11. Testek, testbővítések

11.1 Normális bővítések

11.1.1 Definíció: az $L|K$ algebrai bővítés normális, ha minden K feletti p polinom, amelynek van gyöke L-ben, $L[x]$-ben lineáris faktorok szorzatára bomlik.

Megjegyzés: minden elsőfokú bővítés normális. Ugyanis ha egy $K[x]$-ben irreducibilis polinomnak van gyöke K-ban, akkor elsőfokú és valóban felbomlik lineáris faktorok szorzatára.

11.1.2 Állítás: minden másodfokú bővítés normális.

Bizonyítás: legyen $(L:K)=2$, $p(x)\in K[x]$ irreducibilis, $\alpha\in L$ és $p(\alpha)=0$. Feltehetjük, hogy p főegyütthatója 1. Ekkor p éppen α kanonikus polinomja, eszerint foka osztja a bővítés fokát. Eszerint p első- vagy másodfokú. Az első esetben $p=x-\alpha$, a másodikban $L[x]$-ben $(x-\alpha)|p(x)$ miatt $p(x)=(x-\alpha)\cdot q(x)$, ahol $q(x)$ csak elsőfokú lehet.

Példa: $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ nem normális. Ugyanis $p(x)=x^3-2$ irreducibilis a Schönemann-Eisenstein kritérium szerint. Ennek $\alpha=\sqrt[3]{2}$ gyöke, azaz $p(x)=q(x)\cdot(x-\alpha)$. Ha $q(x)$ felbomlana $\mathbb{Q}(\sqrt[3]{2})$[x]-ben két lineáris polinom szorzatára, akkor az a felbontás $\mathbb{C}[x]$-ben is működne, hiszen $\mathbb{Q}(\sqrt[3]{2})\le\mathbb{C}$. Viszont $\mathbb{C}$-ben p másik két gyöke nem valós, azaz p lineáris faktorokra bontása nem valós együtthatós. Így $q(x)$ irreducibilis $\mathbb{Q}(\sqrt[3]{2})$-ben, azaz $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ nem normális.

11.1.3 Tétel: az $L|K$ véges bővítés normális $\Leftrightarrow$ izomorf valamely $p(x)\in K[x]$ felbontási testével.

Bizonyítás: $\Leftarrow$: legyen L az 1 főegyütthatójú $f(x)\in K[x]$ polinom felbontási teste, azaz $L=K(\alpha_1,\alpha_2,\dots,\alpha_n)$, ahol $\prod_{k=1}^{n}(x-\alpha_k)=f(x)$. Legyen p olyan K feletti irreducibilis polinom, melynek gyöke $\beta\in L$ és lássuk be, hogy p előáll L feletti lineáris polinomok szorzataként. Tudjuk, hogy β előáll $g(\alpha_1,\dots,\alpha_n)$ alakban, ahol $g\in K[x_1,\dots,x_n]$. (Emlékeztető: az ilyen alakban előálló L-beli elemek halmaza zárt a műveletekre és tartalmazza $\{\alpha_1,\dots,\alpha_n\}$-t, tehát maga L, különben L feleslegesen nagy lenne $K(\alpha_1,\dots,\alpha_n)$-nek.) Definiáljuk az alábbi segédpolinomot:

$$h(x)=\prod_{\sigma\in S_n}\left(x-g(\alpha_{1\sigma},\dots,\alpha_{n\sigma})\right)\in L[x].$$

Ennek együtthatói az $\alpha_1,\dots,\alpha_n\in L$ számok szimmetrikus polinomjai K-beli együtthatókkal, mert a definíció szimetrikus és $g\in K[x_1,\dots,x_n]$. A szimmetrikus polinomok alaptétele szerint $h(x)$ előáll $\alpha_1,\dots,\alpha_n$ elemi szimmetrikus polinomjainak, azaz p együtthatóinak K-beli együtthatós polinomjaként. Tehát $h(x)\in K[x]$. $h(\beta)=0$, hiszen $h(x)$ definíciójában σ-t az identikus permutációnak választva a megfelelő tényező $(x-\beta)$. Mivel β kanonikus polinomja p, ennek osztania kell h-t $K[x]$-ben. Ekkor persze $L[x]$-ben is osztja, azaz p $L[x]$-beli irreducibilis faktorai h irreducibilis faktorai közül valók, így lineárisak.

$\Rightarrow$: mivel L véges bővítés, előáll $K(\alpha_1,\dots,\alpha_n)$ alakban. Legyen α_k kanonikus polinomja p_k. A p_k polinomok mindegyike irreducibilis $K[x]$-ben és van gyöke L-ben. Ha $L|K$ normális, akkor mindegyik felbomlik lineáris faktorok szorzatára, így $q(x)=\prod_{k=1}^{n}p_k(x)$ is. Állítsuk elő $q(x)$ felbontási testét úgy, hogy K-hoz először $\alpha_1,\dots,\alpha_n$-t adjungáljuk, majd a többi gyökét. Ily módon q felbontási testét kapjuk L felett, ami maga L, hiszen q minden gyöke L-beli. Tehát L előáll q K feletti felbontási testeként.

11.1.4 Állítás: ha $L|K$ véges bővítés, akkor található egy olyan $N|K$ normális bővítés, amelyre $K\le L\le N$ és N a lehető legkisebb, azaz tetszőleges $M|K$ L-t fedő normális bővítésre található egy N-el izomorf N^*, amelyre $L\le N^*\le M$.

Bizonyítás: mivel L véges bővítése K-nak, előáll $L=K(\alpha_1,\alpha_2,\dots,\alpha_n)$ alakban. Legyen α_k kanonikus polinomja p_k, $q(x)=\prod_{k=1}^{n}p_k(x)$. Állítsuk elő K felett q felbontási testét úgy, hogy először az $\alpha_1,\dots,\alpha_n$ gyököket adjungáljuk, aztán a többit. Legyen a kapott bővítés N. Ez **11.1.3** szerint normális bővítés és nyilván K minden $\{\alpha_1,\dots,\alpha_n\}$-t fedő M normális bővítésének tartalmaznia kell q felbontási testét, hiszen $p_1,\dots,p_n$ mindegyike lineáris faktorokra kell bomoljon $M[x]$-ben.

11.1.5 Definíció: a fenti N bővítést $L|K$ normális lezárásának nevezzük.

Példa: $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ normális lezárása $\mathbb{Q}(\sqrt[3]{2},\varepsilon_3)$, azaz $p(x)=x^3-2\in\mathbb{Q}[x]$ felbontási teste (p gyökei $\sqrt[3]{2},\varepsilon_3\cdot\sqrt[3]{2}$ és $\varepsilon_3^2\cdot\sqrt[3]{2}$).

11.1.6 Definíció: legyen $\Phi\subseteq K[x]$ polinomok egy halmaza. Φ felbontási teste az a legszűkebb $L|K$ bővítés, amelyben minden $f\in\Phi$ lineáris faktorok szorzatára bomlik. Némi fáradsággal belátható, hogy ez izomorfia erejéig értelmes. Ha a Φ-beli polinomok gyökeinek halmaza $\{\alpha_\kappa|\kappa\in\mathbf{I}\}$, akkor L azon elemek halmaza, melyek előállnak véges sok α_κ K feletti polinomjaként.

11.1.7 Állítás: az $L|K$ bővítés pontosan akkor normális, ha előáll valamely $\Phi\subseteq K[x]$ felbontási testeként.

Bizonyítás: ha $L|K$ normális, akkor előáll, mint elemei kanonikus polinomjai halmazának felbontási teste.

Legyen $L|K$ Φ felbontási teste, $\beta\in L$ tetszőleges. Ekkor β előáll véges sok α_κ K feletti polinomjaként. Legyen ezen véges sok α_κ K feletti kanonikus polinomjainak szorzata g, g felbontási teste K felett L'. Ekkor $\beta\in L'\subseteq L$ és $L'|K$ normális. Eszerint β minden konjugáltja benne van L'-ben, így L-ben is. Azaz L tetszőleges elemének minden konjugáltja is L-beli, $L|K$ normális.

Megjegyzés: ez alapján definiálható tetszőleges $L|K$ bővítés normális lezárása, mint az L-beli elemek K feletti kanonikus polinomjai halmazának felbontási teste. Ez a szokott értelemben egyértelmű és a lehető legkisebb L-t fedő normális bővítés.

11.1.8 Állítás: ha $M|K$ normális bővítés és $K\le L\le M$, akkor $M|L$ is.

Bizonyítás: ha $M|K$ normális bővítés, akkor M előáll valamely $\Phi\subseteq K[x]$ felbontási testeként. Ekkor persze $\Phi\subseteq L[x]$ és Φ L feletti felbontási teste is M, ezért $M|L$ normális.

$L|K$-ról nem tudunk semmit, hiszen M-et $L|K$ normális lezárásának választva $M|K$ automatikusan normális lesz.

Megjegyzés: abból, hogy $L|K$ és $M|L$ normális bővítések, nem következik, hogy $M|K$ is normális. Ugyanis $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ nem normális (nincs benne $\pm i\cdot\sqrt[4]{2}$), pedig $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ és $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ másodfokú, azaz normális bővítések.

11.1.9 Állítás: ha $L|K$ normális és $f\in K[x]$ irreducibilis, akkor f irreducibilis faktorai $L[x]$-ben azonos fokúak és megkaphatóak egymásból úgy, hogy minden együttható helyére valamelyik konjugáltját írjuk.

Bizonyítás: legyen $L|K$ normális bővítés. Legyen $f\in K[x]$ irreducibilis és $L[x]$-ben $f(x)=p_1\cdot p_2\cdot\ldots\cdot p_s$ az irreducibilis faktorokra bontása. Azt akarjuk belátni, hogy $deg\,p_i\ge deg\,p_j$. Legyen $p_i(x)=x^m+a_{m-1}x^{m-1}+\ldots+a_1x+a_0$. Legyen továbbá a_k konjugáltjainak halmaza A_k. Tekintsük a $h(x)=\prod_{\forall k:\,a_k^*\in A_k}(a_m^*x^m+a_{m-1}^*+\ldots+a_1^*+a_0^*)$ polinomot – ez egy $\prod_{k=0}^m|A_k|=\prod_{k=0}^m gr_K(a_k)$ tényezőből álló szorzat. Mivel L normális, minden k-ra $A_k\subseteq L$, azaz minden tényező $L[x]$-beli. Következésképp $h(x)$ minden $L[x]$-ben irreducibilis faktora legfeljebb m-edfokú.

Jelölje A_k elemeinek s-edik elemi szimmetrikus polinomját $\sigma_s(A_k)$. $h(x)$ együtthatói olyan K-beli együtthatós polinomjai $(\cup_{k=0}^m A_k)$-nak, melyek minden $k\in\{0,\ldots,m\}$-re szimmetrikus polinomjai A_k elemeinek. A szimmetrikus polinomok alaptételét $m+1$-szer alkalmazva K feletti polinomjai $\cup_k(\cup_s\sigma_s(A_k))$-nak. Vegyük észre, hogy $\sigma_s(A_k)$ az a_k kanonikus polinomjának egyik együtthatója, azaz K-beli $\Rightarrow$ $h(x)\in K[x]$.

p_i tényezőként szerepel $h(x)$-ben, azaz $L[x]$-ben $p_i|h$. Véve p_i egy α gyökét $h(\alpha)=f(\alpha)=0$. $f(x)\in K[x]$ irreducibilis és van közös gyöke $h(x)\in K[x]$-el, azaz $K[x]$-ben $f|h$. Ez persze $L[x]$-ben is fennáll, azaz f irreducibilis faktorai $h(x)$ irreducibilis faktorai közül valók, így legfeljebb m-edfokúak $\Rightarrow$ $deg\,p_j\le m=deg\,p_i$.

Ekkor minden p_i foka azonos. Így f minden irreducibilis faktora a $h(x)$ definíciójában szereplő tényezők egyike, tehát valóban csak az együtthatók konjugálásában térhetnek el egymástól.

11.2 Szeparábilis bővítések

11.2.1 Definíció: a $p(x)\in K[x]$ irreducibilis polinom szeparábilis, ha felbontási testében minden gyöke egyszeres. Inszeparábilis, ha van többszörös gyöke.

Nézzük meg, milyen lehet egy inszeparábilis irreducibilis polinom. Legyen $f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n\in K[x]$ irreducibilis. $(f,f')|f$, tehát (f,f') csak 1 vagy f lehet. f-nek pontosan akkor van többszörös gyöke, ha f és f' legnagyobb közös osztója nem 1, azaz ha $f|f'$. $deg\,f'<deg\,f$ miatt ez pontosan $f'\equiv 0$ esetén áll fenn. Azaz f inszeparábilis $\Leftrightarrow$ $\sum_{k=1}^n k\cdot a_kx^{k-1}\equiv 0$ $\Leftrightarrow$ $\forall k\in\{1,\ldots,n\}$: $k\cdot a_k=0$.

Ha a test karakterisztikája 0, akkor akkor erre aligha számíthatunk, hiszen $n\cdot a_n\neq 0$. Ha $char\,K=p>0$, akkor pontosan a $q(x)=\sum_{k=0}^{m}a_{kp}x^{kp}$ alakú polinomok deriváltja lesz az azonosan 0 polinom, azaz pontosan az ilyen alakú irreducibilis polinomok lesznek inszeparábilisek. Hogy van-e egyáltalán ilyen irreducibilis polinom, az a testtől függ.

11.2.2 Definíció: legyen α algebrai K felett. α szeparábilis, ha kanonikus polinomja szeparábilis.

11.2.3 Definíció: az $L|K$ algebrai bővítés szeparábilis, ha minden α eleme szeparábilis. Persze minden elsőfokú bővítés szeparábilis.

11.2.4 Definíció: az $f\in K[x]$ polinom szeparábilis, ha minden irreducibilis faktora az.

11.2.5 Definíció: a K test perfekt, ha minden irreducibilis polinomja szeparábilis. Másként megfogalmazva:

- minden polinomja szeparábilis;
- minden véges bővítése szeparábilis;
- minden algebrai bővítése szeparábilis;
- minden K felett algebrai elem szeparábilis.

Megjegyzés: minden 0 karakterisztikájú test perfekt.

11.2.6 Megjegyzés: vegyük észre, hogy a binomiális tétel értelmében egy $p\neq 0$ karakterisztikájú testben $(a\pm b)^p=a^p\pm b^p$, így a p^f-edik hatványra emelés és az összeadás (kivonás, ellentettképzés) felcserélhető műveletek. Ezt igen gyakran fogjuk használni, külön hivatkozás nélkül.

11.2.7 Tétel: legyen $char\,K=p>0$. Ekkor K perfekt $\Leftrightarrow\ \forall\alpha\in K:\ \exists\sqrt[p]{\alpha}\in K:\ \left(\sqrt[p]{\alpha}\right)^p=\alpha$.

Megjegyzés: ha létezik, akkor egyértelmű, hiszen $a^p-b^p=(a-b)^p$, így a nullosztómentességből $a^p=b^p\Leftrightarrow a=b$.

Bizonyítás: $\Leftarrow$: $\lightning\ \exists f\in K[x]$ irreducibilis, inszeparábilis polinom. Ekkor $f(x)=\sum_{k=1}^{n}a_{kp}x^{kp}$. Legyen $c_k=\sqrt[p]{a_{kp}}$. Így $\left(\sum_{k=1}^{n}c_kx^k\right)^p=\sum_{k=1}^{n}c_k^px^{kp}=f(x)$, azaz f mégsem irreducibilis, $\lightning$.

$\Rightarrow$: tegyük fel, hogy az $a\in K$ elemnek nincs p-edik gyöke. Legyen $f(x)=x^p-a$, f felbontási teste L, $\alpha\in L$ gyöke f-nek. Ekkor $x^p-a=x^p-a-(\alpha^p-a)=x^p-\alpha^p=(x-\alpha)^p$. Eszerint f minden $K[x]$-ben irreducibilis faktora $(x-\alpha)\in L[x]$ hatványa. Ennek pontosan egy hatványa lehet irreducibilis – a legalacsonyabb olyan hatványa, amely $K[x]$-beli –, legyen ez $(x-\alpha)^k$. Így $f(x)=\left((x-\alpha)^k\right)^m$, amiből $k|p$, azaz $k=1$ vagy $k=p$. Az előbbi lehetetlen, hiszen $\alpha\notin K$. Így $(x-\alpha)^p$ irreducibilis, ezért inszeparábilis és K nem perfekt.

Példa: legyen P tetszőleges, p karakterisztikájú test ($p>0$), t transzcendens P felett. Ekkor $P(t)$-ben t-nek nincs p-edik gyöke. Ha ugyanis valamely $\varphi(t)\in P(t)$ p-edik hatványa t lenne, ahol φ P feletti racionális törtfüggvény, akkor φ-t felírva az $f,g\in P[x]$ polinomok hányadosaként $h(x)=\left(f(x)\right)^p-x\cdot\left(g(x)\right)^p$-nek gyöke lenne t. Ez lehetetlen, mert $h(x)$ nem azonosan 0, így nem lehet gyöke a t transzcendens szám. Eszerint x^p-t inszeparábilis $P(t)[x]$-ben, $P(t)$ nem perfekt.

11.2.8 Állítás: ha $K\leq L\leq M$ és $M|K$ szeparábilis, akkor $L|K$ és $M|L$ is szeparábilis.

Bizonyítás: ha $M|K$ szeparábilis, akkor M minden eleme szeparábilis K felett $\Rightarrow$ $L\subseteq M$ minden eleme is, azaz $L|K$ is szeparábilis.

Legyen $\alpha\in M$ tetszőleges. Legyen kanonikus polinomja $K[x]$-ben p, $L[x]$-ben q. Ekkor $L[x]$-ben $q|p$. p-nek nincs többszörös gyöke, mert $M|K$ szeparábilis. Eszerint q-nak sem lehet többszörös gyöke, azaz α szeparábilis L felett.

11.2.9 Állítás: legyen $N|K$ normális bővítés, $char\,K=p>0$, $f_0\in K[x]$ irreducibilis, amelynek van N-ben gyöke. Ekkor f_0 felírható $\prod_{k=1}^{n}(x-\alpha_k)^{p^r}$ alakban, ahol $\alpha_k\in N$ páronként különböző elemek, $r\in\mathbb{N}$.

Bizonyítás: mivel $N|K$ normális, f_0 felbomlik lineáris faktorok szorzatára: $f_0(x)=\prod_{k=1}^{n}(x-\alpha_k)^{s_k}$, ahol az α_k-k páronként különböző N-beli elemek, $s_k\in\mathbb{Z}^+$. Ha f_0 inszeparábilis, akkor előáll $\sum_{i=1}^{m}a_{ip}x^{ip}$ alakban. Legyen $f_1(x)=\sum_{i=1}^{m}a_{ip}x^i$, így $f_0(x)=f_1(x^p)$. f_1-nek gyöke $\alpha_k^p\in L$, ezért felbomlik lineáris faktorok szorzatára: $f_1(x)=\prod_{j=1}^{l}(x-\beta_j)^{t_j}$, amiből $\prod_{k=1}^{n}(x-\alpha_k)^{s_k}=f_0(x)=f_1(x^p)=\prod_{j=1}^{l}(x^p-\beta_j)^{t_j}$.

A bal oldalon $N[x]$-ben irreducibilis (lineáris) polinomok szorzata áll $\Rightarrow$ a jobb oldal minden $(x^p-\beta_j)$ tényezőjét osztja valamely $(x-\alpha_{k(j)})$, azaz gyöke $\alpha_{k(j)}$ $\Rightarrow$ $\alpha_{k(j)}^p=\beta_j$ $\Rightarrow$ $x^p-\beta_j=x^p-\alpha_{k(j)}^p=(x-\alpha_{k(j)})^p$. Továbbá minden α_k p-edik hatványa gyöke f_1-nek, tehát a β_j-k éppen az α_k^p számok: $f_1(x)=\prod_{k=1}^{n}(x-\alpha_k^p)^{t_k}$ és $f_0(x)=\prod_{k=1}^{n}(x^p-\alpha_k^p)^{t_k}=\prod_{k=1}^{n}(x-\alpha_k)^{p\cdot t_k}$.

Ha f_1 szeparábilis, akkor minden t_k 1 és az állítás $r=1$ választással teljesül. Ha f_1 is inszeparábilis, akkor $\sum a_{i\cdot p^2}x^{ip}$ alakú, legyen $f_2(x)=\sum a_{i\cdot p^2}x^i$. Ennek gyökei hasonló módon éppen az α_k számok p^2-edik hatványai és az α_k gyök multiplicitása f_0-ban p^2-szerese az $\alpha_k^{p^2}$ gyök f_2-beli multiplicitásának. Ezt folytatva valamelyik f_r szeparábilis lesz (amíg nem szeparábilis, addig tovább tudunk lépni és idővel meg kell állnunk, mert $deg\, f_i$ szigorúan csökken), ekkor $f_r(x)=\prod_{k=1}^{n}\left(x-\alpha_k^{p^r}\right)$ és $f_0(x)=f_r\left(x^{p^r}\right)=\prod_{k=1}^{n}(x-\alpha_k)^{p^r}$.

11.2.10 Következmény: ha α inszeparábilis K felett, akkor alkalmas hatványa szeparábilis, továbbá ezen hatvány kitevője p hatványa és $gr_K\alpha$ osztója.

Bizonyítás: legyen f α kanonikus polinomja K felett, L pedig f felbontási teste, majd alkalmazzuk az előző állítást.

11.2.11 Definíció: legyen $K\le L$ és $\alpha\in L$ algebrai K felett. α-t tisztán inszeparábilisnek nevezzük, ha kanonikus polinomjának egyetlen gyöke α (a felbontási testben). Az $L|K$ bővítés tisztán inszeparábilis, ha minden eleme tisztán inszeparábilis.

11.2.12 Lemma: az $L|K$ bővítésben α tisztán inszeparábilis $\Leftrightarrow$ $\alpha\in K$, vagy $char\, K=p>0$ és $\alpha^{p^n}\in K$ valamely $n\in\mathbb{N}$-re.

Bizonyítás: $\alpha\in K$ esetén az állítás igaz. Szorítkozhatunk tehát az $\alpha\in L\setminus K$ esetre. Ekkor ha α tisztán inszeparábilis, akkor inszeparábilis, azaz $char\, K=p>0$.

$\Rightarrow$: ha α tisztán inszeparábilis, akkor kanonikus polinomja $(x-\alpha)^m$ alakú, ahol $x-\alpha$ alacsonyabb hatványa még nincs benne $K[x]$-ben. Legyen $m=p^n\cdot s$, ahol $p\nmid s$. $\nuparrow$ $s\ne 1$, ekkor $(x-\alpha)^{p^n}\notin K[x]$. Ha ennek legkisebb indexű $L\setminus K$-beli együtthatója a_t, akkor $(x-\alpha)^m=\left((x-\alpha)^{p^n}\right)^s$-ben x^t együtthatója $s\cdot a_t+(\dots)$, ahol a fel nem sorolt tagok K-beliek. $s\cdot a_t\notin K$, azaz $(x-\alpha)^m\notin K[x]$, $\lightning$. Így hát $s=1$, ebből $(x-\alpha)^{p^n}=x^{p^n}-\alpha^{p^n}\in K[x]$ és $\alpha^{p^n}\in K$.

$\Leftarrow$: legyen $\alpha^{p^n}\in K$. Ekkor α gyöke $(x-\alpha)^{p^n}=x^{p^n}-\alpha^{p^n}\in K[x]$-nek, tehát kanonikus polinomja osztja $(x-\alpha)^{p^n}$-t. Ennek egyetlen gyöke α, azaz a kanonikus polinomnak is.

Megjegyzés: a lemmából látszik, hogy ha $K\le L$ és α inszeparábilis K felett, akkor L felett is az. Ezt gyakran ki fogjuk használni.

11.2.13 Állítás: ha β tisztán inszeparábilis K felett, akkor $K(\beta)|K$ tisztán inszeparábilis bővítés.

Bizonyítás: azt fogjuk belátni, hogy ha $\beta^q\in K$: $q=p^r$, akkor $\forall\gamma\in K(\beta)$ elemre $\gamma^q\in K$. Nos, γ előáll $\gamma=g_\gamma(\beta)=\sum_{k=0}^{q-1}c_k\beta^k$: $c_k\in K$ alakban. Ekkor $\gamma^q=\left(g_\gamma(\beta)\right)^q=\sum_{k=0}^{q-1}c_k^q\cdot(\beta^q)^k\in K$, azaz γ valóban tisztán inszeparábilis.

11.2.14 Állítás: ha $M|L$ és $L|K$ tisztán inszeparábilis bővítések, akkor $M|K$ is az. Ugyanis tetszőleges $\alpha\in M$ elem alkalmas $q=p^r$-edik hatványa L-beli, e hatvány alkalmas $q'=p^{r'}$-edik hatványa pedig már K-beli.

11.2.15 Következmény: ha $\beta_1,\dots,\beta_n$ tisztán inszeparábilisek K felett, akkor $K(\beta_1,\dots,\beta_n)|K$ tisztán inszeparábilis bővítés.

Bizonyítás: az előző állítás szerint elegendő belátni, hogy $K(\beta_1,\dots,\beta_k)|\,K(\beta_1,\dots,\beta_{k-1})$ tisztán inszeparábilis. Mivel β_k tisztán inszeparábilis például $K(\beta_1,\dots,\beta_{k-1})$ felett is, **11.2.13** miatt kész vagyunk.

11.2.16 Lemma: ha α szeparábilis K felett, akkor $K(\alpha)\setminus K$-ban nincs tisztán inszeparábilis elem.

Bizonyítás: legyen α kanonikus polinomja f, foka n. $\nuparrow$ $\exists\beta\in K(\alpha)\setminus K$ tisztán inszeparábilis elem, azaz $\beta^q\in K, q=p^r$. Állítsuk elő β-t α legfeljebb $n-1$-edfokú, K-beli együtthatós polinomjaként: $\beta=g(\alpha)$. Ekkor α gyöke a $K(\beta)[x]$-beli $g(x)-\beta$ polinomnak. Legyen α kanonikus polinomja $K(\beta)$ felett $h(x)=\sum_{k=0}^{d}\gamma_k x^k$. $h(x)$ osztja $\left(g(x)-\beta\right)$-t, így $deg(h)\le deg(g)\le n-1<gr_K(\alpha)=deg(f)$. α szeparábilis K felett, tehát h-nak határozottan kevesebb gyöke van, mint f-nek. Továbbá $\vartheta(x):=\left(h(x)\right)^q=\sum_{k=0}^{d}\gamma_k^q\cdot x^{kq}\in K[x]$, mert $c_k\in K(\beta)$ miatt $c_k^q\in K$ (ld. **11.2.13** bizonyítását). $\vartheta(a)=0$, így $K[x]$-ben $f|\vartheta$. Viszont ϑ-nak ugyanannyi különböző gyöke van, mint h-nak, tehát kevesebb, mint f-nek, $\lightning$.

11.2.17 Következmény: ha $N|K$ egy szeparábilis bővítés normális lezárása, akkor $N\setminus K$-ban nincs tisztán inszeparábilis elem.

Bizonyítás: jelölje az említett véges szeparábilis bővítést $L|K$. $\nuparrow$ $\exists\gamma\in N\setminus K$ tisztán inszeparábilis elem. Ezen γ elem N-en belül belefoglalható egy véges bővítésbe, amely persze előáll $K(\alpha_1,\dots,\alpha_m)$ alakban, ahol minden α_i vagy L-beli, vagy egy L-beli konjugáltja, továbbá $\gamma\notin K(\alpha_1,\dots,\alpha_{m-1})$. Mivel α_m szeparábilis K felett, még inkább

szeparábilis $K'=K(\alpha_1,\dots,\alpha_{m-1})$ felett, hasonlóan γ tisztán inszeparábilis K' felett. De az iménti lemma szerint $K'(\alpha_m)\setminus K'$-ben nincs K' felett tisztán inszeparábilis elem, $\lightning$.

11.2.18 Tétel: ha $N|K$ normális, inszeparábilis bővítés, akkor $N\setminus K$-ban van tisztán inszeparábilis elem. Átfogalmazva: ha egy normális bővítésben nincs nem-triviális tisztán inszeparábilis elem, akkor a bővítés szeparábilis.

Bizonyítás: legyen $\beta\in N\setminus K$ inszeparábilis. Ekkor K feletti kanonikus polinomja – jelölje $f(x)$ – $N[x]$-ben lineáris faktorokra bomlik, azaz $f(x)=\prod_{k=1}^{m}(x-\beta_k)^q \;:\; q=p^r$. A $g(x)=\prod_{k=1}^{m}(x-\beta_k)=\sum_{k=0}^{m}\gamma_k x^k$ jelöléssel $\sum_{k=0}^{m}\gamma_k^q x^{kq}=\big(g(x)\big)^q=f(x)\in K[x]$. Ezért $\forall k\colon \gamma_k^q\in K$, így minden γ_k tisztán inszeparábilis K felett. Továbbá nem lehet mind K-beli, mert akkor $g(x)\in K[x]$ lenne és $f(x)=\big(g(x)\big)^q$ nem lenne irreducibilis $K[x]$-ben.

11.2.19 Következmény: szeparábilis bővítés normális lezárása szeparábilis, mert nincs benne nem-triviális tisztán inszeparábilis elem.

11.2.20 Tétel: ha $\alpha_\kappa \;:\; \kappa\in\mathbf{I}$ szeparábilisek K felett, akkor $K(\alpha_k\colon \kappa\in\mathbf{I})|K$ szeparábilis.

Bizonyítás: elég belátni, hogy a normális lezárás szeparábilis. Ezt megkaphatjuk úgy, hogy K-hoz az összes α_κ összes konjugáltját adjungáljuk, azaz előáll $N=K(\alpha'_\lambda\colon \lambda\in\mathbf{J})$ alakban, ahol minden α'_λ szeparábilis K felett. Vegyünk egy tetszőleges $\beta\in N\setminus K$ elemet. Ez benne van egy olyan normális bővítésben is, ahol csak véges sok $\alpha'_i \;:\; i=1\dots m$ elemet adjungálunk K-hoz. $\lightning\ \beta$ inszeparábilis. Ekkor $M\setminus K$-ban **11.2.18** miatt van egy γ tisztán inszeparábilis elem. Ez viszont ugyanúgy lehetetlen, mint **11.2.17** bizonyításánál, $\lightning$.

11.2.21 Lemma: ha $N|K$ normális bővítés és $f(x)\in K[x]$ irreducibilis, akkor f $N[x]$-ben irreducibilis faktorai vagy mind szeparábilisek, vagy mind inszeparábilisek.

Bizonyítás: ha minden faktor szeparábilis, akkor kész vagyunk. Legyen hát $g\in N[x]$ inszeparábilis irreducibilis faktor. Ekkor $g(x)$-ben az x^{kp} hatványokhoz tartozók kivételével minden együttható 0. Ha az együtthatók helyére konjugáltjaikat írjuk, a 0-k megmaradnak. így az inszeparábilitás is. **11.1.9** szerint ily módon f minden $N[x]$-beli irreducibilis faktora megkapható, tehát ezek egytől-egyig inszeparábilisek.

11.2.22 Tétel: szeparábilis bővítés szeparábilis bővítése szeparábilis, azaz ha $L|K$ és $M|L$ szeparábilis, akkor $M|K$ is. Másképp megfogalmazva: ha $L|K$ szeparábilis és α szeparábilis L felett, akkor K felett is az.

Bizonyítás: legyen $L|K$ szeparábilis bővítés, $N|K$ a normális lezárása, α szeparábilis L felett. Azt kell belátnunk, hogy α szeparábilis K felett. Tudjuk a **11.2.19 következményből**, hogy $N|K$ is szeparábilis. Persze α az N felett is szeparábilis.

Legyen α kanonikus polinomja K felett f, N felett g. Jelölje $\alpha_1=\alpha,\alpha_2,\dots,\alpha_n$ f gyökeit a felbontási testben. Mivel g szeparábilis, a **11.2.21** lemma szerint $N[x]$-ben f minden irreducibilis faktora szeparábilis. Bármely α_i elem N feletti kanonikus polinomja f valamely irreducibilis faktora, azaz minden α_i szeparábilis N felett.

Legyen $M=N(f)=N(\alpha_1,\dots,\alpha_n)$. Ekkor $M|N$ normális és a **11.2.20** tétel szerint szeparábilis. Azaz $M\setminus N$-ben nincs N felett tisztán inszeparábilis elem, így K felett tisztán inszeparábilis sem. Szintén nincs K felett tisztán inszeparábilis elem $N\setminus K$-ban, összefoglalva az egész $M\setminus K$-ban nincs. Azaz a $K(f)\le M$ normális bővítésre $K(f)\setminus K\subseteq M\setminus K$ nem tartalmaz K felett tisztán inszeparábilis elemet, így **11.2.18** szerint szeparábilis.

11.2.23 Állítás: tetszőleges $L|K$ bővítéshez található olyan S közbülső test, hogy $S|K$ szeparábilis és $L|S$ tisztán inszeparábilis bővítés. Speciálisan a K felett szeparábilis L-beli elemek résztestet alkotnak.

Bizonyítás: tekintsünk egy, a Zorn-lemma szerint létező maximális szeparábilis bővítést L és K között. Legyen ez S. $\beta\in L\setminus S$ esetén β nem lehet szeparábilis K felett, hiszen akkor S felett is szeparábilis lenne, **11.2.20** és **11.2.22** alapján $S(\beta)|S$ és $S(\beta)|K$ is szeparábilis bővítés lenne, ami ellentmond S maximalitásának. Azaz S éppen $L\setminus K$ szeparábilis elemeiből áll.

Legyen $\beta\in L$ tetszőleges és vegyük a **11.2.10**-ben nyert szeparábilis hatványát. Ez persze S-beli, azaz β tisztán inszeparábilis S felett.

11.3 Véges testek

11.3.1 Megjegyzés: ha $a\in\mathbb{N}$, $a>1$. akkor az euklideszi algoritmus alapján $a^d-1\,|\,a^n-1 \Leftrightarrow d\,|\,n$. Ugyanígy $x^d-1\,|\,x^n-1 \Leftrightarrow d\,|\,n$.

11.3.2 Tétel: tetszőleges $f\in\mathbb{Z}^+$, p prím esetén pontosan egy $q=p^f$ elemű test létezik és minden véges test ilyen.

Bizonyítás: legyen K tetszőleges véges test. Ekkor $char\,K$ nem 0, azaz p prím. $\{0,1,1+1,\dots,p-1\}$ zárt a műveletekre, így egy $\mathbb{F}_p$-vel izomorf résztestét adja K-nak. Eszerint K véges vektortér $\mathbb{F}_p$ felett. Dimenzióját f-el jelölve $(K,+)\simeq(\mathbb{F}_p^f,+)$, speciálisan $|K|=q$. Az állítás második felét ezzel beláttuk. Lássuk most be, hogy valóban létezik p^f elemű test.

Tekintsük a $\vartheta(x)=x^q-x\in\mathbb{F}_p[x]$ polinomot. Legyen K ennek egy felbontási teste. $\vartheta(x)$ minden gyöke egyszeres, mert deriváltja -1, azaz $(\vartheta,\vartheta')=1$.

Lemma: ϑ gyökei résztestet alkotnak K-ban. Ugyanis ha a,b gyöke ϑ-nak, akkor $a^q=a$ és $b^q=b$, amiből $(a\pm b)^q=a^q\pm b^q=a\pm b$ a binomiális tétel szerint, $(a^{-1})^q=(a^q)^{-1}=a^{-1}$ és $(ab)^q=a^qb^q=ab$ csak úgy. Összefoglalva $a\pm b, a^{-1}, ab$ is gyöke ϑ-nak.

Eszerint K személyesen a ϑ gyökeiből álló halmaz, azaz egy q elemű test. Már csak az egyértelműség van hátra.

Legyen K egy q elemű test. Ekkor K^* egy $q-1$ elemű (kommutatív) csoport $\Rightarrow\ \forall\in K^*\colon \alpha^{q-1}=1 \Rightarrow \forall\alpha\in K\colon \alpha^q-\alpha=0$. Tehát K minden eleme gyöke a fenti ϑ-nak, elemei tehát épp ϑ összes gyökét adják, K pedig ϑ egyértelmű felbontási teste.

Bizonyítás II.: jelölje $\mathbb{F}_p$-t K. Azt állítjuk, hogy K felett van f-edfokú irreducibilis polinom. Ha ez igaz, akkor ennek egy α gyökét adjungálva K-hoz f-edfokú bővítést, azaz p^f elemű testet kapunk. (Az egyértelműséget ugyanúgy bizonyítjuk, mint az előbb.) Legyen $F_d(x)$ a K feletti 1 főegyütthatójú d-edfokú irreducibilis polinomok szorzata (ilyenből véges sok van, tehát a szorzat értelmes). Legyen továbbá $\pi(x)=\prod_{d:\,d|f}F_d(x)$.

Lemma: egy $g(x)\in K[x]$ d-edfokú irreducibilis polinom pontosan akkor osztja $\varphi(x)=(x^q-x)$-et, ha $d\,|\,f$.

Bizonyítás: $\Rightarrow$: $g(x)\,|\,\varphi(x)$ esetén legyen α gyöke g-nek. Ekkor $[K(\alpha):K]=d$. $K(\alpha)$ multiplikatív csoportjának rendje p^d-1, tehát $K(\alpha)$ minden eleme gyöke $\left(x^{p^d}-x\right)$-nek. Ez p^d különböző gyök, így $x^{p^d}-x$ összes gyöke éppen $K(\alpha)$. $K(\alpha)$-ban minden elem előáll α legfeljebb $d-1$-edfokú K-beli együtthatós polinomjaként. Egy tetszőleges β elemére tehát $\beta^q=(b_0+b_1\alpha+\dots+b_{d-1}\alpha^{d-1})^q=b_0+b_1\alpha+\dots+b_{d-1}\alpha^{d-1}$, mert $b_i\in K$ miatt $b_i^q=b_i$ és $g(\alpha)=0$, $g(x)\,|\,\varphi(x)$ miatt $\alpha^q=\alpha$. Eszerint $x^{p^d}-x$ minden gyöke gyöke $\varphi(x)$-nek is, azaz $x^{p^d}-x\,|\,x^q-x \Rightarrow p^d-1\,|\,p^f-1 \Rightarrow d\,|\,f$.

$\Leftarrow$: $d\,|\,f$-ből $x^{p^d}-x\,|\,\varphi(x)$. Ha g d-edfokú irreducibilis és α egy gyöke, akkor a fenti módon $K(\alpha)$ minden eleme gyöke $\left(x^{p^d}-x\right)$-nek, így $\varphi(x)$-nek is. Speciálisan $\varphi(\alpha)=0$, azaz α kanonikus polinomja – ez éppen g – osztja φ-t.

Következmény: $\varphi(x)=\pi(x)$. Ugyanis a lemma szerint π minden tényezője osztja φ-t és φ minden gyökének kanonikus polinomja szerepel π definíciójában. Így a két oldal gyökei megegyeznek. π-nek minden gyöke egyszeres, mert páronként különböző 1 főegyütthatójú irreducibilis polinomok szorzata. φ-nak szintén minden gyöke egyszeres, mert deriváltja -1.

Legyen most N_d a d-edfokú, 1 főegyütthatós K feletti irreducibilis polinomok száma. A $deg(x^q-x)=deg\left(\prod_{d:\,d|f}F_d(x)\right)$ egyenlőségből $p^f=\sum_{d:\,d|f}d\cdot N_d$ minden f-re. Ebből Möbius-transzformálással $f\cdot N_f=\sum_{d|f}p^d\cdot\mu\left(\frac{f}{d}\right)=(p^f+\mu_1p^{f-1}+\dots)$; az első tag a $d=f$ esetből jön. Mindenhol máshol p kisebb hatványai szerepelnek és az együtthatók $1,-1,0$ közül valók. A teljes összeg értéke pozitív, mert p^f-et nem lehet ellensúlyozni. Ezért $N_f\neq0$ és épp ezt akartuk belátni.

11.3.3 Definíció: a $q=p^f$ elemű testet $\mathbb{F}_q$-val vagy $GF(q)$-val jelöljük.

11.3.4 Állítás: $\mathbb{F}_q$ multiplikatív csoportja $\mathbb{F}_q^*\simeq Z_{q-1}$.

Bizonyítás: jelölje $\mathbb{F}_q$-t az egyszerűség kedvéért K. $\forall a\in K^*\colon o(a)\,|\,q-1$, mert egy csoportelem rendje osztja a csoport rendjét. Jelölje $d\,|\,q-1$ esetén $\psi(d)$ a K^*-beli d-edrendű elemek számát. Ha $\psi(d)\geq1$, akkor legyen a olyan, hogy $o(a)=d$. Ekkor az $1,a,a^2,a^3,\dots,a^{d-1}$ elemek páronként különbözőek és mindegyikre teljesül $x^d-1=0$. Ezek tehát x^d-1 összes gyökét adják K-ban, köztük van minden d-edrendű elem. $1,a,a^2,a^3,\dots,a^{d-1}$ közül pontosan azok

d-edrendűek, melyek kitevője relatív prím d-hez. Így ha $\psi(d)\neq 0$, akkor $\psi(d)=\varphi(d)$. Minden K^*-beli elemnek pontosan egy rendje van, így

$$|K^*|=q-1=\sum_{d:\, d|q-1}\psi(d)\leq\sum_{d:\, d|q-1}\varphi(d)=q-1.$$

Egyenlőség áll fenn, azaz minden $d|q-1$ esetén egyenlőség áll fenn, speciálisan $\psi(q-1)\neq 0$, azaz K^*-ban van $q-1$-edrendű elem (ún. primitív gyök). Az ezen elem által generált részcsoport $q-1$ elemű, így maga K^*. Eszerint K^*-ot generálja egy eleme $\Rightarrow$ $K^*\simeq Z_{q-1}$.

Megjegyzés: $\mathbb{F}_q\leq\mathbb{F}_r \Rightarrow q$ és r ugyanazon p prím hatványai, hiszen ekkor $char\,\mathbb{F}_q=|\{0,1,1+1,\ldots\}|=char\,\mathbb{F}_r$.

11.3.5 Állítás: $\mathbb{F}_{p^d}\leq\mathbb{F}_{p^f} \Leftrightarrow d|f$.

Bizonyítás: $\Rightarrow$ ha $\mathbb{F}_{p^d}\leq\mathbb{F}_{p^f}$, akkor $\mathbb{F}_{p^f}$ egy $\mathbb{F}_{p^d}$ feletti véges dimenziós vektortér, azaz $p^f=|\mathbb{F}_{p^f}|=|\mathbb{F}_{p^d}|^{\mathbf{dim}}=p^{d\cdot\mathbf{dim}}$.

$\Leftarrow$: $d|f \Leftrightarrow p^d-1|p^f-1 \Leftrightarrow x^{p^d-1}-1\,|\,x^{p^f-1}-1\;x^{p^d}-x\,|\,x^{p^f}-x \Leftrightarrow$ a bal oldali polinom $\mathbb{F}_p$ feletti felbontási teste résztest a másik felbontási testben $\Leftrightarrow \mathbb{F}_{p^d}\leq\mathbb{F}_{p^f}$.

11.3.6 Állítás: $Aut(\mathbb{F}_{p^f})=\langle\varphi\rangle\simeq Z_f$, ahol $\varphi: a\mapsto a^p$ a Frobenius-automorfizmus.

Bizonyítás: **11.2.6** szerint φ művelettartó. A magja ideál, ferde testben viszont csak két ideál van, (0) és (1). Ez utóbbi nem lehet $Ker\,\varphi$, hiszen $1\varphi=1$, azaz $Ker\,\varphi=\{0\}$, φ injektív. Mivel $\mathbb{F}_{p^f}$ véges, bijektív. Tehát $\varphi\in Aut(\mathbb{F}_{p^f})$. $\varphi: a\mapsto a^p$, $\varphi^2: a\mapsto a^{p^2}$, …, $\varphi^f: a\mapsto a^{p^f}$. $\mathbb{F}_{p^f}^*$ ciklikus, tehát van p^f-1 rendű eleme, ezt legelőször φ^f viszi önmagába. Így $o(\varphi)=f$.

Másrészt $\mathbb{F}_{p^f}$ minden ψ automorfizmusa helybehagyja az $1,1+1,\ldots$ elemeket, tehát a beágyazott $\mathbb{F}_p$-t. ψ természetesen kiterjed egy $\mathbb{F}_p[x]$ feletti automorfizmussá, amely $\mathbb{F}_p[x]$-re megszorítva identitás. Legyen α a multiplikatív csoport egy generátoreleme, kanonikus polinomja g. Persze $deg\,g\leq f$. Ekkor α képe gyöke $g\psi=g$-nek és α képe már meghatározza az automorfizmust $\Rightarrow$ legfeljebb annyi automorfizmus van, ahány gyöke g-nak, azaz legfeljebb f. Ezzel az állítást beláttuk.

11.3.7 Következmény: $\mathbb{F}_q$ perfekt. Ugyanis $\varphi: a\mapsto a^p$ automorfizmus, azaz minden elemnek van p-edik gyöke.

11.3.8 Wedderburn-tétel: minden véges ferdetest kommutatív.

Bizonyítás (Witt): legyen D véges ferdetest. Tekintsük D centrumát, F-et. F nem üres és zárt a kivonásra. $F^*=Z(D^*)$ miatt a szorzásra és a multiplikatív inverzképzésre is, tehát résztest D-ben. F véges test, így **11.3.2** szerint $\mathbb{F}_q$-val izomorf valemely $q=p^f$-re, D pedig egy F feletti véges vektortér. Legyen dimenziója n. Azt akarjuk belátni, hogy $n=1$.

$|D^*|=q^n-1$. Bontsuk D^*-ot konjugált osztályokra. Jelölje α konjugált osztályának méretét $c(\alpha)$. Legyen $\alpha\in D\setminus F$, ekkor $c(\alpha)=|F^*: C_{D^*}(\alpha)|$. Könnyen látható, hogy a D-beli centralizátor, $C_D(\alpha)=C_{D^*}(\alpha)\cup\{0\}$ részferdetest D-ben, speciálisan vektortér F felett, ezért $q^{d(\alpha)}$ elemű. Így $C_{D^*}(\alpha)$ indexe F^*-ban $\frac{q^n-1}{q^{d(\alpha)}-1}$. Mivel $\alpha\notin Z(D)$, $C_D(\alpha)\neq D$, azaz $d(\alpha)<n$. Tudjuk, hogy $q^{d(\alpha)}-1|q^n-1$ miatt $d(\alpha)|n$. Ha $\alpha\in F$, akkor $c(\alpha)=1$.

Legyen $\Phi_n(x)$ az n-edik körosztási polinom (az a $\mathbb{Z}[x]$-beli polinom, melynek gyökei a primitív n-edik komplex egységgyökök).

Lemma: ha $d<n$ és $d|n$, akkor $\Phi_n(x)$ osztja $\frac{x^n-1}{x^d-1}$-t. Ugyanis $\frac{x^n-1}{x^d-1}$ gyökei pontosan azok az n-edik egységgyökök, melyek nem d-edik egységgyökök – minden primitív n-edik egységgyök ilyen.

Jelölje $\Phi_n(q)$-t r. Ez egy egész szám és minden $d(\alpha)<n$, $d(\alpha)|n$ esetén osztja $\frac{x^n-1}{x^{d(\alpha)}-1}$-t. Tehát r minden F^*-on kívüli konjugált osztály méretét osztja, továbbá D^* méretét is. Osztja tehát F^* méretét, $q-1$-et is. $r=\prod_{k:\,(n,k)=1}(q-\varepsilon_n^k)$. $\nexists\ n>1$, ekkor ez néhány – de legalább egy – $q-1$-nél nagyobb abszolútértékű komplex szám szorzata. Tehát ha $n>1$, akkor $|r|>q-1$, ami $r|q-1$ fényében $\lightning$.

11.4 Galois-csoport és alkalmazásai

11.4.1 Definíció: az $L|K$ bővítés Galois-bővítés, ha véges, normális és szeparábilis.

11.4.2 Tétel: ha $L|K$ véges, szeparábilis bővítés, akkor egyszerű.

Bizonyítás: ha K véges test, akkor L is az, tehát multiplikatív csoportja ciklikus. Egy generálóelemet adjungálva az egész L-t megkapjuk, tehát $L|K$ egyszerű.

Legyen most $|K|$ végtelen. Először azt látjuk be, hogy ha $K(\alpha,\beta)$ véges, szeparábilis bővítés, akkor előáll $K(\vartheta)$ alakban. Legyen α kanonikus polinomja f, β kanonikus polinomja g, továbbá fg felbontási testében – jelölje M – $f(x)=(x-\alpha_1)\cdot(x-\alpha_2)\cdot\ldots\cdot(x-a_n)$ és $g(x)=(x-\beta_1)\cdot\ldots\cdot(x-\beta_k)$, ahol $\alpha_1=\alpha,\beta_1=\beta$. Tekintsük az $\alpha_i+x\beta_j=\alpha+x\beta$ egyenletek $z_{ij}=\frac{\alpha-\alpha_i}{\beta_j-\beta}$ megoldásait, ahol $j\neq 1$. Mivel $L|K$ szeparábilis, $\beta_j\neq\beta$, tehát ezek értelmesek. Véges sok z_{ij} van, azaz található K-nak olyan c eleme, amely ezek egyikével sem egyezik meg. Legyen $\vartheta=\alpha+c\beta$. Ekkor $K(\vartheta)\leq K(\alpha,\beta)$. Tekintsük $K(\vartheta)[x]$-ben a $g(x),f(\vartheta-cx)$ polinomokat. β gyöke mindkettőnek és mindkettő lineáris faktorokra bomlik az $M|K$ normális bővítésban. Más közös gyökük nem lehet, hiszen $\vartheta-c\beta_j$ nem egyezhet meg semelyik α_i-vel c választása folytán. Így $g(x)$ és $f(\vartheta-cx)$ legnagyobb közös osztója $x-\beta$. Két $K(\vartheta)[x]$-beli polinom legnagyobb közös osztója is $K(\vartheta)[x]$-beli, így a β együttható eleme $K(\vartheta)$-nak. Ekkor persze $\alpha=\vartheta-c\beta$ is, azaz $K(\alpha,\beta)=K(\vartheta)$.

Legyen L a K végtelen test véges, szeparábilis bővítése. Minden véges bővítés előáll véges sok elem adjungálásával, azaz $L=K(\alpha_1,\ldots,\alpha_n)$. Alkalmazzunk n szerinti indukciót. $n=1$ esetén az állítás igaz. Ha $n>1$, akkor legyen $M=(\alpha_1,\ldots,\alpha_{n-1})$. $M|K$ véges szeparábilis bővítés, így az indukciós feltétel szerint egyszerű: $M=K(\beta)$. Az előző bekezdés szerint ekkor $L=K(\vartheta,\alpha_n)$ is egyszerű.

11.4.3 Megjegyzés: egy $\varphi:K\to L$ ferdetestek közti homomorfizmus vagy beágyazás (injekció, monomorfizmus), vagy $Im\,\varphi=\{0\}$ (triviális homomorfizmus). Ugyanis $Ker\,\varphi\lhd K$, de ferdetestben összesen két ideál van, (0) és (1) – ez épp a fenti két esetet adja.

11.4.4 Definíció: legyenek K,L,M testek, $K\leq L$ és $K\leq M$. A $\varphi:L\to M$ leképezés K-homomorfizmus, ha homomorfizmus és K-ra megszorítva identitás. K-monomorfizmus, ha nem triviális K-homomorfizmus. Az $L|K$ bővítésnél L K-automorfizmusait relatív automorfizmusnak is szoktuk nevezni.

11.4.5 Definíció: az $L|K$ testbővítés Galois-csoportja az L test K-automorfizmusainak csoportja a kompozícióra. (Gondoljuk meg, hogy ez valóban csoport.) Jelölése $\Gamma(L|K)$.

Példák:

– $\Gamma\left(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}\right)=\{1\}$. Ugyanis $\mathbb{Q}(\sqrt[3]{2})$ minden ψ $\mathbb{Q}$-automorfizmusa generálja $\mathbb{Q}(\sqrt[3]{2})[x]$ egy $\mathbb{Q}[x]$-automorfizmusát (ezek ugyan gyűrűk, de a fogalom itt is ugyanúgy definiálható). $(\sqrt[3]{2})\psi$ gyöke $(x^3-2)\psi=(x^3-2)$-nek. A másik két gyök komplex, azaz nincs benne $\mathbb{Q}(\sqrt[3]{2})$-ben, tehát $(\sqrt[3]{2})\psi$ csak $\sqrt[3]{2}$ lehet, azaz ψ az identitás.

– $\Gamma(\mathbb{R}|\mathbb{Q})=\{1\}$, mert $\mathbb{Q}$ sűrű $\mathbb{R}$-ben és $\mathbb{R}$ minden automorfizmusa rendezéstartó, ugyanis $a<b$ pontosan akkor teljesül, ha (x^2+a-b)-nek van gyöke $\mathbb{R}\setminus\{0\}$-ban, ez utóbbi tulajdonságot pedig $\mathbb{R}$ minden automorfizmusa helybenhagyja.

Innentől a leképezéseket felső indexszel jelöljük, mint a permutációcsoportoknál tettük.

11.4.6 Tétel: ha $L|K$ Galois-bővítés, akkor $|\Gamma(L|K)|=[L:K]$.

Bizonyítás: $L|K$ véges szeparábilis bővítés, így egyszerű: $L=K(\alpha)$. Legyen α kanonikus polinomja f. Mivel $L|K$ normális, f lineáris faktorokra bomlik $L[x]$-ben: $f(x)=(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$, ahol $n=deg\,f=gr_K(\alpha)=[L:K]$. L minden ψ K-automorfizmusa kiterjed $L[x]$ egy $K[x]$-automorfizmusává, azaz $f^\psi=f$. Ebből $0=0^\psi=\left(f(\alpha)\right)^\psi=f^\psi(\alpha^\psi)=f(\alpha^\psi)$. Azaz α képe valamely α_i, így Γ legfeljebb n elemű, hiszen α képe már meghatározza az automorfizmust. Másrészt $\alpha\mapsto\alpha_i$ minden $i\in\{1,\ldots,n\}$-re kiterjeszthető L egy K-automorfizmusává és ezek különbözőek, mert $L|K$ szeparábilis, tehát az α_i-k különbözőek.

11.4.7 Definíció: az $\lambda_1,\lambda_2,\ldots,\lambda_n:K\to L$ testhomomorfizmusok lineárisan összefüggőek, ha valamely $\alpha_1,\ldots,\alpha_n\in L$ nem csupa 0 számokra $\alpha_1\lambda_1+\alpha_2\lambda_2+\ldots+\alpha_n\lambda_n$ az azonosan 0 leképezés. Ha ez nem teljesül, akkor lineárisan függetlenek.

11.4.8 Tétel (Dedekind): ha $\lambda_1,\lambda_2,\ldots,\lambda_n:K\to L$ páronként különböző monomorfizmusok, akkor lineárisan függetlenek.

Bizonyítás: $\nexists\ \sum_{k=1}^n\alpha_k\lambda_k=0$ valamely $(\alpha_k)_{k=1}^n$ nem csupa 0 számokra. Tekintsünk egy olyan ellenpéldát, amelynél n minimális (ekkor nyilván egyik α_k sem 0). $n>1$, mert egy egyetlen monomorfizmusból álló halmaz nem lehet lineárisan összefüggő, hiszen $\alpha_1\lambda_1$-ben $1\in K$ képe $\alpha_1\in L\setminus\{0\}$. Legyen $c\in K\setminus\{0\}$ tetszőleges elem.

$$\begin{array}{rl} \underline{\odot} & \alpha_1(cx)^{\lambda_1}+\alpha_2(cx)^{\lambda_2}+\ldots+\alpha_n(cx)^{\lambda_n}=0 \\ \underline{\boxdot} & \alpha_1\cdot x^{\lambda_1}+\alpha_2\cdot x^{\lambda_2}+\ldots+\alpha_n\cdot x^{\lambda_n}=0 \\ \odot-c^{\lambda_n}\cdot\boxdot & \alpha_1\cdot\left(c^{\lambda_1}-c^{\lambda_n}\right)\cdot x^{\lambda_1}+\ldots+\alpha_{n-1}\cdot\left(c^{\lambda_{n-1}}-c^{\lambda_n}\right)\cdot x^{\lambda_{n-1}}=0 \end{array}$$

Válasszuk c-t úgy, hogy $c^{\lambda_1}\neq c^{\lambda_n}$ teljesüljön. Ezt megtehetjük, hiszen $\lambda_1\neq\lambda_2$. Ekkor $\alpha_k'=\alpha_k\cdot\left(c^{\lambda_k}-c^{\lambda_n}\right)$ választással találtunk egy $n-1$ elemű ellenpéldát, ↯.

11.4.9 Tétel: ha K test, G pedig $Aut(K)$ véges részcsoportja, akkor $K_0=\{\alpha\in K\,|\,\forall g\in G\colon \alpha^g=\alpha\}$ résztest K-ban és $[K\colon K_0]=|G|$.

Bizonyítás: $K_0\leq K$ nyilvánvaló. Legyen $G=\{\lambda_1,\lambda_2,\ldots,\lambda_m\}$, $m=[K\colon K_0]$.

↾ $m<n$. Legyen $x_1,\ldots,x_m$ K bázisa K_0 felett. Tekintsük $y_1,\ldots,y_n$-re az alábbi homogén lineáris egyenletrendszert:

$$\begin{array}{c} x_1^{\lambda_1}\cdot y_1+x_1^{\lambda_2}\cdot y_2+\ldots+x_1^{\lambda_n}\cdot y_n=0 \\ x_2^{\lambda_1}\cdot y_1+x_2^{\lambda_2}\cdot y_2+\ldots+x_2^{\lambda_n}\cdot y_n=0 \\ \vdots \\ x_m^{\lambda_1}\cdot y_1+x_m^{\lambda_2}\cdot y_2+\ldots+x_m^{\lambda_n}\cdot y_n=0 \end{array}$$

Ez n ismeretlen és m egyenlet, $m<n$. Van tehát nem triviális megoldás. Rögzítsünk egy ilyen $y_1,\ldots,y_n$-t. Legyen most $x\in K$ tetszőleges. Írjuk fel $\alpha_1x_1+\alpha_2x_2+\ldots+\alpha_mx_m\ :\ \alpha_k\in K_0$ alakban. Szorozzuk meg az egyenletrendszer k-adik sorát α_k-val. Mivel $\alpha_k\in K_0$, $\alpha_k=\alpha_k^{\lambda_1}=\alpha_k^{\lambda_2}=\ldots=\alpha_k^{\lambda_n}$, tehát azt kapjuk, hogy

$$(\alpha_kx_k)^{\lambda_1}y_1+(\alpha_kx_k)^{\lambda_2}y_2+\ldots+(\alpha_kx_k)^{\lambda_n}y_n=0\qquad(k=1,2,\ldots,m).$$

Ezeket az egyenleteket összeadva $x^{\lambda_1}y_1+x^{\lambda_2}y_2+\ldots+x^{\lambda_n}y_n=0$. Ez $\forall x\in K$-ra teljesül és nem minden y_i nulla, azaz a $\lambda_1,\ldots,\lambda_n$ különböző beágyazások lineárisan összefüggőek, ez Dedekind tétele szerint ↯.

↾ $m>n$. Ekkor választhatóak olyan $x_1,x_2,\ldots,x_{n+1}\in K$ elemek, melyek K_0 felett lineárisan függetlenek. Az

$$\begin{array}{c} x_1^{\lambda_1}\cdot y_1+x_2^{\lambda_1}\cdot y_2+\ldots+x_{n+1}^{\lambda_1}\cdot y_{n+1}=0 \\ x_1^{\lambda_2}\cdot y_1+x_2^{\lambda_2}\cdot y_2+\ldots+x_{n+1}^{\lambda_2}\cdot y_{n+1}=0 \\ \vdots \\ x_1^{\lambda_n}\cdot y_1+x_2^{\lambda_n}\cdot y_2+\ldots+x_{n+1}^{\lambda_n}\cdot y_{n+1}=0 \end{array}$$

egyenletrendszernek van nem triviális megoldása. Legyen r minimális, amelyre van olyan nem triviális megoldás, amelyben r nullától különböző y_i van, a maradék $n-r+1$ pedig 0. Feltehetjük, hogy éppen $y_1,\ldots,y_r\neq0$ és $y_{r+1}=\ldots=y_{n+1}=0$. Ekkor

$$\underline{\odot}\qquad x_1^{\lambda_i}\cdot y_1+x_2^{\lambda_i}\cdot y_2+\ldots+x_r^{\lambda_i}\cdot y_r=0\qquad(i=1,\ldots,n)$$

Alkalmazzuk $\odot$-re $\lambda\in G$-t. Kapjuk, hogy

$$x_1^{\lambda_i\lambda}\cdot y_1^{\lambda}+x_2^{\lambda_i\lambda}\cdot y_2^{\lambda}+\ldots+x_r^{\lambda_i\lambda}\cdot y_r^{\lambda}=0\qquad(i=1,\ldots,n).$$

Viszont $\lambda_i\mapsto\lambda_i\lambda$ G egy permutációja, hiszen csoport. Tehát ugyanez más sorrendben felírva

$$\underline{\boxdot}\qquad x_1^{\lambda_i}\cdot y_1^{\lambda}+x_2^{\lambda_i}\cdot y_2^{\lambda}+\ldots+x_r^{\lambda_i}\cdot y_r^{\lambda}=0\qquad(i=1,\ldots,n).$$

Legyen $y=y_1$ és vonjuk ki $\odot$ y^{λ}-szorosából $\boxdot$ y-szorosát:

$$x_1^{\lambda_i}(y_1y^{\lambda}-y_1^{\lambda}y)+x_2^{\lambda_i}(y_2y^{\lambda}-y_2^{\lambda}y)+\ldots+x_r^{\lambda_i}(y_ry^{\lambda}-y_r^{\lambda}y)=0\qquad(i=1,\ldots,n).$$

Tehát $y_k^*=y_ky^{\lambda}-y_k^{\lambda}y$ $(k=1,\ldots,r)$, $y_{r+1}^*=\ldots=y_{n+1}^*=0$ is megoldása az egyenletrendszernek, továbbá $y_1^*=0$. r minimális volt, tehát ez csak úgy lehetséges, ha triviális megoldást találtunk, azaz $y_k^*=0$ $(k=1,\ldots,r)$. Eszerint $k\leq r$ -re $\forall\lambda\in G\colon(y_ky^{-1})^{\lambda}=y_ky^{-1}$. Így $\alpha_k=y_ky^{-1}$ $(k=1,\ldots,r)$ definíció szerint eleme K_0-nak és nem nulla, hiszen $y_k\neq0$. Ekkor $y_k=y\alpha_k$. Írjuk fel most $\odot$ azon sorát, ahol λ_i G egységeleme, azaz az identitás:

$$\begin{array}{rl} x_1^{\lambda_i}\cdot y_1+x_2^{\lambda_i}\cdot y_2+\ldots+x_r^{\lambda_i}\cdot y_r=0 & \lambda_i=id_K \\ y\cdot(\alpha_1x_1+\alpha_2x_2+\ldots+\alpha_{n+1}x_{n+1})=0 & \end{array}$$

A zárójelben az $x_1,\ldots,x_{n+1}$ elemek K_0 feletti nem triviális lineáris kombinációja áll, ami nem 0, hiszen függetlenek. Továbbá $y\neq0$, mert úgy választottuk. ↯.

Tehát csak $m=n$ lehetséges és éppen ezt akartuk belátni.

11.4.10 Definíció: a $f\in K[x]$ polinom Galois-csoportja alatt felbontási testének (mint K bővítésének) Galois-csoportját értjük. Jelölése $\Gamma(f)$.

Legyen f felbontási teste L, ekkor $L[x]$-ben $f(x)=(x-\alpha_1)(x-\alpha_2)...(x-\alpha_m)$ és $L=K(\alpha_1,...,\alpha_m)$. L egy K-automorfizmusát meghatározza az α_k-k képe, hiszen hatványaik már generálják L-t. Továbbá ha $\varphi\in\Gamma(L|K)$, akkor f minden gyökének képe gyöke f képének, azaz f-nek. Tehát $\{\alpha_1,...,\alpha_m\}$-re megszorítva minden φ egy permutáció, azaz $\Gamma\le S_n$. Ráadásul Γ minden eleme megtart minden olyan K-beli együtthatós összefüggést, ami az α_k-k hatványaira vonatkozik. Például ha egy negyedfokú polinom gyökeire $\alpha_1+\alpha_2=\alpha_3+\alpha_4$ teljesül, akkor a Galois-csoport $\langle(\alpha_1\alpha_2),(\alpha_3\alpha_4),(\alpha_1\alpha_3)(\alpha_2\alpha_4)\rangle\le S_4$ csoport részcsoportja. Belátható, hogy ha φ a gyökök egy olyan permutációja, amely minden ilyen összefüggést megtart, akkor kiterjeszthető L egy K-automorfizmusává. Ha esetleg van többszörös gyök, az nem „eshet szét", tehát a Galois-csoport egy kisebb fokú permutációcsoportba van beágyazva.

Példa: a Q kvaterniócsoport nem áll elő negyedfokú polinom Galois-csoportjaként, mert S_4-nek nincs Q-val izomorf részcsoportja, hiszen 2-Sylowja D_4.

Megjegyzés: $\Gamma(f)$ tranzitív permutációcsoport a gyökök felett $\Leftrightarrow$ f egy irreducibilis polinom hatványa. Ha ugyanis f-nek van két különböző irreducibilis faktora, akkor azok gyökeit Γ egyik eleme sem tudja egymás közt cserélgetni, azaz Γ intranzitív. Ha f irreducibilis, akkor bármely két gyökét fel lehet cserélni a felbontási test egy K-automorfizmusával, $\Gamma(f^n)=\Gamma(f)$ pedig nyilvánvaló.

11.4.11 Definíció: legyen $L|K$ Galois-bővítés, $\Gamma=\Gamma(L|K)$. $K\le M\le L$ esetén legyen $M^*=\{\varphi\in\Gamma\,|\,\forall x\in L\colon x^\varphi=x\}$, $1\le H\le\Gamma$-ra pedig $H^\circ=\{x\in L\,|\,\forall\varphi\in H\colon x^\varphi=x\}$. M^* nyilván részcsoportja lesz Γ-nak, H° pedig közbülső test $L|K$-ban.

11.4.12 Állítás: **(1)** $H_1\le H_2\Rightarrow H_1^\circ\ge H_2^\circ$, **(2)** $M_1\le M_1\Rightarrow M_1^*\ge M_2^*$, **(3)** $H^{\circ *}\ge H$ és **(4)** $M^{\circ *}\ge M$. Mindegyik nyilvánvaló.

11.4.13 Állítás: ha $L|K$ Galois-bővítés és $K\le\Gamma$, akkor $[H^\circ\colon K]=\frac{[L\colon K]}{|H|}$. Ugyanis a bal oldal a fokszámtétel (**7.10.3**) szerint $\frac{[L\colon K]}{[L\colon H^\circ]}$, **11.4.9** alapján pedig $[K\colon H^\circ]=|H|$, hiszen véges bővítésnél $\Gamma(L|K)$ véges, így $H\le\Gamma$ is.

11.4.14 Állítás: legyen $M|K$ véges, normális, $K\le L\le M$, $\tau\colon L\to M$ K-monomorfizmus. Ekkor létezik olyan $\sigma\colon M\to M$ K-automorfizmus, amelynek L-re való megszorítása τ.

Bizonyítás: legyen M a p polinom felbontási teste K felett. Ekkor persze L feletti felbontási teste is M. p felbontási teste L^τ felett is M, azaz a $\tau\colon L\to L^\tau$ izomorfizmus lépésenként kiterjeszthető egy $M\to M$ izomorfizmussá ugyanúgy, mint amikor azt láttuk be, hogy egy polinom két felbontási teste izomorf.

11.4.15 Lemma: legyen $K\le L\le N\le M$ és legyen $N|K$ normális, $\sigma\colon L\to M$ K-monomorfizmus. Ekkor $L^\sigma\le N$.

Bizonyítás: tetszőleges $\alpha\in L$ σ szerinti képe gyöke α K feletti kanonikus polinomjának, hiszen azt σ helybenhagyja. Ez N-ben lineáris faktorokra bomlik, tehát minden gyöke N-beli, így α^σ is.

11.4.16 Tétel: legyen $L|K$ tetszőleges véges bővítés. Ekkor az alábbi három feltétel ekvivalens:

- **(1)** $L|K$ normális;
- **(2)** van olyan $K\le L\le N$, ahol $N|K$ normális és $\forall\tau\colon L\to N$ K-monomorfizmus L egy automorfizmusa;
- **(3)** amennyiben $K\le L\le M$, úgy $\forall\tau\colon L\to M$ K-monomorfizmus L egy automorfizmusa.

Bizonyítás: **(3)** $\Rightarrow$ **(2)**: válasszuk N-t $L|K$ normális lezárásának és alkalmazzuk a feltételt $M=N$-re.

(2) $\Rightarrow$ **(1)**: legyen $K\le L\le N$ a feltételnek megfelelő, $\alpha\in L$. Legyen α kanonikus polinomja K felett p. p N felett lineáris faktorokra bomlik, hiszen p irreducibilis, $\alpha\in N$ és $p(\alpha)=0$. Legyen ennek egy tetszőleges gyöke $\beta\in N$. Az a $\varphi\colon K(\alpha)\to K(\beta)$ K-izomorfizmus, amely α-t β-ba viszi, a szokott módon kiterjeszthető egy $\tau\colon L\to N$ K-monomorfizmussá. A feltétel szerint ez L egy automorfizmusa, így $\beta=\alpha^\tau\in L$. L tetszőleges α elemének bármely β konjugáltja is L-ben van, tehát $L|K$ normális.

(1) $\Rightarrow$ **(3)**: legyen $L|K$ véges, normális. L és L^τ véges dimenziós vektorterek K felett és izomorfak, tehát dimenziójuk azonos. A lemma szerint $L^\tau\le L$, ezt összevetve $L^\tau=L$.

11.4.17 Állítás: legyen az $L|K$ véges, szeparábilis bővítés normális lezárása $N|K$ és $[L\colon K]=n$. Ekkor az $L\to N$ K-monomorfizmusok száma n. Ezt egyelőre nem bizonyítjuk

11.4.18 Tétel: legyen $L|K$ Galois-bővítés. Ekkor $|\Gamma(L|K)|=[L:K]$.

Bizonyítás: ha akarjuk, alkalmazhatjuk az előző állítást. Ha nem akarjuk, akkor vegyük észre, hogy **11.4.2** szerint $L|K$ egyszerű, azaz $L=K(\alpha)$, ahol α kanonikus polinomja szeparábilis és foka $n=[L:K]$. Γ minden eleme α-t valamely konjugáltjába viszi és α képe meghatározza a leképezést, tehát $|\Gamma|\le n$. Másrészt α minden konjugáltjába átvihető L egy K-automorfizmusával, így $\Gamma\ge n$ is teljesül.

11.4.19 Állítás: legyen Γ az $L|K$ Galois-bővítés Galois-csoportja. Ekkor $\Gamma^{o}=K$.

Bizonyítás: tudjuk **11.4.9**-ből, hogy $[L:\Gamma^{o}]=|\Gamma|$. Az előző tétel szerint $|\Gamma|=[L:K]$ és nyilván $K\le\Gamma^{o}$.

11.4.20 Galois-elmélet alaptétele: a $*:M\mapsto M^{*}$ és $\circ:H\mapsto H^{o}$ leképezések egymás inverzei.

Bizonyítás: $M^{*o}=M$ következik az előző állításból, hiszen $L|M$ is Galois-bővítés és $M^{*}=\Gamma(L|M)$. Ezt alkalmazva $M=H^{o}$-ra $(H^{o})^{*o}=H^{o}$. **11.4.9** szerint $|H|=[L:H^{o}]$ és $|H^{o*}|=[L:H^{o*o}]$. A két egyenlet jobb oldala megegyezik, így a bal is, azaz $|H|=|H^{o*}|$. Mindkettő véges csoport és $|H|\le|H^{o*}|$, tehát $H=H^{o*}$.

Megjegyzés: $*$ ill. $\circ$ izomorfizmus L résztesthálójának $[K,L]$ intervalluma és Γ részcsoporthálójának duálisa között.

Megjegyzés: minden véges csoport előáll alkalmas Galois-bővítés Galois-csoportjaként. Hogy minden véges csoport előáll-e $\mathbb{Q}$ valamely Galois-bővítésének csoportjaként, megoldatlan kérdés.

11.4.21 Állítás: legyen M közbülső test az $L|K$ Galois-bővítésben, $\Gamma=\Gamma(L|K)$. Ekkor **(2)** M normális $\Leftrightarrow$ $M^{*}\lhd\Gamma$ és ez esetben **(2)** $\Gamma(M|K)\simeq\Gamma/M^{*}=\Gamma/\Gamma(L|M)$.

Bizonyítás: legyen M tetszőleges közbülső test, $\gamma\in\Gamma$, $\tau\in M^{*}$, x_1 pedig M^{γ} tetszőleges eleme, azaz $x_1=x^{\gamma}:\ x\in M$. Ekkor $x_1^{\gamma^{-1}\tau\gamma}=x^{\tau\gamma}=x^{\gamma}=x_1\ \Rightarrow\ \gamma^{-1}\tau\gamma\in(M^{\gamma})^{*}$, azaz $\gamma^{-1}M^{*}\gamma\le(M^{\gamma})^{*}$. Hasonlóan $\gamma(M^{\gamma})^{*}\gamma^{-1}\le M^{*}$, ezt jobbról γ-val, balról az inverzével szorozva és az előzővel összevetve $\gamma^{-1}M^{*}\gamma=(M^{\gamma})^{*}$.

(1): Ha $M|K$ normális, akkor $\forall\gamma\in\Gamma:\ M^{\gamma}=M$, így $\forall\gamma\in\Gamma:\ \gamma^{-1}M^{*}\gamma=(M^{\gamma})^{*}=M^{*}\ \Rightarrow\ M^{*}\lhd\Gamma$. Ha $M^{*}\lhd\Gamma$, akkor legyen $\sigma:M\to L$ tetszőleges K-monomorfizmus. σ kiterjeszthető L egy τ K-automorfizmusává, azaz Γ egy elemévé. Ekkor $(M^{\tau})^{*}=\tau^{-1}M^{*}\tau=M^{*}$, amiből $M^{\tau}=M$, speciálisan $M^{\sigma}=M$. Ez M minden L-be menő σ K-monomorfizmusára teljesül, tehát $M|K$ normális **11.4.16** szerint.

(2): legyen $M|K$ normális. Ekkor a Γ-n értelmezett $\psi:\tau\mapsto\tau|_{M}$ leképezés $\Gamma(M|K)$-ba képez, mert L minden K-automorfizmusa M-re megszorítva is automorfizmus. Továbbá $\Gamma(M|K)$ minden σ eleme előáll képként, mert kiterjeszthető L egy K-automorfizmusává. Azaz $\Gamma(M|K)\simeq\Gamma/Ker\,\psi$, ahol $Ker\,\psi$ éppen L azon automorfizmusainak halmaza, melyek M-en identikusak, azaz M^{*}, más néven $\Gamma(L|M)$ elemei.

Megjegyzés: minden Galois-bővítés egyszerű **11.4.2** szerint, hiszen véges és szeparábilis.

11.4.22 Tétel: az $L|K$ véges bővítés pontosan akkor egyszerű, ha véges sok közbülső test van.

Bizonyítás: ha K véges, akkor az állítás igaz. Ugyanis véges test véges bővítése is véges test, tehát multiplikatív csoportja ciklikus, ezért a bővítés egyszerű. A közbülső testek száma nyilván véges. Legyen most K végtelen test.

$\Rightarrow$: legyen $L|K$ véges bővítés, véges sok közbülső testtel. Ekkor L előáll $L=K(\alpha_1,\dots,\alpha_n)$ alakban. Alkalmazzunk n szerinti indukciót. Ha $n=1$, akkor $L|K$ egyszerű. Ha $n\ge2$, akkor az indukciós feltevés szerint $K(\alpha_1,\dots,\alpha_{n-1})|K$ egyszerű, azaz előáll $K(\beta)$ alakban és $L(\alpha_n,\beta)$. Legyen tetszőleges $a\in K$ elemre $M_a=K(\alpha_n+a\beta)$. Nyilván $K\le M_a\le L$. Csak véges sok közbülső test van és K-nak végtelen sok eleme, így a skatulya-elv szerint található olyan $a,a'\in K$, amelyre $M_a=M_{a'}=M$. A $\beta=\frac{\alpha_n+a\beta-(\alpha_n+a'\beta)}{a-a'}$ felírásból látható, hogy $\beta\in M$. Ekkor persze $\alpha_n=(\alpha_n+a'\beta)-a'\beta$ is M-beli, így $L=K(\alpha_n,\beta)\le M\le L$, amiből $L=K(\alpha_n+a\beta)$ valóban egyszerű.

$\Leftarrow$: legyen $L|K$ egyszerű, azaz $L=K(\alpha)$ és $K\le M\le L$. Legyen α kanonikus polinomja K felett p, M felett q. $M[x]$-ben $q(x)|p(x)$. Legyen $q(x)=x^{m}+a_{m-1}x^{m-1}+\dots+a_2x^2+a_1x+a_0$ és $M_0=K(a_0,a_1,\dots,a_{n-1})\le M$. Legyen α kanonikus polinomja M_0 felett s. Ekkor $q(x)\in M_0[x]$, így s osztja q-t $M_0[x]$-ben. Ezért $[L:M]=deg\,q\ge deg\,s=[L:M_0]=[L:M]\cdot[M:M_0]$. Leosztva $[L:M]$-el $1\ge[M:M_0]$, amiből $M=M_0=K(a_0,a_1,\dots,a_{m-1})$. Tehát az M közbülső testet egyértelműen meghatározza q. p-nek $L[x]$-ben véges sok (1 főegyüttható) osztója van, tehát csak véges sok M létezhet.

11.5 Az algebra alaptétele

A tétel azt mondja ki, hogy $\mathbb{C}$ algebrailag zárt, azaz minden legalább elsőfokú $\mathbb{C}[x]$-beli polinomnak ban gyöke. Ez ekvivalens azzal, hogy $\mathbb{C}$-bek nincs algebrai bővítése ($\mathbb{C}|\mathbb{C}$-n kívül, ami érdektelen). Most adunk rá két bizonyítást.

Bizonyítás I.: legyen $f\in\mathbb{C}[x]$. Ha van gyöke, akkor jó. Ha nincs, akkor az $\frac{1}{f}$ függvény az egész komplez számsíkon értelmes, folytonos és differenciálható („egészfüggvény"). Ha $|z|\to\infty$, akkor $|f(z)|\to\infty$, azaz az egy elegendően nagy sugarú origó közepű körön kívül $|\frac{1}{f}|<1$. $\frac{1}{f}$ a körön belül is korlátos, mert kompakt halmazon folytonos függvény mindig korlátos. Liouville tétele szerint minden korlátos egész függvény konstans, tehát f konstans. Azaz ha egy $\mathbb{C}[x]$-beli polinomnak nincs gyöke, akkor konstans.

Bizonyítás II.: felhasználjuk, hogy minden $\mathbb{R}[x]$-beli páratlan fokú polinomnak van valós gyöke és hogy minden $\mathbb{C}$-beli elemnek van négyzetgyöke. Az első állítás miatt $\mathbb{R}$-nek nincs nem triviális páratlan fokú bővítése, a második miatt $\mathbb{C}$-nek nincs másodfokú bővítése. ($\mathbb{R}$ és $\mathbb{C}$ perfekt, így minden véges bővítésük egyszerű, tehát minden bővítés foka az adjungált α elem kanonikus polinomjának foka. Speciálisan minden véges bővítéshez található azonos fokú irreducibilis polinom.)

Vegyünk egy $L|\mathbb{C}$ véges bővítést és lássuk be, hogy $L=\mathbb{C}$. Tekintsük az $L|\mathbb{R}$ szintén véges bővítést. Legyen a normális lezárása N. $N|\mathbb{R}$ Galois-bővítés, mert véges, normális és $\mathbb{R}$ perfekt. Legyen Galois-csoportja Γ. $|\Gamma|=[N:\mathbb{R}]=[N:\mathbb{C}]\cdot[\mathbb{C}:\mathbb{R}]=2\cdot[N:\mathbb{C}]$. Eszerint Γ rendje páros. Legyen a 2-Sylowja P. Ekkor $|\Gamma:P|$ páratlan. A Galois-bővítések alaptételéből $|\Gamma:P|=[P^o:\mathbb{R}]$, azaz P^o páratlan bővítése $\mathbb{R}$-nek, így maga $\mathbb{R}$. Eszerint Γ 2-csoport, így persze $\Gamma(N|\mathbb{C})$ is. $\nuparrow$ $\Gamma(N|\mathbb{C})\neq\{1\}$. Ekkor Sylow II. tétele szerint $\Gamma(N|\mathbb{C})$-nak van 2 indexű részcsoportja, M. Erre $[M^*:\mathbb{C}]=|\Gamma:M|=2$, $\lightning$.

Így $N=\mathbb{C}$ – ezt akartuk belátni.

11.6 Algebrai lezárás

11.6.1 Definíció: $\bar{K}$ algebrai lezárása K-nak, ha **(1)** $\bar{K}|K$ algebrai bővítés és **(2)** $\bar{K}$ algebrailag zárt.

11.6.2 Tétel: minden testnek létezik algebrai lezárása.

Bizonyítás: először konstruálunk egy $K_1\geq K$ algebrai bővítést, amelyben minden K feletti irreducibilis polinomnak van gyöke. Legyen Φ a K feletti, 1 főegyütthatójú irreducibilis polinomok halmaza. Minden f eleméhez vegyünk egy x_f változót, legyen ezek halmaza χ. Legyen továbbá $R=K[\chi]$. R egy irdatlan nagy polinomgyűrű lesz, de azért ne rettenjünk meg. Tekintsük $\forall f\in\Phi$-re $f(x_f)$-et – ez $K[x_f]\subseteq R$ egy eleme lesz. Így hát van értelme tekinteni az általuk R-ben generált ideált, $A=(f(x_f)|f\in\Phi)$-t. $\nuparrow$ $1\in A$. Ekkor 1 előáll véges sok $f(x_f)$ R-beli együtthatós lineáris kombinációjaként:

$$1=u_1f_1(x_{f_1})+u_2f_2(x_{f_2})+\ldots+u_nf_n(x_{f_n})\ :\ u_k\in R\ .$$

Vegyük minden egyes f_k-hoz annak egy α_k gyökét és adjungáljuk K-hoz. A kapott test felett a fenti egyenlet minden behelyettesítési érték mellet fenn kell álljon. Viszont $x_{f_k}=\alpha_k$ esetén a jobb oldal 0, a bal pedig 1, $\lightning$.

Tehát $A\subsetneq R$. A Zorn-lemma alkalmazásával beágyazható egy M maximális ideálba, mert R egységelemes. Legyen K_1 az R/M faktorgyűrű. Mivel M maximális ideál és R kommutatív, ez test lesz. Legyen φ a $K\to R$ beágyazás, ψ az $R\to K_1$ faktorleképezés. $\varphi\psi$-ben $1\in K$ képe K_1 egységeleme $\Rightarrow$ $\varphi\psi$ nem triviális, tehát beágyazás. $\forall f\in\Phi$: $f(x_f)\in M$, így $f^{\psi}(x_f^{\psi})=(f(x_f))^{\psi}=0$. Tehát $K[x]$ minden irreducibilis polinomjának van gyöke K_1-ben, mégpedig x_f^{ψ}.

R (mint K feletti vektortér) minden elemét generálják az x_f elemek hatványai (ez adódik a $K[\chi]$ polinomgyűrű definíciójából), azaz K_1 (mint K feletti vektortér) minden elemét generálják az $\{x_f^n|f\in\Phi,n\in\mathbb{N}\}$ elemek képei. Ezek persze benne is vannak K_1-ben, azaz $K_1=K(x_f^{\psi}|f\in\Phi)$. Mivel x_f^{ψ} algebrai K felett, $K_1|K$ algebrai.

Hasonló módon készíthetünk K_1-hez egy K_2-t, amelyben minden K_1 felett irreducibilis polinomnak van gyöke. Ezt megszámlálható sokszor elvégezve kapunk egy $K=K_0\leq K_1\leq K_2\leq\ldots$ sorozatot. Legyen $L=\bigcup_{n\in\mathbb{N}}K_n$.

$L|K$ algebrai, mert minden eleme benne van valamely $K_n|K$ algebrai bővítésben. Véve egy $p(x)\in L[x]$ polinomot, annak csak véges sok együtthatója van, azaz alkalmas K_n-nel lefedhető. Így $p(x)\in K_n[x]$ és a konstrukció miatt van gyöke $K_{n+1}\subseteq L$-ben. Tehát L algebrailag zárt.

11.6.3 Állítás: ha $L|K$ algebrai, normális és minden K feletti polinomnak van gyöke L-ben, akkor L algebrailag zárt.

Bizonyítás: legyen p (legalább elsőfokú) L feletti polinom, α ennek egy gyöke. Elegendő belátnunk, hogy $\alpha\in L$. Legyen α kanonikus polinomja K felett q. Feltételeink szerint q-nak van gyöke L-ben. $L|K$ normális, így q minden gyöke – köztük α is – L-beli.

Ennek segítségével másképp is befejezhetjük az előző bizonyítást: L-t választhatjuk K_1 normális lezárásának. Mindkét esetben nyilvánvaló, hogy L-nél szűkebb bővítés nem lehet algebrailag zárt.

11.6.4 Állítás: legyen $M|K$ algebrai bővítés, $K\le L\le M$. Legyen továbbá C algebrailag zárt bővítése K-nak, $\sigma: L\to C$ egy K-monomorfizmus. Ekkor σ kiterjeszthető egy $\tau: M\to C$ beágyazássá (ez persze K-monomorfizmus lesz).

Bizonyítás: vegyünk olyan (N,φ) párok $\mathcal{N}$ halmazát, ahol $L\le N\le M$ és $\varphi: N\to C$ kiterjesztése σ-nak. Definiáljuk felettük az alábbi részbenrendezést: $(N,\varphi)\le(N',\varphi') \Leftrightarrow N\le N'$ és $\varphi'|_N=\varphi$. Egy $\mathcal{N}$-beli $\mathcal{L}=\{(N_\kappa,\varphi_\kappa)\,|\,\kappa\in\mathbf{I}\}$ láncra tekintsük azt az $(N^*,\varphi^*)\in\mathcal{N}$ elemet, ahol $N^*=\bigcup_{\kappa\in\mathbf{I}}N$ és $\varphi^*: N^*\to C$ oda viszi az $\alpha\in N^*$ elemet, ahova az α-t fedő N_κ -khoz tartozó φ_κ leképezések. Mivel L lánc, bármely két ilyen φ_κ egyike kiterjesztése a másiknak, tehát ugyanoda képezik α-t, így α^{φ^*} jóldefiniált. Nyilván $\forall\kappa\in\mathbf{I}$: $(N_\kappa,\varphi_\kappa)\le(N^*,\varphi^*)$, azaz minden $\mathcal{N}$-beli lánc lefedhető $\mathcal{N}$ egy elemével. A Zorn-lemma szerint tehát $\mathcal{N}$-ban van egy (N_0,φ_0) maximális elem.

↯ $N_0<M$. Ekkor $\exists\alpha\in M\setminus N_0$. α algebrai N_0 felett, hiszen algebrai K felett. Így $N_0<N_0(\alpha)\le M$. Legyen α minimálpolinomja N_0 felett m_α, ennek φ_0 szerinti képe m_α^*. $m_\alpha^*\in C[x]$, azaz van egy α^* gyöke C-ben. Terjesszük ki φ_0-t N_0-ról $N_0(\alpha)$-ra úgy, hogy α képe α^* legyen. Ez a szokott módon megtehető és egy (N_0,φ_0)-nál nagyobb $\mathcal{N}$-beli elemet kapunk, ami (N_0,φ_0) maximalitása miatt ↯. Tehát a maximális elem (M,τ) alakú és mi épp ezt a τ-t kerestük.

11.6.5 Következmény: az algebrai lezárás izomorfia erejéig egyértelmű. Ha ugyanis L-t K-nak, M-et és C-t K két különböző algebrai lezárásának, σ-t pedig K identitásának választjuk, akkor τ egy $M\to C$ K-monomorfizmus lesz. Továbbá szürjektív, mert ha $\alpha\in C$ minimálpolinomja K felett p, akkor p M-beli gyökeit τ csak p C-beli gyökeibe képezheti – ez két azonos méretű véges halmaz, τ injekció, tehát α előáll képként.

Megjegyzés: az állítás szerint K-nak minden algebrailag zárt C bővítésen belül van egy és – személyesen, nem csupán izomorfia erejéig – csakis egy algebrai lezárása. ($M=\overline{K}$ választással az állítás kiadja a C-n belüli lezárás létezését. Kettő nem lehet, mert minden $K[x]$-beli polinom gyökei adottak C-ben és $\overline{K}$ minden eleme előáll ilyen alakban.)

11.6.6 Állítás: $\overline{\mathbb{Q}}=\mathbb{A}$.

Bizonyítás: $\mathbb{A}|\mathbb{Q}$ algebrai bővítés, mert úgy definiáltuk. $p(x)\in\mathbb{A}[x]$-re $\mathbb{Q}$-hoz adjungálva az együtthatókat majd a gyököket véges sok véges bővítést végzünk, így algebrai bővítést kapunk. Eszerint $p(x)$ minden gyöke algebrai $\mathbb{Q}$ felett, így $\mathbb{A}$-beli. Ezért $\mathbb{A}$ algebrailag zárt. Másképp: $\mathbb{A}$-ra nyilvánvalóan teljesülnek **11.6.3** feltételei.

Megjegyzés: $[\mathbb{A}:\mathbb{Q}]=\aleph_0$. Ugyanis $|\mathbb{A}|=\aleph_0$ miatt több nem lehet. Véges pedig azért nem lehet, mert a Schönemann-Eisenstein kritérium miatt $\forall n\in\mathbb{N}$-re x^n-p irreducibilis $\Rightarrow$ felbontási teste $\mathbb{Q}$ felett tehát legalább n-edfokú, így $\forall n$: $[\mathbb{A}:\mathbb{Q}]\ge n$.

11.7 Polinomok megoldása gyökjelekkel

11.7.1 Definíció: az $L|K$ bővítés radikálbővítés, ha előáll $L=K(\alpha_1,\alpha_2,\dots,\alpha_n)$ alakban, ahol $\forall k\exists n(k)$: $\alpha_k^{n(k)}\in K(\alpha_1,\dots,\alpha_k)$. A feltételeknek megfelelő $(\alpha_k)_{k=1}^n$ sorozatokat radikálsorozatnak hívjuk. Minden radikálbővítés véges.

11.7.2 Definíció: legyen $\mathit{char}\,K=0$. Az $f(x)\in K[x]$ polinomra azt mondjuk, hogy megoldható gyökjelekkel, ha felbontási teste beágyazható egy $R|K$ radikálbővítésbe.

11.7.3 Lemma: legyen az $L|K$ véges bővítés normális lezárása $N|K$. Ekkor N-ben található véges sok $L|K$-val izomorf $L_k|K$ $(k=1,\dots,s)$ bővítés, melyek együtt generálják N-t.

Bizonyítás: legyen $L=K(\alpha_1,\alpha_2,\dots,\alpha_n)$, a megfelelő minimálpolinomok $m_1,\dots,m_n$. N éppen az $f=m_1\cdot\dots\cdot m_n$ polinom felbontási teste, hiszen normális bővítése K-nak és generálják az α_k elemek konjugáltjai. Vegyük f egy tetszőleges β gyökét, ez persze gyöke valamelyik m_k-nak. Legyen $M=K(\alpha_1,\dots,\alpha_{k-1})$. Így $M(\alpha_k)|K\simeq M(\beta)|K$ a szokott módon és a megfelelő K-monomorfizmus **11.4.14** szerint kiterjeszthető egy $\gamma_\beta: L\to L$ K-automorfizmussá. L^{γ_β} egy L-el izomorf bővítés lesz, mely fedi β-t. Ha β-val befutjuk f gyökeit, a megfelelő L^{γ_β} bővítések által generált test fedni fogja f összes gyökét, azaz kiadja a felbontási testet.

11.7.4 Lemma: legyen az $R|K$ radikálbővítés normális lezárása N. Ekkor $N|K$ is radikálbővítés.

Bizonyítás: az előző lemma szerint $N|K$-t generálja véges sok $R|K$-val izomorf bővítés. Elég tehát belátni, hogy véges sok radikálbővítés radikálbővítést generál, amihez elég, hogy két radikálbővítés radikálbővítést generál. Márpedig ha $R_1=K(\alpha_1,\dots,\alpha_n)$ és $R_2=K(\beta_1,\dots,\beta_k)$ radikálbővítések, továbbá az imént radikálsorozattal adtuk meg őket, akkor nyilván $(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_k)$ is radikálsorozat, azaz $R=(R_1,R_2)=K(\alpha_1,\dots,\beta_k)$ is radikálbővítés.

11.7.5 Lemma: legyen K nulla karakterisztikájú, p prím, $L|K$ az $x^p-1\in K[x]$ polinom felbontási teste. Ekkor $\Gamma(L|K)$ Abel-csoport.

Bizonyítás: x^p-1 deriváltja px^{p-1}, tehát nincs többszörös gyöke. Két gyökének szorzata is gyök, tehát gyökei p-edrendű részcsoportot adnak L^*-ban. Ez persze ciklikus, tehát a gyökök egy $\varepsilon_p\in L$ elem hatványai, így Γ elemei jellemezhetőek azzal, hogy ε_p-t hova viszik. Ha $\varphi:\varepsilon_p\mapsto\varepsilon_p^i$ és $\psi:\varepsilon_p\mapsto\varepsilon_p^j$ a Galois-csoport elemei, akkor $\varphi\psi$ és $\psi\varphi$ egyaránt ε_p^{ij}-be viszik ε_p-t, tehát φ és ψ felcserélhetőek.

11.7.6 Lemma: legyen $char\,K=0$ és tegyük fel, hogy x^n-1 lineáris faktorokra bomlik K-ban. x^n-a felbontási teste legyen L. Ekkor $\Gamma(L|K)$ Abel-csoport.

Bizonyítás: legyen $\alpha\in L$ gyöke x^n-a-nak. Ekkor az összes gyök $\{\varepsilon\cdot\alpha\,|\,\varepsilon:\ \varepsilon^n-1=0\}$. Γ egy elemét leírja, hogy α-t melyik konjugáltjába viszi. Ha $\varphi:\alpha\mapsto\varepsilon\alpha$ és $\psi:\alpha\mapsto\zeta\alpha$ a Galois-csoport elemei, akkor $\alpha^{\varphi\psi}=\varepsilon^\psi\alpha^\psi=\varepsilon\zeta\alpha=\zeta^\varphi\alpha^\varphi=\alpha^{\psi\varphi}$, mert $\varepsilon,\zeta\in K$. Így φ és ψ felcserélhetőek.

11.7.7 Tétel: legyen K nulla karakterisztikájú, $L|K$ normális, $K\le L\le R$ és $R|K$ radikálbővítés. Ekkor $\Gamma(L|K)$ feloldható.

Bizonyítás: elég belátni, hogy ha R normális lezárása N, akkor $\Gamma(N|K)$ feloldható. Ugyanis **11.4.21** szerint $\Gamma(L|K)$ ennek faktorcsoportja és feloldható csoport faktorcsoportja feloldható. A második lemma szerint $N|K$ is radikálbővítés. Legyen $N=K(\alpha_1,\alpha_2,\dots,\alpha_n)$ ahol $(\alpha_k)_{k=1}^n$ radikálsorozat. Feltehetjük, hogy $n(k)$ mindig prím, hiszen ha $n(k)=p\cdot s$, akkor beiktathatunk α_k elé α_k^p-t és véges sok ehhez hasonló lépés után már minden $n(k)$ prím lesz.

Alkalmazzunk n szerinti teljes indukciót. $n=0$ esetén $\Gamma=\{1\}$, ez valóban feloldható. Tegyük fel, hogy n-nél rövidebb sorozatra az állítás igaz és lásuk be n hosszúakra is.

Legyen $\alpha_1^p\in K$. Tekintsük x^p-1 felbontási testét N felett, legyen ez N'. Ha N az $f(x)\in K[x]$ polinom felbontási teste volt, akkor N' az $f(x)\cdot(x^p-1)$ felbontási teste. Jelölje továbbá K' azt a résztestet N'-ben, melyet K elemei és x^p-1 gyökei generálnak. Ez felbontási teste lesz x^p-1-nek K felett, azaz N,N',K' mind normális bővítése K-nak.

Ismét **11.4.21** szerint elég belátni, hogy $\Gamma(N'|K)$ feloldható, hiszen ennek $\Gamma(N|K)$ homomorf képe. Továbbá $\Gamma(K'|K)\simeq\Gamma(N'|K)/\Gamma(N'|K')$ a harmadik lemma szerint Abel-csoport, mert $K'|K$ az x^p-1 polinom felbontási teste. Elegendő tehát $\Gamma(N'|K')$ feloldhatóságát bizonyítani. Tekintsük az $K'(\alpha_1)|K'$ bővítést. $\alpha_1^p\in K'$, hiszen $K\le K'$ és K' -ben vannak p-edik egységgyökök, így a negyedik lemma szerint ez normális bővítés és Galo is-csoportja feloldható. $N'|K'(\alpha_1)$ pedig $K_1=K'(\alpha_1)$ jelöléssel előáll $K_1(\alpha_2,\dots,\alpha_n)|K_1$. Ez egy n-nél rövidebb normális radikálbővítés, így $\Gamma(N'|K_1)$ az indukciós feltevés szerint feloldható. Még egyszer alkalmazva **11.4.21**-et $\Gamma(K_1|K')\simeq\Gamma(N'|K')/\Gamma(N'|K_1)$. Az itt szereplő három csoportból kettőről már beláttuk, hogy feloldható, így a harmadik, $\Gamma(N'|K')$ is az.

11.7.8 Következmény: $f(x)=x^5-6x+3\in\mathbb{Q}[x]$ nem oldható meg gyökjelekkel.

Bizonyítás: a Schönemann-Eisenstein kritériumot $p=3$-ra alkalmazva láthatjuk, hogy f irreducibilis. Eszerint Galois-csoportja, Γ tranzitív $\alpha_1,\dots,\alpha_5$ felett. Így rendje osztható 5-tel, következésképp van ötödrendű eleme. S_5-ben csak az ötelemű ciklusok ilyenek, tehát alkalmas jelöléssel $(12345)\in\Gamma$. f deriváltja $5x^4-6$. Ennek szemmel láthatóan

két valós gyöke van, azaz f először monoton növő, majd monoton csökkenő, végül ismét monoton növő $\mathbb{R}$-ben. Legfeljebb 3 valós gyöke lehet tehát, ennyi pedig van is, mert behelyettesítési értéke (-2)-ben -17, (-1)-ben 8, 0-ban 3, 1-ben -2, 2-ben 23 és folytonos $[-2,+2]$-n. A maradék két gyök komplex, mégpedig egymás komplex konjugáltja. A komplex konjugálás megszorítása a felbontási testre tehát egyrészt $\mathbb{Q}$-automorfizmus, másrészt a gyökök felett egy transzpozíció. Ha ismét átbetűzünk és az (12345) ciklus helyett esetleg a négyzetét vesszük, akkor azt kapjuk, hogy $\langle(12),(12345)\rangle \leq \Gamma \leq S_5$. Viszont a bal oldalon is S_5 áll, így $\Gamma = S_5$. Ez nem feloldható, így f nem oldható meg gyökjelekkel.

Megjegyzés: az „általános n-edfokú polinom" semmilyen 0 karakterisztikájú K testre nem oldható meg gyökjelekkel, ha $n \geq 5$. Az „általános n-edfokú polinom megoldása gyökjelekkel" kifejezés alatt azt értjük, hogy van egy csodálatos képletünk, amelybe beírva az $f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0 \in K[x]$ polinom együtthatóit megkapjuk a megoldásokat. (Meg persze sok hamis gyököt, mert a gyökvonás nem egyértelmű – K perfekt –, de összesen is csak véges sokat.) A képletnek nem szabad az a_k-k konkrét értékeitől függnie, azaz ha $\{a_k \mid 0 \leq k \leq n-1\}$-t változóknak tekintjük, akkor is megfelelő megoldást kell kapnunk. Vegyük hát az $T=K(a_0,a_1,\ldots,a_{n-1})$ bővítést, ahol minden a_k transzcendens és semmi közük egymáshoz (értsd: semmilyen $K[a_0,a_1,\ldots,a_{n-1}]$-beli nemnulla polinom nem tűnik el rajtuk, azaz a_{k+1} $K(a_0,a_1,\ldots,a_k)$ felett is transzcendens). A képletnek T felett is működnie kell, azaz ha vesszük T felett $f(x)$ felbontási testét, annak Galois-csoportja feloldható kell legyen. Ez a Galois-csoport viszont S_n, ami $n \geq 5$ -re nem feloldható.