Eötvös Loránd Tudományegyetem
Természettudományi Kar

Az inverz Galois probléma

Andó Szabolcs

Témavezető:
Zábrádi Gergely, egyetemi docens

Bsc Szakdolgozat
Algebra és Számelmélet tanszék

Budapest, 2020

NYILATKOZAT

Név: ANDÓ SZABOLCS
ELTE Természettudományi Kar, szak: matematika Bsc
NEPTUN azonosító: GGWQX7
Szakdolgozat címe: Az inverz Galois probléma

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, 2020. május 22.

Andó Szabolcs

a hallgató aláírása

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőmnek, Zábrádi Gergelynek a sok hasznos segítségért és iránymutatásért, illetve azért, hogy négy félév alatt megszerettette velem az algebrát. Szeretném továbbá megköszönni a családomnak, hogy támogattak egyetemi éveim során, külön köszönöm Dórinak, hogy mindvégig tartotta bennem a lelket. Nélkülük nem jöhetett volna létre ez a dolgozat.

Bevezetés

Az inverz Galois probléma az algebra, illetve az algebrai számelmélet egyik legnehezebb, máig megoldatlan problémája. A kérdés legegyszerűbb megfogalmazása, hogy minden véges csoport előáll-e, mint $\mathbb{Q}$, vagyis a racionális számok testének valamely Galois-bővítésének Galois-csoportja. A kérdést természetesen nemcsak $\mathbb{Q}$, de tetszőleges rögzített K testre lehet vizsgálni, és vannak esetek, melyekben tudjuk a választ, ezek közé tartozik $\mathbb{C}(x)$, vagyis a komplex számtest feletti racionális törtfüggvények teste, amely felett a válasz a fenti kérdésre igenlő. Ez Riemann egzisztenciatételének következménye.

Annak ellenére, hogy a probléma máig megoldatlan, számos fontos részeredmény ismert. Az első nagy áttörés Hilbert nevéhez fűződik, ő volt az, aki először tanulmányozta a kérdést. A [11] cikkben leírt, ma Hilbert irreducibilitási tétele néven ismert tétel biztosítja, hogy a problémában $\mathbb{Q}$ lecserélhető $\mathbb{Q}(x)$-re, vagyis a $\mathbb{Q}$ feletti racionális törtfüggvények testére olyan értelemben, hogy ha egy G véges előáll, mint egy $L_1/\mathbb{Q}(x)$ Galois-bővítés Galois-csoportja, akkor van olyan $L_2/\mathbb{Q}$ Galois-bővítés is, amelynek Galois-csoportja G.

Azt már nagyon régen tudták, hogy minden Abel csoport előáll $\mathbb{Q}$ feletti Galois-bővítés Galois-csoportjaként. Ennél azonban több is igaz: Hilbert után következő nagy áttörést Šafarevič érte el, ő megmutatta, hogy minden feloldható csoportra is igaz az inverz Galois probléma állítása. Ennek bizonyítása megtalálható a [15] cikkben.

Šhafarevič tétele mellett a másik legfontosabb eredmény Shih (illetve Thompson, Fried, Belyi és Matzat) nevéhez fűződik [17], aki bevezette a merevségi feltételt, amely egy tisztán csoportelméleti kritérium arra, hogy egy csoport előálljon $\mathbb{Q}$ felett. Ez áll rengeteg mai nagy részeredmény mögött. Egy fontos példa erre Thompsonhoz köthető [18], ő volt az, aki előállította a Monster (Szörnyeteg) csoportot Galois-csoportként $\mathbb{Q}$ felett.

A szakdolgozat fő célja a merevség megismerése és alkalmazása. A munka nagy része Helmut Völklein Groups as Galois Groups: An introduction című [19] könyvét követi (a bevezetés egy része is). Ez alól kivétel az első fejezet, melyben bevezetésként megnézünk két példát csoportokra, melyeket közvetlenül elő tudunk állítani $\mathbb{Q}$ Galois-bővítéseinek csoportjaiként, ennek 1.1 része Serge Lang Algebra című könyvének [14] 273. oldalának 6. példája alapján készült, az 1.2 pedig az 1.2.3 következményig bezárólag Zábrádi Gergely Tanár Úr előadásaiból született, az 1.2.5 tétel bizonyításának alapötletének forrása pedig [8]. A 2. szakasz célja az $L/K(x)$ alakú bővítések megismerése, ahol K algebrailag zárt. Ezek elágazási típusának megismerése fontos eszköz, hiszen $\mathbb{Q}$ beágyazható algebrailag zárt $K \subseteq \mathbb{C}$ testekbe, és $K(x)$ bővítéseinek csoportjai bizonyos feltételek mellett realizálhatóak $\mathbb{Q}(x)$ felett is. Az említett fejezet 2.1 és 2.2 alfejezete, továbbá a 4.1 a Völklein-könyv 2. fejezetét dolgozza fel, az eredmények (Puiseux tételének kivételével) megtalálhatóak benne. A 2.3 rész egy példát dolgoz ki a fejezet korábbi részeinek megértéséhez, ez a fent említett könyvben egy feladatként van megfogalmazva. A 3. fejezet Riemann egzisztenciatételét járja körbe, mely elengedhetetlen a merevség használatához. Ebben a 3.1, 3.3, és 3.4 Völklein könyvének 5. fejezetét követi (bizonyos kivételektől eltekintve, amelyek jelezve vannak), míg a 3.2-ben a 4. fejezet összefoglalása található. A 4. fejezetben a 4.2 rész Hilbert irreducibilitási tételéről szól, ebben le van írva a merevséghez szükséges rész Völklein könyvének 1. fejezetéből. A 4.3 szakaszban megismerjük annak a feltételeit, hogy egy $\mathbb{Q} \leq K$ algebrailag zárt test esetén egy $L/K(x)$ alakú bővítés csoportja mikor állítható elő $\mathbb{Q}$ felett is, a 4.4-ben pedig kimondjuk a merevségi tételt és egy alkalmazását. Az említett két alfejezet Völklein könyvében a 3. fejezet elejét dolgozza fel.

A szakdolgozatban implicit módon fel van téve a Galois-elmélet [6], illetve ennél tágabban az absztrakt algebra [2] alapszintű ismerete, és a fenti olvasmányokban leírt definíciókat hivatkozás nélkül használjuk, azonban az állításokra általában hivatkozunk. Ez alól kivételt képez a nagyon sokszor használt Galois-elmélet főtétele. Amennyiben azt használjuk, akkor mindig a [6] 2.12 tételt értjük alatta. Ha L/K egy véges testbővítés, akkor $\mathrm{Gal}(L/K)$-val jelöljük a relatív automorfizmusok csoportját (azaz L-nek a K-t fixen hagyó automorfizmusainak csoportját) függetlenül attól, hogy L/K Galois-e vagy sem. Végtelen testbővítések esetén az $\mathrm{Aut}(L/K)$ jelölést használjuk (ez alól van egy kivétel, lásd 4.3.6). A 3. fejezet megértése igényel némi topológiai tudást a fedőterekről ([1] 7.3 fejezet) és alapvető komplex függvénytani ismereteket [3].

A [19] könyv melletti döntésnek az az oka, hogy egyrészt nagyon alapos bevezetést ad a matematika itt vizsgált területébe, másrészt a témában megszületett más könyvek (lásd [9] és [16]) többnyire messze meghaladják a Bsc ismeretanyagának szintjét, azonban az említett olvasmányok mélyebb betekintést adhatnak a témába.

Tartalomjegyzék

1. Példák csoportok előállítására

Ebben a fejezetben néhány egyszerű példát nézünk bizonyos csoportokra, és ezeket közvetlenül állítjuk elő Galois-csoportként $\mathbb{Q}$ felett.

1.1. A p-edik szimmetrikus csoport, ahol p prím

Elsőként az S_p csoportot nézzük meg, ahol S_p a p-edik szimmetrikus csoport, és p prím. Később a merevség alkalmazásával minden szimmetrikus csoportot elő tudunk majd állítani Galois-csoportként $\mathbb{Q}$ felett, azonban ezt az esetet közvetlenül is meg tudjuk nézni. Szükségünk lesz egy egyszerű lemmára a szimmetrikus csoportok generálásával kapcsolatban. Úgy fogunk az S_p csoportra hivatkozni, mint az $\{1, 2, ..., p\}$ halmaz permutációinak csoportjára.

1.1.1. Lemma. Legyen $n \geq 2$ pozitív szám, és (i, j) transzpozíció S_n-ben a következő tulajdonsággal: ha $a \equiv j - i \pmod{n}$ és $1 \leq a \leq n$, akkor a és n relatív prímek. Ekkor az S_n csoportot generálja a $\sigma = (1, 2, 3, ..., n)$ ciklus és a $\tau = (i, j)$ transzpozíció.

Bizonyítás. Jelöljük a σ és τ által generált részcsoportot H-val. Feltehető, hogy $i < j$. Ekkor $a = j - i$. Az $(1, a + 1) = \sigma^{-i}\tau\sigma^i$, hiszen transzpozíció konjugáltja transzpozíció, és $\sigma^{-i}\tau\sigma^i(1) = a + 1$. Emiatt az $(1, a + 1) \in H$. Ha m pozitív egész, akkor m-re indukcióval belátom, hogy ha $k = am$ (modulo n értve a szorzást), akkor az $(1, k + 1) \in H$. Beláttuk $m = 1$-re, tehát tegyük fel, hogy $m = r$-ig is tudjuk, és tekintsük az $m = r + 1$-et. Ekkor, ha $s_1 = ra+1$, és $s_2 = (r+1)a+1$, akkor előállítjuk az (s_1, s_2) transzpozíciót: $\sigma^{ra}(1, a+1)\sigma^{-ra} = (s_1, s_2)$, hiszen könnyen láthatóan s_1-et s_2-be viszi, hiszen a-val eltolja. Emiatt $(s_1, s_2) \in H$, az indukciós feltevésből $(1, s_1) \in H$, vagyis $(1, s_1)(s_1, s_2)(1, s_1) = (1, s_2) \in H$, amivel az indukció teljes.

Ebből következik, hogy minden $k \leq p$ pozitív egészre az $(1, k) \in H$, hiszen n és a relatív prímek, ami miatt valamely m pozitív egészre $am \equiv k - 1 \pmod{n}$. Ekkor pedig bármely $1 \leq l_1, l_2 \leq n$ egészre $(1, l_1)(1, l_2)(1, l_1) = (l_1, l_2)$, vagyis H tartalmazza az összes transzpozíciót. Triviális, hogy összes transzpozíció generálja S_n-et (ez a [2] 4.2.5 Kérdés után le van írva, de könnyű meggondolni), tehát $H = S_n$, vagyis készen vagyunk. □

1.1.2. Állítás. Legyen $f(x) \in \mathbb{Q}[x]$ irreducibilis polinom, melynek foka p prím. Ha f-nek $\mathbb{C}$ felett pontosan 2 nem valós gyöke van, akkor f felbontási testének Galois-csoportja $\mathbb{Q}$ felett S_p.

Bizonyítás. Legyen K a felbontási teste f-nek, és $G = \mathrm{Gal}(K/\mathbb{Q})$. Ha G-t úgy tekintjük S_p részcsoportjának, hogy az f gyökein ható csoportként értelmezzük, akkor G-ben a [2] 6.4.12 Következmény miatt f-nek minden gyöke azonos pályán van. Ekkor a pálya-stabilizátor lemma ([2] 4.5.8 Tétel) miatt $|G|$-t osztja ezen pálya elemszáma, vagyis p. Ekkor Cauchy tétele ([2] 4.11.19 Következmény) miatt van p-edrendű elem G-ben. Ez az elem permutációnként értelmezve felírható diszjunkt ciklusok szorzataként ([2] 4.2.21 Tétel) és rendje a ciklusok hosszainak legkisebb közös többszöröse, tehát mivel p prím, van a ciklusok között p hosszúságú, vagyis egy darab p hosszú ciklusról van szó. A gyökök megfelelő címkézése után feltehető, hogy ez az $(1, 2, 3, ..., p)$ ciklus. A K beágyazható $\mathbb{C}$-be, tehát tekintsük K-t ennek résztesteként. A komplex konjugálás egy automorfizmusa $\mathbb{C}$-nek, tehát megszorítása K-ra szintén automorfizmus, ráadásul olyan, amely $\mathbb{Q}$-t helyben hagyja. Ezért ez benne van G-ben, és a gyökökön egy transzpozíció, hiszen a két komplex gyököt megcseréli, és a többi

gyököt helyben hagyja (hiszen azok valósak). Innen az 1.1.1 lemmából készen vagyunk, hiszen p prím, tehát ha az adott transzpozíció (i, j), akkor a $j - i = a$ (feltéve, hogy $j > i$) mindig relatív prím p-hez. □

1.1.3. Állítás. Minden p prímre létezik olyan $f(x) \in \mathbb{Q}[x]$ p-edfokú polinom, amely irreducibilis, és gyökei között pontosan 2 nem valós van (ha $\mathbb{C}$-beli gyökeit tekintjük).

Bizonyítás. Vegyünk $b_1, ..., b_{p-2}$ véges sok különböző egész számot, továbbá egy a pozitív egész számot. Tekintsük a

$$g(x) = (x^2 + a)(x - b_1)(x - b_2)...(x - b_{p-2}) = x^p + c_{p-1}x^{p-1} + ... + c_0$$

p-edfokú polinomot. Ezek után vegyünk egy q prímszámot, és tekintsük a $g_n(x) = g(x) + \frac{q}{q^{np}}$ polinomokat $n = 1, 2, ...$ esetén. Belátjuk, hogy ez minden n-re irreducibilis. Ehhez a polinom q-hoz tartozó Newton-poligonját ([7] 3. Definíció) hívjuk segítségül. A rácspontok, amelyeket tekintünk, $1 < i < p$-re $(-i, j)$ alakúak, ahol $j \geq 0$, hiszen ez esetben c_i a megfelelő együtthatója g_n-nek is, ami egész. A maradék két rácsopont közül az egyik a $(-p, 0)$, a másik a $(0, v_q(c_0 + \frac{q}{q^{np}}))$. Ekkor

$$v_q\left(c_0 + \frac{q}{q^{np}}\right) = v_q(q^{-np+1}(c_0 q^{np-1} + 1)) = -np + 1,$$

hiszen $c_0 q^{np-1} + 1$ nem osztható q-val. Tehát a két szélső rácspont a $(-p, 0)$ és a $(0, -np+1)$, és az ezeket összekötő szakasz az $x = -p$-nél nagyobb koordinátákra szigorúan az $y = 0$ egyenes alatt helyezkedik el. Mivel az összes többi rácspont y koordinátája legalább 0, ezért az említett összekötő szakasz lesz a Newton-poligon, továbbá ezen nem lesz más rácspont a két szélsőn kívül (hiszen p és $-np + 1$ relatív prímek), ami a [7] 8. következmény miatt azt jelenti, hogy $g_n(x)$ irreducibilis.

Végezetül belátjuk, hogy elég nagy n esetén $g_n(x)$ komplex gyökei közül pontosan 2 nem lesz valós. Nevezzük el $i\sqrt{a}$-t b_{p-1}-nek, és $-i\sqrt{a}$-t b_p-nek. Ekkor a $g(x)$ polinom gyökeinek halmaza a $B = \{b_i : 1 \leq i \leq p\}$. Vegyünk egy olyan $\varepsilon > 0$ értéket, amelyre ezen gyökök ε sugarú környezete diszjunkt ($\mathbb{C}$-ben), ekkor világos, hogy a nem valós gyökök ε sugarú környezete diszjunkt a valós tengelytől. Tekintsük a B halmaz minden b_i elemére azt a γ_i Jordan-görbét, amely pozitív irányítás szerint végigmegy a b_i pont ε sugarú környezetének határán. A Rouché-tétel ([3] 41. oldal) szerint ha

$$|g(x) - g_n(x)| < |g(x)| \ \forall x \in \gamma_i,$$

akkor $g_n(x)$-nek és $g(x)$-nek ugyanannyi gyöke van γ_i belsejében. Legyen

$$\delta := \min\{|g(x)| : \exists i x \in \gamma_i\}.$$

Ez a minimum a Weierstrass tétel alapján létezik, hiszen egy kompakt halmazon nézzük, és pozitív, hiszen a megadott halmazon sehol sem vesz fel 0-t $g(x)$. Vegyünk egy olyan N értéket, amelyre $\frac{q}{q^{Np}} < \delta$. Ekkor minden $n \geq N$ számra $|g(x) - g_n(x)| = \frac{q}{q^{np}} < \delta \leq |g(x)|$, ha $x \in \gamma_i$, tehát a Rouché tétel szerint $g_n(x)$-nek minden b_i ε sugarú környezetében van gyöke. Mivel multiplicitással számolva pontosan n gyöke van, ezért meg is van minden gyöke. Azok a gyökök, amelyek a valós b_i-k környezetéből kerülnek ki, valósak, hiszen ha

nem azok lennének, akkor a konjugáltjuk is gyök lenne, márpedig a b_i környezetében $g_n(x)$-nek csak 1 gyöke van. Azon gyökök, amelyek a nem valós gyökök környezetében vannak, nem lehetnek valósak, hiszen a megadott környezetek diszjunktak a valós tengelytől. Megkaptuk tehát, hogy ha $n > N$, akkor $g_n(x)$-nek pontosan 2 nem valós gyöke van. □

1.1.4. Következmény. Ha p prím, akkor S_p előáll, mint $\mathbb{Q}$ egy Galois-bővítésének Galois-csoportja.

Bizonyítás. Valóban, az 1.1.3 állításban leírt polinom felbontási teste az 1.1.2 állítás alapján megfelelő lesz. □

1.2. Abel-csoportok

1.2.1. Definíció (Körosztási test)**.** Legyen K test, $\mathrm{char}K = 0$ és $N \geq 1$ egész szám. Legyen továbbá

$$\mu_n := \{x^n - 1 \text{ polinom gyökei}\}.$$

Ekkor a $K(\mu_n)$-et a K feletti n-edik körosztási testnek nevezzük. A [6] 2.9 következménye miatt $K(\mu_n)/K$ Galois.

1.2.2. Állítás. Legyen $\varepsilon \in K(\mu_n)$ primitív n-edik egységgyök. Ekkor, amennyiben $\tau \in \mathrm{Gal}(K(\mu_n)/K)$, akkor van olyan j, amelyre $(j, n) = 1$ és $\tau(\varepsilon) = \varepsilon^j$, továbbá a

$$\mathrm{Gal}(K(\mu_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \tau \mapsto j \pmod n,$$

ahol $(\mathbb{Z}/n\mathbb{Z})^\times$ az n-nél kisebb, n-hez relatív prím pozitív egészek csoportja a modulo n szorzásra, injektív csoporthomomorfizmus.

Bizonyítás. Legyen $\Phi_n(x)$ az n-edik körosztási polinom. Ennek ε gyöke, tehát $\tau(\varepsilon)$ is gyöke. Ebből következik, hogy $\tau(\varepsilon)$ is primitív n-edik egységgyök, emiatt $\tau(\varepsilon) = \varepsilon^j$ alkalmas j pozitív egészre, melyre $(n, j) = 1$. Ebből következik, hogy $j \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Belátjuk, hogy homomorfizmus. Legyen $\sigma, \tau \in \mathrm{Gal}(K(\mu_n)/K)$, és $\tau(\varepsilon) = \varepsilon^j$, illetve $\sigma(\varepsilon) = \varepsilon^k$. Ekkor $\sigma \circ \tau(\varepsilon) = \sigma(\varepsilon^j) = \sigma(\varepsilon)^j = \varepsilon^{kj}$, tehát $\sigma \circ \tau \mapsto kj$, vagyis valóban homomorfizmus. Már csak az hiányzik, hogy injektív. Ehhez azt kell belátni, hogy a magja triviális, vagyis ha $\tau \neq \mathrm{id}$, akkor $\tau(\varepsilon) \neq \varepsilon$. Ez nyilvánvaló, hiszen $K(\mu_n) = K(\varepsilon)$. □

1.2.3. Következmény. $K = \mathbb{Q}$ esetén $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ a fenti izomorfizmussal.

Bizonyítás. A $\mathbb{Q}(\mu_n)/\mathbb{Q}$ bővítés a $\Phi_n(x)$ irreducibilis polinom felbontási teste, tehát $|\mathbb{Q}(\mu_n) : \mathbb{Q}| = \varphi(n)$ (itt $\varphi(n)$ az Euler-függvény), és mivel a bővítés Galois, ezért $|\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, tehát az 1.2.2 állításbeli injekció a rendek egyenlősége miatt izomorfizmus a két csoport között. □

Ahhoz, hogy minden Abel-csoportot elő tudjunk állítani, mint $\mathbb{Q}$ egy véges Galois-bővítésének csoportját, szükség lesz a számelméletből Dirichlet tételére.

1.2.4. Tétel (Dirichlet)**.** Ha egy számtani sorozat első eleme a, és differenciája d, továbbá $(a, d) = 1$, akkor a számtani sorozatban végtelen sok prímszám van.

1.2.5. Tétel. Legyen G véges Abel-csoport. Ekkor létezik $\mathbb{Q}$-nak olyan $L/\mathbb{Q}$ Galois-bővítése, melynek Galois-csoportja $\mathrm{Gal}(L/\mathbb{Q}) \cong G$.

Bizonyítás. A véges Abel-csoportok alaptétele ([2] 4.9.15 Tétel) miatt G felbontható prímhatványrendű ciklikus csoportok direkt szorzatára: $G \cong Z_{p_1} \times ... \times Z_{p_i}$, ahol $p_1, ..., p_i$ (nem feltétlenül különböző) prímhatványok, és a Z_{p_i} a p_i-rendű ciklikus csoport. Első lépésként minden p_j számhoz hozzárendelünk egy-egy q_j prímet úgy, hogy $q_j \equiv 1 \pmod{p_j}$, és a q_j-k mind különbözőek legyenek. Ezt Dirichlet tételével (1.2.4 Tétel) hajtjuk végre. Vegyük a $p_1 + 1$ kezdő elemű, p_1 differenciájú számtani sorozatot. Ebben a Dirichlet tétel szerint van prím. Legyen ez q_1. Világos, hogy ez megfelelő. Ezután indukcióval definiálom a többit. Tegyük fel, hogy q_k-ig már definiáltuk, és definiálni akarjuk q_{k+1}-et. Vegyük a $p_{k+1} + 1$ kezdetű, p_{k+1} differenciájú számtani sorozatot. Ebben Dirichlet tétele szerint végtelensok prímszám van, tehát van benne olyan, amit még nem használtunk egyik q_j-re sem korábban. Válasszuk ezt q_{k+1}-nek. Látható, hogy ezzel a módszerrel célba érünk.

A $\mathrm{Gal}(\mathbb{Q}(\mu_{q_j})/\mathbb{Q})$ Galois csoport izomorf a $q_j - 1$ rendű ciklikus csoporttal az 1.2.3 következmény miatt, hiszen $(\mathbb{Z}/q_j\mathbb{Z})^\times \cong Z_{q_j-1}$, mivel q_j prím. Tegyük fel, hogy $q_j - 1 = np_j$. Ekkor Z_n beágyazható $\mathrm{Gal}(\mathbb{Q}(\mu_{q_j})/\mathbb{Q})$ ba, hiszen beágyazható Z_{q_j-1}-be. A Galois-elmélet főtételében a Z_n-nek megfelelő közbülső test legyen K_j. Belátjuk, hogy $K_j/\mathbb{Q}$ Galois. A $\mathbb{Q}(\mu_{q_j})/K_j$ bővítés a főtétel alapján Galois, és a $H_1 := \mathrm{Gal}(\mathbb{Q}(\mu_{q_j})/K_j)$ csoportjának fixteste pontosan K_j. Ha veszünk egy $\sigma \in H_2 := \mathrm{Gal}(\mathbb{Q}(\mu_{q_j})/\mathbb{Q})$ automorfizmust, akkor $\sigma(K_j)$ pontosan a $\sigma H_1 \sigma^{-1}$ részcsoport fixteste lesz, hiszen ha $g \in H_2$, és $\alpha \in K_j$, akkor $g\sigma(\alpha) = \sigma(\alpha) \Leftrightarrow \sigma^{-1}g\sigma(\alpha) = \alpha \Leftrightarrow \sigma^{-1}g\sigma \in H_1 \Leftrightarrow g \in \sigma H_1 \sigma^{-1}$. Megvan tehát, hogy $\sigma(K_j)$ a $\sigma H_1 \sigma^{-1}$ részcsoport fixteste, azonban Abel csoportban vagyunk, tehát $\sigma H_1 \sigma^{-1} = H_1$, emiatt $\sigma(K_j) = K_j$, vagyis minden $\sigma \in H_2$ fixen hagyja K_j-t. $K_j/\mathbb{Q}$ egyszerű bővítés ([6] 1.15 Tétel), tehát $K_j = \mathbb{Q}(\beta)$, és β minimálpolinomjának minden gyöke $\mathbb{Q}(\mu_{q_j})$-ben van (hiszen az Galois), és mivel ennek a testnek minden $\mathbb{Q}$-automorfizmusa fixen hagyja K_j-t, ezért ezen gyökök mind K_j-ben vannak, tehát $K_j/\mathbb{Q}$ valóban Galois ([6] 2.5 Állítás $(iv) \Rightarrow (i)$). Ekkor a $H_2 \to \mathrm{Gal}(K_j/\mathbb{Q})$ megszorítás magja pontosan H_1, tehát a homomorfizmustétel ([2] 4.7.16 Tétel) miatt a képe izomorf a H_2/H_1 faktorcsoporttal. A Galois-elmélet főtételének második állítása szerint $|K_j : \mathbb{Q}| = |Z_{q_j-1} : Z_n| = p_j$, tehát $\mathrm{Gal}(K_j/\mathbb{Q})$ és H_2/H_1 rendje megegyezik, így a fenti megszorítás szürjektív, vagyis $\mathrm{Gal}(K_j/\mathbb{Q}) \cong H_2/H_1$, azaz ciklikus. Mivel láttuk, hogy rendje p_j, ezért $\mathrm{Gal}(K_j/\mathbb{Q}) \cong Z_{p_j}$.

Legyen $r = \prod_{j=1}^{i} q_j$, és tekintsük a $\mathbb{Q}(\mu_r)/\mathbb{Q}$ bővítést. Világos, hogy $\mathbb{Q}(\mu_r)$-be beágyazható minden $\mathbb{Q}(\mu_{q_j})$. A fokszámtételből egyszerűen következik (lásd [20] 3.5 lemma, 13. oldal), hogy ha $j_1 \neq j_2$, akkor

$$\mathbb{Q}(\mu_{q_{j_1}}) \cap \mathbb{Q}(\mu_{q_{j_2}}) = \mathbb{Q}. \tag{1}$$

Ezzel az is világos, hogy minden $j = 1, ..., i$-re $K_j \leq \mathbb{Q}(\mu_r)$, és bármely kettő különböző K_j metszete $\mathbb{Q}$. Legyen $L := \mathbb{Q}(K_1 \cup ... \cup K_i)$. Azt állítjuk, hogy $L/\mathbb{Q}$ Galois. Vegyük fel $\mathbb{Q}$-nak a $\bar{\mathbb{Q}}$ algebrai lezárását úgy, hogy $\mathbb{Q}(\mu_r) \leq \bar{\mathbb{Q}}$. Ekkor, ha veszünk egy $\tau : L \hookrightarrow \bar{\mathbb{Q}}$ beágyazást, akkor $\tau(L) = L$, mert a [6] 2.5 állításának $(i) \Rightarrow (ii)$ iránya miatt $\tau(K_j) = K_j$ minden $j = 1, ..., i$-re, és ezek generálják L-et. Ekkor ugyanazon állítás $(ii) \Rightarrow (i)$ iránya miatt $L/\mathbb{Q}$ Galois.

Már csak az hiányzik, hogy $\mathrm{Gal}(L/\mathbb{Q}) \cong G$. Ezt i-re indukcióval látjuk be. Mivel $i = 1$-re triviális, tegyük fel, hogy $i = k$-ig beláttuk, és legyen $i = k+1$. Legyen $\mathbb{Q}(K_1 \cup ... \cup K_k) = L'$. Az indukciós feltevés szerint $\mathrm{Gal}(L'/\mathbb{Q}) \cong Z_{p_1} \times ... \times Z_{p_k}$, és $\mathrm{Gal}(K_{k+1}/\mathbb{Q}) \cong Z_{p_{k+1}}$. Mivel az Euler függvény gyengén multiplikatív, ezért $|\mathrm{Gal}(\mathbb{Q}(\mu_{\frac{r}{q_{k+1}}})/\mathbb{Q})| \cdot |\mathrm{Gal}(\mathbb{Q}(\mu_{q_{k+1}})/\mathbb{Q})| = \varphi(\frac{r}{q_{k+1}})\varphi(q_{k+1}) = \varphi(r) = |\mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})|$, tehát bijekció van a $(g_1, g_2) \in \mathrm{Gal}(\mathbb{Q}(\mu_{\frac{r}{q_{k+1}}})/\mathbb{Q}) \times$

$\mathrm{Gal}(\mathbb{Q}(\mu_{q_{k+1}})/\mathbb{Q})$ párok és a $g \in \mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})$ elemek között, méghozzá a következő módon:

$$g \mapsto \left(g|_{\mathbb{Q}(\mu_{\frac{r}{q_{k+1}}})}, g|_{\mathbb{Q}(\mu_{q_{k+1}})} \right).$$

Ez azt jelenti speciálisan, hogy mivel $K_{k+1} \leq \mathbb{Q}(\mu_{k+1})$, és $L' \leq \mathbb{Q}(\mu_{\frac{r}{q_{k+1}}})$, ezért minden $g \in \mathrm{Gal}(K_{k+1}/\mathbb{Q})$ elem egyértelműen terjeszthető ki L-re úgy, hogy L'-n az identitást kapjuk (ez azon múlik, hogy g kiterjeszthető $\mathbb{Q}(\mu_{q_{k+1}})$-re, lásd 4.3.7 tétel). Ez azt jelenti, hogy $\mathrm{Gal}(L/L') \cong \mathrm{Gal}(K_{k+1}/\mathbb{Q}) \cong Z_{p_{k+1}}$. Pontosan ugyanígy az is teljesül, hogy $\mathrm{Gal}(L/K_{k+1}) \cong \mathrm{Gal}(L'/\mathbb{Q}) \cong Z_{p_1} \times ... \times Z_{p_k}$.

Mivel $K_{k+1} \cap L' = \mathbb{Q}$, ezért a $\mathrm{Gal}(L/K_{k+1})$ és $\mathrm{Gal}(L/L')$ által generált részcsoport fixteste $\mathbb{Q}$, vagyis ők ketten generálják $\mathrm{Gal}(L/\mathbb{Q})$-t. Mivel fixtesteik generálják L-et, ezért $\mathrm{Gal}(L/K_{k+1}) \cap \mathrm{Gal}(L/L') = \{1\}$. A $\mathrm{Gal}(L/\mathbb{Q})$ csoport Abel, hiszen ha veszünk belőle két $g_1, g_2 \in \mathrm{Gal}(L/\mathbb{Q})$ elemet, akkor $g_1 g_2$ megegyezik $g_2 g_1$-gyel minden K_j-re megszorítva (hiszen $\mathrm{Gal}(K_j/\mathbb{Q})$ Abel), tehát megegyeznek az egész L-en. Abel csoportban minden részcsoport normálosztó, tehát ebből a [2] 4.9.12 tétel alapján

$$\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(L/K_{k+1}) \times \mathrm{Gal}(L/L'),$$

vagyis $\mathrm{Gal}(L/\mathbb{Q}) \cong Z_{p_1} \times ... \times Z_{p_k} \times Z_{p_{k+1}}$. Innen az indukcióból készen vagyunk. □

Ezzel beláttuk, hogy minden véges Abel csoportra van Galois-bővítés azzal a csoporttal. Sőt, minden ilyet egy körosztási testbe beágyazva hoztunk létre. Ezt lehet erősíteni is.

1.2.6. Tétel (Kronecker-Weber)**.** Legyen $L/\mathbb{Q}$ tetszőleges véges Galois-bővítés, melynek Galois-csoportja Abel. Ekkor L beágyazható egy körosztási testbe, vagyis valamely n pozitív egészre $L \leq \mathbb{Q}(\mu_n)$.

Bizonyítás. A bizonyítás megtalálható a [5] jegyzetben (5.2.1 Tétel). □

2. Algebrailag zárt testek

Ebben a fejezetben $L/K(x)$ alakú testbővítésekről lesz szó, ahol K algebrailag zárt. A fejezet célja az, hogy definiáljuk egy ilyen bővítés elágazási típusát. Ez egy fontos eszköz lesz a későbbiekben.

2.1. Formális Laurent-sorok teste

A szakdolgozat során sokszor szükség lesz arra, hogy bizonyos testbővítésekről belássuk, hogy Galois-bővítések. Erre az egyik legjobb módszert az alábbi fontos tétel szolgáltatja.

2.1.1. Tétel (Artin tétele)**.** Legyen K egy test, $\mathrm{char}K = 0$, és $G \leq \mathrm{Aut}(K)$ véges csoport. Ha $F \leq K$ a fixteste G-nek, akkor K/F Galois és Galois-csoportja $\mathrm{Gal}(K/F) = G$.

Artin tétele nem csak 0 karakterisztikában teljesül, nekünk azonban csak erre a speciális esetre lesz szükségünk; mivel 0 karakterisztikában minden bővítés szeparábilis és minden véges szeparábilis bővítés egyszerű ([6] 1.15 Tétel), ezért a tétel következik [6] 2.11 (ii) állításából.

2.1.2. Definíció (Formális Laurent-sorok teste K fölött)**.** Legyen K egy test. Legyen Λ azon $(a_i)_{i\in\mathbb{Z}}$ alakú sorozatok halmaza, ahol $a_i \in K\ \forall i \in \mathbb{Z}$, és $\exists N \in \mathbb{Z}$, hogy $a_i = 0\ \forall i < N$. Az összeadást az $(a_i) + (b_i) = (a_i + b_i)$, a szorzást pedig az $(a_i) \cdot (b_i) = (c_i)$ összefüggésekkel definiáljuk, ahol $c_i = \sum_{j+k=i} a_j b_k$. Ez az összeg nyilván véges. Λ-t ezzel a két művelettel a K fölötti formális Laurent-sorok testének nevezzük és $K((t))$-vel jelöljük, abban az értelemben, hogy $(a_i) = \sum_{i=N}^{\infty} a_i t^i$. Ennek a $\sum_{i=0}^{\infty} a_i t^i$ alakú elemekből álló részgyűrűjét (vagyis azon elemeket, ahol N nemnegatív) a K fölötti formális hatványsorgyűrűnek nevezzük és $K[[t]]$-vel jelöljük.

2.1.3. Állítás. A formális Laurent-sorok teste valóban test.

Bizonyítás. Triviális, hogy összeadásra Abel-csoportot alkot. A szorzás kommutativitása a definíció szimmetrikus voltából következik. Az egységelem az az (e_i) sorozat lesz, amelyre $e_0 = 1$, és $e_i = 0\ \forall i \neq 0$. Világos, hogy ez valóban egység. Elég megmutatni, hogy minden nemnulla elemnek van inverze erre az egységelemre nézve. Egy adott (a_i) sorozatra definiáljuk a következő (b_i) sorozatot: legyen $N \in \mathbb{Z}$ az a szám, melyre $a_i = 0\ \forall i < N$, de $a_N \neq 0$. Legyen $b_j = 0\ \forall j < -N$, és $b_{-N} = a_N^{-1}$. A többi j-re a következő egyenletrendszerből kapjuk meg b_j-t:

$$\sum_{j+k=i} a_k b_j = 0, i = 1, 2, ...$$

Ez induktívan megoldható b_j-re, méghozzá $j = -N + 1$-től az indexek szerint növekvő sorrendben. Ez a (b_i) sorozat valóban (a_i) inverze, amivel beláttuk, hogy $K((t))$ test. □

2.1.4. Megjegyzés. A formális hatványsorgyűrű nyilván részgyűrűje $K((t))$-nek.

2.1.5. Lemma (Hensel-lemma)**.** Legyen $F \in K[[t]][y]$ normált polinom. Ekkor nyilván $F = \sum_{i=0}^{\infty} F_i t^i$, ahol $F_i \in K[y]$. Ha $\exists g, h \in K[y]$ normált, egymáshoz relatív prím polinomok, hogy $F_0 = g \cdot h$, akkor $\exists G, H \in K[[t]][y]$, hogy $G_0 = g$, $H_0 = h$, és $F = G \cdot H$.

Bizonyítás. Legyen $m := \deg(F) = \deg(F_0)$, $r = \deg(g)$ és $s = \deg(h)$. Ekkor minden pozitív i-re $\deg(F_i) < m$. Keresünk $G = \sum_{i=0}^{\infty} G_i t^i$ és $H = \sum_{i=0}^{\infty} H_i t^i$ alakú polinomokat (y-ban polinomok), melyekre $G_0 = g$, $H_0 = h$, és minden pozitív i-re $\deg(G_i) < r$ és $\deg(H_i) < s$. Ha ilyeneket találunk, az bizonyítja az állítást, hiszen a fokokra vonatkozó feltétel biztosítja, hogy G és H normált legyen. Ekkor

$$F = GH \Leftrightarrow F_n = \sum_{i+j=n} G_i H_j, n = 0, 1, ...$$

Így elég a fenti egyenletrendszert kielégítő G_i-ket és H_j-ket találni. Induktívan, n-re növekvő sorrendben oldjuk meg az n-edik egyenletet, vagyis adjuk meg G_n-et és H_n-et. Első esetben $n = 0$-ra a $G_0 = g$ és $H_0 = h$ megoldja az első $F_0 = G_0 H_0$ egyenletet. Ezután az indukciós feltevés szerint az első n egyenletet megoldottuk, vagyis megadtuk G_i-t és H_i-t $\forall 0 \leq i \leq n-1$, hogy az első n egyenletet megoldják. Ekkor az $n+1$-edik egyenlet a következőképpen írható:

$$G_0 H_n + H_0 G_n = F_n - \sum_{i=1}^{n-1} G_i H_{n-i}$$

Az egyenlet jobb oldalát nevezzük U_n-nek. U_n-t ismerjük az indukciós feltevés szerint, és a foka kisebb m-nél. $G_n, H_n \in K[y]$ megtalálása a feladat, amelyek megoldják az egyenletet, továbbá $\deg(G_n) < r$, és $\deg(H_n) < s$. G_0 és H_0 relatív prímek, tehát a [2] 3.2.7 tétele alapján $\exists P, Q \in K[y]$, hogy $G_0 P + H_0 Q = U_n$. Maradékos osztással $P = H_0 S + R$, ahol $R, S \in K[y]$, $\deg(R) < s$. Legyen $H_n = R$ és $G_n = Q + G_0 S$. Ekkor $\deg(H_n) < s$ és $H_0 G_n = U_n - G_0 H_n$ miatt $\deg(H_0 G_n) < m$, tehát $\deg(G_n) < r$. Ezzel az indukció teljes. □

2.1.6. Jelölés. Az i/n ($i, n \in \mathbb{Z}$, ahol n rögzített) alakú racionális számok additív csoportját jelöljük a következőképpen: $\mathbb{Z}n^{-1}$. Ez izomorf $\mathbb{Z}$-vel az $i/n \mapsto i$ által megadott izomorfizmussal. Legyen K egy test, és $\Lambda = K((t))$. Legyen Λ_n az $(a_j)_{j \in \mathbb{Z}n^{-1}}$ alakú sorozatok halmaza, ahol minden i-re $a_i \in K$. Definiáljuk az összeadást és szorzást ugyanúgy, mint a 2.1.2 Definícióban. Nyilván Λ_n test, hiszen izomorf Λ-val az $(a_j)_{j \in \mathbb{Z}n^{-1}} \mapsto (b_i)_{i \in \mathbb{Z}}$, $b_i = a_{i/n}$ izomorfizmussal. Nevezzük t ősképét a megadott izomorfizmusnál τ-nak. Igaz továbbá, hogy $\Lambda \leq \Lambda_n$ a következő beágyazással: $(b_i)_{i \in \mathbb{Z}} \mapsto (a_j)_{j \in \mathbb{Z}n^{-1}}$, ahol $a_j = 0$ $\forall j \notin \mathbb{Z}$, és $a_j = b_j$ $\forall j \in \mathbb{Z}$. Világos, hogy ekkor $\tau^n = t$. Egy tetszőleges $(a_j) \in \Lambda_n$ sorozatra a $\sum_{j \in \mathbb{Z}n^{-1}} a_j t^j = \sum_{i \in \mathbb{Z}} a_{i/n} \tau^i = \sum_{i \in \mathbb{Z}} b_i \tau^i$ szimbolikus jelöléseket használjuk, így $\Lambda_n = K((t^{1/n})) = K((\tau))$. Ezt a jelölést a fejezet további részében használjuk.

2.1.7. Lemma. Legyen K algebrailag zárt test, $\mathrm{char} K = 0$, és $\varepsilon_n \in K$ primitív n-edik egységgyök. Ekkor Λ_n/Λ Galois, és foka n; $\mathrm{Gal}(\Lambda_n/\Lambda) = \langle \omega \rangle$ ciklikus, ahol ω-t a $\sum_{i \in \mathbb{Z}} b_i \tau^i \mapsto \sum_{i \in \mathbb{Z}} (b_i \varepsilon_n^i) \tau^i$ hozzárendeléssel definiáljuk. Ezenkívül $\Lambda_n = \Lambda(\tau)$, ahol $\tau^n = t$.

Bizonyítás. Triviális, hogy ω a Λ_n egy automorfizmusa. Világos az is, hogy az ω által fixen hagyott elemek pont Λ elemei. Emiatt Artin tételéből (2.1.1 Tétel) következik, hogy Λ_n/Λ Galois és $\mathrm{Gal}(\Lambda_n/\Lambda) = \langle \omega \rangle$. A rendje ω-nak nyilván n, tehát $|\Lambda_n : \Lambda| = n$, és $\omega^i(\tau) = \varepsilon_n^i \tau$, tehát a Galois-csoport egyik nemtriviális eleme sem hagyja fixen τ-t, emiatt $|\Lambda(\tau) : \Lambda| \geq n$ ([6] 1.10 Következmény), amiből $\Lambda_n = \Lambda(\tau)$. □

2.1.8. Lemma. Legyen L egy test, és α algebrai elem L felett. Legyen $f(x) = \sum_{i=0}^{n} a_i x^i$ olyan $n > 0$-fokú polinom L felett, melynek α gyöke. Ekkor

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

olyan n-edfokú normált polinom, melyre $g(a_n\alpha) = 0$. Világos, hogy $L(\alpha) = L(a_n\alpha)$.

Bizonyítás. Triviális. □

2.1.9. Lemma. Legyen K algebrailag zárt és 0 karakterisztikájú. Legyen $F \in K[[t]][y]$ y-ban normált és nem konstans. Ekkor valamilyen n-re F-nek van gyöke Λ_n-ben.

Bizonyítás. Indirekt tegyük fel, hogy az állítás hamis, és legyen F minimális fokú ellenpélda. Ekkor $n = \deg(F) \geq 2$. Írjuk fel F-et $F(y) = y^n + a_{n-1}y^{n-1} + ... + a_0$ alakban, ahol $a_i \in K[[t]]$. A $G(y) = F(y - \frac{a_{n-1}}{n})$ összefüggéssel definiált polinomban az y^{n-1} együtthatója 0. Nyilván az, hogy F-nek és G-nek van-e gyöke, ekvivalens, tehát feltehetjük, hogy y^{n-1} együtthatója F-ben 0 (hiszen kicserélhetjük F-et G-re). K algebrai zártsága miatt F_0 felbomlik gyöktényezők szorzatára. Ha $F_0(y) \neq (y-b)^n$ semmilyen b-re, akkor különböző gyöktényezők vannak F_0-ban, emiatt felírható egymáshoz relatív prím polinomok szorzataként, vagyis a 2.1.5 lemma miatt $F = G \cdot H$, amelyek F-nél kisebb fokúak, tehát van gyökük valamilyen Λ_n-ben. Ez ellentmondás.

A továbbiakban tehát $F_0(y) = (y-b)^n$ valamilyen b-re. Mivel y^{n-1} együtthatója F-ben 0, ezért F_0-ban is 0, tehát $nb = 0$. A karakterisztika 0, emiatt $b = 0$. Feltehető tehát, hogy $F_0 = y^n$. Ebből következik, hogy minden a_i konstans együtthatója 0. Mivel az $F(y) = y^n$ polinomnak gyöke a 0, ezért van olyan $i \in \{0, 1, ..., n-2\}$, amire $a_i \neq 0$. Innentől csak az ilyen i-ket vesszük figyelembe. Legyen m_i olyan, hogy teljesüljön $a_i = ct^{m_i} + p_i$, ahol p_i-ben t-nek csak m_i-nél magasabb hatványai fordulnak elő, és $c \in K$ nem nulla. Ekkor $m_i > 0$. Legyen u a legkisebb $m_i/(n-i)$ alakban felírható szám. Nyilván $u \in \mathbb{Q}$, és $u > 0$, tehát felírható $u = l/k$ alakban, ahol $k, l \in \mathbb{Z}$, $k, l > 0$.

Ágyazzuk be Λ-t $\Lambda_k = K((\tau))$-ba a 2.1.6 jelölésben leírt módon. Tekintsük az $F^*(y) = \tau^{-ln}F(\tau^l y) = y^n + \sum_{i=0}^{n-2} a_i\tau^{l(i-n)}y^i$, összefüggéssel definiált $F^* \in K[[\tau]][y]$ polinomot. Ebben y^i együtthatója (ha nem nulla), egy Laurent-sor τ-ban a következő alakban: $a_i\tau^{l(i-n)} = at^{m_i}\tau^{l(i-n)} + q_i = a\tau^{E_i} + q_i$, ahol q_i-ben csak E_i-nél magasabb fokú tagok vannak és $E_i = k(n-i)(\frac{m_i}{n-i} - u) \geq 0$. Nyilvánvalóan van olyan i, amire $E_i = 0$ (hiszen valamely i-re definíció szerint $u = m_i/(n-i)$). Legyen $F^*(y) = \sum_{i=0}^{\infty} F_i^*\tau^i$. F_0^* az algebrai zártság miatt gyöktényezőkre bomlik. Tegyük fel, hogy $F_0^*(y) = (y-d)^n$ valamilyen d-re. Mivel F_0^*-ban y^{n-1} együtthatója 0, ezért $nd = 0$, vagyis a 0 karakterisztika miatt $d = 0$. $F_0^*(y) = y^n$ Viszont nem lehet, hiszen valamilyen i-re $E_i = 0$. Ekkor tehát F_0^* különböző gyöktényezőkből áll, így felbomlik relatív prím polinomok szorzatára, tehát alkalmazhatjuk rá a 2.1.5 lemmát, amennyiben kicseréljük az állításban t-t τ-ra. $F^* = GH$, ahol $G, H \in K[[\tau]][y]$. H foka szigorúan kisebb, mint n, tehát van gyöke valamely $\Lambda_k(\tau^{1/k'}) = \Lambda_{kk'}$-ben. Így F^*-nak, és végül F-nek is van gyöke $\Lambda_{kk'}$-ben. □

2.1.10. Tétel. Legyen K algebrailag zárt, 0 karakterisztikájú test. Legyen Δ/Λ véges, n-fokú testbővítés. Ekkor $\Delta = \Lambda(\delta)$, ahol $\delta^n = t$.

Bizonyítás. Δ/Λ egyszerű, hiszen véges és szeparábilis ([6] 1.15 Tétel). Ez alapján tehát $\Delta = \Lambda(\theta)$ valamely $\theta \in \Delta$ elemre, és legyen $F(y) \in \Lambda[y]$ a θ minimálpolinomja. Szeretnénk belátni, hogy $F(y)$-nak van gyöke valamely $\Lambda_{n'}$ testben. Mivel $F(y)$-ra ez pontosan akkor teljesül, ha $t^i F(y)$-ra, tehát feltehető, hogy $F(y) \in K[[t]][y]$. Ezenkívül a 2.1.8 lemma alapján feltehető, hogy normált y-ban és világos, hogy nem konstans, tehát a 2.1.9 lemma szerint van olyan n' szám, melyre $F(y)$-nak van gyöke $\Lambda_{n'}$-ben. Legyen ez a gyök θ'. Emiatt $\Delta \subseteq \Lambda_{n'}$. Mivel $\mathrm{Gal}(\Lambda_{n'}/\Lambda)$ ciklikus, ezért, tekintve, hogy a Galois-elmélet főtétele miatt a részcsoportjai bijektíven megfeleltethetőek a $\Lambda_{n'}$ és Λ között lévő testeknek, tehát $\Delta = \Lambda_n$ valamely n-re, amely osztja n'-t. Így $\delta = t^{1/n}$ választással $\Delta = \Lambda(\delta)$, és $\delta^n = t$. □

2.1.11. Következmény (Puiseux tétele)**.** $\bigcup_{i=1}^{\infty} \Lambda_i$ algebrailag zárt, vagyis ez a formális Laurent-sorok testének algebrai lezárása.

Bizonyítás. Vegyünk egy $f(y) \in \bigcup_{i=1}^{\infty} \Lambda_i[y]$ irreducibilis polinomot. Belátjuk, hogy ennek van gyöke $\bigcup_{i=1}^{\infty} \Lambda_i$-ben. Az $f(y)$-nak az összes a_j együtthatójára teljesül, hogy $a_j \in \Lambda_{n_j}$ valamely n_j számokra. Emiatt van olyan m (például az n_j-knek a legkisebb közös többszöröse), amelyre $a_j \in \Lambda_m$, minden együtthatóra. Ekkor $f(y) \in \Lambda_m[y]$. Jelöljük Λ_m-et $K((\tau))$-val (2.1.6 Jelölés), ahol $\tau^m = t$, illetve $K((t)) = \Lambda$. Bővítsük Λ_m-et $f(y)$ egyik gyökével, és legyen a kapott test Δ. Ez egy véges bővítés, tehát a 2.1.10 tételt használhatjuk, ha a tételben kicseréljük Λ-t Λ_m-re a 2.1.6 jelölésben leírt izomorfizmussal. Ekkor $\Delta = \Lambda_m(\delta)$, ahol $\delta^k = \tau$. Világos, hogy Δ ekkor Λ_m-izomorf $\Lambda_{mk} = K((\tau_0))$-val a $\delta \mapsto \tau_0$ hozzárendeléssel (ez az említett tétel bizonyításából látszik). Emiatt $f(y)$-nak van gyöke Λ_{mk}-ban, vagyis $\bigcup_{i=1}^{\infty} \Lambda_i$ algebrailag zárt. Az, hogy ez algebrai bővítés Λ felett, triviális, tehát valóban ez az algebrai lezárt. □

2.2. Az elágazási típus

K ebben az alfejezetben is mindenütt algebrailag zárt test lesz, melyre $\mathrm{char}K = 0$ (még ha nem is mindenhol lesz kimondva), és $L/K(x)$ alakú testbővítésekről lesz szó, ahol $K(x)$ a K feletti racionális törtfüggvények teste. Ennek oka Hilbert irreducibilitási tétele (lásd 4.2).

2.2.1. Jelölés. Legyen K algebrailag zárt, 0 karakterisztikájú test, ebben $(\varepsilon_n)_{n\in\mathbb{N}}$ primitív n-edik egységgyökök rendszere kompatibilis, vagyis ha n, k, l természetes számokra teljesül, hogy $n = kl$, akkor $\varepsilon_n^l = \varepsilon_k$. Legyen Δ/Λ n-fokú véges Galois-bővítés. Ekkor a 2.1.10 tétel miatt $\Delta = \Lambda(\delta)$, és $\delta^n = t$. Nyilván egyértelműen létezik $\mathrm{Gal}(\Delta/\Lambda)$-nak egy ω eleme, amelyre $\omega(\delta) = \varepsilon_n \delta$. Ezt az ω-t a $\mathrm{Gal}(\Delta/\Lambda)$ kitüntetett generátorának nevezzük. Ez valóban generátor. Legyen $\mathbb{P}^1_K = K \cup \{\infty\}$, ahol $\infty \notin K$ formális jelölés. K-nak bármely α automorfizmusát kiterjeszthetjük $\mathbb{P}^1_K$-re úgy, hogy $\alpha(\infty)$-t ∞-nek definiáljuk. Bármely $p \in \mathbb{P}^1_K$-re jelöljük $\vartheta_p : K(x) \to K(t)$-vel azt az izomorfizmust, amelyet a következő hozzárendelések valamelyike határoz meg: ha $p \neq \infty$, akkor $x \mapsto t + p$, ha $p = \infty$, akkor $x \mapsto 1/t$. A fejezet további részében ezen jelöléseket használjuk.

2.2.2. Állítás. Legyen K algebrailag zárt test, $\mathrm{char}K = 0$, és Δ/Λ n-fokú véges Galois-bővítés. Ekkor ha $\delta' \in \Delta$, és $\exists n' \in \mathbb{Z}$, $n' \geq 1$, hogy $(\delta')^{n'} = t$, akkor $\omega(\delta') = \varepsilon_{n'}\delta'$. Speciálisan, ha $\Lambda \subseteq \Delta' \subseteq \Delta$, akkor $\omega|_{\Delta'}$ lesz $\mathrm{Gal}(\Delta'/\Lambda)$ kitüntetett generátora.

Bizonyítás. Az első állítást elég $\delta' = \delta^{n/n'}$-re bizonyítani, hiszen bármely más lehetőség ennek és egy egységgyöknek szorzata. Valóban, mivel ε_n-ek kompatibilisek, ezért $\omega(\delta') = \varepsilon_n^{n/n'}\delta' = \varepsilon_{n'}\delta'$. A második állítás ennek triviális következménye. □

2.2.3. Állítás. Legyen K algebrailag zárt test, $\mathrm{char}K = 0$, $L/K(x)$ véges Galois-bővítés, melynek Galois-csoportja $G = \mathrm{Gal}(L/K(x))$. Rögzítsünk egy $p \in \mathbb{P}^1_K$ elemet. Ekkor a következők igazak:

(a) $\vartheta_p : K(x) \to K(t)$ kiterjeszthető egy $\vartheta : L \to L_\vartheta$ izomorfizmussá, ahol L_ϑ részteste egy olyan Δ-nak, amelyre teljesül hogy Δ/Λ véges Galois-bővítés. Ekkor L_ϑ invariáns $\mathrm{Gal}(\Delta/\Lambda)$-ra nézve. Legyen $g_\vartheta \in G$ a következő: $g_\vartheta = \vartheta^{-1} \circ \omega \circ \vartheta$, ahol ω a $\mathrm{Gal}(\Delta/\Lambda)$ kitüntetett generátora. Ha $\tilde{\Delta}/\Lambda$ szintén véges Galois-bővítés, amire $L_{\tilde{\vartheta}} \leq \tilde{\Delta}$, és $\tilde{\vartheta} : L \to L_{\tilde{\vartheta}}$ egy ϑ_p-t kiterjesztő izomorfizmus, akkor $g_{\tilde{\vartheta}}$ és g_ϑ a G-nek ugyanazon C_p konjugáltosztályában vannak. Ez a C_p csak L-től és p-től függ.

(b) Legyen $e_{L,p}$ a C_p osztály elemeinek közös rendje. $L/K(x)$-nek vegyük egy primitív γ elemét. Legyen $F \in K(x)[y]$ γ minimálpolinomja. Jelöljük $\vartheta_p F \in K(t)[y]$-nal azt a polinomot, amelyet úgy kapunk, hogy F együtthatóit megváltoztatjuk a ϑ_p-nél vett képükre. Ekkor $\vartheta_p F$ minden irreducibilis tényezőjének foka $n = e_{L,p}$. Ezenkívül az (a) részben választhatjuk Δ-t Λ_n-nek.

(c) Választhatjuk (b) részben γ-t úgy, hogy $F(y) = F(x, y) \in K[x, y]$ normált y-ban. Ekkor $F(y)$-nak a $D(x)$ diszkriminánsa $K(x)$ fölött $K[x]$-nek egy nemnulla eleme. Ha $p \in K$ és $D(p) \neq 0$, akkor $e_{L,p} = 1$.

(d) Ha $L' \subseteq L$ olyan, hogy $L'/K(x)$ véges Galois-bővítés, akkor G megszorítása $G' = \mathrm{Gal}(L'/K(x))$-re C_p-t abba a C'_p-be küldi, ahol C'_p az (a) ponttal analóg módon van definiálva L helyett L'-re.

Bizonyítás. (a) ϑ létezését a (b) részben bizonyítjuk. Tekintsük a (b) pontban definiált $\vartheta_p F$-et. Ennek a gyökei generálják L_ϑ-t $K(t)$ fölött, amely gyököket $\mathrm{Gal}(\Delta/\Lambda)$ permutálja, így rá nézve L_ϑ invariáns. A második, $\tilde{\vartheta}$-ról szóló állítás belátásához feltehető, hogy $\exists \Delta_0$, hogy Δ_0/Λ véges Galois-bővítés, és $\Delta, \Delta' \subseteq \Delta_0$. Ekkor $\vartheta_p F$ gyökei generálják L_ϑ-t és $L_{\tilde{\vartheta}}$-t is, így $L_\vartheta = L_{\tilde{\vartheta}}$. Legyen $h = \vartheta^{-1}\tilde{\vartheta} \in G$, és ω_0 a $\mathrm{Gal}(\Delta_0/\Lambda)$ kitüntetett generátora. Mivel $\omega_0|_\Delta = \omega$, ezért $g_{\tilde{\vartheta}} = \tilde{\vartheta}^{-1}\omega_0\tilde{\vartheta} = h^{-1}\vartheta^{-1}\omega_0\vartheta h = h^{-1}g_\vartheta h$.

(b) Legyen H a $\vartheta_p F$-nek egy irreducibilis tényezője és legyen $\Delta = \Lambda[y]/(H)$. Δ/Λ véges testbővítés, és H-nak (így $\vartheta_p F$-nek is) van Δ-ban gyöke. Legyen ez a gyök γ'. Emiatt ϑ_p kiterjeszthető egy $\vartheta : L \to L_\vartheta$ izomorfizmussá, ahol $L_\vartheta = K(t)[\gamma'] \subseteq \Delta$, és, mint tudjuk, $L = K(x)[\gamma]$. Ezzel (a) bizonyítása teljes. Vegyük azt a $\mathrm{Gal}(\Delta/\Lambda) \to \mathrm{Gal}(L_\vartheta/K(t))$ homomorfizmust, amit az L_ϑ-ra való megszorítással nyerünk. Ez $\Delta = \Lambda(\gamma')$ miatt injektív, emiatt ω és $\omega|_{L_\vartheta}$ rendje megegyezik. Ez a rend nyilvánvalóan egyenlő g_ϑ rendjével, vagyis $e_{L,p}$-vel, $|\Delta : \Lambda|$ pedig értelemszerűen megegyezik ω rendjével. Így $\deg(H) = |\Delta : \Lambda| = e_{L,p}$. A második állítás abból következik, hogy $|\Delta : \Lambda| = n$ miatt Δ izomorf Λ_n-nel a 2.1.10 tétel miatt.

(c) Egy x^i-vel való szorzás és a 2.1.8 lemma alapján feltehetjük, hogy $F \in K[x, y]$, és y-ban normált. Emiatt $D(x) \in K[x]$. F irreducibilis, tehát a 0 karakterisztika miatt szeparábilis, tehát $D(x)$ nem nulla. Ha $p \in K$ és $D(p) \neq 0$, akkor $F(p, y)$ is szeparábilis. A 2.1.5 lemma feltételeit ellenőrizzük $\vartheta_p F \in \Lambda[y]$ polinomra. $(\vartheta_p F)_0(y) = F(p, y)$, tehát szeparábilis, vagyis gyöktényezőkre bomlik. A 2.1.5 lemma alapján (ha elvégezzük a lemmabeli faktorizálást annyiszor, ahánygyöktényező van) $\vartheta_p F$ is gyöktényezőkre bomlik $\Lambda[y]$-ban. Így a (b) rész miatt $e_{L,p} = \deg(H) = 1$.

(d) Legyen $\vartheta : L \to \Delta$ az (a)-beli kiterjesztése ϑ_p-nek. Ekkor $\vartheta' = \vartheta|_{L'}$ egy izomorfizmus L' és $\vartheta(L')$ között és szintén kiterjeszti ϑ_p-t. Így $g_{\vartheta'} = (\vartheta')^{-1}\omega\vartheta' = \vartheta^{-1}\omega\vartheta|_{L'} = g_\vartheta|_{L'}$. Ez pont a (d)-beli állítás. □

2.2.4. Definíció (G csoport p-hez asszociált konjugáltosztálya)**.** Legyen $L/K(x)$ egy véges Galois-bővítés és $G = \mathrm{Gal}(L/K(x))$ és $p \in \mathbb{P}^1_K$. Definiáljuk g_ϑ-t úgy, mint a 2.2.3 állítás (a) részében. Ekkor g_ϑ konjugáltosztályát C_p-vel jelöljük és a G csoport p-hez asszociált konjugáltosztályának nevezzük.

2.2.5. Definíció (Elágazási index)**.** Legyen $L/K(x)$ véges Galois-bővítés és $p \in \mathbb{P}^1_K$. Ekkor a $\mathrm{Gal}(L/K(x))$ p-hez asszociált konjugáltosztályában lévő elemek közös rendjét $e_{L,p}$-vel jelöljük és L elágazási indexének nevezzük p-nél.

2.2.6. Definíció (Elágazási pont)**.** Legyen $L/K(x)$ véges Galois-bővítés és $p \in \mathbb{P}^1_K$. Ekkor p-t elágazási pontnak nevezzük, ha $e_{L,p} > 1$.

2.2.7. Lemma. Legyenek $L/K(x)$ és $L'/K(x)$ n-edfokú véges Galois-bővítések, és $G = \mathrm{Gal}(L/K(x))$, $G' = \mathrm{Gal}(L'/K(x))$. Legyen G-ben C_p, G'-ben pedig C'_p a p-hez asszociált konjugáltosztály. Legyen α egy automorfizmusa K-nak és legyen m az a szám, amire $\alpha^{-1}(\varepsilon_n) = \varepsilon_n^m$. Tegyük fel, hogy $\exists\lambda : L \to L'$ izomorfizmus, hogy $\lambda|_K = \alpha$ és $\lambda(x) = x$. Ez a λ indukál egy $\lambda^* : G \to G'$ csoportizomorfizmust a következő hozzárendeléssel: ha $g \in G$, akkor $g \mapsto \lambda g\lambda^{-1}$. Ekkor $C'_{\alpha(p)} = \lambda^*(C_p)^m$, ahol $\lambda^*(C_p)^m$-t a következőképpen értelmezzük: ha C egy konjugáltosztály G-ben, és $g \in C$, akkor g^m konjugáltosztályát jelöljük C^m-mel. (Ez nyilván független $g \in C$ választásától.)

Bizonyítás. Rögzítsük $p \in \mathbb{P}^1_K$-et és legyen $k = e_{L,p}$. Ekkor k osztja n-et ($n = |G|$), emiatt, és ε_k-k kompatibilitása miatt $\alpha^{-1}(\varepsilon_k) = \varepsilon_k^m$. Legyen $\widetilde{\alpha}$ az az automorfizmusa $\Lambda_k = K((\tau))$-nak, amelyet a $\sum b_i\tau^i \mapsto \sum \alpha(b_i)\tau^i$ hozzárendeléssel nyerünk. Világos, hogy $\widetilde{\alpha}|_K = \alpha$. A 2.1.6 jelölésben definiált beágyazással tekintsük ismét $\Lambda = K((t))$-t Λ_k résztestének, ahol $t = \tau^k$, és legyen $\omega \in \mathrm{Gal}(\Lambda_k/\Lambda)$ az a generátor, amire $\omega(\tau) = \varepsilon_k\tau$. Ekkor $\widetilde{\alpha}^{-1}\omega\widetilde{\alpha}(\tau) = \widetilde{\alpha}^{-1}(\omega(\tau)) = \alpha^{-1}(\varepsilon_k)\tau = \varepsilon_k^m\tau = \omega^m(\tau)$ miatt $\widetilde{\alpha}^{-1}\omega\widetilde{\alpha} = \omega^m$. A 2.2.3 állítás (b) része alapján $\exists\vartheta$ izomorfizmus L-ről Λ_k egy résztestére, amelyre $\vartheta|_{K(x)} = \vartheta_p$. Tekintsük a $\vartheta' := \widetilde{\alpha} \circ \vartheta\lambda^{-1}$ izomorfizmust L'-ről Λ_k egy résztestére. Erre igaz, hogy $\vartheta'|_{K(x)} = \vartheta_{\alpha(p)}$. Ennek belátásához két dolog kell. Egyrészt, ϑ' az identitás K-n, hiszen $\widetilde{\alpha}|_K = \lambda|_K = \alpha$. Másrészt, ha $p \neq \infty$, akkor $\vartheta'(x) = \widetilde{\alpha}(\vartheta(x)) = \widetilde{\alpha}(t + p) = t + \alpha(p)$, és $p = \infty$-re $\vartheta'(x) = \widetilde{\alpha}(\vartheta(x)) = \widetilde{\alpha}(1/t) = 1/t$. Végül a lemma állításának belátásához elég, hogy $g_{\vartheta'} = (\vartheta')^{-1}\omega\vartheta' = \lambda\vartheta^{-1}\widetilde{\alpha}^{-1}\omega\widetilde{\alpha}\vartheta\lambda^{-1} = \lambda\vartheta^{-1}\omega^m\vartheta\lambda^{-1} = \lambda g_\vartheta^m\lambda^{-1} = \lambda^*(g_\vartheta)^m$. □

2.2.8. Definíció (Elágazási típus)**.** Legyen a $(G, P, \mathbf{C})$ hármasban G egy csoport, P véges részhalmaza $\mathbb{P}^1_{\mathbb{C}}$-nek és $\mathbf{C} = (C_p)_{p\in P}$ pedig G nemtriviális konjugáltosztályainak egy családja, P elemeivel indexelve. $(G, P, \mathbf{C})$-t és $(G', P', \mathbf{C}')$-t ekvivalensnek nevezzük, ha $P = P'$ és létezik olyan $G \to G'$ izomorfizmus, amely C_p-t C'_p-be képezi minden $p \in P$-re. Ez nyilván ekvivalenciareláció ezeken a hármasokon. Jelölje egy $(G, P, \mathbf{C})$ hármas ekvivalenciaosztályát $\mathcal{T} = [G, P, \mathbf{C}]$. Az ilyen $\mathcal{T}$-ket elágazási típusnak nevezzük.

2.2.9. Megjegyzés. Egy $L/K(x)$ véges Galois-bővítés elágazási típusa alatt a következő hármast értjük: $\mathcal{T} = [\mathrm{Gal}(L/K(x)), P, (C_p)_{p\in P}]$, ahol P az elágazási pontok halmaza, C_p pedig a p-hez asszociált konjugáltosztály, ha $p \in P$.

2.3. Egy példa

Ebben az alfejezetben megvizsgáljuk az egyik legegyszerűbb példát az $L/K(x)$ alakú bővítésekre. Azt fogjuk megnézni, hogy milyen véges csoportok állhatnak elő Galois-csoportként, és mi az elágazási típus, ha a bővítés $K(y)/K(x)$ alakú, ahol K algebrailag zárt, $\mathrm{char}(K) = 0$, és x, y transzcendens elemek K felett, vagyis $K(x)$, valamint $K(y)$ egyaránt izomorf a racionális törtfüggvények testével. Világos, hogy ha egy ilyen alakú Galois-bővítést veszünk, akkor ennek Galois-csoportja beágyazható $\mathrm{Aut}(K(y)/K)$-ba, hiszen ha egy automorfizmus fixen hagyja $K(x)$-et, akkor speciálisan K-t is.

2.3.1. Állítás. Legyen $y' \in K(y)$. Pontosan akkor teljesül, hogy $K(y) = K(y')$, ha léteznek olyan $a, b, c, d \in K$, $ad - bc \neq 0$ elemek, hogy $y' = \frac{ay+b}{cy+d}$, vagyis y' előáll y-ból lineáris törtfüggvény alakban.

Bizonyítás. Nézzük a könnyebbik irányt, és tegyük fel, hogy y' előáll megfelelő együtthatókkal $y' = \frac{ay+b}{cy+d}$ alakban. Be fogom látni, hogy ekkor $y \in K(y')$. Tudjuk, hogy a lineáris törtfüggvények reprezentálhatóak a mátrixukkal, és azt is tudjuk, hogy ha két lineáris törtfüggvényt komponálunk, akkor a kapott függvény reprezentálható a két mátrix szorzatával. Tekintsük tehát az

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

mátrixot, és nevezzük l_1-nek az általa reprezentált lineáris törtfüggvényt. Tudjuk, hogy $l_1(y) = y'$. M determinánsa a feltétel alapján nem 0, tehát invertálható. Tekintsük az

$$M^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

által reprezentált l_2 lineáris törtfüggvényt. Mivel $MM^{-1} = I$, ahol I az egységmátrix, ezért $l_2 \circ l_1 = \mathrm{id}$. Emiatt

$$l_2(y') = l_2(l_1(y)) = y.$$

Ez alapján $\frac{ey'+f}{gy'+h} = y$, tehát y előáll y'-ből racionális törtfüggvény alakban, tehát $y \in K(y')$. Ebből következik, hogy $K(y) \leq K(y')$, és mivel azt már tudtuk, hogy $K(y') \leq K(y)$, ezért $K(y) = K(y')$.

A másik irány belátásához tegyük fel, hogy $K(y) = K(y')$ és $y' = P(y)/Q(y)$, ahol P és Q egymáshoz relatív prím polinomok. Indirekt tegyük fel, hogy $\deg(P) \geq 2$. Szeretnénk egy olyan $a_1 \in K$ elemet találni, hogy a $P(x)/Q(x) = a_1$ egyenletet több K-beli elem is kielégítse. Tegyük fel, hogy a $0 = a_1$ nem ilyen. Ez azt jelenti, hogy $P(x)/Q(x) = 0$-nak legfeljebb egy megoldása van. Ez ekvivalens azzal, hogy $P(x) = 0$-nak legfeljebb egy megoldása van, hiszen P és Q relatív prímek, tehát nincs közös gyökük. Mivel K algebrailag zárt, ezért P gyöktényezőkre bomlik (hiszen nem konstans), tehát ha csak egy gyöke van, akkor $P(x) = (x - d_1)^n$ valamely $d_1 \in K$-ra. Mivel P és Q relatív prímek, ezért léteznek $b_1, c_1 \in K$ elemek, hogy $b_1 \cdot P(x) + c_1 \cdot Q(x) = 1$ ([2] 3.2.7 Tétel). Ha felírjuk, hogy $P(x)(b_1 + 1) + Q(x)c_1 = 0$, az ekvivalens azzal, hogy $P(x) + 1 = 0$. Ha ennek csak egy megoldása lenne, akkor $P(x) + 1 = (x - d_2)^n$ teljesülne, viszont $P(x) = (x - d_1)^n$-ben x^{n-1} együtthatója egyrészt nd_1, másrészt nd_2 (hiszen $n \neq 2$, vagyis a +1-es nincs rá hatással), tehát $d_1 = d_2$, de ez ellentmondás, hiszen $d_1^n = d_2^n - 1$ (hiszen ez a konstans tagja $P(x)$-nek), tehát $P(x)(b_1 + 1) + Q(x)c_1 = 0$-nak több megoldása van. Ha $b_1 + 1 \neq 0$, akkor tehát az

$a_1 = -\frac{c_1}{b_1+1}$ jó választás. Ha $b_1 + 1 = 0$, akkor tekintsük ugyanígy például a $P(x)(3b_1 + 1) + Q(x)3c_1 = 0$ egyenletet, ebből jön a $-\frac{3c_1}{3b_1+1} = a_1$ megoldás. Mindenképpen találtunk egy $a_1 \in K$ elemet, amelyre létezik $x_1 \neq x_2 \in K$, hogy $P(x_1)/Q(x_1) = P(x_2)/Q(x_2) = a_1$. Mivel feltettük, hogy $K(y) = K(y')$, ezért $y \in K(y')$, vagyis $y = P_0(y')/Q_0(y')$ valamely P_0, Q_0 relatív prím polinomokra. Ekkor

$$\frac{P_0\left(\frac{P(y)}{Q(y)}\right)}{Q_0\left(\frac{P(y)}{Q(y)}\right)} = y,$$

tehát ha például behelyettesítjük x_1-et, vagy x_2-t, akkor, mivel formális átalakítások után ez a függvény visszaadja y-t, ezért ebbe behelyettesítve is az identitást kell kapnunk rájuk ott, ahol a belső függvény értelmezve van. Ekkor

$$x_2 = \frac{P_0\left(\frac{P(x_2)}{Q(x_2)}\right)}{Q_0\left(\frac{P(x_2)}{Q(x_2)}\right)} = \frac{P_0(a_1)}{Q_0(a_1)} = \frac{P_0\left(\frac{P(x_1)}{Q(x_1)}\right)}{Q_0\left(\frac{P(x_1)}{Q(x_1)}\right)} = x_1,$$

ez viszont ellentmond annak, hogy $x_1 \neq x_2$. Ez azt jelenti, hogy $\deg(P) \geq 2$ nem lehet, tehát $\deg(P) \leq 1$. Tegyük fel, hogy $\deg(Q) \geq 2$. Ekkor, mivel az első rész alapján $K(y') = K(1/y')$, ezért $1/y'$-t tekintve megint ugyanúgy ellentmondásra jutunk, vagyis $\deg(Q) \leq 1$. Ezek alapján fel lehet írni y'-t ilyen alakban:

$$y' = \frac{ay + b}{cy + d}.$$

Tegyük fel indirekt, hogy $ad - bc = 0$. Ekkor az

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

mátrix determinánsa 0, tehát a rangja nem kettő, tehát a két sora egymás skalárszorosai, tehát két eset van. Első esetben $a = b = 0$, amelyből következik, hogy $y' = 0$, vagyis $y' \in K$, ami ellentmondás. Második esetben $\exists \lambda \in K$, hogy $c = \lambda \cdot a$, és $d = \lambda \cdot b$, tehát

$$y' = \lambda \frac{ay + b}{ay + b} = \lambda,$$

tehát $y' \in K$. Ez megint ellentmondás, tehát $ad - bc \neq 0$, amivel beláttuk az állítást. □

2.3.2. Következmény. $\mathrm{Aut}(K(y)/K)$ izomorf $\mathrm{PGL}_2(K)$-val, vagyis a kétdimenziós projektív általános lineáris csoporttal K felett.

Bizonyítás. Csinálunk egy $\varphi : \mathrm{Aut}(K(y)/K) \to \mathrm{PGL}_2(K)$ izomorfizmust. Ha veszünk egy $\alpha \in \mathrm{Aut}(K(y)/K)$ elemet, azt egyértelműen meghatározza, hogy hova küldi y-t. Az, hogy α automorfizmus, az előző állítás alapján ekvivalens azzal, hogy

$$\alpha(y) = \frac{ay + b}{cy + d}$$

alakban felírható valamely $a, b, c, d \in K$, $ad - bc \neq 0$ elemekre. Legyen $\varphi(\alpha)$ az a lineáris törtfüggvény, amelyet az

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

mátrix határoz meg.

Először be kell látnunk, hogy ez jóldefiniált hozzárendelés. Vegyünk egy tetszőleges $\alpha \in \mathrm{Aut}(K(y)/K)$ automorfizmust, amelyre

$$\alpha(y) = \frac{a_1 y + b_1}{c_1 y + d_1} = \frac{a_2 y + b_2}{c_2 y + d_2},$$

és be kell látnunk, hogy a két kapott mátrix ekvivalens $\mathrm{PGL}_2(K)$-ban. Ha a fenti egyenlőség teljesül, akkor szorozva a nevezőkkel azt kapjuk, hogy $a_1c_2y^2 + (c_2b_1 + a_1d_2)y + b_1d_2 = a_2c_1y^2 + (c_1b_2 + a_2d_1)y + b_2d_1$. Ez a két polinom együtthatónként egyenlő, tehát $a_1/c_1 = a_2/c_2$, és $b_1/d_1 = b_2/d_2$, vagyis valamely $\lambda, \mu \in K$ párra $\lambda a_1 = a_2$, $\lambda c_1 = c_2$, $\mu b_1 = b_2$, $\mu d_1 = d_2$, tehát most y együtthatójára felírva: $\lambda c_1 b_1 + \mu a_1 d_1 = \mu b_1 c_1 + \lambda a_1 d_1$, vagyis átrendezve $\lambda(b_1c_1 - a_1d_1) = \mu(b_1c_1 - a_1d_1)$, tehát mivel $a_1d_1 - b_1c_1 \neq 0$, ezért $\lambda = \mu$. Az jött tehát ki, hogy

$$\lambda \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

Ezek $\mathrm{PGL}_2(K)$-ban ekvivalensek, hiszen ha két lineáris törtfüggvény mátrixai egymás skalárszorosai, akkor ekvivalensek. Beláttuk tehát, hogy jóldefiniált. Az világos, hogy homomorfizmus, hiszen tudjuk, hogy a mátrixszorzás a lineáris törtfüggvényeket komponálja, tehát már csak az kell, hogy bijektív.

Tekintsük a szürjektivitást. Ha van egy nemnulla determinánsú $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mátrixunk, akkor az előáll az $\alpha : K(y) \to K(y), y \mapsto \frac{ay+b}{cy+d}$ automorfizmus képeként.

Az injektivitáshoz tegyük fel, hogy $\alpha_1, \alpha_2 \in \mathrm{Aut}(K(y)/K)$ képei ekvivalensek:

$$\varphi(\alpha_1) = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \varphi(\alpha_2) = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

Ha két $\mathrm{PGL}_2(K)$-beli mátrix ekvivalens, akkor egymás skalárszorosai (legyen ez a skalár $\lambda \in K$), viszont az pont azt jelenti, hogy

$$\alpha_1(y) = \frac{a_1 y + b_1}{c_1 y + d_1} = \frac{\lambda a_1 y + \lambda b_1}{\lambda c_1 y + \lambda d_1} = \frac{a_2 y + b_2}{c_2 y + d_2} = \alpha_2(y),$$

vagyis $\alpha_1 = \alpha_2$, amivel beláttuk az injektivitást, tehát φ valóban izomorfizmus. □

2.3.3. Tétel. A $\mathrm{PGL}_2(K)$ csoport véges részcsoportjai izomorfia erejéig pontosan a ciklikus- és diédercsoportok, továbbá A_4, S_4 és A_5, ahol A_i az alternáló, és S_i a szimmetrikus csoportot jelenti.

Bizonyítás. Csak azt bizonyítjuk, hogy a ciklikus- és a diédercsoportok mind beágyazhatók $\mathrm{PGL}_2(K)$-ba, a teljes bizonyítás megtalálható a [13] műben.

Legyen Z_n az n elemű ciklikus csoport, és $\varepsilon_n \in K$ primitív n-edik egységgyök (ilyen van, hiszen K algebrailag zárt). Úgy tekintjük Z_n-et, mint az n-nél kisebb természetes számok additív csoportját modulo n. Tekintsük a következő beágyazást:

$$\varphi : Z_n \to \mathrm{PGL}_2(K), i \mapsto \begin{pmatrix} \varepsilon_n^i & 0 \\ 0 & 1 \end{pmatrix}.$$

Be kell látni, hogy ez beágyazás, vagyis injektív homomorfizmus. Nézzük a művelettartást. Legyen $i, j \in Z_n$.

$$\varphi(i)\varphi(j) = \begin{pmatrix} \varepsilon_n^i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \varepsilon_n^j & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \varepsilon_n^{i+j} & 0 \\ 0 & 1 \end{pmatrix} = \varphi(i+j),$$

tehát homomorfizmus. Világos az is, hogy két ilyen alakú mátrix nem skalárszorosa egymásnak, tehát injektív.

Most legyen D_n diédercsoport, és ismét $\varepsilon_n \in K$ primitív n-edik egységgyök. Most D_n-et a következő módon reprezentáljuk két generátorral és három relációval: $D_n = \langle a, b | a^2 = 1, b^n = 1, aba^{-1} = b^{-1} \rangle$. Ez valóban D_n-et reprezentálja, és a felel meg egy tükrözésnek, b pedig egy n-edrendű forgatásnak. Most veszünk egy φ homomorfizmust $\mathrm{PGL}_2(K)$-ba:

$$a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, b \mapsto \begin{pmatrix} \varepsilon_n & 0 \\ 0 & 1 \end{pmatrix}.$$

Nézzük meg, hogy teljesülnek-e a relációk: $a^2 = 1$ és $b^n = 1$ világos, hogy teljesül.

$$\varphi(a)\varphi(b)\varphi(a)^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \varepsilon_n & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon_n \end{pmatrix},$$

és ez a mátrix $\mathrm{PGL}_2(K)$-ban ekvivalens $\varphi(b)^{-1}$-zel.A relációk tehát teljesülnek, már csak azt kell belátni, hogy injektív lesz, ehhez pedig elég belátni, hogy a képben lesz legalább $2n$ db elem. Világos, hogy minden $i = 0, 1, ..., n-1$-re $\varphi(b^i) = \begin{pmatrix} \varepsilon_n^i & 0 \\ 0 & 1 \end{pmatrix}$, és $\varphi(b^i a b^{-i}) = \begin{pmatrix} 0 & \varepsilon_n^i \\ \varepsilon_n^{-i} & 0 \end{pmatrix}$, és ezek páronként különbözőek, tehát előáll $2n$ db különböző elem. Ezzel készen vagyunk. □

2.3.4. Megjegyzés. Ha tekintjük a $K = \mathbb{R}$ esetet (bár $\mathbb{R}$ nem algebrailag zárt), akkor mivel $\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{PGL}_2(\mathbb{R})$, ezért ekvivalensen tekinthetjük $\mathrm{SO}_3(\mathbb{R})$ véges részcsoportjait is, amelyek szintén azonosak a fenti tételben leírtakkal. Ennek egy magyar nyelvű szemléletes bizonyítása megtalálható a [4] jegyzetben (6.2.10 Tétel).

Az alfejezet további részéhez szükségünk lesz Lüroth híres tételére.

2.3.5. Tétel (Lüroth tétele)**.** Legyen $L_1 \leq L_2$ különböző testek, továbbá x transzcendens L_1 felett, és $L_2 \leq L_1(x)$. Ekkor létezik $y \in L_1(x)$, hogy $L_2 = L_1(y)$.

2.3.6. Következmény. A $K(y)/K(x)$ alakú véges Galois-bővítések Galois-csoportjaként pontosan a ciklikus csoportok, a diédercsoportok, A_4, S_4 és A_5 állnak elő.

Bizonyítás. Más csoport nem állhat elő a 2.3.2 következmény és a 2.3.3 tétel miatt. Azt kell csak belátni, hogy ezek mind előállnak. Vegyünk egy, a fentiek közüli csoportot, és egy olyan $G \leq \mathrm{Aut}(K(y)/K)$ részcsoportot, amely vele izomorf. Be fogjuk látni, hogy ez a Galois-csoportja valamely $K(y)/K(x)$ bővítésnek. Legyen L a fixteste G-nek. Artin tétele (2.1.1 Tétel) szerint $K(y)/L$ Galois és Galois-csoportja G. Lüroth tétele szerint (2.3.5) $L = K(x)$ valamely $x \in K(y)$-ra. □

Az alfejezet befejezéseként megnézünk egy-egy példát arra, amikor a Galois-csoport ciklikus- vagy diédercsoport, és ezekben meghatározzuk az elágazási pontok számát és az elágazási típust. Ehhez szükségünk lesz egy lemmára, ami a Hensel-lemma (2.1.5 Lemma) közvetlen következménye.

2.3.7. Lemma. Ha $g \in K[[t]]$ konstans a_0 tagja nem nulla, akkor minden n-re van n-edik gyöke $K[[t]]$-ben.

Bizonyítás. Nézzük a Hensel lemma (2.1.5 Lemma) jelöléseivel az $F(z) \in K[[t]][z]$, $F(z) = z^n - g$ polinomot: erre az $F_0(z) = z^n - a_0$ polinom szeparábilis és gyökténye zőkre bomlik K-ban (hiszen K algebrailag zárt), tehát $F(z)$-nek van gyöke $K[[t]]$-ben a Hensel-lemma miatt. □

2.3.8. Példa (Ciklikus csoportok)**.** Legyen Z_n az n-elemű ciklikus csoport. Legyen y transzcendens elem K felett, és $x = y^n$. Azt állítjuk, hogy ekkor $\mathrm{Gal}(K(y)/K(x))$ izomorf Z_n-nel. Ez algebrai bővítés, hiszen y algebrai $K(x)$ felett: gyöke az $f(z) \in K(x)[z]$, $f(z) = z^n - x$ polinomnak. Legyen $\varepsilon_n \in K$ primitív n-edik egységgyök. Ekkor $f(z)$ gyökei az $\varepsilon_n^i y$ alakú elemek. Tehát $f(z)$ a következő gyöktényezőkre bomlik $K(y)$ felett: $f(z) = (z-y)(z-\varepsilon_n y)...(z-\varepsilon_n^{n-1} y)$. Az $f(z)$ összes gyöke $K(y)$-ban van, emiatt $K(y)$ az $f(z)$ felbontási teste lesz, tehát Galois ([6] 2.9 Következmény). A Galois-csoportjában lévő elemek $f(z)$ gyökeit permutálják, tehát a következő $g_i : K(y) \to K(y), y \mapsto \varepsilon_n^i y$ elemek vannak benne, amelyek $K(x)$-et jól láthatóan fixen hagyják. Ha Z_n-et az n-nél kisebb számok csoportjának tekintjük a modulo n összeadásra, akkor az $i \mapsto g_i$ jól láthatóan izomorfizmus a két csoport között. Ezért a Galois-csoport Z_n.

Nézzük meg, hogy mik az elágazási pontok. Legyen $p \in \mathbb{P}^1_K$, és $p \neq 0$, $p \neq \infty$. Ki kell terjesztenünk a

$$\vartheta_p : K(x) \to K(t), x \mapsto t + p$$

izomorfizmust $K(y)$-ra. Tekintsük $\Lambda = K((t))$-t. A 2.3.7 lemma miatt Λ-ban van n-edik gyöke $t + p$-nek. Legyen ez a gyök γ. Ezek alapján a

$$\vartheta : K(y) \to \Lambda, y \mapsto \gamma$$

kiterjeszti ϑ_p-t, tehát a 2.2.3 állításban leírt Δ-nak választhatjuk Λ-t, vagyis $\mathrm{Gal}(\Delta/\Lambda)$ a triviális csoport. Ebből következik, hogy ω, vagyis a kitüntetett generátor az identitás, következményképp $g_\vartheta = \vartheta^{-1} \circ \omega \circ \vartheta = \mathrm{id}$, tehát az asszociált konjugáltosztály triviális. Világos, hogy ekkor az elágazási index $e_{K(y),p} = 1$, vagyis p nem lehet elágazási pont. Csak a 0 és a ∞ a lehetséges elágazási pontok. Nézzük a 0-t. A 2.2.3 állításban lévő Δ-nak ekkor tartalmaznia kell $t^{1/n}$-et, hiszen $\vartheta_p(x) = t$, tehát $\vartheta(y)^n = t$, vagyis $\Lambda_n \subseteq \Delta$, és emiatt $e_{K(y),0} \geq n$, de nem lehet nagyobb n-nél, hiszen n elemű a csoport. Ebből következik, hogy $e_{K(y),0} = n$. A ∞-t tekintve $\vartheta_\infty(x) = 1/t$, tehát $t^{-1/n} \in \Delta$, vagyis $t^{1/n} \in \Delta$, vagyis az előbbi

érveléshez hasonlóan $e_{K(y),\infty} = n$. Az is világos a 2.2.3 (b) pontja alapján, hogy $\Delta = \Lambda_n$ jó választás.

Végül megnézzük, hogy micsoda C_0 és C_∞. Tekintsünk egy rögzített kompatibilis egységgyök-rendszert K-ban. Legyen $\omega \in \mathrm{Gal}(\Lambda_n/\Lambda)$ a kitüntetett generátor, vagyis ($\Lambda_n = \Lambda(\delta)$, $\delta = \vartheta(y)$ mellett, ahol ϑ a 0-hoz készített kiterjesztés) $\omega(\delta) = \varepsilon_n\delta$. Ekkor, ha a 0-t nézzük, akkor $g_\vartheta(y) = \vartheta^{-1} \circ \omega \circ \vartheta(y) = \vartheta^{-1}(\varepsilon_n\delta) = \varepsilon_n y$. Ha a ∞-hez definiált ϑ-t nézzük, akkor $\vartheta(y) = \delta^{-1}$, vagyis $g_\vartheta(y) = \vartheta^{-1} \circ \omega \circ \vartheta(y) = \vartheta^{-1}(\varepsilon_n^{-1}\delta^{-1}) = \varepsilon_n^{-1}y$. Világos, hogy C_0 és C_∞ külön-külön lehet bármelyik generátorelemet tartalmazó egyelemű konjugáltosztály (hiszen Abel-csoportban vagyunk, és a generátorelemek szerepe Z_n-ben szimmetrikus), tehát az érdekes, hogy egymáshoz képest micsodák. A fenti érvelésből kiderült, hogy egymás inverzei, tehát a C_∞-ben lévő generátor az inverze a C_0-ban lévőnek. Ezzel meg is határoztuk az elágazási típust, hiszen ezen belül már bármely választás ekvivalens: két elágazási pont van, és az asszociált konjugáltosztályok 1-1 generátorból állnak, melyek egymás inverzei.

2.3.9. Példa (Diédercsoportok)**.** Legyen D_n az n-edik diédercsoport. Legyen y transzcendens K felett, és $x = (y^{2n}+1)/y^n$. Azt állítjuk, hogy ekkor a Galois-csoport D_n. Vegyük az $f(z) \in K(x)[z]$, $f(z) = z^{2n} - xz^n + 1$ polinomot. Ennek gyöke y. Könnyű ellenőrizni, hogy ez $K(y)$ felett gyöktényezőkre bomlik: $f(z) = (z-y)(z-\varepsilon_n y)...(z-\varepsilon_n^{n-1}y)(z-y^{-1})(z-\varepsilon_n y^{-1})...(z-\varepsilon_n^{n-1}y^{-1})$. Ez azért van így, mert a fentiek mind gyökei $f(z)$-nek, és páronként különböznek. Ez azt jelenti, hogy $K(y)$ a felbontási teste $f(z)$ polinomnak (világos, hogy $f(z)$ minden gyöke benne van), tehát Galois ([6] 2.9 Következmény). Vegyük ismét a D_n-nek a következő reprezentációját: $D_n = \langle a, b | a^2 = 1, b^n = 1, aba^{-1} = b^{-1}\rangle$. Ezt beágyazzuk a Galois-csoportba úgy, hogy: $a \mapsto g_a$, ahol $g_a(y) = y^{-1}$, és $b \mapsto g_b$, ahol $g_b(y) = \varepsilon_n y$. A relációk teljesülnek, hiszen $g_a^2(y) = y$, $g_b^n(y) = y$, és $g_a \circ g_b \circ g_a^{-1}(y) = g_a \circ g_b(y^{-1}) = g_a(\varepsilon_n^{-1}y^{-1}) = \varepsilon_n^{-1}y = g_b^{-1}(y)$. Ezenkívül bijektív is, hiszen könnyű látni, hogy megkapjuk az összes olyan leképezést, ami y-t elviszi $f(z)$ egy gyökébe, és ez elég, mert a Galois-csoport, és D_n egyaránt $2n$ elemű.

Nézzük az elágazási pontokat. Legyen $p \in K$. Az y-nak a ϑ_p általi képe olyan elem kell, hogy legyen, amely gyöke a minimálpolinom ϑ_p általi képének (vagyis annak a polinomnak, amelyet úgy kapunk a minimálpolinomból, hogy az együtthatóit kicseréljük a ϑ_p általi képükre). A minimálpolinom képe $z^{2n} - (t+p)z^n + 1$. Belátom, hogy ha $p \neq \pm 2$, akkor ez gyöktényezőkre bomlik Λ-ban. Ehhez a Hensel-lemma (2.1.5 Lemma) alapján elég belátni, hogy $z^{2n} - pz^n + 1$ különböző gyöktényezőkre bomlik K felett. Ha ezt z^n polinomjaként nézzük, akkor a diszkrimináns $4-p^2$, tehát nem nulla, vagyis van két megoldás, amelyeknek az n-edik hatványa különböző. Ezek legyenek a és b. Ha ε_n primitív n-edik egységgyök, akkor $a \neq \varepsilon_n^i b$ semmilyen i-re sem, hiszen akkor megegyezne a és b n-edik hatványa. Ezek szerint tehát a minimálpolinom képe gyöktényezőkre bomlik, hiszen van $2n$ darab különböző gyöke: $a, \varepsilon_n a, ..., \varepsilon_n^{n-1}a, b, \varepsilon_n b, ..., \varepsilon_n^{n-1}b$. Az első esettel analóg érvelés miatt ha $p \in \mathbb{P}^1_K$, és $p \neq \pm 2$, $p \neq \infty$, akkor p nem elágazási pont.

Belátom, hogy a 2, a -2 és a ∞ elágazási pontok. Nézzünk egységgyökök egy rögzített kompatibilis rendszerét K-ban. Tekintsük a 2-t, és $\tau = t^{1/2}$ választással $\Lambda(\tau) = \Lambda_2$-t. Azt állítjuk, hogy a $\vartheta_2 : K(x) \to K(t), x \mapsto t+2$ hozzárendelést kiterjeszthetjük $\vartheta : K(y) \to \Lambda_2$ alakban, viszont $K(y) \to \Lambda$ alakban nem. Azt kell megmutatni, hogy a

$$p_1(z) = z^{2n} - (t+2)z^n + 1 = (z^n - \frac{t}{2} - 1)^2 - \frac{t^2}{4} - t$$

polinomnak van gyöke Λ_2-ben, ugyanis ezen polinom egyik gyöke lehet csak y képe.

Először is kell egy olyan elem $\gamma_1 \in \Lambda_2$ elem, amelynek négyzete $\frac{t^2}{4}+t$, hiszen ha γ_0 egy gyöke $p_1(z)$-nek, akkor $\gamma_0^n - \frac{t}{2} - 1$ pont ilyen lesz. Mivel $\frac{t^2}{4}+t = t(\frac{t}{4}+1)$, ezért először tekintsük $\frac{t}{4}+1$-et. A 2.3.7 lemma alapján $\frac{t}{4}+1$-nek Λ-ban is van gyöke, tehát egyrészt, mivel t gyöke τ, ezért van Λ_2-ben négyzetgyöke $\frac{t^2}{4}+t$-nek, másrészt Λ-ban nincs, hiszen ha lenne, akkor $\frac{t}{4}+1$ gyökével elosztva $t^{1/2} \in \Lambda$ adódna, ami ellentmondás. Ezzel beláttuk, hogy $e_{K(y),2} > 1$.

Ha γ_1-et $K((\tau))$-beli hatványsornak tekintjük, akkor a konstans tagja 0 (hiszen egy $K[[t]]$-beli elemet szoroztunk meg τ-val). Mivel γ_0-t úgy kapjuk meg, ha $\gamma_1+\frac{t}{2}+1$-ből n-edik gyököt vonunk, ezért a 2.3.7 lemma szerint elég ellenőrizni, hogy ennek a konstans tagja nem nulla (ha a lemmában kicseréljük t-t τ-ra). Márpedig a konstans tag 1, hiszen γ_1 konstans tagja 0. Ezzel megkaptuk az áhított $\vartheta : K(y) \to \Lambda_2$ kiterjesztést $y \mapsto \gamma_0$-val. Ezek alapján a $\mathrm{Gal}(\Delta/\Lambda)$ kitüntetett generátora másodrendű, vagyis g_ϑ legfeljebb másodrendű. Ez azt jelenti, hogy $e_{K(y),2} = 2$. Pontosan ugyanezzel a gondolatmenettel $e_{K(y),-2} = 2$. Vagyis, ha n páratlan, akkor $C_2 = C_{-2}$ a tükrözések konjugáltosztálya, hiszen csak a tükrözések a másodrendűek. Ha n páros, akkor D_n-ben három konjugáltosztály van, amely szóba jöhet: egyrészt, a csúcsokon átmenő tengelyre való tükrözésekből álló konjugáltosztály, másrészt az oldalakon átmenő tengelyre való tükrözésekből álló konjugáltosztály, harmadrészt a 180°-os forgatásból álló egyelemű osztály.

Tegyük fel, hogy n nem 2-hatvány. A 180°-os forgatás nem jöhet szóba, mert a 2.2.3 állítás (d) pontja alapján ha vesszük a $K(y^i) \leq K(y)$ résztestet, ahol i a legnagyobb 2-hatvány, ami osztja n-et, akkor C_2 a megszorítás homomorfizmus után C_2'-be megy, ahol C_2' a 2-höz asszociált konjugáltosztály a $\mathrm{Gal}(K(y^i)/K(x))$ csoportban, amely izomorf $D_{\frac{n}{i}}$-vel, ahol $\frac{n}{i}$ páratlan, vagyis C_2'-ben tükrözések vannak. Emiatt C_2 nem lehet a 180°-os forgatás osztálya, hiszen az a centrumban van, a tükrözések pedig nem (C_2-t írtunk, de C_{-2}-re ugyanígy igaz). Ha n 2-hatvány, akkor sem lehet sem C_2, sem C_{-2} a 180°-os forgatás, ekkor szintén a $G' = \mathrm{Gal}(K(y^n)/K(x))$-re szorítjuk meg G-t, és itt C_2' és C_{-2}' a nemtriviális elemből áll, hiszen G' ugyanúgy D_1-ként tekinthető (a kételemű csoportról van szó), és itt az a a nemtriviális elem, és a b triviális, tehát van benne egy "tükrözés" és az identitás. Mivel a $G \to G'$ megszorításnál a 180°-os forgatás az identitásba megy, szintén tükrözésekből kell állnia C_2-nek és C_{-2}-nek.

Világos ezek alapján, hogy C_2 és C_{-2} tükrözésekből áll. Azt kell megnézni, hogy megegyeznek-e. Definiáljuk a következő elemet G-ben minden $i \leq n$-re: $h_i(y) = \varepsilon_n^i y^{-1}$. Már definiáltuk $p_1(z)$-t a 2-höz, most definiáljuk a -2-höz $p_2(z)$-t: $p_2(z) = z^{2n} - (t-2)z^n + 1$. Világos, hogy ϑ_2 kiterjesztésénél y csak $p_1(z)$ gyökeibe, ϑ_{-2} kiterjesztésénél csak $p_2(z)$ gyökeibe mehet. Ezek felbomlanak Λ_2-ben a következő módon, ha n páros: $p_1(z) = q_1(z)q_2(z)$, ahol $q_1(z) = (z^n + \tau z^{\frac{n}{2}} - 1)$, és $q_2(z) = (z^n - \tau z^{\frac{n}{2}} - 1)$, továbbá $p_2(z) = q_3(z)q_4(z)$, ahol $q_3(z) = (z^n + \tau z^{\frac{n}{2}} + 1)$, és $q_2(z) = (z^n - \tau z^{\frac{n}{2}} + 1)$. Tudjuk, hogy $\mathrm{Gal}(\Lambda_2/\Lambda)$ kitüntetett generátora, vagyis ω elküldi τ-t $-\tau$-ba, tehát pontosan kicseréli q_1-et q_2-vel, és q_3-at q_4-gyel. Világos, hogy a h_i elemek pontosan a tükrözések, és páros, illetve páratlan i-k szerint választódik el a két konjugáltosztály. Be fogjuk látni, hogy ha i páratlan, akkor $h_i \notin C_2$, és ha j páros, akkor $h_j \notin C_{-2}$, és ez nyilván biztosítja, hogy $C_2 \neq C_{-2}$. Legyen i páratlan, és tekintsük h_i-t. Tegyük fel indirekt, hogy $h_i \in C_2$, vagyis létezik egy ϑ kiterjesztése ϑ_2-nek, amelyre $g_\vartheta(y) = \varepsilon_n^i y^{-1}$, vagyis $\vartheta^{-1} \circ \omega \circ \vartheta(y) = \varepsilon_n^i y^{-1}$. Világos, hogy mindkét oldalra alkalmazva ϑ-t, az adódik, hogy $\omega(\vartheta(y)) = \varepsilon_n^i \vartheta(y)^{-1}$. Láttuk, hogy ω megcseréli q_1 és q_2 gyökeit, tehát ha $\vartheta(y)$ gyöke az egyiknek, akkor $\omega(\vartheta(y))$ gyöke a másiknak. Tegyük fel, hogy $\vartheta(y)$ gyöke mond-

juk q_1-nek. Azt állítjuk, hogy ekkor $\varepsilon_n^i \vartheta(y)^{-1}$ is gyöke q_1-nek, és mivel p_1 szeparábilis, így nem lehet gyöke q_2-nek, tehát $\omega(\vartheta(y))$ nem gyöke q_2-nek, ami ellentmondás. Nézzük tehát (világos, hogy $(\varepsilon_n^i)^{\frac{n}{2}} = -1$): $q_1(\varepsilon_n^i \vartheta(y)^{-1}) = \vartheta(y)^{-n} - \tau\vartheta(y)^{-\frac{n}{2}} - 1 = -\vartheta(y)^{-n} q_1(\vartheta(y)) = 0$, vagyis megkaptuk az ellentmondást. Ugyanígy ellentmondást kapunk, ha feltesszük, hogy $\vartheta(y)$ gyöke q_2-nek. Emiatt $h_i \notin C_2$. Most legyen j páros, és tegyük fel indirekt, hogy $h_j \in C_{-2}$. Ez azt jelenti, hogy létezik olyan $\tilde{\vartheta}$ kiterjesztése ϑ_{-2}-nek, hogy $g_{\tilde{\vartheta}}(y) = \varepsilon_n^j y^{-1}$. Úgy, mint az előbb, ebből azt kapjuk, hogy $\omega(\tilde{\vartheta}(y)) = \varepsilon_n^j \tilde{\vartheta}(y)^{-1}$. Be fogjuk látni, hogy ha $\tilde{\vartheta}(y)$ gyöke q_3-nak, akkor $\varepsilon_n^j \tilde{\vartheta}(y)^{-1}$ is, ami ellentmondás, hiszen $\omega(\tilde{\vartheta}(y))$ ekkor q_4 gyöke kell, hogy legyen. Tegyük fel tehát, hogy $q_3(\tilde{\vartheta}(y)) = 0$. Ekkor, mivel $(\varepsilon_n^j)^{\frac{n}{2}} = 1$, ezért $q_3(\varepsilon_n^j \tilde{\vartheta}(y)^{-1}) = \tilde{\vartheta}(y)^{-n} + \tau\tilde{\vartheta}(y)^{\frac{n}{2}} + 1 = \tilde{\vartheta}(y)^{-n} q_3(\tilde{\vartheta}(y)) = 0$. Ugyanígy $\tilde{\vartheta}(y)$ nem lehet gyöke q_4-nek sem. Ebből következik, hogy $C_2 \neq C_{-2}$.

Most következik a ∞. A $\vartheta_\infty : K(x) \to K(t), x \mapsto 1/t$ leképezést kell kiterjeszteni. A kiterjesztésben y képe a minimálpolinom képének, vagyis

$$r(z) = z^{2n} - \frac{1}{t} z^n + 1 = \left(z^n - \frac{1}{2t} \right)^2 - \frac{1}{4t^2} + 1$$

polinomnak az egyik gyöke. Ezt a gyököt γ_2-vel fogjuk jelölni anélkül, hogy tudnánk, mi az.

Legyen γ_3 a négyzetgyöke a $\frac{1}{4t^2} - 1 = t^{-2}(\frac{1}{4} - t^2)$-nek Λ-ben (ilyen van, ugyanis a t^{-2}-nek négyzetgyöke t^{-1}, és a másik tényezőnek a 2.3.7 lemma van egy γ_4 négyzetgyöke). Tehát $\gamma_3 = \gamma_4 \cdot t^{-1}$. Úgy fogjuk megkapni γ_2-t, hogy n-edik gyököt vonunk $\gamma_3 + \frac{1}{2t} = t^{-1}(\gamma_4 + \frac{1}{2})$-ből. Mivel γ_4 konstans tagja választható $1/2$-nek (világos, hogy $\pm\frac{1}{2}$ a konstans tag, és ha $-\frac{1}{2}$ lenne, akkor $-\gamma_4$ is jó választás), ezért a $\gamma_4 + \frac{1}{2}$-ből tudunk n-edik gyököt vonni $K[[t]]$-ben a 2.3.7 lemma alapján. Tehát a keresett kifejezésnek pontosan akkor van n-edik gyöke, ha t^{-1}-nek van, vagyis ha t-nek van. Ezek alapján tehát $\Delta = \Lambda(t^{1/n}) = \Lambda_n$. Ebből következik, hogy $e_{K(y),\infty} = n$, tehát C_∞ egy n-edrendű forgatásból és az inverzéből áll.

Ezzel meghatároztuk az elágazási típust: 3 elágazási pont van, és páratlan n esetén a 3 konjugáltosztályból kettő a tükrözések osztálya, a harmadik egy n-edrendű forgatásból és az inverzéből áll, páros n esetén megkapjuk mindkét tükrözésekből álló konjugáltosztályt, és szintén egy n-edrendű forgatást és az inverzét. Ezen belül bármely választás ekvivalens, hiszen az n-edrendű forgatások szerepe szimmetrikus a tükrözésekre nézve.

3. Riemann egzisztenciatétele

A merevségi kritérium használatához elengedhetetlen Riemann egzisztenciatétele, mostantól rövidítve RET. Ez a név számos különböző, de kapcsolatban álló eredményt takar, nekünk az algebrai változatra lesz szükségünk. A fejezet fő célja ennek belátása. A probléma azonban az, hogy ennek nem ismert tisztán algebrai bizonyítása, ezért távolabbról kell indulnunk. Az első két alfejezetben kimondjuk az analitikus és a topologikus változatot. A harmadik és negyedik alfejezetben ezekből levezetjük a számunkra szükséges formáját a tételnek.

3.1. Az Analitikus Verzió

A tétel analitikus verziójának kimondásához szükség lesz néhány definícióra.

3.1.1. Definíció (Komplex differenciálható struktúra)**.** Legyen Y topologikus tér. Ezen térképnek nevezünk egy (V, φ) párt, ha $V \subseteq Y$ nyílt részhalmaz és $\varphi : V \to U$ egy homeomorfizmus, ahol $U \subseteq \mathbb{C}$. (V_1, φ_1) és (V_2, φ_2) térképeket kompatibilisnek hívjuk, ha $\varphi_1 \circ \varphi_2^{-1} : \varphi_2(V_1 \cap V_2) \to \varphi_1(V_1 \cap V_2)$ biholomorf (vagyis holomorf, bijektív és az inverze is holomorf). Atlasznak nevezünk egy $\{(V_i, \varphi_i) : i \in I\}$ térképekből álló halmazt, ha a benne lévő térképek kompatibilisek és $\bigcup_{i \in I} V_i = Y$. Két atlasz ekvivalens, ha az uniójuk is atlasz. Y-on komplex differenciálható struktúrának nevezzük atlaszok egy ekvivalenciaosztályát.

3.1.2. Definíció (Riemann-felület)**.** Legyen Y összefüggő Hausdorff-tér. Ekkor Y-t egy komplex differenciálható struktúrával Riemann-felületnek nevezzük.

3.1.3. Definíció (Analitikus leképezés)**.** Legyen Y és Z két Riemann-felület, és $f : Y \to Z$ folytonos leképezés. Tegyük fel, hogy minden (V, φ) térképre Y-on és minden (V', φ') térképre Z-n, amelyekre igaz, hogy $f(V) \subseteq V'$, teljesül, hogy $\varphi' f \varphi^{-1} : \varphi(V) \to \varphi'(V')$ holomorf. Ekkor f-et analitikusnak nevezzük.

3.1.4. Definíció (Meromorf függvény)**.** Legyen Y Riemann-felület. Ekkor egy $f : Y \to \mathbb{P}^1_{\mathbb{C}}$ analitikus leképezést meromorf függvénynek nevezünk, ha nem konstans ∞. Az összes meromorf függvény halmazát Y-on $\mathcal{M}(Y)$-nal jelöljük.

3.1.5. Állítás. $\mathcal{M}(Y)$ test a pontonkénti szorzásra és összeadásra, mint műveletre nézve.

Bizonyítás. Ha $f, g \in \mathcal{M}(Y)$, akkor először definiáljuk $f \pm g$-t és $f \cdot g$-t azokon a pontokon, amelyek nem pólusok, ez értelemszerű. Minden pólus körül vehetünk egy térképet, és azon tekintve a függvény Laurent-sorba fejthető a pólus körül. A Laurent-sorokat összeadva, kivonva és szorozva $f \pm g$ és $f \cdot g$ egyértelműen kiterjed meromorf függvénnyé a pólusokra. Már csak a szorzásra vett inverz létezése hiányzik. Vegyünk egy tetszőleges $f \in \mathcal{M}(Y)$ függvényt. Azon pontok halmaza, amelyek egy környezetében f eltűnik, értelemszerűen nyílt. Ennek komplementere belátjuk, hogy szintén nyílt. Vegyünk egy pontot ebből a komplementerből, vagyis egy olyan pontot amelynek környezetében torlódnak azon pontok, ahol a függvény nem 0, és indirekt tegyük fel, hogy torlódnak a környezetében a nullhelyek is. Vegyünk a pontunk körül egy (V, φ) térképet. Ekkor a térképen tekintve a függvényt, azt látjuk, hogy a komplex síkon egy tartományon értelmezett függvény nullhelyei torlódnak. Ez a hatványsorokra vonatkozó unicitás tétel ([3] 24. oldal) miatt azt jelenti, hogy $f|_V \equiv 0$, vagyis a pont egy környezetében a függvény konstans nulla, ami ellentmond a feltevésünknek.

Tehát ha van olyan pont, amelynek környezetében f eltűnik, akkor $f \equiv 0$, hiszen az összes ilyen pont Y-ban nyílt és zárt halmazt alkot egyszerre, tehát Y összefüggő volta miatt ez vagy az egész Y, vagy az üres halmaz. Tehát, ha $f \neq 0$, akkor f lokálisan $(z-a)^n g(z)$ alakban írható fel, ahol $g(z)$-nek nincsen sem nullhelye, sem pólusa. Így világos, hogy $1/f$-et hogy definiáljuk, és f nullhelyein pólusa, f pólusain nullhelye lesz, és így $1/f$ meromorf függvény Y-on. □

Így már kimondható az analitikus változat. A bizonyítás megtalálható például [19] 6. fejezetében.

3.1.6. Tétel (RET − Az Analitikus Verzió)**.** Legyen Y kompakt Riemann-felület. Ekkor bármely $a_1, a_2, ..., a_n \in Y$ különböző pontokra és $c_1, c_2, ..., c_n$ komplex számokra létezik egy f meromorf függvény Y-on, amelyre $f(a_i) = c_i$, ha $i = 1, 2, ..., n$.

3.1.7. Megjegyzés. ([10] alapján) Riemann eredetileg a Riemann felületekkel (ahogy ma hívjuk őket) kapcsolatos úttörő kutatásai során fedezte fel a tételt. Ez az eredmény sokáig vitákat generált, hiszen az eredeti bizonyítás felhasználta az akkor még nem bizonyított Dirichlet-elvet. Hilbert ezt később belátta, teljessé téve a bizonyítást. A RET-nek számos formája van, és kapcsolódik a matematika sok területéhez: komplex függvénytanhoz, a topológiához, az algebrai geometriához és a számelmélethez.

Riemann úgy fedezte fel az egzisztenciatételt, hogy a Riemann-gömbön értelmezett többértékű függvényeket egy Riemann-felületen értelmezett egyértékű függvényként definiálta. A felületet így többértékű függvények értelmezési tartományainak összességeként definiálta, tehát ebből már adódott egy nem konstans meromorf függvény, ami definiált egy fedő leképezést. Ez később motiválta az absztrakt Riemann-felületek kutatását.

Az alfejezetet egy komplex polinomokról szóló tétellel zárjuk, amelyet később használni fogunk; ez kijön az implicitfüggvény tétel komplex változatából is, de a [19] könyvben megtalálható egy teljes bizonyítás (1.18).

3.1.8. Tétel. Legyen $f(x, y) \in \mathbb{C}[x, y]$ egy y-ban n-edfokú polinom. Legyen $c_0 \in \mathbb{C}$ olyan, hogy $f(c_0, y) \in \mathbb{C}[y]$ szeparábilis és n-edfokú. Ekkor léteznek c_0-nak egy U környezetén értelmezett $\psi_1, \psi_2, ..., \psi_n$ holomorf függvények, amelyekre teljesül, hogy bármely $c \in U$-ra $f(c, y) \in \mathbb{C}[y]$-nak n különböző gyöke van, és ezek $\psi_1(c), \psi_2(c), ..., \psi_n(c)$.

3.2. A Topologikus Verzió

Ahhoz, hogy majd levezethessük az algebrai változatot, kell némi topologikus előkészület, ugyanis az algebrai elágazási típusoknak definiálni fogjuk topologikus analógjait. Az alábbi eredmények bizonyítással együtt [19] 4. fejezetében megtalálhatóak. Ebben a szakaszban szükség lesz a fedő leképezések ismeretére, az ehhez kapcsolódó definíciók és alaptételek szintén megtalálhatóak [19] 4. fejezetében, de benne vannak [1] 7.3. alfejezetében is.

3.2.1. Definíció (Fedő-transzformáció)**.** Legyenek R és S topologikus terek, és $f : R \to S$ fedő leképezés. Jelöljük $\mathrm{Deck}(f)$-fel azon $\alpha : R \to R$ homeomorfizmusok halmazát, amelyekre $f \circ \alpha = f$. Világos, hogy $\mathrm{Deck}(f)$ csoportot alkot a kompozícióra nézve. Ez a fedő-transzformációk csoportja, elemei a fedő-transzformációk.

3.2.2. Definíció (Galois-fedés)**.** Legyen $f : R \to S$ fedő leképezés. Ezt Galois-fedésnek nevezzük, ha R és S összefüggő, és $\mathrm{Deck}(f)$ tranzitívan hat az $f^{-1}(p)$ alakú halmazokon, ahol $p \in S$. Véges Galois-fedésnek hívjuk f-et, ha $\mathrm{Deck}(f)$ véges rendű.

3.2.3. Jelölés. A továbbiakban a következő jelöléseket használjuk:

(i) $\mathbb{K}(r) = \{z \in \mathbb{C} : 0 < |z| < r\}$, ahol $r > 0$.

(ii) $\mathbb{P}^1 := \mathbb{P}^1_{\mathbb{C}}$ ahol $\mathbb{P}^1_{\mathbb{C}}$ az előző fejezetben használt jelölés. Ehhez a továbbiakban egy topológiát is hozzáértünk, amelynek bázisnyílt halmazai a $D(p, r)$ alakú halmazok, ahol $D(p, r)$-et a következőképpen értelmezzük:

(iii) Ha $p \neq \infty$, akkor legyen $D(p, r) = \{z \in \mathbb{C} : |z - p| < r\}$. Ha $p = \infty$, akkor legyen $D(p, r) = \{z \in \mathbb{C} : |z| > \frac{1}{r}\} \cup \{\infty\}$.

A következő technikai állítások alapvető fontosságúak abban, hogy az algebrai RET-hez szükséges konstrukciók topológiai analógjait definiálni tudjuk.

3.2.4. Állítás. Legyen $f : E \to \mathbb{K}(r)$ n-rétű fedés (n véges), ahol E összefüggő.

(a) Ekkor $\exists \varphi : E \to \mathbb{K}(r^{1/n})$ homeomorfizmus, amire $\varphi(u)^n = f(u)$, ha $u \in E$. Ezt a továbbiakban úgy jelöljük, hogy $\varphi^n = f$. Továbbá φ egy n-edik egységgyökkel való szorzás erejéig egyértelmű, azaz ha φ és φ' is a fenti tulajdonsággal bír, akkor van olyan ε n-edik egységgyök, amelyre $\varphi' = \varepsilon\varphi$.

(b) $\mathrm{Deck}(f)$ az n-edrendű ciklikus csoport. Ebben van egy és csak egy σ elem a következő tulajdonsággal: bármely $\varphi : E \to \mathbb{K}(r^{1/n})$ homeomorfizmusra, melyre $\varphi^n = f$, teljesül, hogy $\varphi \circ \sigma^{-1} = \varepsilon_n\varphi$, ahol $\varepsilon_n = e^{\frac{2\pi i}{n}}$, és $i = \sqrt{-1}$ szimbolikus jelölés. Ez a σ generálja $\mathrm{Deck}(f)$-et.

3.2.5. Definíció ($\mathrm{Deck}(f)$ kitüntetett generátora)**.** Legyen $f : E \to \mathbb{K}(r)$ n-rétű fedés (n véges), ahol E összefüggő. Ekkor a 3.2.4 állítás (b) pontjában definiált σ elemet $\mathrm{Deck}(f)$ kitüntetett generátorának nevezzük.

3.2.6. Állítás. Legyen $P \subseteq \mathbb{P}^1$ véges halmaz, és legyen $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés. Rögzítsünk egy $p \in P$-t.

(a) Legyen $D = D(p, r)$, ahol r olyan, hogy $D \cap P = \{p\}$. Ezenkívül legyen $D^* = D \setminus \{p\} \subseteq \mathbb{P}^1 \setminus P$. Ha $p \neq \infty$, akkor legyen $\kappa_p : D^* \to \mathbb{K}(r)$ az a homeomorfizmus, amelyre $\kappa_p(z) = z - p$ minden $z \in D^*$-ra, ha pedig $p = \infty$, akkor $\kappa_p(z) = 1/z$ minden $z \in D^*$-ra. Tekintsük egy E összefüggőségi komponensét $f^{-1}(D^*)$-nak. Ekkor $f_E = \kappa_p \circ f|_E$ egy véges rétű fedő leképezés, amely E-ről $\mathbb{K}(r)$-re képez. Az ilyen E-ket a továbbiakban p feletti r szintű körszerű komponenseknek nevezzük.

(b) Legyen $0 < \hat{r} < r$. Ekkor minden p feletti r szintű E körszerű komponensre pontosan egy $\hat{E}$ p feletti $\hat{r}$ szintű körszerű komponens van, amelyre $\hat{E} \subseteq E$. Hasonlóképpen minden $\hat{E}$-hez egyértelműen van E, amelyre $\hat{E} \subseteq E$, így egyértelmű megfeleltetés van az r szintű és az $\hat{r}$ szintű p feletti körszerű komponensek között tartalmazással. Ha $\hat{E} \subseteq E$, akkor $f_{\hat{E}} = f_E|_{\hat{E}}$ és $\hat{E} = f_E^{-1}(\mathbb{K}(\hat{r}))$.

(c) A $H := \mathrm{Deck}(f)$ csoport tranzitívan permutálja $f^{-1}(D^*)$ összefüggőségi komponenseit. Ha E egy komponense $f^{-1}(D^*)$-nak, akkor legyen H_E a stabilizátora E-nek H-ban. Ha H_E hatását megszorítjuk E-re, akkor egy $H_E \to \mathrm{Deck}(f_E)$ izomorfizmust kapunk. Emiatt H_E ciklikus.

(d) Legyen $h_E \in H_E$ az az elem, amit az előző pontban definiált izomorfizmus $\mathrm{Deck}(f_E)$ kitüntetett generátorába képez. Legyen $h \in H$ és $E' = h(E)$. Ekkor $hh_Eh^{-1} = h_{E'}$. Emiatt a h_E alakú elemek egy konjugáltosztályt alkotnak H-ban, legyen ez C_p^{top}. Ez a konjugáltosztály csak p (és f) kiválasztásától függ, D-től nem. Legyen n a C_p^{top}-beli elemek közös rendje. Ekkor n megegyezik az $f_E : E \to \mathbb{K}(r)$ fedés rétegszámával bármely $E \subseteq f^{-1}(D^*)$ összefüggőségi komponensre. Speciálisan, $C_p^{\mathrm{top}} = \{1\}$ pontosan akkor, ha f_E homeomorfizmus.

3.2.7. Definíció (H_E kitüntetett generátora)**.** Legyen $P \subseteq \mathbb{P}^1$ véges halmaz, és legyen $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés. Rögzítsünk egy $p \in P$-t. Tekintsük a 3.2.6 állítás (c) részében definiált $H_E \to \mathrm{Deck}(f_E)$ izomorfizmust. Legyen $h_E \in H_E$ az az elem, amely ennél az izomorfizmusnál megfelel $\mathrm{Deck}(f_E)$ kitüntetett generátorának. Ezt a h_E elemet H_E kitüntetett generátorának nevezzük.

3.2.8. Definíció (H csoport p-hez asszociált konjugáltosztálya)**.** Legyen $P \subseteq \mathbb{P}^1$ véges halmaz, és legyen $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés. Rögzítsünk egy $p \in P$-t. Tekintsük a 3.2.6 állítás (d) részében definiált konjugáltosztályt. Ezt a H csoport p-hez asszociált konjugáltosztályának nevezzük és C_p^{top}-vel jelöljük.

3.2.9. Definíció (Ideális pont)**.** Legyen $P \subseteq \mathbb{P}^1$ véges halmaz, és legyen $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés. Azt mondjuk, hogy $r > 0$ megfelelően kicsi, ha minden $p \in P$-re $D(p, r) \cap P = \{p\}$. Rögzítsünk egy $p \in P$-t. Az E és $\hat{E}$ p feletti megfelelően kis szintű körszerű komponenseket (3.2.6 állítás (a) részében volt definiálva) ekvivalensnek nevezzük, ha $E \subseteq \hat{E}$ vagy $\hat{E} \subseteq E$, és ez szintén az említett állítás alapján ekvivalenciareláció. Az ekvivalenciaosztályokat R-nek a p fölötti ideális pontjainak nevezzük.

3.2.10. Állítás. Legyen $P \subseteq \mathbb{P}^1$ véges halmaz, és legyen $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés. Legyen $\bar{R}$ az R-nek és összes ideális pontjának diszjunkt uniója minden $p \in P$ felett. Ebben egy V részhalmaz nyílt, ha $V \cap R \subseteq R$ nyílt és minden $\pi \in V$ ideális pontra van olyan $E \in \pi$, hogy $E \subseteq V$. Ezzel a topológiával $\bar{R}$ összefüggő kompakt Haussdorff-tér. Ekkor f kiterjed egy folytonos szürjektív $\bar{f} : \bar{R} \to \mathbb{P}^1$ leképezéssé, amelyben $\bar{f}(\pi) = p$ minden π ideális pontra p felett. Továbbá minden $\alpha \in \mathrm{Deck}(f)$ egyértelműen kiterjed egy $\bar{\alpha} : \bar{R} \to \bar{R}$ homeomorfizmussá, ahol $\bar{f} \circ \bar{\alpha} = \bar{f}$.

3.2.11. Definíció (Elágazási típus)**.** Legyen $P \subseteq \mathbb{P}^1$ véges halmaz, és legyen $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés. Legyen $H = \mathrm{Deck}(f)$, és minden $p \in P$-re C_p^{top} a p-hez asszociált konjugáltosztály H-ban. Legyen $P' = \{p \in P : C_p \neq \{1\}\}$. Vegyük a 2.2.8 definícióban definiált ekvivalenciarelációt a $(G, P, \mathbf{C})$ hármasokon. Ekkor az f elágazási típusa a $(H, P', (C_p)_{p \in P'})$ hármas ekvivalenciaosztálya.

3.2.12. Tétel (RET − A Topologikus Verzió)**.** Legyen $\mathcal{T} = [G, P, (K_p)_{p \in P}]$ egy elágazási típus. Legyen $r = |P|$, és legyen $P = \{p_1, p_2, ..., p_r\}$. Ezen feltételek mellett pontosan akkor létezik olyan f Galois fedése $\mathbb{P}^1 \setminus P$-nek, amelynek elágazási típusa $\mathcal{T}$, ha léteznek olyan $g_1, g_2, ..., g_r \in G$ generátorok, amelyekre $g_1 \cdot g_2 \cdot ... \cdot g_r = 1$ és $g_i \in K_{p_i}$, ha $i = 1, 2, ..., r$.

3.2.13. Megjegyzés. A tételbeli ekvivalencia egyik irányánál kicsit több is igaz: ha $f : R \to \mathbb{P}^1 \setminus P$ egy véges Galois-fedés és $P' = \{p \in P : C_p \neq \{1\}\} = \{p_1, p_2, ..., p_r\}$, akkor léteznek $g_1, g_2, ..., g_r \in \mathrm{Deck}(f)$ generátorok, amelyekre $g_1 \cdot g_2 \cdot ... \cdot g_r = 1$ és $g_i \in C_{p_i}$, ha $i = 1, 2, ..., r$. Vagyis nem szükséges, hogy minden konjugáltosztály nemtriviális legyen.

3.3. Riemann-felületek

Az algebrai változat levezetéséhez szükségünk lesz néhány lemmára a Riemann-felületekről. A terv az lesz, hogy azonosítjuk egymással a véges Galois-fedések és a véges Galois-bővítések elágazási típusát. Ehhez kell majd az analitikus változat, viszont ehhez meg kell értenünk a Riemann-felületek bizonyos tulajdonságait.

3.3.1. Állítás. Legyen $P \subseteq \mathbb{P}^1$ véges részhalmaz, $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés, és $H = \mathrm{Deck}(f)$.

(a) Vegyük f által jóllefedett $U \subseteq \mathbb{P}^1 \setminus P$ nyílt részhalmazokat, amelyekre $\{0, \infty\} \not\subseteq U$. Most tekintsük az olyan V halmazokat, amelyekre teljesül, hogy V összefüggőségi komponense $f^{-1}(U)$-nak valamely U-ra. Ekkor $f|_V$ nyilván homeomorfizmus V és U között. Definiáljunk egy φ leképezést a következőképpen: legyen $\varphi := f|_V$, ha $\infty \notin U$, és $\varphi := 1/f|_V$, ha $\infty \in U$. Ekkor a (V, φ) térképek atlaszt alkotnak R-en, így R Riemann-felület. Továbbá $f : R \to \mathbb{P}^1$ is, illetve minden $\alpha \in H$-ra $\alpha : R \to R$ is analitikus leképezés.

(b) Tekintsük a 3.2.10 állításban definiált $\bar{R}$ teret és az $\bar{f} : \bar{R} \to \mathbb{P}^1$ kiterjesztését f-nek. Legyen π egy ideális pontja R-nek, és $p = \bar{f}(\pi)$. Ekkor minden $E \in \pi$-re $f_E = \kappa_p \circ f|_E : E \to \mathbb{K}(r)$ egy véges n-rétű fedés, ahol f_E és κ_p ugyanaz, mint a 3.2.6 állítás (a) részében volt. Továbbá létezik egy $\varphi : E \to \mathbb{K}(r^{1/n})$, amelyre $\varphi^n = f_E$, és ez kiterjed egy $\varphi_\pi : V_\pi \to \mathbb{K}(r^{1/n}) \cup \{0\}$ homeomorfizmussá, ahol $V_\pi = E \cup \{\pi\}$ és $\varphi_\pi(\pi) = 0$.

(c) A (V_π, φ_π) és (V, φ) térképek együttesen atlaszt alkotnak $\bar{R}$-en, ezzel $\bar{R}$ egy kompakt Riemann-felület. Továbbá $\bar{f} : \bar{R} \to \mathbb{P}^1$ analitikus, illetve minden $\alpha \in H$ egyértelműen kiterjed egy $\bar{\alpha} : \bar{R} \to \bar{R}$ analitikus homeomorfizmussá, amelyre $f \circ \bar{\alpha} = f$.

(d) Legyen $g \in \mathcal{M}(\bar{R})$, amelyre $g \circ \bar{\alpha} = g$ minden $\alpha \in H$-ra. Ekkor $g = g' \circ f$ valamely $g' \in \mathcal{M}(\mathbb{P}^1)$-re.

Bizonyítás. (a) Legyen (V_1, φ_1) és (V_2, φ_2) a fentiek közül két térkép. Ekkor $\varphi_1\varphi_2^{-1} : \varphi_2(V_1 \cap V_2) \to \varphi_1(V_1 \cap V_2)$ vagy az identitás, vagy pedig a $z \mapsto 1/z$ hozzárendeléssel definiált leképezés, vagyis biholomorf. A térképek tehát kompatibilisek, és nyilván lefedik R-et, vagyis atlaszt alkotnak R-en. A térképek által meghatározott lokális koordinátákban minden $\alpha \in H$-ra α az identitás lesz, f pedig vagy az identitás, vagy a $z \mapsto 1/z$ által megadott függvény, vagyis f és α minden $\alpha \in H$-ra analitikus.

(b) f_E véges n-rétű fedés a 3.2.6 állítás (a) és (d) részei miatt. A 3.2.4 állítás (a) része miatt létezik φ, amelyre $\varphi^n = f_E$. Végül φ_π homeomorfizmus, mivel π-nek az $\hat{E} \cup \{\pi\}$ alakú környezeteit (ezek környezetbázist alkotnak) φ megfelelteti a $D(0, \hat{r}^{1/n})$ alakú körlapoknak a 3.2.6 állítás (b) része miatt.

(c) Vegyünk egy (V_π, φ_π) alakú, és egy (V, φ) alakú térképet. Legyen $p = \bar{f}(\pi)$ és vegyük a 3.2.6 állítás (a) részében definiált κ_p függvényt. A (b) rész szerint $\varphi_\pi^n = f_E = \kappa_p \circ \bar{f}$ a $V \cap V_\pi$-n van értelmezve. Tekintsük a $\varphi\varphi_\pi^{-1} : \varphi_\pi(V \cap V_\pi) \to \varphi(V \cap V_\pi)$ függvényt. Amennyiben $\infty \notin f(V)$, akkor ezt a függvényt a $z \mapsto \kappa_p^{-1}(z^n)$, ha pedig $\infty \in f(V)$, akkor a $z \mapsto 1/\kappa_p^{-1}(z^n)$ hozzárendelés definiálja, hiszen például az első esetben $\varphi\varphi_\pi^{-1}(z) = \varphi(\bar{f}^{-1}(\kappa_p^{-1}(z^n))) = \kappa_p^{-1}(z^n)$. Mindkét esetben holomorf függvényt kapunk, tekintsük a deriváltat. Első esetben a derivált: $(\kappa_p^{-1})'(z^n) \cdot nz^{n-1}$, ami csak a nullában tűnhet el, de $0 \notin \varphi_\pi(V \cap V_\pi)$. Ugyanígy a második esetben sem tűnhet el a derivált. Az is igaz továbbá, hogy $\varphi\varphi_\pi^{-1}$ homeomorfizmus, hiszen φ és φ_π is az. Emiatt biholomorf, amiből következik (V_π, φ_π) és (V, φ) kompatibilitása. Ahhoz, hogy az állításban leírt térképek atlaszt alkotnak, már csak két (V_π, φ_π) alakú térképről kell belátni, hogy kompatibilis, hiszen a másik típusúakról már az (a) részben belláttuk. Legyen tehát (V_π, φ_π) és $(V'_{\pi'}, \varphi'_{\pi'})$ két ilyen térkép. Ha $\pi \neq \pi'$, akkor a metszetük lefedhető a (V, φ) alakú térképekkel. Emiatt feltehető, hogy $\pi = \pi'$. A 3.2.6 állítás (b) része miatt feltehetjük, hogy $V_\pi \subseteq V'_\pi$. Legyen $V_\pi = E \cup \{\pi\}$, ahol $E \in \pi$ r szintű. Ekkor a 3.2.4 állítás (a) része miatt a $\varphi'_\pi\varphi_\pi^{-1} : D(0, r^{1/n}) \to D(0, r^{1/n})$ függvény megegyezik valamely ε egységgyökkel való szorzással, tehát biholomorf. Ebből következik a kompatibilitás, vagyis beláttuk, hogy az állításban definiált térképek atlaszt alkotnak.

Azt, hogy $\bar{f} : \bar{R} \to \mathbb{P}^1$ analitikus, elég az ideális pontokra belátni, hiszen közönséges pontokra következik az (a) részből. Először is tegyük fel, hogy π ideális pont nem a ∞ felett van. Ekkor az $\bar{f}\varphi_\pi^{-1}$ függvény definiáló hozzárendelése a $z \mapsto \kappa_p^{-1}(z^n)$, vagyis $\bar{f}\varphi_\pi^{-1}$ analitikus $D(0, r^{1/n})$-en. Emiatt $\bar{f}$ analitikus π körül. Most tegyük fel, hogy π egy ∞ feletti ideális pont. Ekkor azt kell belátni, hogy $g \circ \bar{f}\varphi_\pi^{-1}$ analitikus $D(0, r^{1/n})$-en, ahol $g(z) = 1/z$. Ez teljesül, hiszen a $z \mapsto z^n$ függvényről van szó. Ebben az esetben $\bar{f}$ szintén analitikus π körül. Beláttuk tehát, hogy $\bar{f}$ analitikus. Tekintsünk most egy $\alpha \in H$-t. A 3.2.10 állításból tudjuk, hogy minden ilyen α egyértelműen kiterjeszthető egy $\bar{\alpha} : \bar{R} \to \bar{R}$ homeomorfizmussá, amelyre $\bar{f}\bar{\alpha} = \bar{f}$. Az (a) részből tudjuk, hogy α analitikus R-en. Vegyünk tehát egy π ideális pontot és körülötte egy (V_π, φ_π) térképet. Ekkor $(\bar{\alpha}(V_\pi), \varphi_\pi \circ \bar{\alpha}^{-1})$ is egy ilyen térkép. Ebben a lokális koordinátarendszerben $\bar{\alpha}$ egy ε egységgyökkel való szorzás, vagyis analitikus. Emiatt $\bar{\alpha}$ analitikus.

(d) Nyilván $\bar{\alpha}$ ($\alpha \in H$) elemek egy H-val izomorf csoportot alkotnak a kompozícióra nézve egy olyan izomorfizmussal, amely $\bar{\alpha}$-t α-ba küldi. Ezzel H-t azonosítottuk analitikus izomorfizmusok (vagyis analitikus homeomorfizmusok, melyeknek inverze is analitikus) egy csoportjával $\bar{R}$-en. Ez a csoport tranzitívan hat az $f^{-1}(p)$ alakú halmazokon, ahol $p \in \mathbb{P}^1$. Ez a Galois-fedés definíciójából következik $p \notin P$ esetén. Most belátjuk $p \in P$-re. Tekintsük a 3.2.6 állításban definiált D^*-ot, ekkor a a p feletti ideális pontok $f^{-1}(D^*)$ összefüggőségi komponenseinek felelnek meg. Ezeken a komponenseken a 3.2.6 állítás (c) része miatt H tranzitívan hat. Ezzel beláttuk azt, hogy a fenti csoport tranzitívan hat $f^{-1}(p)$-n minden $p \in \mathbb{P}^1$-re. Emiatt g ugyanazt az értéket veszi fel $f^{-1}(p)$ pontjain, legyen ez az érték $g'(p)$. Ha $U \subseteq \mathbb{P}^1 \setminus (P \cup \{\infty\})$ jóllefedett f által, és V egy összefüggőségi komponense $f^{-1}(U)$-nak, akkor világos, hogy $g'|_U = g \circ (f|_V)^{-1}$. Ez meromorf, hiszen hiszen f és g is analitikus. Ezt minden U jóllefedett környezetre elmondva adódik, hogy g' meromorf a $\mathbb{P}^1 \setminus (P \cup \{\infty\})$ halmazon. Az nyilvánvaló, hogy g' folytonos a $\mathbb{P}^1 \setminus (P \cup \{\infty\})$ pontjaiban. Ekkor viszont ezek a pontok mind megszüntethető szingularitások, tehát g' meromorf. □

3.4. Az Algebrai Verzió

Most már kimondható az alábbi kulcsfontosságú tétel. Ez segíteni fog abban, hogy az algebrai és a topológiai elágazási típusokat azonosítani tudjuk egymással. Az algebrai változat egyik iránya ebből következik majd.

3.4.1. Tétel. Legyen P véges részhalmaza $\mathbb{P}^1$-nek, és $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés. Legyen $\bar{f} : \bar{R} \to \mathbb{P}^1$ a 3.2.10 állításban konstruált kiterjesztés. Tekintsük $H = \mathrm{Deck}(f)$-t úgy, mint analitikus izomorfizmusok egy csoportja $\bar{R}$-en, a 3.3.1 állítás (d) részének bizonyításához hasonlóan (az $\bar{\alpha}$ elemekből álló csoportról van szó, de egyszerűsítve csak α-t fogunk írni). Legyen $\mathbb{C}(\bar{f}) \leq \mathcal{M}(\bar{R})$ az a résztest, amelyet $\bar{f}$ és a konstans komplex értékű függvények generálnak.

(a) Minden $\alpha \in H$-ra legyen $\iota_\alpha : \mathcal{M}(\bar{R}) \to \mathcal{M}(\bar{R})$ az a függvény, amelyet a $g \mapsto g \circ \alpha^{-1}$ hozzárendelés definiál. Ekkor minden $\alpha \in H$-ra ι_α automorfizmusa $\mathcal{M}(\bar{R})$-nek. Ezenkívül az is teljesül, hogy $\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f})$ Galois-bővítés, és az $\alpha \mapsto \iota_\alpha$ által meghatározott $\iota : H \to \mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f}))$ leképezés izomorfizmus.

(b) Minden $p \in P$ elemhez legyen C_p^{top} a hozzá asszociált konjugáltosztály $H = \mathrm{Deck}(f)$-ben (3.2.8 Definíció), C_p^{alg} pedig a p-hez asszociált konjugáltosztály $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f}))$-ben az algebrailag definiált módon (2.2.4 Definíció) $x = \bar{f}$ értelmezéssel. Ekkor, ha $p \notin P$, akkor $C_p^{\mathrm{alg}} = \{1\}$. Minden $p \in P$-re a $\iota : H \to \mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f}))$ izomorfizmus C_p^{top} konjugáltosztályt C_p^{alg}-ra képezi. Ez egy megfeleltetést ad az $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés topologikus elágazási típusa és az $\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f})$ véges Galois-bővítés algebrai elágazási típusa között.

Bizonyítás. (a) A ι_α jóldefiniált, hiszen $g \in \mathcal{M}(\bar{R})$-re $g \circ \alpha^{-1} \in \mathcal{M}(\bar{R})$, hiszen α analitikus izomorfizmus $\bar{R}$-en. Világos, hogy automorfizmus. Triviális, hogy $\iota_\alpha(\bar{f}) = \bar{f}$, hiszen α fedőtranszformáció, tehát $\mathbb{C}(\bar{f})$-re megszorítva az identitás lesz. Szintén világos, hogy $\iota_{\alpha\beta} = \iota_\alpha \iota_\beta$, tehát ι egy homomorfizmus H-ról $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f}))$ egy G részcsoportjára. A G csoport fixteste olyan $g \in \mathcal{M}(\bar{R})$ elemekből áll, amelyekre $g \circ \alpha = g$ minden $\alpha \in H$-ra. A 3.3.1 állítás (d) része alapján minden ilyen g-re $g = g' \circ \bar{f}$ valamely $g' \in \mathcal{M}(\mathbb{P}^1)$-re. Ha tudnánk, hogy

$$\mathcal{M}(\mathbb{P}^1) = \mathbb{C}(z),$$

akkor ebből következne, hogy $g \in \mathbb{C}(\bar{f})$. Be kell látni tehát, hogy $\mathcal{M}(\mathbb{P}^1) = \mathbb{C}(z)$. Mivel az identitás $\mathbb{P}^1$-en, vagyis a racionális törtfüggvényként z-ként jelölt leképezés meromorf, ezért minden komplex együtthetós racionális törtfüggvény is az, hiszen $\mathcal{M}(\mathbb{P}^1)$ test, tehát $\mathbb{C}(z) \leq \mathcal{M}(\mathbb{P}^1)$. A másik irány belátásához vegyünk egy tetszőleges $h \in \mathcal{M}(\mathbb{P}^1)$ függvényt. Mivel $\mathbb{P}^1$ kompakt, ezért csak véges sok izolált szingularitása lehet, hiszen különben az izolált szingularitásoknak lenne torlódási pontja. Ezek legfeljebb pólusok lehetnek, hiszen meromorf függvényről van szó. Nevezzük el a pólusokat $p_1, p_2, ..., p_s$-nek. Feltehető, hogy a ∞ nincs a pólusok között, mert ha mégis, akkor h helyett nézhetjük $1/h$-t. Ha $i = 1, ..., s$, akkor legyen h Laurent sora p_i körül $\sum_{n=N}^{\infty} a_n(z - p_i)^n$, ahol $N < 0$. Legyen $h_i(z) = \sum_{n=N}^{-1} a_n(z - p_i)^n$. Világos, hogy $h_i \in \mathbb{C}(z)$, és h_i egyetlen pólusa p_i-ben van, továbbá $h - h_i$-nek nincs pólusa p_i-ben. Ekkor $h_0 = h - \sum_{i=1}^{s} h_i$ meromorf függvény $\mathbb{P}^1$-en, és nincs pólusa, tehát ha megszorítjuk $\mathbb{C}$-re, akkor korlátos holomorf függvény lesz, vagyis Liouville

tétele ([3] 28. oldal) miatt konstans. Tehát $h = h_0 + \sum_{i=1}^{s} h_i \in \mathbb{C}(z)$, vagyis $\mathcal{M}(\mathbb{P}^1) \leq \mathbb{C}(z)$, tehát a másik irány is megvan. Beláttuk tehát, hogy $g \in \mathbb{C}(\bar{f})$.

Ebből következik, hogy G csoport fixteste $\mathcal{M}(\bar{R})$-ben $\mathbb{C}(\bar{f})$. Emiatt Artin tétele (2.1.1 Tétel) szerint $\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f})$ Galois-bővítés, melynek Galois-csoportja G. Már csak $\iota : H \to G$ injektivitása hiányzik. Ehhez Riemann egzisztenciatételének analitikus változatát használjuk. Legyen $\alpha \in H$ olyan, hogy $\iota_\alpha = \mathrm{id}$. Az injektivitáshoz azt kell belátni, hogy ekkor $\alpha = \mathrm{id}$. Legyen $a \in \bar{R}$ és $p = f(a)$. Ekkor $a, \alpha(a) \in f^{-1}(p)$. A RET analitikus verziója (3.1.6 Tétel) alapján létezik $g_0 \in \mathcal{M}(\bar{R})$, amely $f^{-1}(p)$ halmaz elemein különböző értékeket vesz fel, mivel $f^{-1}(p)$ véges halmaz (hiszen f véges Galois-fedés). Tehát $g_0(\alpha(a)) = \iota_\alpha(g_0)(\alpha(a)) = g_0(\alpha^{-1}(\alpha(a))) = g_0(a)$, vagyis $\alpha(a) = a$. Tehát α valóban az identitás. Ez bizonyítja, hogy ι injektív.

(b) A második fejezethez hasonlóan jelöljük Λ-val $\mathbb{C}((t))$-t, vagyis a formális Laurent-sorok testét $\mathbb{C}$ felett. Valójában két állítás van megfogalmazva.

Az első állítás $\mathbb{P}^1 \setminus P$ elemeire vonatkozik, tehát legyen $p \in \mathbb{P}^1 \setminus P$, és $v \in \bar{f}^{-1}(p)$. Ekkor létezik (V, φ) térkép, ami egyrészt olyan, mint amit a 3.3.1 állítás (a) részében leírtunk, másrészt $v \in V$. Ha $p \neq \infty$, akkor feltehető, hogy $\infty \notin \varphi(V)$ (hiszen V-nek tudjuk egy megfelelő részhalmazát venni), és az is, hogy $\varphi = \bar{f}|_V$, hiszen f meromorf, és egy jóllefedett környezetre megszorítva homeomorfizmus. Ha $p = \infty$, akkor feltehető, hogy $\varphi = 1/(\bar{f}|_V)$. Minden $g \in \mathcal{M}(\bar{R})$ Laurent-sorba fejthető v körül (világos, hogy lokális koordinátákban egy Riemann felületen Laurent-sorba fejthető egy függvény, hiszen az olyan, mintha egy $\mathbb{P}^1$-en értelmezett függvényünk lenne):

$$g = \sum_{i=N}^{\infty} a_i(\varphi - \varphi(v))^i.$$

Így létre tudunk hozni egy $\vartheta : \mathcal{M}(\bar{R}) \to \Lambda$ gyűrűhomomorfizmust, amelynél $g \mapsto \sum_{i=N}^{\infty} a_i t^i$. Mivel ez nemnulla, ezért injektív (hiszen két testről van szó), tehát beágyazás. Ha $p \neq \infty$, akkor $\bar{f} = \varphi = p + (\varphi - \varphi(v))$ megszorítva V-re, tehát $\vartheta(\bar{f}) = p + t$. Ha $p = \infty$, akkor $\bar{f} = 1/\varphi = 1/(\varphi - \varphi(v))$ megszorítva V-re, tehát $\vartheta(\bar{f}) = 1/t$. Emiatt ϑ kiterjesztése a 2.2.3 állításbeli $\vartheta_p : \mathbb{C}(\bar{f}) \to \mathbb{C}(t)$ leképezésnek (az állításbeli x helyett $\bar{f}$-re). Ezenkívül az említett állításbeli Δ-t vehetjük Λ-nak, tehát $\omega = \mathrm{id}$, tehát $g_\vartheta = \mathrm{id}$, tehát valóban $C_p^{\mathrm{alg}} = \{1\}$.

A másik állítás P elemeiről szól, tehát legyen mostantól $p \in P$, és $\pi \in f^{-1}(p)$ egy ideális pont. Legyen (V_π, φ_π) egy térkép π körül a 3.3.1 állítás alapján, vagyis $V_\pi = E \cup \{\pi\}$ és $\varphi_\pi^n = \kappa_p \circ \bar{f}$ V_π-n. Minden $g \in \mathcal{M}(\bar{R})$ Laurent-sorba fejthető π körül:

$$g = \sum_{i=N}^{\infty} b_i \varphi_\pi^i.$$

Ekkor a $\vartheta : \mathcal{M}(\bar{R}) \to \Lambda_n = \mathbb{C}((\tau))$ gyűrűhomomorfizmus, amit $g \mapsto \sum_{i=N}^{\infty} b_i \tau^i$ határoz meg (Λ_n és τ ugyanaz, mint a 2.1.6 jelölésben), ismét beágyazás. Szintén a 2.1.6 jelöléshez hasonlóan Λ-t Λ_n résztestének tekintjük. Abból, hogy $\varphi_\pi^n = \kappa_p \circ \bar{f}$, kapjuk, hogy $p \neq \infty$ esetén $\bar{f} = \kappa_p^{-1} \circ \varphi_\pi^n = p + \varphi_\pi^n$, tehát $\vartheta(\bar{f}) = p + \tau^n = p + t$, és $p = \infty$ esetén $f = 1/\varphi_\pi^n$, tehát $\vartheta(\bar{f}) = 1/\tau^n = 1/t$. Ez alapján ϑ megintcsak kiterjesztése a 2.2.3 állításbeli $\vartheta_p : \mathbb{C}(\bar{f}) \to \mathbb{C}(t)$-nek, és ezúttal az állításban leírt Δ ezúttal választható Λ_n-nek. Legyen ω a kitüntetett generátora $\mathrm{Gal}(\Lambda_n/\Lambda)$-nak (2.2.1 Jelölés). Definíció szerint $\vartheta^{-1} \circ \omega \circ \vartheta \in C_p^{\mathrm{alg}}$, ezenkívül

szintén definíció szerint $h_E \in C_p^{\text{top}}$, ahol h_E a kitüntetett generátora E stabilizátorának H-ban (3.2.7 Definíció). Ha belátnánk, hogy $\iota(h_E) = \vartheta^{-1} \circ \omega \circ \vartheta$, abból következne az állítás, tehát ez van még hátra. Definíció szerint h_E fixen hagyja E-t, tehát V_π-t is, és az $f_E = \kappa_p \circ f : E \to \mathbb{K}(r)$ fedés kitüntetett generátorát indukálja. A 3.2.4 állítás (b) része miatt $\varphi_\pi \circ h_E^{-1} = \varepsilon_n \varphi_\pi$, hiszen E-n $\varphi_\pi^n = f_E$. Legyen most $g \in \mathcal{M}(\bar{R})$. Az eddigiek alapján π egy környezetében. $\iota(h_E)(g) = g \circ h_E^{-1} = \sum_{i=N}^{\infty} b_i (\varphi_\pi \circ h_E^{-1})^i = \sum_{i=N}^{\infty} b_i (\varepsilon_n \varphi_\pi)^i = \sum_{i=N}^{\infty} (b_i \varepsilon_n^i) \varphi_\pi^i$. Ezenkívül a 2.1.7 lemma alapján

$$\omega\Big(\sum_{i=N}^{\infty} b_i \tau^i\Big) = \sum_{i=N}^{\infty} (b_i \varepsilon_n^i) \tau^i.$$

Ebből következik tehát, hogy

$$\iota(h_E) = \vartheta^{-1} \circ \omega \circ \vartheta.$$

Ebből világos, hogy ι ráképezi C_p^{top}-ot C_p^{alg}-ra. □

Az előző tétel biztosította, hogy egy véges Galois-fedéshez találjunk egy véges Galois-bővítést, amivel azonosítani tudjuk az elágazási típusát. Most ennek fordítottját próbáljuk meg előkészíteni.

3.4.2. Lemma. Legyen L egy test, és $f(x, y) \in L[x, y]$ szeparábilis polinom, ha úgy tekintünk rá, mint egy $L(x)$ feletti polinom y-ban. Ekkor véges sok kivétellel minden $b \in L$-re az $f(b, y) \in L[y]$ polinom szeparábilis.

Bizonyítás. A 2.1.8 lemma alapján feltehető, hogy f normált y-ban. A $D(x) \in L[x]$ diszkrimináns nem nulla, hiszen f szeparábilis y-ban. Minden $b \in L$ elemre $f(b, y) \in L[y]$ diszkriminánsa $D(b)$, ez pedig csak olyan b elemekre lehet nulla, amelyek gyökei $D(x)$-nek. Ezt a véges sok elemet kivéve $f(b, y)$ mindig szeparábilis. □

3.4.3. Lemma. Legyen $D \subseteq \mathbb{C}$ nyílt és összefüggő, továbbá $p_0 \in D$ és $D_0 = D \setminus \{p_0\}$. Tekintsük $\mathcal{M}(D)$-t a megszorítás általi beágyazással $\mathcal{M}(D_0)$ résztestének. Ekkor $\mathcal{M}(D)$ algebrailag zárt $\mathcal{M}(D_0)$-ban.

Bizonyítás. Legyen $g \in \mathcal{M}(D_0)$ algebrai $\mathcal{M}(D)$ felett. Ez azt jelenti, hogy van egy polinom, amelynek g gyöke:

$$a_n g^n + a_{n-1} g^{n-1} + ... + a_0 = 0,$$

és amelyre $a_i \in \mathcal{M}(D)$ minden $i = 0, 1, ..., n$-re és $a_n \neq 0$ $(n \geq 1)$. Feltehetjük, hogy egyik együtthatónak sincs pólusa p_0-ban, hiszen meg tudjuk szorozni $z - p_0$ elég nagy hatványával, hogy ez teljesüljön, továbbá a 2.1.8 lemma miatt feltehetjük, hogy $a_n = 1$. Ezek után felírható, hogy

$$g^n = -a_{n-1} g^{n-1} - a_{n-2} g^{n-2} - ... - a_0.$$

Mivel p_0 egy környezetében minden a_i korlátos, ezért g is korlátos. Ez azért van, mert ha vesszük egy kis környezetét p_0-nak, amelyben $K \in \mathbb{R}$ közös korlát a_i-k abszolút értékére, akkor egy $K \cdot n$-nél nagyobb abszolút értékű számra nem lehet egyenlő a fenti egyenlőség két oldala. Ekkor g kiterjeszthető p_0-ra meromorf módon, hiszen legfeljebb megszüntethető szingularitása lehet ott, tehát $g \in \mathcal{M}(D)$. □

3.4.4. Lemma. Legyen $L/\mathbb{C}(x)$ véges Galois-bővítés. Világos, hogy létezik egy $F(x,y) \in \mathbb{C}[x,y]$ polinom, amely y-ban $\mathbb{C}(x)$ felett irreducibilis, és $\mathbb{C}(x)$ felett L a felbontási teste. Legyen n az F foka, ha úgy tekintünk rá, mint egy polinom y-ban. A 3.4.2 lemma alapján csak véges sok $p \in \mathbb{C}$-re teljesül, hogy hogy az $F(p,y) \in \mathbb{C}[y]$ polinomnak n-nél kevesebb különböző gyöke van. Legyen P az a halmaz, amelyben ez a véges sok p szerepel, kiegészítve a ∞-nel. Legyen

$$R' = \{(u, v_1, v_2, ..., v_n) \in \mathbb{C}^{n+1} : u \in \mathbb{P}^1 \setminus P \text{ és } F(u, v_1) = ... = F(u, v_n) = 0\},$$

ahol R'-t az indukált topológiával topologikus térnek tekintjük. Ekkor a következők teljesülnek.

(a) Az $f' : R' \to \mathbb{P}^1 \setminus P, (u, v_1, v_2, ..., v_n) \mapsto u$ leképezés fedés, amelyre tekinthetjük S_n-t Deck(f') részhalmazaként úgy, hogy a $v_1, ..., v_n$ koordinátákat permutálja.

(b) Legyen R egy összefüggőségi komponense R'-nek. Ekkor az $f = f'|_R : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedés.

(c) Ha $i = 1, 2, ..., n$, akkor a $g_i : R \to \mathbb{C}$, $(u, v_1, ..., v_n) \mapsto v_i$ leképezés kiterjeszthető egy $\bar{R}$-en értelmezett $\bar{g}_i$ meromorf függvénnyé úgy, hogy $F(\bar{f}, \bar{g}_i) = 0$ és a $\bar{g}_1, \bar{g}_2, ..., \bar{g}_n$ leképezések generálják $\mathcal{M}(\bar{R})$-et $\mathbb{C}(\bar{f})$ felett.

Bizonyítás. (a) A 3.1.8 tétel alapján minden $u_0 \in \mathbb{P}^1 \setminus P$-hoz léteznek olyan $\psi_1, ..., \psi_n$ holomorf függvények az u_0 egy U környezetén értelmezve, hogy minden $u \in U$-ra pontosan $\psi_1(u), ..., \psi_n(u)$ a gyökei $F(u,y) \in \mathbb{C}[y]$-nak. Legyen $\sigma \in S_n$-re

$$V_\sigma = \{(u, \psi_{\sigma(1)}(u), ..., \psi_{\sigma(n)}(u)) : u \in U\},$$

ekkor V_σ-k diszjunkt uniója alkotja $(f')^{-1}(U)$-t. Ezek valóban diszjunktak, hiszen $F(u,y)$ szeparábilis, tehát minden gyöke különböző. Az $U \to V_\sigma$, $u \mapsto (u, \psi_{\sigma(1)}(u), ..., \psi_{\sigma(n)}(u))$ leképezés, és az $f'|_{V_\sigma} : V_\sigma \to U$ egymás inverzei, tehát mindketten homeomorfizmusok. Ha U-t kompaktnak és összefüggőnek választjuk, akkor emiatt V_σ is az lesz, és ekkor a V_σ-k összefüggőségi komponenseit alkotják $(f')^{-1}(U)$-nak, tehát minden $D \subseteq U$ nyílt, u_0 középpontú körlap jóllefedett környezete u_0-nak, tehát f' fedés. Ez alapján az is világos, hogy S_n beágyazható Deck(f)-be a fenti módon, hiszen a jóllefedett környezetek őseit permutálja.

(b) Először belátjuk, hogy f fedés. Ehhez először is kell, hogy szürjektív. Válasszunk egy tetszőleges $p \in \mathbb{P}^1 \setminus P$, és egy $a \in R$ pontot. Mivel $\mathbb{P}^1 \setminus P$ útösszefüggő, ezért létezik egy $\gamma : [0,1] \to \mathbb{P}^1 \setminus P$ út, melynek kezdőpnotja $f(a)$, és végpontja p. A fedő utak tétele ([1] 7.3.5 Tétel) miatt ennek az útnak van egy $\tilde{\gamma}$ felemeltje a kezdőponttal R'-ben, ekkor $\tilde{\gamma}$ R-ben van, hiszen R összefüggőségi komponens. Ez azt jelenti, hogy a $\tilde{\gamma}$-nak a b végpontjára $f(b) = p$, vagyis f szürjektív. Legyen U egy f' által jóllefedett környezet. Az $f'^{-1}(U)$-nak minden V összefüggőségi komponense vagy benne van R-ben, vagy diszjunkt tőle. Amelyek R-ben vannak, azok továbbra is összefüggőségi komponensei $f^{-1}(U)$-nak is, és f homeomorf módon képezi őket U-ra, tehát tehát U f által szintén jóllefedett környezet, vagyis f fedés.

Legyen $u \in \mathbb{P}^1 \setminus P$. Ekkor, ha $v, v' \in f^{-1}(u)$, akkor van olyan $\alpha \in$ Deck(f'), amelyre $\alpha(v) = v'$. Ez azért van, mert v és v' koordinátái megegyeznek (hiszen ezek u-n kívül pontosan az $F(u,y) \in \mathbb{C}[y]$ polinom gyökei), tehát az (a) rész alapján megfelelő Deck(f')-beli elemmel tudjuk a koordinátákat úgy permutálni, hogy $v \mapsto v'$ teljesüljön. Ekkor α

saját magára képezi R-et, hiszen összefüggő halmaz képe összefüggő, és $v \in R$-re $\alpha(v) \in R$. Ez szimmetrikus módon teljesül α^{-1}-re is, tehát $\alpha|_R \in \mathrm{Deck}(f)$. Ebből következik, hogy $\mathrm{Deck}(f)$ trenzitívan hat $f^{-1}(u)$-n, tehát f Galois fedés. Világos, hogy $\deg(f) \leq \deg(f') = n!$, tehát f véges Galois-fedés.

(c) Minden $u \in R$ pontnak van egy V_σ alakú környezete. Tekintsük R-en a 3.3.1 állításban definiált komplex differenciálható struktúrát. Ebben a $(f|_{V_\sigma}, V_\sigma)$ alakú párok térképek. Egy ilyen térképet tekintve $\bar{g}_i$ megegyezik a $\psi_{\sigma(i)}$ függvénnyel, tehát meromorf R-en. Azt, hogy $\bar{g}_i$ meromorf $\bar{R}$-en, az abból fog következni, hogy ha $\mathcal{M}(\bar{R})$-et a megszorítás által indukált beágyazással $\mathcal{M}(R)$ résztestének tekintjük, akkor $\mathcal{M}(\bar{R})$ algebrailag zárt $\mathcal{M}(R)$-ben, hiszen ha $h \in \mathcal{M}(R)$ algebrai $\mathcal{M}(\bar{R})$ felett, akkor meromorf $\bar{R} \setminus R$ minden pontjában a 3.4.3 lemma alapján, hiszen az egy véges halmaz, tehát $\bar{h} \in \mathcal{M}(\bar{R})$ (és $\bar{h}|_R = h$). Be fogjuk látni, hogy g_i algebrai $\mathcal{M}(R)$ felett. Ha $v = (u, v_1, ..., v_n) \in R$, akkor $F(u, v_i) = 0$, tehát minden $v \in R$-re $F(f(v), g_i(v)) = 0$. Tehát ha f-et és g_i-t $\mathcal{M}(R)$ elemeiként vizsgáljuk, akkor $F(f, g_i) = 0$. Mivel $f \in \mathcal{M}(\bar{R})$, ez pont azt jelenti, hogy g_i algebrai $\mathcal{M}(\bar{R})$ felett, tehát $\bar{g}_i \in \mathcal{M}(\bar{R})$.

Már csak az van hátra, hogy $\bar{g}_i$-k generálják $\mathcal{M}(\bar{R})$-et $\mathbb{C}(\bar{f})$ felett. Mivel a 3.4.1 tétel alapján $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f})$ minden eleme ι_α alakú, ezért elég belátni, hogy ha ι_α fixen hagyja az összes $\bar{g}_i$-t, akkor $\iota_\alpha = \mathrm{id}$, ami ekvivalens azzal, hogy $\alpha = \mathrm{id}$. Tegyük tehát fel, hogy ι_α-nak $\bar{g}_1, ..., \bar{g}_n$ mind fixpontja. Ekkor minden $v \in R$-re és $i = 1, 2, ..., n$-re $\bar{g}_i(v) = \bar{g}_i(\alpha^{-1}(v))$, és az is teljesül, hogy $\bar{f}(v) = \bar{f}(\alpha^{-1}(v))$, tehát $v = \alpha^{-1}(v)$, hiszen koordinátánként megegyezik. Emiatt $\alpha = \mathrm{id}$. □

Ezzel készen vagyunk az előkészületekkel, már be tudjuk bizonyítani a keresett változatát Riemann egzisztenciatételének.

3.4.5. Tétel (RET − Az Algebrai Verzió)**.** Legyen $\mathcal{T} = [G, P, (C_p)_{p \in P}]$ egy elágazási típus. Legyen $r = |P|$, és számozzuk meg P elemeit: $p_1, p_2, ..., p_r$. Ezen feltételek mellett pontosan akkor létezik $\mathcal{T}$ típusú véges Galois-bővítése $\mathbb{C}(x)$-nek, ha léteznek G-ben $g_1, g_2, ..., g_r$ generátorok, amelyekre teljesül, hogy $g_1 \cdot g_2 \cdot ... \cdot g_r = 1$, és $g_i \in C_{p_i}$, ha $i = 1, 2, ..., r$.

Bizonyítás. Először belátjuk azt az irányt, hogy ha léteznek megfelelő generátorai G-nek, akkor létezik $\mathbb{C}(x)$-nek olyan véges Galois-bővítése, amelynek elágazási típusa $\mathcal{T}$. A topologikus verzió (3.2.12 tétel) alapján van egy olyan véges $f : R \to \mathbb{P}^1 \setminus P$ Galois-fedés, amelynek elágazási típusa $\mathcal{T}$. A 3.4.1 tételban definiált $\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f})$ véges Galois-bővítés elágazási típusa ezzel megegyezik (ugyanazon tétel alapján). Mivel $\mathbb{C}(\bar{f})$ és $\mathbb{C}(x)$ értelemszerűen izomorf, ezért ez az irány készen van.

A másik irány belátásához vegyünk egy $L/\mathbb{C}(x)$ véges Galois-bővítést. Legyen $F(x, y) \in \mathbb{C}[x, y]$ olyan, mint a 3.4.4 lemmában. Tekintsük az ugyanabban a lemmában definiált $f : R \to \mathbb{P}^1 \setminus P$ véges Galois-fedést. Mivel a (c) részben definiált $\bar{g}_i$ függvények gyökei az irreducibilis $F(\bar{f}, y)$ polinomnak $\mathbb{C}(\bar{f})$ felett, ezért $\mathcal{M}(\bar{R})$ a felbontási teste $F(\bar{f}, y)$-nak $\mathbb{C}(\bar{f})$ felett. Ez azt jelenti, hogy van egy $L \to \mathcal{M}(\bar{R})$ izomorfizmus a két test között, amelyre $x \mapsto \bar{f}$. A 3.4.1 tétel (b) része szerint a bővítés elágazási pontjai pontosan azok a $p \in P$ pontok, amelyekre $C_p^{\mathrm{top}} \neq 1$. A 3.2.13 megjegyzés alapján ekkor léteznek $\mathrm{Deck}(f)$-nek $h_1, h_2, ..., h_r$ generátorai, amelyekre $h_1 \cdot h_2 \cdot ... \cdot h_r = 1$, és minden i-re $h_i \in C_p^{\mathrm{top}}$. Ekkor a 3.4.1 tételben definiált ι izomorfizmust tekintve a $g_i = \iota(h_i)$ generátorok a $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(\bar{f}))$ csoportban a tétel (b) része miatt szintén bírni fognak a kívánt tulajdonságokkal. Mivel láttuk, hogy L izomorf $\mathcal{M}(\bar{R})$-rel, ezért ebből következik a tétel másik iránya. □

Ennek az eredménynek van egy érdekes és széles körben ismert közvetlen következménye.

3.4.6. Következmény. Minden véges csoport előáll, mint $\mathbb{C}(x)$ alkalmas Galois-bővítésének Galois-csoportja. Ez azt jelenti, hogy az inverz Galois-problémára ezen test felett pozitív választ kapunk. □

3.4.7. Példa. A 2.3.8 és a 2.3.9 példákban meghatároztuk egyes bővítések elágazási típusait. Most legyen $K = \mathbb{C}$, és ellenőrizzük, hogy RET (3.4.5 Tétel) feltételei teljesülnek-e ezekben az esetekben.

(i) A 2.3.8 példában vizsgált esetben két elágazási pont van, és az asszociált konjugáltosztályok 1-1 generátorelemből állnak, melyek egymás inverzei. Ebben az esetben tehát világos, hogy ha a két konjugáltosztályból összeszorozzuk egymással az elemeket, akkor 1-et kapunk, továbbá generátorokról van szó.

(ii) A 2.3.9 példában a Galois-csoport izomorf D_n-nel. Ha n páratlan, akkor három elágazási pont van, és a konjugáltosztályok közül kettő a tükrözések konjugáltosztálya, a harmadik pedig egy n-edrendű forgatásból és az inverzéből áll. Egy n-edrendű forgatás és egy tükrözés mindig generálja D_n-et, tehát bármilyen elemeket választunk, generátorok lesznek. Mivel bármely forgatást meg tudjuk kapni két tükrözés szorzataként, ezért ha a forgatásból és az inverzéből álló osztály nem C_2, akkor világos, hogy találunk g_1, g_2, g_3 generátorokat, hogy $g_1 \cdot g_2 \cdot g_3 = 1$. Ha pedig C_2 a tükrözések osztálya, akkor válasszunk tetszőlegesen egy $g_1 \in C_1$, és $g_2 \in C_2$ elemet. Világos, hogy $g_1 \cdot g_2$ tükrözés, tehát $g_3 = g_1 \cdot g_2$ választással $g_1 \cdot g_2 \cdot g_3 = 1$.

Ha n páros, akkor szintén 3 elágazási pont van, és megkapjuk a tükrözések két konjugáltosztályát, és szintén egy n-edrendű forgatásból és az inverzéből álló osztályt. Szintén bárhogy választunk elemeket, generátorokat kapunk. Ha nem C_2 a forgatás és inverzének osztálya, akkor készen vagyunk, hiszen bármely n-edrendű forgatást megkapunk, mint két olyan tükrözés szorzata, amelyek közül az egyik tengelye oldalakon, a másiké csúcsokon megy át (tehát ha választunk egy forgatást, akkor a tükrözéseket tudjuk úgy választani, hogy az inverzét adják). Ez azért van, mert ha a forgatás α szögű, akkor ha választunk két tengelyt, melyek $\alpha/2$ szöget zárnak be, akkor a megfelelő tükrözések jók lesznek. Márpedig ha $\alpha/2$ szöget zárnak be, akkor ha mindkettő például a csúcsokon megy át, akkor $\frac{n}{2} \cdot \alpha = k \cdot 360°$, tehát a forgatás nem lesz n-edrendű. Ugyanígy baj, ha mindkettő az oldalakon megy át, tehát a két tükrözés nem lesz konjugált (hiszen az egyiknek a tengelye az oldalak középpontjain, a másiké a csúcsokon megy át).

A harmadik esethez legyen C_1 és C_3 a két tükrözésekből álló osztály, és C_2 pedig az n-edrendű forgatás és inverzének osztálya. Ismét válasszunk tetszőlegesen egy $g_1 \in C_1$, és egy $g_2 \in C_2$ elemet. Be kell látni, hogy $g_1 \cdot g_2 \in C_3$, vagyis azt, hogy nem konjugált g_1-gyel, hiszen az világos, hogy tükrözés. Már láttuk, hogy ha két tükrözés konjugált, akkor nem lehet n-edrendű forgatás a szorzatuk, és emiatt g_1 és $g_1 \cdot g_2$ nem lehet konjugált, hiszen a szorzatuk $g_1 \cdot (g_1 \cdot g_2) = g_2$, vagyis egy n-edrendű forgatás. Beláttuk tehát, hogy $g_1 \cdot g_2 \in C_3$, tehát legyen $g_3 = g_1 \cdot g_2$, ekkor $g_1 \cdot g_2 \cdot g_3 = g_3 \cdot g_3 = 1$. Ez azt jelenti, hogy itt is teljesülnek RET feltételei.

4. A merevségi kritérium

Az eddigiekkel a tarsolyunkban már definiálhatjuk a merevséget. Ez a fő eszközünk arra, hogy egy $\mathbb{C}(x)$ feletti bővítést realizáljunk $\mathbb{Q}(x)$ felett, és ennek alapja RET lesz, ugyanis a merevség definíciója nagyon hasonló a tétel kimondásához.

4.1. RET és a gyenge merevség

4.1.1. Definíció (Reguláris testbővítés)**.** Az L/K testbővítést regulárisnak nevezzük, ha K algebrailag zárt L-ben, vagyis minden $K[x]$-beli polinom L-beli gyöke benne van K-ban is.

4.1.2. Definíció (Konjugáltosztályok merev, gyengén merev r-ese)**.** Legyen $(C_1, C_2, ..., C_r)$ egy G csoport konjugáltosztályaiból álló r-es. Ezt gyengén merevnek nevezzük, ha a következő 2 feltétel teljesül:

(i) Léteznek $g_1, ..., g_r$ generátorok G-ben, amelyekre $g_1 \cdot ... \cdot g_r = 1$ és $g_i \in C_i$, ha $i = 1, ..., r$.

(ii) Ha $g_1', ..., g_r'$ egy másik generátorhalmaz az (i) tulajdonsággal, akkor létezik egy γ automorfizmusa G-nek, amelyre $\gamma(g_i) = g_i'$, ha $i = 1, ..., r$.

Merevnek nevezzük a fenti r-est, ha (i) teljesül, és (ii)-ben a γ automorfizmus előáll, mint egy kitüntetett $g \in G$ elemmel való konjugálás, és ez a g egyértelmű.

4.1.3. Állítás. A merevség esetén az a kritérium, hogy g egyértelmű, ekvivalens azzal, hogy G centruma triviális.

Bizonyítás. Tegyük fel, hogy g egyértelmű, és legyen $h \in Z(G)$. Ekkor tetszőleges $g' \in G$-re $(gh)g'(gh)^{-1} = ghg'h^{-1}g^{-1} = gg'g^{-1}hh^{-1} = gg'g^{-1}$, tehát gh is olyan elem, amellyel való konjugálás szolgáltatja γ-t. Emiatt $g = gh$, tehát $h = 1$, vagyis $Z(G)$ valóban triviális.

Most tegyük fel, hogy $Z(G)$ triviális, és legyen g_1 és g_2 olyan elemek, amelyekkel való konjugálás a γ automorfizmus. Legyen $h = g_1^{-1}g_2$. Ekkor $g_2 = g_1h$. Legyen $g' \in G$ tetszőleges. Ekkor $\gamma(g') = (g_1h)g'(g_1h)^{-1} = g_1hg'h^{-1}g_1^{-1}$, másrészt $\gamma(g') = g_1g'g_1^{-1}$, tehát $g_1hg'h^{-1}g_1^{-1} = g_1g'g_1^{-1}$, vagyis $hg'h^{-1} = g'$. Ebből következik, hogy $h \in Z(G)$, ami $Z(G) = \{1\}$ miatt azt jelenti, hogy $h = 1$, vagyis $g_1 = g_2$, tehát g valóban egyértelmű. □

4.1.4. Definíció (Merev, gyengén merev típus)**.** Egy $\mathcal{T} = [G, P, (C_p)_{p \in P}]$ elágazási típust merevnek, illetve gyengén merevnek nevezünk, ha a P elemeit indexelni tudjuk a következőképpen: $P = \{p_1, ..., p_r\}$ (itt $r = |P|$), és a $C_i = C_{p_i}$ konjugáltosztályok egy merev, illetve gyengén merev r-est alkotnak G-ben.

4.1.5. Tétel. Minden gyengén merev típusra létezik $\mathbb{C}(x)$-nek egy véges Galois-bővítése, amely ilyen típusú, és ez egyértelmű egy $\mathbb{C}(x)$-izomorfizmus erejéig.

Bizonyítás. A létezés egyenes következménye RET-nek (3.4.5 tétel). Nézzük az egyértelműséget. Tegyük fel, hogy $L_1/\mathbb{C}(x)$ és $L_2/\mathbb{C}(x)$ elágazási típusa megegyezik, és gyengén merev. Feltehető, hogy $L_1, L_2 \leq L$, ahol $L/\mathbb{C}(x)$ véges Galois-bővítés. Legyen $G = \mathrm{Gal}(L/\mathbb{C}(x))$, és $G_j = \mathrm{Gal}(L_j/\mathbb{C}(x))$, valamint $\rho_j : G \to G_j$ a megszorítás, ha $j = 1, 2$. Minden $p \in \mathbb{P}^1$-re legyen C_p és $C_p^{(j)}$ az asszociált konjugáltosztály G-ben, illetve G_j-ben. Ekkor a 2.2.3

lemma (d) pontja miatt $\rho_j(C_p) = C_p^{(j)}$. Számozzuk meg P pontjait: $p_1, ..., p_r$. RET miatt léteznek $g_1, ..., g_r$ generátorai G-nek, amelyekre $g_1 \cdot ... \cdot g_r$, és $g_i \in C_{p_i}$, ha $i = 1, ..., r$. Ekkor $\rho_j(g_1), ..., \rho_j(g_r)$ generátorok G_j-ben ugyanazon tulajdonságokkal. Mivel $L_1/\mathbb{C}(x)$ és $L_2/\mathbb{C}(x)$ típusa megegyezik, ezért létezik egy $\epsilon : G_2 \to G_1$ izomorfizmus, amely $C_p^{(2)}$-t $C_p^{(1)}$-re képezi minden p esetén. Ekkor $\epsilon(\rho_2(g_1)), ..., \epsilon(\rho_2(g_r))$ is bírnak azon tulajdonságokkal, mint $\rho_1(g_1), ..., \rho_1(g_r)$. L_1 és L_2 elágazási pontjai megegyeznek, tehát azokat az indexeket, amelyekre p_i nem elágazási pont, elhagyhatjuk, ezáltal feltehetjük, hogy p_i elágazási pont minden $i = 1, ..., r$-re. Emiatt a gyenge merevségi feltétel miatt van G_1-nek egy δ automorfizmusa, amelyre $\delta(\epsilon(\rho_2(g_i))) = \rho_1(g_i)$, ha $i = 1, ..., r$. Tehát $\gamma = \delta \circ \epsilon$ egy $G_2 \to G_1$ izomorfizmus, amely $\rho_2(g_i)$-t minden i-re $\rho_1(g_i)$-be képezi, vagyis $\rho_1 = \gamma \circ \rho_2$. Ez alapján $\mathrm{Ker}\rho_1 = \mathrm{Ker}\rho_2$, és ennek fixteste egyrészt L_1, másrészt L_2. Ebből következik, hogy $L_1 = L_2$, tehát készen vagyunk. □

4.2. Hilbert irreducibilitási tétele

Eddig $L/K(x)$ alakú bővítésekről volt szó, és ebben az alfejezetben megválaszolásra kerül a kérdés, hogy miért: Hilbert irreducibilitási tétele alapján ha egy csoport előáll $\mathrm{Gal}(L_1/\mathbb{Q}(x))$ alakban, akkor előáll Galois-csoportként $\mathbb{Q}$ felett is, mint $\mathrm{Gal}(L_2/\mathbb{Q})$ (mindkét bővítés Galois). Ez azon múlik, hogy $\mathbb{Q}$ Hilbert-féle test (angolul *hilbertian*). A tétel legegyszerűbb formájában arról szól, hogy ha $f(t, x)$ egy kétváltozós polinom, mely irreducibilis $\mathbb{Q}[t, x]$-ben, akkor végtelen sok $t' \in \mathbb{Q}$ számra $f(t', x)$ irreducibilis $\mathbb{Q}$ felett egyváltozós polinomként.

4.2.1. Definíció (Hilbert-féle test)**.** Legyen K egy test, és tekintsük az $f(t, x) \in K[t, x]$ kétváltozós irreducibilis nemkonstans polinomokat. Hilbert-féle testnek nevezzük K-t, ha bármilyen olyan f polinomra, ami a fenti tulajdonságokkal rendelkezik, K felett van végtelen sok $b \in K$ érték, hogy az egyváltozós $f(b, y) \in K[y]$ polinom irreducibilis.

4.2.2. Tétel. Tegyük fel, hogy K Hilbert-féle. Ekkor, ha G előáll egy Galois-bővítés Galois-csoportjaként $K(x_1, ..., x_m)$ felett, akkor előáll Galois-csoportként K-nak egy Galois-bővítésével is.

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

Bizonyítás. Ennek a tételnek, továbbá az előző eredménynek a bizonyítása megtalálható [19] 1. fejezetében. □

4.2.4. Megjegyzés. Mivel minden Hilbert-féle test minden véges bővítése Hilbert-féle, ebből az is következik, hogy minden algebrai számtest Hilbert-féle.

Az alfejezet zárásaként megfogalmazunk egy, a témához kapcsolódó lemmát, amelyre később szükség lesz. Az alábbi triviális megjegyzés is hasznunkra lesz a későbbiekben.

4.2.5. Megjegyzés. Legyen K egy test, melynek karakterisztikája 0. Ha ennek $K_1 = K(a_1, ..., a_r)$ egy végesen generált bővítése, és $t_1, ..., t_s$ az a_i-knek egy maximális K felett algebrailag független részhalmaza, akkor K_1 véges a tisztán transzcendens $K(t_1, ..., t_s)$ bővítés felett. Ez valóban teljesül, hiszen a bővítés algebrai és végesen generált.

4.2.6. Lemma. Legyenek $x_1, ..., x_m$ független transzcendens elemek egy 0 karakterisztikájú K test felett, és vezessük be a következő jelölést: $\mathbf{x} = (x_1, ..., x_m)$. Legyen $\bar{K}$ az algebrai lezártja K-nak.

(a) Ha K'/K véges Galois-bővítés, akkor a megszorítással kapott $\mathrm{Gal}(K'(\mathbf{x})/K(\mathbf{x})) \to \mathrm{Gal}(K'/K)$ leképezés izomorfizmus. Speciálisan, minden közbülső test $K(\mathbf{x})$ és $K'(\mathbf{x})$ között $K''(\mathbf{x})$ alakú, és $|K''(\mathbf{x}) : K(\mathbf{x})| = |K'' : K|$.

(b) Legyen $f(\mathbf{x}, y) \in K(\mathbf{x})[y]$ irreducibilis polinom $K(\mathbf{x})$ felett, és legyen $L = K(\mathbf{x})[y]/(f)$ a megfelelő testbővítése $K(\mathbf{x})$-nek. Ekkor L akkor, és csak akkor reguláris K felett, ha f irreducibilis $\bar{K}(\mathbf{x})$ felett. Ha ez a helyzet, akkor $f(\mathbf{x}, y)$ irreducibilis $K_1(\mathbf{x})$ felett K-nak minden K_1 bővítésére, amelyre $x_1, ..., x_m, y$ lineárisan független transzcendens elemek K_1 felett.

Bizonyítás. (a) A $G = \mathrm{Gal}(K'/K)$ csoport természetes módon $x_1, ..., x_m$-et helyben hagyva hat $K'(\mathbf{x})$-en, emiatt Artin tételéből (2.1.1 Tétel) következik, hogy $K'(\mathbf{x})/K(\mathbf{x})$ Galois, és Galois-csoportja G. A második állításhoz (a)-ban a Galois-elmélet főtételét fogjuk használni. Bármely $K_0 \leq K'(\mathbf{x})$ közbülső test megfelel egy $H \leq G$ részcsoport fixtestének. Tekintsük H fixtestét K'-ben, ha G-t úgy tekintjük, mint $\mathrm{Gal}(K'/K)$. Legyen ez a fixtest K''. Teljesül, hogy $K''(\mathbf{x}) = K_0$, hiszen világos, hogy mindkettő a H csoport fixteste, hiszen az első állítást alkalmazhatjuk $K''(\mathbf{x})/K(\mathbf{x})$-re. Ezzel az (a) rész készen van.

(b) Legyen $\widehat{K}$ a K test algebrai lezártja L-ben (vagyis azon L-beli elemek részteste, melyek algebraiak K felett, lásd [2] 6.2.12 Tétel), és α a képe y-nak L-ben. Ekkor $f(\alpha) = 0$, és α kielégít egy $|L : \widehat{K}|$-adfokú $\hat{f}(y) \in \widehat{K}(\mathbf{x})[y]$ polinomot, mely osztja f-et. Ebből következik, hogy ha $\widehat{K} \neq K$, akkor f nem irreducibilis $\widehat{K}(\mathbf{x})[y]$-ban, és így $\bar{K}(\mathbf{x})[y]$-ban sem, amivel az ekvivalencia egyik irányát megkaptuk.

A másik irányhoz tegyük fel, hogy $\widehat{K} = K$ (vagyis L reguláris K felett), és legyen K' tetszőleges véges Galois-bővítése K-nak. Vegyük $K(\mathbf{x})$ algebrai lezárását úgy, hogy az tartalmazza $K'(\mathbf{x})$-et és L-et, és ebben jelöljük L'-vel a $K'(\mathbf{x})$ és L által generált résztestet. Az (a) rész miatt $L \cap K'(\mathbf{x}) = K''(\mathbf{x})$ valamely K'' közbülső testre K és K' között. Világos, hogy $K'' \subseteq \widehat{K}$, hiszen $\widehat{K}$ az algebrai lezártja K-nak L-ben, emiatt $K'' = K$, vagyis $L \cap K'(\mathbf{x}) = K(\mathbf{x})$. Az (a) rész miatt $K'(\mathbf{x})/K(\mathbf{x})$ Galois, tehát $|L' : K'(\mathbf{x})| = |L : K(\mathbf{x})|$. Viszont $L' = K'(\mathbf{x})[\alpha]$ miatt f irreducibilis $K'(\mathbf{x})$ felett. Mivel K' tetszőleges véges Galois-bővítése volt K-nak, ezért f nyilván irreducibilis $\bar{K}(\mathbf{x})$ felett is.

Most nézzük (b) másik állítását. Tegyük fel indirekt, hogy f felbomlik $f = gh$ alakban, ahol $g, h \in K_1(\mathbf{x})[y]$, és $\deg(g)$, illetve $\deg(h)$ legalább 1, ha y polinomjaiként tekintünk rájuk. Nyilván alkalmas skalárral szorozva feltehető, hogy g normált y-ban. Feltehető, hogy K_1-et K felett generálják g, mint $x_1, ..., x_m, y$-beli racionális törtfüggvény együtthatói, és ezen együtthatók közül egy, amit t-vel jelölünk, transzcendens K felett (hiszen ha mind algebrai, akkor algebrai a bővítés, tehát benne van $\bar{K}(\mathbf{x})$-ben). A 4.2.5 megjegyzés miatt K_1 véges egy $K_2 = K(t_1, ..., t_s)$ test felett, ahol $t_1, ..., t_s$ független transzcendens elemek K felett, és $t = t_1$. Van egy végtelen $A \subseteq \mathrm{Aut}(K_2/K)$ részhalmaz, amelyre minden $\alpha \in A$ különböző értéket vesz fel t-n (pl. $\alpha(t) = t + c$, $c \in K$, és $\alpha(t_i) = t_i$, ha $i > 1$, lásd 2.3.1 Állítás, ehhez az irányhoz nem használtuk az algebrai zártságot). Ezek az α-k kiterjeszthetőek K_1 beágyazásává $\bar{K}_2$-be, illetve $K_1(\mathbf{x})[y]$ beágyazásává $\bar{K}_2(\mathbf{x})[y]$-ba (helyben hagyva $x_1, ..., x_m, y$-t). Ezeket a beágyazásokat g-re alkalmazva f-nek végtelensok különböző osztóját kapjuk $\bar{K}_2(\mathbf{x})[y]$-ban, melyek mind normáltak. Ez az ellentmondás bizonyítja az állítást. □

4.3. Az alaptest szűkítése

Ebben a részben arról lesz szó, hogy ha van egy $L/K(x)$ Galois-bővítésünk, és κ egy résztest K-ban, akkor van-e $\kappa(x)$-nek egy Galois-bővítése ugyanazzal a csoporttal. Látható, hogy így szeretnénk elérni, hogy egy $L_1/\mathbb{C}(x)$ alakú bővítés csoportját megkapjuk egy $L_2/\mathbb{Q}(x)$ bővítés csoportjaként. Nem pontosan ezt fogjuk tenni, hanem $\mathbb{C}$ algebrailag zárt része lesz majd K, és ennek κ résztesteit fogjuk nézni. Ezen kívül a bővítésről fel fogjuk tenni, hogy a típusa merev. A szakaszban szükségünk lesz $\mathbb{C}$ egységgyökeire, ha nem rögzítjük ezt, akkor automatikusan az $\varepsilon_n = e^{\frac{2\pi i}{n}}$-et (itt $i = \sqrt{-1}$) fogjuk érteni alatta.

4.3.1. Definíció (Résztest felett definiált bővítés)**.** Azt mondjuk, hogy $L/K(x)$ (vagy röviden L) definiált $\kappa \leq K$ felett, ha létezik egy $L_\kappa \leq L$ résztest, amely Galois $\kappa(x)$ felett, reguláris κ felett, és $|L_\kappa : \kappa(x)| = |L : K(x)|$.

4.3.2. Lemma. Legyen K egy algebrailag zárt részteste $\mathbb{C}$-nek, és $L/K(x)$ definiált κ felett. Legyen $n = |L : K(x)|$.

(a) Legyen θ egy primitív eleme az $L_\kappa/\kappa(x)$ bővítésnek (vagyis $L_\kappa = \kappa(x)(\theta)$). Ekkor $L = K(x)(\theta)$. Ezenkívül L definiált minden κ' közbülső testre κ és K között, és a definícióban leírt testet választhatjuk $L_{\kappa'} = \kappa'(x)(\theta)$-nak.

(b) A megszorítás L_κ-ra izomorfizmus a $G = \mathrm{Gal}(L/K(x))$ és a $\mathrm{Gal}(L_\kappa/\kappa(x))$ csoportok között.

(c) Ha κ algebrailag zárt, akkor $L/K(x)$ és $L_\kappa/\kappa(x)$ elágazási típusa természetes módon megegyezik.

Bizonyítás. (a) Legyen θ minimálpolinomja $F(y) \in \kappa(x)[y]$. Ekkor, mivel $L_\kappa = \kappa(x)[y]/(F)$ reguláris κ felett, ezért a 4.2.6 lemma (b) része miatt $F(y)$ irreducibilis $\kappa'(x)[y]$-ban is. Emiatt az $L_{\kappa'} = \kappa'(x)(\theta)$ n-edfokú $\kappa'(x)$ felett. Mivel $F(y)$ minden gyöke $L_\kappa \subseteq L_{\kappa'}$-ben van, ezért $L_{\kappa'}/\kappa'(x)$ Galois, és $L_{\kappa'} = \kappa'(x)[y]/(F)$, tehát a 4.2.6 lemma miatt $L_{\kappa'}$ reguláris κ' felett. Ebből következik, hogy L definiált κ' felett. Az első állítás ennek speciális eseteként megkapható, hiszen $K(x)(\theta)$ $K(x)$-nek egy n-edfokú bővítése ($\kappa' = K$-ra), és $K(x)(\theta) \subseteq L$, tehát $L = K(x)(\theta)$.

(b) A G csoport $F(y)$ gyökeit permutálja L-ben. Ezen gyökök generálják L_κ-t $\kappa(x)$ felett, tehát G-re invariáns L_κ. Emiatt a megszorítás egy $G \to \mathrm{Gal}(L_\kappa/\kappa(x))$ homomorfizmus. Az (a) rész miatt ez injektív (hiszen θ képe meghatározza egy mindkét csoport elemeit), tehát a rendek egyenlősége miatt izomorfizmus.

(c) Legyen θ egy primitív eleme az $L_\kappa/\kappa(x)$ bővítésnek. Tekintsük a 2.2.1 jelölésbeli $\vartheta_p : K(x) \to K(t)$ izomorfizmus 2.2.3 állításbeli $\vartheta : L \to \Delta$ kiterjesztését, amely beágyazás, és ahol Δ egy véges Galois-bővítése $\Lambda = K((t))$-nek. A 2.3.1 állítás miatt $\vartheta(\kappa(x)) = \kappa(t)$, emiatt $\vartheta(L_\kappa) = \kappa(t)(\theta')$, ahol $\theta' = \vartheta(\theta)$. Emiatt ϑ megszorításával L_κ egy beágyazását kapjuk $\Delta_\kappa := \kappa((t))(\theta')$-ba. Jelöljük ezt a beágyazást $\tilde{\vartheta}$-mal. A $\mathrm{Gal}(\Delta/\Lambda)$ kitüntetett generátorának megszorítása a $\mathrm{Gal}(\Delta_\kappa/\kappa((t)))$ kitüntetett generátora (értelemszerűen). Ebből következik, hogy $g_\vartheta \in G$ megszorítása $g_{\tilde{\vartheta}} \in \widetilde{G}$, ahol $\widetilde{G} = \mathrm{Gal}(L_\kappa/\kappa(x))$. Emiatt a megszorítás által definiált $G \to \widetilde{G}$ izomorfizmus a p-hez asszociált konjugáltosztályt G-ben ráképezi a p-hez asszociált konjugáltosztályra $\widetilde{G}$-ben minden $p \in \kappa \cup \{\infty\}$-re.

Már csak azt kell belátni, hogy az elágazási pontok megegyeznek. Ehhez elég belátni, hogy $L/K(x)$ elágazási pontjai $\kappa \cup \{\infty\}$-ben vannak az előző megállapítás miatt. A 2.1.8 lemma miatt θ választható úgy, hogy $F(y)$ olyan legyen, mint a 2.2.3 állítás (c) részében, és ugyanazon állítás miatt $D(x)$, vagyis $F(y)$ diszkriminánsa $\kappa[x]$-nek egy nemnulla eleme, és a ∞-től különböző elágazási pontjai L-nek $D(x)$ gyökei között vannak. Ez κ algebrailag zártsága miatt azt jelenti, hogy κ-ban vannak, tehát beláttuk, hogy $L/K(x)$ és $L_\kappa/\kappa(x)$ elágazási pontjai megegyeznek. Ebből a fentiek alapján következik, hogy megegyezik az elágazási típus. □

4.3.3. Lemma. Ha $K \leq \mathbb{C}$ algebrailag zárt, $L/K(x)$ n-edfokú Galois-bővítés, melynek Galois-csoportja G, továbbá $\kappa \leq K$, akkor L definiált κ-nak egy $\kappa' \leq K$ végesen generált bővítése felett.

Bizonyítás. Legyen θ egy primitív eleme $L/K(x)$-nek, és minimálpolinomja legyen $F(y) \in K(x)[y]$. Mivel $F(y)$-nak minden θ_i gyöke L-ben van, ezért ezek a gyökök mind felírhatóak $\theta_i = f_i(\theta)$ alakban, ahol $f_i \in K(x)[y]$. Legyen κ' az a test, amit úgy kapunk, ha κ-t bővítjük az F és az f_i polinomok együtthatóival. Ez nyilván végesen generált bővítés K-ban, és azt állítjuk, hogy L definiált κ' felett. Világos, hogy $L_{\kappa'} := \kappa'(x)(\theta)$ Galois $\kappa'(x)$ felett, mivel tartalmazza az összes θ_i-t ([6] 2.5 Állítás $(iv) \Rightarrow (i)$). Világos, hogy κ' algebrai lezártja benne van K-ban, tehát a 4.2.6 lemma miatt $L_{\kappa'} = \kappa'(x)[y]/(F)$ reguláris $\kappa'(x)$ felett, továbbá mivel $F(y)$ irreducibilis $\kappa'(x)[y]$-ban (nyilván), ezért a bővítés foka $n = |L : K(x)|$, tehát készen vagyunk. □

4.3.4. Definíció (α-izomorfozmus)**.** Legyen α egy automorfizmusa K-nak. Ez kiterjeszthető x helybenhagyásával $K(x)$ egy automorfizmusává. Ha $L/K(x)$ egy véges Galois-bővítés, akkor α-izomorfizmusnak nevezzük az olyan $\lambda : L \to L'$ testizomorfizmusokat, amelyekre $L'/K(x)$ véges Galois-bővítés, és $\lambda|_{K(x)} = \alpha$. Egy ilyen izomorfizmus indukál egy $g \mapsto \lambda g \lambda^{-1}$ csoportizomorfizmust a Galois-csoportok között, amelyet $\lambda^* : \mathrm{Gal}(L/K(x)) \to \mathrm{Gal}(L'/K(x))$ módon jelölünk.

4.3.5. Lemma. Legyen $K \leq \mathbb{C}$ algebrailag zárt, és $L/K(x)$ véges Galois-bővítés. Minden $\alpha \in \mathrm{Aut}(K)$ automorfizmusra van egy $\lambda : L \to L'$ α-izmomorfizmus $K(x)$-nek valamely L' véges Galois-bővítésére. Ha L definiált κ felett és $\alpha|_\kappa = \mathrm{id}$, akkor választhatjuk λ-t úgy, hogy $L = L'$, és $\lambda^* = \mathrm{id}$.

Bizonyítás. A létezésről szóló állításhoz feltehető, hogy $L = K(x)[y]/(F)$ alakban van megadva. Ha α-t x és y helybenhagyásával kiterjesztjük $K(x)[y]$ automorfizmusává, amelynél F képe G, akkor ez egy λ gyűrűizomorfizmust indukál L és $L' = K(x)[y]/G$ között. Emiatt $L'/K(x)$ szintén véges és Galois, tehát λ α-izomorfizmus.

A második állításhoz, mivel L definiált κ felett, ezért a 4.3.2 lemma (a) része miatt feltehető, hogy $F(y) \in \kappa(x)[y]$ olyan, hogy $L_\kappa = \kappa(x)[y]/(F)$. Ha $\alpha|_\kappa = \mathrm{id}$, akkor $F = G$, tehát $L = L'$. Ha θ primitív eleme az $L_\kappa/\kappa(x)$ bővítésnek, és $g \in \mathrm{Gal}(L/K(x))$, akkor $\lambda^*(g)(\theta) = \lambda g \lambda^{-1}(\theta) = g(\theta)$, hiszen λ elemenként rögzíti L_κ-t, és a 4.3.2 lemma (a) része miatt $g(\theta) \in L_\kappa$, továbbá $L = K(x)(\theta)$, vagyis $\lambda^* = \mathrm{id}$. □

4.3.6. Jelölés. Legyen κ egy test. Tudjuk (lásd [5] A.1 fejezet), hogy ennek a $\bar{\kappa}$ algebrai lezártja létezik és izomorfia erejéig egyértelmű. Persze $\bar{\kappa}/\kappa$ bővítés általában nem véges. Tekintsük a $\mathrm{Gal}(\bar{\kappa}/\kappa)$ Galois-csoportot. Annak ellenére, hogy csak véges Galois-elmélettel

foglalkozunk a szakdolgozat során, ezt használni fogjuk, mint formális jelölést; az értelmezése ugyanaz, mint véges esetben: $\bar{\kappa}$-nak a κ-t fixen hagyó automorfizmusainak csoportja a kompozícióra nézve. Ez az egyetlen végtelen Galois-csoport, amit használni fogunk.

4.3.7. Tétel. Legyen κ egy test, κ'/κ véges Galois-bővítés, és $\bar{\kappa}$ az algebrai lezártja κ-nak, amelyre $\kappa' \leq \bar{\kappa}$. Ekkor a $\mathrm{Gal}(\bar{\kappa}/\kappa) \to \mathrm{Gal}(\kappa'/\kappa)$ homomorfizmus, amelyet a megszorítás indukál, szürjektív.

Bizonyítás. Vegyünk egy $g \in \mathrm{Gal}(\kappa'/\kappa)$ elemet. Azt kell belátni, hogy kiterjeszthető $\bar{\kappa}$-nak egy κ-automorfizmusává. A [12] 11.6.4 állításában válasszuk K-t κ-nak, L-et κ'-nek, M-et és C-t egyaránt $\bar{\kappa}$-nak, továbbá σ-t g-nek (hiszen g egy κ-t fixen hagyó beágyazása κ'-nek $\bar{\kappa}$-ba). Ekkor az említett állítás szerint g kiterjed $\bar{\kappa}$-nak egy g' injektív endomorfizmusává, ami κ-t elemenként fixen hagyja. Azt kell belátnunk, hogy ez automorfizmus lesz, ehhez a szürjektivitás hiányzik. Ehhez vegyünk egy $\gamma \in \bar{\kappa}$ elemet, és be kell látnunk, hogy ez benne van g' képében. Vegyük γ-nak az $F(y) \in \kappa[y]$ minimálpolinomját. Ekkor g' az F gyökeit F gyökeibe kell, hogy vigye, és mivel F-nek véges sok gyöke van, ezért g' injektivitása F gyökeinek halmazán szürjektivitást is jelent. Speciálisan megkapjuk γ-t, tehát $g' \in \mathrm{Gal}(\bar{\kappa}/\kappa)$, és készen vagyunk. □

4.3.8. Lemma. Legyen $L/K(x)$ véges Galois-bővítés, melynek G a Galois-csoportja, és tegyük fel, hogy G centruma triviális, továbbá L definiált $\kappa \leq K$ felett. Ekkor L_κ egyértelmű, vagyis pontosan egy $L_\kappa \subseteq L$ résztest van, amely n-edfokú és Galois $\kappa(x)$ felett, és reguláris κ felett.

Bizonyítás. Tegyük fel, hogy L_κ és $\widetilde{L}_\kappa$ is megfelel a definíciónak. Legyen $M \leq L$ az a résztest, amelyet L_κ és $\widetilde{L}_\kappa$ generál. Ekkor $M/\kappa(x)$ Galois, hiszen $L_\kappa/\kappa(x)$ és $\widetilde{L}_\kappa/\kappa(x)$ is Galois, innen pedig következik a [6] 2.5 állítás $(iv) \Rightarrow (i)$ irányból. Legyen κ' a κ algebrai lezártja M-ben. Ekkor κ', és így $\kappa'(x)$ invariáns a $\mathrm{Gal}(M/\kappa(x))$ minden elemére nézve, így a [6] 2.5 állítás $(ii) \Rightarrow (i)$ implikációja miatt $\kappa'(x)/\kappa(x)$ Galois (hiszen ha beágyazzuk M-et az algebrai lezártba, akkor M képe egyértelmű, és ekkor az invariancia miatt $\kappa'(x)$ képe is az). Ha θ' primitív eleme az $M/\kappa'(x)$ bővítésnek, akkor a 4.2.6 lemma miatt θ'-nek a $\kappa'(x)$ feletti minimálpolinomja irreducibilis $K(x)$ felett is, tehát a foka legfeljebb n (ahol $n = L/K(x)$), hiszen $\theta' \in L$. Ebből következik, hogy $|M : \kappa'(x)| \leq n$, viszont ha vesszük $L_\kappa/\kappa(x)$-nek egy primitív θ elemét, akkor a 4.3.2 lemma (a) része miatt $|\kappa'(x)(\theta) : \kappa'(x)| = n$, márpedig $\theta \in M$ miatt $|M : \kappa'(x)| \geq |\kappa'(x)(\theta) : \kappa'(x)|$. Ezek alapján $|M : \kappa'(x)| = n$, tehát $M = \kappa'(x)(\theta)$. Az $M = \kappa'(x)(\theta)$ testet generálja a $\kappa'(x)$ és az L_κ, továbbá a 4.2.6 lemma (a) része miatt $\kappa'(x) \cap L_\kappa = \kappa(x)$, hiszem L_κ reguláris κ felett. Emiatt a Galois-elmélet főtételét használva a $\mathrm{Gal}(M/L_\kappa)$ és a $\mathrm{Gal}(M/\kappa'(x))$ két olyan részcsoport $\mathrm{Gal}(M/\kappa(x))$-ben, melyek metszete $\{1\}$ (hiszen fixtesteik generálják M-et), és generálják $\mathrm{Gal}(M/\kappa(x))$-et (hiszen fixtesteik metszete $\kappa(x)$). A Galois-főtételéből könnyen kijön, hogy normálosztók is (lásd [2] 6.6.8 állítás, ebből következik, hogy egy részcsoport a Galois-csoportban pontosan akkor normálosztó, ha a hozzá tartozó közbülső test Galois az alaptest felett). Ebből ([2] 4.9.12 Tétel) megkaptuk, hogy

$$\mathrm{Gal}(M/L_\kappa) \times \mathrm{Gal}(M/\kappa'(x)) = \mathrm{Gal}(M/\kappa(x)).$$

Ugyanez teljesül L_κ helyett $\widetilde{L}_\kappa$-ra, ebből következik, hogy

$$\mathrm{Gal}(M/\widetilde{L}_\kappa) \times \mathrm{Gal}(M/\kappa(x)) = \mathrm{Gal}(M/\kappa(x)).$$

Mivel $M = \kappa'(x)(\theta)$, ezért a 4.3.2 lemma (a) és (b) része miatt $\mathrm{Gal}(M/\kappa'(x))$ izomorf G-vel. Emiatt $\mathrm{Gal}(M/\kappa'(x))$ centruma is triviális, tehát centralizátora $\mathrm{Gal}(M/\kappa(x))$-ben $\mathrm{Gal}(M/L_\kappa)$, de úgyanúgy $\mathrm{Gal}(M/\widetilde{L}_\kappa)$ is, tehát $L_\kappa = \widetilde{L}_\kappa$, vagyis beláttuk, hogy L_κ egyértelmű. □

4.3.9. Megjegyzés. Ha a fenti lemmában nem kötjük ki, hogy G centruma triviális legyen, de κ algebrailag zárt, akkor is igaz az állítás. Ha a bizonyításon végignézünk, akkor addig a pontig, hogy $M = \kappa'(x)(\theta)$, nem használtuk ki, hogy a centrum triviális, és ebből $\kappa = \kappa'$ miatt következik, hogy $M = \kappa(x)(\theta) = L_\kappa$, tehát valóban, L_κ egyértelmű.

Mostmár kimondható a κ felett definiáltság számunkra leginkább hasznos kritériuma, amelyet majd használunk.

4.3.10. Állítás. Legyen $L/K(x)$ véges Galois-bővítés, melynek G a Galois-csoportja, és tegyük fel, hogy G centruma triviális. Tegyük továbbá fel, hogy $\kappa \leq K$, és $K = \bar{\kappa}$. Ekkor L pontosan akkor definiált κ felett, ha minden $\alpha \in \mathrm{Gal}(\bar{\kappa}/\kappa)$ automorfizmusra létezik L-nek egy λ α-automorfizmusa, amelyre $\lambda^* = \mathrm{id}$.

Bizonyítás. A 4.3.5 lemmából következik az egyik irány, hiszen ha L definiált κ felett, és $\alpha \in \mathrm{Gal}(\bar{\kappa}/\kappa)$, akkor $\alpha|_\kappa = \mathrm{id}$, tehát az említett lemma második állításából készen vagyunk.

Nézzük a másik irányt. A 4.3.3 lemma alapján tudjuk, hogy L definiált κ-nak valamely $\kappa_1 \leq K$ végesen generált bővítése felett. Mivel $\kappa_1 \leq K$, ezért κ_1/κ algebrai bővítés, tehát mivel végesen generált és algebrai, ezért véges. Ezen kívül a 4.3.2 lemma miatt vehetjük κ_1 normális lezárását, tehát feltehetjük, hogy κ_1/κ véges Galois-bővítés, melyre L definiált κ_1 felett.

Legyen $L_1 = L_{\kappa_1}$. Szeretnénk belátni, hogy $L_1/\kappa(x)$ Galois. Vegyük $\kappa(x)$-nek a algebrai lezárását úgy, hogy az tartalmazza L_1-et. Legyen ez K_0. Vegyünk egy $\tau : L_1 \hookrightarrow K_0$ $\kappa(x)$-homomorfizmust. Ennek megszorítása $\kappa_1(x)$-re egy $\alpha_1 \in \mathrm{Gal}(\kappa_1/\kappa)$ elem, hiszen κ_1/κ Galois, és a 4.2.6 lemma alapján a megszorítás $\mathrm{Gal}(\kappa_1(x)/\kappa(x)) \to \mathrm{Gal}(\kappa_1/\kappa)$ izomorfizmus, és a [6] 2.5 Állítás $(i) \Rightarrow (ii)$ implikáció miatt $\alpha_1(\kappa_1(x)) = \kappa_1(x)$. Ezt a 4.3.7 tétel alapján kiterjeszthetjük egy $\alpha \in \mathrm{Gal}(\bar{\kappa}/\kappa)$ automorfizmussá. A feltevés szerint L-nek van egy λ_0 α-automorfizmusa, amelyre $\lambda_0^* = \mathrm{id}$. L_{κ_1} egyértelműsége miatt (4.3.8 Lemma) $\lambda_0(L_1) = L_1$. Legyen $\lambda_2 = \lambda_0|_{L_1}$. Tudjuk tehát, hogy $\lambda_2 \in \mathrm{Gal}(L_1/\kappa(x))$. Ha tekintjük a $\tau \circ \lambda_2^{-1} : L_1 \hookrightarrow K_0$ beágyazást, akkor ez fixen hagyja $\kappa_1(x)$-et, tehát $L_1/\kappa_1(x)$ Galois volta miatt $\tau \circ \lambda_2^{-1}(L_1) = L_1$ ([6] 2.5 Állítás $(i) \Rightarrow (ii)$). Ebből, és $\lambda_2(L_1) = L_1$-ből következik, hogy $\tau(L_1) = L_1$, tehát $L_1/\kappa(x)$ Galois ([6] 2.5 Állítás $(ii) \Rightarrow (i)$).

Vegyünk egy tetszőleges $\alpha_2 \in \mathrm{Gal}(\kappa_1/\kappa)$ elemet, és terjesszük ki a 4.3.7 szerint $\alpha_0 \in \mathrm{Gal}(\bar{\kappa}/\kappa)$ automorfizmussá. A feltevés szerint ez tovább kiterjed egy λ α_0-automorfizmussá, melyre $\lambda^* = \mathrm{id}$. Legyen $\lambda|_{L_1} = \lambda_1$. Mivel $\lambda^* = \mathrm{id}$, ezért minden $g \in G$-re $\lambda g = g\lambda$. Az L_1-re való megszorítással a 4.3.2 lemma (b) részéből azt nyerjük, hogy $\lambda_1 g_1 = g_1 \lambda_1$ minden $g_1 \in G_1 = \mathrm{Gal}(L_1/\kappa_1(x))$-re. Ez azt jelenti, hogy λ_1 benne van C-ben, ahol C a centralizátora G_1-nek $H = \mathrm{Gal}(L_1/\kappa(x))$-ben. Mivel minden $\alpha_2 \in \mathrm{Gal}(\kappa_1/\kappa)$ kiterjeszthető egy egy $\lambda_1 \in C$ elemmé, ezért ha tekintjük a H/G_1 faktorleképezést, akkor $H/G_1 \cong \mathrm{Gal}(\kappa_1(x)/\kappa(x))$ miatt (ez a Galois-elmélet főtételéből kijön, lásd [2] 6.6.7 Tétel (2), megjegyezvén, hogy $\kappa_1(x)/\kappa(x)$ Galois) ez C-re megszorítva szürjektív, tehát C és G_1 generálják H-t. Mivel $G_1 \cap C \subseteq Z(G_1)$, ezért $G_1 \cong G$ miatt (4.3.2 lemma (b)) $G_1 \cap C = \{1\}$ (hiszen G centruma triviális). Az világos, hogy G_1 normálosztó. Be kell látnunk, hogy C is az. Tehát ha $c \in C$, és $h \in H$, akkor

be kell látnunk, hogy $hch^{-1} \in C$, vagyis tetszőleges $g_2 \in G_1$-re $(hch^{-1})g_2(hch^{-1})^{-1} = g_2$. Tehát: $(hch^{-1})g_2(hch^{-1})^{-1} = hch^{-1}g_2hc^{-1}h^{-1}$, mivel $h^{-1}g_2h \in G$, ezért ez kommutál c-vel, vagyis c és c^{-1} kiesik, és látható, hogy a h-k és h^{-1}-ek is kiesnek, vagyis valóban g_2-t kapunk eredményül. Ezek alapján tehát C is normálosztó, tehát $G_1 \times C = H$ ([2] 4.9.12 Tétel).

Legyen L_κ a fixteste C-nek L_1-ben. Ekkor Artin tétele (2.1.1 Tétel) miatt L_1/L_κ Galois, és csoportja C. Ekkor világos, hogy $\mathrm{Gal}(L_\kappa/\kappa(x)) \times C = H$, amiből kapjuk, hogy $\mathrm{Gal}(L_\kappa/\kappa(x)) \cong G_1 \cong G$. A Galois-elmélet főtételének második állítása miatt $|L_\kappa : \kappa(x)| = |H : C| = |G_1|$, tehát $L_\kappa/\kappa(x)$ Galois, és $\mathrm{Gal}(L_\kappa/\kappa(x)) \cong G$.

Már csak az hiányzik, hogy L_κ reguláris κ felett. $C \leq H$ és $G_1 \leq H$ fixtesteinek metszete H fixteste kell, hogy legyen, hiszen G_1 és C generálják H-t, vagyis $L_\kappa \cap \kappa_1(x) = \kappa(x)$. Ha veszünk egy κ-együtthatós polinomot, és indirekt feltesszük, hogy van gyöke $L \setminus \kappa$-ban, akkor van gyöke $L_1 \setminus \kappa_1$-ben is, hiszen $L_\kappa \subseteq L_1$. Ez ellentmondás, hiszen L_1 reguláris κ_1 felett, tehát L reguláris κ felett. Ezzel készen vagyunk. □

4.3.11. Definíció (Racionális konjugáltosztály)**.** Legyen G egy csoport, melyre $|G| = n$. Ekkor G-nek egy C konjugáltosztályát racionálisnak nevezzük, ha minden olyan m pozitív egészre, amelyre $(m, n) = 1$, teljesül, hogy $C^m = C$. (Itt C^m alatt a következőt értjük: ha $g \in C$, akkor C^m a g^m konjugáltosztálya.)

4.3.12. Tétel. Legyen $L/K(x)$ véges Galois-bővítés, és $\kappa \leq K$ olyan, hogy $\bar{\kappa} = K$. Legyen $L/K(x)$ elágazási típusa $\mathcal{T} = [G, P, (C_p)_{p\in P}]$. Ekkor, ha $P \subset \kappa \cup \{\infty\}$, és minden $p \in P$-re C_p racionális, továbbá $\mathcal{T}$ merev, akkor L definiált κ felett.

Bizonyítás. Ellenőrizni fogjuk, hogy a 4.3.10 állítás által megadott feltételek teljesülnek-e. Mivel $L/K(x)$ típusa merev, ezért a 4.1.3 állítás alapján $G = \mathrm{Gal}(L/K(x))$ centruma triviális.

Rögzítsünk egy $\alpha \in \mathrm{Gal}(\bar{\kappa}/\kappa)$-t. A 4.3.5 lemma szerint van egy $\lambda : L \to L'$ α-izomorfizmus valamely L'-be, amelyre $L'/K(x)$ véges és Galois. Legyen $G' = \mathrm{Gal}(L'/K(x))$ és C_p, illetve C'_p a p-hez asszociált konjugáltosztály G-ben, illetve G'-ben. Legyen $|G| = n$ és $\varepsilon_n = e^{\frac{2\pi i}{n}} \in K$ (hiszen $K \leq \mathbb{C}$ algebrailag zárt). Legyen továbbá m az a szám, melyre $\alpha^{-1}(\varepsilon_n) = \varepsilon_n^m$, ekkor világos, hogy $(m, n) = 1$. Ha $p \in \mathbb{P}^1_K$, akkor a 2.2.7 lemma következtében $C'_p = \lambda^*(C_p)^m = \lambda^*(C_p^m) = \lambda^*(C_p)$ (hiszen a feltevés szerint $\alpha(p) = p$). Ez azt jelenti, hogy a $\lambda^* : G \to G'$ izomorfizmus biztosítja $L/K(x)$ és $L'/K(x)$ típusának ekvivalenciáját.

Feltehető, hogy valamely $F, F' \in K(x)[y]$ polinomokra $L = K(x)[y]/(F)$ és $L' = K(x)[y]/(F')$. Legyen $M = \mathbb{C}(x)[y]/(F)$ és $M' = \mathbb{C}(x)[y]/(F')$. Ekkor $M/\mathbb{C}(x)$ Galois (ugyanúgy $M'/\mathbb{C}(x)$ is), hiszen $L \leq M$, és L tartalmazza F összes gyökét, és így M is. Ezenkívül M és M' reguláris $\mathbb{C}$ felett, hiszen $\mathbb{C}$ algebrailag zárt. Ugyanígy L és L' reguláris K felett, tehát a 4.2.6 lemma (b) részének következtében F és F' irreducibilis $\mathbb{C}(x)$ felett is, így $|L : K(x)| = \deg(F) = |M : \mathbb{C}(x)|$ és $|L' : K(x)| = \deg(F') = |M' : \mathbb{C}(x)|$, vagyis M, és M' is definiált K felett, továbbá M_K $K(x)$-izomorf L-lel és M'_K $K(x)$-izomorf L'-vel. Ekkor a 4.3.2 lemma (c) része miatt $M/\mathbb{C}(x)$ és $M'/\mathbb{C}(x)$ típusa megegyezik $L/K(x)$ típusával. Ez a típus merev, így a 4.1.5 tétel következtében M és M' $\mathbb{C}(x)$-izomorf egymással. A 4.3.9 megjegyzés miatt minden $M \to M'$ $\mathbb{C}(x)$ izomorfizmus M_K-t M'_K-be képezi, tehát a megszorítás egy $K(x)$-izomorfizmus M_K és M'_K között, tehát L és L' $K(x)$-izomorfak.

Legyen $\mu \in \mathrm{Hom}_{K(x)}(L', L)$ izomorfizmus. Ekkor a $\chi := \mu\lambda$ egy α-automorfizmusa L-nek. Mivel, amint láttuk, $\lambda^*(C_p) = C'_p$, ezért $\chi^*(C_p) = \mu^*(\lambda^*(C_p)) = \mu^*(C'_p) = C_p$.

Mivel χ^* fixen hagyja a C_p konjugáltosztályokat, ezért ez megfelel a 4.1.2 definícióbeli γ automorfizmusnak (hiszen a definícióban előálló generátorok képei is nyilván megfelelőek lesznek), és mivel a típus merev, ezért χ^* előáll, mint egy $g \in G$ elemmel való konjugálás, vagyis $\chi^* = g^*$. Ekkor a $\psi = g^{-1}\chi$ nyilván egyrészt α-automorfizmusa L-nek (hiszen g fixen hagyja K-t), és az is világos, hogy $\psi^* = \mathrm{id}$. Ez a ψ tehát teljesíti a 4.3.10 állítás feltételeit, vagyis az említett állítás miatt L definiált κ felett. □

4.4. Merevség és alkalmazásai

Az utolsó alfejezetben kimondjuk és belátjuk belátjuk a merevségi tételt, majd ismertetjük egy alkalmazását.

4.4.1. Tétel. Legyen G egy véges csoport, melynek vannak $C_1, ..., C_r$ konjugáltosztályai, amelyek racionálisak és merev r-est alkotnak. Legyen továbbá $P = \{p_1, ..., p_r\} \subset \mathbb{Q} \cup \{\infty\}$ tetszőleges r elemű halmaz, $C_{p_i} = C_i$ és $\mathcal{T} = [G, P, (C_p)_{p \in P}]$. Ekkor van olyan $L/\mathbb{C}(x)$ bővítés, melynek típusa $\mathcal{T}$, és amely bővítés definiált $\mathbb{Q}$-nak egy tisztán transzcendens $\mathbb{Q}(x_1, ..., x_n)$ bővítése felett.

Bizonyítás. Világos, hogy a $\mathcal{T}$ egy merev típus. Ekkor a 4.1.5 tétel következtében létezik egy $L/\mathbb{C}(x)$ bővítés, melynek típusa $\mathcal{T}$. Ez definiált $\mathbb{Q}$-nak egy végesen generált κ_1 bővítése felett (4.3.3 Lemma). A 4.2.5 megjegyzés miatt van $\mathbb{Q}$-nak egy $\kappa = \mathbb{Q}(x_1, ..., x_s)$ bővítése, ahol $x_1, ..., x_s$ független transzcendens elemek $\mathbb{Q}$ felett, és κ_1/κ véges. Legyen $K = \bar{\kappa}$.

A 4.3.2 lemma (a) része miatt L definiált K felett (hiszen $\kappa_1 \leq K$). Ekkor $L_K/K(x)$ típusa a 4.3.2 lemma (c) része miatt $\mathcal{T}$. A 4.3.12 tétel feltételei az L_K, K, κ hármasra triviálisan teljesülnek, hiszen $\mathbb{Q} \subseteq \kappa$, tehát L_K definiált κ felett. Emiatt L is definiált κ felett (hiszen az L-hez tartozó L_κ résztestet választhatjuk ugyanannak, mint az L_K-hoz tartozót). Ezzel készen vagyunk. □

4.4.2. Tétel (Merevségi tétel)**.** Legyen G egy véges csoport, melynek vannak $C_1, ..., C_r$ konjugáltosztályai, amelyek racionálisak és merev r-est alkotnak. Ekkor G előáll $\mathbb{Q}$ egy Galois-bővítésének Galois-csoportjaként.

Bizonyítás. Vegyünk egy tetszőleges r elemű $P = \{p_1, ..., p_r\} \subset \mathbb{Q} \cup \{\infty\}$ halmazt. Legyen $C_{p_i} := C_i$, ha $i = 1, ..., r$. Ekkor, ha $\mathbf{C} = (C_p)_{p \in P}$, akkor tekintsük a $\mathcal{T} = [G, P, \mathbf{C}]$ típust. A 4.4.1 tétel miatt van egy $\kappa = \mathbb{Q}(x_1, ..., x_n)$ tisztán transzcendens bővítés, illetve egy $L/\mathbb{C}(x)$ $\mathcal{T}$ típusú bővítés, amely definiált κ felett. Ekkor a 4.3.2 lemma (b) része miatt $G \cong \mathrm{Gal}(L_\kappa/\kappa(x)) = \mathrm{Gal}(L_\kappa/\mathbb{Q}(t_1, ..., t_s, x))$. Ekkor a 4.2.2 tétel alapján van egy $M/\mathbb{Q}$ bővítés, amelyre $\mathrm{Gal}(M/\mathbb{Q}) \cong G$. □

Ez a tétel azért nagyon fontos, mert tisztán csoportelméleti kritériumot ad arra, hogy egy csoport előálljon, mint $\mathbb{Q}$ egy Galois-bővítésének Galois-csoportja. A fejezet zárásaként előállítjuk a szimmetrikus és alternáló csoportokat $\mathbb{Q}$ felett.

4.4.3. Lemma. Legyen G egy véges csoport, benne C_1, C_2, C_3 konjugáltosztályok. Legyenek továbbá g_1, g_2, g_3 elemek G-ben úgy, hogy $g_i \in C_i$ és $g_1 g_2 g_3 = 1$. Ekkor a (C_1, C_2, C_3) hármas pontosan akkor merev, ha G centruma triviális, és minden $g_2' \in C_2$-re, amelyre $(g_1 g_2')^{-1} \in C_3$, valamint g_1 és g_2' generálják G, teljesül az is, hogy van olyan $h \in G$, amelyre $hg_1h^{-1} = g_1$ és $hg_2'h^{-1} = g_2$.

Bizonyítás. Nézzük az egyik irányt. Ha a (C_1, C_2, C_3) hármas merev, akkor a 4.1.3 állítás miatt G centruma triviális. A $g_1, g_2', (g_1 g_2')^{-1}$ hármas ekkor megfelelő generátorok a merevség definíciójához, tehát van olyan $h \in G$, amelyre $hg_1h^{-1} = g_1$ és $hg_2'h^{-1} = g_2$. Ezzel az egyik irány készen van.

Most a másik irány következik. A 4.1.3 állítás alapján, ha G centruma triviális, akkor elegendő annyit ellenőrizni, hogy tetszőleges másik hármasra, ami kielégíti a merevség definíciójában lévő feltételeket, van olyan elem G-ben, amely az egyik hármast átkonjugálja a másikba, hiszen ezen elemnek az egyértelműsége következik az említett állításból. Az világos, hogy ha konjugálunk egy megfelelő generátorhármast, akkor ismét megfelelő hármashoz jutunk, tehát ha van egy másik g_1', g_2', g_3' hármasunk, akkor feltehető, hogy $g_1' = g_1$. Ekkor világos, hogy g_2' eleget tesz a fenti követelményeknek, így a feltétel szerint létezik egy $h \in G$ elem, amelyre $hg_1h^{-1} = g_1$ és $hg_2'h^{-1} = g_2$, amiből következik, hogy $hg_3'h^{-1} = g_3$. Ezzel készen vagyunk. □

4.4.4. Lemma. Jelöljük $C^{(i)}$-vel S_n (itt $n \geq 3$) azon konjugáltosztályát, amelyben az i hosszúságú ciklusok vannak (világos, hogy az i hosszú ciklusok konjugáltosztályt alkotnak). Ekkor $C^{(2)}$, $C^{(n-1)}$ és $C^{(n)}$ merev hármast alkot S_n-ben.

Bizonyítás. Tekintsük a $\tau = (n-1, n)$, $\sigma = (1, ..., n-1)$, és $\pi = (n-1, n, n-2, ..., 2, 1)$ ciklusokat. Ezek láthatóan a megfelelő konjugáltosztályokból kerülnek ki. Az 1.1.1 lemma alapján $(1, 2, 3, ..., n) = \tau \cdot \pi^{-1} \cdot \tau$ és $(n-1, n) = \tau_2$ generálja S_n-et (hiszen $n-(n-1) = 1$), tehát τ, σ és π generálja S_n-et. Az világos, hogy $\sigma \cdot \tau \cdot \pi = 1$. A 4.4.3 lemma alapján elég két dolgot ellenőrizni: az világos, hogy ha $n \geq 3$, akkor S_n centruma triviális. Most tegyük fel, hogy $\tau' \in C^{(2)}$, és τ', illetve σ generálják G-t, és $\tau'\sigma \in C^{(n)}$. Világos, hogy ekkor $\tau' = (j, n)$ alakú. Az is teljesül továbbá, hogy $\sigma^{n-1-j}\tau'(\sigma^{n-1-j})^{-1} = 1$, hiszen transzpozíció konjugáltja transzpozíció és világos, hogy az $n-1$-et a j-be viszi. Az triviális, hogy σ^{n-1-j} a σ-t önmagába konjugálja, így a 4.4.3 lemmából készen vagyunk. □

4.4.5. Lemma. Legyen G véges csoport, benne (C_1, C_2, C_3) merev, racionális konjugáltosztályokból álló hármas. Ekkor G-nek minden 2 indexű részcsoportja előáll $\mathbb{Q}$ egy Galois-bővítésének Galois-csoportjaként.

Bizonyítás. Válasszunk három különböző $p_1, p_2, p_3 \in \mathbb{Q}$ számot. Legyen $C_i = C_{p_i}$ és $P = \{p_1, p_2, p_3\}$. Ha $\mathcal{T} = [G, P, (C_p)_{p \in P}]$, akkor a 4.4.1 tétel miatt létezik egy tisztán transzcendens $\kappa = \mathbb{Q}(t_1, ..., t_s) \subset \mathbb{C}$ bővítése $\mathbb{Q}$-nak, és egy $L/\mathbb{C}(x)$ véges Galois-bővítés, melynek típusa $\mathcal{T}$ és definiált κ felett. Legyen $M = L_\kappa$.

Ekkor $\mathrm{Gal}(M/\kappa(x)) \cong G$ egy rögzített μ izomorfizmussal. Legyen $H \leq G$ egy tetszőleges 2 indexű részcsoport. A Galois-elmélet főtételében ennek megfelelő $N \leq M$ testre teljesül, hogy $|N : \kappa(x)| = |G : H| = 2$. Mivel minden véges szeparábilis bővítés egyszerű ([6] 1.15 Tétel), ezért van $N/\kappa(x)$-nek egy primitív θ eleme (hiszen 0 karakterisztikában minden bővítés szeparábilis). Mivel a bővítés foka 2, ezért $\theta^2 := f \in \kappa(x)$. Ekkor tehát $N = \kappa(x)(\theta)$. Tegyük fel, hogy $f(x) = \frac{P(x)}{Q(x)}$ valamely $P, Q \in \kappa[x]$ polinomokra. Ekkor $\kappa(x)(\theta) = \kappa(x)(\theta \cdot Q(x))$, tehát θ-t $\theta \cdot Q(x)$-re cserélve feltehető, hogy $f \in \kappa[x]$. Feltehető továbbá, hogy ha f-et $\kappa[x]$-ben irreducibilis tényezők szorzatára bontjuk, akkor minden tényező maximum egyszer szerepel (hiszen különben θ ismét szorozható megfelelő polinommal). Ekkor az is teljesül, hogy f-nek nincsen többszörös gyöke $\mathbb{C}$-ben, hiszen ha indirekt feltesszük, hogy van, akkor ezen gyök minimálpolinomja κ felett legalább kétszer szerepel f

tényezői között, ami ellentmondás. Mivel M reguláris κ felett, ezért f nem lehet konstans. Ekkor θ minimálpolinomja $y^2 - f$, amelynek másik gyöke $-\theta$, így $N/\kappa(x)$ Galois. Ekkor világos, hogy f-ből nem lehet négyzetgyököt vonni $\mathbb{C}(x)$-ben, tehát $N' := \mathbb{C}(x)(\theta)$ mellett $N'/\mathbb{C}(x)$ kvadratikus bővítés, és ugyanúgy, mint az előbb, ez is Galois.

A 2.2.3 lemma (d) része alapján az $N'/\mathbb{C}(x)$ bővítés elágazási pontjai az $L/\mathbb{C}(x)$ elágazási pontjai közül kerülnek ki, nevezetesen p_1, p_2 és p_3 közül. Írjuk fel f-et $\mathbb{C}[x]$-ben gyöktényezőkre bontva:

$$f(x) = c\prod_{i=1}^{n}(x - q_i),$$

ahol a q_i-k mind különbözőek. Nézzük meg így az $N'/\mathbb{C}(x)$ bővítés elágazási pontjait. Tekintsük először a q_j elemeket. A $\vartheta_{q_j} : \mathbb{C}(x) \to \mathbb{C}(t), x \mapsto t + q_j$ függvényt kell kiterjeszteni. Ekkor ϑ_{q_j} az f-et a $\vartheta_{q_j} f(t) = c\prod_{i=1}^{n}(t + q_j - q_i)$-ba küldi, tehát θ ennek a négyzetgyökébe megy. Láthatóan $\vartheta_{q_j} f(t) = t \cdot h_0(t)$, ahol $h_0(t)$ konstans tagja nem nulla, és így a 2.3.7 lemma alapján van négyzetgyöke $\mathbb{C}((t))$-ben. A 2.2.3 lemmabeli Δ-nak tartalmaznia kell $\vartheta_{q_j} f(t)$ négyzetgyökét, és az előző megállapítás miatt pontosan akkor van $\vartheta_{q_j} f(t)$-nek négyzetgyöke Δ-ban, ha t-nek van, tehát Λ_2 jó választás Δ-nak. Az is világos ebből (mivel Λ-ban t-nek nincsen négyzetgyöke), hogy q_j elágazási pont. Hogyha választunk egy $a \in \mathbb{C}$ elemet, amely különbözik minden q_i-től, akkor a 2.3.7 lemma miatt van Λ-ban n-edik gyöke $\vartheta_a f(t)$-nek, és így a nem elágazási pont (hiszen $\Delta = \Lambda$ választással a $\mathrm{Gal}(\Delta/\Lambda)$ kitüntetett generátora triviális, így $g_{\vartheta_a} = 1$). Már csak a ∞ van hátra. A $\vartheta_\infty : \mathbb{C}(x) \to \mathbb{C}(t), x \mapsto 1/t$ függvényt kell kiterjszteni. Világos, hogy

$$\vartheta_\infty f(t) = ct^{-n}\prod_{i=1}^{n}(1 - q_i t) = t^{-n}h_1(t),$$

és θ-t ennek a négyzetgyökébe kell küldeni. Világos, hogy mivel ismét a 2.3.7 lemma miatt $h_1(t)$-nek van négyzetgyöke Λ-ban, ezért $\vartheta_\infty f(t)$-ből pontosan akkor tudunk Δ-ban négyzetgyököt vonni, ha t^{-n}-ből tudunk, ekvivalensen ha t^n-ből tudunk. Mivel az elágazási pontok a p_1, p_2, p_3-ból kerülnek ki, ezért a ∞ nem elágazási pont, tehát t^n-ből tudunk Λ-ban négyzetgyököt vonni, ami azt jelenti, hogy n páros. Az $n = 0$ eset nem lehetséges, mivel f nem konstans. Továbbá mivel az előbbiek alapján f gyökei a p_i-k közül kerülnek ki, ezért $\deg(f) = n \leq 3$, tehát $n = 2$. Mivel a p_i-k szerepe szimmetrikus, ezért feltehető, hogy $f(x) = c(x - p_1)(x - p_2)$ (hiszen f-nek nincs többszörös gyöke).

Legyen $z = \frac{\theta}{x - p_2}$. Világos, hogy $\kappa(x)(\theta) = \kappa(x)(z)$, ahol $z^2 = \frac{cx - xp_1}{cx - cp_2}$, vagyis ez x-nek egy lineáris törtfüggvénye. Ekkor $x \in \kappa(z^2)$ (lásd 2.3.1 állítás bizonyítása, ennél az iránynál nem használtuk K algebrai zártságát), tehát $N = \kappa(x)(\theta) = \kappa(x)(z) = \kappa(z)$ izomorf a racionális törtfüggvények testével. Ekkor $H \cong \mathrm{Gal}(M/N) = \mathrm{Gal}(M/\kappa(z)) = \mathrm{Gal}(M/\mathbb{Q}(t_1, ..., t_s, z))$, ahonnan a 4.2.2 tételből készen vagyunk. □

4.4.6. Következmény. Minden szimmetrikus és alternáló csoport előáll $\mathbb{Q}$ egy Galois-bővítésének Galois-csoportjaként.

Bizonyítás. Valóban, S_n előáll a 4.4.2 tétel miatt, hiszen a 4.4.4 lemmában leírt konjugáltosztályok nyilván racionálisak, nem csak merevek, és A_n szintén előáll a 4.4.5 lemma következtében, hiszen ez S_n-nek egy 2 indexű részcsoportja. □

Irodalomjegyzék

[1] Szűcs András. *Topológia*. URL: http://bolyai.cs.elte.hu/~szucs/Top1-2.pdf.

[2] Kiss Emil. *Bevezetés az algebrába*. Elméleti matematika. Typotex, 2007. ISBN: 978-963-9664-48-7.

[3] Halász Gábor. *Bevezető Komplex Függvénytan*. Komplex függvénytani füzetek. Typotex, 2008. ISBN: 978-963-9664-95-1.

[4] Moussong Gábor. *Geometria*. URL: http://etananyag.ttk.elte.hu/FiLeS/downloads/_19_Moussong_Geometria.pdf.

[5] Zábrádi Gergely. *Algebrai számelmélet jegyzet*. URL: https://zabradi.web.elte.hu/Jegyzetek/algszamjegyzet.pdf.

[6] Zábrádi Gergely. *K-homomorfizmusok, szeparábilis bővítések, Galois-elmélet*. URL: https://zabradi.web.elte.hu/Jegyzetek/szeparabilis.pdf.

[7] Zábrádi Gergely. *Racionális együtthatós polinomok Newton-poligonja*. URL: https://zabradi.web.elte.hu/Jegyzetek/Newton_poligon.pdf.

[8] Eknath Ghate. *The Kronecker-Weber Theorem*. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.614.5118&rep=rep1&type=pdf.

[9] B.H. Matzat Gunter Malle. *Inverse Galois theory*. 1. kiad. Springer monographs in mathematics. Springer, 2002. ISBN: 3540628908.

[10] David Harbater. "Riemann's Existence Theorem". *"The Legacy of Bernhard Riemann After 150 Years" (ed. by L. Ji, F. Oort, S.-T. Yau), Higher Education Press and International Press, Beijing-Boston* (2015), 275–286. old.

[11] D. Hilbert. "Uber die Irreducibilitat ganzer rationaler Functionen mit ganzzahligen Coefficienten". ger. *J. reine angew. Math.* 110 (1892), 104–129. old.

[12] Pelikán József. *Algebra jegyzet*. URL: https://pelikan.web.elte.hu/11_Testek.pdf. Testek, testbővítések fejezet.

[13] F. Klein. "Ueber binäre Formen mit linearen Transformationen in sich selbst". ger. *Mathematische Annalen* 9 (1875), 183–208. old. URL: http://eudml.org/doc/156695.

[14] Serge Lang. *Algebra*. 3. kiad. Graduate Texts in Mathematics 211. Springer-Verlag New York, 2002. ISBN: 9780387953854.

[15] Alexander Schmidt és Kay Wingberg. "Safarevic's theorem on solvable groups as Galois groups". (1998. okt.). URL: https://arxiv.org/abs/math/9809211.

[16] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics Series. A K Peters, 1992. ISBN: 0867202106.

[17] Kuang-yen Shih. "On the construction of Galois extensions of function fields and number fields". *Mathematische Annalen* 207 (1974), 99–120. old. URL: https://doi.org/10.1007/BF01362150.

[18] John G. Thompson. "Some finite groups which appear as Gal L/K, where $K \subseteq Q(\mu_n)$". *Group Theory, Beijing 1984*. Szerk. Hsio-Fu Tuan. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, 210–230. old. ISBN: 978-3-540-39793-9.

[19] Helmut Völklein. *Groups as Galois Groups: An Introduction*. Cambridge Studies in Advanced Mathematics. Press Syndicate of the University of Cambridge, 1996. ISBN: 0-521-56280-5.

[20] Tom Weston. *Algebraic Number Theory*. URL: `https://people.math.umass.edu/~weston/cn/notes.pdf`.