Dem. (1) $X^{p^n}-X \in (\mathbb{Z}/p\mathbb{Z})[X]$ es separable,
ya que $D(X^{p^n}-X) = -1$.
Por 4.1.4 y 3.5.1 (char. de extn. de Gal)
sigue la afirmación.
(2) Por el teorema principal de teoría de Gal:
$|\mathrm{Aut}(K)| = |\mathrm{Aut}(K/\mathbb{Z}/p\mathbb{Z})| = n$.
$\Rightarrow$ Basta verificar que $|\langle F \rangle| = n$;
Sea $a \in K^*$ generador del grupo cíclico K^*.
entonces $F^i(a) = a^{(p^i)}$ son el diferentes
para $i = 0, 1, \ldots, n-1$

Cor. Sea p un número primo, y $n \in \mathbb{N}_+$. Si K
es un campo con p^n elementos, y F su autom. de
Frobenius, entonces
$\mathrm{Fix}(K, \langle F^i \rangle)$, $i \in \mathbb{N}$, $i | n$ son
precisamente los subcampos de K.

Obs. Los campos con p^n elementos se denotan
muchas veces con $\mathbb{F}_{p^n}$ o $GF(p^n)$,

Galois field

4.2. El teorema del elemento primitivo

4.2.1 Obs. Si k es un campo finito
entonces cada extn. finita $K \supset k$ es
simple, i.e. $\exists a \in K : K = k[a]$
"a es el. primitivo".

$\overset{k \text{ es finito}}{\Rightarrow}$
Claro, porque K^* es cíclico.

<u>4.2.2 Prop.</u> Una extn. $K \supset k$ de campos es simple y alg $\iff$ $K \supset k$ solo tiene un # fin. de campos intermedios

<u>Dem</u> (idea)

"$\Rightarrow$" Sea $K = k(a)$, $f \in k[X]$ pol. min ~~sobre~~ de a/k.

$f \in K[X]$ solo tiene # fin. de divisores ~~normados~~ mónicos porque $K[X]$ es fact.

Sea $\mathcal{Z}$ el conjunto de campos intermedios de $K \supset k$ y $\mathcal{D}$ el conjunto de divisores ~~normados~~ mónicos de $f \in K[X]$

$\mathcal{Z} \to \mathcal{D}$, $L \mapsto$ pol mín. de a/L es inyectivo!

"$\Leftarrow$" $K \supset k$ es alg (extn. transc. tiene infinidad de campos intermedios por 1.6.2) y finita i.e.

$K = k[a_1, \dots, a_n]$.

Si k es fin la afirmación sigue de la obs. 4.2.1.

En otro caso procedemos por ind. / n

Sea $K = k(a_1, a_2)$ entonces

$k_x := k(a_1 + x a_2)$ $\forall x \in k$

k infinito $\overset{\text{fin}}{\Rightarrow}$ $\exists\, x \neq y$: $k_x = k_y \Rightarrow$

$a_1 + y a_2 \in k_x \Rightarrow \underset{(a_1 + x a_2) - (a_1 + y a_2)}{\underset{\shortparallel}{(x-y) a_2}} \in k_x \Rightarrow a_2 \in k_x \Rightarrow a_1 \in k_x$

$\Rightarrow k(a_1, a_2) = k(a_1 + x a_2) \dots$

4.2.3 Cor. (Teorema del Elemento Primitivo) Cada extn fin y sep. es trav. con el primit.
En. part. cada extn. de Gal. sea simple
y si char$(\mathbb{Q})=0$ cada extn. finita es simple

Dem. $K = \mathbb{Q}(a_1, \dots, a_n)$ con $a_1, \dots, a_n$ sep. $/\mathbb{Q}$.

$\overset{3.5.5}{\Longrightarrow}$ $\exists L \supset K$ t.q. $L \supset \mathbb{Q}$ Gal

solo trav. #fin de campos intermedios $\Rightarrow$ $K \supset \mathbb{Q}$ solo #fin de cuerpos intermedios

$\overset{4.2.2}{\Longrightarrow}$ $K \supset \mathbb{Q}$ trav. simple. $\square$

4.3. Raíces unitarias

4.3.1. Def. Sea K un campo y $n \in \mathbb{N}_+$.
$a \in K$ se llama <u>n-ésima raíz unitaria</u> en K
si $a^n = 1$,
i.e. si a es cero del polinomio $X^n - 1 \in K[X]$.
Denotamos con K_n el campo de desc. de $X^n - 1$,
y con $E_n(K) < K_n^*$ los ceros de $X^n - 1$

4.3.2. Obs. Sea $n \in \mathbb{N}_+$, entonces vale

(1) $\{e^{2\pi i k/n} \mid k = 0, 1, \dots, n-1\} \subset \mathbb{C}$ es el conjunto de las raíces n-ésimas en $\mathbb{C}$.

(2) Si p es un primo, entonces cada elemento de $(\mathbb{F}_{p^n})^*$ es $(p^n - 1)$-ésima raíz unitaria

(3) Si K es un campo y $d \in \mathbb{N}$ con $d \mid n$ entonces podemos identificar K_d como un sub-campo de K_n

(4) Si char$(\mathbb{Q}) = p > 0$ entonces $K_n = K_{np}$

(5) $E_n(K)$ es un subgrupo cíclico con K^*
$|E_n(K)| = n \Leftrightarrow$ char$(K) \nmid n$

(6) $K_n \supset K$ es extn. de Gal. (use (3) $\Rightarrow$ sep.) (4): podemos suponer

4.3.3 Def. Sea $n \in \mathbb{N}_+$, ~~el grupo~~ denotamos a ~~grupo~~ ~~$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$~~ $(\mathbb{Z}_n)^*$ el grupo de las unidades de $\mathbb{Z}/n\mathbb{Z}$.

$\varphi(n) := |\{ m \in \mathbb{N} \mid 1 \leq m \leq n \wedge \mathrm{mcd}(m,n) = 1\}|$

"función φ de Euler"

4.3.4 Prop.

(1) $\forall n \in \mathbb{N}_+ : \quad \mathbb{Z}_n^* = \{ m + n\mathbb{Z} \mid \mathrm{mcd}(m,n) = 1\}$

(2) $|\mathbb{Z}_n^*| = \varphi(n)$

(3) Si $\mathrm{mcd}(m,n) = 1$ entonces $\varphi(mn) = \varphi(m)\varphi(n)$ y $\mathbb{Z}_{mn}^* = \mathbb{Z}_m^* \times \mathbb{Z}_n^*$

(4) $\varphi(p^n) = p^{n-1}(p-1)$

(5) $\mathbb{Z}_{p^n}^* \cong \begin{cases} C_{p-1} \times C_{p^{n-1}} & p \neq 2 \\ C_2 \times C_{2^{n-2}} & p = 2,\ n \geq 2 \end{cases}$

4.3.5 Def. Sea K un campo y $n \in \mathbb{N}_+$ una n-ésima raíz $\xi \in K_n$ se llama primitiva si $|\langle \xi \rangle| = n$ $\quad (\langle \xi \rangle < K^*)$

$PE_n(K) := \{ \xi \in E_n(K) \mid \xi \text{ primitiva}\}$

4.3.6 Obs. Sea K un campo $n \in \mathbb{N}_+$ t.q. $\mathrm{char}(K) \nmid n$, entonces:

1) $\xi \in PE_n(K) \Leftrightarrow \langle \xi \rangle = E_n(K)$

2) ~~Sea~~ $\xi \in PE_n(K)$ se tiene $\xi^m \in PE_n(K) \Leftrightarrow \mathrm{mcd}(m,n) = 1$.

$\Rightarrow |PE_n(K)| = \varphi(n)$

(3) ~~Si~~ Para $d \in \mathbb{N}_+$ con $d|n$ se tiene
$$E_d(K) < E_n(K) \text{ y}$$
$$PE_d(K) = \{\xi \in E_n(K) \mid |\langle \xi \rangle| = d\}$$

(4) $$E_n(K) = \dot{\bigcup_{\substack{d|n \\ d\geq 1}}} PE_d(K).$$

$\square$

4.3.7 Def. Sea K un campo, $n \in \mathbb{N}_+$ con $\mathrm{char}(K) \nmid n$. Sean $\xi_1, \dots, \xi_{\phi(n)}$ las n-ésimas ~~raizes~~ ~~unit~~ unitarias primitivas. Entonces el polinomio
$$\Phi_n(X) := \prod_{i=1}^{\phi(n)} (X - \xi_n)$$
se llama el <u>n-ésimo polinomio ciclotómico</u>.

4.3.8 Prop. Sea K un campo, $n \in \mathbb{N}_+$ con $\mathrm{char}(K) \nmid n$, entonces

(1) $\deg(\Phi_n) = \varphi(n)$

(2) $$X^n - 1 = \prod_{\substack{d|n \\ d\geq 1}} \Phi_d$$

(3) Los coeficientes de Φ_n están de la forma $m \cdot 1$ con $m \in \mathbb{Z}$

<u>Dem</u> (1) y (2) claro por def y 4.3.6.

(3) Inducción / n. <u>$n = 1$</u>: $\Phi_1 = X - 1$

<u>$n > 1$</u> Sea $\Phi'_n := \prod_{\substack{d|n}} \Phi_n \in (\mathbb{Z} \cdot 1)[X] \in K[X]$

$$\Phi_n \cdot \Phi'_n = X^n - 1 \underset{\substack{\uparrow \\ \text{div con res. en } (\mathbb{Z}\cdot 1)[X]}}{=} \overset{0<d<n}{} q \cdot \Phi'_n + r \quad \text{con } \deg(r) < \deg(\Phi'_n$$

$\Rightarrow \quad + = \Phi(q-\phi_n)\,\Phi_n' \quad \Downarrow \quad \square$

$\phi_1 = X-1$
$\phi_2 = X+1$
$\phi_3 = X^2+X+1$
$\phi_4 = X^2+1$
$\phi_6 = X^2-X+1$
$\phi_{10} = X^4-X^3+X^2-X+1$

<u>Obs.</u> Por (2) los ϕ_n se pueden calcular recursivamente. A pesar de la impresión para n pequeño, los coef. pueden ser arbitrariamente grandes.

<u>4.3.9 Prp.</u> Sea K un campo, $n \in \mathbb{N}_+$ con $char(K) \nmid n$, entonces existe un hom. inyectivo de grupos ι $Aut(K_n; K) \longrightarrow \mathbb{Z}_n^*$

$\sigma \longmapsto l + n\mathbb{Z}$ ~~[si $\sigma(\xi_1) = \xi_1^l$]~~ t.q. $\sigma(\xi_1) = \xi_1^{l_\sigma}$

Dem. estandar.

<u>4.3.10 Prp.</u> Sea $n \in \mathbb{N}_+$, $\Phi_n \in \mathbb{Z}[X]$ el n-ésimo pol. ciclotómico y $Q_n \supset Q$ el campo de desc. de $X^n-1 \in Q[X]$. Entonces

(1) $\Phi_n \in Q[X]$ es irreducible
(2) $[Q_n : Q] = \varphi(n)$
(3) $Aut(Q_n; Q) \cong \mathbb{Z}_n^*$.

<u>Obs.</u> (1) ~~es difícil~~ no es fácil, pero factible con nuestros medios, implica (2) y (3):

(2) Φ_n es por (1) el pol. mínimo de cualquier raíz ~~anom~~ n-ésima primitiva $\xi \in Q_n$. Por $Q_n = Q(\xi)$ tenemos $[Q_n : Q] = deg(\Phi_n) = \varphi(n)$

(3) Como $Q_n \supset Q$ es Galois, $|Aut(Q_n : Q)| = [Q_n : Q] = \varphi(n)$. Pero $Aut(Q_n : Q) \hookrightarrow \mathbb{Z}_n^*$ por 4.3.9 y $|\mathbb{Z}_n^*| = \varphi_n$. $\square$

4.4. Extensiones metacíclicas y ~~solución por radicales~~

4.4.1 Def. Sea $K \supset k$ una extensión de campos y L_1, L_2 campos intermedios de $K \supset k$. Entonces denotamos con $L_1 * L_2$ el mas pequeño campo intermedio L de $K \supset k$ con $(L_1 \cup L_2) \subset L$.

4.4.2 Lema Sea $K \supset k$ una extensión de campos y $L_1 \subset L_2$ y L campos intermedios de $K \supset k$.
Si $L_2 \supset L_1$ es ~~Gaextn.~~ de Galois entonces también $(L \cdot L_2) \supset (L \cdot L_1)$ lo es y
$Aut(L \cdot L_2 ; L \cdot L_1)$ es isomorfo a un subgrupo de $Aut(L_2 ; L_1)$.

Dem. Por hipotesis, L_2 es el campo de desc. de un polinomio separable $f \in L_1[X]$. Si adjuntamos a $L \cdot L_1$ todos los ceros de f, obtenemos $L \cdot L_2$.
Por eso $L \cdot L_2 \supset L \cdot L_1$ es normal y finito.
Un factor irreducible f' de f en $L_1[X]$ puede factorisar se en $(L \cdot L_1)[X]$, Pero como f' es separable, también sus factores en $(L \cdot L_1)[X]$ lo son $\Rightarrow (L \cdot L_2) \supset (L \cdot L_1)$ es extn. de Galois. Cada automorfismo $\sigma \in Aut(L \cdot L_2, L \cdot L_1)$ nos da por restricción un * automorfismo $\bar{\sigma} \in Aut(L_2 ; L_1)$. Obviamente, $\bar{?}$ es un hom. de grupos, que es inyectivo ya que en ambos casos un automorfismo es determinado por su efecto sobre los ceros de f. □

* $\sigma \in Aut(L \cdot L_2, L \cdot L_1)$ permuta los ceros de $f \in (L \cdot L_1)[X]$ y es determinado por eso. Pero los ceros de f estan en $L_2 \Rightarrow \sigma(L_2) \subset L_2$

4.4.3. Def. Una extensión $K \supset k$ de campos ~~se~~ es cíclica si $K \supset k$ es ~~gal.~~ extn. de Galois y $\mathrm{Aut}(K;k)$ es cíclico.
$K \supset k$ es metacíclica si existe una cadena de campos intermedios $k = L_0 \subset L_1 \subset \dots \subset L_n = K$ t.q. $L_i \supset L_{i-1}$ es cíclica para $i = 1, 2, \dots, n$.

4.4.4 Obs. Por la transitividad de la separabilidad, extensiones metacíclicas son separables.
Si $K \supset k$ es una extn. de Galois, entonces $K \supset k$ es metacíclica $\Leftrightarrow$ $\mathrm{Aut}(K;k)$ es soluble.

4.4.5 Lema Sean L_1, L_2 campos intermedios de la extn. de campos $K \supset k$.
Si $L_1 \supset k$ y $L_2 \supset k$ son metacíclicas, entonces también $(L_1 \cdot L_2) \supset k$ lo es.

Dem. Sean
$k = K_0' \subset K_1' \subset \dots \subset K_m' = L_1$ y
$k = K_0'' \subset K_1'' \subset \dots \subset K_n'' = L_2$ cadenas de campos intermedios como en la def. ~~de~~ 4.4.3.
Entonces, en la cadena
$k = K_0' \subset K_1' \subset \dots \subset K_m' = L_1 \subset L_1 K_1'' \subset \dots \subset L_1 \cdot K_n'' = L_1 \cdot L_2$
las extensiones $L_1 K_{i+1}'' \supset L_1 K_i''$ son cíclicas por el Lema 4.4.2.

4.4.6. Sea $K \supset k$ una extn. metacíclica. Entonces $K \supset k$ es separable y finita.

$\overset{3.5.5.}{\Longrightarrow}$ $\exists L \supset K$ t.q. $L \supset k$ es extn. de Galois,

Sean $\{\varphi(K) \mid \varphi \in Aut(L, k)\} = \{K_1, \dots, K_n\}$ los campos intermedios de $L \supset k$ que son conjugados a K, entonces

$K^+ := K_1 \cdot K_2 \cdot \ldots \cdot K_n$ es metacíclico por 4.4.5

y $K^+ \supset k$ es extn. de Galois, ya que
$$Fix(L, K^+) = \bigcap_{\varphi \in Aut(L,k)} \varphi \circ Fix(L, K) \circ \varphi^{-1} \triangleleft Aut(L, k).$$

K^+ se llama la envolvente de Galois de K.

4.5. Solución por Radicales

Sea k un campo. Una equación $X^n - a = 0$ $(a \in k^*)$ se llama equación pura. Si $p := char(k)$ y $p \nmid n$ entonces $f := X^n - a$ es un polinomio separable

4.5.1. Prp. Para $n \in \mathbb{N}_+$ con $p \nmid n$ ($p = char(k)$) sea $k_n = k$ (i.e. k contiene ya todas las n-esimas raíces unitarias) entonces

(a) $Gal(X^n - a, k)$ es cíclico $(a \in k^*)$

(b) Para cada extensión cíclica $K \supset k$ existe $\alpha \in K$ con $K = k[\alpha]$ y $\alpha^n \in k$.

Obs. Si $X^n - a \in \mathbb{Q}[X]$ irred. (en part. $a \neq 1$ si $n \geq 2$)

$\Longrightarrow Gal(X^n - a, \mathbb{Q}) = (\mathbb{Z}_n^+) \rtimes_\varphi \mathbb{Z}_n^*$ $\quad \varphi: \mathbb{Z}_n^* \xrightarrow{\sim} Aut(\mathbb{Z}/n\mathbb{Z}, +)$ $\quad a \mapsto a\cdot$ $\quad \nabla$

Pf. (1) Sea $K \supset k$ el campo de desc. de $X^n - a \in k[X]$.

$\xi \in k$ una n-ésima raiz unitaria primitiva.

Si $\alpha \in K$ es un cero de $X^n - a$, entonces $\{\alpha, \xi\alpha, \dots, \xi^{n-1}\alpha\}$ es el conjunto de todos los ceros de $X^n - a$. Por eso, $K = k(\alpha)$

Entonces, cada $\sigma \in Aut(K, k)$ es únicamente determinado por $\sigma(\alpha) = \xi^m \alpha$, es decir por la clase lateral $m + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$.

$\Longrightarrow$ Tenemos un hom. inyectivo de grupos

$Aut(K, k) \longmapsto (\mathbb{Z}/n\mathbb{Z}, +)$

(2) Sea $Aut(K, k) = \langle \sigma \rangle$, $\xi \in k$ ~~una~~ n-ésima raiz unitaria primitiva.

Los automorfismos $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ son elementos K-lin. indep. en ~~el~~ $Hom_k(K, K)$ (3.2.7)

Por eso, existe $x \in K$ ~~con~~ donde ~~la~~ "resolvente de Lagrange"

$(\xi, x) := x + \xi\sigma(x) + \xi^2\sigma^2(x) + \dots + \xi^{n-1}\sigma^{n-1}(x) \neq 0$

Ahora, observamos

$\sigma(\xi, x) = \sigma(x) + \xi\sigma^2(x) + \dots + \xi^{n-1} x = \xi^{-1}(\xi, x)$

$\Longrightarrow \sigma((\xi, x)^n) = (\sigma(\xi, x))^n = \xi^{-n}(\xi, x)^n = (\xi, x)^n$

$\Longrightarrow (\xi, x)^n \in k$

De $\sigma^m(\xi, x) = \xi^{-m}(\xi, x)$ $(m = 0, 1, \dots, n-1)$

vemos que ~~la~~ $|Aut(k[(\xi, x)], k)| \geq n$

Como $[K : k] = n$ necesariamente $K = k[(\xi, x)]$. $\square$

4.5.2. Def. Se dice que ~~la~~ una extn. de campos $K \supset k$ es una <u>extensión por radicales</u> si $K = k(a_1, a_2, \dots, a_n)$ y $a_1^{e_1} \in k$, $a_i^{e_i} \in k(a_1, \dots, a_{i-1})$ $i = 2, 3, \dots, n$ $(e_1, \dots, e_n \in \mathbb{N}_+)$

4.5.3 Prop. Sea K un campo, $f \in K[X]$ irreducible y $L \supset K$ el campo de descomposición de f y $G := \mathrm{Aut}(L/K)$. Sea un grupo soluble, con $n := |G|$ y $\mathrm{char}(K) \nmid n$. Entonces $L_{(n)} \supset K$ es una extensión por radicales. (donde se descompone f en factores lineales) (campo de desc. de $X^n - 1 \in L[X]$).

<u>Dem.</u> Como G es soluble, tenemos una serie normal $G = N_0 \trianglerighteq N_1 \supset \dots \supset N_e = \{e\}$ con N_{i-1}/N_i cíclico de orden primo p_i $(i = 1, 2, \dots, e)$. Por el teorema principal de teoría de Galois, esto corresponde a una cadena de campos intermedios

$$K = L^{(0)}_0 \subset L^{(1)}_1 \subset \dots \subset L^{(e)}_e = L$$

donde cada $L^{(i)}_i \supset L^{(i-1)}_{i-1}$ es una extn. cíclica de grado p_i

$[\; L^{(i)} = \mathrm{Fix}(L, N_i)$ y $N_i = \mathrm{Aut}(L, L^{(i)})$

$N_1 \trianglelefteq N_0 \Rightarrow L_1 \supset L_0 = K$ Gal y $\mathrm{Aut}(L_1^{(1)}, L_0^{(0)}) \cong N_0/N_1$ cí

$L = L^{(e)} \supset L^{(1)}_1$ Gal, $\mathrm{Aut}(L^{(e)}, L^{(1)}) = N_1 \trianglerighteq N_2$

$\Rightarrow L^{(2)}_2 \supset L^{(1)}_1$ Gal y $\mathrm{Aut}(L^{(2)}_2, L^{(1)}_1) \cong N_1/N_2$ cícl... $]$

Podemos identificar K_n como un subcampo de L_n entonces $L_n = K_n \cdot L$.
Además $K_{p_i} \subset K_n$ y $p_i \neq char(K)$ $\forall i$.
En la cadena de campos

$$K_n = K_n \cdot L^{(0)} \subset K_n L^{(1)} \subset \dots \subset K_n \cdot L^{(e)} = L_n,$$

las extensiones $K_n \cdot L^{(i)} \supset K_n \cdot L^{(i-1)}$ son cíclicas por el Lema 4.4.2. $i=1,2,\dots,e$
Por Prop. 4.5.1 existen $a_i \in K_n \cdot L_i$ t.q. $a_i^{p_i} \in K_n \cdot L^{(i-1)}$ $\forall i = 1,\dots,e$
es decir $L_n \supset K_n$ es una extn. por radicales. Pero $K_n \supset K$ también es extn. por radicales (trivial)
$\Rightarrow L_n \supset K$ es extn. ~~por~~ por radicales $\square$

4.5.4. Prop. Sea k un campo con $char(k) = 0$ y $f \in k[X]$ irreducible. Si f tiene un cero en una extensión por radicales $K \supset k$, entonces $Gal(f, k)$ es un grupo soluble.

~~Sea K =~~

Dem: Sea $K = k(a_1, \dots, a_n)$ como en Def. 4.5.1
y $L^{(i)} := k(a_1, \dots, a_i)$ $i = 0, 1, \dots, n$
(y $a_i^{e_i} \in L^{(i-1)}$)

Sea $\mathscr{k} := l_1 \cdots l_n$ y K_l el campo de las ~~extensiones~~ ~~raíz~~ l-ésimas raíces unitarias ~~en K y~~ sobre K y ~~[illegible]~~ $\mathscr{k}_l \subset K_l$ el campo de las ~~raíces~~ l_i-ésimas raíces unitarias sobre $\mathscr{k}$,

$\mathscr{k}_{l_i} \subset \mathscr{k}_l \quad \forall i$

En la cadena de campos intermedios

$$\mathscr{k} \subset \mathscr{k}_l \subset \mathscr{k}_l L_1^{(1)} \subset \cdots \subset \mathscr{k}_l L_1^{(n)} = K_n$$

las extensiones $\mathscr{k}_l L^{(i)} \supset \mathscr{k}_l L^{(i-1)}$ son cíclicas por el Lema 4.4.2

y $\mathscr{k}_l \supset \mathscr{k}$ es abeliana

(i.e. $\mathrm{Aut}(\mathscr{k}_l, \mathscr{k})$ abeliano) por Prop. 4.3.9.

Por eso $K_n \supset \mathscr{k}$ es extr metacíclica.

$\overset{4.4.6}{\Longrightarrow}$ La envolvente de Galois $K^+ \supset K$ es metacíclica $/ \mathscr{k}$

$\Longrightarrow \mathrm{Aut}(K_n^+, \mathscr{k})$ es soluble.

El campo de descomposición Z de f esta contenido en K_n^+ ($K_n^+ \supset \mathscr{k}$ normal)

y $Z \supset \mathscr{k}$ es Gal.

$\Rightarrow \mathrm{Aut}(Z, \mathscr{k}) \cong \mathrm{Gal}(f, \mathscr{k})$ es soluble por ser un cociente de $\mathrm{Aut}(K_n^+, \mathscr{k})$.

$\square$