NYILATKOZAT

Név: Szöri Vajk

ELTE Természettudományi Kar, szak: matematika

NEPTUN azonosító: CD62K5

Szakdolgozat címe:
Hilbert irreducibilitási tétele

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2022.05.31

a hallgató aláírása

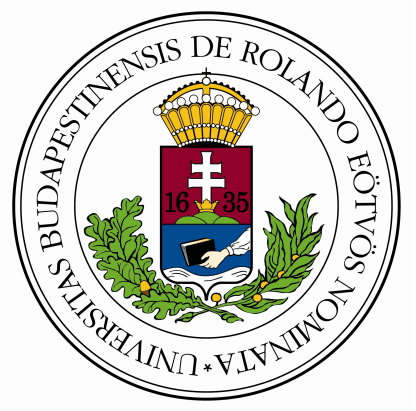
Eötvös Loránd Tudományegyetem
Természettudományi Kar

Hilbert irreducibilitási tétele

Szőri Vajk

Témavezető:
Zábrádi Gergely, egyetemi docens

BSc Szakdolgozat
Algebra és Számelmélet Tanszék



Budapest, 2022.

Tartalomjegyzék

1. Bevezetés **3**

2. Hilbert-féle testek **5**
2.1. Polinom együtthatóinak specifikációja 8
2.2. Hilbert-féle testek alapvető tulajdonságai 13

3. A racionális számok teste Hilbert-féle **17**
3.1. A gyökök analitikája 17
3.2. Hilbert irreducibilitási tétele 19

4. Hilbert-féle testek algebrai bővítései **25**
4.1. Weissauer tétele 25

5. Alkalmazások **29**
5.1. Weissauer tételének alkalmazásai 29
5.2. Elemi számelméleti alkalmazások 30

1. fejezet

Bevezetés

Az inverz Galois-probléma, azaz hogy minden véges csoport előáll-e a racionális számok testének alkalmas bővítésének Galois-csoportjaként, az egyik leghíresebb megoldatlan kérdés az algebrai számelméletben. Hilbert fő motivációja ez a probléma volt irreducibilitási tételének igazolásakor. A tétel azt állítja, hogy ha egy racionális együtthatós $r + s$-változós polinom irreducibilis, akkor az első r változó helyére behelyettesíthetünk alkalmas racionális számokat úgy, hogy a kapott s-változós polinom is irreducibilis legyen. A tétel nemcsak az inverz Galois-probléma szempontjából fontos: többek között Wilesnak a Fermat-sejtésre adott bizonyítása is használja, de számos elemien elmondható számelméleti kérdést is meg lehet segítségével válaszolni.

A második fejezetben először néhány a későbbiekben fontos állítást bizonyítok. Majd ezek segítségével három ekvivalens feltétellel definiálom a Hilbert-féle testeket. Az első két feltétel segítségével belátom, hogy a Hilbert-féle testek végesen generált bővítései is Hilbert-félék. A harmadik feltétel pedig Hilbert irreducibilitási tételének és Weissauer tételének bizonyításánál hasznos. A fejezet második felében pedig néhány tulajdonságát mutatom be a Hilbert-féle testeknek, amelyek segítenek a struktúrájuk megértésében.

A harmadik fejezetben egy elemi bizonyítást mutatok be Hilbert irreducibilitási tételére, amelynek alapötlete Karl Dörge-től származik. Ehhez először belátunk egy tételt komplex együtthatós polinomok gyökeiről. Ezután bevezetem a ritka halmazok fogalmát, majd kimondok egy tételt a Laurent-sorok egészértékeivel kapcsolatban, aminek a bizonyítása csak elemi analízist igényel, de erre csak a fejezet végén kerül sor. Ennek a segítségével pedig bebizonyítom Hilbert irreducibilitási tételét. A negyedik fejezet Weissauer tételét vizsgálja, ami bizonyos feltételek mellet biztosítja egy Hilbert-féle

test nem végesen generált bővítéseinek a Hilbert-féleségét. Az ötödik fejezetben ennek és Kronecker és Weber tételének segítségével bebizonyítom, hogy $\mathbb{Q}_{ab}$: $\mathbb{Q}$ összes egységgyökkel való bővítése Hilbert-féle. A dolgozat Helmut Völklein Groups as Galois Groups: An introduction[1] című könyve alapján készült

2. fejezet

Hilbert-féle testek

Továbbiakban legyen K egy 0 karakterisztikájú test, és $x, y, x_1, x_2, ...$ független transzcendensek K felett.

2.0.1. Definíció. Legyen L egy test és F egy részteste. Azt mondjuk, hogy $\hat{K} \subset L$ K egy algebrai lezártja L-ben, ha tartalmazza az összes K felett algebrai elemet, ami L-ben van.

2.0.2. Definíció. Legyen L egy test és F egy részteste. Azt mondjuk, hogy L reguláris F felett, ha F algebrailag zárt L-ben.

2.0.3. Tétel (Artin tétele)**.** *Ha G egy véges csoport automorfizmusa K testnek, akkor K/F Galois-bővítés, ahol F a G fixteste.*

Bizonyítás. A bizonyítás megtalálható [2] -ben. □

2.0.4. Tétel (Galois-elmélet főtétele)**.** *Legyen F/K egy véges Galois-bővítés $G = Gal(F/K)$ Galois-csoporttal. Ekkor a*

$$K \leq L \leq F \text{ közbülsőtestek} \iff H \leq G \text{ részcsoportok}$$
$$\psi : L \mapsto Gal(F/L)$$
$$F^H \hookleftarrow H : \phi$$

leképezések egymás inverzei (speciálisan mindkettő bijekció). Továbbá ha $L \iff H$ a fenti megfeleltetésben, akkor $|F : L| = |H|$ (azaz F/L is Galois) és $|L : K| = |G : H|$.

Bizonyítás. A bizonyítás megtalálható [3]-ban. □

2.0.5. Állítás. *Tegyük fel, hogz $x_1, ..., x_n$ algebrailag függetlenek K test fölött, és legyen $x = (x_1, ..., x_n)$. Legyen $\overline{K}$ K egy algebrai lezártja.*

1. *Ha K'/K egy véges Galois-bővítés, akkor $K'(x)/K(x)$ is az, valamint $G(K'(x)/K(x)) \to G(K'/K)$ megszoritás egy izomorfizmus, továbbá minden test $K(x)$ és $K'(x)$ $K"(x)$ alakú, és $|K"(x) : K(x)| = |K" : K|$.*

2. *Legyen $f(x, y) \in K(x)[y]$ irreducibilis $K(x)$ fölött, és legyen $L = K(x)[y]/f(x, y)a$ hozzá tartozó testbővítés. Ekkor L reguláris K fölött pontosan akkor, ha f irreducibilis $\overline{K}(x)$ fölött. Ha ez teljesül, akkor $f(x, y)$ irreduciblis $K_1(x)$ fölött, ahol K_1 K olyan testbővítése, hogy $x_1, ..., x_n, y$ független transzcendensek K_1 fölött.*

Bizonyítás. 1. $G = G(K'/K)$ hat $K'(x)$-en, és fixen hagyja $K(x)$-et. Ekkor 2.0.3 alapján $K'(x)/K(x)$ Galois-bővítés, és $G = G(K'(x)/K(x)$. Az állítás többi része következik a Galois-elmélet főtételéből, mivel az egy bijekciót mond ki a köztes testek és a Galois-csoport részcsoportjai között.

2. Legyen $\hat{K}$ K algebrai lezártja L-ben, és legyen α y képe L-ben ekkor $f(\alpha) = 0$, valamint α gyöke egy polinomnak $\hat{f}(y) \in \hat{K}(x)[y]$, aminek a foka $|L : \hat{K}(x)|$, és $\hat{f}$ osztja f-et. Ebből adódik hogy, ha $\hat{K} \neq K$, akkor f nem irreducibilis $\hat{K}(x)[y]$-ban, ezért $\overline{K}(x)[y]$-ban sem.
A másik irányhoz tegyük fel, hogy $\hat{K} = K$, és legyen K' egy véges Galois-bővítése K-nak. Legyen L' L és $K'(x)$ egy összetétele $K(x)$ egy algebrai lezártjában. Az állítás első feléből adódik a következő: $L \cap K'(x) = K"(x)$, ahol $K"$ egy test K és K' között. Ekkor $K" \subset \hat{K}$, ezért $K" = K$, vagyis $L \cap K'(x) = K(x)$. Tehát $L' = K'(x)(\alpha)$.Legyen $g(y) \in K'(x)[y]$ α minimálpolinomja.K'/K egy Galois-bővítés. Legyen $g_i(y) \in K'(x)[y]$ a polinom, amit akkor kapunk ha $\sigma_i \in Gal(K'(x)/K(x))$-t alkalmazzuk, g együtthatóin. Ekkor $g_i(\alpha) = 0$ minden i-re hiszen α σ_i invariáns. De mivel g α minimálpolinomja, ezért $g|g_i$, de azonos fokúak és normáltak, tehát $g_i = g$ minden i-re. Ebből adódik, hogy g együtthatói $Gal(K'(x)/K(x)$ invariánsak, tehát $K(x)$ beliek, vagyis $g[y] \in K(x)[y]$. De f α minimálpolinomja $K(x)$ felett, ezért $f|g$. Vagyis $f = g$, mivel azonos fokúak. Ezért f irreducibilis $K'(x)$ felett, amiből adódik, hogy K' felett is. De K' egy tetszőleges véges Galois-bővítése volt K-nak, vagyis f irreducibilis $\overline{K}(x)$ felett is.

Az állítás utolsó részéhez tegyük fel, hogy f szorzattá bomlik mint $f = gh$ valamilyen $g, h \in K_1(x)[y]$ polinomokra, melyek foka ≥ 1. Feltehetjük, hogy g normált y-ban. Valamint fel tehetjük, hogy K_1-et K felett generálják g együtthatói, és valamelyik együttható, hívjuk t-nek, transzcendens K felett. Az alábbi lemma szerint K_1 véges bővítése egy $K_2 = K(t_1, ..., t_s$ testnek, ahol $t_1, ...t_s$ független transzcendensek K felett, és $t = t_1$. Létezik egy végtelen részhalmaz $A \subset Aut(K_2/K)$, hogy minden $\alpha \in A$ különböző értéket vesz fel t helyen (pl.:$\alpha(t) = t + c, c \in K$, és $\alpha(t_i) = t_i$ minden $i >$ 1-re). Ezek az α-k kiegészíthetők K_1 $\overline{K}_2$ be való beágyazásaivá, és tovább $K_1(x)[y]$ $\overline{K}_2(x)[y]$-ba való beágyazásaivá(fixen hagyva $x_1, ..., x_m, y-t$).Ezeket g-re alkalmazva kapunk végtelen sok különböző normált polinomot $\overline{K}_2(x)[y]$-ban, amelyek osztják f-et (hiszen ezek f együtthatóit fixen hagyják mert azok $K(x)$ beliek). Ez ellentmondás.

□

2.0.6. Lemma. *Tegyük fel, hogy $K_1 = K(a_1, ..., a_r)$ egy végesen generált bövítése K-nak. Ha $\{t_1, ..., t_s\} \subset \{a_1, ..., a_r\}$ maximális számú algebrailag független transzcendensek K felett, akkor K_1 egy véges algebrai bővítése $K(t_1, ..., t_s)$-nek*

Bizonyítás. Egyértelmű □

2.0.7. Lemma. *Legyen α algebrai L test fölött. Legyen $f(y) = \sum_{i=0}^{n} a_i y^i$ egy polinom L fölött, aminek a foka $n > 0$ és $f(\alpha) = 0$. Ekkor*

$$g(Y) = Y^n + \sum_{i=0}^{n-1} a_i a_n^{n-i-1} Y^i$$

z egy normált polinom, aminek a foka n és $g(a_n) = 0$.

Bizonyítás. Kiemelés után adódik. □

Legyen $f(y) \in D[y]$ egy polinom D alaptételes gyűrű felett és legyen a foka ≥ 1. Ekkor $f(y)$ pontosan akkor irreducibilis $D[y]$-ban, ha irreducibilis $F[y]$-ban, ahol F D hányadosteste. Továbbá $f(y)$-t primitívnek nevezzük, ha nem azonosan nulla, és az együtthatóinak a legnagyobb közös osztója 1. Ha g(y) nem azonosan nulla polinom F felett, akkor létezik $d \in F$, egységszeresig egyértelmű, hogy $d \cdot g(y)$ primitív. Továbbá minden test feletti véges változós polinom gyűrű alaptételes.Ezek bizonyítás megtalálható [4]-ben.

2.0.8. Lemma. *Legyen $f(x_1, ..., x_{s-1})$ egy polinom $s \geq 2$ változóval K felett, aminek a foka ≥ 1 x_s-ben. Ekkor f irreducibilis mint egy s változós polinom pontosan akkor, ha irreduciblis és primitív mint x_s egy polinomja a $D = K[x_1, ..., xs - 1$ gyűrű felett.*

Bizonyítás. Először tegyük fel, hogy f irreducibilis és primitív mint x_s egy polinomja D felett. Ekkor ha $f = gh$ valamilyen $g, h \in K[x_1, ..., x_s]$ polinomokra, akkor az egyiknek, például g-nek, valójában D belinek kell lennie. De mivel f primitív, ezért g egység D-ben, vagyis $g \in K$. Ebből adódik, hogy f irreducibilis mint egy s változós polinom. A másik irány egyértelmű. □

2.1. Polinom együtthatóinak specifikációja

2.1.1. Állítás. *Legyen K/F egy véges Galois-bővítés és $G = Gal(K/F)$. Legyen R egy részgyűrű F-ben, aminek F a hányadosteste. Legyen α olyan, hogy $F(\alpha) = K$ valamint létezik $f(y) \in R[y]$ normált polinom, hogy $f(\alpha) = 0$ és f foka $n = |K : F|$. Végül legyen A egy véges részcsoport K-ban, ami tartalmazza α-t, és invariáns G-re. Legyen $S = R[A]$ K-nak a részgyűrűje, amit R és A generál. Ékkor van olyan $u \neq 0$ R-ben, hogy minden ω homomorfizmusra R-ből egy F' testbe amire $\omega(u) \neq 0$ a következők teljesülnek:*

1. *ω kiegészíthető egy homomorfizmussá $\tilde{\omega} : S \to K'$, ahol K' egy véges testbővítése F'-nek. Feltehetjük, hogy K'-t generálja $\tilde{\omega}(S)$ F' felett.*

2. *Minden $\tilde{\omega}$-ra K' test Galois F' felett, és generálja $\alpha' = \tilde{\omega}(\alpha)$ F' felett. Tudjuk, hogy $f'(\alpha') = 0$, ahol $f'(y) \in F'[y]$ a polinom, amit kapunk, ha alkalmazzuk ω-t f együtthatóin. Ezért $|K' : F'| = |K : F|$ pontosan akkor, ha f' irreducibilis. Ekkor K' F'-izomorf $F'[y]/(f')$-vel.*

3. *Tegy-k fel, hogy f' irreducibilis. Ekkor minden $\tilde{\omega}$-hoz egyértelműen létezik egy izomorfizmus $G \to G' = Gal(K'/F'), \sigma \mapsto \sigma'$, hogy $\tilde{\omega}(\sigma(s)) = \sigma'(\tilde{\omega}(s))$ minden $\sigma \in G, s \in S$ mellett.*

Bizonyítás. Mivel K/F egy Galois-bővítés, ezért $f(y)$ szeparábilis, tehát a diszkriminánsa D_f egy nem nulla eleme R-nek. Továbbá $\omega(D_f$ a diszkrimánsa $f'(y)$-nak a polinomnak, amit akkor kapunk, ha ω-t alkalmazzuk f együtthatóin. Továbbiakban csak olyan ω-kat veszünk, amelyekre $\omega(D_f) \neq 0$. Ekkor $f'(yO)$ szeparábilis.

Az $R[y]$ beli ideál I, amit f generál a magja az alábbi természetes leképezésnek: $R[y] \to R[\alpha], h \mapsto h(\alpha)$. Valóban, ha $h \in R[y]$ és $h(alpha) = 0$, akkor $h = gf$ valamilyen $g \in F[y]$-ra, mivel f α minimálpolinomja. Legyen $f = \sum_{i=0}^{n} a_i y^i, g = sum_{j=0}^{m} b_j y^j$, ahol $a_i \in R, b_j \in F$. Mivel f normált, ezért $b_m \in R$(mert megegyezik h legnagyobb együtthatójával). A második legnagyobb együtthatója h-nak $b_{m-1} + b_m a_{n-1}$, ezért $b_{m-1} \in R$. Ezt folytatva adódik, hogy $b_j \in R$. Tehát $g \in R$, és így $h \in I$. Ez a következő természetes izomorfizmust adja:

$$\phi : R[y]/I \to R[\alpha].$$

Első eset $R[A] = R[\alpha]$
Belátjuk, hogy ekkor 1-3 teljesül minden $\omega : R \to F'$, amire $\omega(D_f) \neq 0$.

Egészítsük ki ω-t egy leképezéssé $R[y] \to F'[y]$ (y-t fixen hagyja).Ez a leképezés f-et f'-be küldi, ezáltal az alábbi homomorfizmust indukálja:

$$\psi : R[y]/I = R[y]/fR[y] \to F'[y]/f'F'[y] = F'[y]/(f').$$

Legyen

$$\chi = \psi \circ \phi^{-1} : R[\alpha] \to F'[y]/(f').$$

1. Legyen $K' = F'[y]/(g')$, ahol g' egy irreducibilis osztója f'-nek. Ekkor K' egy véges testbővítése F'-nek. Ha χ-t komponáljuk a természetes leképezéssel $F'[y]/(f') \to F'[y]/(g')$, akkor egy homomorfizmust kapunk $S = R[\alpha] \to K'$, ami kiterjeszti ω-t.
2.Tudjuk, hogy $K' = F'[\omega(S)] = F'[\tilde{\omega}(\alpha)] = F'[\alpha']$, mivel feltettük, hogy $S = R[\alpha]$

α konjugáltjai F felett $\alpha_1, \alpha 2, ...\alpha_n$ mind $A \subset S$-ben vannak a feltétel szerint. Legyenek $\alpha'_1, ..., \alpha'_n$ a képeik $\tilde{\omega}$-ra nézve. $\tilde{\omega}$-t alkalmazva $f = (y - \alpha_1)...(y - \alpha n)$-re kapjuk, hogy $f'(y) = (y - \alpha'_1, ..., (y - \alpha_n)$.Tehát K' tartalmazza α' összes F' feletti konjugáltját, vagyis normális F' felett. Valamint K'/F' szeparábilis hiszen f' az. Ebből adódik, hogy K'/F' egy Galois-bővítés.2 további része nyilvánvaló.
3. Tegyük fel, hogy f' irreducibilis. Ekkor $\alpha'_1, .., \alpha'_n$ konjugáltak F' felett és páronként különbözőek, hiszen f' szeparábilis. Ekkor minden $i = 1, ..., n$-hez egyértelműen létezik egy $\sigma'_i \in G' = Gal(K'/F')$, hogy $\sigma'_i(\alpha') = \alpha'_i$. Valamint egyértelműen létezik egy $\sigma_i \in G = Gal(K/F)$, amire $\sigma_i(\alpha) = \alpha_i$. Tehát $\sigma_i \mapsto \sigma'_i$ egy bijekció $G \to G'$.

Most legyen $s \in S = R[\alpha]$ rögzített. s írható $h(\alpha)$ alakba, ahol $h(y) \in R[y]$. Legyen $h'(y) \in F'[y]$ a polinom, amit akkor kapunk, ha ω-t alkalmazzuk h együtthatóin Ekkor
$\sigma_i'(\tilde{\omega}(s)) = \sigma_i'(\tilde{\omega}(\alpha)) = \sigma_i'(h'(\alpha')) = \tilde{\omega}(h(\alpha_i)) = \tilde{\omega}(\sigma_i(h(\alpha))) = \tilde{\omega}(\sigma_i(s))$.
Ez bizonyítja, hogy $\sigma'(\tilde{\omega}(s)) = \tilde{\omega}(\sigma(s))$ minden $s \in S$ és $\sigma \in G$. Speciálisan $(\sigma\tau)'(\alpha') = (\sigma\tau)'(\tilde{\omega}(\alpha)) = \tilde{\omega}(\sigma\tau(\alpha)) = \sigma'(\tilde{\omega}(\tau(\alpha))) = \sigma'\tau'(\alpha')$. Tehát a leképezés $\sigma \mapsto \sigma'$ egy homomorfizmus, ezért egy izomorfizmus is.
/bf 2. eset Általános eset.

Minden $a \in A$ felírható az alábbi alakban:

$$a = \sum_{i=0}^{n-1} b_i \alpha^i$$

ahol $b_i \in F$. Válasszuk $v \neq 0, v \in R$ hogy $vb_i \in R$ minden lehetséges b_i-re. Ez lehetséges, mivel F R hatványteste.Legyen $u = vD_f$ és $\tilde{R} = R[u^{-1}]$. Ekkor minden $b_i \in \tilde{R}$, ezért $A \subset \tilde{R}[\alpha]$, tehát $\tilde{R}[A] = \tilde{R}[\alpha]$.

Ha $\omega : R \to F'$ egy homomorfizmus és $\omega(u) \neq 0$, akkor ω egyértelműen kiegészíthető egy homomorfizmussá $\tilde{R} \to F'$.Alkalmazzuk az első esetet $\tilde{R}$-re. □

A következő lemma tekinthető Hilbert irreduciblitási tételének egy nagyon gyenge vátlozatának.
Ezen túl a majdnem mindenütt kifejezés alatt azt értjük, hogy véges sok eset kivételével mindig teljesül.

2.1.2. Lemma. *Legyen L egy test, és $f(x, y) \in L[x, y]$ egy y-ban szeparábilis polinom. Ekkor a specializált polinom $f(b, y) \in L[y]$ szeparábilis majdnem minden $b \in L$-re.*

Bizonyítás. 2.0.7 alapján fel tehetjük, hogy f normált mint egy y beli polinom. Továbbá a detereminánsa $D(x) \in L[x]$, nem nulla, mert f szeparábilis.Minden $b \in L$-re, a $f(b, y) \in L[y]$ polinomnak a diszkriminánsa $D(b)$. Tehát $f(b, y)$ szeparábilis minden $b \in L$-re, kivéve $D(x)$ gyökeit. □

2.1.3. Állítás. *Legyen L egy véges Galois-bővítése $K(x)$-nek, aminek a rendje $n > 1$. Ekkor létezik egy polinom $f(x, y) \in K[x, y]$, hogy normált és a foka n y-ban, és α, ami generálja L-et $K(x)$ felett és $f(x, \alpha) = 0$. Továbbá:*

(i) Majdnem minden $b \in K$-ra az alábbi teljesül: ha a specializált polinom $f_b(y) := f(b, y)$ irreducibilis $K(x)$-ben, akkor $K[y]/(f_n)$ Galois K felett, és a Galois-csoportja izomorf $G = Gal(L/K(x)$-el.

(ii) Tegyük fel, hogy l egy véges bövítése K-nak L-ben. Legyen $h(x,y) \in l[x,y]$ irreduciblis mint y beli polinom $l[x]$ felett, és tegyük fel, hogy a gyökei L-ben vannk. Ekkor majdnem minden $b \in K$-ra az alábbi teljesül: ha $f(b,y)$ irreducibilis $K[y]$, akkor $h(b,y)$ irreducibilis $l[y]$-ban.

(iii) Létezik poolinommok egy véges halmaza $p_I(x,y) \in k[x][y]$, amelyek irreducibilisek és a fokuk > 1 mint polinomok y-ban $K[x]$ felett, hogy majdnem minden $b \in K$-ra az alábbiak igazak: ha egyik specializált polinomnak $p_I(b,y) \in K(x)$ sincs gyöke K-ban, akkor $f(b,y)$ irreducibilis $K[y]$-ban.

Bizonyítás. Legyen α L generátora $K(x)$ felett, és legyen $f(y) \in K(x)$ α minimálpolinomja. Ekkor f a következő alakban írható: $f(y) = (y-\alpha_1)...(y-\alpha_n)$, ahol $\alpha_1, ..., \alpha_n$ α konjugáltjai $K(x)$ felett.

$b \in K$-hoz legyen $\omega_b : K[x] \to K$ a következő homomorfizmus: $h(x) \mapsto h(b)$. Alkalmazzuk 2.1.1 állítást $F = K(x)$ és $\omega = \omega_b : R = K[x] \to F' = K$. Ekkor $f'(y)$ a polinom, amit akkor kapunk, ha alkalmazzuk ω-t $f(y)$ együtthatóin, megegyezik $f_b(y) = f(b,y)$-nal. Legyen $u = u(x) \in R = K(x)$ mint az 2.1.1 állításban. Ekkor $\omega_b(u) = u(b)$, ezért 2.1.1 állításai teljesülnek minden $b \in K$-ra kivéve u véges sok gyökét. 2.1.1 2-ből és 3-ból következik (i).

Továbbiakban tegyük fel, hogy $b \in K$ nem gyöke u-nak. Ekkor ω_b kiterjeszthető mint $\tilde{\omega} : S \to L'$, ahol S egy részgyűrű L-ben, ami tartalmazza $K[x][\alpha_1, ..., \alpha'_n$-t. és L' egy véges Galois-bővítése K-nak, amit $\tilde{\omega}(S)$ generál. Legyen $\alpha_1, ..., \alpha_n$ a $\tilde{\omega}$ általi képe $\alpha_1, ..., \alpha_n$-nek.Ekkor $f_b(y) = (y-\alpha'_1)...(y-\alpha'_n)$.

(iii) Legyen I egy valódi, nem üres részhalmaza $\{1, ..., n\}$-nek. Mivel f irreducibilis, az alábbi polinom: $\prod_{i\in I}(y-\alpha_i)$ nem lehet $K(x)[y]$-ban. Vagyis kell hogy legyen egy együtthatója d_I, hogy $d_I \notin K(x)$. Ekkor d_1 S-ben van. hiszen minden α_i S beli. És d_I gyöke egy polinomnak $p_I \in K(x)$, ami irreducibilis és a foka > 1. Megválaszthatjuk p_I-t úgy, hogy az együtthatói $K[x]$ beliek legyenek.

Most tegyük fel, hogy f_b nem irreducibilis. Ekkor van létezik egy I mint feljebb, hogy az alábbi polinom: $\prod_{i\in I}(y-\alpha'_i)$ $K[y]$ beli. Ebből adódik, hogy $c := \tilde{\omega}(d_I) \in K$, hiszen ennek a polinomnak az egyik együtthatója. Ha alkalmazzuk $\tilde{\omega}$-t az alábbi egyenleten: $p_I(x, d_I) = 0$, akkor azt kapjuk, hogy $p_I(b,c) = 0$.

(ii) Tegyük fel, hogy f_b irreducibilis, és írjuk h-t a következő alakban:

$$h(x,y) = h_0(x)\prod_{i=1}^{t}(y-\beta_i) \tag{2.1}$$

ahol $h_0(x) \in l[x]$ és $\beta_i \in L$.Feltehetjük, hogy minden β_i benne van a 2.1.1 állítás beli A halmazban, és ezáltal S-ben. Legyen $\beta_i' = \tilde{\omega}(\beta_i)$.

Továbbá fel tehetjük, hogy A tartalmazza l egy K feletti generátor elemét. Ekkor $l \subset S$. Tehát $\tilde{\omega}$ izomorfan megfelelteti l-t L' egy résztestével.Ebből a megfeleltetésből kapjuk a következőt:

$$h(b,y) = h_0(b)\prod_{i=1}^{t}(y-\beta_i')$$

Továbbá, a leképezés 2.1.1 állítás 3 pontjában $H = Gal(L/l(x)) \subset G$-t $H' \subset Gal(L'/l)$-be képezi.

Mivel h irreducibilis mint $l(x)[y]$ beli polinom, ezért szeparábilis is, mert $char(K) = 0$. És $H = Gal(L/l(x))$ csoport permutálja h gyökeit(β_i) tranzitívan. Ezért H' permutálja β_i'-t tranzitívan. Hagyjuk el azt a véges sok b-t, amire $h_0(b) = 0$, és amire $h(b,y)$ nem szeparábilis. Ekkor $h(b,y)$ polinom szeparábilis, és $H' \subset Gal(L'/l)$ csoport permutálja a gyökeit tranzitívan. Ebből adódik, hogy $h(b,y)$ irreducibilis l felett.

□

2.1.4. Következmény. *K-ra a következő feltételek ekvivalensek:*

1. *Minden $f(x,y)$ kétváltozós irreducibilis polinomhoz K felett, aminek a foka y-ban ≥ 1, létezik végtelen sok $b \in K$, hogy a specializált polinom $f(b,y)$ irreduciblis.*

2. *Ha adott L/K egy véges testbővítés, és $h_1(x,y),..,h_m(x,y) \in L[x][y]$ polinomok, melyek irreduciblisek y-ban $L[x]$ felett, akkor létezik végtelen sok $b \in K$, amire a specializált polinomok $h_1(b,y),...,h_m(b,y)$ irreducibilisek $L[y]$-ban.*

3. *Minden $p_1(x,y),...,p_t(x,y) \in K[x][y]$ polinomhoz, amelyek irreducibilisek és a fokuk > 1 y-ban $K(x)$ felett, létezik végtelen sok $b \in K$, hogy egyik specializált polinomnak $p_1(b,y),...,p_t(b,y)$ sincs gyöke K-ban.*

Bizonyítás. 2-ből következik 1 és 3. Ezért elegendő azt bizonyítani, hogy 1-ből és 3-ból is következik 2.

Legyen $h_1(x,y),...,h_m(x,y) \in L[x][y]$ olyan, mint 2-ben. Legyen S_0 ezen polinomok gyökeinek a halmaza $L(x)$ egy algebrai lezártjában, és legyen F egy véges bővítése $L(x)$-nek ami tartalmazza S_0-t és Galois $K(x)$ felett.

Most alkalmazzuk az előző állítást:
2.0.8 alapján a 2.1.3 (ii) beli f polinom irreduciblis mint kétváltozós polinom, ezért 2.1.3 (ii) szerint 1-ből következik 2.
2.1.3 (iii) miatt 3-ból is következik 2. □

2.1.5. Definíció. K testet akkor hívjuk Hilbert-féle testnek, ha teljesíti a fentebb leírt 3 ekvivalens feltétel valamelyikét.

2-ből és 1-ből adódik, hogy egy Hilbert-féle test minden véges bővítése is Hilbert-féle. A következő felyezetben bebizonyítjuk, hogy $\mathbb{Q}$ Hilbert-féle test, tehát minden algebrai számtest(ami $\mathbb{Q}$ felett véges fokú) szintén Hilbert-féle.

2.2. Hilbert-féle testek alapvető tulajdonságai

2.2.1. Állítás. *Tegyük fel, hogy K egy Hilbert-féle test, és $f(x_1,...,x_s)$ egy irreducibilis $s \geq 2$ változós polinom K felett, és a foka x_s-ben ≥ 1.*

1. *Ekkor létezik végtelen sok $b \in K$, hogy a specializált polinom $f(b,x_2,...,x_s)$ irreducibilis K felett*

2. *Minden nem nulla $p \in K[x_1,...,x_s]$-hez létezik $b_1,...,b_{s-1} \in K$, hogy $p(b_1,...,b_{s-1},x_s \neq 0$ és $f(b_1,...,b_{s-1},x_s)$ irreducibilis.*

Bizonyítás. Először megmutatjuk, hogy 2 következik 1-ből.Teljes indukciót használunk s-re. Az $s=2$ eset maga 1, ezért a továbbiakban tegyük fel, hogy $s>2$, és hogy az állítás igaz $s-1$-re. Írjuk fel p-t mint egy polinom $x_2,...,x_s$-ben úgy, hogy néhány együttható $c_j(x_1) \in K[x_1]$. 1 alapján létezik $b_1 \in K$, hogy $f'(x_2,...,x_s := f(b_1,x_2,...,x_s)$ irreducibilis, és $c_j(b_1) \neq 0$ valamilyen j-re. Ekkor $p'(x_2,...,x_{s-1}) := p(b_1,x_2,...,x_{s-1})$ nem nulla. Most alkalmazva az indukciós feltevést kapjuk, hogy vannak olyan $b_2,...,b_{s-1} \in K$-k, hogy $p'(b_2,...,b_{s-1}) \neq 0$ és $f'(b_2,...,b_{s-1},x_s)$ irreducibilis. Ezek kielégítik 2-t.

Legyen d egy egészszám, ami nagyobb mint a legnagyobb fokszám ami előfordul f bármelyik változójában. f Kronecker specializációján a következőt értjük:

$$S_d f(x,y) = f(x, y, y^d, ..., y^{d^{s-2}})$$

Amit felírhatunk az alábbi módon:

$$S_d f(x,y) = g(x) \prod_i g_i(x,y)$$

ahol $g_i(x,y)$ irreducibilis polinomok, melyeknek a foka y-ban ≥ 1, és $g(x) \in K[x]$ nem azonosan nulla. Mivel K Hilbert-féle, ezért létezik végtelen sok $b \in K$, hogy minden $g_i(b,y)$ irreducibilis. Ezentúl csak ilyen b-ket veszünk. Továbbá fel tehetjük, hogy $g(b) \neq 0$, hiszen g-nek csak véges sok gyöke lehet.

Most tegyük fel, hogy $f(b, x_2, ..., x_s)$ reduciblis, legyen $f(b, x_2, ..., x_s) = h(x_2, ..., x_s)h'(x_2, ..., x_s)$, ahol se h se h' nem konstans. A Kronecker specializációk $S_d h(y)$ és $S_d h'(y)$ legyen hasonlóan definiálva mint korábban. Ekkor $S_d f(b,y) = S_d h(y) S_d h'(y)$, tehát $S_d h(y)$ és $S_d h'(y)$ $g_i(b,y)$-ok szorzata. Legyen $H(x,y)$ és $H'(x,y)$ a megfelelő $g_i(x,y)$-ok szorzata.Ekkor $S_d(x.y) = g(x)H(x,y)H'(x,y)$.

Mivel az egészszámok d-edik hatványra emelése egyértelmű, ezért egyértelműen léteznek $\tilde{h}(x_1, ..., x_s)$, $\tilde{h'}(x_1, ..., x_s)$ polinomok, hogy a legmagasabb előforduló fokszámuk kisebb mint d. Ha ez teljesülne $\tilde{f} := \tilde{h}\tilde{h}'$-re, akkor $\tilde{f} = f$ is teljesülne, mert az egészszámok d-edik hatványra emelése egyértelmű. De ez ellentmondana annak, hogy f irreducibilis, hiszen $\tilde{f} = \tilde{h}\tilde{h'}$ és se $\tilde{h}$ se $\tilde{h}'$ nem konstans.

Tehát $\tilde{f}$ tartalmaz egy monomot $\kappa(x_1)x_2^{i_2}, ..., x_s^{i_s}$, ahol $i_v \geq d$, valamilyen v-re, és $\kappa \neq 0$.Vegyük észre, hogy $\tilde{h}(b, x_2, ..., x_s)$ konstansszorosa $h(x_2, ..., x_s)$-nek. Hasonlóan h'-re. Ezért $\tilde{f}(b, x_2, ..., x_s)$ is konstans szorosa $f(b, x_2, ..., x_s)$-nek. Ebből adódik, hogy $\kappa(b) = 0$.

Csak véges sok fajta κ tartozhat $S_d f$ összes lehetséges felbontásához. Ha olyan b-t választunk, ami különbözik ezektől, akkor $f(b, x_2, ..., x_s$ irreduciblis. □

2.2.2. Következmény. *Ha K Hilbert-féle test, akkor minden végesen generált bővítése is az.*

Bizonyítás. Először vegyünk csak tisztán transzcendens bővítéseket $F = K(x_1, ..., x_m)$. Legyen $D = K[x_1, ..., x_m]$, és legyen $f(x,y) \in F[x,y]$ irreduciblis és a foka y-ban ≥ 1. Ekkor 2.0.8 alapján f irreduciblis y-ban $F(x)$ felett. Feltehetjük, hogy $f \in D[x,y]$. 2.0.8 alapján feltehetjük azt is, hogy f irreduciblis mint polinom $x_1, ..., x_m, x, y$ változókban. Ekkor az előző állítás alapján létezik végtelen sok $b \in K$, hogy $f(x_1, ..., x_m, b, y)$ irreduciblis. Ekkor $f(x_1, ..., x_m, b, y)$ irreducibilis y-ban D felett, tehát F felett is. Vagyis F Hilbert-féle test.

Most tegyük fel, hogy L egy tetszőleges végesen generált bővítése K-nak. Ekkor L vagy véges K elett, vagy K egy tisztán transzcendens bővítése felett F. De F Hilbert-féle a korábbiak alapján, tehát L is az hiszen a Hilbert-féle testek véges bővítései szintén Hilbert-félék. □

2.2.3. Megjegyzés. *Valójában $K(x_1, \ldots, x_m)$ Hilbert-féle tetszőleges K testre és $m \geq 1$-re.(lásd[5] 12.10)*

2.2.4. Tétel. *Tegyük fel, hogy K Hilbert-féle test. Ha egy véges csoport G fellép mint Galois-csoport $k(x_1, ..., x_m)$ felett, ekkor G K felett is fellép mint Galois-csoport.*

Bizonyítás. Ha $m > 1$, akkor $K(x_1, ..., x_m) = K(x_1, ..., x_{m-1})(x_m)$. Mivel $K(x_1, ..., x_{m-1})$ Hilbert-féle az előző állítás alapján, így elegendő az $m = 1$ esettel foglalkozni, ami adódik a 2.1.3 (i)-ből. □

2.2.5. Definíció. Legyen G egy véges csoport. Azt mondjuk, hogy G fellép regulárisan K felett, ha valamilyen $m \geq 1$-hez létezik egy Galois-bővítése $K(x_1, ..., x_m)$-nek, ami reguláris K felett, hogy a Galois-csoportja izomorf G-vel.

Az egyik meghatározó tulajdonsága a reguláris megvalósulásnak az, hogy invariáns az alaptest bővítésére.

2.2.6. Következmény. *Tegyük fel, hogy G fellép regulárisan K felett. Ekkor G fellép regulárisan minden K_1 K feletti testbővítés felett is. Vagyis G fellép Galois-csoportként K_1 felett, ha K_1 Hilbert-féle.*

Bizonyítás. Tegyük fel, hogy $x_1, ..., x_m$ egymástól független transzcendensek K_1 felett, és legyen $x = (x_1, ..., x_m)$. Fel tehetjük, hogy $G = Gal(F/K(x))$, ahol F reguláris K felett. Legyen $n = |G| = |F : K(x)|$. Írjuk F-t $F = K(x)[y]/(f)$ alakba, valamilyen $f(x, y) \in K(x)[y]$ mellett.Ekkor f irreduciblis $\overline{K_1}(x)$ felett 2.0.3 2 alapján. Ezért $F_1 = K_1(x)[y]/(f)$ egy testbővítése $K_1(x)$-nek, a foka n és reguláris K_1 felett. Valamint F_1 Galois K_1 felett, hiszen f minden $K_1(x)$ feletti gyöke benne van F-ben. Ekkor $Gal(F_1/K_1(x))$ és $Gal(F/K(x))$ azonos rendűek, és a korábbi beágyazható a másikba egy megszorítással. Tehát izomorfak. Ez bizonyítja az állítás első felét.Az állítás másik fele adódik az előző tételből. □

2.2.7. Példa. *A szimmetrikus csoport S_n minden K test felett regulárisan fellép.*

Vegyük az alábbi polinomot nem meghatározott együtthatókkal:

$$f(y) = y^n + x_1 y^{n-1} + ... + x_n = \prod_{i=1}^{n}(y - t_i)$$

ekkor $f \in K(x_1, ..., x_n)[y]$. *Tehát a gyökei is* $t_1, ..., tn$ *egymástól független transzcendensek* K *felett.* S_n *természetes hatása* $t_1, ..., t_n$*-en (az indexek permutációja) kiegészül* S_n *egy hatásává a* $K(t_1, ..., t_n)$ *testen. Ennek a hatásnak a fixteste* F *tartalmazza* $x_1, ..., x_n$*-t, és* $|K(t_1, .., t_n)| = |S_n| = n!$. *Ugyanakkor mivel* $t_1, ..., t_n$ *egy olyan polinom gyökei, ami* n*-ed fokú* $K(x_1, ..., x_n)$ *felett, ezért* $|K(t_1, ..., t_n) : K(x_1, ..., x_n)| \leq n!$. *Ebből adódik, hogy* $F = K(x_1, ..., x_n)$. *2.0.3 alapján:*

$$Gal(K(t_1, ..., t_n)/K(x_1, ..., x_n)) = S_n.$$

Tehát S_n *fellép regulárisan* K *felett.*

3. fejezet

A racionális számok teste Hilbert-féle

3.1. A gyökök analitikája

3.1.1. Tétel. *Legyen $f(x,y) \in \mathbb{C}[x,y]$ egy polinom, aminek a foka y-ban $n \geq 1$. Legyen $c_0 \in \mathbb{C}$ olyan, hogy a specializált polinom $f(c_0,y) \in \mathbb{C}[y]$ szeparábilis. Ekkor léteznek holomorf függvények $\psi_1, ..., \psi_n$ amelyek definiálva vannak c_0 egy U környezetében, hogy minden $c \in U$-ra a polinomnak, $f(c,y)$-nak, n különböző gyöke van: $\psi_1(c), ..., \psi_n(c)$.*

Bizonyítás. Elegendő belátni, hogy $f(c_0,y)$ minden γ gyökéhöz létezik holomorf ψ, ami definiálva van c_0 körül, valamint $\psi(c_0 = \gamma$ és $f(c,\psi(c)) = 0$ minden c-re, ami közel van c_0-hoz. Valóban, minden c-re, ami elég közel van c_0-hoz az n darab ψ függvény különböző értékeket vesz fel c-n, vagyis előáll $f(c,y)$ mindne gyöke.

Feltehetjük, hogy $c_0 = \gamma = 0$(lecseréljük x-et $x - c_0$-ra y-t $y - \gamma$-ra).Vagyis egy olyan ψ-t keresünk, ami holomorf, $\psi(0) = 0$ és

$$f(t,\psi(t)) = 0 \tag{3.1}$$

minden t-re, ami elég közel van 0-hoz. Egy ilyen ψ Taylor sorba fejthető 0 körül a következő féleképpen: $\psi(t) = \sum_{i=1}^{\infty} a_i t^i$.

A feltevés szerint $f(0,0) = 0$, tehát

$$f(x,y) = ax + by + \text{magasabb fokú tagok.}$$

Itt $b = (\partial f/\partial y)(0,0) \neq 0$, hiszen 0 egyszeres gyöke $f(0,y)$-nak. Feltehetjük, hogy $b = 1$,különben leosztunk vele.Ekkor

$$g(x,y) := y - f(x,y)$$

polinomnak nincs se konstans, se y-beli tagja.3.1 feltétel ekvivalens az alábbival:

$$\psi(t) = g(t, \psi(t))$$

Ez az egyenlőséeg lehetővé teszi ψ együtthatóinak rekurzív kiszámítását, ha jobb oldalt hatványsorba fejtjük 0 körül. Valóban a t^i-hez tartozó együttható a jobb oldalon csak olyan a_j-ktől függ, amelyekre $j < i$, és g együtthatóitól. A rekurzió végeztével megkapjuk a_i-t g együtthatóinak egy pozitív egész együtthatós polinomjaként.

Ezek az a_i-k egyértelműen meghatátozzák $\psi(t)$ hatványsorát az alábbi formában:

$$\psi(t) = \sum_{i=0}^{\infty} a_i t^i$$

ami formálisan megoldja 3.1 egyenletet. De még be kell bizonyítani hogy a konvergencia sugara pozitív.

Legyen C egy pozitív konstans, ami nagyobb mint g bármelyik együtthatójának az abszolútértéke. Tekintsük az alábbi függvényt:

$$\tilde{g}(t,u) = C(-1 - u + \tfrac{1}{(1-t)(1-u)})$$

Ha megoldjuk a $u = \tilde{g}(t,u)$ másodfokú egyenletet u-ban t függvényében, akkor a következőt kapjuk:

$$\tilde{\psi}(t) = \tfrac{1}{2(C+1)}\left(1 - \tfrac{\sqrt{1-t(1+(1+2C)^2)+t^2(1+(1+2C)^2)}}{1-t}\right)$$

egy holomorf függvény, ami definiálva van 0 körül és $\tilde{\psi}(0) = 0$, továbbá:

$$\tilde{\psi}(t) = \tilde{g}(t, \tilde{\psi}(t)). \tag{3.2}$$

(Itt a négyzetgyök függvénynek azt az ágát alkalmaztuk 1 körül, amelyikre $\sqrt{1} = 1$.) A geometria sor a következőt adja:

$$\tilde{g}(t,u) = C(t + t^2 + tu + u^2 + ...) = C\left(-1 - u + \sum_{\mu,\nu=0}^{\infty} t^\mu u^\nu \right)$$

Minden $|t| < 1, |u| < 1$.-re. Ebből és a 3.2 egyenletből adódik, hogy $\tilde{\psi}$ Taylor-sorának az együtthatóit, $\tilde{a}_i$-ket,ugyanannak a polinomnak a segítségével kaptuk meg mint az a_i-ket, csak most $\tilde{g}$ együtthatóira alkalmaztuk, amelyek mind megegyeznek C-vel. Mivel C nagyobb abszolút értékben mint g bármelyik együtthatója, ezért $|a_i| \leq \tilde{a}_i$ minden i-re. De a $\sum_{i=1}^{\infty} \tilde{a}_i t^i$ Taylor-sor konvergenciasugara pozitív, tehát a $\psi(t) = \sum_{i=1}^{\infty} a_i t^i$ konvergenciasugara is az. □

3.2. Hilbert irreducibilitási tétele

3.2.1. Definíció. Legyen $M \subset \mathbb{N}$. Azt mondjuk, hogy M ritka, ha létezik olyan κ valósszám, hogy $0 < \kappa < 1$ és

$$|M \cap \{1, ..., N\}| \leq N^{\kappa}$$

majdnem minden N-re.

3.2.2. Megjegyzés. *Könnyen látható, hogy mindne véges halmaz ritka. Általánosabban ritka halmazok véges uniója is ritka.*

3.2.3. Tétel. *Legyen $i_0 \in \mathbb{Z}$, és legyen*

$$\phi(t) = \sum_{i=i_0}^{\infty} a_i t^i$$

egy Laurent-sor komplex együtthatókkal, ami konvergens minden $t \neq 0$-ra 0 egy környezetében $\mathbb{C}$-ben. Legyen $B(\phi)$ azon $b \in \mathbb{N}$-ek halmaza, amelyekre $\phi(1/b)$ definiálva van és egész. Ekkor $B(\phi)$ egy ritka halmaza, ha ϕ nem egy Laurent polinom.

A tétel bizonyítás elemi kalkulus. Majd a fejezet végén bebizonyítjuk. Először belátjuk, hogy $\mathbb{Q}$ Hilbert-féle test.

3.2.4. Állítás. *Legyen $p(x, y) \in \mathbb{Q}[x][y]$ irreduciblis $\mathbb{Q}$ felett és legyen a foka $r > 1$ y-ban. Ekkor majdnem minden $x_0 \in \mathbb{Z}$-re teljesülnek az alábbiak:*

a Létezik $\epsilon > 0$ és holomorf függvények $\psi_1(t), .., \psi_r(t)$, amelyek úgy vannak definiálva komplex t-re, ahol $|t| < \epsilon$, hogy $\psi_1(t), .., \psi_r(t)$ a $p(x_0 + t, y) \in \mathbb{Q}[y]$ polinom gyökei.

b Ha valamelyik $\psi_i(t)$ a t törtfüggvénye (komplex együtthatókkal), akkor csak véges sok olyan $q \in \mathbb{Q}$ van, hogy $\psi_i(q) \in \mathbb{Q}$.

c Legyen $B(p, x_0)$ a halmaza az összes $b \in \mathbb{N}$-nek, amire $p(x_0 + \frac{1}{b}, c) = 0$ valamilyen $c \in \mathbb{Q}$-ra. Ekkor $B(p, x_0$ egy ritka halmaz.

Bizonyítás. A Polinom p irreducibilis, tehát szeparábilis ($\mathbb{Q}(x)$ felett). Tehát $p(x_0, y)$ szeparábilis majdnem minden $x_0 \in \mathbb{Z}$-re 2.1.2 alapján. Ezen túl csak ilyen x_0-t vegyünk.

(a) A 3.1.1 tételből következik

(b) Tegyük fel, hogy $\psi := \psi_i$ egy törtfüggvény t-ben. Ekkor $p(x_0 + t, \psi(t))$ azonosan nulla. Tehát $p(x_0 + x, \psi(x)) = 0$ $\mathbb{C}(x)$-ben, valamilyen x elemre, ami transzcendens $\mathbb{C}$ felett. Ekkor $\psi(x) \in \mathbb{C}(x)$ algebrai $\mathbb{Q}(x)$ felett, ezért $\bar{\mathbb{Q}}(x)$ felett is. De $\bar{\mathbb{Q}}(x)$ algebrailag zárt $\mathbb{C}(x)$ felett (Valóban minden irreducibilis polinom $\bar{\mathbb{Q}}(x)$ felett irreducibilis $\mathbb{C}(x)$ felett is 2.0.3 2 alapján). Ebből következik, hogy $\psi(x) \in \bar{\mathbb{Q}}(x)$.

Minden $\beta \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-ra legyen ψ^β az a törtfüggvény, amit akkor kapunk, ha β-t alkalmazzuk ψ együtthatóin. Ekkor $\psi^\beta(q) = \psi(q)$ minden $q \in \mathbb{Q}$-ra, ahol $\psi(q) \in \mathbb{Q}$. Ha végtelen sok ilyen q létezik, akkor $\psi^\beta = \psi$ minden β-ra, tehát ψ együtthatói racionálisak. Ekkor $\psi(x - x_0 \in \mathbb{Q}(x)$ $p(x, y)$ egy nullhelye $\mathbb{Q}(x)$ felett. Ez ellentmond a feltételezéssel miszerint p irreducibilis $\mathbb{Q}(x)$ felett.

(c) Feltehetjük, hogy $p(x, y) \in \mathbb{Z}[x, y]$. Írjuk p-t a következő alakba:

$$p(x, y) = \sum_{i=0}^{r} p_i(x) y^i$$

ahol $p_i(x) \in \mathbb{Z}[x]$.Megfelelően nagy R-re az alábbi kifejezés:

$$x^R p\big(x_0 + \frac{1}{x}, y\big) = \sum_{i=0}^{r} x^R p_i\big(x_0 + \frac{1}{x}\big) y^i$$

$\mathbb{Z}[x, y]$ egy eleme. Jelölje $p_i(x)$ az y^i-hez tartozó együtthatót. Ekkor $h(x) := p'_r(x)$ egy nem nulla eleme $\mathbb{Z}[x]$-nek. Legyen:

$$p'(x, Z) = Z^r + \sum_{i=0}^{r-1} p'_i(x) h(x)^{r-i-1} Z^i$$

egy eleme $\mathbb{Z}[x, Z]$-nek.

Tegyük fel, hogy $p(x_0 + \frac{1}{b}, c) = 0$, ahol $c \in \mathbb{Q}, b \in \mathbb{Z}$. Mivel $p'(b, Z) \in \mathbb{Z}[Z]$ egy normált polinom, tehát $h(b)c$ egy algebrai elem $\mathbb{Z}$ felett. De mivel $h(b)c \in \mathbb{Q}$ ezért $\mathbb{Z}$ beli.

Ha továbbá $|1/b| < \epsilon$, akkor $c = \psi_i(1/b)$ valamilyen $i = 1, ..., r$-re ((a) alapján). Tehát $h(b)\psi_i(1/b) = h(b)c \in \mathbb{Z}$.

Legyen $\phi_i(t) = h(t^{-1}\psi_i(t)$, ahol $0 < |t| < \epsilon, i = 1, ..., r$. Ekkor az előbbi alapján ha $b \in B(p, x_0)$ és $1/b < \epsilon$, akkor $\phi_i(1/b) = h(b)\psi_i(1/b) \in \mathbb{Z}$ valamilyen $i = 1, ..., r$-re. Ekkor $B(p, x_0)$ valamilyen véges halmaz erejéig benne van a $B(\phi_i)$-k uniójában. 3.2.3 tétel alapján $B(\phi_i)$ egy ritka halmaz ha ϕ_i nem egy törtfüggvény. Ugyanakkor ha ϕ_i és ezáltal ψ_i is törtfüggvény, akkor (b) szerint $B(\phi_i)$ véges. Ebből adódik, hogy $B(p, x_0)$ ritka. □

3.2.5. Tétel (Hilbert irreducibilitási tétele)**.** $\mathbb{Q}$ *egy Hilbert-féle test.*

Bizonyítás. Ha adott egy polinom $p_j(x, y) \in \mathbb{Q}[x][y]$ mint a 2.1.5 definíció 3. pontjában, választhatunk $x_0 \in \mathbb{Z}$-t mint a 3.2.4 állításban ami működik minden p_j-re. Legyen C azon $b \in \mathbb{N}$-ek halmaza, melyekre egyik specializált polinom $p_j(x_0 + \frac{1}{b}, y)$ sincs gyöke $\mathbb{Q}$-ban. Legyen $B = \mathbb{N}\backslash C$. Ekkor B a $B(p_j, x_0)$ halmazok unijója. Melyek a 3.2.4 állítás (c) része értelmében ritkák. Tehát B is ritka, ami azt jelenti hogy a komplementere, C egy végtelen halmaz. Ez igazolja a feltevést. □

Hátra van még a 3.2.3 tétel bizonyítása. Ez egy általános középérték tételen alaszik, ami H.A. Schwarz nevéhez köthető.

3.2.6. Lemma. *Legyen $s_0 < s_1 < \cdots < s_m$ valós számok, ahol $m \geq 1$. Legyen $\chi(s)$ egy valósértékű függvény ami definiálva van $s_0 \geq s \geq s_m$-re, és m-szer folytonosan deriválható. Legyen V_m a Vandermonde determináns*

$$V_m = \begin{vmatrix} 1 & s_0 & s_0^2 & \dots & s_0^m \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & s_m & s_m^2 & \dots & s_m^m \end{vmatrix} = \prod_{i>j}(s_i - s_j)$$

Ekkor létezik egy σ szám $s_0 < \sigma < s_m$, hogy

$$\frac{\chi^{(m)}(\sigma)}{m!} = \frac{1}{V_m} \begin{vmatrix} 1 & s_0 & \dots & s_0^{m-1} & \chi(s_0) \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & s_m & \dots & s_m^{m-1} & \chi(s_m) \end{vmatrix}$$

Bizonyítás. Legyen $F(s)$ az alábbi függvény:

$$F(s) = \begin{vmatrix} 1 & s_0 & \dots & s_0^{m-1} & \chi(s_0) \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & s_{m-1} & \dots & s_{m-1}^{m-1} & \chi(s_{m-1}) \\ 1 & s & \dots & s^{m-1} & \chi(s) \end{vmatrix}$$

Legyen

$$c = \frac{F(s_m)}{(s_m - s_0 \dots (s_m - s_{m-1})}$$

és

$$G(s) = F(s) - c(s - s_0) \dots (s - s_{m-1}).$$

Ekkor $G(s)$ eltűnik az alábbi $m+1$ helyen: $s_0, \dots, s_m$. Ezért $G^{(m)}(s)$ eltűnik, legalább egy σ köztes pontban. Mivel $G^{(m)}(s) = F^{(m)}(s) - m!c$, ezért:

$$F^{(m)}(\sigma) = m!c.$$

Ugyanakkor, ha kifejtjük a determinánst, ami definálja $F(s)$-t a következőt kapjuk:

$$F(s) = \sum_{i=0}^{m-1} c_i s^i + V_{m-1}\chi(s)$$

ahol a c_i-k konstansok, amik $s_0, ..., s_m$-től függnek, és V_{m-1} a Vandermonde determinánsa $s_0, ..., s_m$-nak. Tehát

$$F^{(m)}(\sigma) = V_{m-1}\chi^{(m)}(\sigma).$$

Ha összevetjük $F^{(m)}(\sigma)$ két alakját, akkor a következőt kapjuk:

$$\frac{\chi^{(m)}(\sigma)}{m!} = \frac{c}{V_{m-1}} = \frac{F(s_m)}{(s_m - s_0) \dots (s_m - s_{m-1})V_{m-1}} = \frac{F(s_m}{V_m}.$$

$F(s_m)$ definíciója alapján készen vagyunk. □

3.2.3 tétel bizonyítása

Bizonyítás. Legyen $\phi(t)$ olyan, mint 3.2.3 tételben, és tegyük fel, hogy nem egy laurent polinom. Továbbá tegyük fel, hogy $B(\phi)$ végtelen. Ekkor a következőt tudjuk:

3.2.7. Lemma. *ϕ együtthatói valósak.*

Bizonyítás. Az alábbi sorozat:

$$\bar{\phi}(t) = \sum_{i=i_0}^{\infty} \bar{a}_i t^i$$

komplex konjugált együtthatókkal, konvergencia sugara ugyankkora, mint ϕ-é. Tehát $\bar{\phi}(1/b) = \phi(1/b)$ minden $b \in B(\phi)$-re. $\bar{\phi} = \phi$, mivel $B(\phi)$ végtelen. □

Ebből adódik, hogy $\chi(s) := \phi(s^{-1})$ egy valós értékű függvény. Tudjuk hogy $\chi(s)$ az alábbi alakba írható:

$$\chi(s) = \sum_{i=i_0}^{\infty} a_i s{-}i.$$

3.2.8. Lemma. *Létezik olyan $\lambda > 0$ és $m, S \in \mathbb{N}$, hogy a következő teljesül: Ha $s_0, \ldots, s_m \in F$ olyan, hogy $\chi(s_0, \ldots, \chi(s_m) \in \mathbb{Z}$ és $S < s_0 < \cdots < s_m$, akkor*

$$s_m - s0 \geq s_0^{\lambda}$$

Bizonyítás. Elég nagy m-re az alábbi sorozatnak:

$$\chi^{(m)}(s) = \sum_{i=\mu}^{\infty} d_i s{-}i$$

csak olyan tagjai vannak, amelyekben az s negatív hatványa szerepel, vagyis $\mu > 0$. Itt a d_i-k valós számok, és feltehetjük, hogy $d_\mu \neq 0$, hiszen ϕ nem egy Laurent-polinom. Ekkor $S^\mu \chi^{(\mu)}(s)$ tart d_μ-höz, ahogy s tart a végtelenbe. Ezért létezik olyan $S > 0$, hogy $0 < |S^\mu \chi^{(\mu)}(s)| < |2d_\mu|$ minden $s \geq S$-re.

Most tegyük fel, hogy $s_0, \ldots, s_m$ olyan, mint a lemma feltétetlében, válasszuk σ-t úgy, mint 3.2.6 lemmában. Ekkor $\frac{V_m \chi^{(m)}(\sigma)}{m!}_1$ egy nem nulla egész szám, tehát az abszolútértéke ≥ 1. Vagyis $V_m \geq \frac{1}{|\chi^{(m)}(\sigma)|}$, és így:

$$(s_m - s_0)^{(m+1)(m+2)/2} \geq V_m \geq \frac{1}{|\chi^{(m)}(\sigma)|} \geq \frac{1}{|2d_\mu|}\sigma^\mu \geq \frac{1}{|2d_\mu|} s_0^\mu.$$

Ezért

$$s_m - s_0 \geq \left(\frac{1}{|2d_\mu|}^{2/(m+1)(m+2)} s_0^{2\mu/(m+1)(m+2)}.\right.$$

Tehát bármilyen $\lambda < 2\mu/(m+1)(m+2)$ megfelel □

3.2.9. Lemma. *Legyen $b_1 < b_2 < \ldots$ pozitív egészek egy végtelen sorozata, ahol $b_{i+1} - b_i \geq b_i^\lambda$, valamilyen $\lambda > 0$ mellett. Ekkor a $B = \{b_1, b_2, \ldots\}$ halmaz ritka.*

Bizonyítás. Minden pozitív egész N-hez legyen N' azon $b \in B$-k száma, amik $\sqrt{N} < b \leq N$.Ekkor $(N'-1)\sqrt{N}^\lambda \leq N$. Ezért:

$$N' - 1 \leq N^{1-\frac{\lambda}{2}}.$$

Tehát

$$|B \cap 1, \ldots, N| \leq \sqrt{N} + N' \leq \sqrt{N} + N^{1-\frac{\lambda}{2}} + 1.$$

Ebből következik, hogy B ritka. □

$B(\phi)$ definíció szerint azon $b \in \mathbb{Z}$-k halmaza, melyekre $\chi(b) = \phi(1/b)$ egész szám. Hagyjuk el $B(\phi)$-ből az összes S-nél kisebb számot, ahol S olyan mint 3.2.8 lemmában. Ekkor 3.2.8 alapján a maradék felírható mint m darab részhalmaz uniója, ahol mindegyik részhalmaz 3.2.8 alapján olyan alakú mint a 3.2.9 beli B halmaz, ami ritka, tehát $B(\phi)$ is ritka. □

4. fejezet

Hilbert-féle testek algebrai bővítései

Minden végesen generált bővítése egy Hilbert-féle testnek szintén Hilbert-féle. Ezt jól kiegészíti Weissauer tétele, ami Hilbert-féle testek végtelen algebrai bővítéseiről szól. Weissauer eredeti bizonyítása nem standard metódusokat használt, később Fried adott rá egy algebrai bizonyítást, ennek az ötletét követjük itt.

4.1. Weissauer tétele

4.1.1. Lemma. *Legyen K egy Hilbert-féle test, és legyen L/K véges. Legyen $\pi, \tilde{\pi} \in L[x_1, x_2][y]$, normált y-ban, ahol x_1, x_2 algebrailag független L felett. Tekintsük π-t és $\tilde{\pi}$-t y beli polinomoknak $L(x_1, x_2$ felett, és tegyük fel, hogy π-nek nincs gyöke $\tilde{\pi}$ felbontási testében. Ekkor bármely nem nulla $\nu \in L[x_1, x_2]$-höz létezik $b_1, b_2 \in K$ amire $\nu(b_1, b_2) \neq 0$, hogy $\pi(b_1, b_2, y)$-nek nincsen gyöke $\tilde{\pi}(b_1, b_2, y)$ felbontási testében. Itt $\pi(b_1, b_2, y)$-t és $\tilde{\pi}(b_1, b_2, y)$-t y beli polinomnak tekintjük L felett*

Bizonyítás. Legyen $F/L(x_1, x_2)$ egy véges Galois-bővítés, ami tartalmazza π és $\tilde{\pi}$ összes gyökét. Legyen α $F/L(x_1, x_2)$ egy generátora, és f α minimálpolinoma $f(y) = f(x_1, x_2, y) \in L[x_1, x_2][y]$. Ekkor 2.0.8 és 2.2.1 2 alapján léteznek $b_1, b_2 \in L$ amire $\nu(b_1, b_2) \neq 0$, hogy $f(b_1, b_2, y)$ irreducibilis L felett. Kihasználva azt, hogy K Hilbert-féle a 2.1.4 2, és a 2.2.1 2 bizonyítása alapján tudunk olyan b_1, b_2-t választani, ami K beli. Mostantól csak ilyeneket veszünk.

Legyen $\omega_{b_1,b_2} : L[x_1, x_2] \to L$ a kiszámítási homomorfizmus $h(x_1, x_2) \mapsto h(b_1, b_2)$.2.1.1 alapján feltehetjük(miután ν-t lecseréltük νu-ra egy alkalmas $u \in L[x_1, x_2]$ mellet), hogy ω_{b_1,b_2} kiegészül egy $\omega : S \to F'$ homomorfizmussá, ahol S egy részgyűrű K-ban, ami tartalmazza π és $\tilde{\pi}$ összes gyökét, és F' egy véges Galois-bővítése L-nek. Mivel $f(b_1, b_2, y)$ irreducibilis feltehetjük, hogy létezik egy $G = Gal(F/L(x_1, x_2)) \to G' = Gal(F'/L), \sigma \mapsto \sigma'$ izomorfizmus, amire $\omega\sigma(s) = \sigma'\omega(s)$ teljesül minden $s \in S, \sigma \in G$ mellett.

Továbbá feltehetjük, hogy π szeparábilis. Ekkor a diszkriminánsa, D, nem nulla eleme $L[x_1, x_2$-nek. Ha ν-t lecseréljük $D\nu$-re, akkor feltehetjük, hogy $\pi(b_1, b_2, y)$ is szeparábilis(lásd 2.1.2 bizonyítása).

Írjuk π-t a következő formába: $\pi(y) = (y - \beta_1) \dots (y - \beta_s)$. Ekkor $\pi(b_1, b_2, y) = (y - \beta'_1) \dots (y - \beta'_s)$, ahol $\beta'_i = \omega(\beta_i$. Hasonlóan $\tilde{\pi}(y) = (y - \gamma_1) \dots (y - \gamma_t)$ és $\tilde{\pi}(b_1, b_2, y) = (y - \gamma'_1) \dots (y - \gamma'_t)$. A lemma feltétele szerint minden β_i-hez van olyan $\sigma \in G$, ami fixen hagyja az 0sszes γ_ν-t, de a β_i-ket nem; legyen $\sigma(\beta_i) = \beta_j$, ahol $\beta_i \neq \beta_j$.

Ekkor σ' fixen hagyja az összes γ_ν-t.$\beta'_i \neq \beta'_j$ mivel $\pi(b_1, b_2, y)$ szeparábilis, tehát σ' nem hagyja fixen β'_i-t. □

4.1.2. Tétel (Weissauer)**.** *Legyen K Hilbert-féle test, legyen N K egy Galois-bővítése, és legyen M egy véges bővítése N-nek és $M \neq N$. Ekkor M Hilbert-féle test.*

Bizonyítás. A 3-as kritériánt használjuk a 2.1.5 definícióból. Tehát legyenek $p_j(x, y) \in M[x][y]$-ok irreducibilis polinomok, melyek foka > 1 y-ban $M(x)$ felett. Azt kell igazolni, hogy létezik végtelen sok olyn $b \in M$, hogy egyik $p_j(b, y)$ specializált polinomnak sincs gyöke M-ben.

Feltehetjük, hogy p_j normált y-ban (csak hagyjuk el azt a véges sok b-t amelyek gyökei a legmagasabb fokszámú y beli együtthatónak, vagyis $a_j(x) = 0$ valamelyik p_j-re). Továbbá feltehetjük, hogy az 0sszes p_j különböző, tehát a szorzatuk $p(x, y)$ szeparábilis y-ban. Azt kell megmutatnunk, hogy létezik végtelen sok $b \in M$, hogy $p(b, y)$-nak nincsen gyöke M-ben.

A következő lemma alapján feltehetjük, hogy nincs olyan $\gamma \in \bar{M}(x)$, hogy $p(x, \gamma) = 0$.

4.1.3. Lemma. *Tegyük fel, hogy $q = p_j$-re az alábbiak teljesülnek: $q(x, g(x)) = 0$ valamilyen $g(x) \in \bar{M}(x)$. Ekkor csak véges sok olyan $b \in M$ van, amire $q(b, y)$-nak van M-ben gyöke.*

Bizonyítás. q összes $M(x)$ beli gyöke $\bar{M}(x)$-ben van, mivel $\bar{M}(x)$ Galois $M(x)$ felett. Tehát $q(x, y) = \prod_i (y - g_i(x))$, ahol $g_i(x) \in \bar{M}(x)$, de $g_i(x) \notin M(x)$,

hiszen q irreducibilis és a foka > 1 y-ban. Ekkor csak véges sok olyan $b \in M$ van hogy $g_i(b) \in M$ (hasonlóan adódik mint 3.2.4 (b) részének a bizonyítása). □

Ágyazzuk be M-et K valamilyen $\bar{K}$ algebrai lezártjába. Legyen $M = N(\theta)$. Ekkor $\theta \notin N$. Legyen L egy véges Galois-bővítése K-nak, ami tartalmazza θ-t és $p(x, y)$ együtthatóit. Válasszunk egy $\tilde{\theta} \in L$-et, ami θ konjugáltja $\hat{K} := N \cap L$ felett, de $\tilde{\theta} \neq \theta$.

Most vezessünk be új változókat x_1, x_2-t, és $\pi(y) :=](x_1 + \theta x_2, y)$,$\tilde{\pi}(y) := p(x_1 + \tilde{\theta} x_2, y)$ y beli $L(x_1, x_2$ feletti polinomokat.

4.1.4. Lemma. *π-nek nincsen gyöke $\tilde{\pi}$ egy felbontási testében.*

Bizonyítás. Legyen $t = x_1 + \theta x_2, \tilde{t} = x_1 + \tilde{\theta} x_2$. Ekkor $L(x_1, x_2 = L(t, \tilde{t})$, ezért t transzcendens $L(\tilde{t})$ felett. Tudjuk, hogy $\pi(y) = p(t, y) \in L[t, y]$. Legyen $h(y)$ egy irreducibilis osztója π-nek $\bar{L}(t)[y]$-ban. Ekkor $h(y)$ foka > 1 y-ban, mert $\pi(y)$-nak nincsen gyöke $\tilde{L}(t)$-ben azon feltevés szerint, hogy $p(x, y)$-nak nincs y beli gyöke $\bar{M}(x) = \bar{L}(x)$-ben.

Legyen $\tilde{F}$ egy felbontási teste $\tilde{\pi}(y)$-nak $\bar{L}(\tilde{t})$ felett. Mivel t transzcendens $\tilde{L}(\tilde{t})$ felett, ezért $\tilde{F}$ felett is, $h(y)$ irreducibilis $\tilde{F}(t)$ felett is 2.0.3 2 alapján. De $\tilde{F}(t)$ tartalmazza $\tilde{\pi}(y)$ minden $L(x_1, x_2)$ feletti gyökét és $L(x_1, x_2)$-t, tehát tartalmazza $\tilde{\pi}$ egy $\tilde{S}$ $L(x_1, x_2$ feletti felbontási testét. Tehát h-nak nincsen gyöke $\tilde{S}$-ben. De h egy tetszőleges osztója volt π-nek, ezért π-nek sincsen gyöke $\tilde{S}$-ben.

□

Legyen $\hat{M}$ N és L kompozit teste ($\bar{K}$-ban). Ekkor $\hat{M}$ egy Galois-bővítése K-nak

4.1.5. Lemma. *Ha F egy véges Galois-bővítése L-nek $\hat{M}$ − ben, akkor F Galois $\hat{K}$ felett.*

Bizonyítás. Létezik $\hat{K}$ egy véges Galois-bővítése N_0, ami N-beli és F $\hat{M}_0$-ban van, ami N_0 és L kompozit teste. Tudjuk, hogy $N_0 \cap L = \hat{K}$, ezért $Gal(\hat{M}_0/\hat{K}) = Gal(\hat{M}_0/L) \times Gal(\hat{M}_0/N_0$. Tehát minden normálosztó $Gal(\hat{M}_0/L)$-ban normálosztó $Gal(\hat{M}_0/\hat{K})$-ban is. □

4.1.6. Lemma. *Rendeljük $b_1, b_2 \in K$-hoz az alábbi $L[y]$ beli polinomokat: $\pi_{b_1,b_2}(y) := p(b_1 + \theta b_2, y)$ és $\tilde{\pi}_{b_1,b_2}(y) := p(b_1 + \tilde{\theta} b_2, y)$. Ha π_{b_1,b_2}-nek van gyöke $\hat{M}$-ben, akkor a gyök $\tilde{\pi}_{b_1,b_2}$ egy L feletti felbontási testében van.*

Bizonyítás. Legyen $F = L(\beta_1, ..., \beta_m)$, ahol a β_i-k π_{b_1,b_2} gyökei $\hat{M}$-ben. Ekkor F Galois L felett, tehát 4.1.5 miatt $\hat{K}$ felett is. Vagyis minden $\sigma \in Gal(L/\hat{K})$ kiterjed egy σ_F F-automorfizmussá. Létezik olyan σ, hogy $\sigma(\theta = \tilde{\theta}$. Ez a σ π_{b_1,b_2}-et $\tilde{\pi}_{b_1,b_2}$-be képezi, ezáltal $\tilde{\beta}_i = \sigma_F(\beta_i)$ a $\tilde{\pi}_{b_1,b_2}$ polinom gyökei L felett. □

4.1.1 és 4.1.4 alapján, létezik végtelen sok $b_1, b_2 \in K$, hogy π_{b_1,b_2}-nak nincsen egy gyöke sem M-ben (mivel $M \subset \hat{M}$). Tehát $b = b_1 + \theta b_2$ végtelen sok olyan $b \in M$ elemet ad, amire $p(b, y) = \pi_{b_1,b_2}(y)$-nak nincs egy gyöke sem M-ben. □

4.1.7. Megjegyzés. *A bizonyításból látszik, hogy a kívánt $b \in M$ elemek választhatók $K(\theta)$-ból, ahol θ egy tetszőleges generátora M-nek N felett. Tehát 2.1.3 (ii) és (iii) alapján tetszőleges $h(x, y) \in M[x][y]$-ra, ami irreducibilis $M(x)$ felett létezik végtelen sok $b \in K(\theta)$, hogy $h(b, y)$ irreducibilis $M[y]$-ban. Ugyanakkor, magában K-ban nem biztos hogy létezik ilyen b (lásd 5.1.3 példa).*

5. fejezet

Alkalmazások

5.1. Weissauer tételének alkalmazásai

Weissauer tétele segítségével $\bar{\mathbb{Q}}$ számos $\mathbb{Q}$ felett végtelen résztestéről belát-hatjuk, hogy Hilbert-féle, de a feltétel, hogy $M \neq N$ létfontosságú, azaz,$\mathbb{Q}$ nem minden Galois-bővítése Hilbert-féle. Egy triviális példa erre $\bar{\mathbb{Q}}$.

5.1.1. Tétel (Kronecker és Weber)**.** *$\mathbb{Q}_{ab}$ a test, amit akkor kapunk, ha $\mathbb{Q}$-t minden egységgyökkel bővítünk, a kompozitteste $\mathbb{Q}$ minden véges Abel-féle bővítésének(olyan bővítés, aminek a Galois-csoportja Abel csoport).*

5.1.2. Következmény. *$\mathbb{Q}_{ab}$ Hilbert-féle test.*

Bizonyítás. Legyen $K = \mathbb{Q}, N = \mathbb{Q}_{ab} \cap \mathbb{R}$ és $M = \mathbb{Q}_{ab}$. Tudjuk, hogy $M = N(i)$, mert $\mathbb{Q}_{ab}$ invariáns a komplex konjugáslásra, ezért minden $z = a + bi \in \mathbb{Q}_{ab}$-ra $a = 1/2(z + \bar{z}) \in N$ és hasonlóan $b \in N$. Tehát elegendő belátni, hogy N Galois $\mathbb{Q}$ felett. Elegendő belátni, hogy $\mathbb{Q}_n \cap \mathbb{R}$ Galois $\mathbb{Q}$ felett, ahol $\mathbb{Q}_n$ az n-edik egységyökkel vett bővítés. Ugyanakkor ismert, hogy $Gal(\mathbb{Q}_n/!)$ Abel-csoport, tehát minden $\mathbb{Q}$ és $\mathbb{Q}_n$ közötti test Galois $\mathbb{Q}$.

□

5.1.3. Példa. *Tekintsük az $f(x, y) = y^2 - x \in \mathbb{Q}[x, y]$ polinomot, ami irreducibilis $\bar{\mathbb{Q}}(x)$ felett.*

1. *Jelölje $\mathbb{Q}_{solv}$ $\mathbb{Q}$ összes véges feloldható bővítésének a kompozit testét. $\mathbb{Q}$ zárt a gyökvonásra, tehát $f(b, y)$ szorzattá bomlik minden $b \in \mathbb{Q}_{solv}$-re. Vagyis $\mathbb{Q}_{solv}$ nem Hilbert-féle test.*

2. *Kronecker és Weber tétele alapján minden racionális szám négyetgyöke megtalálható $\mathbb{Q}_{ab}$-ben, hiszen egy racionális szám gyökével való bővítés Abel-féle. Vagyis $f(b,y)$ szorzattá bomlik minden $b \in \mathbb{Q}$-ra. Tehát Weissauer tételében nem mindig lehet a kívánt $b \in M$-ket K-ból választani.*

5.1.4. Állítás. *Tegyük fel, hogy K Hilbert-féle test. Ha G fellép regulárisan K felett, akkor minden $m \geq 1$-hez $K(x_1, \ldots, x_m)$-nek, ami reguláris K felett, létezik egy Galois-bővítése, aminek a Galois-csoportja izomorf G-vel.*

Bizonyítás. 2.0.5 1 alapján m-et egyszerűen növelhetjük új változók hozzáadásával. Tehát elegendő azt belátni, hogy m csökkenthető.

Legyen $G = Gal(L/K(x))$, ahol L reguláris K felett, és $x = (x_1, \ldots, x_m)$. Írjuk L-et az alábbi alakba: $L = K(x)[y]/(f)$, ahol $f(x,y) \in K(x)[y]$. Ekkor f irreducibilis $\bar{K}(x)$ felett 2.0.5 2 alapján. Továbbá feltehetjük, hogy f normált y-ban, és $K[x][y]$-ban van.

Tegyük fel, hogy $m \geq 2$. Legyen $\kappa = K(x_1^2, x_2, \ldots, x_{m-1})$
(K helyett,mert az már foglalt), $N = \bar{K}(x_1^2, x_2, ..., x_{m-1})$, $M = \bar{K}(x_1, \ldots x_{m-1})$, mint Weissauer tételében. Ekkor $M = N(\theta)$, ahol $\theta = x_1$. Valamint κ Hilbert-féle 2.2.2 miatt. Továbbá 4.1.7 alapján, bármely $h(x_m, y) \in M[x_m][y]$ $M(x_m)$ felett irreducibilis polinomhoz létezik végtelen sok $b \in \kappa(\theta)$, hogy $h(b,y)$ irreducibilis M felett.

Legyen $K' = K(x_1, \ldots x_{m-1})$. Ekkor $K(x) = K'(x_m)$. Tehát $f \in K[x][y] = K'[x_m][y] \subset M[x_m][y]$. Tudjuk, hogy f irreducibilis $\bar{K}(x) = M(x_m)$ felett. Ezért az előző bekezdés értelmében, létezik végtelen sok $b \in \kappa(\theta) = K'$, amire $h_b(y) := f(x_1, \ldots, x_{m-1}, b, y)$ irreducibilis $M = \bar{K}(x_1, \ldots, x_{m-1})$ felett. Ekkor $L' := K'[y]/(h_b)$ egy véges bővítése K'-nek, és regulátis K felett 2.0.5 2 alapján. 2.1.3 (i) alapján L' Galois K' felett és $Gal(L'/K') = G$. Vagyis az állítás teljesül $m-1$-re is, így indukcióval bizonyítottuk az állítást. □

5.2. Elemi számelméleti alkalmazások

5.2.1. Állítás. *Legyen $g(x) \in \mathbb{Z}[x]$ és tegyök fel, hogy $g(x)$ négyzetszám véges sok kivétellel minden x racionális számra. Ekkor van olyan $f(x) \in \mathbb{Z}[x]$ polinom, amire $g(x) = f(x)^2$*

Bizonyítás. Tekintsük az alábbi $\mathbb{Q}[x,y]$ beli polinomot:

$$h(x,y) = y^2 - g(x)$$

Ha ez a polinom irreducibilis akkor Hilbert irreducibilitási tétele és alapján létezik végtelen sok $b \in \mathbb{Q}$, hogy $h(b,y) = y^2 - g(b)$ irreducibilis, de g majdnem minden b-re négyzetszám, vagyis $h(b,y) = y^2 - a^2 = (y-a)(y+a)$ majdnem minden $b \in \mathbb{Z}$-re.

Tehát h nem lehet irreducibilis, vagyis $h(x,y) = (y - f(x))(y - \tilde{f}(x))$ valamilyen $f(x), \tilde{f}(x) \in \mathbb{Q}[x]$-ekre. De

$$y^2 - g(x) = (y - f(x))(y - \tilde{f}(x)) = y^2 - (f(x) + \tilde{f}(x))y + f(x)\tilde{f}(x)$$

vagyis $f(x) = -\tilde{f}(x)$, tehát $g = f^2$, ekkor $f \in \mathbb{Z}[x]$, mivel $g \in \mathbb{Z}[x]$. □

5.2.2. Megjegyzés. *Az állítás akkor is igaz ha négyzet helyett tetszőleges n szerepel, illetve ha racionális helyett csak egész számokra követeljük meg, hogy $g(x)$ négyzetszám legyen. De az utóbbi állításhoz az irreducibilitási tétel egy erősebb verziója kell.*

Irodalomjegyzék

[1] Helmut Völklein. *Groups as Galois Groups: An Introduction*. Cambridge Studies in Advanced Mathematics. Press Syndicate of the University of Cambridge, 1996.

[2] Nathan Jacobson. *Basic algebra I*. W. H. Freeman, 1974. chapter 4.

[3] Zábrádi Gergely. K-homomorfizmusok, szeparábilis bővítések, galois-elmélet. https://zabradi.web.elte.hu/Jegyzetek/szeparabilis.pdf.

[4] Kiss Emil. *Bevezetés az algebrába*. Typotex, 2007.

[5] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. Springer, 1986.