes from linear independence.

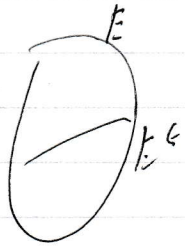
3/30/2022

Proof of part (A) $\left(G \leq_{\text{finite}} \mathrm{Aut}(E) \Rightarrow |G| = [E:E^G]\right)$ E. Artin ~1945

Suppose $n = |G| < [E:E^G] = m$. Again we want a contradiction.

Fix $\alpha_1, \alpha_2, \ldots \alpha_{n+1} \in E$ linearly independent over E^G.

Fix $\{\sigma_1, \ldots \sigma_n\} = G$. Consider the system



$$(*) \quad \begin{cases} \sigma_1(\alpha_1)x_1 + \ldots + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(\alpha_1)x_1 + \ldots + \sigma_n(\alpha_{n+1})x_{n+1} = 0 \end{cases}$$

($\sigma_1 = 1_G$, σ_n)

As the number of unknowns $(n+1)$ is greater than the number of equations (n), then there is a non-trivial solution $\langle \beta_1, \beta_2 \ldots \beta_{n+1} \rangle$ of $(*)$. (in E)

① Minimalize

② Normalize

Claim: Not all β_i's are in E^G.

Pf. By the 1st equation in $(*)$ $\sigma_1(\alpha_1)\beta_1 + \ldots \sigma_1(\alpha_{n+1})\beta_{n+1} = 0$.

Since $\sigma_1 = 1_G$, $\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_{n+1}\beta_{n+1} = 0$.

If not all β_i's are zero, and they are all in E^G, then $\{\alpha_1, \ldots \alpha_{n+1}\}$ is not linearly independent. Contradiction.

① Therefore, let m ($m \leq n+1$) be the smallest integer s.t. $\bar{\beta} := \langle \beta_1, \ldots \beta_m, 0, \ldots 0 \rangle$ solves $(*)$ and

② $\beta_i \neq 0$ $\forall\, 1 \leq i \leq m$. Multiplying each β_i's in $\bar{\beta}$ by β_m^{-1}, we get another solution $\beta_m^{-1} \cdot \bar{\beta}$ of $(*)$:

$\langle \beta_1, \ldots, \beta_{m-1}, 1, \ldots 0 \rangle$. Substituting this into $(*)$,

Compare

$$(**) \quad \begin{cases} \sigma_1(\alpha_1)\beta_1 + \ldots + \sigma_1(\alpha_{m-1})\beta_{m-1} + \sigma_1(\alpha_m) = 0. \\ \vdots \\ \sigma_n(\alpha_1)\beta_1 + \ldots + \sigma_n(\alpha_{m-1})\beta_{m-1} + \sigma_n(\alpha_m) = 0. \end{cases}$$

By renaming if necessary and using the claim above, we may assume $\beta_1 \notin E^{\in}$. By definition of $E^{\in}$, $\beta_1 \notin E^{\in} \Rightarrow \exists\, \sigma \in \in$ such that $\sigma(\beta_1) \neq \beta_1$. Let $k_0 \leq n$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$.

Apply σ_{k_0} to the previous system:

$$\begin{cases} \sigma_{k_0}\circ\sigma_1(\alpha_1)\cdot\sigma_{k_0}(\beta_1) + \dots + \sigma_{k_0}\circ\sigma_1(\alpha_{m-1})\,\sigma_{k_0}(\beta_{m-1}) + \sigma_{k_0}\circ\sigma_1(\alpha_m) = 0 \\ \\ \sigma_{k_0}\circ\sigma_n(\alpha_1)\cdot\sigma_{k_0}(\beta_1) + \dots + \sigma_{k_0}\circ\sigma_1(\alpha_{m-1})\,\sigma_{k_0}(\beta_{m-1}) + \sigma_{k_0}\circ\sigma_n(\alpha_m) = 0. \end{cases}$$

What is $\{\sigma_{k_0}\circ\sigma_i \mid 1 \leq i \leq n\}$? Since $\in$ is a group and $\in = \{\sigma_1, \dots \sigma_n\}$ and multiplication is injective, $\Rightarrow \in = \{\sigma_1, \dots \sigma_n\}$. After renaming (replace $\sigma_{k_0}\circ\sigma_i$ by σ_j to respect the row in which it appears).

$$\text{(***) complete} \Rightarrow \begin{cases} \sigma_1(\alpha_1)\,\sigma_{k_0}(\beta_1) + \dots + \sigma_1(\alpha_{m-1})\,\sigma_{k_0}(\beta_{m-1}) + \sigma_1(\alpha_m) = 0 \\ \vdots \\ \sigma_n(\alpha_1)\,\sigma_{k_0}(\beta_1) + \dots + \sigma_n(\alpha_{m-1})\,\sigma_{k_0}(\beta_{m-1}) + \sigma_n(\alpha_m) = 0. \end{cases}$$

Compute (**) - (***):

$$④ \begin{cases} \sigma_1(\alpha_1)\,[\beta_1 - \sigma_{k_0}(\beta_1)] + \dots + \sigma_1(\alpha_{m-1})[\beta_{m-1} - \sigma_{k_0}(\beta_{m-1})] = 0 \\ \vdots \\ \sigma_n(\alpha_1)\,[\beta_1 - \sigma_{k_0}(\beta_1)] + \dots + \sigma_n(\alpha_{m-1})[\beta_{m-1} - \sigma_{k_0}(\beta_{m-1})] = 0. \end{cases}$$

Let $\beta_i' := [\beta_i - \sigma_{k_0}(\beta_i)]$ for $1 \leq i \leq m-1$.

Let $\bar{\beta}' = \langle \beta_1', \beta_2' \dots \beta_{m-1}', 0 \dots 0 \rangle$. Using ④, this solves (*) as well. If at least one of them is non-zero, then this contradicts the minimality of $\bar{\beta}$.

Technical Theorem $\boxed{G \leq_f \mathrm{Aut}(E) \Rightarrow [E:E^G] = |G|}$

So how to show $\exists i \in n-1$ s.t. $\beta_i' \neq 0$? Claim: $\beta_i' \neq 0$.

Pf. By the choice of σ_{k_0}, we have $\sigma_{k_0}(\beta_1) \neq \beta_1$.

$\Rightarrow \beta_1 - \sigma_{k_0}(\beta_1) \neq 0 \Rightarrow \beta_i' \neq 0$ □

note: the contradiction comes from minimality.

Corollaries: ① If E/F is finite, then $|\mathrm{Aut}(E/F)| \leq [E:F]$

Moreover, $F = E^{\mathrm{Aut}(E/F)}$ (group) $\Leftrightarrow$ E/F is Galois. ($|\mathrm{Aut}(E/F)| = [E:F]$)

we proved this in the case that E is a splitting field

Pf. let $G = \mathrm{Aut}(E/F)$. Since E/F is finite, let $n := [E:F]$, and pick $\{b_1, b_2 \dots b_n\} \subseteq E$ a F-basis. Note that if $\sigma, \tau \in G$ and $\sigma(b_k) = \tau(b_k)$ $\forall k \in [1,n]$, then $\sigma = \tau$.

$\sigma(\sum_{i}^{\text{finite}} f_i b_k) = \tau(\sum f_i b_k)$

$\rightarrow |G| \leq |S_n| = n! < \infty$ ("permutation")

* dubious argument, there is no requirement that σ and τ have to permute b_i, the case if they're the roots of some equation. e.g. primitive element theorem we could argue that $E = F(b_1, b_2 \dots b_n)$ and then σ and τ must map b_i to some other root of equation i, so n^n upper bound. (p580)

~~Alternatively, $[E:E^G] = [E:E^{\mathrm{Aut}(E/F)}]$~~

Note also $E \geq E^G \geq F$ by definition.

By the multiplication formula, $[E:F] = [E:E^G] \cdot [E^G:F]$.

Since $G \leq_{\text{finite}} \mathrm{Aut}(E)$, $[E:F] \overset{\text{theorem}}{=} |G| \cdot [E^G:F]$

$\overset{\text{def}}{=} |\mathrm{Aut}(E/F)| \cdot [E^G:F]$. Since $[E^G:F] \geq 1$, $|\mathrm{Aut}(E/F)| \leq [E:F]$

$[E:F] = |\mathrm{Aut}(E/F)| \Leftrightarrow [E^G = F] = 1$

$\Leftrightarrow E^G = F$.

But $G = \mathrm{Aut}(E/F)$, as in the "moreover" claim.

21-374 Rani cancelled 2 classes...

4/6/2022

Recall: E/F is Galois $\Leftrightarrow$ E/F is finite and $|\mathrm{Aut}(E/F)| = [E:F]$.

More corollaries from the technical theorem:

Cor 2 Suppose E/F finite. TFAE: (1) E/F Galois. "counting"
(2) $F = E^{\mathrm{Aut}(E/F)}$ "restatement" in terms of fixed fields

pf. (1) $\Rightarrow$ (2) by $\Leftarrow$ in "moreover"
(2) $\Rightarrow$ (1) Enough to show $[E:F] = |\mathrm{Aut}(E/F)|$. Assuming (2), use $\Rightarrow$ in "moreover"

Cor 3 If $G \leq_{\text{finite}} \mathrm{Aut}(E)$, then $G = \mathrm{Aut}(E/E^G)$.

pf. Clearly $G \subseteq \mathrm{Aut}(E/E^G) \Rightarrow |G| \leq |\mathrm{Aut}(E/E^G)|$ (fixing the elements fixed by G)

By the theorem, $|G| = [E:E^G]$. The multiplication formula gives

$$[E:F] = [E:E^G]\cdot[E^G:F] = |G|\cdot[E^G:F]$$

$$|G| = [E:E^G] \leq |\mathrm{Aut}(E/E^G)|$$

$$\leq [E:E^G]$$ (cor 1)

equality!

$$\Rightarrow |G| = |\mathrm{Aut}(E/E^G)|.$$

$$G \subseteq \mathrm{Aut}(E/E^G) \wedge |G| = |\mathrm{Aut}(E/E^G)| \Rightarrow G = \mathrm{Aut}(E/E^G).$$

Cor 4 $G_1 \neq G_2 \leq_{\text{finite}} \mathrm{Aut}(E) \Rightarrow E^{G_1} \neq E^{G_2}$.

"injective"

pf. Otherwise $\exists\, G_1 \neq G_2 \leq_{\text{finite}} \mathrm{Aut}(E)$ s.t. $E^{G_1} = E^{G_2}$.

$$G_1 = \mathrm{Aut}(E/E^{G_1}) = \mathrm{Aut}(E/E^{G_2}) = G_2,$$ contradiction.

($G_1 = \mathrm{Aut}(E/E^{G_1})$ by cor 3; $E^{G_1} = E^{G_2}$; $\mathrm{Aut}(E/E^{G_2}) = G_2$ by cor 3)

We proved earlier that

$p \in F[x]$ separable (no multiple roots), E splitting field of p over F,
then $|\mathrm{Aut}(E/F)| = [E:F]$. (Prop 5, 14.1)

We can "extend" Cor 2: TFAE
(1) E/F Galois.
(2) $F = E^{\mathrm{Aut}(E/F)}$
(3) E is a splitting field of a separable $p \in F[x]$

We know (1) $\Leftrightarrow$ (2), (3) $\Rightarrow$ (1).

Where does the "energy" behind the corollaries so far come from? It came from $E \leq_f \mathrm{Aut}(E) \Rightarrow [E:E^G] = |G|$.
We need another source to show (1) $\Rightarrow$ (3):

Theorem. Suppose E/F Galois. Then there is $p \in F[x]$ separable s.t. E is the splitting field of p/F.

* (Moreover, if $q \in F[x]$ is any irreducible polynomial that has a root in E, then q splits in E and q is separable. $\exists \alpha \in E, q(\alpha) = 0$)

Pf. Main lemma:

Fix $\{\sigma_1, \sigma_2, \dots \sigma_n\} = G := \mathrm{Aut}(E/F)$. Assume $\sigma_1 = \mathrm{id}_E$.

Since $q(\alpha) = 0$, also $q(\sigma_\ell(\alpha)) = 0 \quad \forall\, 1 \leq \ell \leq n$.

Consider $A := \{\sigma_\ell(\alpha) \mid 1 \leq \ell \leq n\}$. Let $\{\sigma_1 \dots \sigma_k\}$ be an enumeration of A ($k \leq n$).

Given $\gamma \in G$, and consider $\{\gamma(\alpha_1) \dots \gamma(\alpha_k)\} = \{\gamma \circ \sigma_\ell(\alpha) \mid 1 \leq \ell \leq n\}$ all roots
(Since G is a group) bijectivity... $= \{\sigma_\ell(\alpha) \mid 1 \leq \ell \leq n\} = \{\alpha_1 \dots \alpha_n\}$

21-374 4/6/2022

let $f(x)=\prod_{i=1}^{k}(x-\alpha_i)$. considering action of τ on α_i's. we have established $\tau(f)=f$ (coefficients are unchanged)

Since $\forall \tau \in \underbrace{\mathrm{Aut}(E/F)}_{G}$, $\tau(f)=f$, and E/F Galois (i.e. $F=E^{\mathrm{Aut}(E/F)}$)

$\Rightarrow f \in F[x]$ (since we showed that the coefficients are in $E^{\mathrm{Aut}(E/F)}$).

since $\sigma_1 = id_E$, we have $\alpha \in \{\alpha_i \mid 1\le i\le k\}$

So $f\in F[x]$ and $f(\alpha)=0$.

q is irreducible $\Rightarrow q \mid f$ in $F[x]$ $\Big\}$ $f=q$. So q splits in E.

In $E[x]$, $f \mid q$ since every α_i is root of q

As $\alpha_i \neq \alpha_j$ where $1\le i\neq j\le k$, q is separable.

(Lemma $\Rightarrow$ Theorem) Since E/F is finite, fix $\{\beta_1,\beta_2,\dots \beta_m\}$ basis of E/F. let $m_k \in F[x]$ be the minimal, monic, irreducible polynomial for β_k.

Consider $\prod_{k=1}^{m} m_k \in F[x] =: \epsilon$ (remove multiple roots). Let $g\in F[x]$ be the square-free component of ϵ. by the lemma, the m_k's are all separable and E is the splitting field of ϵ, but it also splits $g\in F[x]$. ✓

4/11/2022

Galois Correspondence (part 1) Let E/F be Galois, and $G := \mathrm{Aut}(E/F)$.

Then $H \leq G \mapsto E^H$ is a bijection between $\{H \mid H \leq G\}$ and $\{K \mid F \leq K \leq E\}$.

pf. By corollary 4 (p55), $H \mapsto E^H$ is injective, for $H \leq G$. Why is it surjective?

Given $K \leq E$ s.t. $K \geq F$, we have to find $H \leq G$ s.t. $K = E^H$.

[Since E/F is Galois, let $p \in F[x]$ be separable, such that E is the splitting field of p/F.
A polynomial is still separable in any field extension - so $F \leq K \Rightarrow p \in K[x]$ is separable in K.
$\Rightarrow E$ is still the splitting field of p/K.

Use the last theorem again: we get E/K is Galois. (so E/F Gal $\Rightarrow E/K$ Gal)
where $F \leq K \leq E$

By corollary 2, $E^{\mathrm{Aut}(E/K)} = K$. Take $H := \mathrm{Aut}(E/K)$, and notice that $H \leq G$.

(Application) Corollary. [Primitive Element Theorem] If $K/\mathbb{Q}$ finite, then there is $\alpha \in K$ s.t. $K = \mathbb{Q}(\alpha)$.
↑ true for any char-0 field

- Suppose E/F is Galois, then $\{K \mid F \leq K \leq E\}$ is finite. This follows from
$[E:F] = |\underbrace{\mathrm{Aut}(E/F)}_{G}| \Rightarrow G < \aleph_0$. By the bijection above, $|\{H \mid H \leq G\}| \leq 2^{|G|} < \aleph_0$
$\|$
$|\{K \mid F \leq K \leq E\}|$
- (1) $p \in F[x]$ separable $\Leftrightarrow \gcd(p, p') = 1$
(2) $p \in F[x]$ irred, $\mathrm{char}\, F = 0 \Rightarrow p$ separable
- Suppose F has char 0, $K \geq_{\text{finite}} F$. Then there is $K^* \geq K$ s.t. K^*/F is Galois. ('Galois closure')

pf. Suppose $\{\beta_1, \ldots, \beta_m\} \subseteq K$ is F-basis of K. Let $m_k \in F[x]$ monic, irred polynomial s.t. $m_k(\beta_k) = 0$.
Let $G = \prod_{k=1}^{m} m_k$, and let g be the square-free part of G. Since $\mathrm{char}\, F = 0$, m_k irred, m_k's are all separable. Now K^* splits separable poly $g \in F[x] \Rightarrow K^*/F$ is Galois.

Remark: Every finite extension is finitely generated.
(converse is not true (e.g. $\mathbb{R} \to \mathbb{C}$)
Every finite extension is cls. algebraic.

21-374 **If F has char 0 and K/F is finite, then there is $\alpha \in K$ s.t. $K = F(\alpha)$** 4/11/2022

We are now in a position to prove (a stronger version of) the Primitive Element Theorem.

Pf. By the last ~~theorem~~ lemma, we $\exists K^* \supseteq K$ s.t. K^*/F is Galois. By a corollary of ECT, we know $|\{E \mid F \subseteq E \subseteq K^*\}|$ is finite.

- Argue by induction on n: If $K = F(\alpha_1, \dots \alpha_n)$, then $\exists \alpha \in K$ s.t. $K = F(\alpha)$.
- Enough to show $\forall \alpha_1, \alpha_2 \; \exists \alpha \in K^*, F(\alpha_1, \alpha_2) = F(\alpha)$. [since $F(\alpha_1, \alpha_2, \alpha_3) = (F(\alpha_1))(\alpha_2, \alpha_3)$)] 4/13/2022

(Pf continued)

$n = 1$: trivial.

$n > 1$: w.T.s $\forall \alpha_1, \alpha_2 \in K, \exists \gamma \in F(\alpha_1, \alpha_2)$ s.t. $F(\alpha_1, \alpha_2) = F(\gamma)$

Since $\mathrm{char}\, F = 0$, $\mathbb{Q} \leq F$ (isomorphic to F's prime field)

(consider $t \mapsto F(\alpha_1 + t\alpha_2)$ function from $\mathbb{Q}$ into $\{L : F \subseteq L \subseteq K\} \subseteq \{L : F \subseteq L \subseteq K^*\}$

domain is $\mathbb{Q}$ (infinite!)

Finite! see p62, K^*/F Galois

By the 'infinite' version of the pigeonhole principle,
$\exists t_1 \neq t_2 \in \mathbb{Q}$ s.t. $F(\alpha_1 + t_1\alpha_2) = F(\alpha_1 + t_2\alpha_2)$ $(=: L)$

In particular $\underbrace{\alpha_1 + t_1\alpha_2}_{x} \in \underbrace{F(\alpha_1 + t_2\alpha_2)}_{y}$

As $x - y \in F(\alpha_1 + t_2\alpha_2)$, $(t_1 - t_2)\alpha_2 \in F(\alpha_1 + t_2\alpha_2)$

As $(t_1 - t_2) \neq 0$, we invert it to get $\alpha_2 \in F(\alpha_1 + t_2\alpha_2)$

Take $\gamma = \alpha_1 + t_2\alpha_2$

so $\alpha_1 \in F(\gamma)$,

$\alpha_2 \in F(\gamma)$. Thus $F(\alpha_1, \alpha_2) = F(\gamma)$.

$t_2\alpha_2 \in F(\alpha_1 + t_2\alpha_2)$

$\Rightarrow (\alpha_1 + t_2\alpha_2) - t_2\alpha_2 \in F(\alpha_1 + t_2\alpha_2)$

$\alpha_1 \in F(\alpha_1 + t_2\alpha_2)$

FTGT (continued) Suppose E/F is Galois.

(2) $H_1, H_2 \leq \mathrm{Aut}(E/F)$, $K_\ell = E^{H_\ell}$, $\ell = 1,2$

$H_1 \leq H_2 \iff E^{H_2} \leq E^{H_1}$

(3) $H \leq \underbrace{\mathrm{Aut}(E/F)}_{=:G} \Rightarrow$ then $[E:E^H] = |H|$

$(\iff [E^H:F] = [G:H])$

Pf. (2) ($\Rightarrow$) Trivial. Fixed by $H_1 \Rightarrow$ fixed by H_2

let $a \in E^{H_2}$. $\forall \sigma \in H_2$, $\sigma(a) = a$. As $H_1 \leq H_2$, $\forall \sigma \in H_1, \sigma(a) = a \Rightarrow a \in E^{H_1}$.

($\Leftarrow$) Cor 3 If $G \leq_{\text{finite}} \mathrm{Aut}(E)$, then $G = \mathrm{Aut}(E/E^G)$.

Suppose $E^{H_2} \leq E^{H_1}$. Then $H_1 = \mathrm{Aut}(E/E^{H_1})$, $H_2 = \mathrm{Aut}(E/E^{H_2})$

Since $E^{H_2} \subseteq E^{H_1}$, if $\sigma \in \mathrm{Aut}(E/E^{H_1})$ then $\sigma \in \mathrm{Aut}(E/E^{H_2})$.

So $H_1 \leq H_2$.

(3) Suppose $H \leq \underbrace{\mathrm{Aut}(E/F)}_{G}$. we proved last time that E/F Galois, $F \subseteq K \leq E \Rightarrow E/K$ Galois

middle of p62.

In particular, E/E^H is Galois. By the first definition,

$[E:E^H] = |\mathrm{Aut}(E/E^H)|$.

By Cor 3, $\quad * = |H|$

By the multiplication formula, $[E:F] = [E:E^H] \cdot [E^H:F]$

$= |H| \cdot [E^H:F]$

Since $[E:F] = |G|$, $\quad |G| = |H| \cdot [E^H:F]$

By Lagrange, $[E^H:F] = [G:H]$

fields $\quad \uparrow\uparrow$ groups!

21-374

4/13/2022

Goal: (2nd "Application" of Gal T)

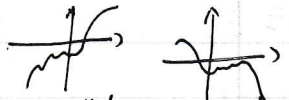
$\mathbb{C}$ is alg closed. $\Leftrightarrow$ FUNDAMENTAL THEOREM of ALGEBRA
$\forall p \in \mathbb{C}[x], \exists \alpha \in \mathbb{C}, p(\alpha)=0.$

we use the following facts: (1) Sylow's First Theorem (Group Th) 'p-Sylow subgroup'
G finite, p prime, $m, n \in \mathbb{Z}$, $|G| = mp^n$, where $(m,p)=1$.
Then $\exists P \leq G$ of cardinality p^n.

p74, 21-375 (2) If G has cardinality p^n for some p prime, $n \geq 1$, then there is $H \leq G$, $|H| = p^{n-1}$. (actually consequence of the above) Known actually

(3) If $p(x) \in \mathbb{R}[x]$ is of odd degree, then $\exists \alpha \in \mathbb{R}, p(\alpha)=0$.

Pf. Using continuity, and $a_n > 0$ or $a_n < 0$, $n = \deg p$



"intermediate value theorem"

- doesn't work for rational functions $\mathbb{Q} \to \mathbb{Q}$
e.g. $f(x) = x^2 - 2$ on $[1,2]$

* (1)–(4) Come from Algebra.
(5)–(6) Come from Analysis.

Lemma. If $z \in \mathbb{C}$, then $\sqrt{z} \in \mathbb{C}$
Write $z = re^{i\theta}$, $\sqrt{z} = \sqrt{r}e^{i\theta/2}$...

4/15/2022

(3) $\forall F$ with $\mathrm{char}\, F = 0$, if $K \supsetneq F$ finite, then $\exists K^* \supseteq K$ s.t. K^*/F is Galois.

p64 (4) (GCT) Suppose E/F Galois, $G = \mathrm{Aut}(E/F)$. Let $H \leq G$.
$[E : E^H] = |H| \Rightarrow [E^H : F] = [G : H]$

(5) "

(4) Primitive Element Theorem
$\mathrm{char}\, F = 0$, E/F finite $\Rightarrow \exists \alpha \in E$, $E = F(\alpha)$

(6) There is no $F \supsetneq \mathbb{C}$ s.t. $[F : \mathbb{C}] = 2$. (implied by FTA) otherwise $\exists$ irreducible polynomial of deg 2
$ax^2+bx+c=0$, $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ (from Babylonia)

Pf. Otherwise $\exists \alpha \in F$ s.t. $F = \mathbb{C}(\alpha)$
Since $\alpha \notin \mathbb{C} \Rightarrow \exists m_\alpha$ monic, irreducible s.t. $m_\alpha(\alpha) = 0$.
$\deg m_\alpha = [\mathbb{C}(\alpha) : \mathbb{C}] = 2$, but m_α can be solved! So $\alpha \in \mathbb{C}$, contradiction. 65

Pf. Suppose $\mathbb{C}$ is not alg closed $\Rightarrow \exists p \in \mathbb{C}[x]$ without a solution. So there is $F/\mathbb{C}$ finite extension. ($F \supsetneq_{\text{finite}} \mathbb{C}$) $\quad [F:\mathbb{R}] = [F:\mathbb{C}][\mathbb{C}:\mathbb{R}]$

Apply ③, $F \leftarrow \mathbb{R}$, $K \leftarrow F$. We get $E \supseteq F$ s.t. $E/\mathbb{R}$ is Galois.

$G = \mathrm{Aut}(E/\mathbb{R})$ is finite [def Galois], so $|G| = 2^n \cdot m$, $(m,2)=1$.
[prime factorization]

By ① (Sylow), $\exists P \leq G$, $|P| = 2^n$. $\quad -(A)$

By ④, $[E^P : \mathbb{R}] = [G:P] \overset{\text{Lagrange}}{=} \dfrac{|G|}{|P|} = \dfrac{2^n \cdot m}{2^n} = m \quad -(B)$

E, $E/\mathbb{R}$ Galois. $F \neq \mathbb{C}$

(A)+(B) $\quad [E^P : \mathbb{R}] = m$.

By PET, $\exists \alpha \in E^P$ s.t. $E^P = \mathbb{R}(\alpha)$

$\Rightarrow \deg m_\alpha = m$ odd, but by ① m_x can be solved ($\Rightarrow \alpha \in \mathbb{R}$)

In other words, $m = 1$. So $|G| = 2^n$.

Since $\mathrm{Aut}(E/\mathbb{C}) \leq \mathrm{Aut}(E/\mathbb{R}) = G$, there is $k \leq n$ s.t. $|\mathrm{Aut}(E/\mathbb{C})| = 2^k$, $k \leq n$.

By Fact ②, $\exists H \leq \mathrm{Aut}(E/\mathbb{C})$, $|H| = 2^{k-1}$, IF $k \geq 1$.

Consider E^H: it is a subfield of E but $E^H \supseteq \mathbb{C}$

Fact: E/F Galois and $E \supseteq K \supseteq F \Rightarrow E/K$ Galois (p64, P62).

$\therefore [E:\mathbb{C}]$ is Galois (since $\mathbb{C} \supseteq \mathbb{R}$)

Using ④, $[E^H : \mathbb{C}] = [\mathrm{Aut}(E/\mathbb{C}) : H] = 2^k / 2^{k-1} = 2$

This implies there is an extension of degree 2; not possible by ⑥. So $k = 0$.

~~$|\mathrm{Aut}(E^H/\mathbb{C})| = 2^0 = 1$.~~

~~So $n=1$, $|E| = 2^n \cdot m = 2^1 \cdot 1 = 1$~~ $\Rightarrow |\mathrm{Aut}(E/\mathbb{C})| = 1$ ($k=0$)

$\Rightarrow [E:\mathbb{C}] = 1$

$\Rightarrow E = \mathbb{C}$ □

Remark. This proof, due to E. Artin (~1930), doesn't use all the information on $\mathbb{C}, \mathbb{R}$.

We used only the completeness of $\mathbb{R}$ and Euler's formula.

'real-closed fields'

There are different examples of fields $F \subseteq E$ s.t. $[E:F] = 2$

↑ looks like real numbers; ordered & complete (IVT)

4/12/2022

Theorem Let E/F be Galois, $F \le K \le E$.

Remaining parts of FTGT:
1. K/F is Galois $\Leftrightarrow$ $\mathrm{Aut}(E/K) \trianglelefteq \mathrm{Aut}(E/F)$,
2. K/F is Galois $\Rightarrow$ $\mathrm{Aut}(K/F) \cong \dfrac{\mathrm{Aut}(E/F)}{\mathrm{Aut}(E/K)}$. (quotient by normal subgroup) p48.

Facts. (A) (Uniqueness of Alg closures) If k/F is finite, then $\exists\, \gamma : k \to \overline{F}$ s.t. $\gamma \wedge F = \mathrm{id}_F$.

pf of lemma (B) Let E/F be Galois, $p \in F[x]$ irreducible s.t. $\exists \alpha \in E$, $p(\alpha) = 0 \Rightarrow p$ splits $E[x]$

(FTGT) bijection (C) When E/F is Galois,
$H \mapsto E^H$ (for $H \le \mathrm{Aut}(E/F)$)
$K \mapsto \mathrm{Aut}(E/K)$ (for $F \le K \le E$)
are mutual inverses
$E^{\mathrm{Aut}(E/K)}$ (p58, or from bijection) "H" (p64)

(D) (FGT) Let E/F be Galois, $F \le K \le E$. $[K:F] = [\mathrm{Aut}(E/F) : \mathrm{Aut}(E/K)]$
and $[E:K] = |\mathrm{Aut}(E/K)|$.

(E) (Uniqueness of Splitting fields) If $\gamma : k_1 \cong k_2$, $p \in k_1[x]$, E_1 splitting field of p/k_1 and E_2 " $\gamma(p)/k_2$
Then $\exists\, \tau : E_1 \cong E_2$, $\tau \supseteq \gamma$.

(F) (First Isomorphism) $\varphi : G_1 \to G_2$ surj homo $\Rightarrow G_2 \cong G_1/\ker\varphi$.

(G) Let $H \le G$. Then $H \trianglelefteq G \Leftrightarrow \forall \sigma \in G$, $\sigma H \sigma^{-1} = H$ (we always have $\sigma H \sigma^{-1} \supseteq H$)
conjugate containment (another characterization is left coset = right coset)

Proof of theorem.

let $F \subseteq K \subseteq E$. By (9), $\exists H \leq \mathrm{Aut}(E/F)$ s.t. $K = E^H$. Consider (contains K, since K is finitely generated)

$$\mathrm{Emb}(K,F) := \{\tau : K \to \overline{F} \mid \tau \upharpoonright F = \mathrm{id}_F\}.$$

Clearly $\mathrm{Aut}(K/F) \subseteq \mathrm{Emb}(K,F)$ using (A). We are interested in when equality occurs.

- Remark: $\sigma \in \mathrm{Aut}(E) \Rightarrow \sigma[K] \leq E$.
- Claim: If $\tau \in \mathrm{Emb}(K,F)$, then $\tau[K] \in E$.

Proof. Given $\alpha \in K$, pick $m_\alpha \in F[x]$ irreducible such that $m_\alpha(\alpha) = 0$. (α is also over F so $\tau(b\alpha^5) = \tau(b)[\tau(\alpha)]^5 \ldots$) Since $\alpha \in K \subseteq E$, using (B) E contains all the roots of m_α. But $\tau(\alpha)$ is a root of p (since $\tau(p) = p$ for $\tau \upharpoonright F = \mathrm{id}_F$) $\Rightarrow \tau(\alpha) \in E$.

Since E/F is Galois, by definition there exists $p \in F[x]$ separable s.t. E is splitting field of p/F. Since K is between F and E, E " p/K.

Idea: Given K/F Galois. Show $\sigma \overset{\varphi}{\mapsto} \sigma \upharpoonright K$ for $\sigma \in \mathrm{Aut}(E/F)$ is a surjective homomorphism to $\mathrm{Aut}(K/F)$, $\ker\varphi = \mathrm{Aut}(E/K)$, then use (F). ($\mathrm{Aut}(E/F) \twoheadrightarrow \mathrm{Aut}(K/F)$)

Given $\sigma \in \mathrm{Aut}(E/F)$, let $\tau := \sigma \upharpoonright K$. $\tau : K \cong \tau[K]$, $\tau \upharpoonright F = \mathrm{id}$. As $p \in F[x]$, $\tau(p) = p$. So E splitting field of $p/K \Rightarrow E$ similarly splits $p/\tau[K]$.

Using (E), $\exists \sigma \in \mathrm{Aut}(E/F)$, $\sigma \supseteq \tau$.

Suppose $\sigma_1, \sigma_2 \in \mathrm{Aut}(E/F)$ agree on K. Then $\sigma_1^{-1} \circ \sigma_2 = \mathrm{id}_K$.

$\Leftrightarrow \sigma_1^{-1} \circ \sigma_2 \in H \Leftrightarrow \sigma_1 H = \sigma_2 H$

$\sigma^{-1} \circ \sigma_2 \in \mathrm{Aut}(E/K) = \mathrm{Aut}(E/E^H) \overset{\text{by def.}}{=} H$ (opposite directions obvious)

Namely $|\{\sigma \upharpoonright K : \sigma \in \mathrm{Aut}(E/F)\}| = [\mathrm{Aut}(E/F) : H]$ (index is no. of cosets)

$\mathrm{Aut}(E/K)$

we could have just started here to prove (1) and (2) ~~[E:F] by (9)~~ (repeated next page)

E^H !

By (D), $[\mathrm{Aut}(E/F):H] = [K:F]$ (right to left)

So $|\mathrm{Emb}(K,F)| = [K:F]$ ① As before $\mathrm{Emb}(K,F) \cong \mathrm{Aut}(K/F)$ ②

By definition, $*$ K/F is Galois $\Leftrightarrow [K:F] = |\mathrm{Aut}(K/F)|$ ③

① + ② + ③ K/F is Galois $\Leftrightarrow \mathrm{Emb}(K,F) = \mathrm{Aut}(K,F)$.

Continuing our work on $\sigma \mapsto \sigma|_K$, consider for some fixed $\sigma_i \in \mathrm{Aut}(E/F)$

$$G_i := \{\sigma_* \in \mathrm{Aut}(E/F) \mid (\forall k \in K)\ \sigma_*(\sigma_i(k)) = \sigma_i(k)\} \leq \mathrm{Aut}(E/F)$$

Recall $K = E^{H = \mathrm{Aut}(E/k)}$. Since $E^{G_i} = \sigma_i[K]$ ($F = E^{\mathrm{Aut}(E/F)}$), $|G_i| = [E:\sigma_i[K]] = [E:K] = |H|$. Moreover, $\sigma_i H \sigma_i^{-1} \subseteq G_i$ by direct computation

Then $\sigma_i H \sigma_i^{-1} = H$. Note $\sigma_i[K] = K \Leftrightarrow G_i = H$, $\forall \sigma \in \mathrm{Aut}(E/F)$. But $\sigma_i[K] = K$ $\forall \sigma_i \in \mathrm{Aut}(E/F)$

$\Leftrightarrow \sigma_i H \sigma_i^{-1} = G_i$ $(\forall i)$ $\Leftrightarrow G_i = H$

by injectivity of $\sigma_i|_K$ $\Leftrightarrow |\mathrm{Emb}(K/F)| = |\mathrm{Aut}(K/F)|$

$\Leftrightarrow [K:F] = |\mathrm{Aut}(K/F)|$ as shown above.

To summarize, K/F is Galois $\Leftrightarrow \forall \sigma \in \mathrm{Aut}(E/F)$, $\sigma H \sigma^{-1} = H$. This is claim ①, by ⑤.

For $\sigma \in \mathrm{Aut}(E/F)$, consider $\sigma|_K$. Always $\sigma|_K \in \mathrm{Emb}(K,F) \cong \mathrm{Aut}(K/F)$ if K/F Galois

$\mathrm{Aut}(E/F)$ $\mathrm{Aut}(K/F)$

So $\sigma \mapsto \sigma|_K$ is surjective because $\chi \in \mathrm{Aut}(K/F)$ can be extended to $\sigma_i : E \cong E$

$\subseteq \mathrm{Emb}(K,F)$

Since $\mathrm{id}_{\mathrm{Aut}(K/F)} = \mathrm{id}_K$, $\ker \varphi = H$. By the first isomorphism theorem,

$$\mathrm{Aut}(K/F) \cong \frac{\mathrm{Aut}(E/F)}{H} = \frac{\mathrm{Aut}(E/F)}{\mathrm{Aut}(E/K)}$$

Solution by Radicals Given $p \in F[x]$, $p = \sum_{k=0}^{n} a_k x^k$. How do we characterize a solution by radicals A?

$A \leftarrow$ Expression in terms of $+, \cdot, -, /, \sqrt[m]{\ldots}$ "syntactic"

Field Theoretic Formulation of "solvable by Radicals":

→ There must exist $\{K_i \mid i \le t\}$, $t \in \mathbb{N}$ s.t.

$F = K_0 \subsetneq K_1 \subsetneq \ldots K_{i-1} \subsetneq K_i \ldots \subsetneq K_t$, where K_t contains E, the splitting field of p/F

and $\forall i < t$, $K_{i+1} = K_i(\alpha_i)$ for α_i some root of $x^m - a$ for some $a \in K_i, m \in \mathbb{N}$

("big enough")

('how many times we take roots')

$\alpha_i = \sqrt[m]{a}$

Lemma If p is solvable by radicals, then there exists $\{K_i\}$ as above such that $[K_{i+1} : K_i] = p_i$ prime. (in a char-0 field)

Pf. Suppose $\{K_i' \mid i \le t'\}$ is a "witness". If $m_j = [K_{i+1}' : K_i']$ is composite, we can factor m_j and find $p \mid m_j$, find $K_i' \subsetneq K_{i,1}^* \subsetneq K_{i+1}$ of degree p. Repeat this for m_j/p and K_i^*.

(primitive element theorem!)

Eventually we get $K_i = K_i' \subsetneq K_i^* \subsetneq K_i^{**} \ldots \subsetneq K_{i+1}$, each extension prime.

(instead of adjoining $\sqrt[m_j]{a}$, adjoin $\sqrt[p]{a}$. (irreducible polynomial has degree $m_j/p \ldots$))

"Solvable Groups" Let G be a group.

(1) $G' = \langle \{[aba^{-1}b^{-1}] \mid a, b \in G\} \rangle$ 'commutator subgroup', 'derivative' $\triangleleft G$ (normal subgroup!)

(2) Let $N \triangleleft G$, G/N commutative $\iff N \supseteq G'$.

(3) G is solvable iff $\exists n \in \mathbb{N}$ where $G^{(k+1)} = [G^{(k)}]'$, $G^{(0)} = \{1_G\}$

Remark: If G is commutative, $G' = \{1_G\}$. Otherwise, one step before we must be commutative!

④ Suppose G solvable. If $\varphi: G \to H$ homo, then $\varphi[G]$ is solvable

" If $H \leq G$, then H is also solvable.

⑤ Suppose $N \trianglelefteq G$. If G/N is solvable and N is solvable, then G is solvable.

Gal: Main Theorem

Let F, $p \in F[x]$, $\operatorname{char} F = 0$. E splitting field of p/F. If p is solvable by radicals, then

[group!] $\operatorname{Aut}(E/F)$ is solvable. (by $\operatorname{Aut}(E/F)$, what splits over F)

Prop. There is $p \in \mathbb{Q}[x]$ of degree 5 such that its Galois group is S_5, and S_5 is not solvable.

Corr. Thus p has no solutions by radicals.

Def. $\alpha \in F$ is an nth root of unity iff $\alpha^n - 1 = 0$. Note $1' = n_\lambda$ using the formal derivative (in a char 0 field).

$U_n(F) := \{\alpha \in F \mid \alpha^n = 1\}$, this is a subgroup of $(F^*, \cdot)$ with respect to multiplication.

$\alpha \in F$ is an nth primitive root of unity (generator) provided $\langle \alpha \rangle = U_n(\alpha)$.

existence of primitive root? - see sec 5.5, Prop 18 - Uniq not...

Example. $F = \mathbb{C}$, $U_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{\frac{2\pi i k}{n}} \mid 0 \leq k < n\} \cong \mathbb{Z}/n\mathbb{Z}$.

$e^{2\pi i k/n}$ is a primitive nth root of unity if $(k,n) = 1$. ← φ-function...

- Suppose $K_{i+1} = K_i(\alpha_i)$, where $a \in K_i$ and $\alpha_i^m - a = 0$ for some m. If K_{i+1} contains $U_m(E)$, then K_{i+1} is a splitting field of $x^m - a \Rightarrow K_{i+1}$ is Galois $/K_i$.

(separable since the m roots are $\{a z_1, a z_2, \ldots a z_m\}$ for the m roots of unity)

By the same argument,

- Suppose $p \in F[x]$, $n = \deg p$, and for every q prime s.t. $q \mid n!$, F contains all the qth roots of unity. Then for all $i \leq t$, K_t/K_i, K_{i+1}/K_i, and K_i/F are Galois.

? see p76 $K_{i+1} = K_i(\alpha_i)$ $\alpha_i^m - a = 0$ (not necessarily = 1!) max deg of splitting field

21-374 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$ not Galois because $\mathbb{Q}(\sqrt[3]{2})$ does not contain non-real numbers. 4/25/2022

Special Case of Main Theorem:

E splitting field of p/F

Suppose $p \in F[x]$, $\operatorname{char} F = 0$, $n = \deg p$, and F contains all the qth roots of unity for $q \mid n!$. (see previous claims) "makes things easier"

Then p solvable $\Rightarrow \operatorname{Aut}(E/F)$ is solvable.

Pf. By lemma, [p71] we may assume $\exists \{K_i\}_{i \le t}$ s.t. $F = K_0 \subsetneq K_1 \cdots \subsetneq K_i \subsetneq K_i(\alpha_i) \cdots \subsetneq K_t \supseteq E$, where $[K_{i+1} : K_i] = p_i$ (prime), $\alpha_i^{p_i} \in K_i$.

Let $G_1 = \operatorname{Aut}(K_t/K_1)$, $G = \operatorname{Aut}(K_t/F) = G_0 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq G_t = \{1\}$.

Since K_{i+1}/K_i Galois, $|\operatorname{Aut}(K_{i+1}/K_i)| = [K_{i+1} : K_i] = p_i$.

By the last part of ECT, $\operatorname{Aut}(K_{i+1}/K_i) \cong \dfrac{\operatorname{Aut}(K_t/K_i)}{\operatorname{Aut}(K_t/K_{i+1})}$ ["$F \le K \le E$"; $K_i \le K_{i+1} \le K_t$]

$\Rightarrow \left| \dfrac{\operatorname{Aut}(K_t/K_i)}{\operatorname{Aut}(K_t/K_{i+1})} \right|$ is p_i ($\Rightarrow$ cyclic!) (prime order)

$\Rightarrow \dfrac{\operatorname{Aut}(K_t/K_i)}{\operatorname{Aut}(K_t/K_{i+1})}$ is abelian.

We also know by ECT $G_i \trianglerighteq G_{i+1}$ ('N') for all i.

G_1/G_{i+1} Abelian $\Rightarrow G_1' \le G_{i+1}$ (Fact (2) page 71)

By induction, $G^{(t)} \le G_t$ but $G_t = \{1\}$ by definition. This means $G^{(t)} = 1$.

So G is solvable. ($\operatorname{Aut}(K_t/F)$ is solvable). We are left with showing $\operatorname{Aut}(E/F)$ is solvable.

↳ Since K_t is a splitting field of some poly/F (up to particular fix...)

K_t/F is Galois $\Rightarrow K_t/E$ is Galois since $F \le E \le K_t$

$\therefore \operatorname{Aut}(E/F) \cong \dfrac{\operatorname{Aut}(K_t/F)}{\operatorname{Aut}(K_t/E)}$. So $\operatorname{Aut}(E/F)$ ('N') is a homomorphic image of $\operatorname{Aut}(K_t/F)$ 'G' by... 73

$\mathrm{Aut}(K_t/F)$ $\quad$ $\mathrm{Aut}(E/F)$

$\sigma \in \mathbb{E} \mapsto \sigma N$ (mapping to cosets)

By property (4) p 572 $\mathrm{Aut}(K_t/F)$ is solvable $\Rightarrow$ $\mathrm{Aut}(E/F)$ is solvable.

Main theorem $p \in F[x]$, E sp.f. of p/F, $\mathrm{char}\, F = 0$.

If p is solvable by radicals/F, then $\mathrm{Aut}(E/F)$ is solvable.

Lemma Suppose $\mathrm{char}\, F = 0$, $n \in \mathbb{N}^+$, $E = F(\alpha)$ and α is a primitive n^{th} root of unity.
~ Prop 36, 14.7 Then E is splitting field of $x^n - 1$ and $\mathrm{Aut}(E/F)$ is abelian.

Pf. $\langle \alpha^k \mid k < n \rangle$ are all distinct roots of $x^n - 1$. So E/F is a splitting field.

Take $\sigma \in \mathrm{Aut}(E/F)$. What is $\sigma(\alpha)$? Note that $\sigma(\alpha)$ ($\in U_n(E)$) determines σ since α generates $U_n(E)$. Look at $\{e^{2\pi i k/n} \mid k \le n\} \subseteq \mathbb{C}$.

$\sigma(\alpha) = \alpha^{k_\sigma}$, $0 \le k_\sigma < n$. Since α is a primitive root, α^{k_σ} is also primitive. (must generate $U_n(E)$)

- So we found $\sigma \mapsto k_\sigma$ from $\mathrm{Aut}(E/F)$ into $\mathbb{Z}/n\mathbb{Z}$ (multiplicative group!)
- Let $\sigma, \tau \in \mathrm{Aut}(E/F)$. $\sigma \circ \tau(\alpha) = \sigma(\alpha^{k_\tau})$ relatively prime nos. $\le n$

$= [\tau(\alpha)]^{k_\tau}$

$= (\alpha^{k_\sigma})^{k_\tau} = \alpha^{k_\sigma k_\tau}$

So $\mathrm{Aut}(E/F)$ is isomorphic to a subgroup of the invertible elements of $\mathbb{Z}/n\mathbb{Z}$.

$\therefore$ $\mathrm{Aut}(E/F)$ is cyclic $\Rightarrow$ abelian.

Proof of Main Theorem

Suppose $\{K_i \mid i \le t\}$ is a radical tower for p/F,

$K = K_0 \subsetneq \cdots \subsetneq K_i \subsetneq K_{i+1} \cdots \subsetneq K_t \supseteq E$ (E splitting field of p over F).

$K_i = K_{i-1}(\alpha_i)$

We may assume as before that $[K_{i+1} : K_i] = p_i$ is prime. Let $n = \prod p_i$. We find $\alpha \in \bar{F}$ some nth primitive root of unity (e.g. $e^{2\pi i/n}$).

exists since the simple p_i have elements $\Rightarrow$ cyclic!

Consider $F = K_0 \leq K_0(\alpha) \leq \dots K_i(\alpha) \leq K_{i+1}(\alpha) \dots \leq K_t(\alpha)$.

We know, by the lemma, $F(\alpha)/F$ is a splitting field of separable polynomial $X^n - 1$.

So $F(\alpha)/F$ is a Galois extension. Then $\mathrm{Aut}(F(\alpha)/F) \cong \mathrm{Aut}(K_t(\alpha)/F)$ by ECT.

'H' $\qquad$ 'E' $\qquad$ $\mathrm{Aut}(K_t(\alpha)/F(\alpha))$ 'N'

But by the lemma, $\mathrm{Aut}(F(\alpha)/F)$ is also abelian. Recall that E abelian $\Rightarrow E = \{1\}$ ($\Leftarrow$ every abelian group is solvable). $H \cong E/N \Rightarrow E/N$ is solvable.

Using the previous theorem, $\mathrm{Aut}(K_t(\alpha)/F(\alpha))$ is solvable. Using property (5), since $F(\alpha)$ contains all the desired roots of unity

we conclude that $\mathrm{Aut}(K_t(\alpha)/F)$ is solvable.

As E is some splitting field over F (as in the preceding Wecken version), E/F is Galois.

So $\mathrm{Aut}(E/F) \cong \dfrac{\mathrm{Aut}(K_t(\alpha)/F)}{\mathrm{Aut}(K_t(\alpha)/E)}$. As $\mathrm{Aut}(E/F)$ is a homomorphic image of the solvable group $\mathrm{Aut}(K_t(\alpha)/F)$, $\mathrm{Aut}(E/F)$ is solvable.

there is some technical difficulty here, so for simplicity we assume the polynomial is irreducible

21-374 4/29/2022

see p72.

Galois extensions are not transitive in general, so we do not know K/F is Galois a priori.

We get around this by

(1) Using something weaker: Show K/F is a splitting field

(2) Avoiding GCT in key parts of the proof on p73 and p75.

Theorem (to answer (2)) Suppose $F \leq K \leq E$ s.t. E/K splitting field and K/F splitting field.

Then $\forall \sigma \in \mathrm{Aut}(E/F)$, $\varphi(\sigma) := \sigma|_K$, $\varphi : \mathrm{Aut}(E/F) \to \mathrm{Aut}(K/F)$ is surjective homomorphism with $\ker \varphi = \mathrm{Aut}(E/K)$

↳ Then by 1st isomorphism theorem, $\mathrm{Aut}(K/F) \cong \dfrac{\mathrm{Aut}(E/F)}{\mathrm{Aut}(E/K)}$

Pf. As K/F is a splitting field of some p/F, let $\alpha_1, \dots \alpha_n \in K$ be all the roots of p. So $K = F(\alpha_1 \dots \alpha_n)$.

Given $\sigma \in \mathrm{Aut}(E/F) \Rightarrow \sigma|_F = id_F \Rightarrow \sigma(p) = p$ (keeps coefficients unchanged)

$\sigma(\alpha_i)$ is also a root of p (midterm!). So $\sigma(\alpha_i) \in \{\alpha_1 \dots \alpha_n\}$.

Why is $\sigma|_K$ onto K? Since $\{\sigma(\alpha_i) \mid 1 \leq i \leq n\} = \{\alpha_1 \dots \alpha_n\}$, so $\sigma|_K[K]$ generates K.

(1) So $\varphi(\sigma) \in \mathrm{Aut}(K/F)$

(2) φ is clearly a homomorphism

(3) $\ker \varphi = \{\sigma \in \mathrm{Aut}(E/F) \mid \varphi(\sigma) = id_K\} = \{\sigma \in \mathrm{Aut}(E/F) \mid \sigma|_K = id_K\} = \mathrm{Aut}(E/K)$.

Why φ is onto $\mathrm{Aut}(K/F)$? Given $\gamma \in \mathrm{Aut}(K/F)$, as E is splitting field/K, $\exists \sigma \in \mathrm{Aut}(E) \geq \gamma$. So $\varphi(\sigma) = \gamma$.

Theorem (Abel-Ruffini)

There exists $q(x) \in \mathbb{Q}$ of degree 5 that has no solutions by radicals.

Proof. Take $q(x) = x^5 - 4x + 2$. (2 divides 2 and 4 (and 0), but not 1; 4 does not divide 1) Let E be its splitting field.

Fact (Eisenstein Criterion, Ch 9.4): $q(x)$ is irreducible. Since $\mathbb{Q}$ is char 0, we know q is separable.

Thus E is Galois over $\mathbb{Q}$. Let $\{\alpha_1, \alpha_2 \dots \alpha_5\} \subseteq \mathbb{C}$ be the five roots of q. (deg q)

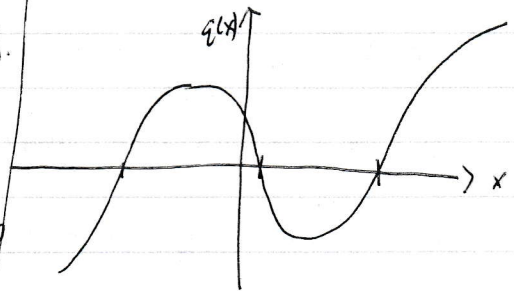
Then $E = \mathbb{Q}(\alpha_1 \dots \alpha_5)$.

Given $\sigma \in \mathrm{Aut}(E)$ ($= \mathrm{Aut}(E/\mathbb{Q})$ — automorphism must fix the prime field), $\{\sigma(\alpha_i) \mid 1 \le i \le 5\} = \{\alpha_1 \dots \alpha_5\}$

So we can identify $\sigma \in \mathrm{Aut}(E)$ with a permutation of $\{\alpha_1, \dots \alpha_5\}$.

Since the permutations of $\{\alpha_1 \dots \alpha_5\}$ are isomorphic to S_5, we conclude that $\mathrm{Aut}(E) \le S_5$. (up to isomorphism)

Let's graph $y = q(x)$ on $\mathbb{R}$.



Set $q'(x) = 5x^4 - 4 = 0$.

Take $c = \sqrt[4]{4/5}$, $q(c) < 0$

$q(-c) > 0$

Suppose α_1, α_2 and α_3 are the 3 real roots. So $\alpha_4, \alpha_5 \in \mathbb{C} - \mathbb{R}$.

Necessarily $\overline{\alpha_4} = \alpha_5$, $\overline{\alpha_5} = \alpha_4$, if we take σ to be complex conjugation.

$\Rightarrow$ The group of permutations of $\{\alpha_1 \dots \alpha_5\}$ contains the transposition (α_4, α_5). (*)

Any degree-5 polynomial with only 3 real roots is thus a counterexample.

$[E:\mathbb{Q}] = [E:\mathbb{Q}(x_1)] \cdot [\mathbb{Q}(x_1):\mathbb{Q}]$.

Since f is irreducible of degree 5, $[\mathbb{Q}(x_1):\mathbb{Q}] = 5$.

Since $E/\mathbb{Q}$ is Galois, $[E:\mathbb{Q}] = |\mathrm{Aut}(E)| \; (= |\mathrm{Aut}(E/\mathbb{Q})|)$

$\Rightarrow 5 \mid |\mathrm{Aut}(E)|$.

Recall Cauchy's Theorem: Let G be finite, p a prime s.t. $p \mid |G|$. Then there is $G_1 \leq G$ such that $|G_1| = p$ & G_1 contains a generator

Thus, there is $\sigma \in \mathrm{Aut}(E)$ of order 5.

Fact (Ch1, DF): (**) let $H \leq S_n$ for n prime. If $\exists \tau \in H$ same form transposition (swapping of two elements only) and $\exists \sigma \in H$ of order n, then $H = S_n$. → show this yields all transpositions of form $(i\ i+1)$ → show $(i\ i+1)$ yields all possible transpositions

see Keith Conrad's notes online too

Using these facts (* + **), we get $\mathrm{Aut}(E) = S_5$. It remains to show that S_5 is not solvable.

In general, $n \geq 5 \Rightarrow S_n$ is not solvable. We sketch the proof below:

(1) $S_n' = A_n$ (ch 3.5) (alternating group) (regardless of n)

(2) When $n \geq 5$, A_n has no proper normal subgroup

$\Leftrightarrow A_n$ is simple.

So either $A_n' = A_n$ or $A_n' = \{1\}$. But A_n (when $n \geq 5$) is not abelian, so $A_n' = A_n$.

Then $\forall k$, $S_n^{(k+1)} = A_n^{(k)} = A_n \neq \{1\}$. Thus S_n is not solvable.

□

21-374 'Galois +'

$[E:F] = |Aut(E/F)|$ finite

Let E/F be Galois, $G := Aut(E/F)$. Then

$\{K \mid F \leq K \leq E\}$ (fields) $\cong$ (bijection) $\{H \mid H \leq G\}$ (finite groups)

$K \longmapsto Aut(E/K)$ ↙ all finite!

$E^H = \{a \in E \mid \forall \sigma \in H, \sigma(a) = a\} \longleftarrow H$

Furthermore, ① $[E:E^H] = |H|$, ② $H_1, H_2 \leq Aut(E/F)$, $H_1 \leq H_2 \iff E^{H_2} \leq E^{H_1}$

③ E/E^H is Galois, and $Aut(E/E^H) = H$.

④ E^H/F Galois $\iff Aut(E/E^H) \triangleleft G$.

⑤ $Aut(E^H/F) \cong Aut(E/F) / Aut(E/E^H)$

Key Technical: Let E be a field, G be a finite subgroup of $Aut(E)$. Denote $F := E^G$. (fixed elements under all of G)
Then $[E:F] = |G|$.

Prerequisites:
- Linear Algebra
- $\chi : G \to L^\times$ (group → mult. group of L) group homomorphism is a character from G to L. They are linearly independent if $(\forall a_1, a_2, \ldots a_n \in L)\left[(\forall g \in G)\left(\sum_{i=1}^n a_i \chi_i(g) = 0\right) \Rightarrow a_1, a_2, \ldots a_n = 0\right]$

Theorem: If $\{\chi_1, \chi_2 \ldots \chi_n\}$ are distinct characters from G to L, then they are linearly independent over L.

This yields the following corollaries:

ⓐ If E/F is finite, then $|Aut(E/F)| \leq [E:F]$

ⓑ E/F is Galois $\iff F = E^{Aut(E/F)} \iff \exists p \in F[x]$ separable, E splitting field of p over F

↓ Main lemma: Let E/F Galois. If $q \in F[x]$ is any irreducible polynomial with a root in E, then q splits in E and q is separable.

ⓒ $G \leq_{\text{finite}} Aut(E) \Rightarrow G = Aut(E/E^G)$

ⓓ $G_1, G_2 \leq_{\text{finite}} Aut(E)$, $G_1 \neq G_2 \Rightarrow E^{G_1} \neq E^{G_2}$

Using these results, we can prove the main bijection, ①② (key technical, H finite) and ③ ($F \leq E^H \leq E$, then ⓑ ...) p64 of Theorem

Ref