Testelmélet és Galois-elmélet

Egyenletek megoldása gyökjelekkel

2009. április 10.

Definíció: normállánc, normállánc faktorai, feloldható csoport

A G csoport **normálláncának** nevezzük G részcsoportjainak egy $G_0, \ldots, G_n$ sorozatát, amelyre

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

teljesül. A G_i/G_{i-1} faktorcsoportokat e normállánc **faktorainak** nevezzük; n a normállánc **hossza**.

Definíció: normállánc, normállánc faktorai, feloldható csoport

A G csoport **normálláncának** nevezzük G részcsoportjainak egy $G_0, \ldots, G_n$ sorozatát, amelyre

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

teljesül. A G_i/G_{i-1} faktorcsoportokat e normállánc **faktorainak** nevezzük; n a normállánc **hossza**.

Definíció: normállánc, normállánc faktorai, feloldható csoport

A G csoport **normálláncának** nevezzük G részcsoportjainak egy $G_0, \ldots, G_n$ sorozatát, amelyre

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

teljesül. A G_i/G_{i-1} faktorcsoportokat e normállánc **faktorainak** nevezzük; n a normállánc **hossza**.
Azt mondjuk, hogy a G csoport **feloldható**, ha G-nek van olyan normállánca, amelynek faktorai Abel-csoportok.

Példák feloldható csoportokra.

Az S_3 csoport feloldható,

Példák feloldható csoportokra.

Az S_3 csoport feloldható,

Példák feloldható csoportokra.

Az S_3 csoport feloldható, az

$$\{\mathrm{id}\} \triangleleft A_3 \triangleleft S_3$$

normállánc faktorai Abel-csoportok:

$$A_3/\{\mathrm{id}\} \cong A_3 = \langle (1\,2\,3) \rangle, \quad S_3/A_3 \cong C_2.$$

Példák feloldható csoportokra.

Az S_3 csoport feloldható, az

$$\{\mathrm{id}\} \triangleleft A_3 \triangleleft S_3$$

normállánc faktorai Abel-csoportok:

$$A_3/\{\mathrm{id}\} \cong A_3 = \langle (1\,2\,3) \rangle, \quad S_3/A_3 \cong C_2.$$

Az S_4 csoport is feloldható,

Példák feloldható csoportokra.

Az S_3 csoport feloldható, az

$$\{\mathrm{id}\} \triangleleft A_3 \triangleleft S_3$$

normállánc faktorai Abel-csoportok:

$$A_3/\{\mathrm{id}\} \cong A_3 = \langle (1\,2\,3) \rangle, \quad S_3/A_3 \cong C_2.$$

Az S_4 csoport is feloldható, az

$$\{\mathrm{id}\} \underset{C_2}{\triangleleft} \{\mathrm{id}, (1\,2)(3\,4)\} \underset{C_2}{\triangleleft} \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \underset{C_3}{\triangleleft} A_4 \underset{C_2}{\triangleleft} S_4$$

normállánc faktorai Abel-csoportok

Példák feloldható csoportokra.

Az S_3 csoport feloldható, az

$$\{\mathrm{id}\} \triangleleft A_3 \triangleleft S_3$$

normállánc faktorai Abel-csoportok:

$$A_3/\{\mathrm{id}\} \cong A_3 = \langle (1\,2\,3) \rangle, \quad S_3/A_3 \cong C_2.$$

Az S_4 csoport is feloldható, az

$$\{\mathrm{id}\} \underset{C_2}{\triangleleft} \{\mathrm{id}, (1\,2)(3\,4)\} \underset{C_2}{\triangleleft} \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \underset{C_3}{\triangleleft} A_4 \underset{C_2}{\triangleleft} S_4$$

normállánc faktorai Abel-csoportok (sőt prímrendű ciklikus csoportok).

Tétel.

Az A_n n-edfokú alternáló csoport és S_n n-edfokú szimmetrikus csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Az A_n n-edfokú alternáló csoport és S_n n-edfokú szimmetrikus csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leqslant G$ és $N \triangleleft G$. Ekkor igazak a következők:

Tétel.

Az A_n n-edfokú alternáló csoport és S_n n-edfokú szimmetrikus csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leqslant G$ és $N \triangleleft G$. Ekkor igazak a következők:

(a) ha G feloldható, akkor H is feloldható;

Tétel.

Az A_n n-edfokú alternáló csoport és S_n n-edfokú szimmetrikus csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leqslant G$ és $N \triangleleft G$. Ekkor igazak a következők:

(a) ha G feloldható, akkor H is feloldható;

(b) a G csoport pontosan akkor feloldható, ha N és G/N is feloldható.

Definíció: radikál, radikálbővítés.

Legyen $L : K$ tetszőleges testbővítés, $\beta \in L$. Azt mondjuk, hogy β **radikál** K felett, ha $\beta^n \in K$.

Az $L : K$ testbővítés radikálbővítés, ha van az $L : K$ testbővítés küzbülső testeinek olyan $L_0, \ldots, L_r$ sorozata, amelyre teljesülnek a következők:

Definíció: radikál, radikálbővítés.

Legyen $L : K$ tetszőleges testbővítés, $\beta \in L$. Azt mondjuk, hogy β **radikál** K felett, ha $\beta^n \in K$.

Az $L : K$ testbővítés radikálbővítés, ha van az $L : K$ testbővítés küzbülső testeinek olyan $L_0, \ldots, L_r$ sorozata, amelyre teljesülnek a következők:

(1) $L_0 = K$, $L_r = L$,

Definíció: radikál, radikálbővítés.

Legyen $L : K$ tetszőleges testbővítés, $\beta \in L$. Azt mondjuk, hogy β **radikál** K felett, ha $\beta^n \in K$.

Az $L : K$ testbővítés radikálbővítés, ha van az $L : K$ testbővítés küzbülső testeinek olyan $L_0, \ldots, L_r$ sorozata, amelyre teljesülnek a következők:

(1) $L_0 = K$, $L_r = L$,

(2) $L_j = L_{j-1}(\beta_i)$, ahol $\beta_i \in L$ radikál L_{i-1} felett.

Definíció: radikál, radikálbővítés.

Legyen $L : K$ tetszőleges testbővítés, $\beta \in L$. Azt mondjuk, hogy β **radikál** K felett, ha $\beta^n \in K$.
Az $L : K$ testbővítés radikálbővítés, ha van az $L : K$ testbővítés küzbülső testeinek olyan $L_0, \ldots, L_r$ sorozata, amelyre teljesülnek a következők:

(1) $L_0 = K$, $L_r = L$,

(2) $L_j = L_{j-1}(\beta_i)$, ahol $\beta_i \in L$ radikál L_{i-1} felett.

Definíció: gyökjelekkel való megoldhatóság.

Legyen f tetszőleges polinom a K test felett. Azt mondjuk, hogy az f polinom **gyökjelekkel megoldható**, ha van olyan L test, amelyre az $L : K$ testbővítés olyan radikálbővítés, amely felett f elsőfokú polinomok szorzatára bontható.

Egyenletek megoldása gyökjelekkel.
Polinomok feloldható Galois-csoporttal.

Tétel.

Legyen K tetszőleges test. Tegyük fel, hogy az $f \in K[x]$ polinom szeparábilis és Galois-csoportja feloldható, valamint $\mathrm{char}(K) \nmid |\mathrm{Gal}_K(f)|$. Ekkor az f polinom gyökjelekkel megoldható.

Tétel.

Legyen K tetszőleges test. Tegyük fel, hogy az $f \in K[x]$ polinom szeparábilis és Galois-csoportja feloldható, valamint $\mathrm{char}(K) \nmid |\mathrm{Gal}_K(f)|$. Ekkor az f polinom gyökjelekkel megoldható.

Bizonyítás.

Legyen $d = |\mathrm{Gal}_K(f)|$, ε d-edik primitív egységgyök és $L = K(\varepsilon)$. Mivel $\mathrm{char}(K) \nmid d$, ezért $U_d \subseteq L$. Legyen N az f polinom felbontási teste L felett, az N testben f gyökei legyenek $\alpha_1, \ldots, \alpha_n$, valamint legyen $M = K(\alpha_1, \ldots, \alpha_n)$.

Tétel.

Legyen K tetszőleges test. Tegyük fel, hogy az $f \in K[x]$ polinom szeparábilis és Galois-csoportja feloldható, valamint $\mathrm{char}(K) \nmid |\mathrm{Gal}_K(f)|$. Ekkor az f polinom gyökjelekkel megoldható.

Bizonyítás.

Legyen $d = |\mathrm{Gal}_K(f)|$, ε d-edik primitív egységgyök és $L = K(\varepsilon)$. Mivel $\mathrm{char}(K) \nmid d$, ezért $U_d \subseteq L$. Legyen N az f polinom felbontási teste L felett, az N testben f gyökei legyenek $\alpha_1, \ldots, \alpha_n$, valamint legyen $M = K(\alpha_1, \ldots, \alpha_n)$.

Tétel.

Legyen K tetszőleges test. Tegyük fel, hogy az $f \in K[x]$ polinom szeparábilis és Galois-csoportja feloldható, valamint $\mathrm{char}(K) \nmid |\mathrm{Gal}_K(f)|$. Ekkor az f polinom gyökjelekkel megoldható.

Bizonyítás.

Legyen $d = |\mathrm{Gal}_K(f)|$, ε d-edik primitív egységgyök és $L = K(\varepsilon)$. Mivel $\mathrm{char}(K) \nmid d$, ezért $U_d \subseteq L$. Legyen N az f polinom felbontási teste L felett, az N testben f gyökei legyenek $\alpha_1, \ldots, \alpha_n$, valamint legyen $M = K(\alpha_1, \ldots, \alpha_n)$. Mivel az $N : L$ testbővítés Galois-bővítés, azért $\mathrm{Gal}_L(f) = \mathrm{Gal}(N : L)$ fixteste L.

Bizonyítás (folytatás).

Legyen $\sigma \in \mathrm{Gal}_L(f)$.

Bizonyítás (folytatás).

Legyen $\sigma \in \mathrm{Gal}_L(f)$.

Bizonyítás (folytatás).

Legyen $\sigma \in \mathrm{Gal}_L(f)$. Ekkor $\sigma(M) = M$ miatt $\sigma|_M \in \mathrm{Gal}(M : L \cap M)$.

Bizonyítás (folytatás).

Legyen $\sigma \in \mathrm{Gal}_L(f)$. Ekkor $\sigma(M) = M$ miatt $\sigma|_M \in \mathrm{Gal}(M : L \cap M)$. Továbbá a

$$\varrho\colon \mathrm{Gal}_L(f) \to \mathrm{Gal}(M : L \cap M),\ \sigma \mapsto \sigma|_M$$

leképezés homomorfizmus.

Bizonyítás (folytatás).

Legyen $\sigma \in \mathrm{Gal}_L(f)$. Ekkor $\sigma(M) = M$ miatt $\sigma|_M \in \mathrm{Gal}(M : L \cap M)$. Továbbá a

$$\varrho\colon \mathrm{Gal}_L(f) \to \mathrm{Gal}(M : L \cap M),\ \sigma \mapsto \sigma|_M$$

leképezés homomorfizmus. Ha $\sigma|_M = \mathrm{id}_M$, akkor $\sigma = \mathrm{id}_N$, mivel $N = L(\alpha_1, \ldots, \alpha_n)$, azaz ϱ injektív homomorfizmus.

Bizonyítás (folytatás).

Legyen $\sigma \in \mathrm{Gal}_L(f)$. Ekkor $\sigma(M) = M$ miatt $\sigma|_M \in \mathrm{Gal}(M : L \cap M)$. Továbbá a

$$\varrho\colon \mathrm{Gal}_L(f) \to \mathrm{Gal}(M : L \cap M),\ \sigma \mapsto \sigma|_M$$

leképezés homomorfizmus. Ha $\sigma|_M = \mathrm{id}_M$, akkor $\sigma = \mathrm{id}_N$, mivel $N = L(\alpha_1, \ldots, \alpha_n)$, azaz ϱ injektív homomorfizmus. Ekkor

$$\mathrm{Gal}_L(f) \underset{\varrho}{\hookrightarrow} \mathrm{Gal}(M : L \cap M) \leqslant \mathrm{Gal}(M : K) \cong \mathrm{Gal}_K(f)$$

következtében $\mathrm{Gal}_L(f)$ is feloldható, így van olyan

$$\{\mathrm{id}_N\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = \mathrm{Gal}_L(f)$$

normállánca, melynek faktorai ciklikus csoportok.

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

$\Downarrow$

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

$\Downarrow$ (a Galois-elmélet Főtétele)

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

$\Downarrow$ (a Galois-elmélet Főtétele)

$L_j = \varphi(G_j)$ és $\mathrm{Gal}(L_0 : L_j) = \gamma(L_j) = G_j$

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

$\Downarrow$ (a Galois-elmélet Főtétele)

$L_j = \varphi(G_j)$ és $\mathrm{Gal}(L_0 : L_j) = \gamma(L_j) = G_j$

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

$\Downarrow$ (a Galois-elmélet Főtétele)

$L_j = \varphi(G_j)$ és $\mathrm{Gal}(L_0 : L_j) = \gamma(L_j) = G_j$

$L_0 : L_j$ Galois-bővítés és $G_{j-1} \triangleleft G_j = \mathrm{Gal}(L_0 : L_j)$

$\Downarrow$

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

$\Downarrow$ (a Galois-elmélet Főtétele)

$L_j = \varphi(G_j)$ és $\mathrm{Gal}(L_0 : L_j) = \gamma(L_j) = G_j$

$L_0 : L_j$ Galois-bővítés és $G_{j-1} \lhd G_j = \mathrm{Gal}(L_0 : L_j)$

$\Downarrow$ (a Galois-elmélet Főtétele)

Bizonyítás (folytatás).

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen L_i $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$L_0 : L_r$ Galois-bővítés $\Rightarrow$ $L_0 : L_j$ Galois-bővítés

$\Downarrow$ (a Galois-elmélet Főtétele)

$L_j = \varphi(G_j)$ és $\mathrm{Gal}(L_0 : L_j) = \gamma(L_j) = G_j$

$L_0 : L_j$ Galois-bővítés és $G_{j-1} \lhd G_j = \mathrm{Gal}(L_0 : L_j)$

$\Downarrow$ (a Galois-elmélet Főtétele)

$\varphi(G_{j-1}) : L_j$ normális bővítés és $\mathrm{Gal}(L_{j-1} : L_j) \cong G_j / G_{j-1}$.

Bizonyítás (folytatás).

Mivel G_j/G_{j-1} ciklikus, ezért az $L_{j-1} : L_j$ tesbővítés is ciklikus és $[L_{j-1} : L_j] = |G_j/G_{j-1}|$.

Bizonyítás (folytatás).

Mivel G_j/G_{j-1} ciklikus, ezért az $L_{j-1} : L_j$ tesbővítés is ciklikus és $[L_{j-1} : L_j] = |G_j/G_{j-1}|$.

Bizonyítás (folytatás).

Mivel G_j/G_{j-1} ciklikus, ezért az $L_{j-1} : L_j$ tesbővítés is ciklikus és $[L_{j-1} : L_j] = |G_j/G_{j-1}|$. Így $\mathrm{char}(K) \nmid [L_{j-1} : L_j]$, mivel $d \mid |G_j/G_{j-1}|$, és van olyan $\beta_j \in L_{j-1}$ radikál L_j felett, amelyre $L_{j-1} = L_j(\beta)$. Így az $N : L$ bővítés radikálbővítés, aminek következtében az $N : K$ bővítés is az. Az f polinom N felett elsőfokú tényezőkre bomlik, ezért f megoldható radikálokkal.

Bizonyítás (folytatás).

Mivel G_j/G_{j-1} ciklikus, ezért az $L_{j-1} : L_j$ tesbővítés is ciklikus és $[L_{j-1} : L_j] = |G_j/G_{j-1}|$. Így $\mathrm{char}(K) \nmid [L_{j-1} : L_j]$, mivel $d \mid |G_j/G_{j-1}|$, és van olyan $\beta_j \in L_{j-1}$ radikál L_j felett, amelyre $L_{j-1} = L_j(\beta)$. Így az $N : L$ bővítés radikálbővítés, aminek következtében az $N : K$ bővítés is az. Az f polinom N felett elsőfokú tényezőkre bomlik, ezért f megoldható radikálokkal.
Q.E.D.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés Galois-bővítés, $M = L(\beta)$, ahol β gyöke az $x^n - \vartheta \in L[x]$ polinomnak, és $\mathrm{char}(K) \nmid n$. Ekkor van olyan $N : M$ testbővítés, amely radikálbővítés és $N : K$ Galois-bővítés.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés Galois-bővítés, $M = L(\beta)$, ahol β gyöke az $x^n - \vartheta \in L[x]$ polinomnak, és $\mathrm{char}(K) \nmid n$. Ekkor van olyan $N : M$ testbővítés, amely radikálbővítés és $N : K$ Galois-bővítés.

Bizonyítás.

Legyen ε primitív n-edik gyök. Ekkor $M(\varepsilon)[x]$-ben

$$x^n - \vartheta = \prod_{k=0}^{n-1} (x - \varepsilon^k \beta),$$

azaz $M(\varepsilon)$ felbontási teste az $x^n - \vartheta$ polinomnak L felett, amelynek n különböző gyöke van $M(\varepsilon)$-ban, ezért $M(\varepsilon) : L$ Galois-bővítés (és radikál bővítés is).

Bizonyítás (folytatás).

Legyen $f = \prod_{\sigma \in \mathrm{Gal}(L:K)} (x^n - \sigma(\vartheta))$, amelynek felbontási teste $M(\varepsilon)$ felett legyen N. Ha $\gamma \in N$ gyöke $x^n - \sigma(\vartheta)$, akkor

$$x^n - \sigma(\vartheta) = \prod_{k=0}^{n-1} (x - \varepsilon^k \gamma),$$

azaz N felbontási teste f-nek K felett is, és f szeparábilis $M(\varepsilon)$ felett. Ezért az $N : K$ bővítés is szeparábilis.

Bizonyítás (folytatás).

Legyen $f = \prod_{\sigma \in \mathrm{Gal}(L:K)} (x^n - \sigma(\vartheta))$, amelynek felbontási teste $M(\varepsilon)$ felett legyen N. Ha $\gamma \in N$ gyöke $x^n - \sigma(\vartheta)$, akkor

$$x^n - \sigma(\vartheta) = \prod_{k=0}^{n-1} (x - \varepsilon^k \gamma),$$

azaz N felbontási teste f-nek K felett is, és f szeparábilis $M(\varepsilon)$ felett. Ezért az $N : K$ bővítés is szeparábilis.

Bizonyítás (folytatás).

Legyen $f = \prod_{\sigma \in \mathrm{Gal}(L:K)} (x^n - \sigma(\vartheta))$, amelynek felbontási teste $M(\varepsilon)$ felett legyen N. Ha $\gamma \in N$ gyöke $x^n - \sigma(\vartheta)$, akkor

$$x^n - \sigma(\vartheta) = \prod_{k=0}^{n-1} (x - \varepsilon^k \gamma),$$

azaz N felbontási teste f-nek K felett is, és f szeparábilis $M(\varepsilon)$ felett. Ezért az $N : K$ bővítés is szeparábilis.
Mivel tetszőleges $\tau \in \mathrm{Gal}(L : K)$-ra $\tau_f = f$, ezért $f \in K[x]$. Legyen $g \in K[x]$ olyan polinom, amelynek felbontási teste K felett L. Ekkor N az fg polinom felbontási teste K felett, így az $N : K$ bővítés normális, valamint radikálbővítés is.

Bizonyítás (folytatás).

Legyen $f = \prod_{\sigma \in \mathrm{Gal}(L:K)} (x^n - \sigma(\vartheta))$, amelynek felbontási teste $M(\varepsilon)$ felett legyen N. Ha $\gamma \in N$ gyöke $x^n - \sigma(\vartheta)$, akkor

$$x^n - \sigma(\vartheta) = \prod_{k=0}^{n-1} (x - \varepsilon^k \gamma),$$

azaz N felbontási teste f-nek K felett is, és f szeparábilis $M(\varepsilon)$ felett.
Ezért az $N : K$ bővítés is szeparábilis.
Mivel tetszőleges $\tau \in \mathrm{Gal}(L : K)$-ra $\tau_f = f$, ezért $f \in K[x]$. Legyen $g \in K[x]$ olyan polinom, amelynek felbontási teste K felett L. Ekkor N az fg polinom felbontási teste K felett, így az $N : K$ bővítés normális, valamint radikálbővítés is.
Q.E.D.

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$ és β_i az $x^{n_i} - \vartheta_i \in L_{i-1}$ polinom gyöke $(i = 1, \ldots, r)$. Ha $\mathrm{char}(K) \nmid n_1 \cdots n_r$, akkor van olyan $M : L$ testbővítés, amelyre $M : K$ Galois-bővítés és radikálbővítés.

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$ és β_i az $x^{n_i} - \vartheta_i \in L_{i-1}$ polinom gyöke $(i = 1, \ldots, r)$. Ha $\mathrm{char}(K) \nmid n_1 \cdots n_r$, akkor van olyan $M : L$ testbővítés, amelyre $M : K$ Galois-bővítés és radikálbővítés.

Bizonyítás.

Teljes indukcióval igazoljuk az állítást (r-re vonatkozó).

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$ és β_i az $x^{n_i} - \vartheta_i \in L_{i-1}$ polinom gyöke $(i = 1, \ldots, r)$. Ha $\mathrm{char}(K) \nmid n_1 \cdots n_r$, akkor van olyan $M : L$ testbővítés, amelyre $M : K$ Galois-bővítés és radikálbővítés.

Bizonyítás.

Teljes indukcióval igazoljuk az állítást (r-re vonatkozó).

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$ és β_i az $x^{n_i} - \vartheta_i \in L_{i-1}$ polinom gyöke $(i = 1, \ldots, r)$. Ha $\mathrm{char}(K) \nmid n_1 \cdots n_r$, akkor van olyan $M : L$ testbővítés, amelyre $M : K$ Galois-bővítés és radikálbővítés.

Bizonyítás.

Teljes indukcióval igazoljuk az állítást (r-re vonatkozó).
Ha $r = 1$, akkor $M = L(\varepsilon)$-ra teljesül az állítás, ahol ε primitív n_1-edik egységgyök.

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$ és β_i az $x^{n_i} - \vartheta_i \in L_{i-1}$ polinom gyöke $(i = 1, \ldots, r)$. Ha $\mathrm{char}(K) \nmid n_1 \cdots n_r$, akkor van olyan $M : L$ testbővítés, amelyre $M : K$ Galois-bővítés és radikálbővítés.

Bizonyítás.

Teljes indukcióval igazoljuk az állítást (r-re vonatkozó).
Ha $r = 1$, akkor $M = L(\varepsilon)$-ra teljesül az állítás, ahol ε primitív n_1-edik egységgyök.
Tegyük fel, hogy $r - 1$ $(\geqslant 1)$-re teljesül az állítás, legyen $M_{r-1} : L_{r-1}$ olyan testbővítés, amelyre $M_{r-1} : K$ Galois- és radikálbővítés.

Bizonyítás (folytatás).

Legyen $m_r = m_{\beta_r, L_{r-1}}$, és legyen l_r irreducibilis osztója az $m_r \in M_{r-1}[x]$ polinomnak. Legyen γ az l_r polinom gyöke (valamely felbontási testében). Tekintsük az $\mathfrak{i}\colon L_{r-1} \to M_{r-1},\ \alpha \mapsto \alpha$ injektív homomorfizmust. Mivel $\mathfrak{i}_{m_r}(\gamma) = m_r(\gamma) = 0$, ezért van olyan $\mathfrak{j}\colon L_{r-1}(\beta_r) \to M_{r-1}(\gamma)$ injektív homomorfzmus, amely kiterjesztése $\mathfrak{i}$-nek. Feltehető, hogy $L \leqslant M_{r-1}(\beta)$. Legyen $M = M_{r-1}(\beta_r)$. Ekkor $M_{r-1} : K$ Galois bővítés, β_r gyöke az $x^{n_r} - \vartheta_r \in M_{r-1}[x]$ polinomnak és $\mathrm{char}(K) \nmid n_r$. Így van olyan $M_r : M_{r-1}(\beta_r)$ radikálbővítés, amelyre $M_r : K$ Galois-bővítés.

Bizonyítás (folytatás).

Legyen $m_r = m_{\beta_r, L_{r-1}}$, és legyen l_r irreducibilis osztója az $m_r \in M_{r-1}[x]$ polinomnak. Legyen γ az l_r polinom gyöke (valamely felbontási testében). Tekintsük az $\mathfrak{i}\colon L_{r-1} \to M_{r-1},\ \alpha \mapsto \alpha$ injektív homomorfizmust. Mivel $\mathfrak{i}_{m_r}(\gamma) = m_r(\gamma) = 0$, ezért van olyan $\mathfrak{j}\colon L_{r-1}(\beta_r) \to M_{r-1}(\gamma)$ injektív homomorfzmus, amely kiterjesztése $\mathfrak{i}$-nek. Feltehető, hogy $L \leqslant M_{r-1}(\beta)$. Legyen $M = M_{r-1}(\beta_r)$. Ekkor $M_{r-1} : K$ Galois bővítés, β_r gyöke az $x^{n_r} - \vartheta_r \in M_{r-1}[x]$ polinomnak és $\mathrm{char}(K) \nmid n_r$. Így van olyan $M_r : M_{r-1}(\beta_r)$ radikálbővítés, amelyre $M_r : K$ Galois-bővítés.

Bizonyítás (folytatás).

Legyen $m_r = m_{\beta_r, L_{r-1}}$, és legyen l_r irreducibilis osztója az $m_r \in M_{r-1}[x]$ polinomnak. Legyen γ az l_r polinom gyöke (valamely felbontási testében). Tekintsük az $\mathfrak{i}\colon L_{r-1} \to M_{r-1},\ \alpha \mapsto \alpha$ injektív homomorfizmust. Mivel $\mathfrak{i}_{m_r}(\gamma) = m_r(\gamma) = 0$, ezért van olyan $\mathfrak{j}\colon L_{r-1}(\beta_r) \to M_{r-1}(\gamma)$ injektív homomorfzmus, amely kiterjesztése $\mathfrak{i}$-nek. Feltehető, hogy $L \leqslant M_{r-1}(\beta)$. Legyen $M = M_{r-1}(\beta_r)$. Ekkor $M_{r-1} : K$ Galois bővítés, β_r gyöke az $x^{n_r} - \vartheta_r \in M_{r-1}[x]$ polinomnak és $\mathrm{char}(K) \nmid n_r$. Így van olyan $M_r : M_{r-1}(\beta_r)$ radikálbővítés, amelyre $M_r : K$ Galois-bővítés. Az

$$M_r\colon M_{r-1}(\beta_r)\colon M_{r-1}\colon K$$

testláncot tanulmányozva kapjuk, hogy $M_r : K$ radikálbővítés.

Bizonyítás (folytatás).

Legyen $m_r = m_{\beta_r, L_{r-1}}$, és legyen l_r irreducibilis osztója az $m_r \in M_{r-1}[x]$ polinomnak. Legyen γ az l_r polinom gyöke (valamely felbontási testében). Tekintsük az $\mathfrak{i}\colon L_{r-1} \to M_{r-1},\ \alpha \mapsto \alpha$ injektív homomorfizmust. Mivel $\mathfrak{i}_{m_r}(\gamma) = m_r(\gamma) = 0$, ezért van olyan $\mathfrak{j}\colon L_{r-1}(\beta_r) \to M_{r-1}(\gamma)$ injektív homomorfzmus, amely kiterjesztése $\mathfrak{i}$-nek. Feltehető, hogy $L \leqslant M_{r-1}(\beta)$. Legyen $M = M_{r-1}(\beta_r)$. Ekkor $M_{r-1} : K$ Galois bővítés, β_r gyöke az $x^{n_r} - \vartheta_r \in M_{r-1}[x]$ polinomnak és $\mathrm{char}(K) \nmid n_r$. Így van olyan $M_r : M_{r-1}(\beta_r)$ radikálbővítés, amelyre $M_r : K$ Galois-bővítés. Az

$$M_r\colon M_{r-1}(\beta_r)\colon M_{r-1}\colon K$$

testláncot tanulmányozva kapjuk, hogy $M_r : K$ radikálbővítés.
Q.E.D.

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$, β_i az $x^{n_i} - \vartheta_i \in L_{i-1}[x]$ polinom gyöke $(i = 1, \ldots, r)$ és $\mathrm{char}(K) \nmid n_1 \cdots n_r$. Ha az $f \in K[x]$ polinom L felett elsőfokú polinomok szorzatára bontható, akkor $\mathrm{Gal}_K(f)$ feloldható.

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$, β_i az $x^{n_i} - \vartheta_i \in L_{i-1}[x]$ polinom gyöke $(i = 1, \ldots, r)$ és $\mathrm{char}(K) \nmid n_1 \cdots n_r$. Ha az $f \in K[x]$ polinom L felett elsőfokú polinomok szorzatára bontható, akkor $\mathrm{Gal}_K(f)$ feloldható.

Bizonyítás.

Feltehető, hogy $L : K$ Galois-bővítés. Ekkor $L : L_i$ is Galois-bővítés minden i-re $(1 \leqslant i \leqslant r)$, továbbá az $x^{n_i} - \vartheta_i$ polinomnak van gyöke L-ben, ezért elsőfokú polinomok szorzatára bomlik L felett. Ez pedig biztosítja, hogy L tartalmaz primitív n_i-edik egységgyököket. Legyen $n = \text{lk.k.t.}(n_1, \ldots, n_r)$ és ε legyen egy n-edik primitív egységgyök.

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$, β_i az $x^{n_i} - \vartheta_i \in L_{i-1}[x]$ polinom gyöke $(i = 1, \ldots, r)$ és $\mathrm{char}(K) \nmid n_1 \cdots n_r$. Ha az $f \in K[x]$ polinom L felett elsőfokú polinomok szorzatára bontható, akkor $\mathrm{Gal}_K(f)$ feloldható.

Bizonyítás.

Feltehető, hogy $L : K$ Galois-bővítés. Ekkor $L : L_i$ is Galois-bővítés minden i-re $(1 \leqslant i \leqslant r)$, továbbá az $x^{n_i} - \vartheta_i$ polinomnak van gyöke L-ben, ezért elsőfokú polinomok szorzatára bomlik L felett. Ez pedig biztosítja, hogy L tartalmaz primitív n_i-edik egységgyököket. Legyen $n = \text{lk.k.t.}(n_1, \ldots, n_r)$ és ε legyen egy n-edik primitív egységgyök.

Tétel.

Tegyük fel, hogy az $L = L_r : L_{r-1} : \ldots : L_0 : K$, testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$, β_i az $x^{n_i} - \vartheta_i \in L_{i-1}[x]$ polinom gyöke $(i = 1, \ldots, r)$ és $\mathrm{char}(K) \nmid n_1 \cdots n_r$. Ha az $f \in K[x]$ polinom L felett elsőfokú polinomok szorzatára bontható, akkor $\mathrm{Gal}_K(f)$ feloldható.

Bizonyítás.

Feltehető, hogy $L : K$ Galois-bővítés. Ekkor $L : L_i$ is Galois-bővítés minden i-re $(1 \leqslant i \leqslant r)$, továbbá az $x^{n_i} - \vartheta_i$ polinomnak van gyöke L-ben, ezért elsőfokú polinomok szorzatára bomlik L felett. Ez pedig biztosítja, hogy L tartalmaz primitív n_i-edik egységgyököket. Legyen $n = \mathrm{lk.k.t.}(n_1, \ldots, n_r)$ és ε legyen egy n-edik primitív egységgyök. Legyen $L_i' = L_i(\varepsilon)$ és $G_i = \mathrm{Gal}(L : L_i')$ $(i = 0, 1 \ldots, r)$.

Bizonyítás (folytatás).

Mivel $L_i' : L_{i-1}'$ az $x^{n_i} - \vartheta_i \in L_{i-1}'[x]$ polinom felbontási teste, ezért az $L_i' : L_{i-1}'$ bővítés ciklikus. Így $G_i \lhd G_{i-1}$ és $G_{i-1}/G_i \cong \mathrm{Gal}(L_i' : L_{i-1}')$. Ezért a $G_0 = \mathrm{Gal}(L : L_0') = \mathrm{Gal}(L : K(\varepsilon))$ Galois-csoport feloldható. A $K(\varepsilon)$ test az $x^n - 1 \in K[x]$ polinom felbontási teste, ezért $\mathrm{Gal}(K(\varepsilon) : K)$ Abel-csoport, és emiatt feloldható:

$$\mathrm{Gal}(K(\varepsilon) : K) \cong \mathrm{Gal}(L : K)/\mathrm{Gal}(L : K(\varepsilon)) = \mathrm{Gal}(L : K)/G_0$$

ezért $\mathrm{Gal}(L : K)/G_0$ is feloldható. Ez pedig azt jelenti, hogy $\mathrm{Gal}(L : K)$ is feloldható.

Bizonyítás (folytatás).

Legyen $N \leqslant L$ az f polinom felbontási teste. A Galois-elmélet Főtétele szerint:

$$\mathrm{Gal}_K(f) \cong \mathrm{Gal}(N : K) \cong \mathrm{Gal}(L : K)/\mathrm{Gal}(L : N),$$

azaz $\mathrm{Gal}_K(f)$ is feloldható.

Bizonyítás (folytatás).

Legyen $N \leqslant L$ az f polinom felbontási teste. A Galois-elmélet Főtétele szerint:

$$\mathrm{Gal}_K(f) \cong \mathrm{Gal}(N : K) \cong \mathrm{Gal}(L : K)/\mathrm{Gal}(L : N),$$

azaz $\mathrm{Gal}_K(f)$ is feloldható.

Bizonyítás (folytatás).

Legyen $N \leqslant L$ az f polinom felbontási teste. A Galois-elmélet Főtétele szerint:

$$\mathrm{Gal}_K(f) \cong \mathrm{Gal}(N : K) \cong \mathrm{Gal}(L : K)/\mathrm{Gal}(L : N),$$

azaz $\mathrm{Gal}_K(f)$ is feloldható.
Q.E.D.