Def. A field $F = \langle S, +, \cdot, 0, 1 \rangle$ such that $0 \neq 1 \in S$

(constants; $+, \cdot$: binary operations)

- a group
  1) Associativity $\forall x, y, z \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  2) 0 additive identity $\forall x \quad [0 + x = x + 0 = x]$
     $\forall x, \exists y$ s.t. $[x + y = 0]$
  3)* 1 multiplicative identity $\forall x \quad [x \cdot 1 = 1 \cdot x = x]$
     $\forall x \; [x \neq 0 \Rightarrow \exists y \text{ s.t. } x \cdot y = y \cdot x = 1]$

(without 3): commutative ring with identity

  4) Dist $\forall x, y, z \quad [x \cdot (y + z) = x \cdot y + x \cdot z]$

(rings that are not commutative are exemplified by matrices)

  5) Comm $\forall x, y \quad x \cdot y = y \cdot x, \; x + y = y + x$

Examples: $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$

Motivation: Solving (polynomial) equations. General case. Given $a_0, \ldots a_n \in \mathbb{R}$, solve for x: $\sum_{k=0}^{n} a_k x^k = 0$?

$(n=1)$ $ax + b = 0 \Rightarrow x = -\frac{b}{a}$. 3,700 years ago Babylonians.

$(n=2)$ $ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ (but no variables at that time)

Question $(n=3)$ ~1550 Cardano ✓ p630 D&F

$(n=4)$

$(n=5)$ Want to find $f(a_5, a_4, a_3, a_2, a_1, a_0)$ involving $\sqrt[k]{\;}, +, \cdot, -, /$ s.t. if $\alpha, \beta, \gamma, \delta, \varepsilon, \lambda \neq 0$ then $f(\alpha, \beta, \ldots)$ is a root of $\alpha x^5 + \beta x^4 + \gamma x^3 + \delta x^2 + \varepsilon x + \lambda = 0$.

("solution by radicals")

~1810/20 Abel + Ruffini not possible to find $f(x \ldots)$

Evariste Galois Impossibility of solving equations by radicals (can find counterexample)

Applications (group + field theory) &

1) Number theory (algebraic)
2) Algebraic geometry

Digital signal processing (minimize information loss)

Harmonic analysis in finite fields

Encryption ...

Main Ideas

- Galois studied groups to solve problems in fields.

(A)

- Let F be a field. $\varphi: F \to F$ is an automorphism provided
  (1) φ is a bijection
  (2) $\forall x \forall y \; [\varphi(x+y) = \varphi(x) + \varphi(y)]$
  (3) $\forall x, y. \quad \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

Fact $\psi: G \to H$ group hom $\Rightarrow \psi(1_G) = 1_H$. $\quad \psi(1_G \cdot 1_G) = \psi(1_G) = \psi(1_G) \cdot \psi(1_G)$

Cor. $\varphi(1_F) = 1_F$, $\varphi(0_F) = 0_F$

$\mathrm{Aut}(F) := \{\varphi \mid \varphi: F \cong F\}$ = "all automorphisms of F"

Lemma $\varphi, \psi \in \mathrm{Aut}(F) \Rightarrow \varphi \circ \psi \in \mathrm{Aut}(F)$

Pf. (a) $\varphi \circ \psi(x+y) = \varphi(\psi(x+y)) = \varphi(\psi(x) + \psi(y))$

$= \varphi(\psi(x)) + \varphi(\psi(y))$.

Similarly, $\mathrm{Aut}(F)$ is closed under inverses.

Cor. $(\mathrm{Aut}(F), \circ)$ is a group.

($\circ$: composition)

Def. Let F, E be fields. F is a subfield of E provided

1) $F \subseteq E$

2) $\forall a, b \in F$, $a +_F b = a +_E b$, $a \cdot_F b = a \cdot_E b$

Notation $F \leq E$

Examples $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

Def. $\mathrm{Aut}(E/F) = \mathrm{Aut}_F(E) := \{ \varphi \in \mathrm{Aut}(E) \mid (\forall a \in F)\ \varphi(a) = a \}$ ('identity on F')

(for $F \leq E$ fields)

↑ study normal subgroups inside here, group actions... on this set

'Galois group of E over F'

"look inside"

"Field extension" where you're likely to find solutions (between $\mathbb{R}$ and $\mathbb{C}$)

(B) Classification problem. What are the isomorphism types of fields?

Examples: (1) Given an integer n, does there exist a field of cardinality n?

(2) If so, how many fields up to isomorphism of card n exist?

(3) Similarly, for infinite cardinals?

Examples (1) p is prime $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ is a field of p-many elements. (commutative ring; maximal ideal)

Unique up to isomorphism.

see 21-373 notes plus-log. I max $\Rightarrow$ I prime etc.

(2) Suppose n is composite. Does there exist a field of n-many elements?

Theorem (later) If F is a finite field, then $\exists$ prime p and integer n s.t. $|F| = p^n$ and if E field s.t. $|E| = p^n$, then $F \cong E$.

"Easy" Theorem If n is a composite but not power of a prime, then there are no fields of cardinality n.

2, 3, 5 prime, $4 = 2^2$.

Cor. There is no field with 6 elements (minimal counterexample!)

* Sometimes infinite fields are isomorphic, sometimes they are not.
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$...

Theorem 2 ('converse' of Th 1) $\forall p$ prime, $\forall n \geq 1$, $\exists$ field s.t. $|F| = p^n$

Remark. There exists a field F s.t. $F \ncong \mathbb{Q}$ but $|F| = |\mathbb{Q}|$.

Linear Algebra (Review) $\mathbb{R}^3, \mathbb{R}^4 \ldots \mathbb{R}^n$ machine learning. 'SVM'

Def. Let F be a 'base' field. An abelian group $(V, +)$ is a vector space over F (F-vector space) provided $\exists F \times V \to V$ called scalar multiplication, i.e. ① $a \cdot (v_1 + v_2) = av_1 + av_2$ $a \in F, v_1, v_2 \in V$

② $(a \cdot_F b) \cdot v = a \cdot (b \cdot v)$ $\forall a, b \in F, v \in V$

③ $(a+b) \cdot v = av + bv$, $\forall a, b \in F, v \in V$

④ $1_F \cdot v = v$ $\forall v \in V$.

Def Let V be an F-vector space, $X \subseteq V$. The span of X,

$$Sp_F(X) := \left\{ \sum_{i=1}^{n} a_i v_i \mid n \in \mathbb{N}, a_i \in F, v_i \in X \right\}$$

Def Let V_1, V_2 be both F-v.sp. V_1 is a subspace of V_2 provided $(V_1, +_1) \leq (V_2, +_2)$ and $\forall a \in F$ $\forall w \in V_1$, $a \cdot w \in V_1$.

Lemma. $X \subseteq V \Rightarrow Sp_F(X)$ is a subspace of V.

Lemma Suppose F, E are both fields. If $F \overset{\text{subfield}}{\leq} E$, then E is a F-vector space.

Pf. Replace V with E.

Def. Let V be a F-vector space. $X \subseteq V$ is called *linearly independent* provided $v \notin sp_F(X - \{v\})$ for all $v \in X$.

$\Leftrightarrow$ $\forall \{v_1, \dots v_n\} \subseteq X$, $\forall a_1 \dots a_n \in F$ $\sum_{k=1}^{n} a_k v_k = 0 \Rightarrow (a_1 = a_2 \dots a_n = 0)$

Pf. If $\exists a_1, \dots a_n \in F$ s.t. $\exists 1 \leq k \leq n$, $a_n \neq 0$ but $\sum a_k v_k = 0$, $a_k v_k = -\sum a_i v_i$

$v_k = \sum \left(\frac{-a_i}{a_k}\right) v_i \Rightarrow v_k \in sp(X - \{v_k\})$

Cor. $\sum a_k v_k = \sum b_k v_k \Rightarrow a_k = b_k \ \forall k \leq n$.

Def. Let F, V, X be as above.

(1) X *generates* $V \Leftrightarrow V = sp_F(X)$

(2) X is a minimal set of generators

$\Leftrightarrow$ (a) X generates V, and (b) $\forall v \in X$, $sp_F(X - \{v\}) \subsetneq V$.

(3) X is a maximal linearly independent set

$\Leftrightarrow$ (a) X is linearly independent, and (b) $w \in V - X \Rightarrow X \cup \{w\}$ not linearly independent

Theorem. Let F, V, X be as above. TFAE

(1) X is a min set of generators (2) X is a max lin. indep. set.

Def. If (1) holds, then we say X is a *basis* of V.

Theorem A (Existence) Suppose V is F-vector space. If V is finitely generated ($\exists X \subseteq V$ finite, $sp_F(X) = V$) then $\exists X \subseteq V$ basis.

Proof Algorithm. Remove the first vector, if you don't generate anything try replacing another. Repeat until you get a minimal set.

Remark. Statement is true also when V not finitely generated. The proof uses Axiom of Choice / Zorn's Lemma [21-329].

use lemma: If $S=\{v_1,\dots v_n\}$ is a basis for a vector space V and $T=\{w_1,\dots w_m\}$ is a linearly independent set of vectors in V, then $m\le n$.

Theorem B (Uniqueness) Let V be F-vector space. If B_1, B_2 are two bases of V, then $|B_1|=|B_2|$ $(=\dim_F V)$

Def/Remark. The dimension of V over F, $\dim_F V$, is unique.

Def. $F\le E$ (fields), $[E:F]=\dim_F E$

Prop Suppose V, W both F-vector spaces. If $\dim_F V_1=\dim_F V_2$ then $\exists\, T: V_1\cong V_2$.

Proof. Suppose B_ℓ is a basis of V_ℓ $(\ell=1,2)$. Since $\dim V_1=\dim V_2$,

$\exists\, f: B_1\to B_2$ bijection. $V_1=SP_F(B_1)$, $T(\sum a_i v_i):=\sum a_i f(v_i)$

Check T is as required. (bijection)

Prop. Let F be a field. Let P be the smallest subfield of F, i.e.

$P=\bigcap_{K\le F} K$. Easy to show that if $\{K_i \mid i\in I\}$ are subfields, then $\bigcap_{i\in I} K_i$ is also a subfield.

generated by 1. "PRIME FIELD" see proof p17

"complex type"

(Example: ① Consider $\mathbb{R}\le\mathbb{C}$. What is $[\mathbb{C}:\mathbb{R}]$?

$\Rightarrow [\mathbb{C}:\mathbb{R}]=2$. Basis: $\{1,i\}$, $\{1+i, 1-i\}$, $\{a, ib\}$ where $a\cdot b\neq 0$)

If $\dim_F V=n$ (integer) then $V\cong F^n$ $(=F\times\dots F)$ (n times)

② What is $[\mathbb{R}:\mathbb{Q}]$? This is certainly not finite (not even countable!)

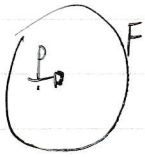
If $[\mathbb{R}:\mathbb{Q}]=n \Rightarrow \mathbb{R}\cong\mathbb{Q}^n \Rightarrow \mathbb{R}$ countable, contradiction.

$|\mathbb{Q}\times\mathbb{Q}|=|\mathbb{Q}|$

21-374 1/24/2022

pf. PS

Theorem If F is a field, its prime field P is either isomorphic to $\mathbb{Q}$ or $P \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.



Corollary. If F is finite, then $F \cong P^d$ where $d = [F:P]$
$\Rightarrow |F| = p^n$ when p is prime
(i.e. No field of 6 elements)

- let R be commutative ring with 1, $\varphi: R_1 \to R_2$ ring homomorphism and $\varphi(1_{R_1}) = 1_{R_2}$. (Cannot 'cancel 1')
- $I \subseteq R$ ideal if $(I, +_R) \leq (R, +_R)$ and $\forall r \in R\ \forall a \in I$, $r \cdot a \in I$.
- $\varphi: R_1 \to R_2$ ring homo, $\ker \varphi = \{a \in R_1 \mid \varphi(a) = 0_{R_2}\}$ is an ideal.
- When I ideal of R, $R/I := \{a + I : a \in R\}$ has operations given by

$$(a+I) \times (b+I) := ab + I$$
$$(a+I) + (b+I) := (a+b) + I$$

$(R/I, \oplus, \odot)$ is also commutative with $1_{R/I} = 1+I$, $0_{R/I} = 0+I = I$.

- (1st Isomorphism) If $\varphi: R_1 \to R_2$ surj homo, then $R_2 \cong R_1/\ker\varphi$

- let R be a ring, $I \subsetneq R$ ideal, I is called a maximal ideal provided there is no ideal $J \subsetneq R$ such that $J \supsetneq I$.

Example: $p\mathbb{Z}$ is maximal ideal of $\mathbb{Z}$ if p prime (add one use, Bezout, contradiction)
$n\mathbb{Z}$ is a max ideal of $\mathbb{Z} \Rightarrow n$ is prime (so we get $\Leftrightarrow$)

- let R, I be as above. I is called prime ideal provided $\forall a, b \in R$-s.t., $a \cdot b \in I \Rightarrow a \in I \vee b \in I$.

- Euclid's lemma: Let $a, b > 0$ integers. p is a prime number. [If $p \mid (ab)$, then $p \mid a \vee p \mid b$.
If $p \nmid c$, $\exists x, y$ $(px + cy) = 1$ (Bezout) etc.]

Corr. p prime $\Rightarrow p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.
($\Leftrightarrow$)

- R is an integral domain $\Leftrightarrow$ R commutative with 1 and $\forall a,b \in R$ [$ab=0 \Rightarrow a=0 \vee b=0$]
  In other words, R has no zero divisors.
  Eg. $\bar{2}, \bar{3}$ are zero divisors in $\mathbb{Z}/6\mathbb{Z}$, since $\bar{2}\cdot\bar{3}=0$.

Theorem. Let R be commutative ring with 1, $I \subsetneq R$ ideal.

(1) I is max $\Leftrightarrow$ R/I field.
(2) I is prime $\Leftrightarrow$ R/I integral domain.

Corr ($\Box$) I max $\Rightarrow$ I prime.

($\Leftarrow$) if I is P.I.D.

$2\cdot 3 \equiv 0 \pmod 6$
$3\cdot 4 \equiv 0$
$2\cdot 3 \equiv 3\cdot 4$
$2\cdot 3 \equiv 3\cdot 4$
$2 \equiv 4$

General Question: Given F field, $p \in F[X]$, is there a root in F?
Find $E \geq F$ s.t. $\exists \alpha \in E$, $p(\alpha)=0$.

1/26/2022

Lemma $\varphi: G_1 \to G_2$ homo. $\ker\varphi = \{1_{G_1}\} \iff \varphi$ is injective

$R_1 \to R_2$ " (same statement for rings)

Question: We want to find some information about the prime field P_F of F.

Theorem: If F is a field, then $P_F \cong (\mathbb{Q}, +, \cdot, 0, 1)$ or $P_F \cong \mathbb{Z}/p\mathbb{Z}$ for prime p.

Proof. Consider $\varphi: \mathbb{Z} \to F$ given by

$(n=0)$ $\varphi(n) := 0_F$.

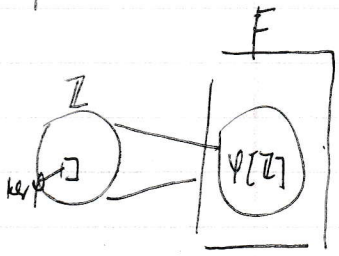
$(n>0)$ $\varphi(\underbrace{1+\dots+1}_{n \text{ times}}) := \underbrace{1_F + \dots + 1_F}_{n \text{ times}}$

$(n=-m<0)$ $\varphi(n) := -(\underbrace{1_F + \dots + 1_F}_{m \text{ times}})$

- Check φ is a ring homomorphism (use distributivity for multiplication)

Case 1: $\ker\varphi = \{0\}$, then φ is injective

Let $R := \varphi[\mathbb{Z}]$ subring of F



$\varphi: \mathbb{Z} \cong R$

"extension ring" $P_F = \{\frac{a}{b} \mid a,b \in R, b \neq 0\} = \{\frac{\varphi(n)}{\varphi(m)} \mid m,n \in \mathbb{Z}, m \neq 0\} \cong \mathbb{Q}$

Case 2: $\ker\varphi \neq \{0\}$. Then R is an integral domain.

$\ker(\varphi) = (\mathrm{ch}(F))\mathbb{Z}$. By the 1st Isomorphism Theorem for rings, $R \cong \mathbb{Z}/\ker\varphi$

Since R int. domain, $\ker\varphi$ is a prime ideal.

$\therefore \exists p$ prime s.t. $\ker(\varphi) = (p) = p\mathbb{Z}$.

$R \cong \mathbb{Z}/p\mathbb{Z}$ integers mod p $\Rightarrow R \cong P_F$

Def. For a field F, $\operatorname{char} F = \begin{cases} 0 & \text{(case 1)} \\ p & \text{(case 2)} \end{cases}$ $\quad P_F \cong \mathbb{Q}$, $P_F \cong \mathbb{Z}/p\mathbb{Z}$

Alternative definition: $\operatorname{char} F = 0 \iff \forall n \geq 1,\ \underbrace{1_F + 1_F + \dots + 1_F}_{n \text{ times}} \neq 0$ (hwk)

otherwise, $\exists\, n \geq 1$ $\underbrace{1_F + 1_F + \dots}_{n \text{ times}} 1_F = 0$

$\operatorname{char} F = \min\{n \geq 1 \mid 1_F + \dots 1_F\} = 0_F$.

Claim $\operatorname{char} F \neq 0 \Rightarrow \operatorname{char} F$ is prime.

Proof. If $\operatorname{char} F = n \geq 1$ not prime, $\exists\, n_1, n_2$ s.t. $n = n_1 \cdot n_2$.

$0_F = \underbrace{1_F + \dots + 1_F}_{n \text{ times}} = (\underbrace{1_F + \dots 1_F}_{n_1 \text{ times}})(\underbrace{1 + \dots 1_F}_{n_2 \text{ times}}) \Rightarrow 0 = a \cdot b$

$\Rightarrow a = 0 \vee b = 0$

Contrary to minimality of n

Theorem If n is composite (and not power of prime), then there is no field with n elements. (e.g. no field with 6 elements)

Proof of theorem. Suppose F is a finite field. $\operatorname{char} F \neq 0$.

(pb) Let p be a prime s.t. $p = \operatorname{char} F$. Namely $P_F \cong \mathbb{Z}/p\mathbb{Z}$

Recall $P_F \leq F \Rightarrow F$ is a vector space over P_F.

$n = [F : P_F] \Rightarrow F \cong P_F^n$ as P_F vector space

$\therefore |F| = |P_F|^n = p^n$.

Theorem Suppose $F \leq K \leq E$ (fields), $[E:F] = [E:K] \cdot [K:F]$

Corr Suppose $F \leq E$ and $[E:F]$ is prime $\Rightarrow \underbrace{\nexists}_{\text{does not exist}}\ K \leq E$ and $K \geq F$

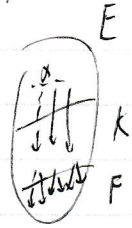
Historical Comments: Emmy Noether / E. Artin, B.L. Van der Waerden

Princeton ~1945 introduced methods of linear algebra to Galois theory

---

Proof. Suppose $n = [E:K]$, $m = [K:F]$

Let $\{\alpha_i \mid 1 \le i \le n\}$ be a basis of E/K, $\{\beta_j \mid 1 \le j \le m\}$ basis of K/F.



Enough to show $\exists B \subseteq E$ basis of E/F of card $n \cdot m$.

Claim Let $B := \{\alpha_i \beta_j \mid 1 \le i \le n, 1 \le j \le m\}$ is a basis of E/F.

Pf. (spanning) Given (arbitrary) $\alpha \in E$, as $\{\alpha_i\}$ is basis of E/K, $\exists \{a_i \mid 1 \le i \le n\} \subseteq K$ such that ① $\alpha = \sum_{i=1}^{n} a_i \alpha_i$. Since $\{\beta_j\}$ basis of K/F,

$\exists \{b_{j,i} \mid 1 \le j \le m\}$ s.t. ② $a_i = \sum_{j=1}^{m} b_{j,i} \beta_j$.

Substitute ② into ①: $\alpha = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} b_{j,i} \beta_j\right) \cdot \alpha_i = \sum_{i=1}^{n} \sum_{j=1}^{m} (\alpha_i \beta_j) b_{j,i} \in \mathrm{Span}_F(B)$

→ we further need to show B is linearly independent.

Enough to show if $\exists \{b_{i,j} \mid 1 \le i \le n, 1 \le j \le m\} \subseteq F$ s.t.

$$\sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij}\, \alpha_i \beta_j = 0 \Rightarrow \forall i, \forall j,\ b_{ij} = 0.$$

$LHS \overset{\text{dist}}{=} \sum_{i=1}^{n} \left(\sum_{j=1}^{m} b_{ij} \beta_j\right) \alpha_i = 0$. By lin. indep of $\{a_i\}$,

$\Rightarrow \forall i \le n,\ \sum_{j=1}^{m} b_{ij} \beta_j = 0$ " $\{b_j\}$,

$\Rightarrow \forall j \le m,\ \beta_j = 0$.

"Extension field" 1/18/2022

Question Given F, field, $p \in F[x]$, find $E \supseteq F$ such that $\exists \alpha \in E$, $p(\alpha)=0$?

Def. F is algebraically closed $\Leftrightarrow \forall p \in F[x], \exists \alpha \in F, p(\alpha)=0$.

The Fundamental Theorem of Algebra (Gauss ~1830) states that $\mathbb{C}$ (complex numbers) is alg. closed

) (algebraic closure) **Theorem $\forall F, \exists E \supseteq F$, E is algebraically closed. ($\forall p \in F[x], \exists \alpha \in E, p(\alpha)=0$)

Facts (1) Let R be commutative ring with 1. R is a field $\Leftrightarrow R$ has no non trivial ideals [$\equiv I$ ideal $\to I=\{0\} \vee I=R$]

(2) $\varphi: R_1 \to R_2$ ring homo, φ injective $\Leftrightarrow \ker\varphi = \{0_{R_1}\}$

(1)+(2)=(3) [Let F be a field, R ring with $1 \neq 0$. If $\varphi: F \to R$ ring homo then φ is injective.]

(counter-example when F is not field: GL_n, determinant)

Pf. Enough to show $\ker\varphi = \{0\}$, using (2).

$\ker\varphi = \{a \in F \mid \varphi(a) = 0_R\}$. Since F, R both have identity the ring homo φ satisfies $\varphi(1_F) = 1_R \neq 0_R$.

So $1 \notin \ker\varphi$, but $\ker\varphi$ is an ideal of F. Since $\ker\varphi \neq F$, $\ker\varphi = \{0\}$ (1)

Def. R is PID (Principal Ideal Domain) $\Leftrightarrow$ (a) R is integral domain

(b) $I \subseteq R$ ideal then $\exists a \in I$, $I = (a) = \{r \cdot a \mid r \in R\}$

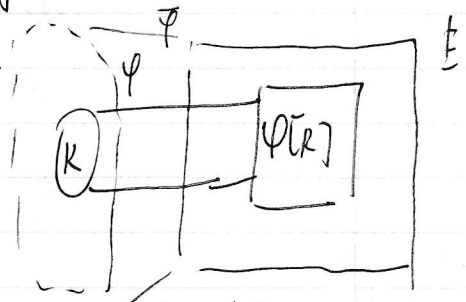
* {PID} $\subseteq$ {UFD}

Examples (1) $\mathbb{Z}$ is PID (2) For F field, $F[x]$ is a PID.

Pf of $F[x]$: $\forall a(x), b(x) \in F[x]$, $\exists q(x), r(x) \in F[x]$ s.t. $a(x) = q(x) \cdot b(x) + r(x)$ $0 \leq \deg r < \deg b$.

Fact $\forall p \in F[x]$, there exists $q \mid p$, $q \in F[x]$, q is irreducible $\overset{R \text{ PID}}{\iff}$ (q) is prime ideal $\overset{R \text{ PID}}{\iff}$ (q) maximal
(q prime)

Lemma Suppose R ring, F field, $\varphi: R \to F$ injective ring homo.
Then there exists a field F s.t. R subring of F and $\exists\, \bar{\varphi}: F \cong E$ s.t. $\bar{\varphi} \supseteq \varphi$



'we imagine' its elements
e.g. rational 'numbers'
To see how elements of R interact with the 'unstable' ones in R first

'seasons', 'glue it in'

e.g. Construction of $\mathbb{Q}$ from $\mathbb{Z}$.
Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$, $(a,b), (c,d) \in A$.
$(a,b) \sim (c,d) \iff ad = bc$ eq. rel. $(1,3) \sim (2,6) \sim (100, 300)$
$\mathbb{Q} := A/\sim = \{[(a,b)]_\sim \mid a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}\}$, idea: $[(a,b)] = a/b$
While $\mathbb{Z} \subsetneq \mathbb{Q}$, we identify $\mathbb{Z}$ with elements of $\mathbb{Q}$. $a \overset{\varphi}{\mapsto} [(a,1)]_\sim$,
'R' 'E'
$\varphi: \mathbb{Z} \to \mathbb{Q}$ ring homomorphism.

Construction of $\mathbb{R}$ from $\mathbb{Q}$ · Cauchy sequences (21-355)
Let $A = \{\{a_n\}_{n=1} \mid \{a_n\}$ is a Cauchy sequence$\}$
$\{a_n\} \sim \{b_n\} \iff \lim |a_n - b_n| = 0$
$\mathbb{R} := A/\sim$.

(Partial) Proof of Theorem**. Given F, $p \in F[x]$. let $q(x) \mid p$ be irreducible factor.
we find E for every p Consider $I := (q)$. By previous facts we know I prime $\Rightarrow$ I max $\Rightarrow$
$F[x]$ PID
$E := F[x]/I$ is a field.
F is field
Since $\varphi: F \to F[x]$ given by $\varphi(a) = a + 0x + 0x^2 + \ldots \in F[x]$
is an injective homomorphism, also $\bar{\varphi}(a) = a + I$ is homo from F to $E = F[x]/I$
Since domain of $\bar{\varphi}$ is F, $\bar{\varphi}$ is injective; ↑ polynomial

$\bar{\varphi}: F \to F[x] \to F[x]/I$

'case'

By the lemma, enough to show $\exists \alpha \in E$ root of $q(x)$.

Claim: $\alpha := x+I$ is a root of q.

Proof: Suppose $q = \sum_{k=0}^{n} a_k x^k$. What is $q(\alpha)$? (computed in $F[x]/I$)

↓ elements are of the form $\{r+I \mid r \in F[x]\}$

what $(a+I)\cdot(b+I) := a\cdot b + I$

$\Rightarrow I^k = (0+I)^k = I$.

$$q(\alpha) = \sum_{k=0}^{n} a_k \alpha^k := \sum_{k=0}^{n} a_k (x+I)^k = \sum_{k=0}^{n} a_k (x^k + I)$$

"syntactical"

$$= \sum_{k=0}^{n} a_k x^k + I^k$$

$$= q(x) + I \underset{q \in I}{=} I = 0_{F} \quad \square$$

To find all roots,
suppose we have α such that $p(\alpha) = 0 \Rightarrow (x-\alpha) \mid p$, $p_1 = \frac{p}{x-\alpha}$, repeat the algorithm.
However, at this point the roots can lie in different 'E's!! ($F[x] \to E[x] \to E'[x] \dots$)

Prop. Use division by remainder, let $q, r \in E[x]$ s.t.

$p = q(x-\alpha) + r(x)$ ($\deg r < \deg(x-\alpha) = 1 \Rightarrow r$ const.

Substitute α. $p(\alpha) = q(\alpha)(\alpha-\alpha) + r$

$0 = q(\alpha)\cdot 0 + r \Rightarrow r = 0$.

$\Rightarrow$ For $p \in E[x]$, $|\{\alpha \in E \mid p(\alpha) = 0\}| \le \deg p$. So this process occurs at most $\deg p$ times.
$\Rightarrow$ Take intersection of all subfields of E containing all the roots

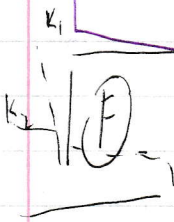
$\Rightarrow$ $E = F[x]/(q) \supset F$. Theorem: $[E:F] = \deg q$. (p17)

Def. Let $p \in F[x]$, $E \geq F$ is called a splitting field of p over F provided

(1) E contains all the roots of p [$\exists\, K \geq E$, if $\exists \alpha \in K, p(\alpha)=0 \Rightarrow \alpha \in E$]

$\Leftrightarrow \exists\, a \in E, \exists \underbrace{\alpha_1, \dots \alpha_k}_{\text{could repeat}} \in E$ s.t. $p(x) = a \prod_{i=1}^{k} (x-\alpha_i)$ 'p splits to linear factors'

(2) If $K \geq F$ s.t. K contains all the roots of p and $K \subseteq E$, then $K = E$. ('smallest')



← Digression → ...

Theorem (later) Take $p \in F[x]$. Suppose K_1, K_2 are both splitting fields of p/F

Then $\exists\, \varphi: K_1 \cong K_2$ s.t. $\forall a \in F,\ \varphi(a) = a$ i.e. $\varphi \wedge F = id_F$

Galois' idea: let $p \in F[x]$, E its splitting field.

Consider $G_p := Aut(E/F)$ ← Galois Group of p
(Group)

Theorem (very much later) p solvable by radicals $\Leftrightarrow \exists\, \{G_k \mid k < m\}, \{1\} \triangleleft \dots G_{k+1} \triangleleft G_k \triangleleft G_0 = G_p$ (normal subgroup)

s.t. G_k / G_{k+1} is cyclic of prime order.

Idea: If complicated, this does not exist ...

Fact $\forall p$ prime, $\forall n \in \mathbb{N}$, $\exists\, q \in \mathbb{F}_p[x]$ s.t. the splitting field of q has p^n many elements. ($\mathbb{Z}/p\mathbb{Z}$, $q = q(x)$)

Def. (recall) F is called algebraically closed provided $\forall p \in F[x], \exists\, a \in F, p(a)=0$.

Example. In $\mathbb{Q}$, no root for $x^2+2=0$. In $\mathbb{R}$, no root for $x^2+2=0$ $\Rightarrow$ Neither is algebraically closed.

Theorem (Gauss) $\mathbb{C}$ is algebraically closed.

$\forall$ fields F, there exists $E \geq F$ s.t. E is algebraically closed.

Remark. If E is algebraically closed then E is infinite. (finite $\Rightarrow (x-x_1)(x-x_2)\dots(x-x_n)+1=0$ has no solution!)

Question: Given $I \subsetneq F[x]$, find $J \subsetneq F[x]$ maximal such that $J \supsetneq I$.

This is good to approximate a proof of existence of algebraically closed extensions which "I contains all polynomials" from $F[\{x_p : p \in F[x]\}]$

I generated by $\{p : p \in F[x]\}$

because then $x_p + J$ is root of p in $R/J =: E$.

construction

$R[x_1 \dots x_n] = R[x_1 \dots x_{n-1}][x_n]$

Suppose I is index set. $R[\{x_i \mid i \in I\}] = \bigcup_{I_0 \subseteq_{\text{finite}} I} R[\{x_i \mid i \in I_0\}]$

Zorn's Lemma etc.

Def. Suppose $F \leq E$ fields, $\alpha \in E$. Denote by $F(\alpha)$ the smallest subfield of E containing $F \cup \{\alpha\}$.

Remark ① $F(\alpha) = \bigcap_{F \leq k \leq E,\ \alpha \in k} k$ ② $F(\alpha) = \{\frac{p(\alpha)}{q(\alpha)} \mid p, q \in F[x],\ q(\alpha) \neq 0\}$ $p(\alpha) = \alpha$, $q(\alpha) = 1$

$F(\alpha)$ is also a subfield in any other subfield because the evaluation is defined by algebraic operations!

Def. When $F \leq E$, $\alpha \in E$, $E = F(\alpha)$ we say that E is a simple extension of F.

Remark. ① $\mathbb{C} = \mathbb{R}(i)$ ② Consider $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

"$\{a+bi \mid a, b \in \mathbb{R}\}$"

③ The dimension of adding $\sqrt{2}$ to $\mathbb{Q}$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Basis is $\{1, \sqrt{2}\}$

④ $[\mathbb{C} : \mathbb{R}] = [\mathbb{R}(i) : \mathbb{R}] = 2$. Basis is $\{1, i\}$.

Theorem 2. Suppose $p \in F[x]$ irreducible, $E := F[x]/I$, $I = (p)$, $\alpha := x + (p)$. Then $\exists\ \varphi : F(\alpha) \cong F[x]/I$ such that $\varphi \wedge F = id_F$ ($\equiv \forall a \in F,\ \varphi(a) = a$). "evaluation at α"

Proof. Consider $\Psi : F[x] \to F(\alpha) \leq E$ given by $\Psi(a(x)) = a(\alpha)$, for all $a(x) \in F[x]$. Verify that Ψ is a ring homo. Since $p(\alpha) = 0$, $p(x) \in \ker \Psi$. Since $F[x]$ PID using and that $\forall a \in F$ (constants), $\Psi(a) = a$

Theorem 1. Let $p \in F[x]$ be irreducible, $d = \deg p$, $I = (p)$. Define $E := F[x]/I$.

Claim: $[E : F] = d$. Moreover $B := \{\alpha^k \mid k < d\} = \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a basis for E/F, where $\alpha = x + I$.

Proof: ① [symmetry] We show every element of E is a linear combination of elements from B.

Given $a(x) \in F[x]$, by division by p we set $q(x), r(x) \in F[x]$ such that $a(x) = q(x) \cdot p(x) + r(x)$ and $\deg r < \deg p\ (= d)$

let $b_0, b_1, \ldots, b_{d-1} \in F$ such that $r(x) = \sum_{k=0}^{d-1} b_k x^k$

Evaluate at $x = \alpha$: $a(\alpha) = q(\alpha) \cdot \underbrace{p(\alpha)}_{=0 \text{ in } E} + r(\alpha) = r(\alpha) = \sum_{k=0}^{d-1} b_k \alpha^k$

But $a(\alpha)$ is $a(x) + I$. $\forall \beta \in E$, $\exists\ r(x) \in F[x]$ of $\deg \leq d-1$. $\beta = \sum_{0}^{d-1} b_k \alpha^k \in \mathrm{Span}_F(B)$

$(a+I)(b+I) = ab + I$ etc.

$\forall \beta \in E$, $\exists a(x) \in F[x]$ s.t. $\beta = a(x) + I = a(\alpha) = \sum_{k=0}^{d-1} b_k \alpha^k$

(2) [Linear Independence] Given $\{b_k \mid k<d\} \subseteq F$ such that $\sum_{k=0}^{d-1} b_k \alpha^k = 0$,

we want to show $b_0 = b_1 = \cdots b_{d-1} = 0$.

If $\sum_{k=0}^{d-1} b_k \alpha^k = 0_E \Leftrightarrow \sum_{k=0}^{d-1} b_k x^k + I = I \ (=(p))$ (where $\alpha = x+I$)

$\therefore \sum_{k=0}^{d-1} b_k x^k \in I \Rightarrow p \mid \sum_{k=0}^{d-1} b_k x^k$

As p is irreducible of degree $d \Rightarrow \sum_{k=0}^{d-1} b_k x^k \equiv 0 \Rightarrow b_0 = b_1 = \cdots = b_{d-1} = 0$]

Proof of Th 2, continued.

$\psi: F[x] \to F(\alpha)$ the fact that p is irreducible we get $\ker\psi = (p)$ maximal. So $F[x]/\ker\psi$ is a field, $\ker\psi = I$. ((p) is I)

By the first isomorphism theorem, $F[x]/I$ is isomorphic to a subfield K of E containing F, i.e. ($\psi(F[x])$)

$\bar{\psi}: \frac{F[x]}{I} \overset{\text{(field iso)}}{\cong} K \leq E$, since $\psi \wedge F = id_F$. Furthermore $\alpha \in K$, since $\alpha = \bar{\psi}(x+I)$

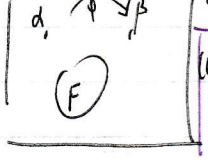
$F[x]$ $F(\alpha)$
$\varphi: R_1 \to R_2$ surj hom
$\Rightarrow R_2 \cong R_1/\ker\varphi$
$F(\alpha) \cong F[x]/I$

So $F(\alpha) \leq K$ by minimality, but $F(\alpha) \geq K$ by ⚠ (The book argues separately that $\bar{\psi}$ is injective - 'field homomorphism' and surjective - $\operatorname{Im}\bar{\psi} \leq F(\alpha)$ $\Rightarrow \operatorname{Im}\bar{\psi} = F(\alpha)$ take the inverse of α)

Corollary. $p \in F[x]$ irreducible, $I = (p)$, $\alpha = x+I \in F[x]/I$. $[F(\alpha):F] = \deg p = d$ and $F(\alpha) \cong F[x]/(p)$

Moreover, $F(\alpha) = \{\sum_{k=0}^{d-1} b_k \alpha^k \mid b_k \in F\}$.

Theorem 3 (Th 8.13.1)



Let $p \in F[x]$ irreducible. If $p(\alpha) = p(\beta)$, then $\exists \varphi: F(\alpha) \cong F(\beta)$ s.t. $\varphi \wedge F = id_F$, $\varphi(\alpha) = \beta$.

(extensions, automorphisms, splitting fields)

Idea: $F(\alpha) \cong F[x]/I \cong F(\beta)$. (the 'inverse' mapping would be α.)

We know (since p irreducible) that $\exists \varphi_1: F(\alpha) \cong F[x]/(p)$, $\varphi_1 \wedge F = id_F$, $\varphi_1(\alpha) = x+I$

Similarly $\exists \varphi_2: F[x]/(p) \cong F(\beta)$ s.t. $\varphi_2 \wedge F = id_F$, $\varphi_2(x + \underbrace{(p)}_{I}) = \beta$

Let $\varphi := \varphi_2 \circ \varphi_1$. $\varphi: F(\alpha) \cong F(\beta)$. $\varphi(\alpha) = \varphi_2(\varphi_1(\alpha)) = \varphi_2(x+I) = \beta$.

Then $\varphi \wedge F = id_F$.

note: from here on we assume E is given

2/4/2022

Def Suppose $F \leq E$. $\alpha \in E$ is called algebraic over F (1/) provided $\exists\, p \in F[x]$ s.t. $p \neq 0$ and $p(\alpha) = 0$.

If $\alpha \in E$ is not algebraic, we say α is transcendental (over F)

(When F is not mentioned, we mean the prime field)

e.g. $\alpha \in \mathbb{R}$ is algebraic $\Leftrightarrow \exists\, p \in \mathbb{Q}[x] \neq 0,\ p(\alpha) = 0$.

Facts (1) For $F \leq E$, $\alpha \in E$ is root of irred $p \in F[x]$ (will be unique monic), then $[F(\alpha) : F] = \deg p$ (Prop 9.11 version)

(2) $F(\alpha) \cong F[x]/(p)$, $\exists\, \varphi : F(\alpha) \cong F[x]/(p)$, $\varphi \wedge F = id_F$, and $\varphi(\alpha) = x + (p)$.

(3) If $\beta \in E$ s.t. $p(\beta) = 0$, then $\exists\, \varphi : F(\alpha) \cong F(\beta)$ s.t. $\varphi \wedge F = id_F$ and $\varphi(\alpha) = \beta$.

Let $F \leq E$, $\alpha \in E$. we say α is algebraic (over) $F \Leftrightarrow \exists\, p \in F[x] \neq 0$ s.t. $p(\alpha) = 0$.

Fact (Cantor ~1874) $|\mathbb{R}| > |\mathbb{Q}| = \aleph_0$. (prime field!)

$$\mathbb{Q}[x] = \bigcup_{n \in \mathbb{N}} \{p \in \mathbb{Q}[x] \mid \underbrace{\deg p = n}_{=: P_n}\}$$

what is $|P_n| = |\mathbb{Q} \times \cdots \times \mathbb{Q}| = |\mathbb{Q}|^n = \aleph_0^n = \aleph_0$.

Fact: $\aleph_0 \cdot \aleph_0 = \aleph_0$. (Define $S(x,y) = 2^x(2y+1) - 1$).

Now we use induction.

$Alg = \{a \in \mathbb{R} \mid a \text{ is alg over } \mathbb{Q}\}$, $(\aleph_0 =)\ |Alg| \leq \aleph_0 \cdot \aleph_0 = \aleph_0$. (each polynomial has finitely many solutions)

- countable -

using $|\mathbb{R}| > \aleph_0 \Rightarrow \exists\, a \in \mathbb{R}$ not alg.

Remark $\{a \in \mathbb{R} \mid a \notin Alg\}$ has cardinality $\mathbb{R}$.

Main Theorem: Suppose $F \leq E, \alpha \in E$. TFAE:

(1) α is algebraic/F

(2) $[F(\alpha):F] < \aleph_0$.

Pf (1)⇒(2) α a/g ⇒ $\exists p \in F[x]$ s.t. $p(\alpha)=0$.

Take $q \in F[x]$ irreducible, $q \mid p$ s.t. $q(\alpha)=0$.

By Fact (1), $[F(\alpha):F] = \deg q \leq \deg p < \aleph_0$.

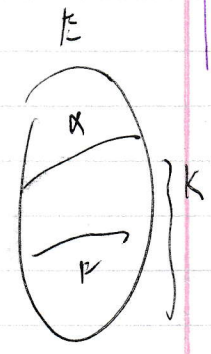
(2)⇒(1) Let $n := [F(\alpha):F]$. [⇒ $\forall \alpha_1, \dots \alpha_{n+1} \in F(\alpha)$, $\exists a_1, \dots a_{n+1} \in F$ not all zero s.t. $\sum a_n \alpha_n = 0$]

Consider $S = \{\alpha^k \mid 0 \leq k \leq n\}$, a set of $n+1$ many vectors. Since $[F(\alpha):F]=n$,

$\exists a_0 \dots a_n \in F$ not all zero s.t. $\sum_{k=0}^{n} a_k \alpha^k = 0$. Let $p(x) := \sum_{k=0}^{n} a_k x^k$, $p(\alpha)=0$.

Theorem (Transitivity of Alg Dependence)

Let $F \leq K \leq E$, $\alpha \in E$. If α is a/g over K and K is a/g/F [$\equiv \forall \beta \in K, \beta$ is algebraic over F] then α is a/g/F. [Use previous theorem.] [p22]



Skewes's conjecture

(Question: Given $F \leq E$, $\alpha, \beta \in E$. If α and β are a/g/F, is $\alpha \pm \beta$ a/g/F? (e.g. is $\sqrt{2}+\sqrt{3}$ a/g?)

Really, we know π, e are both transcendental. But we don't know if $\pi + e$ is algebraic... (probably not)

Theorem(*) Given $F \leq E$. If $K = \{\alpha \in E \mid \alpha$ is a/g/$F\}$, then K is a subfield of E.

Proof. Enough to show given α, β that are a/g/F, then $F(\alpha,\beta)$ is a/g/F.

$\alpha, \beta \in F(\alpha,\beta)$...

Lemma $F \subseteq E$, $\alpha, \beta \in E$. $F(\alpha,\beta) = F(\alpha)(\beta)$.
$(F(\alpha)(\beta) \subseteq F(\alpha,\beta))$

Proof. Clearly, $F(\alpha) \subseteq F(\alpha,\beta)$. As $\beta \in F(\alpha,\beta)$, $F(\alpha,\beta)$ has to contain everything created by β and $F(\alpha)$ otherwise $F(\alpha)(\beta)$ wouldn't be minimal.

$(F(\alpha,\beta) \subseteq F(\alpha)(\beta))$ Since $\alpha \in F(\alpha)$ and $\beta \in F(\alpha)(\beta)$, by minimality of $F(\alpha,\beta)$ we are done.

To show (*) using the main theorem, enough to show $\forall \gamma \in F(\alpha,\beta), [F(\gamma):F] < \aleph_0$.

Clearly, $[F(\gamma):F] \leq [F(\alpha,\beta):F]$ since $F(\gamma)$ is subspace of $F(\alpha,\beta)$.

Enough to show $[F(\alpha,\beta):F]$ finite.

$\Downarrow$ lemma

$[F(\alpha)(\beta):F] < \aleph_0$

Since α a/s/F, $n := [F(\alpha):F]$

β a/s/F, $k := [F(\beta):F] \Rightarrow [F(\alpha)(\beta):F(\alpha)] \leq k$.

→ Recall $F(\alpha) \cong F[x]/I = (p)$

→ Inherently have field - wise scalars as coefficients

→ If there is some irreducible (simpler) polynomial of degree k that is solved by β, then the same polynomial is solvable with coefficients over $F(\alpha)$

Recall the Product formula: $F \leq K \leq E \Rightarrow |E:F| = |E:K| \cdot |K:F|$.

$[F(\alpha)(\beta):F] = [F(\alpha,\beta):F(\alpha)] \cdot [F(\alpha):F] \leq k \cdot n \leq \aleph_0$.

$[K(\alpha):K] < \aleph_0$ doesn't help...

2/7/2022

[Prop 5]

Proof of (Transitivity of Alg Dependence) Let $F \subseteq K \subseteq E$, $\alpha \in E$. If α alg/K and $\forall \beta \in K$, β is alg/F. $\Rightarrow \alpha$ is alg/F.

By characterization in the 'main theorem', we have to show $[F(\alpha):F] < \aleph_0$.

By the assumption of α alg/K, $\exists\, b_0, \dots b_n \in K$ not all zero (e.g. dimension n) such that

$$\sum_{k=0}^{n} b_k \alpha^k = 0 \Rightarrow \alpha \text{ is alg/} F(b_0, \dots b_n) \Leftrightarrow [F(b_0, b_1, \dots b_n)(\alpha) : F(b_0 \dots b_n)] < \aleph_0 \quad (i \le n)$$

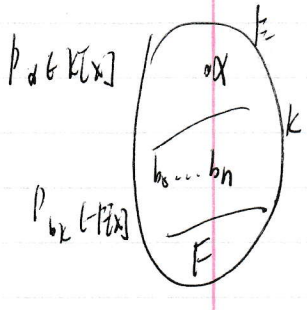
(subfield has smaller dimension)

By the product formula,

$$F(b_0, \dots b_n) = F(b_0 \dots b_{n-1})(b_n)$$

↓ by iteration over $F(\beta, \gamma) \sim F(\gamma)(\beta)$,

$[F(b_0, \dots b_k) : F] < \aleph_0$



By induction,

$$[F(b_0 \dots b_{k+1}) : F] = [F(b_0 \dots b_k)(b_{k+1}) : F(b_0 \dots b_k)] \cdot [F(b_0 \dots b_k) : F]$$

$$\Rightarrow [F(b_0 \dots b_n)(\alpha) : F] < \aleph_0$$

finite extensions are algebraic, so $\alpha, b_0, b_1, \dots$ are algebraic over F.

algebraic closure

⚠ Common mistakes: ① $F \subseteq K \subseteq E$, K alg/F $\not\Leftrightarrow$ $[K:F] < \aleph_0$

$[K(\alpha):F] = [K(\alpha):K]\,[K:F] < \infty$

$< \infty$

counter-example: $F \subseteq K \subseteq E$, K/F but $[K:F]$ is infinite. $\overline{\mathbb{Q}} : \{a \in \mathbb{C} : a \text{ is alg/} \mathbb{Q}\}$ is subfield of $\mathbb{C}$. $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$, $[\overline{\mathbb{Q}} : \mathbb{Q}] = \aleph_0$.

For every n, find irreducible polynomial of degree n. $\alpha \in E$ root of irreducible p, then $[F(\alpha):F] = \deg p$. So we can go $n \to \infty$.

② Find polynomial in E usually doesn't work!

e.g. $\sqrt{2}+\sqrt{3}$ is a root of a polynomial of at least degree 4!

21-374 2/7/2022

Def. $p \in F[x]$, $F \subseteq E$. E is a splitting field of p/F provided E contains all the roots of p and is minimal. $\iff \exists \alpha_1 \dots \alpha_n \in E$, $\exists a \in F$ s.t. $p = a\prod_{i=1}^{n}(x-\alpha_i)$.

$E = F(\alpha_1, \dots \alpha_n)$ "minimality"

($F \subseteq E$, $p \in F[x]$, $\alpha \in E$, $p(\alpha) = 0 \iff (x-\alpha) \mid p$)

(p14)

Theorem (Existence) $\forall F, \forall p$, there exists $E \supseteq F$ the splitting field of p/F.

Theorem (Uniqueness) If $p \in F[x]$, $E_1, E_2 \supseteq F$ both splitting fields of p/F, then $\exists \psi : E_1 \xrightarrow{\text{field}} E_2$ such that $\psi \upharpoonright F = id_F$ ($\equiv \forall a \in F, \psi(a) = a$) → used to construct

We prove a stronger version of uniqueness:

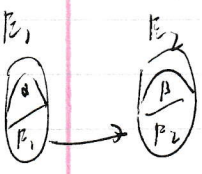
Suppose $F_\ell \subseteq E_\ell$, $\ell \in \{1,2\}$. $p \in F_1[x]$, $\psi : F_1 \cong F_2$.

If E_1 is a splitting field of p/F_1 and E_2 is a splitting field $\psi(p)/F_2$, then $\exists \varphi : E_1 \cong E_2$, $\varphi \supseteq \psi$

→ we can take $F_1 = F_2 = F$, $\psi = id_F$ to get original uniqueness statement.

We will use a generalization of (3) from a previous lecture: $\varphi : p(\alpha) \cong p(\beta)$

(Theorem 8) Suppose $F_\ell \subseteq E_\ell$ ($\ell = 1,2$), $p \in F_1[x]$ irreducible. $\psi : F_1 \cong F_2$. If $\alpha \in E_1$, $\beta \in E_2$ s.t. $p(\alpha) = 0$ and β root of $\psi(p)$ (specific root) then $\exists \varphi : F_1(\alpha) \cong F_2(\beta)$ s.t. $\varphi \supseteq \psi$ and $\varphi(\alpha) = \beta$



Proof Fix $\varphi_1 : F_1(\alpha) \cong \frac{F_1[x]}{(p)}$, ψ induces $\frac{F_1[x]}{(p)} \cong \frac{F_2[x]}{(\psi(p))}$ (more explanations on next page two)

$\varphi_2 : \frac{F_2[x]}{(\psi(p))} \cong F_2(\beta)$ $\Rightarrow \varphi = \varphi_2 \circ \psi \circ \varphi_1$

Lemma. (1) $\varphi : R_1 \cong R_2$, I ideal of R_1 $\iff \varphi[I]$ ideal of R_2. $\Rightarrow F_1[x]/I \cong \frac{F_2[x]}{\varphi^*(I)}$

(2) $\varphi : F_1 \cong F_2$, $p \in F_1[x]$ irred $\iff \psi(p) \in F_2[x]$ is irreducible

$\Downarrow \exists \psi^* : F_1[x] \cong F_2[x]$. $\psi^*(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} \psi(a_k) x^k \in F_2[x]$

④ $\varphi: F_1 \cong F_2$, $p \in F_1[x]$. p is irreducible $\Leftrightarrow$ $\bar{\varphi}(p)$ is irreducible.
$\bar{\varphi}: F_1[x] \cong F_2[x]$. ($\Leftarrow$) let $a(x), b(x) \in F_1[x]$ s.t. $p = a \cdot b$, a, b non-units.
$\bar{\varphi}(p) = \bar{\varphi}(a) \cdot \bar{\varphi}(b) \Rightarrow \bar{\varphi}(p)$ is not irreducible.

⑤ $\varphi: R_1 \cong R_2$, I ideal of R_1. $\exists\, \varphi_2: R_1/I \cong R_2/\varphi(I)$: $\varphi_2(a+I) := \varphi(a) + \varphi(I)$
$\varphi((a+I)\cdot(b+I)) = \varphi_2(ab+I) = (\varphi(a)\varphi(b) + \varphi(I)$
$= (\varphi(a)+\varphi(I)) \cdot (\varphi(b)+\varphi(I))$
$= (\varphi_2(a+I)) \cdot (\varphi_2(b+I))$
verify φ_2 is injective, etc.

Then $F_1 \cong F_2 \xrightarrow{①} F_1[x] \cong F_2[x] \xrightarrow{①+③} F_1[x]/(p) \cong F_2[x]/\varphi[p)] \cong F_2(\beta)$
$F_1(\alpha) \cong$; $\varphi[p)]$ maximal ideal by ①; field

$\varphi: R_1 \cong R_2$.
I is max $\Leftrightarrow$ $\varphi(I)$ is max. To prove ($\Leftarrow$), suppose $\varphi(I)$ is max ideal of R_2 but I not " of R_1.
In other words, $\exists\, J \subsetneq R_1$ ideal, $J \supsetneq I$.
$\varphi(J)$ is ideal of R_2. Since $J \subsetneq R_1$, $\varphi(J) \subsetneq R_2$. But $\varphi(J) \supsetneq R_2$, because
$\exists a \in J - I$, $\varphi(a) \in \varphi(J) - \varphi(I)$
($p \in R$ prime)
PID: prime $\Leftrightarrow$ irreducible (otherwise only $\Leftarrow$)

Cor. $\varphi: F_1 \cong F_2$, $p \in F_1[x]$ irred $\Rightarrow$ $\varphi(p)$ generates a prime ideal in $F_2[x]$
since $F_2[x]$ is PID $\Rightarrow$ $\varphi(p)$ maximal $F_2[x]$.

$\psi\left(\sum a_k x^k + (p)\right) = \sum \varphi(a_k) x^k + \bar{\varphi}(p))$

Idea. ① $\psi: F_1 \xrightarrow{\sim} F_2$ induces $\bar{\psi}: F_1[x] \xrightarrow{\sim} F_2[x]$. $\bar{\psi}(\sum a_k x^k) := \sum \psi(a_k) x^k$

② $p \in F_1[x] \Rightarrow \bar{\psi}(p) \in F_2[x]$

p irreducible $\Rightarrow \bar{\psi}(p)$ irreducible $\Rightarrow (p)$ prime ideal of $F_1[x]$ then $(\bar{\psi}(p))$ " $F_2[x]$

$p \equiv a(x) \cdot b(x) \Rightarrow \bar{\psi}(p) = \bar{\psi}(a) \cdot \bar{\psi}(b)$

③ $\varphi: R_1 \xrightarrow{\sim} R_2$ ring isomorphism, I ideal of R_1, then $\exists \bar{\varphi}: R_1/I \xrightarrow{\sim} R_2/\varphi(I)$ defined by $\bar{\varphi}(a+I) := \varphi(a) + \varphi(I)$

Lemma 8 ("Kronecker's lemma")

Take $p \in F[x]$ irred, $\alpha \in E_1$ root of p.

$\beta \in E_2$ root of $\bar{\psi}(p)$. Then

$F_1(\alpha) \cong F_1[x]/(p) \cong F_2[x]/(\bar{\psi}(p)) \cong F_2(\beta)$ $\quad \varphi \supseteq \psi \Leftrightarrow \forall a \in F_1, \varphi(a) = \psi(a)$

(Proof of Uniqueness of Splitting Fields) p23. $\psi: F_1 \xrightarrow{\sim} F_2$. If E_1 is splitting field of p/F_1, E_2 is splitting field of $\bar{\psi}(p)/F_2$, then $\exists \psi: E_1 \xrightarrow{\sim} E_2, \psi \supseteq \psi$

By induction on degree of p. $\deg p = 1$: p is $ax+b$, $a, b \in F_1$ then clearly all the roots of p are in F_1, so $E_1 = F_1$. Similarly $\bar{\psi}(p)$ has degree 1 so $E_2 = F_2$.

Now let $\deg p > 1$ and $E_1 \supsetneq F_1$. ($\exists \alpha \in E_1 - F_1$ root of p.)

p has an irreducible factor $q \in F_1[x]$ irred s.t. $q \mid p$, $q(\alpha) = 0$.

$\Rightarrow q(x) = (x-\alpha) \cdot r(x)$ for some $r \in F_1[x]$.

Suppose $p(x) = a(x) \cdot q(x)$ for some $a(x) \in F_1[x]$

As $\bar{\psi}(p) = \bar{\psi}(a(x))\, \bar{\psi}(q(x))$ and $q(x)$ is irreducible, also $\bar{\psi}(q(x))$ is irreducible.

As E_2 is splitting field of $\bar{\psi}(p)$, $\exists \beta \in E_2$ root of $\bar{\psi}(q(x))$.

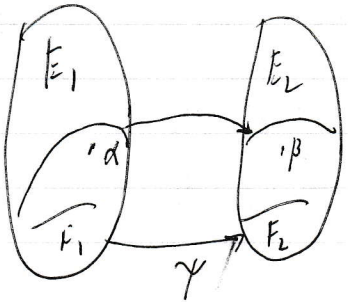
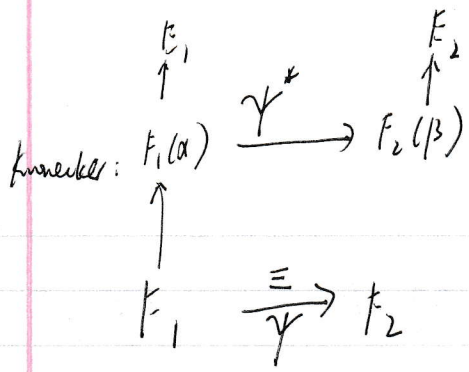


Illustration:

E_2 splitting field of $\bar{\psi}(p)/F_2$ $\Rightarrow$ E_2 contains all the roots of $\bar{\psi}(q)$

We will now proceed to find isomorphism between splitting fields of $q(x)$ and $\bar{\psi}(q(x))$. ~~The splitting fields of $q(x)$ and $p(x)$ are the same, for instance.~~



(previously p) irred in F_1

Let $b(x) \in F_1(\alpha)[x]$ such that $p(x) = (x-\alpha)\cdot b(x)$

$\deg b(x) = \deg p - 1 < \deg p$

Since $\psi^*: F_1(\alpha) \cong F_2(\beta)$, E_1 is a splitting field of $b(x)/F_1(\alpha)$ (by minimality)
$\psi^*(\alpha) = \beta$ $\quad$ E_2 $\quad$ $\psi^*(b)/F_2(\beta)$

$\psi^*(p) = (x-\beta)(\ \ )$

By the induction hypothesis, $\exists\ \varphi: E_1 \cong E_2$, $\varphi \supseteq \psi^*$, so $\varphi \supseteq \psi$ since $\psi^* \supseteq \psi$. $\deg p - 1$

Corollary. $p \in F[x]$, E_1 & E_2 two splitting fields of p/F $\Rightarrow \exists\ \varphi: E_1 \cong E_2$ $\varphi \wedge F = id_F$.

So we let E_p be the splitting field.

Define $G_p := \mathrm{Aut}(E_p/F) = \mathrm{Aut}_F(E_p) = \{ f \in \mathrm{Aut}(E_p) \mid f \wedge F = id_F \}$. captures a lot of information about p.

Theorem. $p \in F[x]$, E splitting field of p/F. Then

(a) $|\mathrm{Aut}(E/F)| \le [E:F]$.

(b) If p has no multiple roots, then $|\mathrm{Aut}(E/F)| = [E:F]$.

(α root of $p \Rightarrow (x-\alpha)^2 \nmid p$)

$\deg p = |\{\alpha \in E \mid p(\alpha) = 0\}|$

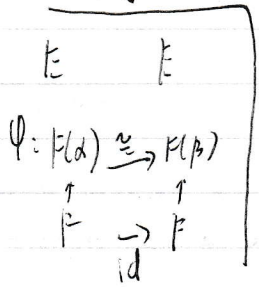
Corollary $p \in \mathbb{Q}[x]$ irreducible, E splitting field of $p/\mathbb{Q}$, then $|\mathrm{Aut}(E/\mathbb{Q})| = [E:\mathbb{Q}]$

does 'derivatives'

Theorem Suppose $p \in F[x]$ irred, E splitting field of p/F and $\alpha, \beta \in E$ s.t. $p(\alpha) = p(\beta) = 0$. Then $\exists\ \psi \in \mathrm{Aut}(E/F)$ s.t. $\psi(\alpha) = \beta$.

proof By Kronecker, there is some $\psi: F(\alpha) \cong F(\beta)$ s.t. $\psi(\alpha) = \beta$, $\psi \wedge F = id_F$.

Apply now the uniqueness of splitting fields: E a splitting field of $p/F_1(\alpha)$ but E is also $\varphi(p)/F_2(\beta)$ (= p)



$\Rightarrow \exists\ \boxed{\varphi^*: E \cong E}$ / $\Rightarrow \varphi^* \wedge F = id_F$, $\varphi^*(\alpha) = \beta$

$\varphi^* \supseteq \varphi$ since $\varphi^* \supseteq \varphi \supseteq id_F$.

Def. $F \leq E$, $\mathrm{Aut}(E/F) := \{\psi : E \xrightarrow{\sim} E \mid \forall c \in F\ \psi(c) = c\} \leq \mathrm{Aut}(E) \leq$ permutations of E (subgp w.r.t. $\circ$)

(ψ fixes F pointwise, i.e. $\psi|_F = \mathrm{id}_F$)

Key Lemma. Suppose $F \leq E$, $p \in F[x]$, $\alpha \in E$. If $p(\alpha) = 0$ then $p(\sigma(\alpha)) = 0$ for $\sigma \in \mathrm{Aut}(E/F)$

(midterm) Pf. Suppose $p = \sum_{k=0}^{n} a_k x^k$, $a_k \in F$. $p(\alpha) = 0 \Rightarrow \sigma(p(\alpha)) = \sigma(0) = 0$.

$$\sigma(p(\alpha)) = \sigma\left(\sum a_k \alpha^k\right) = \sum_0^n \sigma(a_k)\,\sigma(\alpha^k) = \sum \sigma(a_k)\cdot\sigma(\alpha)^k = \sum_0^n a_k [\sigma(\alpha)]^k = p(\sigma(\alpha))$$

($\sigma|_F = \mathrm{id}_F$, $\sigma(a_k) = a_k$)

Remark. (Group Action) Let $F \leq E$. The group $\mathrm{Aut}(E/F)$ acts on E by $\sigma \cdot a = \sigma(a)$ (σ acts on a)

G acts on S: $1_G \cdot x = x$ $\forall x \in S$

$a \cdot (b \cdot x) = (ab) \cdot x$ $\forall a, b \in G$, $\forall x \in S$

$G = \mathrm{Aut}(E/F)$, $S = E$

for $x \in S$, $\mathrm{orbit}(x) = \{a \cdot x \mid a \in G\}$

When $S = E$, x is root of $p \in F[x]$ ... all roots of p, $\sigma(\alpha)$ is root

Questions: ① Given $F \leq E$ fields, what is $\mathrm{Aut}(E/F)$?

② Given a group G, find $E \geq F$ s.t. $\mathrm{Aut}(E/F) \cong G$.

(Open! 'Absolute Galois Groups': For every finite group, there is $E \geq \mathbb{Q}$ s.t. $\mathrm{Aut}(E/\mathbb{Q}) \cong G$.)

We return to the theorems on p26. *$[E:F] \leq n!$ for a polynomial of degree n. (Rmk p26) (conjecture; remove 1 linear factor, induction...)

Def Suppose $F \leq E$. If $[E:F] < \aleph_0$ and $|\mathrm{Aut}(E/F)| = [E:F]$ then we say **E is Galois over F**.

Last time we have proved the uniqueness of splitting fields. $p \in F[x]$, E_1, E_2 splitting fields of p/E then $\exists \psi : E_1 \cong E_2$ $\psi|_F = \mathrm{id}_F$.

Here again, we prove a stronger result.

Aug 5, 14:1

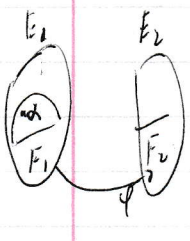
Theorem* Suppose $\varphi: F_1 \cong F_2$, $p \in F_1[x]$.

If E_1 splitting field of p/F_1, E_2 splitting field of $\varphi(p)/F_2$, then

$|\{\psi : E_1 \cong E_2 \mid \psi \supseteq \varphi\}| \leq [E_1 : F_1]$; the inequality becomes equality if p has no multiple roots.

Proof of Theorem* By induction on $[E_1 : F_1]$.

If the dimension $[E_1 : F_1] = 1$, then $E_1 = F_1$, furthermore $F_2 = F_2$. $\psi = \varphi$, necessarily done.



" > 1, let $\alpha \in E_1$ root of an irreducible $\xi \in F_1[x]$ s.t. $\xi \mid p$ and degree $\xi > 1$ (ξ: like $\alpha \in F_1$).

Recall that $\xi \in F_1[x]$ irred, $E_1 \supseteq F_1$, $\alpha \in E_1$ root of $\xi \Rightarrow [F_1(\alpha) : F_1] = \deg \xi$.

As $\varphi: F_1[x] \cong F_2[x]$, we have $\varphi(\xi) \mid \varphi(p)$, $\varphi(\xi)$ irreducible in $F_2[x]$.

Let $\beta \in E_2$ root of $\varphi(\xi)$. By Kronecker's lemma, $\exists\, \varphi^*: F_1(\alpha) \cong F_2(\beta) \supseteq \varphi$.

✓ elaboration

$\varphi^*(\alpha) = \beta$.

If $\psi: E_1 \cong E_2$, $\psi \supseteq \varphi$, $\xi \in F_1[x]$ irred, α root of ξ, $\alpha \in E_1$. Then $\psi(\alpha)$ is root of $\varphi(\xi)$.

$\psi: E_1 \xrightarrow{\cong} E_2$ let $\varphi^* := \psi \restriction F_1(\alpha)$, $\beta := \varphi^*(\alpha)$ is a root of $\varphi(\xi)$ — How many possible values of β? This depends on how many roots $\varphi(\xi)$ has, but $\deg \xi = [F(\alpha) : F]$

$\xi(\alpha) = 0$ $\quad \varphi^*: F_1(\alpha) \to F_2(\beta)$ $\quad$ So $\varphi^*: F_1(\alpha) \cong F_2(\beta)$, $\varphi^*(\alpha) = \beta$.

$\varphi: F_1 \to F_2$

$[F_1(\alpha) : F_1] = \deg \xi \geq \alpha$

$n = [E_1 : F_1] = [E_1 : F_1(\alpha)]\,[F_1(\alpha) : F_1] \Rightarrow [E_1 : F_1(\alpha)] < n$

≥ 2

$[E_2 : F_2(\beta)] < n$.

21374

2/16/2021

(cont) $[F_1(\alpha):F_1] = \deg(\xi) \geq 2$

$n := [E_1:F_1] = [E_1:F_1(\alpha)] \cdot [F_1(\alpha):F_1] \Rightarrow [E_1:F_1(\alpha)] < n$

Similarly, $[E_2:F_2] = [E_2:F_2(\beta)] \cdot [F_2(\beta):F_2] \Rightarrow [E_2:F_2(\beta)] < n$

As E_1 sp'g of $P/F_1(\alpha)$, E_2 splitting field of $\varphi^*(p) (= \varphi(p))/F_2(\beta)$

By induction hypothesis, $\exists \varphi^*: F_1(\alpha) \cong F_2(\beta)$, $\varphi^* \supseteq \varphi$, $\varphi^*(\alpha) = \beta$.

$|\{\psi: E_1 \cong E_2 \mid \psi \supseteq \varphi^*\}| \leq [E_1:F_1(\alpha)]$, with equality when all roots are distinct.

$[E_1:F_1] = [E_1:F_1(\alpha)] \cdot [F_1(\alpha):F] \geq |\{\psi \dots \psi \supseteq \varphi^*\}|$

$\cdot |\{\psi^* \supseteq \varphi\}|$

(1) What is $\mathrm{Aut}\,\mathbb{Q}$? $\mathrm{id}_{\mathbb{Q}} \in \mathrm{Aut}(\mathbb{Q})$

Suppose $\tau \in \mathrm{Aut}(\mathbb{Q})$, $\tau(1) = 1$, $\tau(0) = 0$. But $\tau(1+1) = 1+1 = 2$.

By induction in $n \in \mathbb{N}$, $\tau(n) = n$.

$n \in \mathbb{Z}$, $n < 0 \Rightarrow \tau(n) = \tau(\underbrace{1+\dots+1}_{n \text{ times}}) = -\tau(-n) = n$.

But for $\xi = n/m$,

$\tau(\xi) = \tau\left(\frac{n}{m}\right) = \frac{\tau(n)}{\tau(m)} = \frac{n}{m} = \xi$ ... so $\boxed{\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}}$

(2) $\mathbb{R} \subseteq \mathbb{C}$. What is $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ (AKA $\mathrm{Aut}_{\mathbb{R}}\mathbb{C}$)? $\mathrm{id}_{\mathbb{C}} \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$ certainly.

Fact: $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(-i)$

i is a root of x^2+1 $\Leftrightarrow$ $x^2+1 \in \mathbb{R}[x]$ is irreducible.

$\tau(i^2+1) = [\tau(i)]^2 + 1$

$\tau \in \mathrm{Aut}(\mathbb{C}/\mathbb{R}) \Rightarrow \tau(i)$ is also a root x^2+1.

$\Rightarrow \tau(i) \in \{i, -i\}$.

$(x+i)/(x-i)$

$\mathbb{C}$ is a splitting field of x^2+1 over $\mathbb{R}$!

$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, z \to \bar{z}\} \Rightarrow |\mathrm{Aut}(\mathbb{C}/\mathbb{R})| = 2 = [\mathbb{C}:\mathbb{R}]$

$z = a+ib$, $a,b \in \mathbb{R}$ $\Rightarrow \bar{z} = a-ib$

Conversely

Given G, find F s.t. $G = \mathrm{Aut}(F/\mathbb{Q})$?

(weakly $\leq$)

$\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \mathrm{Aut}(\mathbb{R})$, because

If $\sigma \in \mathrm{Aut}(\mathbb{R}) \Rightarrow \sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ ($\mathbb{Q}$ is prime subfield)

~~$\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{Id}\}$~~ Exercise ($= \mathrm{Aut}(\mathbb{Q})$)

$\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ is huge! Axiom of choice etc.

$= \mathrm{Aut}(\mathbb{C})$

Idea: $F \subseteq K \subseteq E$. Question what can be said of $\mathrm{Aut}(E/F)$ vs $\mathrm{Aut}(E/K)$?

Remark: $\mathrm{Aut}(E/K) \leq \mathrm{Aut}(E/F)$ clearly by set inclusion.

Suppose $H \leq \mathrm{Aut}(E)$. Is there $F \subseteq E$ s.t. $H = \mathrm{Aut}(E/F)$?

Def. Given E, $H \leq \mathrm{Aut}(E)$, let

$E^H = \{a \in E \mid (\forall \sigma \in H)\ \sigma(a) = a\}$ be the fixed field of H.

Theorem. E, H as above $\Rightarrow E^H \subseteq E$.

E^σ

Lemma. Suppose E field, $\sigma : E \to E$ field homomorphism. Then $\{a \in E \mid \sigma(a) = a\}$ is a subfield of E.

Proof. Clearly $0, 1 \in 0^\sigma$, $\sigma(0) = 0$ and $\sigma(1) = 1$ necessarily

$x, y \in E^\sigma \Rightarrow$ show $x - y \in E^\sigma$: $\sigma(x-y) = \sigma(x) - \sigma(y) = x - y$

(σ hom of $(E,+)$)

$x, y \in E^\sigma$, $y \neq 0 \Rightarrow \sigma(x/y) = \sigma(x \cdot y^{-1}) = \sigma(x) \cdot \sigma(y)^{-1} = x \cdot y^{-1}$.

Proof of Theorem. $E^H = \bigcap_{\sigma \in H} E^\sigma \leq E$ (lemma)

21374 2/16/2012

Question. Given F finite, what is $\mathrm{Aut}(F)$?

Fact. If F finite field, then $\exists$ p prime, F has $\mathbb{L} \subseteq F$ prime with p many elements

$\mathbb{L} \cong \mathbb{Z}/p\mathbb{Z}$. So $\exists\, n = [F:\mathbb{L}]$

Theorem If $|F| = p^n$ (p is prime), then $\mathrm{Aut}(F)$ is cyclic of order n.

find generator... (see Frobenius mapping $x \mapsto x^p$ later)

2/18/2012

Theorem (Prop 9) Given $F \subseteq E$, if $\alpha \in E$ is algebraic/F then there exists a monic polynomial $m_\alpha \in F[x]$ irreducible s.t. $m_\alpha(\alpha) = 0$. Furthermore

(1) m_α as above is unique, and

(2) for every $p \in F[x] \neq 0$, $p(\alpha) = 0 \Rightarrow m_\alpha \mid p$

Cor. $F \subseteq E$, if $\alpha \in E$ alg/F then $F(\alpha) \cong F[x]/(m_\alpha)$

Pf: Consider $S = \{n \geq 1 : \exists\, q \in F[x] \neq 0,\ q(\alpha) = 0,\ n = \deg q\}$

Since α alg, $S \neq \emptyset$. Let $d = \min S$, and take $q_0 \in F[x]$ s.t. $\deg(q_0) = d$ and $q_0(\alpha) = 0$.

$q_0 = \sum_{k=0}^{d} a_k x^k$ for some $a_k \in F$. Let $m_\alpha := \frac{1}{a_d} \cdot q_0 \in F[x]$. Then m_α is monic and $m_\alpha(\alpha) = 0$.

Claim: $m(\alpha)$ is irreducible. Otherwise, $\exists\, a(x), b(x) \in F[x]$, $\deg(a), \deg(b) \geq 1$ s.t.

$m_\alpha = a \cdot b$. $0 = m_\alpha(\alpha) = a(\alpha) \cdot b(\alpha) \Rightarrow$ (no zero divisors in field) $a(\alpha) = 0 \vee b(\alpha) = 0$ contradiction!

(2) Given $p \in F[x] \neq 0$, s.t. $p(\alpha) = 0$. Let $q(x) \in F[x]$, $r(x) \in F[x]$ s.t.

Euclidean domain. $a = bq + r$, $f(r) < f(b)$
$f(a) \leq f(ab)$ for nonzero a, b
f: 'degree' function

$p(x) = q(x) \cdot m_\alpha(x) + r(x)$, and $\deg r < \deg m_\alpha$.

$p(\alpha) = q(\alpha) \cdot m_\alpha(\alpha) + r(\alpha)$

$0 = q(\alpha) \cdot 0 + r(\alpha) \Rightarrow \alpha$ is a root of $r(\alpha)$.

Since $\deg r < n$, By minimality of n above, we conclude $r = 0$. So $m_\alpha \mid p$.

(2) $\Rightarrow$ (1) any other that has root α is 'larger' than m_α. $\cong$ minimal factor for any integer $\to$ Euclid!

Theorem (Binomial). Let R be commutative with 1. $\forall a,b \in R, \forall n \in \mathbb{N}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}$

(freshman's dream)

Corollary. Suppose F field has $\text{char } F = p$ (prime). Then $\forall a,b \in F$, $(a+b)^p = a^p + b^p$.

Pf. By the binomial theorem, $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$

Since p is prime. $p \mid \binom{p}{k}$ $\forall\ 0 < k < p$

(Since $\text{char } F = p$, $a + \dots + a = a(1 + \dots + 1)$ (n times) $= a \cdot 0 = (1 + \dots + 1) = 0$.)

($p \cdot n$ times; p times)

Def. Let p be prime. The Frobenius mapping χ_p is defined by

$$\chi_p(a) := a^p.$$

('Frobenius automorphism')

Main lemma. Suppose F is a finite field of $\text{char } p$. Then $\chi_p \in \text{Aut}(F)$. Otherwise χ_p is injective homo if F is not finite.

Pf. 1) χ_p homo 2) χ_p bijective

1) Given $a,b \in F$, $\chi_p(a \cdot b) = (ab)^p \overset{\text{commutativity}}{=} a^p \cdot b^p = \chi_p(a) \cdot \chi_p(b)$.

2) $\chi_p(a+b) = (a+b)^p = a^p + b^p = \chi_p(a) + \chi_p(b)$

(freshman's dream)

2) Injective. Enough to show $\ker(\chi_p) \neq \{0\}$. Clearly $\chi_p(1) = 1^p = 1 \neq 0$, so $\ker(\chi_p) \subsetneq F$

But $\ker(\chi_p)$ being an ideal, F field, implies $\ker(\chi_p) = 0$.

Surjective. Use the pigeonhole principle, since $|F| < \infty$, χ_p injective $\Rightarrow$ χ_p surjective as well.

Theorem (Late) If F is finite, $p = \text{char } F$, $|F| = p^n$ for some n. Then $\text{Aut}(F) = \{\chi_p{}^k \mid 0 \le k < n\}$.

Remark (Main lemma) $|F| < \infty$, $\text{char } F = p$ then $\{\chi_p{}^k \mid k \in \mathbb{Z}\} \subseteq \text{Aut}(F)$, clearly. χ_p^{-1} = inverse of χ_p etc.

It is far more non-trivial to show that there are no other automorphisms.

idea: splitting field of polynomials

$|\text{Aut}(\text{spl})| = |\text{Aut}(\text{base field})|$

21-374 2/18/2022

The idea is to use $|\mathrm{Aut}(E/F)| = [E:F]$ when E is splitting field of p/F without multiple roots. But how to check for multiple roots?

Next time we will find a necessary and sufficient algebraic condition on $p \in F[x]$ equivalent to p having no multiple roots $\Leftrightarrow \gcd(p,p') = 1$

Def. Given $\sum_{k=0}^{n} a_k x^k \in F[x]$, $p' := \sum_{k=1}^{n} \underbrace{k \cdot a_k}_{\text{add } k \text{ times}} x^{k-1}$ 'formal derivative'

Lemma $p, q \in F[x]$. (a) $(p+q)' = p' + q'$

(b) $(p \cdot q)' = p \cdot q' + p' \cdot q$ ('Leibniz')

2/21/2022

Def. Take polynomial $p \in F[x]$, E splitting field of p/F. $\alpha \in E$ is a multiple root of p provided $(x-\alpha)^2 \mid p$ (in $E[x]$) [$\Leftrightarrow$ there exists $h(x) \in E[x]$ such that $p = (x-\alpha)^2 h(x)$]

Question. Given $p \in F[x]$, does p have multiple roots?

Theorem. For any $p \in F[x]$, p has no multiple roots if and only if $\gcd(p,p') = 1$ in $F[x]$.

(↑ valid in Euclidean ring)

Proof. ($\Leftarrow$) Suppose $E \supseteq F$, $\alpha \in E$ multiple root of $p \Rightarrow \exists\, g(x) \in E[x]$, $p = (x-\alpha)^2 g(x)$.

Then gives $p' = 2(x-\alpha)\cdot g(x) + (x-\alpha)^2 g'(x)$. By substitution of $\alpha = x$,

$p'(\alpha) = 0 \Rightarrow m_\alpha \mid p'$, but also $m_\alpha \mid p$. So $m_\alpha \mid \gcd(p,p') \Rightarrow \gcd(p,p') \neq 1$.

(Fact: Let $E \supseteq F$, $p \in F[x]$, $\alpha \in E$, $p(\alpha) = 0$. Then $\exists\, m_\alpha \in F[x]$ monic, irreducible such that $m_\alpha(\alpha) = 0$ and $\forall\, q \in F[x]$, $q(\alpha) = 0 \Rightarrow m_\alpha \mid q$)

($\Rightarrow$) Suppose $\gcd(p,p') \neq 1$. Then $\exists\, q \in F[x]$, $q \mid p$ and $q \mid p'$.

Let $\alpha \in E$ be a root of q, $q(\alpha) = 0 \Rightarrow (x-\alpha) \mid q(x)$

$q \mid p \Rightarrow \exists\, h(x) \in F[x]$, $p = (x-\alpha)\,h(x)$

$g(\alpha)=0$ by assumption

$f = gh \Rightarrow f'(\alpha) = h(\alpha) + (x-\alpha)\cdot h'(\alpha)$

($f'(\alpha)=0$, $(x-\alpha)\cdot h'(\alpha)=0$)

$\Rightarrow g'(\alpha)=0$ or $h(\alpha)=0$. If $h(\alpha)=0$, then $(x-\alpha)^2 \mid f$.

Example. Suppose F has characteristic p prime, $n\geq 1$. The polynomial $x^{p^n}-x$ has no multiple roots over $\mathbb{F}_p$.

Define $g(x) := x^{p^n}-x$. We have to show $(g, g')=1$. Evaluate the derivative of g:

$g' = p^n \cdot x^{(p^n-1)} - 1$. Since $\operatorname{char} F = p$, $g' = 0 - 1 = -1$.

Theorem. Denote $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The splitting field of $g/\mathbb{F}_p$ has p^n many elements.

(Fact: Let $F \leq E$, $\sigma \in \operatorname{Aut}(E/F)$, $K = \{a \in E \mid \sigma(a) = a\} \leq E$.)

Proof of theorem. Let E be a splitting field of $g/\mathbb{F}_p$. Consider $K = \{a \in E \mid \chi_p^n(a) = a\} \leq E$.

$= \{a \in E \mid (\chi_p)^n = a^{p^n} = a\}$

$= \{a \in E \mid a \text{ root of } g(x)\}$.

Since $g(x)$ has no multiple roots, $|K| = p^n$ (degree of g). But E is the splitting field of $g/\mathbb{F}_p$, so (cannot be larger)

$\Rightarrow K = E \Rightarrow |E| = p^n$.

Corollary. $\forall p$ prime, $\forall n \geq 1$, $\exists$ field E such that $|E| = p^n$.

Proof. Take $g \in \mathbb{F}_p[x]$, g given by $x^{p^n}-x$. Let E be its splitting field. By previous theorem, $|E| = p^n$.

Theorem. Let p be prime, $n \geq 1$. If E_1, E_2 are both fields such that $|E_1| = |E_2| = p^n$ then $E_1 \cong E_2$.

Proof. By uniqueness of splitting fields, it is enough to show that any E s.t. $|E| = p^n$ is splitting field of $g/\mathbb{F}_p$.

But we just take $K = \{a \in E \mid \chi_p^n(a) = a\} \leq E$. $\rightarrow$ or an isomorphic copy

Since $g(x)$ has no multiple roots, $|K| = p^n$. So $K = E_i$ are splitting fields.

E contains the n roots of g and nothing else.

2/23/2022

To summarize our discussion thus far, we have shown the existence and uniqueness of splitting fields: $\forall p$ prime, $\forall n \geq 1$ $\exists F \supseteq \mathbb{F}_p$ of cardinality p^n. Furthermore, if $|E| = p^n$, then $F \cong E$.

So we can write $\mathbb{F}_{p^n}$ for the splitting field of $g(x) := x^{p^n} - x$

Question: What is $\mathrm{Aut}(\mathbb{F}_{p^n})$?

Fact $\chi_p \in \mathrm{Aut}(\mathbb{F}_{p^n}) \Rightarrow \{\chi_p^k \mid k \in \mathbb{Z}\} \leq \mathrm{Aut}(\mathbb{F}_{p^n})$

As $\mathrm{Aut}(\mathbb{F}_{p^n})$ is finite, there are many $k_1 \neq k_2 \in \mathbb{Z}$ s.t. $\chi_p^{k_1} = \chi_p^{k_2}$.

(subset of permutations)

Theorem. $\mathrm{Aut}(\mathbb{F}_{p^n}) = \{\chi_p^k \mid k < n\}$ $(\leq)$

Remark. $\chi_p^k \circ \chi_p^l = \chi_p^{k+l} \Rightarrow \mathrm{Aut}(\mathbb{F}_{p^n})$ is cyclic of order of n, and generated by χ_p.

(composition $\circ$ exponentiation)

Recall: $p \in F[x]$, E sp field of p/F, then $\mathrm{Aut}(E/F) \leq [E:F]$. If in addition we assume that p has no multiple roots, then $|\mathrm{Aut}(E/F)| = [E:F]$.

We also know that $\{\chi_p^k \mid k < n\} \leq \mathrm{Aut}(\mathbb{F}_{p^n})$

So we need to show

(A) $0 \leq k_1 \neq k_2 < n \Rightarrow \chi_p^{k_1} \neq \chi_p^{k_2}$, and

(B) $|\mathrm{Aut}(\mathbb{F}_{p^n})| = n$.

To show (B), use $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, $\mathbb{F}_{p^n}$ splitting field of $g(x) = x^{p^n} - x$, and that g has no multiple roots. So $|\mathrm{Aut}(\mathbb{F}_{p^n})| = |\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Suppose E is a field, and $\mathbb{P}$ is its prime field. Then $\mathrm{Aut}(E) = \mathrm{Aut}(E/\mathbb{P})$. Any automorphism must fix the prime field.

(A) Proof by contradiction: Suppose there exist $k_1 < k_2 < n$ s.t. $\chi_p^{k_1} = \chi_p^{k_2}$. These are functions!

Then $\forall a \in \mathbb{F}_{p^n}$, $\chi_p^{k_1}(a) = \chi_p^{k_2}(a)$. Apply $\chi_p^{-k_1}$ to both sides, then

$\forall a \in \mathbb{F}_{p^n}$ $\chi_p^{k_1-k_1}(a) = \chi_p^{k_2-k_1}(a)$

$\forall a \in \mathbb{F}_{p^n}$ $a = \chi_p^{k_2-k_1}(a) = a^{(p^{k_2-k_1})}$ (by def of χ_p)

Define $g(x) = x^{p^{k_2-k_1}} - x \in \mathbb{F}_p[x]$

$\forall a \in \mathbb{F}_{p^n}$, $g(a) = 0$. But $\deg g < p^{k_2} \leq_{k_2<n} p^n$, so we can't have that many (p^n) solutions!

Def. $p \in F[x]$ is separable provided p has no multiple roots in some alg closure of $F[x]$

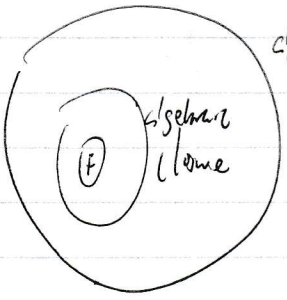
We will prove the existence and uniqueness of algebraic closures (algebraically closed + 'not too big' (all elements algebraic over F)

If E_1, E_2 both algebraic closures of F, then $\exists\, \psi: E_1 \cong E_2$, $\psi \upharpoonright F = id_F$.

E.g. $\mathbb{C} \supset \mathbb{R}$. So what is $\overline{\mathbb{F}}_p$?

$\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$!

13.4, Prop 29.



[The textbook replaces 'algebraically closed' with 'splits completely over $\overline{F}$'. We show this is equivalent to our definition above.]

Take a root of some $f(x)$ in $\overline{F}[x]$.

$F \leq \overline{F} \leq \overline{F}(\alpha)$.

$\alpha \in \overline{F}(\alpha)$, α alg over $\overline{F}$,

$\overline{F}$ alg over $F \Rightarrow \alpha$ alg over F

$\Rightarrow \alpha \in \overline{F}$.

Thus $\overline{F}[x]$ is algebraically closed.

21-374 2/25/2022

$(P, \leq)$

POSET: preorder: Reflexivity + Transitivity + Anti-symmetry

LINEAR ORDER: POSET + $\forall x \in P, y \in P,\ x \leq y$ or $y \leq x$

$(P, \leq)$

Def. Let $(P, \leq) \in$ POSET. $m \in P$ is called maximal provided $\neg \exists a \in P\ (a \geq m \wedge a \neq m)$

Examples (a) $S := \{a \in \mathbb{R} \mid a \leq 1\}$ has maximal element $m = 1$.

(b) $P := \mathcal{P}(\{1,2,3\}) - \{1,2,3\} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}\}$

has several maximal elements $\{1,2\}, \{2,3\}, \{1,3\}$

(c) $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ have no maximal elements.

Question Let $(P, \leq)$ be POSET. What is a sufficient condition for there to exist $m \in P$ maximal?

→ If P is finite, can prove by induction

→ Infinite case?

Def. Let $(P, \leq)$ be a POSET. $C \subseteq P$ is a chain provided $(C, \leq)$ is linearly ordered

$(\forall x, y \in C,\ x \leq y$ or $y \leq x)$

A poset $(P, \leq)$ is linearly ordered $\Leftrightarrow P$ is a chain.

E.g. $\{\emptyset, \{1\}, \{1,2\}, \{1,2,3\}\}$

ZORN'S LEMMA: Let $(P, \leq)$ be a POSET. If for every chain $C \subseteq P$, $\exists\ b \in P$ upper bound of C, then $\exists\ m \in P$ maximal.

AC $\leftrightarrow$ WO ($\leftrightarrow$ Induction)

Kuratowski AC $\leftrightarrow$ ZL en Français

Max Zorn (1936) Paper showing applications of ZL to algebra

Theorem. Let R be a commutative ring with 1. If $I \subsetneq R$ ideal then there exists a maximal ideal $J \subsetneq R$ s.t. $J \supseteq I$.

Fact $R = F[x]$, $I \subsetneq F[x]$ is max $\Leftrightarrow \exists p \in F[x]$ irreducible, $I = (p)$

if $1 \in J$ the ideal is not proper

Proof of theorem: Consider $\mathcal{P} = \{J \subseteq R \mid 1 \notin J, J \text{ ideal}, J \supseteq I\}$

Let $(\mathcal{P}, \subseteq)$ be our POSET.

Observe $J^* \in \mathcal{P}$ maximal (with respect to $\subseteq$) $\Rightarrow J^*$ is a maximal ideal of R.

It is enough to show that $\mathcal{P}$ has a maximal element.

Using Zorn's Lemma, we just have to show if $\mathcal{C} \subseteq \mathcal{P}$ is a chain, then $\exists b \in \mathcal{P}$ upper bound of $\mathcal{C}$.

Claim $\forall \mathcal{C} \subseteq \mathcal{P}$, if $\mathcal{C}$ is a chain then $\exists b \in \mathcal{P}$ upper bound.

Pf. Let $B := \bigcup \mathcal{C}$. Clearly B does not contain 1, and $b \supseteq I$.

We have to show that B is a ring (obvious) and that it is an ideal.

- Additive subgroup: $x+y \in B$ if $x, y \in B$

  find min index such that $x, y \in C_k$.

- Closure under left multiplication $r, a \in B \Rightarrow r \cdot a \in B$

21-374 Midterm 1 Review 2/28/2022

Let F be a field. Then there exists $P \leq F$ prime field the subfield generated by 1.

Theorem. ① $P \cong \mathbb{F}_p$ $(= \mathbb{Z}/p\mathbb{Z})$ $\operatorname{char} F = p$
② $P \cong \mathbb{Q}$ $\operatorname{char} F = 0$

These are the only two cases.

Consider $\mathbb{Z} \xrightarrow{\varphi} F$ given by $\varphi(1+\dots+1) = 1_F + \dots + 1_F$

φ is a homomorphism. $\mathbb{Z}/\ker\varphi \leq F$.

Fact. $F \leq E \Rightarrow$ E is F-vector space, $[E:F] = \dim_F E$. (F: coefficients; size of basis; (in other contexts, degree of some polynomial) $|\operatorname{Aut}(E/F)|$ etc.)

Corollary. $|F| < \aleph_0$ field $\Rightarrow \exists$ p prime, $\exists$ $n \geq 1$, $|F| = p^n$.

As F is a vector space over $\mathbb{F}_p$, $F \cong \mathbb{F}_p \times \dots \times \mathbb{F}_p$ (as vector spaces).

Theorem. $|F| = p^n \Rightarrow F$ is the splitting field of $g \in \mathbb{F}_p[x]$, where $g(x) = x^{p^n} - x$.

Dimension Multiplication Formula. Let $F \leq K \leq E$. Then $[E:F] = [E:K]\cdot[K:F]$.

Proof sketch. $\{\alpha_i \mid i \leq n\}$ K-basis of E; $\{\beta_j \mid j \leq m\}$ F-basis of K $\Big\}$ $\{\alpha_i\beta_j \mid i \leq n, j \leq m\}$ is F-basis of E/F.

Let $F \leq E$. $\alpha \in E$ alg/F $\Leftrightarrow \exists$ $p \in F[x] \neq 0$ such that $p(\alpha) = 0$.

Theorem. α alg $F \Leftrightarrow [F(\alpha):F] < \aleph_0$.

$F(\alpha)$ is the smallest subfield of E containing $F \cup \{\alpha\} = \left\{\frac{p(\alpha)}{q(\alpha)} \mid p, q \in F[x], q(\alpha) \neq 0\right\}$
"simple extension of F by α".

*Theorem. Given $f \in F[x]$. There exists $E \geq F$ such that $\exists \alpha \in E$, $p(\alpha) = 0$. Furthermore,
(1) $E \cong F[x]/(m_\alpha)$, where $m_\alpha \in F[x]$ is irreducible and monic, $m_\alpha(\alpha) = 0$.
(2) m_α as above is unique.
(3) If $g \in F[x]$ s.t. $g(\alpha) = 0$, then $m_\alpha \mid g$.
(4) $F(\alpha) \cong F[x]/(m_\alpha)$ (PID)

$\overline{\varphi}: F_1[x] \cong F_2[x]$, $\overline{\varphi}(\sum a_k x^k) := \sum \varphi(a_k) x^k$ (extend to)

Kronecker Lemma (Theorem 8). Given $F_\ell \le E_\ell$, $\ell \in \{1,2\}$, $\varphi: F_1 \cong F_2$, $p \in F_1[x]$ irred.
If $\alpha \in E_1$ is a root of p, $\beta \in E_2$ is a root of $\varphi(p)$, then $\exists\, \varphi^*: F_1(\alpha) \cong F_2(\beta)$, $\varphi^* \supseteq \varphi$, $\varphi^*(\alpha) = \beta$.

Idea: $F_1(\alpha) \cong \frac{F_1[x]}{(p)} \cong \frac{F_2[x]}{(\varphi(p))} \cong F(\beta)$

$\alpha \mapsto x + (p) \mapsto x + (\varphi(p)) \mapsto \beta$.

Uniqueness of splitting fields. Given $F_\ell \le E_\ell$, $\ell = 1,2$, $\varphi: F_1 \cong F_2$. Let $f \in F_1[x]$. E_1 splitting field of f/F_1, E_2 spfield of $\varphi(f)/F_2$ then $\exists\, \varphi^*: E_1 \cong E_2$, $\varphi^* \supseteq \varphi$.

Interesting case: $\exists\, p \in F_1[x]$ irred, $\deg p > 1$, $p \mid f$. Pick $\alpha \in E_1$ root of p.
$\beta \in E_2$ " $\varphi(p)$.

$$\begin{array}{ccc} E_1 & & E_2 \\ \uparrow & & \uparrow \\ F_1(\alpha) & \xrightarrow{\psi} & F_2(\beta) \\ \uparrow & & \uparrow \\ F_1 & \xrightarrow{\varphi} & F_2 \end{array}$$

By Kronecker, $\exists \psi: F_1(\alpha) \cong F_2(\beta)$, $\psi \supseteq \varphi$, $\psi(\alpha) = \beta$.

E_1 sp field of $f/(x-\alpha) =: f_1$

E_2 " $\psi(f)/x-\beta = \psi(f_1)$.

As $\deg(f_1) < \deg f$, we can use the induction hypothesis (to show) that $\exists \varphi^*: E_1 \cong E_2$, $\varphi^* \supseteq \psi$.

Def. $p \in F[x]$. A minimum field $E \supseteq F$ and containing all the roots of p is called a splitting field.

By iteration, a splitting field always exists.

Automorphisms: ...

$\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$, $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$. $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \mathrm{conj}\}$ ($z \mapsto \bar{z}$)

Remark $|\mathrm{Aut}(\mathbb{C})| = 2^{(2^{\aleph_0})}$.

Key Facts. $\sigma \in \mathrm{Aut}(E) \Rightarrow K = \{a \in E \mid \sigma(a) = a\} \le E$.

"Freshmen's Dream": If $\mathrm{char} F = p > 0$, then $\forall c \in F$, $\forall b \in F$, $(a+b)^p = a^p + b^p$.

$\Rightarrow \chi_p(a) = a^p$ is injective homomorphism from F to F.

*The proof requires $0 \neq 1$. By PHP, if $|F| < \aleph_0$, then $\chi_p \in \mathrm{Aut}(F)$.

21-374 Midterm 1 Review 2/28/2002

Def. $p \in F[x]$ has no multiple roots ("separable") provided $\nexists\, \alpha \in E$ for some $E \geq F$, then $(x-\alpha)^2 \mid p$.

Theorem. $p \in F[x]$. p is separable $\Leftrightarrow (p, p') = 1$ ← the derivative of p

* We do formal computations with Π.

Ex. If F is a field of characteristic 0 and $p(x) \in F[x]$ is irreducible, then $p(x)$ has no repeated roots.

The monic polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ is separable.

Application: Take splitting field of $f/\mathbb{F}_p$. It has at least p^n many elements. However the degree of f is p^n.

Let E be splitting field of $f/\mathbb{F}_p$, $K = \{\alpha \in E \mid \chi_p^n(\alpha) = \alpha\} \leq E$ has exactly p^n many elements.
↑ 'key fact'

Lemma. Let $F \leq E$, $\alpha, \beta \in E$. $F(\alpha,\beta) = F(\alpha)(\beta) = F(\beta)(\alpha)$. 'Iterated extensions'

(Application of mult formula) $F \leq E$, $\alpha, \beta \in E$. If both α and β are algebraic over F, then
$\forall\, \gamma \in F(\alpha,\beta)$, γ is algebraic over F.

Pf. Enough to show $[F(\gamma) : F] < \aleph_0$. Since $F(\gamma) \leq F(\alpha,\beta)$, enough to show $[F(\alpha,\beta) : F] \leq \aleph_0$.
'subspace'

$$[F(\alpha,\beta) : F] = [F(\alpha)(\beta) : F] = [F(\alpha)(\beta) : F(\alpha)] \cdot [F(\alpha) : F]$$

finite since α is algebraic

$\leq [F(\beta) : F]$ finite since β algebraic.

(counting diagrams)
E is splitting field of $p/F \Rightarrow |\mathrm{Aut}(E/F)| \leq [E : F]$. Equality follows if all roots of p are unique.

Corollary. $\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle \chi_p \rangle = \{\chi_p^k \mid k \in \mathbb{N}\}$.