Here is an application of the last theorem.

<u>Def 111:</u> A field F is called algebraically closed if every polynomial $P \in F[X] \setminus F$ has a root in F.

<u>Examples:</u> $\mathbb{C}$ is algebraically closed. This has been proven in complex analysis.

<u>Def 112:</u> Let $P \in F[X] \setminus F$ and F be an alg. closed field. Suppose $\deg P \geq 2$.

$$P = (X - \alpha_1) \cdots (X - \alpha_{\deg(P)}).$$

The element

$$\prod_{\substack{i<j}} (\alpha_i - \alpha_j)^2 =: \operatorname{disc}(P)$$

is called the discriminant of P.

(For $\deg(P) = 1$ just set $\operatorname{disc}(P) = 1$)

<u>Prop 113:</u> 1) Let $P \in \mathbb{C}[X]$,

$$P(X) = X^2 + bX + c.$$

Then $\operatorname{disc}(P) = -4c + b^2$.

2) The polynomial
$$P = X^3 + aX + b \in \mathbb{C}[X]$$
has discriminant $-4a^3 - 27b^2$

<u>Proof:</u> 1) $P = (X - t_1)(X - t_2)$
$$(t_1 - t_2)^2 = (t_1 + t_2)^2 - 4t_1t_2 = b^2 - 4c$$

2) The polynomial $\prod_{1 \le i < j \le 3} (T_i - T_j)^2 =: D$ is symmetric of degree 6.

$\Rightarrow \exists\, Q \in \mathbb{C}[X_1, \dots, X_3]$ of weight 6 s.t. $Q(S_1, S_2, S_3) = D$.

Let t_1, t_2, t_3 be the roots of P.

Then $D(t_1, t_2, t_3) = Q(\underbrace{S_1(t_1, t_2, t_3)}_{=0}, S_2, S_3)$
$$= c\, S_2^3(t_1, \dots) + d\, S_3^2(t_1, t_2, t_3).$$

Further $c, d \in \mathbb{Z}$ by Theorem 109 and they only depend on D and not on P.

Let's plug in examples ~~of~~ for P.

$$P = X(X-1)(X+1) = X^3 - X$$

$$\operatorname{disc}(P) = (0-1)^2(0-(-1))^2(-1-1)^2 = 4$$

$$\Rightarrow \quad -c = 4.$$

$$P = (X-1)^2(X+2) = (X^2-2X+1)(X+2)$$

$$= X^3 - 3X + 2$$

$$\operatorname{disc}(P) = 0$$

$$\Rightarrow \quad 0 = -4(-3)^3 + d \cdot 2^2 \Rightarrow d = -27$$

$\square$

III Algebraic field extensions

III 1. First definitions

Def 113: 1) A field extension is a pair of two fields E, F s.t. $E \supseteq F$ and F is a subfield of E. We write $E|F$. We call E an extension field of F.

2) Given a field extension $E|F$ and a subset $S \subseteq E$, we recall that

$F(S)$ is the smallest subfield of E which contains $S \cup F$ and

$F[S]$ is the smallest subring of E which contains $F \cup S$.

If $S = \{\alpha_1, \dots, \alpha_e\}$ we also write $F(\alpha_1, \dots, \alpha_e)$ and $F[\alpha_1, \dots, \alpha_e]$.

3) Let $E|F$ be a field extension.
An element $\alpha \in E$ is called algebraic over F if $\exists$ monic $P \in F[X]$: $P(\alpha) = 0$.

otherwise we call α <u>transcendent</u> over F.

4) let $E|F$ be a field extension and $E_1|F$ and $E_2|F$ be subextension of $E|F$.

We call $E_1(E_2) = F(E_1 \cup E_2)$

the <u>compositum</u> of E_1 with E_2. Write E_1E_2.

5) A field extension $E|F$ is called algebraic if every element of E is algebraic over F.

<u>Example</u>: 1) $E := \mathbb{R}$, $F := \mathbb{Q}$, $\alpha := \sqrt{2}$ is algebraic over $\mathbb{Q}$, because $p = X^2 - 2$ satisfies $p(\sqrt{2}) = 0$.

In fact, $F(\sqrt{2})|F$ is algebraic because

- $F(\sqrt{2}) = F[\sqrt{2}]$, because $a + b\sqrt{2}$ has inverse $(a - b\sqrt{2}) \frac{1}{a^2 - b^2 2}$ if $(a,b) \neq (0,0)$

and

- $a + b\sqrt{2}$ is the root of
$$p = X^2 - 2aX + (a^2 - b^2 \cdot 2)$$

2) $E := F(X) | F$. X is not algebraic over F. <u>Proof</u>: Assume $\alpha := X$ is algebraic over F.

Then $\exists\; P \in F[T] \setminus F$: $P(\alpha) = 0$ in $F(X)$.

In fact $\alpha \in F[X]$, so $P(\alpha) \in F[X]$

~~$1 = \deg_X P(\alpha) = (\deg_T P)(\deg_X \alpha) = \deg_T P \geq 1$~~

We have $P(T) = \sum_{i=0}^{d} a_i T^i$, $d := \deg P \geq 1$.

So $\deg_X (P(\alpha)) = \deg_X \sum_{i=0}^{d} a_i X^i = d \geq 1 \neq -\infty$

So $P(\alpha) \neq 0$ ↯. $\square$

You get similarly : $\forall\, Q \in F[X] \setminus F$:

Q is transcendent over F.

<u>Prop 11.4</u>: Let $E|F$ be a field extension and $\alpha \in E$. Then are equivalent:

1° α is algebraic over F

2° $F[\alpha]$ is a finite dimensional F-vector space.

3° $F[\alpha]|F$ is algebraic ~~...~~ and $F[\alpha]$ is a field.

Proof: $3^\circ \Rightarrow 1^\circ$ ✓

$1^\circ \Rightarrow 2^\circ$: $1^\circ \Rightarrow \exists\ P \in F[X] \setminus F$: $P(\alpha) = 0$.

w.l.o.g. P is monic (otherwise consider $\frac{1}{\lambda}P$ with λ the leading coefficient).

$$F[\alpha] = \sum_{i=0}^{\infty} F\alpha^i$$

$$= \{ \lambda_1 \alpha^{i_1} + \lambda_2 \alpha^{i_2} + \dots + \lambda_k \alpha^{i_k} \mid k \in \mathbb{N}, \lambda_1, \dots, \lambda_k \in F,\ i_1, \dots, i_k \in \mathbb{N}_0 \}$$

P has the form $P = X^d + a_{d-1} X^{d-1} + \dots + a_1 X + a_0$

$P(\alpha) = 0 \Rightarrow \alpha^i P(\alpha) = 0\ \forall i \geq 0$.

$$\Rightarrow \forall_{i \geq 0}: \alpha^{d+i} = -\sum_{j=0}^{d-1} a_j \alpha^{j+i}.$$

Thus by induction we get for all $i \in \mathbb{N}_0$

$$\alpha^{d+i} \in F + F\alpha + \dots + F\alpha^{d-1}$$

$$\Rightarrow \dim_F F[\alpha] \leq d.$$

$2^\circ \Rightarrow 3^\circ$: Consider the map

$$\varphi : F[X] \longrightarrow F[\alpha] \quad \varphi(P) = P(\alpha).$$

φ is a ring homomorphism and $\mathfrak{p} = \ker(\varphi) \neq (0)$ because otherwise

$$\dim_F F[\alpha] = \dim_F F[X] \underset{\uparrow}{=} \infty.$$

$\{1, X, X^2, \dots\}$ is an F-basis

We have $F[X]/\mathfrak{p} \simeq F[\alpha]$.

$\Rightarrow$ $\mathfrak{p}$ is a prime ideal because $F[\alpha]$ is an integral domain since $F[\alpha] \subseteq E$.

$F[X]$ is a PID by Prop 76(5), so every non-zero prime ideal is maximal.

$\Big((0) \subsetneq \underset{\text{prime}}{\underset{\uparrow}{(P)}} \subseteq \underset{\text{max}}{\underset{\uparrow}{(Q)}} \Rightarrow Q \mid P \underset{\underset{P,Q \text{ prime elements}}{\uparrow}}{\Rightarrow} Q, P$ are associates

$\Rightarrow (P) = (Q)\Big)$

$\Rightarrow$ $F[X]/\mathfrak{p}$ is a field $\Rightarrow$ $F[\alpha]$ is a field.

Now take $\beta \in F[\alpha]$.

$\dim_F F[\alpha] < \infty \Rightarrow \{1, \beta, \beta^2, \dots\}$ is not linearly independent.

$\Rightarrow \exists\, P \in F[X] \setminus F : P(\beta) = 0.$ $\square$

Remark 115: 1) Let $E|F$ be a field extension. Then are equivalent for $\alpha \in E$:

1° α is algebraic over F.

2° $F(\alpha) = F[\alpha]$

(exercise.)

2) The proof of Prop. 114 shows in fact that α is algebraic over F iff $\exists$ a subring $R \subseteq E$ containing F: $\alpha \in R$ and $\dim_F R < \infty$.

Corollary 116: Let $E|F$ be a field extension and $S \subseteq E$. Then are equivalent:

1° $F(S)|F$ is algebraic

2° $\forall_\alpha \in S$: α is algebraic over F.

end of lecture 21

Proof: In a homework problem you are going to show

$$F(S) = \left\{ \frac{P(\alpha_1,\dots,\alpha_k)}{Q(\alpha_1,\dots,\alpha_k)} \,\middle|\, k \in \mathbb{N}_0,\ \alpha_1,\dots,\alpha_k \in S,\ P, Q \in F[X_1,\dots,X_k] \text{ s.t. } Q(\alpha_1,\dots,\alpha_k) \neq 0 \right\}$$

$1^\circ \Rightarrow 2^\circ$: ✓ by definition of an algebraic field extension.

$2^\circ \Rightarrow 1^\circ$: Take $\beta \in F(S)$.

$\Rightarrow \underset{k \in \mathbb{N}_0}{\exists}\ \exists\ \alpha_1, \dots, \alpha_k \in S: \ \beta \in F(\alpha_1, \dots, \alpha_k)$.

If $k = 0$, then $\beta \in F$ is algebraic over F. So, consider $k > 0$.

$\forall_{i=1,\dots,k}$: α_i is algebraic over F

$\Rightarrow \forall_{i=1,\dots,k}$: α_i — " — $F(\alpha_1, \dots, \alpha_{i-1})$

Prop 114 $\Rightarrow \forall_{i=1,\dots,k}: \dim_{F(\alpha_1,\dots,\alpha_{i-1})} F(\alpha_1, \dots, \alpha_{i-1})(\alpha_i) < \infty$

$\Rightarrow \dim_F F(\alpha_1) < \infty$ and if for $i > 1$

$\dim_F F(\alpha_1, \dots, \alpha_{i-1}) < \infty$ then $\dim_F F(\alpha_1, \dots, \alpha_i) < \infty$

$$\dim_F F(\alpha_1, \dots, \alpha_i) = \dim_F F(\alpha_1,\dots,\alpha_{i-1}) \cdot \dim_{F(\alpha_1,\dots,\alpha_{i-1})} F(\alpha_1,\dots,\alpha_i)$$

Thus by induction we get

$$\dim_F F(\alpha_1, \dots, \alpha_k) < \infty$$

and therefore $\dim_F F(\beta) \le \dim_F F(\alpha_1, \dots, \alpha_k) < \infty$.

Remark 115(2) $\Rightarrow$ β is algebraic over F. $\square$

Prop 117: 1) The composition of two algebraic subextension $E_1|F$ and $E_2|F$ of a field extension $E|F$ is an algebraic field extension

$$\begin{tikzcd} & E_1E_2 & \\ E_1 \arrow[ur, dash] & & E_2 \arrow[ul, dash] \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

2) Let $E|F$ be a field extension and L be an intermediate extension field of F. Then are equivalent:

1° $E|F$ is algebraic

2° $E|L$ and $L|F$ are algebraic.

Proof: 1) $E_2|F$ is algebraic $\Rightarrow$ $\forall \alpha \in E_2$: α is algebraic over E_1

Corollary 116 $\Rightarrow$ $E_1(E_2)\,|\,E_1$ is algebraic

$\Rightarrow$ $E_1E_2|F$ is algebraic by 2)

2) $1^\circ \Rightarrow 2^\circ$ is an easy exercise

$2^\circ \Rightarrow 1^\circ$ Take $\alpha \in E$.

$\overset{2^\circ}{\Rightarrow}$ α is algebraic over L

$\Rightarrow$ $\exists P \in L[X] \setminus L$: $P(\alpha) = 0$.

Let $a_0, \dots, a_d \in L$ be the coefficients of P.

$a_0, \dots, a_d$ are algebraic over F

Prop. 114 $\Rightarrow \dim_F \underbrace{F(a_0, \dots, a_d)}_{=:K} < \infty$

α is algebraic over K, because $P \in K[X]$.

Prop 114 $\Rightarrow \dim_K K(\alpha) < \infty$

Thus $\dim_F K(\alpha) < \infty$

Remark 115(2) $\Rightarrow$ α is algebraic over F $\square$

We need to give some extra notions.

Def 118: 1) A field extension E/F is called finitely generated iff $\exists$ $x_1, \dots, x_e \in E$: $E = F(x_1, \dots, x_e)$.

2) We call $\dim_F E$ the degree of a field extension E/F and denote the degree by $[E:F]$.

3) A field extension is called finite if the degree is finite

(finite field ext. are automatically finitely generated.)

We would like to prove the existence of an algebraic ~~alg~~ closure of a field F. ~~Def~~ ~~Deshalb~~ Therefore we study injective limits in the next section.

III.7. projective and injective limits

Def 119: An ordered set $(J, \leq)$ is called a directed set if $\forall\, i, j \in J\ \exists\, k : i \leq k$ and $j \leq k$.

Example: 1) Every totally ordered set is directed

2) $(\mathbb{R}^2, \leq)$ with

$$(x_1, x_2) \leq (a_1, a_2) \iff_{\text{def}} x_1 \leq a_1 \text{ and } x_2 \leq a_2$$

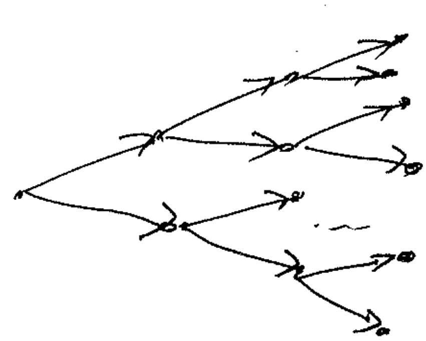
is directed, because

for $(x_1, x_2), (y_1, y_2) \in \mathbb{R}^2$ we have

$$(x_1, x_2) \leq (z_1, z_2) \geq (y_1, y_2)$$

for $z_i := \max\{x_i, y_i\}$.

3)



... a directed tree.

$J :=$ "set of vertices"

$v_1, v_2 \in J$. $v_1 \leq v_2$ if $\exists\ v_1 \to \cdots \to v_2$

$(J, \leq)$ is not directed.

Directed sets are used as index sets for families of whom we want to take something similar to a union ("injective limit") or intersection ("projective limit")

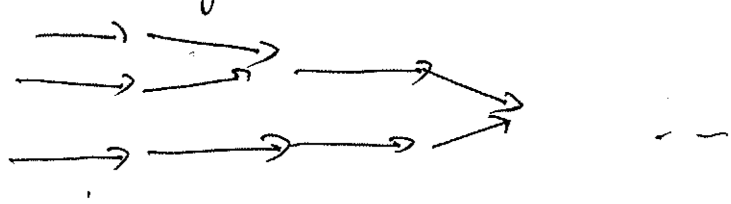
<u>Def 120:</u>

1) An injective system is a family $(f_{i,j} : X_i \to X_j)_{\substack{i \leq j \\ i,j \in J}}$ of maps such that $(J, \leq)$ is a directed set and we have $f_{j,k} \circ f_{i,j} = f_{i,k} \quad \forall i \leq j \leq k$.

2) Analogously we define a projective system: $(f_{i,j} : X_j \to X_i)_{i \leq j}$

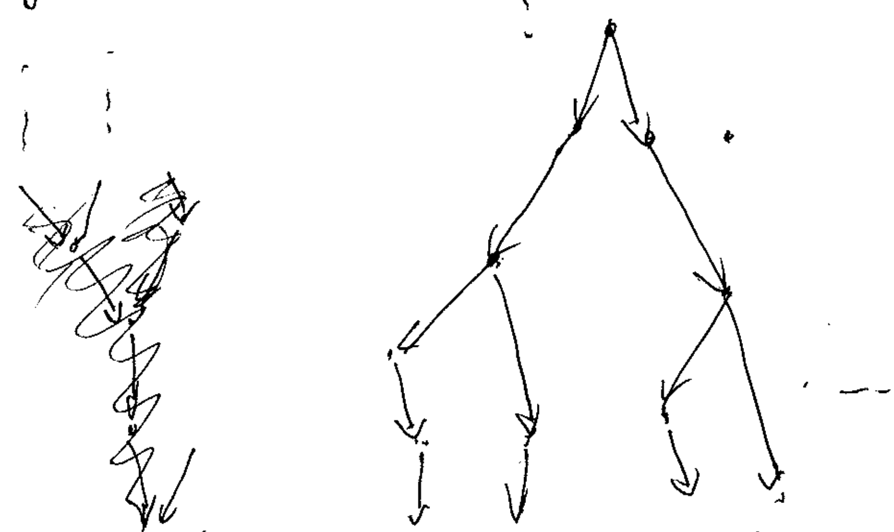
with $f_{k,i} \circ f_{i,j} = f_{k,j} \quad \forall k \leq i \leq j$ ∎.

<u>Picture:</u> injective system



i

projective system



The easiest (injective (projective) system is a family of inclusions:

$$A_i \subseteq A_j \qquad f_{ij} = \mathrm{incl}_{A_i \subseteq A_j} \qquad \begin{matrix} i,j \in \mathbb{N} \\ i \leq j \end{matrix}$$

$$(i,j \in \mathbb{N} \quad i \geq j)$$

We now give the generalization of $\bigcup_{i \in \mathbb{N}} A_i$ $\left(\bigcap_{i \in \mathbb{N}} A_i \right)$.

<u>Def 121:</u> Let $(f_{ij} : X_i \to X_j)_{\substack{i \leq j \\ i,j \in J}}$ be an injective system.

Put $\varinjlim_J X_i := \bigsqcup_{i \in J} X_i \Big/ \sim$

where $\sim$ is the equivalence relation given by the incidence relation:

$\forall\ x_i \in X_i,\ x_j \in X_j :\quad x_i \sim x_j \overset{\text{def}}{\iff}$

$$(i \leq j \text{ and } f_{i,j}(x_i) = x_j) \text{ or}$$

$$(j \leq i \text{ and } f_{j,i}(x_j) = x_i).$$

We call $\varinjlim\limits_{J} X_i$ the injective (or direct) limit of (f_{ij}).

2) Let $(f_{i,j} : X_j \to X_i)_{\substack{i \leq j \\ J}}$ be a projective system. The set

$$\varprojlim_{J} X_i := \left\{ (x_i)_{i \in J} \;\middle|\; \forall_{i \leq j} : f_{i,j}(x_j) = x_i \right\}$$

is called the projective limit of (f_{ij})

Examples / remarks: 1) $J = \mathbb{N}$ $\quad A_i \overset{\text{incl}_{ij}}{\hookrightarrow} A_j$

$$\varinjlim_{J} A_i \doteq \bigcup_{i \in J} A_i$$

Proof: $\quad \bigsqcup_{i \in J} A_i \Big/ \sim \ \xrightarrow{\ \Phi\ } \ \bigcup_{i \in J} A_i$

$$[a]_{\sim} \longmapsto a$$ is well-defined and bijective.

well-defined:

$a \sim b$, $a \in A_i$, $b \in A_j$

$\Rightarrow$ $\exists$ $i_1 = i$, $i_2, i_3, \ldots, i_k = j$: $\exists$ $a_{i_1} \in A_{i_1}, \ldots a_{i_k} \in A_{i_k}$

$i_1 \leq i_2 \geq i_3 \leq i_4 \ldots \gtreqless i_k$:

(or $i_1 \geq i_2 \leq \ldots$)

(*) $\quad ind_{A_{\min(i_j, i_{j+1})}, A_{\max(i_j, i_{j+1})}}(a_{\min}) = a_{\max}$

W.l.o.g. $i \leq j$

To show $a = b$ in $\bigcup_{i \in J} A_i$

(*) implies $a_{\min} = a_{\max}$ in $\bigcup_{i \in J} A_i$.

for every step. So $a = b$ in $\bigcup_J A_i$.

Surjectivity ✓

Injectivity: Take $a \in A_i$ and $b \in A_j$

s.t. $\Phi([a]_\sim) = \Phi([b])$. i.e. $a = b$ in $\bigcup_{i \in J} A_i$.

If $i \leq j$: $A_i \subseteq A_j$ $a = b$ in $\bigcup_J A_i$, so

$ind_{i,j}(a) = a = b$, so $a \sim b$.

If $i \geq j$: Analogously $a \sim b$. $\square$

2) The injective limit always ~~exists~~ is non-empty.

3) Consider a set

$\{X_\lambda \mid \lambda \in \Lambda\}$ (just a set.) indexed by Λ.

$$\mathcal{J} = \{\Lambda' \subseteq \Lambda \mid \Lambda' \text{ is finite}\}$$

$(\mathcal{J}, \subseteq)$ is a directed set.

Let R be a non-zero commutative unitary ring.

$$\left(f_{\Lambda_1, \Lambda_2} : R[X_\lambda \mid \lambda \in \Lambda_1] \xhookrightarrow{\text{incl.}} R[X_\lambda \mid \lambda \in \Lambda_2]\right)_{\Lambda_1 \subseteq \Lambda_2}$$

is an injective system.

We put

$$F[X_\lambda \mid \lambda \in \Lambda] := \varinjlim_{\Lambda' \in \mathcal{J}} F[X_\lambda \mid \lambda \in \Lambda'] .$$

End Lecture 22

4) One can interprete $\bigcap_{\mathbb{N}} A_j$ as a projective limit if $\{A_j \mid j \in \mathbb{N}\}$ is totally ordered s.t. $A_j \subseteq A_i$ if $j \geq i$.

(Exercise on the HW problem sheet.)

5) $\varprojlim_{\mathcal{J}} X_i$ can be empty.

Take $A_n := [n, \infty)$, $n \in \mathbb{N}$.

$$\bigcap_{n \in \mathbb{N}} A_n = \emptyset.$$

6) $X_n := \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$.

$$f_{n,m} : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \qquad n \mid m$$
$$[z]_m \longmapsto [z]_n$$

$(f_{n,m})_{n|m}$ is a projective system.

$\varprojlim_{\mathbb{N}} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}$ is called the

~~Prüfer~~ "ring of profinite integers".

$$\varprojlim_{\mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \left\{ \left([z_n]_n \right)_{n \in \mathbb{N}} \;\middle|\; \forall n|m : \; [z_m]_n = [z_n]_n \right\}$$

$$(z_m \equiv_n z_n)$$

Ex: $([z]_n)_{n \in \mathbb{N}} \in \varprojlim_{\mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$, $z \in \mathbb{Z}$.

$$([1]_1, [1]_2, [2]_3, [3]_4, [2]_5, [5]_6, \ldots$$

by CRT.

We have the following universal property for the injective limit

<u>Prop 122</u>: (i) Let $(f_{ij})_{i\le j\in J}$ be an injective system and let (X, f_i) be a set which satisfies $f_j \circ f_{ij} = f_i \quad \forall i \le j$ and $(*)$:

$(*)$ $\forall_Y \forall_{(g_i)_{i\in J}}$ $g_i : X_i \longrightarrow Y$ satisfying

$$\left(g_j \circ f_{ij} = g_i \quad \forall i \le j \right)$$

$$\exists!\ g : X \longrightarrow Y \text{ s.t.}$$

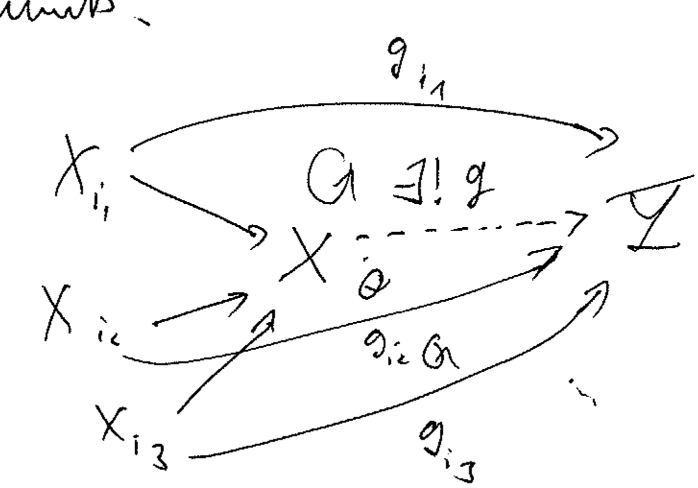
$$\forall i \in J : \quad g \circ f_i = g_i .$$

Then $\varinjlim_J X_i \simeq X$.

(ii) $\varinjlim_J X_i$ with $f_i : X_i \longrightarrow \varinjlim_J X_i$, $x \mapsto (x,i)$, $i \in J$, satisfies $(*)$.

<u>Remark</u>: There is a similar universal property for projective limits.

<u>Proof</u> (Prop 122):



Take $\mathbb{X} := \varprojlim_J X_i$, $g_i : \mathbb{X}_i \to \varprojlim_J X_i$, $x \mapsto [x]_\sim$.

$\Rightarrow \exists\, g : \mathbb{X} \to \varprojlim_J X_i$ s.t.

$$\begin{tikzcd} & \mathbb{X} \arrow[r, "g"] & \varprojlim_J \mathbb{X}_i \\ \mathbb{X}_i \arrow[ur, "f_i"] \arrow[urr, bend right, "g_i"'] \arrow[ur, phantom, shift left=6, "\alpha"] & & \end{tikzcd} \qquad g \circ f_i = g_i \;\; \forall_{i \in I}$$

<u>g is surjective:</u> Take $x \in \mathbb{X}_i$. Then

$$g_i(x) = [x]_\sim = g(f_i(x))$$

<u>g is injective:</u> (1) Claim $\bigcup_{i \in J} f_i(\mathbb{X}_i) = X$.

<u>Proof</u>: If $\bigcup_{i \in J} f_i(\mathbb{X}_i)$ is not X then take

$x_0 \in X \setminus \left(\bigcup_{i \in J} f_i(X_i)\right)$. ~~The map~~

Consider $Y := \{1, 2\}$ and $\tilde{g}_i : X_i \to Y$

$\tilde{g}_i(x) := 1$. Then we can use $\tilde{g} : X \to Y$

$$x \neq x_0 \mapsto 1$$
$$x_0 \mapsto 1$$
$$\text{or } x_0 \mapsto 2$$

for the diagram

$$\begin{tikzcd} X \arrow[r, "\tilde{g}"] & Y \\ X_i \arrow[u, "f_i"] \arrow[ur, "\tilde{g}_i"'] \arrow[ur, phantom, shift left=3, "\alpha"] & \end{tikzcd}$$

So we have no uniqueness ↯.

So $\bigcup_{i \in J} f_i(X_i) = X$ □ (Claim)

Now we can prove injectivity.

Suppose $\exists\, x_{i_1} \in X_{i_1}$ and $x_{i_2} \in X_{i_2}$:

$$g(f_{i_1}(x_{i_1})) = g(f_{i_2}(x_{i_2})),\ \text{i.e.}$$

$$[x_{i_1}]_\sim = [x_{i_2}]_\sim .$$

$(J, \leq)$ is directed $\Rightarrow$ $\exists\, k \geq i_1, i_2$: $f_{i_1 k}(x_{i_1}) =: x_k = f_{i_2 k}(x_{i_2})$

$$\left(i_1 \leq j_2 \geq i_3 \leq j_3 \ \cdots \ i_2 \right)$$

$$k$$

$$f_k(x_k) = f_k \circ f_{i_1 k}(x_1) = f_{i_1}(x_{i_1}) =$$

$$\| $$

$$f_k \circ f_{i_2 k}(x_{i_2}) = f_{i_2}(x_{i_2}) .$$

$$\Longrightarrow f_{i_1}(x_{i_1}) = f_{i_2}(x_{i_2})$$ ▨

The second assertion is an exercise □

Ex: $\exists !\ g : F[X_\lambda \mid \lambda \in \Lambda] \longrightarrow F[X]$

$$P(X_\lambda \mid \lambda \in \Lambda) \longmapsto P(X \mid \lambda \in \Lambda)$$

Ex: $X_{\lambda_1}^2 + 3 X_{\lambda_2} X_{\lambda_1} \longmapsto 4X^2$

Proof: Define for $\Lambda' \subseteq \Lambda$ finite

$$g_{\Lambda'} : F[X_\lambda \mid \lambda \in \Lambda'] \longrightarrow F[X]$$

$$g_{\Lambda'}(P) := P(X \mid \lambda \in \Lambda')$$

$$g_{\Lambda'}(P(X_{\lambda_1}, \dots, X_{\lambda_\ell})) := P(X, \dots, X)$$

$$\Lambda' = \{\lambda_1, \dots, \lambda_\ell\}$$

By Prop 122 (1) there exists the above g.

Remark: There is a similar universal property for projective limits

III.3. Existence of an algebraic closure of a field

Def 123: 1) A field E is called an algebraic closure of a field F if $\exists$ field homomorphism $F \overset{\varphi}{\hookrightarrow} E$, E is algebraically closed. and $E \mid \varphi(F)$ is algebraic.

2) $E \mid F$, a field ext., is called transcendental if it is not algebraic.

Remark: Normally we identify F with its image in E and write $E|F$.

Ex: $\mathbb{Q} \subseteq \mathbb{C}$

$\overline{\mathbb{Q}}^{alg} := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}$

$\overline{\mathbb{Q}}^{alg} | \mathbb{Q}$ is a field extension (homework: $\alpha, \beta \in \overline{\mathbb{Q}}^{alg}, \beta \neq 0$, then $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in \overline{\mathbb{Q}}^{alg}$)

$\overline{\mathbb{Q}}^{alg}$ is algebraically closed:

$$P \in \overline{\mathbb{Q}}^{alg}[X] \setminus \overline{\mathbb{Q}}^{alg}.$$

$$\underset{\substack{\uparrow \\ \mathbb{C} \text{ is alg closed}}}{\Rightarrow} \quad \exists \alpha \in \mathbb{C} : P(\alpha) = 0 \underset{\substack{\uparrow \\ \text{Def of } \overline{\mathbb{Q}}^{alg}, \\ \text{and exercise}}}{\Rightarrow} \alpha \in \overline{\mathbb{Q}}^{alg}.$$

Thm 124: Let F be a field. Then there exists an algebraic closure of F.

Proof: Let $\mathfrak{M}$ be the set of all polynomials $\in F[X] \setminus F$

Consider $F[X_P \mid P \in \mathfrak{M}] =: R$

The ideal $\mathfrak{A} := (P(X_P) \mid P \in \mathfrak{M})_R$ is proper. Otherwise $1 \in \mathfrak{A}$

$\Rightarrow \exists P_1, \dots, P_e : \quad 1 \in (P_1(X_{P_1}), \dots, P_e(X_{P_e}))_{F[X_{P_1}, \dots, X_{P_e}]}$

We show by induction on l ~~...~~ that this is not possible.

$\underline{l=1}$: P_1 is ~~an irreducible~~ polynomial of degree ≥ 1.

Thus every non-zero element of $(P_1(X_{P_1}))_{F[X_{P_1}]}$ has degree ≥ 1. Thus $1 \notin (P_1(X_{P_1}))_{F[X_{P_1}]}$.

$\underline{l>1}$: $\exists\ F \hookrightarrow E$ s.t. E is a field and contains a root of P_l.

($\underline{\text{Proof}}$: $E := F[X]/(\tilde{P}(X))$ where $\tilde{P}$ is an irreducible divisor of P_l.)

If $1 \in (P_1(X_{P_1}), \dots, P_l(X_{P_l}))_{F[X_1, \dots, X_{P_l}]}$

then $1 \in (\quad \cdots \quad)_{E[X_{P_1}, \dots, X_{P_l}]}$.

$\Rightarrow \exists\ S_1, \dots, S_l \in E[X_{P_1}, \dots, X_{P_l}]$:

$$1 = \sum_{i=1}^{l} S_i\, P_i(X_{P_i})$$

Let $\alpha \in E$ be a root of P_l. Plug in α for X_{P_l}.

$$\Rightarrow 1 = \sum_{i=1}^{l-1} S_i(X_{P_1}, \dots, X_{P_{l-1}}, \alpha) \cdot P_i(X_{P_i})$$

$\overset{(JH)}{\Longrightarrow}$ Contradiction, because $1 \notin (p_1(X_{p_1}), \ldots, p_{\ell-1}(X_{p_{\ell-1}}))$

$\subseteq E[X_{p_1}, \ldots, X_{p_\ell}]$.

Now take a maximal ideal $\hat{\mathfrak{a}} \supseteq \mathfrak{a}$.

lecture 23

$$E_1 := F[X_p \mid p \in \mathfrak{M}] \big/ \hat{\mathfrak{a}} \quad \text{is a field}$$

$F \hookrightarrow E_1$.

For every $p \in F[X]$ we have

$$p([X_p]_{\hat{\mathfrak{a}}}) = [0]_{\hat{\mathfrak{a}}} : \quad \text{because } p(X_p) \in \hat{\mathfrak{a}}.$$

$$F_1 := \overline{F}^{\mathrm{alg}, E_1} := \{\beta \in E_1 \mid \beta \text{ is algebraic over } F\}$$

In this way we define

$$F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots \qquad F_{i+1} := \overline{F_i}^{\mathrm{alg}, E_{i+1}}.$$

$$E_{i+1} := F_i[X_p \mid p \in F_i[X] \setminus F] \big/ \hat{\mathfrak{a}}_{i+1}$$

Put $E := \bigcup_{i \in \mathbb{N}} F_i = \varinjlim_{\mathbb{N}} F_i$. (injective limit)

Claim: ~~E/F~~ E is an algebraic closure of F.

Proof (Claim): Put $F_0 := F$

alg: $\forall_{i \in \mathbb{N}}$: $F_i | F_{i-1}$ is algebraic

$\Rightarrow$ $\forall_{i \in \mathbb{N}}$: $F_i | F$ is algebraic by the tower law.

Thus every element of E is algebraic over F.

$\Rightarrow$ $E|F$ is algebraic.

E alg closed: Take $P \in E[X] \setminus E$ and $i \in \mathbb{N}$ s.t. all coefficients of P are in F_i.

Then P has a root in $F_{i+1} \subseteq E$.

□ (Claim)

□ Thm 124.

Def 125: Let F be a field. The characteristic of F is defined to be the number

$$\mathrm{char}(F) = \begin{cases} \min\{n \in \mathbb{N} \mid n \cdot 1_F = 0_F\}, & \text{if } \exists_{n \in \mathbb{N}}: n \cdot 1_F = 0_F \\ 0, & \text{if } \nexists_{n \in \mathbb{N}}: n \cdot 1_F = 0_F \end{cases}$$

Prop 126: Let E be an algebraically closed field and $E_2 | E_1$ be an algebraic field extension together with a field homomorphism $\varphi: E_1 \hookrightarrow E$.

Then there exists a field homomorphism $\tilde{\varphi}: E_2 \longrightarrow E$ s.t. $\tilde{\varphi}\big|_{E_1} = \varphi$.

<u>Proof:</u> $\mathcal{M} = \{(\psi', E') \mid E'$ is an intermediate field between E_1 and E_2 and $\psi': E' \hookrightarrow E$ is a field homomorphism s.t. $\psi'\big|_{E_1} = \varphi \}$

$(\psi', E') \leq (\psi'', E'')$ (both in $\mathcal{M}$)

$\Leftrightarrow_{\text{Def.}}$ $E' \subseteq E''$ and $\psi''\big|_{E'} = \psi'$.

$(\mathcal{M}, \leq)$ is inductively ordered and $\mathcal{M} \ni (\varphi, E_1)$.

Zorn's Lemma $\Rightarrow \exists (\hat{\psi}, \hat{E}) \in \mathcal{M}$ which is maximal w.r.t. "$\leq$".

<u>Claim</u> $\hat{E} = E_2$.

If not, then $\exists \quad \alpha \in E_2 \setminus \hat{E}$.

α is algebraic over $\hat{E}$, because it is over E_1.

Take the polynomial $P_\alpha \in \hat{E}[X] \setminus \hat{E}$ of smallest degree s.t. $P_\alpha(\alpha) = 0$ and P_α is monic.

(the <u>minimal polynomial</u> of α over $\hat{E}$.)

E is algebraically closed.

Define $\hat{\varphi}(P_\alpha)$ to be the polynomial $\sum_{i=0}^{d} \hat{\varphi}(a_i) X^i$

if $P = \sum_{i=0}^{d} a_i X^i$.

$\hat{\varphi}(P_\alpha)$ has a root in E, say β, and we have

$\hat{E}(\alpha) = \hat{E}[\alpha]$ by Prop. 114.

We define $\quad \psi : \hat{E}[\alpha] \longrightarrow E$

via $\quad \psi(Q(\alpha)) := \hat{\varphi}(Q)(\beta)$ for all

$Q \in \hat{E}[X]$.

① We need to show that ψ is well-defined.

Let $Q_1, Q_2 \in \hat{E}[X]$, s.t. $Q_1(\alpha) = Q_2(\alpha)$.

$\Rightarrow (Q_1 - Q_2)(\alpha) = 0 \Rightarrow P_\alpha \mid Q_1 - Q_2$

(because $\{Q \in \hat{E}[X] \mid Q(\alpha) = 0\}$ is an ideal generated by P_α)

$\Rightarrow \quad \hat{\varphi}(P_\alpha) \mid \hat{\varphi}(Q_1) - \hat{\varphi}(Q_2)$

$\Rightarrow \quad (\hat{\varphi}(Q_1) - \hat{\varphi}(Q_2))(\beta) = 0$

$\Rightarrow \quad \hat{\varphi}(Q_1)(\beta) = \hat{\varphi}(Q_2)(\beta)$.

$\Rightarrow \quad \psi(Q_1(\alpha)) = \psi(Q_2(\alpha))$

② ψ is a field homomorphism.

- $\psi(1) = 1$ ✓, because $\hat{\varphi}(1) = 1$
- $\psi(Q_1(\alpha) Q_2(\alpha)) = \hat{\varphi}(Q_1 Q_2)(\beta) \overset{\hat{\varphi} \text{ ringhomor.}}{=} \hat{\varphi}(Q_1)(\beta)\, \hat{\varphi}(Q_2)(\beta)$

$$= \quad \Psi(Q_1(\alpha))\,\Psi(Q_2(\alpha))$$

③ $\Psi\big|_{\hat{E}} = \hat{\varphi}$.

By definition $a \in \hat{E}$. Take the constant polynomial $Q = a \in \hat{E}[X]$.

$\Rightarrow Q(\alpha) = a$. $\qquad \hat{\varphi}(Q) = \hat{\varphi}(a) \in E[X]$, $\hat{\varphi}(a) \in E$

$$\Psi(a) = \Psi(Q(\alpha)) = \hat{\varphi}(Q)(\beta) \stackrel{\downarrow}{=} \hat{\varphi}(a).$$

Then $(\hat{\varphi}, \hat{E}) < (\Psi, \hat{E}[\alpha]) \in \mathcal{M}$ $\lightning$.

Thus $E_2 = \hat{E}$. $\square$

<u>Corollary 127:</u> Let E_1 and E_2 be algebraic closures of a field F.
Then $\exists$ field isomorphism $\varphi : E_1 \xrightarrow{\sim} E_2$ which restricts to the identity of F, i.e. $\varphi|_F = id_F$.

<u>Proof:</u>

⌈<u>Def 128:</u> Let $E|F$ be a field extension and $\alpha \in E$ alg./F.
We call the polynomial $P_\alpha \in F[X] \setminus F$ monic and of minimal degree s.t. $P_\alpha(\alpha) = 0$

the minimal polynomial of α over F.
P_α is automatically irreducible.]

Now we start the proof of Corollary 127.

Prop. 126 $\Rightarrow$ $\exists\ \varphi : E_1 \hookrightarrow E_2$ field homom:

$\varphi|_F = id_F$.

<u>Claim:</u> φ is surjective.

<u>Proof:</u> Assume for deriving a contradiction that φ is not surjective.

$\Rightarrow \exists\ \alpha \in E_2 \setminus \varphi(E_1)$.

Let P_α be the minimal polynomial of α over $\varphi(E_1)$.

E_1 is algebraically closed $\Rightarrow$ $\varphi(E_1)$ too.

$\Rightarrow$ All roots of P_α lie in $\varphi(E_1)$.

$\Rightarrow$ $\alpha \in \varphi(E_1)$ $\lightning$. $\square$ (Claim)

$\square$ Cor 127.

<u>Def 129:</u> Let $E|F$ be a field extension. We define a algebraic closure of F in E to be $\overline{F}^{alg,E} := \{\alpha \in E \mid \alpha \text{ algebraic over } F\}$

Homework shows that $\overline{F}^{alg\,E}$ is an extension field of F in E. We also just write $\overline{F}^E$.

(Idea for the homework: $\alpha, \beta \in \overline{F}^E$.

$\Rightarrow \dim_F F(\alpha, \beta) < \infty$ and

$\alpha \pm \beta$, $\alpha \cdot \beta$ and $\frac{\alpha}{\beta}$ $(\beta \neq 0)$ $\in F(\alpha, \beta)$

So $\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ $(\beta \neq 0)$ $\in \overline{F}^E$)

<u>Examples</u>: 1) $\mathbb{Q} \subseteq \mathbb{C}$.

$\overline{\mathbb{Q}}^{\mathbb{C}}$ is an algebraic closure of $\mathbb{Q}$.

2) $E = \mathbb{Q}(\sqrt{2} + \sqrt[3]{3}, \pi)$

Note π is transcendental over $\overline{\mathbb{Q}}^{\mathbb{C}}$, in particular over $\mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$.

<u>Claim</u>: $\overline{\mathbb{Q}}^E = \mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$.

<u>Proof</u>: "$\supseteq$" ✓ because $\sqrt{2} + \sqrt[3]{3}$ is algebraic over $\mathbb{Q}$.

Write $L := \mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$.

We have $E = L(\pi)$. Assume that there is an element in $L(\pi) \setminus L$ which is algebraic over $\mathbb{Q}$.

Then this element is algebraic over L.
But in $L(X)$ ($\simeq L(\pi)$) there is no element ~~aa~~ outside L which is algebraic.

$$\left(\sum_{i=0}^{d} b_i \frac{P(X)^i}{Q(X)^i} = 0 \qquad (b_d = 1) \text{ and } d \geq 1, Q \neq 0 \right.$$

P and $Q \in L[X]$ co-prime s.t. $\frac{P}{Q} \notin L$

Then $\sum_{i=0}^{d} b_i Q^{d-i} P^i = 0$

$\Rightarrow Q \mid P^d \Rightarrow Q \in L^\times$, because

P and Q are co-prime.!

So $P(X)$ is algebraic over L ↯

because $\deg P \geq 1$, by $\frac{P}{Q} \notin L$. $\Big)$

Thus the assumption is false and thus we have $\overline{\mathbb{Q}}^E = \mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$ $\square$

3) There are infinitely many countable algebraically closed fields in $\mathbb{C}$.
Because if $F \subseteq \mathbb{C}$ is alg. closed and countable (e.g. $\overline{\mathbb{Q}}^{\mathbb{C}}$)

— 2 —

Then $F \neq \mathbb{C}$ and an element $\alpha \in \mathbb{C} \setminus F$ is transcendental over F and $F(\alpha)$ is countable, so $\overline{F(\alpha)}^{\mathbb{C}}$ is countable (homework)

This way we get

$$\underbrace{\overline{\mathbb{Q}}^{\mathbb{C}}}_{F_0} \subsetneq \underbrace{\overline{\overline{\mathbb{Q}}^{\mathbb{C}}(\alpha_1)}^{\mathbb{C}}}_{F_1} \subsetneq F_2 \subsetneq F_3 \subsetneq \dots$$

with $F_{i+1} = \overline{F_i(\alpha_{i+1})}^{\mathbb{C}}$.

4) For every prime number p and every $n \in \mathbb{N}$ there exists a finite field of cardinality p^n.

$$\mathbb{F}_{p^n} := \{\alpha \in \overline{\mathbb{F}_p}^{alg} \mid \alpha^{p^n} = \alpha\} \quad \text{for } n > 1$$

and $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

$\mathbb{F}_{p^n}$ is a subfield of $\overline{\mathbb{F}_p}^{alg}$: $\quad char(\mathbb{F}_p) = p$

$\alpha, \beta \in \mathbb{F}_{p^n} \Rightarrow (\alpha \pm \beta)^{p^n} = \alpha^{p^n} + (-\beta)^{p^n}$

$= \alpha^{p^n} \pm \beta^{p^n}$

if $p = 2$ then $-1 = 1$!

$= \alpha \pm \beta$

$\beta \neq 0 \quad (\alpha \cdot \beta)^{p^n} = \alpha \cdot \beta$

$\left(\frac{\alpha}{\beta}\right)^{p^n} = \frac{\alpha}{\beta}$

end lecture 24

- $0, 1 \in \mathbb{F}_{p^n}$.

$\mathbb{F}_{p^n}$ has p^n elements because $P = X^{p^n} - X$ has no double roots, because ~~if it~~ would have then P and P' would have a common root, but $\gcd(X^{p^n} - X, -1) = 1$.

<u>Prop 130:</u> 1) Let E_1 and E_2 be two finite fields of the same cardinality. Then $E_1 \simeq E_2$.

2) $\exists!$ field of cardinality $|E_1|$ contained in $\overline{\mathbb{F}_{char(E_1)}}$. $\square$

<u>Proof:</u> exercise

<u>Example:</u> 1) $\mathbb{F}_{p^n}$ is a factor ring of $\mathbb{Z}[X]$:

<u>Proof:</u> $\mathbb{F}_{p^n}^\times = \langle \alpha \rangle$ is cyclic.

$$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{F}_{p^n}$$
$$P \longmapsto P(\alpha)$$

is a surjective ring homomorphism.

$\overset{\text{Homom. Theorem}}{\Longrightarrow}$ $\mathbb{Z}[X] / \ker(\varphi) \simeq \mathbb{F}_{p^n}$. $\square$

What is the minimal polynomial of α over $\mathbb{F}_p$?

Claim $P_{\alpha, \mathbb{F}_p} = \overbrace{(X-\alpha)(X-\alpha^p)\cdots(X-\alpha^{p^n})}^{=:Q}$.

Proof: Consider $\varphi_p : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$

$$\varphi_p(x) := x^p$$

the "Frobenius automorphism of $\mathbb{F}_{p^n}$".

This is a field automorphism.

(It is a field homomorphism, in particular injective. $\mathbb{F}_{p^n}$ is finite $\Rightarrow$ φ_p is bijective.)

We have $\varphi_p(Q) = Q$, so

the coefficients of Q lie in $\mathbb{F}_p$.

Further we have

$$\mathbb{F}_p[X] \big/ (P_{\alpha, \mathbb{F}_p}) \simeq \mathbb{F}_p[\alpha] = \mathbb{F}_{p^n}$$

So $n = \dim_{\mathbb{F}_p} \mathbb{F}_{p^n} = \dim_{\mathbb{F}_p} \mathbb{F}_p[X] \big/ (P_{\alpha, \mathbb{F}_p})$

$$= \deg(P_{\alpha, \mathbb{F}_p}).$$

Thus $\deg(Q) = \deg(P_{\alpha, \mathbb{F}_p})$.

Both are monic and $P_{\alpha,\mathbb{F}_p} \mid Q$.

$\Rightarrow \quad P_{\alpha,\mathbb{F}_p} = Q$. $\square$

2) There is only one field of cardinality p^n in $\overline{\mathbb{F}_p}^{alg}$. Therefore, for every field automorphism φ of $\overline{\mathbb{F}_p}^{alg}$, we have $\varphi(\mathbb{F}_{p^n}) = \mathbb{F}_{p^n}$.

III 4. Separable field extensions

Question: Given a field extension $E|F$ and an algebraic closure $\overline{F}^{alg}$ of F. Suppose $E|F$ is algebraic. How many field homomorphisms extending id_F exist from E into $\overline{F}$?

nw.: We just write field homom. from $E_1|F$ to $E_2|F$ later, meaning F-linear field homom. from E_1 to E_2.

diagram:

$$\begin{tikzcd} E_1 \arrow[r] & E_2 \\ F \arrow[u, "\mathrm{incl}"] \arrow[r, "\mathrm{id}_F"'] \arrow[ur, phantom, "\circlearrowleft"] & F \arrow[u, "\mathrm{incl}"'] \end{tikzcd}$$

Prop 131: Let $E|F$ be a finite algebraic extension. Then there exists at most $[E:F]$ many field homomorphisms from $E|F$ to $\overline{F}|F$.

Proof: We prove the following statement. Let E_1 be an intermediate field between E and F and $\varphi_1 : E_1|_F \hookrightarrow \overline{F}|F$ a field homomorphism.

Then $\exists$ at most $[E:E_1]$ many $\varphi: E/F \hookrightarrow \bar{F}/F$ extending φ_1.)

i.e. $\varphi|_{E_1} = \varphi_1$.

We prove by induction on $[E:E_1]$.

$\underline{[E:E_1] = 1:}$ ✓

$\underline{[E:E_1] > 1:}$ Take an element $\alpha \in E \setminus E_1$.

$\underline{\text{Firstly}}$: For every extension

$$\varphi_2 : E_2 := E_1[\alpha] \longrightarrow \bar{F} \text{ of } \varphi_1$$

there exist at most $[E:E_2]$ many extensions to E by (IH).

We have $[E:E_1] = [E:E_2][E_2:E_1]$.

So we only need to show:

$\underline{\text{Secondly}}$: There exist at most

$[E_2:E_1]$ many extensions of φ_1

to E_2.

If $E_2 \subsetneqq E$ then we can use the (IH). So we only have to consider $E = E_2 = E_1[\alpha]$.

Now $\deg(P_{\alpha,E_1}) = [E:E_1]$

For every $\varphi : E|F \longrightarrow \overline{F}|F$ extending φ_1 we have $\varphi(\alpha)$ is a root of $\varphi_1(P_{\alpha,E_1})$.

$$\Big(\varphi_1(P_{\alpha,E_1})(\varphi(\alpha)) = \varphi(P_{\alpha,E_1})(\varphi(\alpha)) = \varphi(P_{\alpha,E_1}(\alpha)) = \varphi(0) = 0 \Big)$$

$$\deg(\varphi_1(P_{\alpha,E_1})) = \deg P_{\alpha,E_1} = [E:E_1].$$

So there are almost $[E:E_1]$ choices for $\varphi(\alpha)$..

φ is uniquely determined by α and φ_1.

$\square$

Let $E|F$ be an algebraic field extension.

__Def. 132:__

1) $\alpha \in E$ is called separable over F if there exist $[F(\alpha):F]$ many field homomorphisms $F[\alpha]|F \hookrightarrow \overline{F}|F$.

2) We call $E|F$ separable if every element of E is separable over F.

__Def. 133:__ Let $P \in F[X]$ be given. We define

$$\frac{dP}{dX} = \sum_{i=1}^{d} i a_i X^{i-1} \in F[X] \text{ if } P \text{ has the form } P = \sum_{i=0}^{d} a_i X^i.$$

Example: a) $F := \mathbb{F}_p(X)$. $\alpha \in \overline{F}$ s.t.

$\alpha^p = X$.

Then $F[\alpha] | F$ is not separable.

Proof: An extension φ of $F \xhookrightarrow{\text{incl.}} \overline{F}$ to $F[\alpha]$

must satisfy $\varphi(\alpha)^p = \varphi(\alpha^p) = \varphi(X) \underset{X \in F.}{=} X$

and two elements $t_1, t_2 \in F[\alpha]$ satisfying

$t_1^p = X = t_2^p$, i.e. $0 = t_1^p - t_2^p \underset{\text{char } F = p}{=} (t_1 - t_2)^p$,

must coincide.

Thus there is only one extension φ.

But $[F[\alpha] : F] > 1$, because $\alpha \notin F$,

because otherwise $\alpha = \dfrac{P(X)}{Q(X)}$, $\gcd(P, Q) = 1$

and $Q \neq 0$, and thus $(Q(X))^p X = P(X)^p$

$\Rightarrow X \mid P(X)$ (X is a prime element)

$\Rightarrow X^p \mid (Q(X))^p X \overset{p>1}{\Longrightarrow} X \mid Q(X)$

$\Rightarrow X \mid \gcd(P, Q) = 1$ ↯. $\square$

b) $\sqrt{2}$ is separable over $\mathbb{Q}$. Take $\overline{\mathbb{Q}} \subseteq \mathbb{C}$

$\mathbb{Q}[\sqrt{2}] \hookrightarrow \overline{\mathbb{Q}}$: $\varphi_1(a+\sqrt{2}\,b) := a+\sqrt{2}\,b$. (inclusion.)

$\varphi_2(a+\sqrt{2}\,b) := a-\sqrt{2}\,b$.

$\varphi_2((a+\sqrt{2}\,b)(c+\sqrt{2}\,d)) = \varphi_2(ac+2bd+\sqrt{2}(ad+bc))$

$= ac+bd-\sqrt{2}(ad+bc)$

$= (a-\sqrt{2}\,b)(c-\sqrt{2}\,d) = \varphi_2(a+\sqrt{2}\,b)\,\varphi_2(c+\sqrt{2}\,d)$.

$\Rightarrow$ φ_2 is a ring homorphism.

$\varphi_2(1)=1$ $\Rightarrow$ φ_2 is a field homomorphism.

In fact $\mathbb{Q}[\sqrt{2}]\,|\,\mathbb{Q}$ is separable.

Prop. 13.4: Let $E|F$ be an algebraic field extension and $\alpha \in E$. Let $\overline{F}$ be an alg. closure of F.
Then are equivalent:

1° α is separable over F.

2° $F[\alpha]|F$ is separable over F

3° $P_{\alpha,F}$ has $\deg P_{\alpha,F}$ pairwise different roots in $\overline{F}$. (i.e. $P_{\alpha,F}$ has no double root in $\overline{F}$)

4° $P_{\alpha,F}$ and $\dfrac{d P_{\alpha,F}}{d X}$ are coprime.

Proof: 1° ⇒ 2°: Take $\beta \in F[\alpha]$.

We have at most $[F[\beta]:F]$ extensions of $F \xrightarrow{\text{incl}} \overline{F}$ to $F[\beta]$ and at most $[F[\alpha]:F[\beta]]$ extensions of each of those to $F[\alpha]$, so to be able to have $[F[\alpha]:F]$ extensions we need $[F[\beta]:F]$ extensions to $F[\beta]$, because $[F[\alpha]:F] = [F[\alpha]:F[\beta]][F[\beta]:F]$.

So β is separable over F.

2° ⇒ 1°: ✓ by definition.

$1^\circ \Rightarrow 3^\circ$: $\quad d := [F[\alpha] : F]$

Let $\varphi_1, \dots, \varphi_d$ be the extensions of $F \xhookrightarrow{\text{incl}} \overline{F}$ to $F[\alpha]$.

We have $\quad F[X]\big/(P_{\alpha,F}) \xrightarrow{\sim} F[\alpha]$, $\quad [X]_{(P_{\alpha,F})} \longmapsto \alpha$

__Claim__: $\deg(P_{\alpha,F}) = [F[\alpha] : F] = d$ ~~and~~

__Proof__: $[X^{\deg(P_{\alpha,F})-1}]_{(P_{\alpha,F})}, \dots, [X^2]_{(P_{\alpha,F})}, [X]_{(P_{\alpha,F})}, [1]_{(P_{\alpha,F})}$

is an F-basis of

$F[X]\big/(P_{\alpha,F})$. So $1, \alpha, \dots, \alpha^{\deg(P_{\alpha,F})-1}$ is an

F-basis of $F[\alpha]$ and therefore

$$[F[\alpha] : F] = \deg(P_{\alpha,F}) \qquad \square \text{ (Claim)}$$

φ_i is determined by $\varphi_i(\alpha)$ and $\varphi_i\big|_F = \text{incl}_{F \hookrightarrow \overline{F}}$.

$\varphi_1, \dots, \varphi_d$ are pairwise different $\Rightarrow$ $\varphi_1(\alpha), \dots, \varphi_d(\alpha)$ are pairwise different.

$$P_{\alpha,F}(\varphi_i(\alpha)) = \sum_{j=0}^{d} a_j(\varphi_i(\alpha))^j \underset{\uparrow}{=} \varphi_i\left(\sum_{j=0}^{d} a_j \alpha^j\right)$$

φ_i is a ring homomorphism and $\varphi_i(a_j) = a_j$

$$= \varphi_i(P_{\alpha,F}(\alpha)) = \varphi_i(0_F) = 0_F.$$

Thus $P_{\alpha,F}$ has d different roots in F.

end lecture 25

$3^\circ \Rightarrow 4^\circ$: $P_{\alpha,F} = (X - \alpha_1)(X - \alpha_2)\cdot\ldots\cdot(X - \alpha_d)$

s.t. $\alpha_i \neq \alpha_j$ for $i \neq j$. $1 \leq i, j \leq d = \deg(P_{\alpha,F})$.

$$\frac{dP_{\alpha,F}}{dX} = \sum_{j=1}^{d} (X - \alpha_1)\cdot\ldots\cdot\widehat{(X - \alpha_j)}\cdot\ldots\cdot(X - \alpha_d).$$

Let Q be the (monic) gcd of $P_{\alpha,F}$ and $\frac{dP_{\alpha,F}}{dX}$.

If $\deg Q \geq 1$ then Q has a root in F, say w.l.o.g. α_1. Then

$$0 = \frac{dP_{\alpha,F}}{dX}(\alpha_1) = (\alpha_1 - \alpha_2)\cdot\ldots\cdot(\alpha_1 - \alpha_d) \neq 0 \ \lightning.$$

Thus $Q = 1$.

$\underline{4^\circ \Rightarrow 3^\circ}$: $\quad P_{\alpha,F} = (X - \alpha_1)^{\nu_1} \cdots (X - \alpha_\ell)^{\nu_\ell}$

$\nu_1, \dots, \nu_\ell \geq 1$, $\ell \leq \deg(P_{\alpha,F})$, $\alpha_i \neq \alpha_j \ \forall i \neq j$.

If $\nu_1 \geq 2$ then $(X - \alpha_1)$ divides

$\frac{dP_{\alpha,F}}{dX}$ in $\overline{F}[X]$, so α_1 is a root of $\frac{dP_{\alpha,F}}{dX}$,

so α_1 is a root of $\gcd\left(P_{\alpha,F}, \frac{dP_{\alpha,F}}{dX}\right)$ by Bézout.

So the gcd of $P_{\alpha,F}$ and $\frac{dP_{\alpha,F}}{dX}$ has degree ≥ 1 ↯

to $\gcd\left(P_{\alpha,F}, \frac{dP_{\alpha,F}}{dX}\right) = 1$. Thus $\ell = \deg(P_{\alpha,F})$ and

$\nu_1 = \dots = \nu_\ell = 1$. $\Rightarrow 3^\circ$.

$\underline{3^\circ \Rightarrow 1^\circ}$: We extend $\quad F \xrightarrow{\text{incl}} \overline{F}$

via $\alpha \longmapsto \alpha_i$

$$\varphi_i\left(\sum_{j=0}^{t} b_j \alpha^j\right) := \sum_{j=0}^{t} b_j \alpha_i^j$$

Well-defined: Suppose $P_1(\alpha) = P_2(\alpha)$,

$P_1, P_2 \in F[X]$. Then $P_{\alpha,F} \mid P_1 - P_2$, because $(P_{\alpha,F}) \ni P_1 - P_2 ..$

$$\begin{array}{c} (P_{\alpha,F}) \\ \parallel \\ \{P \in F[X] \mid P(\alpha) = 0\} \end{array}$$

<u>(vanishing ideal of α in $F[X]$)</u>

$\Rightarrow (P_1 - P_2)(\alpha_i) = 0$

$\Rightarrow \varphi_i(P_1(\alpha)) = P_1(\alpha_i) = P_2(\alpha_i) = \varphi_i(P_2(\alpha))$ □

<u>Example:</u>

1) If $E|F$ is algebraic and $\mathrm{char.}(F) = 0$, then E/F is separable.

<u>Proof:</u> If for $\beta \in E$. $\gcd\left(P_{\beta,F}, \frac{d P_{\beta,F}}{dX}\right) \neq 1$

then this gcd has to be $P_{\beta,F}$, because the only monic divisors of $P_{\beta,F}$ are $P_{\beta,F}$ and 1.

$\Rightarrow P_{\beta,F} \mid \frac{d P_{\beta,F}}{dX}$. But

$\deg \frac{d P_{\beta,F}}{dX} < \deg P_{\beta,F}$

So $\dfrac{dP_{\beta,F}}{dX} = 0.$

Thus $P_{\beta,F}$ is constant, i.e. $\in F$,

because char $F = 0$. $\lightning$ $\deg P_{\beta,F} \geq 1$.
$\square$

2) $\mathbb{F}_{p^n} | \mathbb{F}_p$ is separable, for all prime numbers p and all $n \in \mathbb{N}$. (homework)

Prop 135: Let $E|F$ be algebraic and E_1 be an intermediate field. T.a.e.:

1° E/F is separable

2° E/E_1 and E_1/F are separable.

Proof: $1^\circ \Rightarrow 2^\circ$. E_1/F separable ✓ by definition

E/E_1: $\beta \in E \Rightarrow P_{\beta, E_1} \mid P_{\beta,F}$

So P_{β,E_1} has no double root in $\overline{E}$, so is separable $/E_1$.

$2^\circ \Rightarrow 1^\circ$ $\beta \in E$. Let $a_0, \dots, a_d$ be the coefficients of $P_{\beta, E_1} \in E_1[X] \setminus E_1$.