Algebrai számelmélet
jegyzet

Zábrádi Gergely

2020. november 3.

Tartalomjegyzék

1. fejezet

Bevezetés

Ez a jegyzet a 2014 tavaszi félévben tartott Algebrai Számelmélet c. ELTE Matematikus MSc kurzus alapján készül, és folyamatosan frissül. Az esetleges hibákat/elírásokat szívesen veszem emailben a `zger@cs.elte.hu` email-címre. Köszönöm Csige Tamásnak, Ta The Anhnak, Hoksza Zsoltnak és Seress Dánielnek a segítséget az elírások megtalálásában.

1.1. Miről szól az algebrai számelmélet? – Régen és most

Az algebrai számelmélet eredete a diofantikus egyenletek megoldására tett kísérletekre vezethető vissza. *Diofantosz* az i.sz.i 3. századi alexandriai matematikus volt, aki egészegyütthatós többváltozós polinomegyenleteket vizsgált, és megoldási módszereket dolgozott ki rájuk. Fő műve, az *Arithmetica* sajnos nem maradt fenn teljes egészében. Ennek a könyvnek a margójára írta a francia matematikus *Pierre de Fermat* 1637-ben, hogy $n > 2$ esetén az

$$x^n + y^n = z^n$$

egyenletnek nincs nemtriviális (azaz olyan, amikor $xyz \neq 0$ megoldása az egész számok körében. Ma már azt gondoljuk, hogy Fermat állítólagos bizonyítása – ami nem fért oda a margóra – jó eséllyel hibás volt. Egy lehetséges magyarázat, hogy bizonyítás nélkül felhasználta a *számelmélet alaptételét* az $a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ alakú számok körében, ahol $a_0, \ldots, a_{p-2} \in \mathbb{Z}$, ζ_p pedig egy rögzített primitív p-edik egységgyök valamely p prímszámra. Abban az esetben, ha a számelmélet alaptétele valóban teljesül ezen számok körében, vagy ennél gyengébb feltevéssel, ha p nem osztja az osztályszámot (azaz p egy ún. *reguláris prím*), akkor létezik egy viszonylag elemi bizonyítás a Fermat–sejtésre (*Ernst Kummer* tétele 1850 körül, lsd. 3.12.1. fejezet), de a szomorú igazság az, hogy nem minden p prím reguláris. Sőt, máig megoldatlan probléma, hogy létezik-e végtelen sok reguláris prím (azt tudjuk, hogy létezik végtelen sok *irreguláris*), bár numerikus számítások azt mutatják, hogy a prímek $e^{-1/2}$ része (azaz kb. 60,65%-a) reguláris – ez Siegel sejtése.

Amint a fenti példa is mutatja, fontos kérdés, hogy mely „számok" körében igaz a számelmélet alaptétele, azaz mikor egyértelmű az elemek prímfelbontása. A német matematikus, *Carl Friedrich Gauß* (újra)felismerte ennek fontosságát, és igazolta a számelmélet alaptételét az ún. Gauß-egészek ($a + bi$ alakú számok, $a, b \in \mathbb{Z}$) körében. Túlzás nélkül állíthatjuk, hogy a 19. század elején forradalmasította az algebrai számelmélet (a matematika más területeivel egyetemben): jópár modern elmélet csírája megjelenik már nála – mint pl. az L-függvények

bevezetése vagy az elliptikus görbék komplex szorzása. Gaußnevéhez fűződik a kvadratikus reciprocitási tétel bizonyítása is, amit akár a Langlands program előfutárának is nevezhetünk.

A következő mérföldkő *Peter Gustav Lejeune Dirichlet* munkája volt, aki – modern terminológiával élve – az első „osztályszámformulát" bizonyította kvadratikus formákra 1838-ban. Nevéhez fűződik a Dirichlet-féle egységtétel is (lsd. 3.6.3. fejezet). *Richard Dedekind* nevéhez fűződik az ideál fogalmának megalkotása (1879), ami alapvető fontosságúnak bizonyult a későbbiekben a gyűrűelmélet kialakulásában és fejlődésében. Az ideálokra vonatkozó egyértelmű prímfaktorizáció egy gyengítése a számelmélet alaptételének, mely teljesül a racionális számok tetszőleges véges bővítésében levő algebrai egészek gyűrűjében, és ezáltal a mai napig alapvető fontosságú az algebrai számtestek modern elméletében.

David Hilbert a matematika sok más területével együtt az algebrai számelméletet is modernizálta a 20. század elején. Nevéhez fűződik számos sejtés *osztálytest-elméletben*, melyek nagy részét később *Teiji Takagi*, illetve *Emil Artin* bizonyították a 20-as, 30-as években. A moduláris formák elméletének kidolgozásában is jelentős volt a szerepe. Az Artin-féle reciprocitási tétel fontos mérföldkő volt a Langlands program kialakulásában.

A modern időkben több részterület is fejlődött egymással párhuzamosan, ezekre külön kitérünk röviden. Persze ezek is szorosan összekapcsolódnak egymással.

1.1.1. Diofantikus approximáció, transzcendenciaelmélet

Az alapvető kérdés, hogy egyes irracionális valós számok mennyire közelíthetők racionálisakkal. Dirichlet approximációs tétele szerint tetszőleges α irracionális számhoz végtelen sok olyan $\frac{p}{q} \in \mathbb{Q}$ racionális szám létezik, melyre $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$. Ezt javította meg *Émile Borel* 1903-ban, belátva, hogy a jobb oldalra az erősebb $\frac{1}{\sqrt{5}q^2}$ becslés is írható.

Megfordítva, egyes irracionális számok, nevezetesen az algebrai számok nem közelíthetők túl jól racionálisakkal. Ebben az irányban az első eredmény *Joseph Liouville* nevéhez fűződik az 1840-es évekből, mely szerint ha α gyöke egy legfeljebb n-edfokú racionális együtthatós polinomnak, akkor van olyan (α-tól függő) $c > 0$ konstans, melyre $|\alpha - \frac{p}{q}| > \frac{c}{q^n}$ tetszőleges p és $q \neq 0$ egész számokra. Speciálisan a $\sum_{n=0}^{\infty} 10^{-n!}$ szám nem lehet algebrai, hiszen túl jól lehet közelíteni racionálisakkal. Ennek messzemenő továbbfejlesztése a Thue–Siegel–Roth tétel, mely szerint $\frac{c}{q^{2+\varepsilon}}$-os alsó becslés is igaz (ahol $\varepsilon > 0$ tetszőleges és a c már nemcsak α-tól, hanem ε-tól is függ).

Kapcsolódó fejezet az ún. transzcendencia-elmélet, melynek segítségével különböző valós számok transzcendenciáját lehet igazolni. Az első hatalmas áttörés a Gelfond–Schneider tétel, mely Hilbert 7. problémájára ad pozitív választ: ha a és b algebrai számok úgy, hogy $a \neq 0{,}1$ és b irracionális, akkor a^b bármely értéke transzcendens. Ennek messzemenő általánosítása *Alan Baker* tétele, amiért Baker 1970-ben Fields-érmet kapott. A Fileds-érem odaítélésének fő oka az volt, hogy Baker tétele effektív megoldási módszert adott bizonyos diofantikus egyenletekre, és annak igazolására, hogy egyes egyenleteknek nincs egész megoldása. Bizonyos egyenletek esetében Baker módszere ad egy explicite kiszámolható konstanst, aminél nagyobb abszolútértékű megoldása nem lehet az adott egyenletnek. Ez abban az időben hatalmas áttörésnek számított. Az explicit konstans ugyan általában annyira nagy, hogy az összes megoldás meghatározása közvetlenül még számítógép segítségével sem lehetséges, de más módszerek – mint pl. a Lenstra–Lenstra–Lovász algoritmus – kombinálásával már ez is lehetséges bizonyos esetekben. Íme a tétel (effektív formában):

1.1.1. Tétel (Baker). *Legyenek $\lambda_1, \dots, \lambda_n$ olyan komplex számok, melyekre e^{λ_j} algebrai minden $j = 1, \dots, n$-re, és tegyük fel, hogy $\lambda_1, \dots, \lambda_n$ lineárisan független $\mathbb{Q}$ felett. Továbbá ha $\beta_0, \dots, \beta_n$ nem mind 0 algebrai számok, akkor*

$$|\beta_0 + \beta_1\lambda_1 + \cdots + \beta_n\lambda_n| > H^{-C} \ ,$$

ahol H a β-k magasságának *maximuma (egy konstans, ami csak a β-któl függ), és C egy effektíven kiszámolható szám, ami n-től, a λ-któl, és a β-k fokának maximumától függ. Speciálisan ez a szám nem lehet 0, azaz a λ-k és az 1 nemcsak a racionálisak felett lineárisan függetlenek, hanem az algebrai számok felett is.*

Ennek következménye, hogy az $a_1^{b_1} \dots a_n^{b_n}$ alakú számok mind transzcendensek, ha a b_i-k mind algebrai, de irracionális számok, melyekre $1, b_1, \dots, b_n$ lineárisan független $\mathbb{Q}$ felett, az a_i-k pedig 0-tól és 1-től különböző algebrai számok ($i = 1, \dots, n$).

1.1.2. Aritmetikai algebrai geometria

Az aritmetikai algebrai geometria egy önmagában is szerteágazó része az algebrai számelméletnek. A klasszikus algebrai geometriában polinomegyenletek nullhelyeit (az ún. algebrai varietásokat) vizsgáljuk az affin vagy még inkább a projektív térben. Hilbert nullhelytételének köszönhetően ez technikailag akkor a legkönnyebb (bár akkor sem könnyű, sőt!), ha az alaptest algebrailag zárt (heurisztikusan ennek az az oka, hogy algebrailag zárt test fölött minden egyváltozós polinomnak pontosan annyi gyöke van multiplicitással számolva, amennyi a foka). Ugyanakkor a számelméletben minket nem egy algebrailag zárt test fölötti megoldások érdekelnek, hanem pl. a racionális test feletti megoldások. Az alapvető ötlet ennek kiküszöbölésére a következő: először tekintjük az adott racionális együtthatós $f_1, \dots, f_k \in \mathbb{Q}[x_1, \dots, x_n]$ egyenletek $V(\overline{\mathbb{Q}}) \subseteq \overline{\mathbb{Q}}^n$ megoldásait a $\overline{\mathbb{Q}}$ algebrai lezárt fölött, ahol a klasszikus algebrai geometria módszerei alkalmazhatók. Majd a racionális megoldások nem mások, mint a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *Galois csoport fixpontjai*. Ezért az algebrai számelmélet egyik alapvető célja a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ csoport mélyebb megértése. Ehhez kapcsolódik a máig megoldatlan inverz Galois probléma, hogy minden véges csoport előáll-e ennek a csoportnak a faktorcsoportjaként, vagyis $\mathbb{Q}$ egy véges Galois bővítésének Galois csoportjaként. Gyakran a geometriai objektumokon van egy extra Abel-csoport struktúra is: pl. a legegyszerűbb esetben, amikor a test additív vagy multiplikatív csoportját vesszük, de nagyon fontos példa az elliptikus görbék esete is, melyek pontjain természetes módon értelmezhető egy összeadás művelet. Ekkor a Galois-invariánsok képzése vizsgálható a homologikus algebra eszközeivel: az invariáns-képzés funktor derivált funktorai nem mások, mint a Galois-kohomológia csoportok, melyek alapvető fontosságúak az elméletben.

Egy másik, alapvető fontosságú módszer, hogy nemcsak racionális vagy egész megoldásokat keresünk, hanem modulo p megoldásokat, ahol p egy prímszám, és ezekből próbálunk visszakövetkeztetni az egész, ill. racionális megoldásokra. Ahhoz, hogy ezt a módszert szisztematikusan kiaknázzuk, szükség volt Grothendieck és tanítványainak forradalmasító munkásságára, többek között a *sémák* definíciójára. Ugyanis racionális együtthatós egyenleteket nem lehet modulo p redukálni, csak *egész együtthatós* egyenleteket, tehát szükség volt arra, hogy ne csak testek, hanem tetszőleges egységelemes kommutatív gyűrűk felett csináljunk geometriát. Ebben a szemléletben ha vannak $f_1, \dots, f_k \in \mathbb{Z}[x_1, \dots, x_n]$ polinomjaink, akkor az $R := \mathbb{Z}[x_1, \dots, x_n]/(f_1, \dots, f_k)$ gyűrű *spektrumát*, azaz prímideáljanak (különböző extra

struktúrákkal ellátott) halmazát tekintjük. Pl. Spec$\mathbb{Z}$ a prímszámokból és a (0)-ból áll, és a $\mathbb{Z} \to R$ leképezés (mely egy egész számot a hozzá tartozó konstans polinomba küld) megad egy Spec$R \to$ Spec$\mathbb{Z}$ leképezést a spektrumokon, melynek a p prímszám feletti fibrumára (ősképére) tekinthetünk úgy, mint az egyenletrendszer modulo p redukciójára, az. ún. *generikus* ((0) fölötti) fibrumára pedig mint az egyenletrendszer racionális megoldásaira.

A fenti módszer egyfajta továbbfejlesztése a következő: Veszünk egy p prímszámot, és az egyenletünknek nemcsak modulo p, hanem minden pozitív egész r kitevőre a modulo p^r megoldásait vizsgáljuk. Nyilván ha valamely p^r prímhatványra nincs megoldása egy egész együtthatós polinomegyenletnek modulo p^r, akkor az egész számok körében sem lehet megoldása. Hasonlóképp, ha nincs $\mathbb{R}$ feletti megoldás, akkor sem lehet egész megoldás sem. Az izgalmas kérdés az, hogy milyen feltételekkel igaz ennek a megfordítása, azaz ha van $\mathbb{R}$ feletti megoldás, és minden p prímre és p^r hatványra van modulo p^r megoldás, akkor ebből következik-e, hogy létezik egész megoldás is. Ez az ún. Hasse-féle lokál–globál elv. Ostrowski tétele (4.1.11. Tétel) arra mutat rá, hogy miért analóg ez a két, látszólag különböző feltétel (mármint az $\mathbb{R}$ feletti, illetve a modulo p^r megoldások létezése). Természetesen az túl optimista gondolat, hogy ez *minden* egész együtthatós egyenletre teljesülne, ez sajnos nem igaz. Viszont a Hasse–Minkowski-tétel szerint ez teljesül abban az esetben, amikor az egyenletek legfeljebb másodfokúak.

1.1.3. A Weil-sejtések

A véges testek feletti egyenletek elméletében központi szerepet játszottak (és, bár ezek már tételek, játszanak mind a mai napig) a Weil-sejtések, melyeket röviden vázolunk. Legyen X egy n-dimenziós sima projektív varietás a p elemű $\mathbb{F}_p$ test fölött, azaz homogén polinomegyenletek közös nullhelyeinek a halmaza a valahánydimenziós projektív térben. Az alapkérdés, hogy X-nek hány pontja van $\mathbb{F}_p$ felett, illetve általában az m-edfokú $\mathbb{F}_{p^m}$ bővítés felett, jelöljük tehát az utóbbit N_m-nel ($m \geq 1$). Gyártsuk le a

$$\zeta(X,T) := \exp\left(\sum_{m=1}^{\infty} \frac{N_m T^m}{m}\right)$$

generátorfüggvényt, melynek segítségével egyszerre kezelhetjük minden $m \geq 1$-re az N_m megoldásszámot – ezt nevezik X zeta-függvényének. (Hogy miért pont ezt, az a sejtések megfogalmazásából kiderül.) A priori a fenti formula egy racionális együtthatós formális hatványsort ad. *André Weil* 1949-ben megfogalmazott sejtései, melyek bizonyításáért *Pierre Deligne* 1978-ban Fields-érmet kapott a következők:

1. (Racionalitás) A $\zeta(X,T)$ egy racionális törtfüggvény T-ben. Pontosabban

$$\zeta(X,T) = \frac{P_1(T)P_3(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)}$$

   alkalmas $P_0, \ldots, T_{2n} \in \mathbb{Z}[T]$ polinomokra. Továbbá $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - p^n T$, és $1 \leq k \leq 2n-1$-re a $P_k(T)$ polinomok $P_k(T) = \prod_j (1 - \alpha_{kj} T)$ alakba írhatók valamely $\alpha_{kj} \in \mathbb{C}$ (algebrai egész) számokra.

2. (Függvényegyenlet) Alkalmas E egész számra (E az X *Euler-karakterisztikája*, aminek létezése a sejtés része) a zeta-függvény teljesíti a $\zeta(X, p^{-n}T^{-1}) = \pm p^{\frac{nE}{2}} \zeta(X,T)$ függvényegyenletet.

3. (Riemann-sejtés) A fenti számokra $|\alpha_{kj}| = p^{k/2}$ minden $1 \le k \le 2n-1$-re és j indexre. Speciálisan ha $T = p^{-s}$-t helyettesítünk, akkor a $P_k(p^{-s})$ függvény összes gyöke a kiritikus, $k/2$ valós részű egyenesre esik.

4. (Betti-számok) Amennyiben X egy 0-karakterisztikájú számtest feletti Y sima projektív varietás modulo p redukciójaként jön létre, akkor a P_k foka megegyezik az $Y(\mathbb{C})$ topologikus tér k-adik Betti-számával (azaz a k-adik $\mathbb{Q}$-együtthatós – szinguláris – kohomológiájának dimenziójával).

Weil észrevétele, amire a sejtését alapozta, az volt, hogy ha létezne p karakterisztikában egy kellően jól viselkedő – a topológiából ismert szinguláris kohomológiához hasonló – kohomológia-elmélet, akkor abból következnének a sejtései egy, a Lefschetz-féle fixponttételhez analóg állítás segítségével. Kicsit precízebben az $\mathbb{F}_p$-feletti megoldások nem mások, mint a $\mathrm{Frob}_p\colon x \mapsto x^p$ Frobenius leképezés fixpontjai. Másrészt a Lefschetz-féle fixpont-tétel topológiában a következő:

1.1.2. Tétel (Lefschetz–Hopf)**.** *Legyen M egy kompakt háromszögelhető tér és $f\colon M \to M$ egy folytonos függvény, melyről tegyük fel, hogy véges sok fixpontja van. Ekkor*

$$\sum_{x \in \mathrm{Fix}(f)} i(f,x) = \sum_{k \ge 0} (-1)^k \mathrm{Tr}(f^* \mid H^k(M,\mathbb{Q}))\ ,$$

ahol $i(f,x)$ az x fixpont indexét jelöli.

Tehát f fixpontjainak a számát (pontosabban az f leképezés adott pontbeli indexével megsúlyozott számát) le lehet olvasni az f által a kohomológiákon indukált lineáris leképezések nyomaiból. Egy ilyen, véges testek felett is értelmezhető algebrai kohomológia-elméletnek, az ún. étale kohomológiának a megkonstruálása Grothendieck úttörő munkája, melynek alaptulajdonságaiból következik a fenti 1. és 2. sejtés (az 1-est lásd lentebb, a 2-es pedig a Poincaré-dualitásból következik). A 3. és 4. sejtéshez viszont szükség volt az étale kohomológia további, közel sem triviális tulajdonságaira, melyeket Deligne-nek sikerült igazolnia. A történethez hozzátartozik, hogy az 1. sejtés (a racionalitás) első bizonyítása *Bernard Dwork* nevéhez fűződik 1960-ból, de ő más – p-adikus analitikus – módszereket használt.

Illusztráció céljából megmutatjuk, hogyan következik a racionalitási sejtés egy Lefschetz-féle fixponttételt teljesítő kohomológia-elmélet létezéséből. Továbbá azt is vázoljuk, mi következik a Weil sejtésekből N_m-re, és hogy hogyan lehet ennek alkalmazásaként karakterösszegeket becsülni. A jó hír a következő: a véges testek elméletében minden fixpont indexe 1 lesz, ezért ezzel nem kell törődnünk.

Először tegyük fel a Weil-sejtéseket. Mindkét oldal logaritmusát véve

$$\sum_{m=1}^{\infty} \frac{N_m T^m}{m} = \log \zeta(X,T) = \sum_{k=0}^{2n} (-1)^{k+1} \log P_k(T) = \sum_{k=0}^{2n} (-1)^{k+1} \sum_j \log(1-\alpha_{kj}T) =$$

$$= \sum_{k=0}^{2n} (-1)^k \sum_j \sum_{m=1}^{\infty} \frac{\alpha_{kj}^m T^m}{m} \quad (1.1)$$

adódik. A két oldalon T^m együtthatóját összehasonlítva és felhasználva, hogy $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - p^n T$ az

$$N_m = 1 + p^{nm} + \sum_{k=1}^{2n-1} (-1)^k \sum_j \alpha_{kj}^m = 1 + p^{nm} + O(p^{nm-\frac{m}{2}})$$

egyenletet kapjuk a 3. (Riemann) sejtés felhasználásával. Ez a becslés legjobban $n = 1$, azaz görbék esetén használható. Pl. ha E egy elliptikus görbe, akkor P_1 egy másodfokú polinom, ezért a pontok számára $m = 1$ esetén

$$1 + p - 2\sqrt{p} \leq |E(\mathbb{F}_p)| \leq 1 + p + 2\sqrt{p}$$

becslést kapunk. Ha pl. $f(x) \in \mathbb{Z}[x]$ egy olyan harmadfokú polinom normált, aminek nincs modulo $p > 2$ többszörös gyöke, akkor az $y^2 = f(x)$ elliptikus görbe sima lesz modulo p is. Tehát alkalmazhatjuk a fenti becslést: ennek az egyenletnek modulo p megoldásainak száma p-től maximum $2\sqrt{p}$-ben tér el (hiszen egyetlen „végtelen távoli" pont van a görbén, ha kiterjesztük a projektív síkra). Viszont ennek az egyenletnek a megoldásszámát másképp is megszámolhatjuk: fusson végig x egy teljes maradékrendszeren modulo p, és vizsgáljuk meg, hogy mely x-ekre lesz $f(x)$ kvadratikus maradék, azaz négyzetszám modulo p. Ha $p \mid f(x)$, akkor y modulo p csak 0 lehet, ha $f(x)$ nemnulla kvadratikus maradék, akkor y kétféle lehet, ha pedig $f(x)$ kvadratikus nemmaradék, akkor nincs megfelelő y. Összesítve a megfelelő y-ok száma $1 + \left(\frac{f(x)}{p}\right)$. Mivel az 1-esek pont p-t adnak összegül, a

$$|\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)| \leq 2\sqrt{p}$$

becslést kapjuk, aminél jobb nem ismert.

A racionalitási sejtés bizonyításához tegyük fel, hogy létezik egy, a fenti Lefschetz-féle fixponttételt teljesítő H^* kohomológia-elmélet valamilyen 0-karakterisztikájú K együtthatótesttel. Ekkor az $\mathbb{F}_{p^m}$ testben levő megoldások pontosan a Frob_p^m leképezés fixpontjai, tehát a fixponttétel szerint

$$N_m = \sum_{k \geq 0} (-1)^k \mathrm{Tr}((\mathrm{Frob}_p^m)^* \mid H^k(X, K)) \ .$$

Jelölje α_{kj} a Frob_p^*: $H^k(X, K) \to H^k(X, K)$ lineáris leképezés j-edik sajátértékét. Ekkor $\mathrm{Tr}((\mathrm{Frob}_p^m)^* \mid H^k(X, K)) = \sum_j \alpha_{kj}^m$, hiszen egy leképezés nyoma nem más, mint a sajátértékek összege. A (1.1) egyenlet azt is mutatja, hogy ha a $P_k(T)$ polinomokat a p-Frobenius által indukált leképezés

$$P_k(T) := \det(1 - T\mathrm{Frob}_p^* \mid H^k(X, K))$$

módosított karakterisztikus polinomjának választjuk, akkor $\zeta(X, T)$ valóban a kívánt racionális törtfüggvény alakba írható.

1.1.4. A Birch–Swinnerton-Dyer sejtés

Mint fentebb láttuk, a többváltozós legfeljebb másodfokú polinomok egész megoldásainak kérdését lényegében rendezi a Hasse–Minkowski tétel.

1.1.5. Faltings tétele

1.1.6. Langlands program

2. fejezet

Galois-elméleti bevezető

Az alábbi fejezetben bizonyítás nélkül felhasználjuk, hogy minden K testnek létezik $\overline{K}$ algebrai lezártja. Valójában annyi is elég, hogy minden test beágyazható algebrailag zárt testbe. Ennek bizonyítása a függelékben található.

2.1. K-homomorfizmusok, szeparábilis bővítések

2.1.1. Definíció. Legyen K egy test, és $K \leq L$, illetve $K \leq M$ két bővítése K-nak. Ekkor K-feletti relatív homomorfizmusnak (röviden K-homomorfizmusnak) nevezünk egy $\tau\colon L \to M$ testhomomorfizmust, melyre $\tau_{|K} = \mathrm{id}_K$. Egy ilyen K-homomorfizmust testbővítések izomorfizmusának nevezünk, ha bijektív.

Megjegyzés: a testhomomorfizmus megtartja a testnek a 0-változós műveleteit (konstansok kijelölése) is, azaz $\tau(1) = 1$ mindig. Speciálisan minden τ testhomomorfizmus *injektív*, hiszen $1 \notin \mathrm{Ker}(\tau) \lhd L$ egy ideál, és L-nek csak két ideálja van: $\{0\}$ és L.

2.1.2. Példa. 1. $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) = \{\mathrm{id}, \bar{\cdot}\}$.

2. $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}))| = 2$.

3. $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}))| = 1$, de $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})| = 3$.

Megjegyzés: $\mathrm{Hom}_K(L_1, L_2)$ csak egy halmaz, mindenféle extra struktúra nélkül.

2.1.3. Lemma. *Legyen $\tau \in \mathrm{Hom}_K(L_1, L_2)$ egy K-homomorfizmus, $\alpha \in L_1$, $f(x) \in K[x]$. Ekkor $\tau(f(\alpha)) = f(\tau(\alpha))$.*

Bizonyítás. Legyen $f(x) = a_0 + a_1 x + \ldots a_n x^n$, ekkor $\tau(f(\alpha)) = \tau(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = = \tau(a_0) + \tau(a_1)\tau(\alpha) + \cdots + \tau(a_n)\tau(\alpha)^n = a_0 + a_1\tau(\alpha) + \cdots + a_n\tau(\alpha)^n = f(\tau(\alpha))$, hiszen τ egy testhomomorfizmus és a K elemein identikus. □

A következő állítás, és annak egy későbbi általánosítása kulcsfontosságú a felépítésünkben. Ez lényegében a 6.4.7-es állítás [7]-ben.

2.1.4. Állítás. *Legyen $K \leq K(\alpha)$ és $K \leq L$ két bővítés, α algebrai K felett, $m_\alpha(x) \in K[x]$ a minimálpolinomja. Ekkor a*

$$\begin{array}{rcl} \mathrm{Hom}_K(K(\alpha), L) & \to & \{\beta \in L \colon m_\alpha(\beta) = 0\} \\ \tau & \mapsto & \tau(\alpha) \end{array}$$

leképezés egy bijekció. Speciálisan $|\mathrm{Hom}_K(K(\alpha), L)| \leq \deg(m_\alpha) = |K(\alpha) : K|$.

Bizonyítás. A fenti Lemma miatt minden $\tau \in \mathrm{Hom}_K(K(\alpha), L)$-re $\tau(\alpha)$ gyöke $m_\alpha(x)$-nek, tehát tényleg értelmes a leképezés. Azt kell belátnunk, hogy injektív és szürjektív:

Injektivitás: $K(\alpha)$ minden eleme előáll $g(\alpha)$ alakban, ahol $g(x) \in K[x]$ polinom. Ha $\tau_1(\alpha) = \tau_2(\alpha)$, akkor a fenti Lemma miatt $\tau_1(g(\alpha)) = g(\tau_1(\alpha)) = g(\tau_2(\alpha)) = \tau_2(g(\alpha))$, tehát $\tau_1 = \tau_2$.

Szürjektivitás: Legyen $\beta \in L$ olyan, amire $m_\alpha(\beta) = 0$. Vegyük észre, hogy $K(\alpha) \cong K[x]/(m_\alpha(x))$. A β behelyettesítése egy $\varphi_\beta \colon K[x] \to L$ $(f(x) \mapsto f(\beta))$ homomorfizmust ad. Mivel $m_\alpha(\beta) = 0$, ezért $m_\alpha(x) \in \mathrm{Ker}(\varphi_\beta)$. Továbbá $(m_\alpha(x))$ egy maximális ideál $K[x]$-ben (és $1 \notin \mathrm{Ker}(\varphi_\beta)$), tehát $(m_\alpha(x)) = \mathrm{Ker}(\varphi_\beta)$. A homomorfizmustétel szerint $\mathrm{Im}(\varphi_\beta) \cong K[x]/(m_\alpha(x)) \cong K(\alpha)$, és ennél az izomorfizmusnál $\beta \in \mathrm{Im}(\varphi_\beta)$ éppen $x + (m_\alpha(x)) \in \in K[x]/(m_\alpha(x))$-nek, és így $\alpha \in K(\alpha)$-nak felel meg, tehát kapunk egy olyan K-homomorfizmust $K(\alpha)$-ból $\mathrm{Im}(\varphi_\beta) \leq L$-be, aminél α képe éppen β. □

2.1.5. Definíció. K egy tetszőleges M bővítésében levő α algebrai elem egy (esetleg másik) $K \leq L$ bővítésbeli K-feletti konjugáltjainak azokat a $\beta \in L$ elemeket nevezzük, melyek gyökei α minimálpolinomjának. Ezek a fenti tétel szerint nem mások, mint α lehetséges képei a $\tau \in \mathrm{Hom}_K(K(\alpha), L)$ homomorfizmusoknál.

2.1.6. Definíció. Legyen K egy test, $K \leq L$ egy bővebb test. Egy $\alpha \in L$ algebrai elemet szeparábilisnak nevezünk (K felett), ha K feletti (m_α-val jelölt) minimálpolinomjának nincs többszörös gyöke.

2.1.7. Állítás. *Egy $\alpha \in \overline{K}$ elem pontosan akkor szeparábilis K felett, ha* $|\mathrm{Hom}_K(K(\alpha), \overline{K})| = |K(\alpha) : K|$.

Bizonyítás. Triviális az 2.1.4-es Állításból: m_α-nak pontosan akkor van $\deg(m_\alpha)$ darab különböző gyöke $\overline{K}$-ban, ha nincs többszörös gyöke. □

Megjegyzés: α szeparábilitásához elég, ha van olyan $0 \neq f(x) \in K[x]$ polinom, aminek nincs többszörös gyöke és $f(\alpha) = 0$. Valóban, ekkor $m_\alpha \mid f$-nek sincs többszörös gyöke.

2.1.8. Következmény. *$K \leq L \leq M$ testek, $\alpha \in M$ szeparábilis K felett $\Rightarrow$ L felett is.*

Bizonyítás. A fenti megjegyzést alkalmazzuk. A K feletti minimálpolinomnak nincs többszörös gyöke, és α gyöke. □

A következő állítás az 2.1.4-es Állításnak az általánosítása. Most egy $\tau \colon L \to M$ K-homomorfizmust akarunk kiterjeszteni egyetlen α további elemre. Ez lényegében a 6.4.8-as tétel [7]-ben.

2.1.9. Állítás. *Legyenek $K \leq L \leq L(\alpha)$ és $K \leq M$ testbővítések, ahol α algebrai L fölött. Legyen $m_\alpha(x) \in L[x]$ az α minimálpolinomja L felett. Ekkor minden $\tau \in \mathrm{Hom}_K(L, M)$-re a*

$$\begin{array}{rcl} \{\rho \in \mathrm{Hom}_K(L(\alpha), M) \mid \rho_{|L} = \tau\} & \to & \{\beta \in M \colon \tau(m_\alpha)(\beta) = 0\} \\ \rho & \mapsto & \rho(\alpha) \end{array}$$

leképezés egy bijekció. Itt $\tau(m_\alpha)(x) \in \tau(L)[x] \leq M[x]$ az a polinom, amelyet úgy kapunk, hogy m_α együtthatóira ráalkalmazzuk τ-t.

Megjegyzés: vegyük észre, hogy itt m_α együtthatói nem K-ból, hanem L-ből valók, hiszen ez α-nak az L feletti minimálpolinomja. Ezért kell a 2.1.4-es Állítással ellentétben m_α-nak az együtthatóira is ráalkalmazni τ-t.

Bizonyítás. A bizonyítás teljesen analóg az 2.1.4-es Állítás bizonyításához. Először azt látjuk be, hogy ha ρ egy kiterjesztése τ-nak $L(\alpha)$-ra, akkor $\rho(\alpha)$ valóban gyöke $\tau(m_\alpha)$-nak. Ehhez legyen $m_\alpha(x) = a_0 + a_1 x + \cdots + x^n$ és alkalmazzuk ρ-t az $m_\alpha(\alpha) = 0$ azonosságra: $0 = \rho(a_0 + + \cdots + \alpha^n) = \rho(a_0) + \cdots + \rho(\alpha)^n = \tau(a_0) + \cdots + \rho(\alpha)^n = \tau(m_\alpha)(\rho(\alpha))$, hiszen $\rho(a_i) = \tau(a_i)$ mivel $a_i \in L$ és $\rho_{|L} = \tau$.

Injektivitás: ha $\rho_{1|L} = \tau = \rho_{2|L}$ és $\rho_1(\alpha) = \rho_2(\alpha)$, akkor ρ_1 és ρ_2 megegyeznek $L(\alpha)$-n is.

Szürjektivitás: vegyük észre, hogy $\tau(m_\alpha) \in \tau(L)[x]$ is irreducibilis polinom, hiszen a $\tau \colon L[x] \to \tau(L)[x]$ egy izomorfizmus. Tehát ha β gyöke $\tau(m_\alpha)$-nak, akkor ez is a minimálpolinomja. Így a kívánt ρ leképezés nem más, mint $\rho := \varphi_\beta \circ \tau \circ \varphi_\alpha^{-1}$, ahol $\varphi_\beta \colon \tau(L)[x]/(\tau(m_\alpha)(x)) \to \tau(L)(\beta) \leq M$ homomorfizmus, amit a β behelyettesítése indukál, $\varphi_\alpha \colon L[x]/(m_\alpha(x)) \to L(\alpha)$ izomorfizmus, amit az α behelyettesítése indukál, τ pedig a

$$\tau \colon L[x]/(m_\alpha(x)) \to \tau(L)[x]/(\tau(m_\alpha)(x))$$

izomorfizmus. □

2.1.10. Következmény. *Legyenek $K \leq L$ és $K \leq M$ bővítések. Ekkor $|\mathrm{Hom}_K(L, M)| \leq$ $\leq |L : K|$.*

Bizonyítás. Ha $|L : K| = \infty$, akkor az állítás üres. Egyébként legyen $d = |L : K|$ és $L = K(\alpha_1, \ldots, \alpha_n)$. Indukcióval bizonyítunk n-szerint. $n = 1$-re az állítás az 2.1.4-es Állítás speciális esete. Legyen $n > 1$ és $L_0 = K(\alpha_1, \ldots, \alpha_{n-1})$. Ekkor az indukciós feltevés miatt tetszőleges $\rho \in \mathrm{Hom}_K(L, M)$-re ρ megszorítása L_0-ra legfeljebb $|L_0 : K|$-féle lehet. Továbbá adott $\tau = \rho_{|L_0}$-ra a 2.1.9-as Állítás miatt ρ csak $|L_0(\alpha_n) : L_0| = |L : L_0|$-féle lehet. Az állítás a fokszámtételből következik. □

2.1.11. Következmény. *Legyen $K \leq L$, és $\alpha \in L$ szeparábilis. Ekkor $K(\alpha)$ minden eleme szeparábilis.*

Bizonyítás. Legyen $\beta \in K(\alpha)$. Ekkor α szeparábilis $K(\beta)$ fölött is az 2.1.8-as Következmény miatt. Tehát adott $\tau \in \mathrm{Hom}_K(K(\beta), \overline{K})$-ra τ éppen $|K(\alpha) : K(\beta)|$-féleképpen terjed ki $\rho \colon K(\alpha) \to \overline{K}$ K-homomorfizmussá. Ezért

$$|K(\alpha) : K| = |\mathrm{Hom}_K(K(\alpha), \overline{K})| = |\mathrm{Hom}_K(K(\beta), \overline{K})| \cdot |K(\alpha) : K(\beta)| \ .$$

Az állítás egyszerű osztással következik a fokszámtételből és az 2.1.7-es Állításból . □

2.1.12. Definíció. Egy (véges) L/K bővítés szeparábilis, ha L minden eleme szeparábilis K felett.

Tehát a fenti következmény szerint α pontosan akkor szeparábilis K felett, ha a $K(\alpha)/K$ bővítés szeparábilis.

2.1.13. Állítás. *Az L/K véges bővítés pontosan akkor szeparábilis, ha $|\mathrm{Hom}_K(L,\overline{K})| = |L : K|$.*

Bizonyítás. Ha $|\mathrm{Hom}_K(L,\overline{K})| = |L : K|$ és $\alpha \in L$, akkor adott $\tau \in \mathrm{Hom}_K(K(\alpha),\overline{K})$-ra τ a 2.1.10-es Következmény miatt legfeljebb $|L : K(\alpha)|$-féleképpen terjed ki $L \to \overline{K}$ K-homomorfizmussá. Mivel $|\mathrm{Hom}_K(L,\overline{K})| = |L : K|$, ezért legalább $|L : K|/|L : K(\alpha)| = |K(\alpha) : K|$ darab ilyen τ-nak kell lennie, tehát az állítás következik az 2.1.4-es Állításból.

Visszafelé, ha L/K szeparábilis, akkor $L = K(\alpha_1, \ldots, \alpha_n)$, ahol az α_i-k szeparábilisek K felett. Ha $n = 1$, akkor az állítás következik az 2.1.4-es Állításból. Legyen $L_0 = K(\alpha_1, \ldots, \alpha_{n-1})$. Indukcióval ($n$ szerint) feltehetjük, hogy $|\mathrm{Hom}_K(L_0,\overline{K})| = |L_0 : K|$. Jelöljük $m_{\alpha_n}(x)$-szel α_n L_0 feletti minimálpolinomját, és legyen $\tau \in \mathrm{Hom}_K(L_0,\overline{K})$ tetszőleges. Mivel α_n szeparábilis (K fölött a feltevés szerint, így L_0 fölött is az 2.1.8-as Következmény miatt), és $\overline{K}$ algebrailag zárt, ezért $\tau(m_{\alpha_n})(x)$-nek pontosan $\deg(\tau(m_{\alpha_n})) = \deg(m_{\alpha_n}) = |L : L_0|$ darab gyöke van $\overline{K}$-ban. Tehát az 2.1.9-es Állítás szerint τ pontosan $|L : L_0|$-féleképpen terjed ki $\rho\colon L \to \overline{K}$ K-homomorfizmussá. Így $|\mathrm{Hom}_K(L,\overline{K})| = |L : L_0||\mathrm{Hom}_K(L_0,\overline{K})| = |L : L_0| \cdot |L_0 : K| = |L : K|$. □

2.1.14. Állítás. *Legyen $K \le L \le M$ véges bővítések egy lánca. M/K akkor és csak akkor szeparábilis, ha L/K és M/L szeparábilis. Speciálisan ha $K \le M$ tetszőleges bővítés, akkor M azon elemei, melyek szeparábilisek K felett, résztestet alkotnak.*

Bizonyítás. Először belátjuk, hogy ha M/L és L/K szeparábilis, akkor M/K is az. Ehhez legyen $\beta \in M$ tetszőleges, és $m_\beta(x) \in L[x]$ a minimálpolinomja. Ekkor az 2.1.9-es Állítás miatt minden $\tau \in \mathrm{Hom}_K(L,\overline{K})$ pontosan annyiféleképpen terjed ki $L(\beta)$-ra, ahány gyöke van $\tau(m_\beta)$-nak $\overline{K}$-ban. Mivel M/L szeparábilis, ezért m_β-nak nincsenek többszörös gyökei, így $\tau(m_\beta)$-nak sincsenek. Tehát $\tau(m_\beta)$-nak pontosan $\deg(\tau(m_\beta)) = \deg(m_\beta) = |L(\beta) : L|$ darab gyöke van $\overline{K}$-ban. Így $|\mathrm{Hom}_K(L(\beta),\overline{K})| = |L(\beta) : L| \cdot |\mathrm{Hom}_K(L,\overline{K})| = |L(\beta) : L| \cdot |L : K| = |L(\beta) : K|$, hiszen L/K szeparábilis.

Visszafelé ha M/K szeparábilis, akkor az 2.1.10-es Következmény szerint $|\mathrm{Hom}_K(L,\overline{K})| \le |L : K|$, és $|\mathrm{Hom}_L(M,\overline{L})| \le |M : L|$. Feltehetjük, hogy $L \le \overline{K}$, és azt is, hogy $\overline{L} = \overline{K}$. Viszont adott (fix) $\tau \in \mathrm{Hom}_K(L,\overline{K})$-ra L-et azonosíthatjuk $\tau(L)$-lel, tehát τ pontosan annyiféleképpen terjed ki egy $\rho\colon M \to \overline{K}$ K-homomorfizmussá, amennyi eleme van $\mathrm{Hom}_L(M,\overline{L})$-nak. Azt kaptuk, hogy $|M : K| = |\mathrm{Hom}_K(M,\overline{K})| = |\mathrm{Hom}_K(L,\overline{K})| \cdot |\mathrm{Hom}_L(M,\overline{L})| \le |L : K| \cdot |M : L| = |M : K|$, azaz végig egyenlőség van. Speciálisan $|\mathrm{Hom}_K(L,\overline{K})| = |L : K|$ és $|\mathrm{Hom}_L(M,\overline{L})| = |M : L|$, másszóval mindkettő szeparábilis.

A másik állításhoz legyen $\alpha, \beta \in M$ szeparábilis K fölött. Ekkor $K(\alpha)(\beta)$ is szeparábilis az első állítás szerint K fölött. Tehát minden eleme szeparábilis, speciálisan $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is. □

A következő tétel a [7] 6.3.8-as (és a 6.3.11-es) tétel általánosítása.

2.1.15. Tétel. *Minden véges szeparábilis bővítés egyszerű, azaz minden L/K véges szeparábilis bővítésre van olyan $\alpha \in L$, melyre $L = K(\alpha)$.*

Bizonyítás. Az állítást csak akkor bizonyítjuk, ha K végtelen. Ha K véges és $\alpha \in L^\times$ a multiplikatív csoportnak egy generátoreleme, akkor $L = K(\alpha)$.

Legyen $L = K(\alpha_1, \ldots, \alpha_n)$, $|L : K| = d$ és $\mathrm{Hom}_K(L, \overline{K}) = \{\tau_1, \ldots, \tau_d\}$ (lsd. 2.1.13-as Állítás). Ha találunk olyan $\alpha \in L$-et, melyre a $\tau_1(\alpha), \ldots, \tau_d(\alpha) \in \overline{K}$ elemek mind különbözők, akkor készen vagyunk: Valóban, ha $m_\alpha(x) \in K[x]$-szel jelöljük α minimálpolinomját, akkor $\tau_1(\alpha), \ldots, \tau_d(\alpha)$ mind gyöke m_α-nak, speciálisan $|K(\alpha) : K| = \deg(m_\alpha) \geq d = |L : K|$, így $L = K(\alpha)$, hiszen $K(\alpha) \leq L$.

Az α-t $\alpha = \sum_{i=1}^n \alpha_i \beta^i$ alakban keressük, ahol $\beta \in K$. Legyen $f(x) = \sum_{i=1}^n \alpha_i x^i \in L[x]$ polinom. Ha $1 \leq j \neq k \leq d$, akkor nem lehet, hogy minden $i = 1, \ldots, n$-re $\tau_j(\alpha_i) = \tau_k(\alpha_i)$, hiszen akkor τ_j és τ_k az α_i-k által generált testen, azaz L-en is megegyezne, holott különbözők. Tehát a $\tau_j(f)(x) = \sum_{i=1}^n \tau_j(\alpha_i) x^i \in \overline{K}[x]$ polinomok ($j = 1, \ldots, d$) páronként különbözők. Ez azt jelenti, hogy a $P(x) := \prod_{1 \leq j < k \leq d} (\tau_j(f)(x) - \tau_k(f)(x)) \in \overline{K}[x]$ polinom nem a 0 polinom. Mivel K végtelen, ezért van olyan $\beta \in K$, ami nem gyöke $P(x)$-nek. Tehát

$$\tau_j(f(\beta)) = \tau_j\left(\sum_{i=1}^n a_i \beta^i\right) = \sum_{i=1}^n \tau_j(a_i)\beta^i = \tau_j(f)(\beta) \neq \tau_k(f)(\beta) = \tau_k(f(\beta)) \quad (j \neq k)$$

(hiszen $\beta \in K$ miatt $\tau_j(\beta) = \beta = \tau_k(\beta)$), így az $\alpha := f(\beta)$ választás megfelel. □

2.1.1. Tökéletes testek és a Frobenius

2.1.16. Definíció. Egy K testet *tökéletes*nek (vagy idegen szóval *perfekt*nek) nevezünk, ha minden véges bővítése szeparábilis.

Vegyük észre, hogy minden 0-karakterisztikájú test tökéletes, hiszen 0-karakterisztikában egy irreducibilis polinomnak nem lehet többszörös gyöke. Valóban, ha $f(x) \in K[x]$ irreducibilis, és $\beta \in \overline{K}$ egy többszörös gyöke f-nek, akkor $f(\beta) = f'(\beta) = 0$. Speciálisan f és f' nem relatív prímek, de mivel f irreducibilis, ezért $f \mid f'$. Node $\deg(f') \leq \deg(f) - 1$, tehát $f'(x) = 0$. Ez utóbbi 0-karakterisztikában nem történhet meg. Sőt, $p > 0$ karakterisztikában is csak akkor, ha van olyan $g(x)$ polinom, melyre $f(x) = g(x^p)$. Valóban, ahhoz, hogy minden egy monom deriváltja 0 legyen, az kell, hogy a kitevő p többszöröse legyen.

A továbbiakban karakterizáljuk a tökéletes testeket. Speciálisan látni fogjuk, hogy a 0-karakterisztikájú testek mellett minden véges test is tökéletes.

Legyen k egy $p > 0$ karakterisztikájú test. Ekkor a p-edik hatványra való emelés nemcsak multiplikatív, hanem additív is, azaz a

$$\begin{aligned} \mathrm{Frob}_p \colon k &\to k \\ x &\mapsto x^p \end{aligned}$$

leképezés egy testendomorfizmus. Ezt a leképezést nevezzük a (p-)Frobeniusnak. A Frobenius endomorfizmus (testek esetében) mindig injektív, hiszen minden test nullosztómentes. Viszont nem minden p-karakterisztikájú k testre szürjektív: például a racionális törtfüggvények $\mathbb{F}_p(x)$ testére nem az: az x változó nincs benne a képében.

2.1.17. Állítás. *Egy p-karakterisztikájú k test pontosan akkor tökéletes, ha a p-Frobenius $\mathrm{Frob}_p \colon k \to k$ szürjektív.*

Bizonyítás. Tegyük fel először, hogy a Frobenius nem szürjektív, azaz van olyan $\alpha \in k$, mely nincs benne a képében. Ekkor az $f(x) = x^p - \alpha$ polinomnak nincs gyöke k-ban. Továbbá ha $\beta \in \overline{k}$ egy gyöke f-nek, akkor $\beta^p = \alpha$, azaz $f(x) = x^p - \alpha = (x - \beta)^p$. Tehát f-nek egyetlen p-szeres gyöke van. Másrészt f-nek lineáris faktora nem lehet, hiszen nincs gyöke; ugyanakkor minden irreducibilis tényezőjének csak β lehet gyöke, speciálisan van többszörös gyöke. Viszont egy irreducibilis polinom, melynek van többszörös gyöke, szükségképpen legalább p-fokú, hiszen x^p polinomja. Tehát azt kaptuk, hogy f irreducibilis, így mivel van többszörös gyöke, ezért $k[x]/(f(x))$ egy inszeparábilis bővítése k-nak.

Megfordítva tegyük fel, hogy $f(x) \in k[x]$ egy irreducibilis polinom, melynek van többszörös gyöke. Ekkor van olyan $g(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$, melyre $f(x) = g(x^p)$. Tegyük fel, hogy $\mathrm{Frob}_p \colon k \to k$ szürjektív. Ekkor minden $i = 0,1,\ldots,n$-re van olyan $b_i \in k$, melyre $b_i^p = \mathrm{Frob}_p(b_i) = a_i$, azaz $f(x) = (b_0 + b_1 x + \cdots + b_n x^n)^p$ nem irreducibilis, ami ellentmondás. □

2.1.18. Következmény. *Minden véges test tökéletes.*

Bizonyítás. Egy véges halmazon minden injektív függvény egyben szürjektív is. □

Ahogy fentebb láttuk, a Frobenius *nem* szürjektív a racionális törtfüggvények $\mathbb{F}_p(x)$ testén, azaz ez a test nem tökéletes.

2.2. Galois-bővítések

2.2.1. Definíció. Legyen L/K véges bővítés. $\mathrm{Gal}(L/K) := \mathrm{Hom}_K(L, L)$ a bővítés *Galois-csoportja*, azaz a relatív automorfizmusok csoportja.

Vegyük észre, hogy $\mathrm{Gal}(L/K)$ valóban csoport a kompozícióra nézve. A kompozícióra való zártság és az asszociativitás nyilvánvaló, az identitás az egységelem. Inverz azért létezik, mert minden $\tau \in \mathrm{Hom}_K(L, L)$ szürjektív is (nemcsak injektív), hiszen L végesdimenziós vektortér K felett. Könnyű számolás mutatja, hogy τ^{-1} is művelettartó, tehát eleme $\mathrm{Hom}_K(L, L)$-nek.

2.2.2. Állítás. *A fenti definíció akkor is értelmes, ha L/K nem feltétlenül véges, de algebrai bővítés.*

Bizonyítás. Azt kell belátnunk, hogy minden $\tau \colon L \to L$ K-homomorfizmus szürjektív (a fenti érvelésben csak itt használtuk L/K végességét). Vegyünk egy $\alpha \in L$-et és legyen $m_\alpha(x) \in K[x]$ a minimálpolinomja. Ennek véges sok gyöke lehet csak L-ben: $\{\alpha = \alpha_1, \ldots, \alpha_n\}$. Ekkor minden $i \in \{1, \ldots, n\}$-re $\tau(\alpha_i)$ is gyöke m_α-nak az 2.1.3-as Lemma miatt. Tehát τ permutálja az $\{\alpha = \alpha_1, \ldots, \alpha_n\}$ véges halmazt (hiszen injektív), így α is benne van a képében. □

Megjegyzés: Ha $K \leq L \leq \overline{K}$ (mivel L-nek is van algebrai lezártja, ezt minden további nélkül feltehetjük), akkor minden $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, L)$-beli elemet tekinthetünk $\overline{K}$-ba menő homomorfizmusnak is. Tehát $|\mathrm{Gal}(L/K)| \leq |\mathrm{Hom}_K(L, \overline{K})| \leq |L : K|$ mindig teljesül.

2.2.3. Definíció. Az L/K véges bővítésről azt mondjuk, hogy Galois-bővítés, ha $|\mathrm{Gal}(L/K)| = |L : K|$. (Bizonyos forrásokban a $\mathrm{Gal}(L/K)$ csoportot csak akkor hívják Galois-csoportnak, ha az L/K bővítés Galois.)

2.2.4. Állítás. *Minden Galois-bővítés szeparábilis, speciálisan egyszerű.*

Bizonyítás. Valóban, a fenti megjegyzés miatt ha L/K Galois, akkor $|\mathrm{Hom}_K(L, \overline{K})|$ is egyenlő $|L : K|$-val. □

2.2.5. Állítás. *Legyen $K \leq L (\leq \overline{K})$ egy véges szeparábilis bővítés. A következők ekvivalensek:*

(*i*) *L/K Galois.*

(*ii*) *Minden $\tau\colon L \to \overline{K}$ K-homomorfizmusra $\tau(L) = L$. (Ha nem tesszük fel, hogy L eleve részteste $\overline{K}$-nak, akkor azt kell mondani, hogy minden τ-nak ugyanaz a képtere.)*

(*iii*) *Minden $\alpha \in L$-re α összes $\overline{K}$-beli K fölötti konjugáltja L-ben van. (Azaz az $m_\alpha(x) \in K[x]$ minimálpolinom L felett gyöktényezők szorzatára bomlik.)*

(*iv*) *$L = K(\alpha_1, \ldots, \alpha_n)$ és minden α_i minden $\overline{K}$-beli K-feletti konjugátlja L-ben van.*

Bizonyítás. (*i*) $\iff$ (*ii*), hiszen $L \leq \overline{K}$ miatt minden $\tau \in \mathrm{Hom}_K(L, L)$ tekinthető $L \to \overline{K}$ K-homomorfizmusnak is.

(*ii*) $\Rightarrow$ (*iii*): Legyen $\beta \in \overline{K}$ az α egyik konjugáltja. Ekkor az 2.1.4-es Állítás miatt van olyan $\tau \in \mathrm{Hom}_K(K(\alpha), \overline{K})$, melyre $\tau(\alpha) = \beta$. Továbbá (mivel $L/K(\alpha)$ is szeparábilis) van olyan $\alpha' \in L$, melyre $L = K(\alpha)(\alpha')$. Az 2.1.9-es Állítás szerint így τ kiterjed egy $\rho\colon L \to \overline{K}$ K-homomorfizmussá, melyre $\rho(\alpha) = \tau(\alpha) = \beta$. (*ii*) szerint viszont $\rho(L) = L$, azaz $\beta \in L$.

(*iii*) $\Rightarrow$ (*iv*) triviális. (*iv*) $\Rightarrow$ (*ii*): Minden $\alpha \in L$-re van olyan $f \in K[x_1, \ldots, x_n]$ polinom, melyre $\alpha = f(\alpha_1, \ldots, \alpha_n)$, tehát $\tau(\alpha) = \tau(f(\alpha_1, \ldots, \alpha_n)) = f(\tau(\alpha_1), \ldots, \tau(\alpha_n)) \in L$. Tehát $\tau(L) \leq L$, és mivel $\dim_K \tau(L) = \dim_K L$, ezért $\tau(L) = L$.

□

2.2.6. Példa. (*a*) $\mathbb{C}/\mathbb{R}$ Galois.

(*b*) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ Galois.

(*c*) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ nem Galois.

(*d*) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ és $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ Galois, de $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ mégsem Galois.

2.2.7. Definíció. Legyen $f(x) \in K[x]$ polinom, legyenek f gyökei $\overline{K}$-ban $\{\alpha_1, \ldots, \alpha_n\}$. Ekkor a $K_f := K(\alpha_1, \ldots, \alpha_n) (\leq \overline{K})$ testet f K feletti *felbontási testének* nevezzük.

2.2.8. Megjegyzés. Azokat a véges bővítéseket, melyek valamely polinom felbontási testeként állnak elő, *normális* bővítéseknek nevezzük. Ez azzal ekvivalens, hogy minden irreducibilis polinomnak, melynek van gyöke a bővítésben, gyöktényezők szorzatára bomlik. Abban az esetben, ha a bővítés szeparábilis, ez könnyen következik a 2.2.5. Állításból. Az inszeparábilis eset végiggondolását az olvasóra bízzuk, mivel a továbbiakban erre nem lesz szükségünk.

2.2.9. Példa.

1. $x^2 - 2$ felbontási teste $\mathbb{Q}$ fölött $\mathbb{Q}(\sqrt{2})$.
2. $x^3 - 2$ felbontási teste $\mathbb{Q}$ fölött $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, ahol ε primitív harmadik egységgyök.
3. Ha $K(\alpha)/K$ Galois, akkor $K(\alpha)$ az α minimálpolinomjának felbontási teste.

2.2.10. Következmény. *Ha f szeparábilis polinom (azaz nincs többszörös gyöke), akkor K_f/K Galois. Speciálisan minden véges szeparábilis bővítés beágyazható egy véges Galois-bővítésbe.*

Bizonyítás. Mivel f szeparábilis, ezért $K_f = K(\alpha_1, \ldots, \alpha_n)$ szeparábilis K felett, tehát alkalmazhatjuk a 2.2.5-ös Állítást, melynek (iv)-es feltétele triviálisan teljesül. Továbbá ha L/K véges szeparábilis, akkor az 2.1.15-ös Tétel szerint $L = K(\alpha)$ valamilyen $\alpha \in L$-re, és α minimálpolinomjának felbontási teste tartalmazza L-et (vagy legalábbis egy L-lel izomorf résztestet, ha nem tettük fel, hogy $L \leq \overline{K}$). □

2.2.11. Lemma. *Legyen F/K tetszőleges szeparábilis bővítés és $G := \mathrm{Gal}(F/K)$.*

(i) *Ha $K \leq L \leq F$ közbülső test, akkor $\mathrm{Gal}(F/L) \leq G$.*

(ii) *Ha $H \leq G$, akkor $F^H := \{\alpha \in F \mid \tau(\alpha) = \alpha,\ \forall \tau \in H\}$ egy K-t tartalmazó résztest F-ben. (Definíció: a H* fixteste *F^H.) Továbbá $K \leq F^G \leq F^H \leq F$ és $H \leq \mathrm{Gal}(F/F^H)$.*

Bizonyítás. Mindkettő triviális: (i)-nél $\mathrm{Gal}(F/L)$ éppen azon $F \to F$ automorfizmusokból áll, amiknek L-re való megszorítása az identitás, speciálisan a K-ra való megszorítása is az. (ii)-nél pedig azt kell ellenőrizni, hogy ha $\alpha, \beta \in F^H$, akkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is benne van F^H-ban. Ez közvetlenül látszik a definícióból, hiszen H minden eleme testhomomorfizmus. A további két tartalmazás nyilvánvaló. □

2.2.12. Állítás. *Legyen $F = K(\alpha)$, ahol α algebrai K felett.*

(i) *Ha F/K Galois és $G = \mathrm{Gal}(F/K)$, akkor $F^G = K$.*

(ii) *Ha $F^G = K$ valamilyen $G \leq \mathrm{Gal}(F/K)$ részcsoportra, akkor F/K Galois és $G = \mathrm{Gal}(F/K)$.*

Bizonyítás. (i): Nyilván $K \leq F^G \leq F$, és $G \leq \mathrm{Gal}(F/F^G)$ miatt $|G| \leq |\mathrm{Gal}(F/F^G)| \leq |F : F^G| \leq |F : K| = |G|$, tehát mindenütt egyenlőség áll.

(ii): Legyen m_α az α minimálpolinomja és definiáljuk az $f_\alpha(x) := \prod_{\tau \in G}(x - \tau(\alpha)) \in F[x]$ polinomot. Ekkor ha $\sigma \in G$, akkor $\sigma(f_\alpha)(x) = \prod_{\tau \in G}(x - \sigma\tau(\alpha)) = \prod_{\tau \in G}(x - \tau(\alpha)) = f_\alpha(x)$, hiszen ha τ végigfut G összes elemén, akkor $\sigma\tau$ is végigfut ugyanezeken az elemeken. Tehát az $f_\alpha(x)$ polinom együtthatóit minden $\sigma \in G$ fixálja, azaz $f_\alpha(x) \in F^G[x] = K[x]$. Nyilván $f_\alpha(\alpha) = 0$, ezért $m_\alpha \mid f_\alpha$. Speciálisan $|F : K| = \deg(m_\alpha) \leq \deg(f_\alpha) = |G| \leq |\mathrm{Gal}(F/K)| \leq |F : K|$, ezért mindenhol egyenlőség van, azaz $G = \mathrm{Gal}(F/K)$ és $|\mathrm{Gal}(F/K)| = |F : K|$, másszóval F/K Galois. □

2.2.13. Tétel (Galois-elmélet főtétele)**.** *Legyen F/K egy véges Galois-bővítés $G = \mathrm{Gal}(F/K)$ Galois-csoporttal. Ekkor a*

$$\begin{array}{rcl} \{K \leq L \leq F \text{ közbülsőtestek}\} & \leftrightarrow & \{H \leq G \text{ részcsoportok}\} \\ \psi\colon L & \mapsto & \mathrm{Gal}(F/L) \\ F^H & \mapsfrom & H\colon \varphi \end{array}$$

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

Bizonyítás. Először belátjuk, hogy tetszőleges L közbülsőtestre F/L egy Galois-bővítés. Mivel F/K Galois, ezért szeparábilis is, így az 2.1.15-ös Tétel szerint $F = K(\alpha)$ valamilyen $\alpha \in F$-re. A 2.2.5-ös Állítás (iii) része szerint α K feletti $m_\alpha(x) \in K[x]$ minimálpolinomja gyöktényezők szorzatára bomlik F felett. Viszont α L fölötti f_α minimálpolinomja nyilván osztója m_α-nak, ezért az is gyöktényezők szorzatára bomlik L felett, tehát a 2.2.5 Állítás (iv) része miatt F/L is Galois-bővítés. (Vegyük észre, hogy F/L szeparábilis az 2.1.8-as Következmény szerint és ez kell ahhoz, hogy a 2.2.5-ös Állítást alkalmazhassuk.)

Ha már tudjuk, hogy F/L Galois, akkor legyen $H := \mathrm{Gal}(F/L)$. A 2.2.12(i) szerint $L = F^H$, tehát $\varphi \circ \psi = \mathrm{id}$.

Megfordítva legyen $H \leq G$ tetszőleges, és legyen $L = F^H$. Ekkor 2.2.12(ii) szerint F/L Galois-bővítés és $H = \mathrm{Gal}(F/L)$, azaz $\psi \circ \varphi = \mathrm{id}$. Tehát ψ és φ egymás kétoldali inverzei. Az $|L : K| = |G : H|$ állítás következik a fokszámtételből. □

2.3. Norma és nyom, a normál bázis tétel

Legyen L/K egy véges testbővítés, és $\alpha \in L$. Ekkor az

$$\begin{array}{rccc} s_\alpha \colon & L & \to & L \\ & \beta & \mapsto & \alpha\beta \end{array}$$

egy K-lineáris leképezés.

2.3.1. Definíció. Az α nyomát a $\mathrm{Tr}_{L/K}(\alpha) := \mathrm{Tr}(s_\alpha)$, az α normáját pedig a $N_{L/K}(\alpha) := \det(s_\alpha)$ képlettel definiáljuk.

Vegyük észre, hogy $N_{L/K} \colon L^\times \to K^\times$ egy csoporthomomorfizmus, $\mathrm{Tr}_{L/K} \colon L \to K$ pedig egy K-lineáris leképezés. Továbbá ha $\alpha \in K \subseteq L$, akkor $\mathrm{Tr}_{L/K}(\alpha) = n\alpha$ és $N_{L/K}(\alpha) = \alpha^n$, ahol $n = |L : K|$, hiszen ekkor s_α egy skalármátrix.

2.3.2. Lemma. (i) *Ha $L = K(\alpha)$ egyszerű bővítés, és $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, akkor $\mathrm{Tr}_{L/K}(\alpha) = -a_{n-1}$ és $N_{L/K}(\alpha) = (-1)^n a_0$.*

(ii) *Ha $K \leq L \leq M$ véges bővítések, akkor $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$.*

Bizonyítás. (i) Vegyük észre, hogy ebben az esetben $1, \alpha, \ldots, \alpha^{n-1}$ bázis, melyben s_α mátrixa $\begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$, melynek nyoma $-a_{n-1}$, determinánsa pedig $(-1)^n a_0$.

(ii) Legyen $\beta = (\beta_1, \ldots, \beta_n)$ az L/K bővítés, $\gamma = (\gamma_1, \ldots, \gamma_m)$ pedig az M/L bővítés bázisa és $\alpha \in M$. Speciálisan $\beta\gamma = (\beta_i\gamma_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ az M/K bővítés egy bázisa. Jelöljük a_{ij}-vel az α-val való szorzás mátrixában az i-edik sor j-edik elemét a γ bázisban. Ekkor s_α mátrixa a $\beta\gamma$ bázisban a $\begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{pmatrix}$ blokkmátrix, ahol A_{ki} az a_{ki}-vel való szorzás mátrixa β

bázisban. (Valóban, a_{ki} definíciója szerint $\alpha\gamma_i = \sum_{k=1}^m a_{ki}\gamma_k$, ezért $\alpha\gamma_i\beta_j = \sum_{k=1}^m (a_{ki}\beta_j)\gamma_k$, és $a_{ki}\beta_j$ pedig az A_{ki} mátrix j-edik oszlopának és a $(\beta_1, \dots, \beta_n)$ vektornak a skaláris szorzata az A_{ki} definíciója miatt.) Tehát

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{k=1}^m \mathrm{Tr}(A_{kk}) = \sum_{k=1}^m \mathrm{Tr}_{L/K}(a_{kk}) = \mathrm{Tr}_{L/K}(\sum_{k=1}^m a_{kk}) = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}(\alpha) \ .$$

□

2.3.3. Megjegyzés. A normára is igaz a $N_{L/K} \circ N_{M/L} = N_{M/K}$ összefüggés, de erre most nincs szükségünk, ezért nem bizonyítjuk.

2.3.4. Állítás. *Ha L/K* nem *szeparábilis, akkor* $\mathrm{Tr}_{L/K}$ *azonosan* 0.

Bizonyítás. Vegyük észre, hogy minden 0-karakterisztikájú test tökéletes, azaz minden bővítése szeparábilis. Legyen tehát $\mathrm{char}(K) = p > 0$, és $\alpha \in L$ egy inszeparábilis elem. Ekkor α minimálpolinomja $m_\alpha(x) = g(x^p)$ alakba írható valamilyen $g(x) \in K[x]$ irreducibilis polinomra. Ekkor $K \leq K(\alpha^p) \lneq K(\alpha) \leq L$, ahol a $K(\alpha)/K(\alpha^p)$ egy p-edfokú (tisztán) inszeparábilis bővítés ($|K(\alpha) : K(\alpha^p)| = p$ a fokszámtételből következik, hiszen α^p minimálpolinomja $g(x)$, az inszeparabilitás pedig abból, hogy α p-edik hatványa benne van $K(\alpha^p)$-ben). A 2.3.2(ii)-es Lemma szerint elég belátni, hogy $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)} = 0$. Node α^i ($i = 1, \dots, p-1$) minimálpolinomja ebben a bővítésben $x^p - \alpha^{pi}$, hiszen ez egy p-ed-fokú $K(\alpha^p)[x]$-beli polinom, aminek α^i gyöke, és $\alpha^i \notin K(\alpha^p)$, mivel egyébként α is benne lenne ebben a testben, ugyanis kifejezhető α^p és α^i egész kitevős hatványainak szorzataként. Tehát a 2.3.2(i)-es Lemma szerint $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)}(\alpha^i) = 0$ minden $1 \leq i \leq p-1$-re, sőt, $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)}(1) = |K(\alpha) : K(\alpha^p)| \cdot 1 = p \cdot 1 = 0$. Vagyis a $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)}$ lineáris leképezés eltűnik egy bázison, azaz azonosan 0. □

2.3.5. Lemma (Dedekind)**.** *Legyen L/K véges szeparábilis bővítés. Ekkor* $\mathrm{Hom}_K(L, \overline{K})$ *elemei lineárisan függetlenek $\overline{K}$ felett. (Azaz ha $\{\tau_1, \dots, \tau_n\} = \mathrm{Hom}_K(L, \overline{K})$, $a_1, \dots, a_n \in \overline{K}$, melyre $\sum_{i=1}^n a_i\tau_i \colon L \to \overline{K}$ az azonosan 0 K-lineáris leképezés, akkor $a_1 = \dots = a_n = 0$.)*

Bizonyítás. Legyen $a_1, \dots, a_n \in \overline{K}$. Tegyük fel, hogy $\sum_{i=1}^n a_i\tau_i(\alpha) = 0$ minden $\alpha \in L$-re. Az a_i-k közti nem 0 elemek száma szerinti indukcióval belátjuk, hogy $a_1 = \dots = a_n = 0$. Ha csak 1 darab $\neq 0$ van az a_i-k között, akkor készen vagyunk, hiszen egyik τ_i sem azonosan 0. Tegyük fel most, hogy $a_1 \neq 0 \neq a_2$. Mivel $\tau_1 \neq \tau_2$, ezért van olyan $\beta \in L$, melyre $\tau_1(\beta) \neq \tau_2(\beta)$. Ekkor a $\sum_i a_i\tau_i(\alpha) = 0$ egyenletet $\tau_1(\beta)$-val megszorozva, es levonva a $\sum_i a_i\tau_i(\beta\alpha) = 0$ egyenletből a $\sum_{i=2}^n a_i(\tau_i(\beta) - \tau_1(\beta))\tau_i(\alpha) = 0$ egyenletet kapjuk, melyben az indukciós feltevés miatt minden tag 0. Speciálisan $a_2 = 0$, ami ellentmondás. □

2.3.6. Állítás. *Legyen L/K szeparábilis bővítés, és* $\mathrm{Hom}_K(L, \overline{K}) = \{\tau_1, \dots, \tau_n\}$*. Ekkor* $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \tau_i(\alpha)$*, és* $N_{L/K}(\alpha) = \prod_{i=1}^n \tau_i(\alpha)$*.*

Bizonyítás. Legyen $\beta_1, \dots, \beta_n$ bázis L/K-ban (vegyük észre, hogy ez ugyanaz az n, hiszen feltettük, hogy L/K szeparábilis). Ekkor $S := (\tau_i(\beta_j))_{i,j}$ egy invertálható $n \times n$-es mátrix, hiszen az oszlopai lineárisan függetlenek a Dedekind Lemma miatt. Legyen $A = (a_{kj})_{k,j} \in K^{n \times n}$ az α-val való s_α szorzás mátrixa a $\beta_1, \dots, \beta_n$ bázisban, azaz $\alpha\beta_j = \sum_{k=1}^n \beta_k a_{k,j}$. Utóbbi egyenletre ráalkalmazva a τ_i K-homomorfizmust a

$$\tau_i(\alpha)\tau_i(\beta_j) = \sum_{k=1}^n \tau_i(\beta_k)\tau_i(a_{kj}) = \sum_{k=1}^n \tau_i(\beta_k)a_{kj}$$

egyenletet kapjuk, hiszen $a_{kj} \in K$. Ez pont azt jelenti, hogy

$$\begin{pmatrix} \tau_1(\alpha) & & \\ & \ddots & \\ & & \tau_n(\alpha) \end{pmatrix} S = SA \ ,$$

azaz $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(A) = \sum_{i=1}^n \tau_i(\alpha)$ és $N_{L/K}(\alpha) = \det(A) = \prod_{i=1}^n \tau_i(\alpha)$, hiszen S invertálható. □

2.3.7. Következmény. *Az L/K véges bővítés pontosan akkor szeparábilis, ha $\mathrm{Tr}_{L/K}$ nem azonosan 0.*

Bizonyítás. Ha L/K nem szeparábilis, akkor ez a 2.3.4-es Állítás, ha pedig L/K szeparábilis, akkor a 2.3.6-os Állításból következik, mivel $\mathrm{Tr}_{L/K} = \sum_{i=1}^n \tau_i$ nem azonosan 0 a Dedekind Lemma szerint, hiszen ez egy nemtriviális lineáris kombinációja a τ_i K-homomorfizmusoknak. □

2.3.8. Tétel (Hilbert 90)**.** *Tegyük fel, hogy L/K egy olyan Galois-bővítés, melyre* $\mathrm{Gal}(L/K) = \langle\sigma\rangle \cong Z_n$ *ciklikus (σ-val, mint generátorral) és $\alpha \in L$ egy 1-normájú elem. Ekkor van olyan $0 \neq \beta \in L$ elem, melyre $\alpha = \beta/\sigma(\beta)$.*

Megjegyzés: vegyük észre, hogy a megfordítás triviális, hiszen β és $\sigma(\beta)$ normája megegyezik.

Bizonyítás. A Dedekind Lemma miatt $\mathrm{id}_L, \sigma, \ldots, \sigma^{n-1}$ lineárisan függetlenek, ezért van olyan $\gamma \in L$, melyre

$$\beta := \mathrm{id}_L(\gamma) + \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\ldots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma) \neq 0 \ .$$

Könnyű számolás mutatja, hogy ekkor $\alpha\sigma(\beta) = \beta$. □

2.3.9. Következmény. *Ha $\mu_n \subseteq K$ és L/K olyan Galois-bővítés, melyre* $\mathrm{Gal}(L/K) \cong Z_n$*, akkor $L = K(\beta)$ alkalmas $\beta \in L$ elemmel, melynek minimálpolinomja $x^n - b$ alakú.*

Bizonyítás. Vegyük észre, hogy ha ε egy primitív n-edik egységgyök, akkor $\varepsilon \in K$ miatt $N_{L/K}(\varepsilon) = \varepsilon^n = 1$. Tehát Hilbert 90-es tétele szerint van olyan $0 \neq \beta \in L$, melyre $\beta/\sigma(\beta) = \varepsilon$. Ekkor $\sigma^i(\beta) = \beta\varepsilon^{-i}$, azaz β minimálpolinomja $m_\beta(x) = \prod_{i=0}^{n-1}(x - \beta\varepsilon^i) = x^n - \beta^n \in K[x]$ (hiszen $\sigma^i(\beta)$ mind különböző), azaz $b = \beta^n \in K$. □

2.3.10. Tétel (Normál bázis-)**.** *Legyen L/K egy véges Galois-bővítés és $G := \mathrm{Gal}(L/K)$. Ekkor van olyan $\beta \in L$, melyre a $\{\sigma(\beta) \mid \sigma \in G\}$ halmaz K-lineárisan független, tehát L egy K feletti bázisát alkotja. Egy ilyen bázist L/K* normál bázis*ának nevezünk.*

Bizonyítás. A bizonyítás két esetből áll.

1. eset: $|K|$ végtelen. Mivel L/K Galois, speciálisan szeparábilis, ezért van olyan $\alpha \in L$, melyre $L = K(\alpha)$. Legyen $f(x) \in K[x]$ az α minimálpolinomja. Ez L fölött $f(x) = \prod_{i=1}^n (x - \alpha_i)$ gyöktényezők szorzatára bomlik ($\alpha = \alpha_1$), hiszen L/K Galois bővítés. Legyen $g_i(x) := \frac{f(x)}{f'(\alpha_i)(x-\alpha_i)} \in L[x]$. Ekkor

$$\sum_{i=1}^n g_i(x) = 1 \ , \tag{2.1}$$

hiszen az $1-\sum_{i=1}^n g_i(x)$ egy legfeljebb $n-1$-edfokú polinom, ami az $\alpha_1,\dots,\alpha_n$ n különböző helyen eltűnik. Másrészt

$$g_i(x)g_j(x)\equiv\begin{cases}0 \mod (f(x)) & \text{ha } i\neq j\\ g_i(x) \mod (f(x)) & \text{ha } i=j\end{cases}. \tag{2.2}$$

Valóban, $g_i(x)g_j(x)$-nek gyöke $\alpha_1,\dots,\alpha_n$, ha $i\neq j$. Ha pedig $i=j$, akkor $g_i(x)^2-g_i(x)$-nek gyöke minden α_k $(k=1,\dots,n)$, hiszen $g_i(\alpha_i)^2=g_i(\alpha_i)=1$ és $k\neq i$-re $g_i(\alpha_k)=0$.

Legyen most $\mathrm{Gal}(L/K)=\{\mathrm{id}=\sigma_1,\dots,\sigma_n\}$ és $\alpha_i=\sigma_i(\alpha)\in L$. Képzzük az $A\in L[x]^{n\times n}$ mátrixot a következőképpen: legyen az i-edik sor j-edik eleme $\sigma_i(\sigma_j(g_1(x)))\in L[x]$. Ekkor az (2.1) és (2.2) azonosságok épp azt mutatják, hogy $A^TA\equiv I \mod (f(x))$ (itt I az egységmátrix). Valóban, vegyük észre, hogy $\sigma_i(g_1(x))=\frac{f(x)}{f'(\sigma_i(\alpha))(x-\sigma_i(\alpha))}=g_i(x)$, mivel $f(x)$ együtthatói K-ból valók, speciálisan minden σ_i fixálja őket. Tehát A^TA főátlójában $\sum_{i=1}^n g_i(x)^2$ áll, ami (2.1) és (2.2) kombinálásával 1-gyel kongruens modulo $(f(x))$. A főátlón kívüli elemek pedig $g_i(x)g_j(x)$ alakú tagok összegei, ahol $i\neq j$, tehát oszthatók $f(x)$-szel. Speciálisan $\det(A)^2=$ $=\det(A^TA)\equiv 1 \pmod{(f(x))}$, azaz nem lehet azonosan 0, így $\det(A)$ sem azonosan 0. Mivel K végtelen, van olyan $\gamma\in K$, melyre $\det(A(\gamma))=\det(\sigma_i\sigma_j(g_1(\gamma)))_{i,j}\neq 0$. Ekkor a $\beta=g_1(\gamma)$ választással tegyük fel, hogy $a_1\sigma_1(\beta)+\dots+a_n\sigma_n(\beta)=0$ valamilyen $a_1,\dots,a_n\in K$ elemekkel. Erre a σ_i automorfizmust ráalkalmazva azt kapjuk, hogy $\sum_{j=1}^n a_j\sigma_i\sigma_j(\beta)=0$, hiszen $\sigma_i(a_j)=$ $=a_j$ $(a_j\in K)$. Ez pedig azt jelenti, hogy $A(\gamma)\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}=0$, azaz $a_1=\dots=a_n=0$, mert $A(\gamma)$ invertálható. Azt kaptuk, hogy $\sigma_1(\beta),\dots,\sigma_n(\beta)$ lineárisan független K fölött, azaz egy bázisa L-nek, mint K feletti vektortérnek.

2. eset: $|K|=q=p^f$ véges. Ekkor $\mathrm{Gal}(L/K)$-t generálja a q-Frobenius Frob_q, melynek rendje $n=|L:K|$. A Dedekind Lemma miatt $\mathrm{id},\mathrm{Frob}_q,\dots,\mathrm{Frob}_q^{n-1}$ lineárisan független L felett, speciálisan Frob_q minimálpolinomja minimum n-edfokú. Viszont $\mathrm{Frob}_q^n=\mathrm{id}$, tehát $\mathrm{Frob}_q\colon L\to L$ K-lineáris leképezés minimálpolinomja x^n-1. Tekintsük L-et a $K[x]$ polinomgyűrű feletti modulusnak, ahol az x-szel való szorzás a Frob_q lineáris leképezés. A főideálgyűrű feletti modulusok alaptételéből következik, hogy $L\cong\bigoplus_{i=1}^r K[x]/(f_i(x))$ prímhatványrendű ciklikusak direkt összegeként írható, ahol ráadásul az $f_i(x)$-ek legkisebb közös többszöröse x^n-1 és $\sum_i\deg(f_i)=\dim_K L=n$. Tehát ha $x^n-1=\prod_j g_j(x)^{n_j}$ a K feletti irreducibilisekre való felbontás, akkor minden j-re van olyan i, melyre $g_j(x)^{n_j}\mid f_i(x)$. De ekkor $g_j(x)^{n_j}=f_i(x)$, mivel $\sum_j n_j\deg g_j=n=\sum_i\deg(f_i)$. Speciálisan $L\cong\bigoplus_j K[x]/(g_j(x)^{n_j}\cong K[x]/(x^n-1)$. Ha $\beta\in L$ az $1+(x^n-1)$ képe ennél az izomorfizmusnál, akkor x^k képe éppen $\mathrm{Frob}_q^k(\beta)$, és $\beta,\mathrm{Frob}_q(\beta),\dots,\mathrm{Frob}_q^{n-1}(\beta)$ bázis L-ben, hiszen $1,x,\dots,x^{n-1}$ bázis $K[x]/(x^n-1)$-ben. □

Legyen L/K egy véges Galois-bővítés, $G:=\mathrm{Gal}(L/K)$. Ekkor L-en hat a G csoport K-lineárisan, azaz L, mint n-dimenziós K-vektortér, a G csoport egy reprezentációját alkotja. A fenti tétel azt mutatja, hogy ha L-re mint a KG csoportalgebra feletti modulusra tekintünk, akkor $L\cong KG$ (mint KG feletti balmodulusok). Az izomorfizmust az $KG\ni 1\mapsto\beta\in L$ leképezés szolgáltatja. Tehát L természetes módon a G csoport reguláris reprezentációja (egy 1 rangú szabad KG-modulus). Ez az állítás fontos szerepet játszik a Galois-kohomológiában, speciálisan a Hilbert 90-es tétel általánosításaiban arra az esetre, amikor G nem feltétlenül ciklikus. A következő tételt is lehet a Galois-kohomológián (és a Normál Bázis Tételen) keresztül bizonyítani, de mivel előbbit nem tanuljuk, íme egy elemi bizonyítás:

2.3.11. Tétel (Artin-Schreier-elmélet)**.** *Legyen L/K egy p-edfokú Galois bővítése p karakterisztikájú testeknek. Ekkor van olyan $\alpha \in L$, melynek minimálpolinomja $x^p - x - a$ alakú.*

Bizonyítás. Legyen $\mathrm{Gal}(L/K) = G$, ekkor G egy p-edrendű csoport, tehát ciklikus. Jelöljük σ-val az egyik generátorát. A Dedekind Lemma miatt $1, \sigma, \ldots, \sigma^{p-1}$ linárisan független, tehát $\sigma\colon L \to L$ minimálpolinomja csak $x^p - 1 = (x-1)^p$ lehet. Tehát $(\sigma - 1)(L)$ $p-1$-dimenziós (egyébként már a $p-1$-edik hatványa is 0 lenne), és tartalmazza $K = \mathrm{Ker}(\sigma - 1)$-et. Mivel $1 \in K$, ezért van olyan $\alpha \in L$, melyre $\sigma(\alpha) - \alpha = (\sigma - 1)(\alpha) = 1$. Ezt iterálva azt kapjuk, hogy $\sigma^i(\alpha) = \alpha + i$ mind különbözők ($i = 0, \ldots, p-1$), tehát α minimálpolinomja $\prod_{i=0}^{p-1}(x - -\alpha - i) = (x-\alpha)^p - (x-\alpha) = x^p - x - a$ (ahol $a := \alpha^p - \alpha \in K$), hiszen $y^p - y = \prod_{i=0}^{p-1}(y-i)$ a gyöktényezős felbontás p-karakterisztikában. □

3. fejezet

Algebrai egészek

3.1. Egész elemek gyűrűbővítésben

3.1.1. Definíció. Legyenek $A \leq B$ kommutatív egységelemes gyűrűk. Azt mondjuk, hogy a $b \in B$ elem *egész* A fölött, ha létezik olyan $f(x) \in A[x]$ normált polinom, melyre $f(b) = 0$. Azt mondjuk, hogy a B gyűrű *egész* A *felett*, ha minden $b \in B$ egész.

3.1.2. Lemma. *Legyen $1 \in R$ egy tetszőleges kommutatív gyűrű, és $X \in R^{n\times n}$ egy négyzetes mátrix. Jelölje továbbá X^* azt a mátrixot, melynek i-edik sorának j-edik eleme az X mátrix j-edik sorának i-edik eleméhez tartozó előjeles aldeterminánsa. Ekkor $XX^* = X^*X = \det(X)I$, ahol I az egységmátrix. Speciálisan ha $v \in R^n$ egy oszlopvektor, melyre $Xv = 0$, akkor $\det(X)v = 0$.*

Bizonyítás. Az első állítás nem más, mint az inverz mátrix képlete lineáris algebrából. A második pedig következik az elsőből, hiszen ha $Xv = 0$, akkor $0 = X^*Xv = \det(X)v$. □

Az alábbi lemma nem más, mint a testbővítések elméletéből ismert fokszámtétel általánosítása gyűrűkre. Persze itt gyengébb feltételből bizonyítunk gyengébb állítást.

3.1.3. Lemma. *Gyűrűbővítésnél a moduluskénti végesen generáltság tranzitív, azaz ha $A \leq B \leq C$ egységelemes kommutatív gyűrűk, és B végesen generált mint A-modulus, C pedig végesen generált, mint B-modulus, akkor C is végesen generált, mint A-modulus.*

Bizonyítás. Ha B-t generálja $x_1, \ldots, x_k$ A fölött, C-t pedig generálja $y_1, \ldots, y_l$ B fölött, akkor $\{x_iy_j \mid 1 \leq i \leq k, 1 \leq j \leq l\}$ generálja C-t, mint A-modulust. □

3.1.4. Tétel. *Legyenek $A \leq B$ kommutatív egységelemes gyűrűk, és $b_1, \ldots, b_n \in B$. Ekkor $A[b_1, \ldots, b_n]$ pontosan akkor végesen generált modulus A felett, ha a b_i elemek egészek A felett ($i = 1, \ldots, n$).*

Bizonyítás. Tegyük fel először, hogy a b_i elemek egészek A felett minden $i = 1, \ldots, n$-re. Ha $n = 1$, akkor legyen b_1 minimálpolinomja $m(x) = x^k + a_1x^{k-1} + \cdots + a_k$ (k-adfokú, normált). Ekkor $1, b_1, \ldots, b_1^{k-1}$ nyilván generátorrendszer $A[b_1]$-ben, mint A-modulusban: Egyrészt $A[b_1]$ minden eleme felírható $f(b_1)$ alakban, ahol $f(x) \in A[x]$. Másrészt $f(x)$-et eloszthatjuk maradékosan $m(x)$-szel, hiszen m normált polinom, viszont $f(x) = q(x)m(x) + r(x)$ esetén nyilván

$f(b_1) = r(b_1)$, és r viszont már legfeljebb $k-1$-edfokú. Az indukciós lépés következik a végesen generáltság tranzitivitásából (3.1.3. Lemma).

A visszairányhoz tegyük fel, hogy $w_1, \dots, w_r$ egy véges generátorrendszer $A[b_1, \dots, b_n]$-ben, mint A-modulusban, és legyen $b \in A[b_1, \dots, b_n]$ tetszőleges. Ekkor mivel $\{w_i \mid i = 1, \dots, r\}$ generátorrendszer és $bw_i \in A[b_1, \dots, b_n]$, ezért van olyan $a_{ij} \in A$ $(1 \leq i, j \leq r)$, melyekre $bw_i = \sum_{j=1}^{r} a_{ij} w_j$. Ez pedig azt jelenti, hogy az $X := bI - ((a_{ij}))$ mátrixra $Xw = 0$, ahol $w = (w_1, \dots, w_r)^T \in B^r$. Tehát a 3.1.2-es Lemma szerint $\det(X)w_i = 0$ minden $i = 1, \dots, r$-re. Viszont $\{w_i\}$ egy generátorrendszer B-ben, ezért az $1 \in B$-t is ki lehet fejezni velük, speciálisan $\det(X) = \det(X) \cdot 1 = 0$. Viszont $\det(X)$ nem más, mint egy A-beli együtthatós normált polinom b-ben, melynek b gyöke, tehát b egész A fölött. □

3.1.5. Következmény. *Ha $b \in A[b_1, \dots, b_n]$, ahol $b_1, \dots, b_n$ mind egész A felett, akkor b is egész A felett. Speciálisan B azon elemei, melyek egészek A felett, részgyűrűt alkotnak.*

Bizonyítás. Valóban, ha b_1, b_2 egész, akkor $b_1 \pm b_2, b_1 b_2 \in A[b_1, b_2]$ is az. □

3.1.6. Következmény. *Az „egészség" is tranzitív: Ha $A \leq B \leq C$ egységelemes kommutatív gyűrűk, ahol B egész A fölött, C pedig egész B fölött, akkor C is egész A fölött.*

Bizonyítás. Vegyünk egy tetszőleges $c \in C$ elemet. Ennek B feletti minimálpolinomjában csak véges sok B-beli együttható szerepel (pl. $b_1, b_2, \dots, b_n$), ezek mindegyike egész A fölött, c pedig egész már $A[b_1, \dots, b_n]$ fölött is. Az állítás következik a végesen generáltság tranzitivitásából és a 3.1.4-es Tételből. □

Mivel egész gyűrűbővítések egymásutánja is egész gyűrűbővítés, ezért értelmes az alábbi definíció.

3.1.7. Definíció. Legyen $A \leq B$ kommutatív egységelemes gyűrűk. Ekkor az

$$\overline{A}_B := \{b \in B \mid b \text{ egész } A \text{ fölött}\}$$

gyűrűt nevezzük A *egész lezártjának* B-ben. Ha B adott és ez nem vezet félreértéshez, gyakran elhagyjuk a $_B$ indexet. Speciálisan ha A integritási tartomány, K pedig a hányadosteste, akkor $\overline{A} = \overline{A}_K$-t A *normalizáltjának*, vagy *egész lezártjának* nevezzük. Ha $\mathbb{Q} \leq K$ egy (véges vagy végtelen) testbővítés, akkor $\mathbb{Z}$ egész lezártját K-ban a K-beli algebrai egészek gyűrűjének hívjuk, és $\overline{\mathbb{Z}}_K =: \mathcal{O}_K$-val jelöljük. $\overline{\mathbb{Z}} = \overline{\mathbb{Z}}_{\mathbb{C}}$ nem más, mint az algebrai egészek gyűrűje. Egy A integritási tartományról azt mondjuk, hogy *egészre zárt*, ha $\overline{A}_K = A$, ahol K a hányadostest.

3.1.8. Példa. Az egész számok $\mathbb{Z}$ gyűrűje egészre zárt. Ez nem más, mint a racionális gyöktesztː ha egy $\frac{a}{b}$ racionális szám gyöke egy egész együtthatós normált polinomnak, akkor b osztja a főegyüttható̋t, azaz $b = \pm 1$.

3.2. Diszkrimináns, egész bázis

Legyen L/K egy véges szeparábilis bővítés, $\alpha_1, \dots, \alpha_n$ pedig bázis L-ben, mint K-vektortérben. Jelöljük továbbá $\mathrm{Hom}_K(L, \overline{K})$ elemeit $\sigma_1, \dots, \sigma_n$-nel. Vegyük észre, hogy L/K szeparábilitása épp azt jelenti, hogy $|\mathrm{Hom}_K(L, \overline{K})| = |L : K| = n$.

3.2.1. Definíció. Az $(\alpha_1, \ldots, \alpha_n)$ bázis *diszkriminánsa*

$$d(\alpha_1, \ldots, \alpha_n) := \det((\sigma_i \alpha_j))_{i,j}^2 \ ,$$

azaz azon M mátrix determinánsának négyzete, melynek i-edik sorának j-edik eleme $\sigma_i \alpha_j$ $(1 \leq i, j \leq n)$.

Vegyük észre, hogy *a priori* csak annyit tudunk, hogy $d(\alpha_1, \ldots, \alpha_n) \in \overline{K}$. A következőkben a nyom segítségével belátjuk, hogy valójában $d(\alpha_1, \ldots, \alpha_n) \in K$. Valóban,

$$\mathrm{Tr}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} (\sigma_k \alpha_i)(\sigma_k \alpha_j) \ ,$$

hiszen σ_k egy testhomomorfizmus. Node ez azt jelenti, hogy ha az N mátrix i-edik sorának j-edik eleme $\mathrm{Tr}(\alpha_i \alpha_j) \in K$, akkor $N = M^T M$, speciálisan determinánsa $d(\alpha_1, \ldots, \alpha_n) = \det(M)^2 = \det(N) \in K$.

3.2.2. Példa. Ha pl. $L = K(\alpha)$ egy elem által generált, és a bázisunk elemei $1, \alpha, \ldots, \alpha^{n-1}$, akkor az M mátrix egy Vandermonde-típusú mátrix. Speciálisan ha α szeparábilis K fölött, akkor Galois-konjugáltjai mind különbözők, tehát $d(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$.

A fenti példán alapul az alábbi tétel:

3.2.3. Tétel. *Legyen L/K egy véges szeparábilis bővítés, melyben $\alpha_1, \ldots, \alpha_n$ egy bázis. Ekkor $d(\alpha_1, \ldots, \alpha_n) \neq 0$. Sőt, az L-en, mint K-vektortéren az $(x, y) := \mathrm{Tr}(xy)$ egy nemelfajuló szimmetrikus bilineáris forma.*

Bizonyítás. Mivel L/K szeparábilis (és véges), ezért egyszerű, azaz alkalmas $\alpha \in L$-lel $L = K(\alpha)$. Tehát ebben a bázisban a diszkrimináns nem 0 a fenti példa miatt. Viszont ez azt jelenti, hogy (x, y) egy nemelfajuló bilineáris forma, hiszen egy alkalmas bázisban vett mátrixának nem 0 a determinánsa. Ebből viszont az is következik, hogy semmilyen bázisban sem 0 a determinánsa, azaz $d(\alpha_1, \ldots, \alpha_n) \neq 0$. □

Vegyük észre, hogy így a diszkriminánson keresztül új bizonyítást kaptunk Dedekind tételére (2.3.5-ös Lemma), mely szerint $\mathrm{Hom}_K(L, \overline{K})$ elemei lineárisan függetlenek. Valóban, ha lineárisan összefüggők lennének, akkor az M mátrix sorai is lineárisan összefüggők lennének, holott $\det(M) \neq 0$.

Mostantól legyen A egy *egészre zárt integritási tartomány*, melynek K-val jelöljük a hányadostestét. Legyen továbbá L/K egy véges szeparábilis bővítés, melyben jelöljük B-vel az A felett egész elemek részgyűrűjét. Vegyük észre, hogy mivel A egészre zárt, ezért $A = B \cap K$. Speciálisan $b \in B$ esetén $\mathrm{Tr}_{L/K}(b)$ és $N_{L/K}(b)$ is A-ban van, hiszen mindkettő egész A fölött (b konjugáltjainak, azaz egész elemeknek az összege, ill. szorzata) és K-ban is van. Továbbá ha $b \in B^\times$ (invertálható elem), akkor $b^{-1} \in B$, azaz $N_{L/K}(b), N_{L/K}(b^{-1}) \in A$, melyekre $1 = N(1) = N(b)N(b^{-1})$, azaz $N(b) \in A^\times$. Megfordítva, ha $N(b) \in A^\times$, akkor alkalmas $a \in A$ elemmel $1 = a \cdot \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(b)$, speciálisan b is invertálható B-ben, hiszen ebben a szorzatban b is egy szorzótényező. Egyszóval azt kaptuk, hogy $b \in B^\times \Leftrightarrow N_{L/K}(b) \in A^\times$.

Vegyük észre továbbá, hogy B hányadosteste szükségképpen L. Sőt, L minden elemét fel tudjuk írni b/a alakban, ahol $b \in B$ és $0 \neq a \in A$. Valóban, ha β (A-beli együtthatós) minimálpolinomjának főegyütthatója a, akkor $a\beta$ minimálpolinomja már normált, tehát $a\beta \in B$. Speciálisan az L/K bővítésnek van B elemeiből álló bázisa.

3.2.4. Állítás. *Ha $\alpha_1, \ldots, \alpha_n \in B$ egy bázisa L/K-nak és $d = d(\alpha_1, \ldots, \alpha_n)$, akkor $dB \subseteq$ $\subseteq A\alpha_1 \oplus \ldots \oplus A\alpha_n \subseteq B$.*

Bizonyítás. Mivel $\alpha_1, \ldots, \alpha_n$ egy bázis L/K-ban, ezért lineárisan független K fölött, így A fölött is. Speciálisan az $A\alpha_1 + \cdots + A\alpha_n$ összeg valóban direkt. A második tartalmazás triviális, hiszen $\alpha_1, \ldots, \alpha_n \in B$. Az első tartalmazáshoz legyen $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n \in B$ ($x_1, \ldots, x_n \in$ $\in K$). Ekkor minden $j = 1, \ldots, n$-re

$$A \ni \mathrm{Tr}_{L/K}(\alpha_j\alpha) = \sum_{i=1}^{n} \mathrm{Tr}_{L/K}(\alpha_i\alpha_j)x_i \ .$$

Tehát $N = (\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{i,j}$ mátrixszal $Nx \in A^n$, ahol $x = (x_1, \ldots, x_n)^T$. Ezt megszorozva N^*-gal (N előjeles aldeterminánsaiból álló mátrix) azt kapjuk, hogy $dx = \det(N)x \in A^n$, azaz $dx_i \in A$ minden $i = 1, \ldots, n$-re. □

3.2.5. Definíció. A $w_1, \ldots, w_n \in B$ elemeket a B egy A feletti egész bázisának nevezzük, ha $B = Aw_1 \oplus \ldots \oplus Aw_n$, azaz ha minden $b \in B$ egyértelműen felírható $b = a_1w_1 + \cdots + a_nw_n$ alakban, ahol $a_1, \ldots, a_n \in A$.

Egész bázis nem mindig létezik, létezése azzal ekvivalens, hogy B egy szabad A-modulus. Viszont ha A főideálgyűrű, akkor minden végesen generált torziómentes modulus szabad, speciálisan B is, ahogy azt a következő tétel állítja.

3.2.6. Tétel. *Legyen A egy egészre zárt integritási tartomány, melynek K a hányadosteste, és legyen L/K egy véges szeparábilis bővítés, melyben B az A feletti egészek részgyűrűje. Tegyük fel továbbá, hogy A főideálgyűrű. Ekkor minden $0 \neq M \subseteq L$ végesen generált B-részmodulus (speciálisan $M = B$ is) egy szabad $|L : K|$-rangú modulus A felett.*

Bizonyítás. Először vegyük észre, hogy mivel $M \subseteq L$ benne van egy testben, ezért M szükségképpen torziómentes, hiszen a testek 0-osztómentesek. Továbbá mivel M végesen generált B fölött, és B végesen generált A fölött, ezért M végesen generált A fölött is. Így a főideálgyűrű feletti végesen generált modulusok alaptétele (7.4.1-es tétel [7]-ben) miatt M (torziómentes) ciklikus modulusok direkt összege, azaz szabad. Tehát már csak azt kell belátnunk, hogy rangja megegyezik az L/K bővítés fokával.

Ha $M = B$, akkor a 3.2.4-es állítás szerint $\mathrm{rk}(B) = \mathrm{rk}(dB) \leq \mathrm{rk}(A\alpha_1 \oplus \ldots \oplus A\alpha_n) =$ $= n \leq \mathrm{rk}(B)$, azaz $\mathrm{rk}(B) = n$. Másrészt ha M tetszőleges végesen generált B-modulus, akkor legyen $m_1, \ldots, m_r \in M$ egy generátorrendszer B fölött. Mivel L és így M minden elemét fel tudjuk írni egy B-beli és egy A-beli hányadosaként, ezért a véges sok $m_1, \ldots, m_r$ generátorra van egy közös $0 \neq a \in A$ elem, melyre $am_i \in B$ ($i = 1, \ldots, r$). Viszont ekkor $aM \subseteq B$. Másrészt $Bm_1 \subseteq M$, azaz $\mathrm{rk}(B) = \mathrm{rk}(am_1B) \leq \mathrm{rk}(aM) = \mathrm{rk}(M) \leq \mathrm{rk}(B)$. □

Hogyan találhatunk egész bázist egy gyűrűbővítésben? Az egyszerűség kedvéért legyen $A =$ $= \mathbb{Z}$, $K/\mathbb{Q}$ egy véges bővítés, melyben $\mathcal{O}_K$ az egészek gyűrűje. Vegyük először K-nak egy $\mathcal{O}_K$ elemeiből álló $\alpha_1, \ldots, \alpha_n$ bázisát. Ilyet pl. úgy kaphatunk, ha K-t $K = \mathbb{Q}(\alpha)$ alakba írjuk, ahol α algebrai egész (ezt feltehetjük, hiszen α-t megszorozhatjuk egész együtthatós minimálpolinomjának főegyütthatójával). Ekkor $1, \alpha, \ldots, \alpha^{n-1}$ egy ilyen bázis lesz ($n = |L : K|$). Egy ilyen $\alpha_1, \ldots, \alpha_n$ bázis esetén nyilván $\mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K$. Másrészt legyen $\alpha = \sum_{i=1}^{n} x_i\alpha_i \in$ $\in \mathcal{O}_K$ ($x_1, \ldots, x_n \in \mathbb{Q}$) és $x := (x_1, \ldots, x_n)^T$. Az $M := ((\mathrm{Tr}(\alpha_i\alpha_j))) \in \mathbb{Z}^{n\times n}$ mátrix kiszámolható véges idő alatt, és a $\mathrm{Tr}(\alpha\alpha_i) \in \mathbb{Z}$ összefüggéseket egybegyűjtve azt kapjuk, hogy

$Mx \in \mathbb{Z}^n$. Ez ad egy felső becslést az x_i racionális számok nevezőire. A legtriviálisabb becslés, hogy minden nevező osztója $d = \det(M)$-nek, de egyes együtthatókra ennél jóval jobbat is kaphatunk az M mátrix sorainak (egész együtthatós) Gauß-eliminációjával (M-et mindig felsőháromszög-alakra hozhatjuk úgy is, hogy sorokat permutálunk és sorokból másik sorok egész számszorosát vonjuk le). Tehát $\mathcal{O}_K$ elemeinek meghatározását visszavezettük arra, hogy véges sok elemről kell eldönteni, hogy algebrai egész-e, hiszen $\mathbb{Z}^n$ indexe $M^{-1}\mathbb{Z}^n$-ben véges, mégpedig d. Valóban, mivel az algebrai egészek részgyűrűt alkotnak, ezért elegendő minden nemtriviális mellékosztályból egy-egy elemet megvizsgálni. Sőt, ennek a d-rendű faktorcsoportnak a részcsoportjait kell csak lefedni, amit megtehetünk ennél jóval kevesebb elemmel is. Vegyük észre, hogy ha csak azt a gyengébb állítást használnánk, hogy $dx \in \mathbb{Z}^n$, akkor $d-1$ helyett $d^n - 1$ darab elemet kellene megvizsgálnunk.

Hogyan dönthetjük el egy adott $\alpha \in K$ elemről, hogy algebrai egész-e? Az egyetlen biztos módszer α minimálpolinomjának vagy az α-val való szorzás, mint $\mathbb{Q}$-lineáris leképezés karakterisztikus polinomjának meghatározása. Ha már egyébként is ismerünk egy bázist, akkor általában gyorsabb felírni az utóbbi karakterisztikus polinomot, amihez csak $\alpha\alpha_i$-t kell felírnunk az $\alpha_1, \ldots, \alpha_n$ bázisban minden $i = 1, \ldots, n$-re. Viszont konkrét elemek esetében (főleg ha azt sejtjük, hogy nem egészek) gyorsíthatunk az eljáráson. Egyrészt kihasználhatjuk, hogy az algebrai egészek gyűrűt alkotnak, tehát az adott elemünk hatványainak is teljesítenie kell a korábban a nevezőkre adott feltételt. Gyakran az is hasznos, ha az elemnek csak a normáját írjuk fel, már ebből is kiderül, hogy nem algebrai egész.

Hogyan határozzuk meg az egész bázist, ha már van egy szükséges és elégséges feltételünk az α_i-k ($i = 1, \ldots, n$) együtthatóira? Erre a legjobb módszer a [7] könyvben a főideálgyűrű feletti végesen generált modulusuk (7.4.1-es) alaptételének algoritmikus bizonyítása.

Az alábbi példában a fenti módszer illusztrációjaként meghatározzuk $\mathbb{Q}(\sqrt{13})$ algebrai egészeit.

3.2.7. Példa. $K = \mathbb{Q}(\sqrt{13})$ algebrai egészeiben az 1 és az $\frac{1+\sqrt{13}}{2}$ elemek egész bázist alkotnak.

Bizonyítás. Induljunk ki az $1, \sqrt{13}$ bázisból. Mivel $\mathrm{Tr}(1) = 2$ és $\mathrm{Tr}(\sqrt{13}) = 0$ (hiszen $\sqrt{13}$ konjugáltjai $\pm\sqrt{13}$), ezért $M = \begin{pmatrix} 2 & 0 \\ 0 & 26 \end{pmatrix}$. Legyen $a + b\sqrt{13}$ algebrai egész ($a, b \in \mathbb{Q}$), ekkor $2a \in \mathbb{Z}$ és $26b \in \mathbb{Z}$, tehát $a = a_1/2$ és $b = b_1/26$ alakba írható, ahol $a_1, b_1 \in \mathbb{Z}$. Node $a + b\sqrt{13}$ normája $(a + b\sqrt{13})(a - b\sqrt{13}) = a^2 - 13b^2 = \frac{13a_1^2 - b_1^2}{52} \in \mathbb{Z}$, ezért $13 \mid b_1^2$, azaz $13 \mid b_1$. Tehát $\mathcal{O}_K \subseteq \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}\sqrt{13}$, azaz csak 3 elemet kell megvizsgálnunk. Ezek közül $1/2$ és $\sqrt{13}/2$ nyilván nem egész, de $\frac{1+\sqrt{13}}{2}$ igen. □

3.2.8. Definíció. Legyen $K/\mathbb{Q}$ véges. A $0 \neq I \subset K$ végesen generált $\mathcal{O}_K$-részmodulusokat *törtideáloknak* nevezzük.

A 3.2.6. Tétel szerint az I törtideálnak létezik egy $\alpha_1, \ldots, \alpha_n$ bázisa $\mathbb{Z}$ fölött.

3.2.9. Állítás. *A $d(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$ szám nem függ a $\mathbb{Z}$-bázis választásától.*

Bizonyítás. Legyen $\alpha_1', \ldots, \alpha_n'$ egy másik bázis $\mathbb{Z}$ fölött. Ekkor a S áttérési mátrix invertálható $\mathbb{Z}$ fölött, ezért determinánsa ± 1. Az $(x, y) = \mathrm{Tr}(xy)$ bilineáris forma mátrixa legyen M az $\alpha_1, \ldots, \alpha_n$ bázisban, ill. M' az $\alpha_1', \ldots, \alpha_n'$ bázisban. Ekkor $M' = S^T M S$, speciálisan $d(\alpha_1', \ldots, \alpha_n') = \det(M') = (\det(S))^2 \det(M) = d(\alpha_1, \ldots, \alpha_n)$. □

3.2.10. Definíció. Az I *törtideál diszkriminánsa* $d(I) := d(\alpha_1, \ldots, \alpha_n)$, ahol $\alpha_1, \ldots, \alpha_n$ tetszőleges $\mathbb{Z}$-bázis I-ben. A K *számtest diszkriminánsa* definíció szerint $d_K := d(\mathcal{O}_K)$.

3.2.11. Állítás. *Ha $I \subseteq I'$ törtideálok K-ban, akkor $d(I) = |I' : I|^2 d(I')$. Speciálisan az $|I' : I|$ index véges.*

Bizonyítás. Legyen $\alpha_1, \ldots, \alpha_n$ $\mathbb{Z}$-bázis I-ben, $\alpha'_1, \ldots, \alpha'_n$ pedig I'-ben. Ha S az áttérési mátrix, akkor $d(I) = (\det(S))^2 d(I')$. Node S-et a ([7] 7.4.1. Tétel bizonyításának mintájára) elemi átalakításokkal normálakra lehet hozni, mely során $|\det(S)|$ nem változik. Viszont a normálalakban lévő S mátrix determinánsa nem más, mint a komagjának (azaz $\mathrm{Coker}(S) = \mathbb{Z}^n/\mathrm{Im}(S)$-nek) az elemszáma, tehát $|I' : I| = |\det(S)|$. □

3.3. Dedekind gyűrűk, egyértelmű prímfaktorizáció az ideálokra

Legyen $K = \mathbb{Q}(\sqrt{-5})$. Ebben az egészek gyűrűje nem más, mint $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Viszont $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Könnyű számolás mutatja, hogy ezek mind felbonthatatlanok, tehát nem teljesül a számelmélet alaptétele $\mathbb{Z}[\sqrt{-5}]$-ben.

Legyen mostantól $K/\mathbb{Q}$ tetszőleges véges bővítés, melyben $\mathcal{O}_K$ az egészek gyűrűje.

3.3.1. Tétel. *Az $\mathcal{O}_K$ gyűrű noether, egészre zárt, és minden $0 \neq P \lhd \mathcal{O}_K$ prímideál maximális (azaz $\mathcal{O}_K$ Krull-dimenziója 1).*

Bizonyítás. Noether tulajdonság: Legyen $I \lhd \mathcal{O}_K$ egy ideál. Mivel $\mathcal{O}_K$ végesen generált $\mathbb{Z}$-modulus, és $\mathbb{Z}$ noether, ezért I is végesen generált, mint $\mathbb{Z}$-modulus, speciálisan $\mathcal{O}_K$ felett is.

Egészre zártság: Definíció szerint $\mathcal{O}_K$ nem más, mint $\mathbb{Z}$ egész lezártja K-ban, tehát egészre zárt a 3.1.6. Következmény miatt.

Legyen $P \lhd \mathcal{O}_K$ egy prímideál. Ekkor $\mathcal{O}_K/P$ nullosztómentes, és a 3.2.11. Állítás miatt $\mathcal{O}_K/P$ véges is. De ekkor $\mathcal{O}_K/P$ test, azaz P maximális ideál. □

3.3.2. Definíció. Az R integritási tartomány *Dedekind gyűrű*, ha noether, egészre zárt, és minden $\neq 0$ prímideál maximális.

A célunk a következő tétel bizonyítása:

3.3.3. Tétel. *Egy tetszőleges $\mathcal{O}$ Dedekind gyűrűben minden $(0) \neq I \neq (1)$ ideál előáll prímideálok szorzataként. Az előállítás sorrendtől eltekintve egyértelmű.*

3.3.4. Lemma. *Minden $I \lhd \mathcal{O}$ ideálra léteznek olyan $P_1, \ldots, P_n$ (nem feltétlenül különböző, de $\neq 0$) prímideálok, melyekre $I \supseteq P_1 \ldots P_n$.*

Bizonyítás. Mivel $\mathcal{O}$ noether, ezért az ideálokra teljesül a maximumfeltétel. Tehát ha van olyan ideál, ami nem teljesíti a feladat állítását, akkor van ilyen maximális is. Legyen I tehát maximális, melyre nincsenek ilyen prímideálok. Ekkor I nem lehet prímideál, hiszen akkor az állítás triviálisan teljesülne $P_1 = I$-vel. Viszont ekkor van olyan $b_1, b_2 \in \mathcal{O} \setminus I$ elem, melyre $b_1 b_2 \in I$. Ekkor $I \subsetneq (b_i) + I$ $(i = 1{,}2)$ és I maximalitása miatt van olyan $P_1, \ldots, P_n$ és $P'_1, \ldots, P'_k$ prímek, melyekre $P_1 \ldots P_n \subseteq I + (b_1)$ és $P'_1 \ldots P'_k \subseteq I + (b_2)$. Viszont ekkor $P_1 \ldots P_n P'_1 \ldots P'_k \subseteq (I + (b_1))(I + (b_2)) \subseteq I$. □

3.3.5. Definíció. Legyen $0 \neq I \lhd \mathcal{O}$ egy ideál. Ekkor $I^{-1} := \{x \in K \mid xI \subseteq \mathcal{O}\}$ halmaz az I ideál inverze (itt K az $\mathcal{O}$ hányadosteste). Ez egy végesen generált $\mathcal{O}$-részmodulus K-ban, azaz törtideál.

3.3.6. Lemma. *Legyen $0 \neq I \lhd \mathcal{O}$ egy ideál, illetve $0 \neq P$ egy prímideál $\mathcal{O}$-ban. Ekkor*

$$IP^{-1} := \{\sum a_i x_i \text{ véges } \mid a_i \in I, x_i \in P^{-1}\} \neq I \ .$$

Bizonyítás. Először belátjuk, hogy $P^{-1} \neq \mathcal{O}$. Legyen $0 \neq a \in P$. Ekkor van olyan $P_1, \ldots, P_n$ prímideál $\mathcal{O}$-ban, melyre $P_1 \ldots P_n \subseteq (a) \subseteq P$. Feltehetjük, hogy ez a szorzat rövidíthetetlen. Ekkor mivel P prím, ezért van olyan i, melyre $P_i \subseteq P$, azaz mivel P_i maximális, ezért $P_i = P$. Tehát pl. $P_1 = P$ és a szorzat rövidíthetetlensége miatt $P_2 \ldots P_n \not\subseteq (a)$. Azaz van olyan $b \in P_2 \ldots P_n$, melyre $b \notin (a)$, azaz $a^{-1}b \notin \mathcal{O}$. Másrészt $bP \subseteq P_1 \ldots P_n \subseteq (a)$, ezért $a^{-1}b \in P^{-1}$.

Most tegyük fel, hogy $0 \neq I \lhd \mathcal{O}$ egy olyan ideál, melyre $IP^{-1} = I$. Mivel $\mathcal{O}$ noether, ezért I-nek van egy véges, $\alpha_1, \ldots, \alpha_n$ generátorrendszere. Legyen $b \in P^{-1} \setminus \mathcal{O}$. Ekkor $b\alpha_j = \sum_{i=1}^{n} c_{ij}\alpha_i$ alkalmas $c_{ij} \in \mathcal{O}$ elemekkel, hiszen $b\alpha_j \in P^{-1}I = I$, és $\alpha_1, \ldots, \alpha_n$ generátorrendszer I-ben. Node ekkor b gyöke a $((c_{ij}))$ mátrix karakterisztikus polinomjának, speciálisan egész $\mathcal{O}$ felett, azaz $b \in \mathcal{O}$, hiszen $\mathcal{O}$ egészre zárt. Ez ellentmondás, tehát eredeti feltevésünk hamis volt, azaz $IP^{-1} \neq I$. □

A 3.3.3. Tétel bizonyítása. **Létezés:** Legyen $(0), (1) \neq I \lhd \mathcal{O}$ egy ideál. Tegyük fel indirekten, hogy I nem áll elő prímideálok szorzataként. Mivel $\mathcal{O}$-ban az ideálokra teljesül a maximum feltétel, ezért feltehetjük, hogy I maximális ezzel a tulajdonsággal. Mivel $I \neq (1) = \mathcal{O}$, ezért I benne van egy P maximális ideálban. A 3.3.6. Lemma miatt $\mathcal{O} \subsetneq P^{-1}$ és $I \subsetneq IP^{-1} \subseteq PP^{-1} \subseteq \mathcal{O}$. Így I maximalitása miatt $IP^{-1} = P_1 \ldots P_n$ felírható prímideálok szorzataként. Ugyanezt a lemmát alkalmazva $I = P$-vel azt kapjuk, hogy $P \subsetneq PP^{-1} \subseteq \mathcal{O}$. Mivel P maximális ideál, ezért $PP^{-1} = \mathcal{O}$. Tehát azt kapjuk, hogy $I = IPP^{-1} = P_1 \ldots P_n P$.

Egyértelműség: Legyen $P_1 \ldots P_n = Q_1 \ldots Q_k$ két különböző felírás prímideálok szorzatára. Ekkor $P_1 \supseteq Q_1 \ldots Q_k$, ezért van olyan $1 \leq i \leq k$, melyre $P_1 \supseteq Q_i$. De Q_i maximális, ezért $P_1 = Q_i$. Mindkét oldalt megszorozva P_1^{-1}-zel az állítás n szerinti indukcióval adódik. □

3.3.7. Állítás. *Egy $0 \neq A \leq K$ $\mathcal{O}$-részmodulus pontosan akkor törtideál (azaz végesen generált), ha van olyan $0 \neq c \in \mathcal{O}$, melyre $cA \subseteq \mathcal{O}$.*

Bizonyítás. $\Leftarrow$: Ha van ilyen $0 \neq c \in \mathcal{O}$, akkor $A \subseteq 1/c\mathcal{O}$. Viszont $1/c\mathcal{O}$ egy elemmel generált, és $\mathcal{O}$ noether, ezért A is végesen generált. $\Rightarrow$: Ha A törtideál, akkor elég a generátorainak találnunk egy közös c nevezőt, azzal beszorozva $cA \subseteq \mathcal{O}$. □

3.3.8. Állítás. *A (0)-tól különböző törtideálok halmaza Abel-csoportot alkot a szorzásra nézve. Jele: J_K (ideálcsoport). Az egységelem $(1) = \mathcal{O}$, inverz: $I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}\}$.*

Bizonyítás. Az asszociativitás és a kommutativitás világos, mint ahogy $I(1) = I$ is. Prímideálokra már láttuk, hogy $PP^{-1} = (1)$, továbbá minden $A \lhd \mathcal{O}$ egész ideál prímideálok szorzata: $A = P_1 \ldots P_n$, tehát ha $B = P_1^{-1} \ldots P_n^{-1}$, akkor $AB = BA = (1)$. Viszont azt is be kell látnunk, hogy a fenti képlet ($I = A$-val) megadja B-t. Mivel $AB = \mathcal{O}$, ezért $B \subseteq A^{-1}$. Másrészt $x \in A^{-1}$ esetén $xA \subseteq \mathcal{O}$, ezért $x \in x\mathcal{O} = xAB \subseteq B$, azaz $B = A^{-1}$. Tehát az állítást egész ideálokra beláttuk, egy I törtideál viszont $I = c^{-1}A$ alakba írható, ahol $A \lhd \mathcal{O}$. □

3.3.9. Következmény. *Dedekind gyűrűben minden $I \neq (0)$ törtideál egyértelműen írható $I = P_1^{\alpha_1} \dots P_n^{\alpha_n}$ alakban, ahol $P_i \lhd \mathcal{O}$ prímideálok és $\alpha_i \in \mathbb{Z}$ $(i = 1, \dots, n)$.*

3.3.10. Definíció. Az $\mathcal{O}_K$ Dedekind gyűrű *osztálycsoportja* a $Cl_K = J_K/P_K$ faktorcsoport, ahol P_K a törtfőideálok (azaz $c\mathcal{O}$ alakú törtideálok) részcsoportja J_K-ban.

3.3.11. Állítás. *Az*

$$1 \to \mathcal{O}^\times \to K^\times \to J_K \to Cl_K \to 1$$

sorozat egzakt.

Bizonyítás. Az $\mathcal{O}^\times$-nél és Cl_K-nál világos az egzaktság. A $K^\times \to J_K$ leképezés egy $c \in K^\times$ elemet az általa generált $c\mathcal{O}$ főideálba képez. Tehát képe éppen P_K, magja pedig azon c elemekből áll, melyekre $c\mathcal{O} = \mathcal{O}$, azaz $\mathcal{O}$ egységeiből. □

3.3.12. Állítás. *Egy $\mathcal{O}$ Dedekind gyűrűre a következők ekvivalensek:*

(1) $Cl_K = \{1\}$*;*

(2) $\mathcal{O}$ *főideálgyűrű;*

(3) $\mathcal{O}$*-ban elemekre is igaz a számelmélet alaptétele.*

Bizonyítás. Definíció szerint $Cl_K = \{1\} \Leftrightarrow J_K = P_K$ pontosan akkor teljesül, ha minden törtideál főideál. Ekkor persze $\mathcal{O}$ főideálgyűrű. Viszont ha $\mathcal{O}$ főideálgyűrű, akkor a törtideálok is generálhatók egy elemmel, hiszen ezek egész ideálok hányadosai. Tehát (1) $\Leftrightarrow$ (2). Továbbá (2) $\Rightarrow$ (3) klasszikus (lsd. [7] 5.5.8. Következmény). A (3) $\Rightarrow$ (2) irányhoz elég belátni, hogy minden prímideál főideál, hiszen ilyenek szorzataként minden ideál előáll. Legyen $0 \neq P$ tehát egy prímideál és vegyünk egy $0 \neq a \in P$ elemet. (3) miatt ezt elő tudjuk állítani $a = p_1 \dots p_n$ alakban, ahol $p_i \in \mathcal{O}$ prímek. Mivel P prímideál, ezért van olyan $i \in \{1, \dots, n\}$, melyre $p_i \in$ $\in P$, azaz $(p_i) \subseteq P$. Node az $\mathcal{O}$ Dedekind gyűrűben minden prímideál maximális, tehát (p_i) is, ezért $(p_i) = P$. □

3.4. Rácsok és Minkowski-elmélet

A következő célunk az, hogy belássuk, hogy $K/\mathbb{Q}$ véges bővítés esetén az $\mathcal{O}_K$ gyűrű osztálycsoportja véges. Ehhez szükségünk van némi konvex geometriára.

3.4.1. Definíció. Legyen V egy végesdimenziós vektortér $\mathbb{R}$ felett és $n := \dim V$. $\mathbb{Z}$*-rácsnak* hívjuk V egy

$$\Gamma = \mathbb{Z}v_1 + \dots \mathbb{Z}v_m$$

alakú additív részcsoportját, ha a $v_1, \dots, v_m$ vektorok lineárisan függetlenek. Ha $n = m$, akkor azt mondjuk, hogy a rács teljes. (Ilyenkor azt is mondjuk, hogy Γ egy $\mathbb{Z}$-struktúra V-n.) A Γ rács *fundamentális tartományának* a $\Phi = \{x_1v_1 + \dots x_mv_m \mid 0 \leq x_i < 1, i = 1, \dots, m\}$ halmazt nevezzük.

Vegyük észre, hogy Γ pontosan akkor teljes, ha $\bigcup_{\gamma \in \Gamma}(\Phi + \gamma) = V$.

3.4.2. Állítás. *Egy Γ additív részcsoport V-ben pontosan akkor rács, ha a V-ből örökölt topológiában diszkrét.*

Bizonyítás. Valóban, ha a $v_1, \dots, v_m$ vektorok lineárisan függetlenek, akkor az általuk generált additív részcsoport diszkrét. Visszafelé legyen Γ diszkrét. Belátjuk, hogy ekkor rács. Legyen először V_0 a Γ elemei által generált altér és $m := \dim V_0$. Mivel Γ generátorrendszer V_0-ban, ezért van olyan $u_1, \dots, u_m \in \Gamma$, ami bázis V_0-ban. Legyen $\Gamma_0 := \mathbb{Z}u_1 + \dots + \mathbb{Z}u_m \leq \Gamma$. Ekkor V_0/Γ_0 egy m-dimenziós tórusz, speciálisan kompakt. Ebben Γ/Γ_0 egy diszkrét részhalmaz, tehát véges. Ekkor viszont a $|\Gamma/\Gamma_0|$ egész számmal való szorzás Γ-t Γ_0 egy részcsoportjába képezi injektíven, tehát Γ is egy véges rangú szabad Abel csoport. □

3.4.3. Lemma. *Egy $\Gamma \subset V$ rács pontosan akkor teljes, ha van olyan $M \subset V$ korlátos részhalmaz, melyre $V = \bigcup_{\gamma\in\Gamma}(M + \gamma)$.*

Bizonyítás. Ha Γ teljes, akkor $M = \Phi$ jó lesz.

Visszafelé legyen M korlátos, melyre $V = \bigcup_{\gamma\in\Gamma}(M + \gamma)$, és legyen $V_0 := \mathbb{R}\Gamma$ a Γ által generált altér, továbbá $v \in V$ tetszőleges. Ekkor M tulajdonsága miatt minden $k \in \mathbb{N}$ számra van olyan $a_k \in M$ és $\gamma_k \in \Gamma$, melyre $kv = a_k + \gamma_k$. Ekkor

$$v = \lim_{k\to\infty} \frac{1}{k}(kv) = \lim_k \frac{a_k}{k} + \lim_k \frac{\gamma_k}{k} = \lim_k \frac{\gamma_k}{k} \in V_0$$

hiszen V_0 zárt és M korlátossága miatt $\lim_k \frac{a_k}{k} = 0$. □

Legyen mostantól Γ egy teljes rács. Ekkor a Φ paralelepipedon térfogata nem más, mint a $v_1, \dots, v_n$ oszlopvektorokból álló mátrix determinánsának abszolútértéke. Ezt nevezzük Γ térfogatának és $\mathrm{vol}(\Gamma)$-val jelöljük. Vegyük észre, hogy ez független a bázis (és így Φ) választásától, hiszen az áttérési mátrix egy másik bázisra $\mathrm{GL}_n(\mathbb{Z})$-ben van, tehát egységnyi determinánsú.

3.4.4. Tétel (Minkowski-féle rácspont-)**.** *Legyen $\Gamma \subset V$ egy teljes rács, X pedig egy konvex, origóra középpontosan szimmetrikus részhalmaz, melyre $\mathrm{vol}(X) > 2^n\mathrm{vol}(\Gamma)$. Ekkor az X-ben van az origón kívül is rácspont.*

Bizonyítás. Elég belátni, hogy van olyan $\gamma_1 \neq \gamma_2 \in \Gamma$, melyekre

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset \ .$$

Valóban, ha $x_1/2 + \gamma_1 = x_2/2 + \gamma_2$, akkor $\gamma := \gamma_1 - \gamma_2 = (x_2 - x_1)/2 \in X \cap \Gamma$. Tegyük fel tehát, hogy a $\frac{1}{2}X + \gamma$ ($\gamma \in \Gamma$) halmazok páronként diszjunktak. Ekkor

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma\in\Gamma} \mathrm{vol}(\Phi \cap (\frac{1}{2}X + \gamma)) = \sum_{\gamma\in\Gamma} \mathrm{vol}((\Phi - \gamma) \cap \frac{1}{2}X) =$$
$$= \mathrm{vol}\left(\bigcup_{\gamma\in\Gamma}(\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}(\frac{1}{2}X) = \frac{1}{2^n}\mathrm{vol}(X) \ ,$$

ami ellentmond a feltevésnek. □

3.5. Az osztályszám becslése

Legyen most $K/\mathbb{Q}$ egy véges, n-fokú bővítés. Ekkor a $\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ halmaz pontosan n elemű, hiszen $K/\mathbb{Q}$ szeparábilis, $\mathbb{C}$ pedig algebrailag zárt. Legyen $K_{\mathbb{C}} := \prod_{\sigma\in\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})}\mathbb{C}$ testek direkt szorzata (mint gyűrű). Tekintsük továbbá a

$$\begin{aligned} j\colon K &\to K_{\mathbb{C}} \\ \alpha &\mapsto (\sigma(\alpha))_\sigma = (\dots,\sigma(\alpha),\dots) \end{aligned}$$

gyűrűhomomorfizmust. Értelmezzük továbbá $K_{\mathbb{C}}$-n a $\langle x,y\rangle := \sum_\sigma x_\sigma\overline{y_\sigma}$ hermite-ikus bilineáris formát. Vegyük észre, hogy a kételemű csoport $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, F\}$ hat $K_{\mathbb{C}}$-n a következőképpen: $z\in K_{\mathbb{C}}$ esetén legyen Fz σ-hoz tartozó koordinátája $(Fz)_\sigma := \overline{z_{\overline{\sigma}}}$. Itt $\overline{\sigma}$ az a $K\to\mathbb{C}$ $\mathbb{Q}$-homomorfizmus, melyre $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ ha $\alpha\in K$. Ekkor nyilván

$$\langle Fx, Fy\rangle = \sum_\sigma \overline{x_{\overline{\sigma}}}y_{\overline{\sigma}} = \overline{\langle x,y\rangle} = \langle y,x\rangle\ . \tag{3.1}$$

A konjugálás segítségével értelmezhetjük $K_{\mathbb{C}}$ valós elemeit a következőképpen:

$$K_{\mathbb{R}} := \{z\in K_{\mathbb{C}} \mid Fz = z,\ \text{azaz } z_{\overline{\sigma}} = \overline{z_\sigma}\}\ .$$

Vegyük észre, hogy minden $\alpha\in K$-ra $F(j\alpha) = j\alpha$, tehát a j beágyazás valójában $K_{\mathbb{R}}$-be megy. Az is világos, hogy $K_{\mathbb{R}}$ egy részgyűrű $K_{\mathbb{C}}$-ben. Sőt, a (3.1) azonosság miatt a $\langle\cdot,\cdot\rangle$ megszorítása $K_{\mathbb{R}}$-re egy $K_{\mathbb{R}}\times K_{\mathbb{R}}\to\mathbb{R}$ skaláris szorzás a $K_{\mathbb{R}}$ $\mathbb{R}$ feletti vektortéren. Ez lesz a Minkowski-terünk, melyre az előző fejezet konvex geometriai tételét fogjuk alkalmazni. A térfogatot egyértelműen meghatározza a $\langle\cdot,\cdot\rangle$ skalárszorzás.

Legyen továbbá $\mathrm{Tr}\colon K_{\mathbb{C}}\to\mathbb{C}$ $\mathrm{Tr}(z) := \sum_\sigma z_\sigma$ a nyomfüggvény $K_{\mathbb{C}}$-n. Vegyük észre, hogy a $K/\mathbb{Q}$ bővítéshez tartozó relatív nyomfüggvény nem más, mint $\mathrm{Tr}_{K/\mathbb{Q}} = \mathrm{Tr}\circ j$. Sőt, a Tr $\mathbb{C}$-lineáris leképezést $K_{\mathbb{R}}$-re megszorítva egy $\mathrm{Tr}\colon K_{\mathbb{R}}\to\mathbb{R}$ $\mathbb{R}$-lineáris leképezést kapunk.

Jelöljük $\rho_1,\dots,\rho_r$-rel azon $\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$-beli elemeket, melyek értékkészlete valós. Jelöljük továbbá $\sigma_1,\overline{\sigma_1},\dots,\sigma_s,\overline{\sigma_s}$-sel azon konjugált párokat $\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$-ban, melyek értékkészlete nem valós. Ekkor nyilván $n = r+2s$ a bővítés foka. Ekkor nyilván

$$K_{\mathbb{R}} = \{(z_\tau)_\tau\in K_{\mathbb{C}} = \prod_\tau\mathbb{C} \mid z_{\rho_i}\in\mathbb{R}, z_{\overline{\sigma_j}} = \overline{z_{\sigma_j}}\ (i=1,\dots,r,\ j=1,\dots,s)\}\ .$$

3.5.1. Definíció. Azt mondjuk, hogy K *teljesen valós*, ha $s=0$. K teljesen képzetes, ha $r=0$.

A következőkben választani fogunk egy bázist $K_{\mathbb{R}}$-ben (azaz $K_{\mathbb{R}}$-et azonosítjuk $\mathbb{R}^{r+2s}$-nel), amiben kényelmesen számolni tudunk.

3.5.2. Lemma. *Az*

$$\begin{aligned} f\colon K_{\mathbb{R}} &\to \prod_\tau\mathbb{R} = \mathbb{R}^{r+2s} \\ (z_\tau) &\mapsto (x_\tau) \end{aligned}$$

leképezés egy vektortérizomorfizmus, ahol $x_{\rho_i} := z_{\rho_i}$ $(i = 1, \dots, r)$ *és* $x_{\sigma_j} = \Re(z_{\sigma_j})$, $x_{\overline{\sigma_j}} = \Im(z_{\sigma_j})$ $(j = 1, \dots, s)$. *Ez az izomorfizmus a* $\langle \cdot, \cdot \rangle$ *skalárszorzatot a*

$$(x, y) = \sum_{\tau} \alpha_\tau x_\tau y_\tau$$

skalárszorzatba viszi, ahol $\alpha_\tau = 1$ *ha* τ *valós, és* $\alpha_\tau = 2$, *ha* τ *komplex.*

Bizonyítás. Az izomorfizmus világos, mint ahogy $\alpha_{\rho_i} = 1$ $(i = 1, \dots, r)$ is. A fenti paraméterezéssel $f(z) = x$ és $f(z') = x'$ választással $z_\sigma = x_\sigma + x_{\overline{\sigma}} i$, $z_{\overline{\sigma}} = x_\sigma - x_{\overline{\sigma}} i$, $z'_\sigma = x'_\sigma + x'_{\overline{\sigma}} i$ és $z'_{\overline{\sigma}} = x'_\sigma - x'_{\overline{\sigma}} i$. Tehát

$$z_\sigma \overline{z'_\sigma} + z_{\overline{\sigma}} \overline{z'_{\overline{\sigma}}} = (x_\sigma + x_{\overline{\sigma}} i)(x'_\sigma - x'_{\overline{\sigma}} i) + (x_\sigma - x_{\overline{\sigma}} i)(x'_\sigma + x'_{\overline{\sigma}} i) = 2x_\sigma x'_\sigma + 2x_{\overline{\sigma}} x'_{\overline{\sigma}} \ .$$

□

Tehát az $(\cdot, \cdot)$ Minkowski-féle kanonikus metrika $\mathbb{R}^{r+2s}$-en eltér a szokásostól. Az általa meghatározott kanonikus térfogatra $\mathrm{vol}_{kan}(X) = (\sqrt{2})^{2s} \mathrm{vol}_{Leb}(f(X))$ teljesül, ahol vol_{Leb} a Lebesgue mérték $\mathbb{R}^{r+2s}$-en.

3.5.3. Állítás. *Legyen* $0 \neq A \lhd \mathcal{O}_K$ *egy ideál. Ekkor* $\Gamma := j(A)$ *egy teljes rács* $K_{\mathbb{R}}$*-ben, melynek térfogata* $\mathrm{vol}(\Gamma) = \sqrt{|d_K|} |\mathcal{O}_K : A|$.

Bizonyítás. Vegyünk egy $\mathbb{Z}$ fölötti $\alpha_1, \dots, \alpha_n$ bázist A-ban, valamint legyen $M = ((\tau_i \alpha_k))_{ik}$. Ekkor A diszkriminánsa

$$d(A) = d(\alpha_1, \dots, \alpha_n) = (\det M)^2 = |\mathcal{O}_K : A|^2 d_K \ .$$

Másrészt $\mathrm{vol}(\Gamma)$ nem más, mint a $j(\alpha_i) \in \mathbb{R}^{r+2s}$ $(i = 1, \dots, n)$ vektorok által kifeszített paralelepipedon térfogata a Minkowski-metrikában. Tehát ha Minkowski-metrika szerinti ortonormált bázisban felírjuk a $j(\alpha_i)$ oszlopvektorokat, akkor a kapott C mátrix determinánsának abszolútértéke a keresett térfogat. Tehát ha $N = (\langle j(\alpha_i), j(\alpha_k) \rangle)_{ik} = CC^T$ jelöli a Gram-mátrixot, akkor $\mathrm{vol}(\Gamma)^2 = \det(C)^2 = \det(N)$. Node $\langle j(\alpha_i), j(\alpha_k) \rangle = \sum_{l=1}^{n} \tau_l(\alpha_i) \overline{\tau_l(\alpha_k)}$, ami azt jelenti, hogy $N = M \overline{M}^T$, azaz $\mathrm{vol}(\Gamma) = |\det(M)|$. □

3.5.4. Tétel. *Legyen* $0 \neq A \lhd \mathcal{O}_K$ *egy tetszőleges ideál, és* $c_\tau > 0$ $(\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}))$ *valós számok, melyekre* $c_\tau = c_{\overline{\tau}}$ *és*

$$\prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})} c_\tau > \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} |\mathcal{O}_K : A| \ .$$

Ekkor van olyan $0 \neq \alpha \in A$, *melyre* $|\tau(\alpha)| < c_\tau$ *minden* $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$*-re.*

Bizonyítás. Vegyük az $X = \{ z \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau (\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})) \}$ konvex, origóra szimmetrikus halmazt. Ekkor a 3.5.2. Lemmában levő f átparaméterezéssel

$$f(X) = \{ x \in \prod_{\tau} \mathbb{R} \mid |x_{\rho_i}| < c_{\rho_i} \text{ és } x_{\sigma_j}^2 + x_{\overline{\sigma_j}}^2 < c_{\sigma_j}^2 \ (i = 1, \dots, r, \ j = 1, \dots, s) \} \ .$$

Ennek kanonikus térfogata

$$\mathrm{vol}(X) = 2^s \mathrm{vol}_{Leb}(f(X)) = 2^s \prod_{i=1}^{r} (2c_{\rho_i}) \prod_{j=1}^{s} (\pi c_{\sigma_j}^2) = 2^{r+s} \pi^s \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})} c_\tau > 2^n \mathrm{vol}(\Gamma) \ .$$

A tétel következik a Minkowski-féle rácsponttételből (3.4.4). □

3.5.5. Definíció. Az $\mathfrak{N}(A) := |\mathcal{O}_K : A| \in \mathbb{N}$ számot az A ideál abszolút normájának nevezzük.

Vegyük észre, hogy ha $A = (\alpha)$ egy főideál, akkor $\mathfrak{N}((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$. Valóban, legyen $\omega_1, \ldots, \omega_n$ egész bázis $\mathcal{O}_K$-ban, ekkor $\alpha\omega_1, \ldots, \alpha\omega_n$ pedig egész bázis (α)-ban. Az áttérési mátrix pedig nem más, mint az α-val való szorzás mátrixa. Az állítás következik a 3.2.11. Lemmából és az $N_{K/\mathbb{Q}}$ norma definíciójából.

3.5.6. Állítás. *Legyen $A = P_1^{\nu_1} \ldots P_t^{\nu_t}$ a prímfelbontása az $A \neq 0$ ideálnak. Ekkor $\mathfrak{N}(A) = \prod_{i=1}^t \mathfrak{N}(P_i)^{\nu_i}$. Speciálisan az abszolút norma multiplikatív.*

Bizonyítás. A kínai maradéktétel szerint $\mathcal{O}_K/A = \bigoplus_{i=1}^t \mathcal{O}/P_i^{\nu_i}$. Tehát az állítást elég prímhatványokra belátni. Ha pedig P egy prímideál, akkor az egyértelmű prímfelbontás miatt van ideáloknak egy lánca:

$$\mathcal{O}_K \supsetneq P \supsetneq P^2 \supsetneq \cdots \supsetneq P^\nu \ .$$

Itt a P^i/P^{i+1} részfaktorok mind 1-dimenziós vektorterek $\mathcal{O}_K/P$ fölött. Valóban, ha veszünk egy tetszőleges $\alpha \in P^i \setminus P^{i+1}$ elemet, akkor $P^i \supseteq P^{i+1} + (\alpha) \supsetneq P^{i+1}$. Ezt megszorozva P^{-i}-vel azt kapjuk, hogy $\mathcal{O}_K \supseteq (P^{i+1} + (\alpha))P^{-i} \supsetneq P$. Node P maximális ideál, tehát $P^i = P^{i+1} + (\alpha)$, azaz $\alpha + P^{i+1}$ generálja a P^i/P^{i+1} vektorteret. Viszont minden 1-dimenziós vektortérnek ugyanannyi eleme van, mint az alaptestnek, ezért $|\mathcal{O}_K : A| = |\mathcal{O}_K : P|^\nu$. □

3.5.7. Következmény. *Az abszolút norma kiterjed a törtideálokra egy $\mathfrak{N}\colon J_K \to \mathbb{Q}^\times$ homomorfizmussá.*

3.5.8. Lemma. *Minden $0 \neq A \lhd \mathcal{O}_K$ ideálban van olyan $0 \neq \alpha \in A$ elem, melyre*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(A) \ .$$

Bizonyítás. Legyen $\varepsilon > 0$ tetszőleges rögzített, és válasszunk olyan $0 < c_\tau = c_{\overline{\tau}}$ számokat úgy, hogy

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(A) + \varepsilon \ .$$

Ekkor a 3.5.4. Tétel szerint van olyan $\alpha \in A$, melyre $|\tau(\alpha)| < c_\tau$ minden $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$-re. Az állítás következik abból az észrevételből, hogy $N_{K/\mathbb{Q}}(\alpha) = \prod_\tau \tau(\alpha)$, ha ε-nal tartunk 0-hoz. □

Elérkeztünk ebben a fejezetben a főtételünkhöz:

3.5.9. Tétel. *Ha $K/\mathbb{Q}$ egy véges bővítés, akkor a Cl_K osztálycsoport véges.*

Bizonyítás. Az első lépésben belátjuk, hogy adott $M > 0$ valós számra csak véges sok A ideál van $\mathcal{O}_K$-ban, melynek abszolút normájára $\mathfrak{N}(A) \leq M$. Mivel minden ideál előáll prímideálok szorzataként, és a norma egy 1-nél nagyobb egész szám, ezért elég belátni az állítást prímideálokra. Viszont ha P egy prímideál melyre $\mathfrak{N}(P) \leq M$, akkor $\mathcal{O}_K/P$ egy véges test, melynek karakterisztikája egy $0 < p$ prímszám. Viszont ekkor $(p) \subseteq P$ és $p \leq |\mathcal{O}_K/P| = \mathfrak{N}(P) \leq M$. Node fix M-re véges sok M-nél kisebb prímszám van, és rögzített p prím is csak véges sok P prímideálban lehet benne: azokban, melyek szerepelnek (p) prímtényezős felbontásában.

A második lépésben azt látjuk be, hogy ha $A \lhd \mathcal{O}_K$ egy tetszőleges ideál, akkor van olyan A_1 ideál $\mathcal{O}_K$-ban, melynek osztálya $[A_1] = [A] \in Cl_K$ és

$$\mathfrak{N}(A_1) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} =: M \ .$$

Először is alkalmas $\gamma \in \mathcal{O}_K$ elemmel a $B := \gamma A^{-1}$ törtideál egy egész ideál (azaz $\subseteq \mathcal{O}_K$). A 3.5.8. Lemma miatt van olyan $\alpha \in B$ elem, melyre $|N_{K/\mathbb{Q}}(\alpha)| \leq M\mathfrak{N}(B)$. Ez viszont azt jelenti, hogy az $A_1 = \alpha B^{-1} = \alpha\gamma^{-1}A$ választással $\mathfrak{N}(A_1) \leq M$ és $[A_1] = [A]$, hiszen hányadosuk az $(\alpha\gamma^{-1})$ főideál. Be kell még látnunk, hogy A_1 egy egészideál. Ez viszont világos, hiszen $(\alpha) \subseteq B$ miatt $\alpha B^{-1} \subseteq \mathcal{O}_K$.

A két lépésből nyilvánvalóan következik az állítás, hiszen ha végtelen sok ideálosztály lenne, akkor végtelen sok ideál lenne M-nél kisebb normával. □

3.5.10. Definíció. $h_K := |Cl_K|$ a K test *osztályszáma.*

A Minkowski-elmélet egy másik fontos következménye a következő

3.5.11. Tétel. *Legyen* $|K/\mathbb{Q}| = n$. *Ekkor* $|d_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}$. *Speciálisan* $|d_K| \to \infty$ *ha* $n \to \infty$ *és* $n > 1$ *esetén* $|d_K| > 1$.

Bizonyítás. Vegyünk egy $\varepsilon > 0$ valós számot és legyen $t = \sqrt[n]{n!\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} + \varepsilon}$. Tekintsük továbbá $K_{\mathbb{R}}$-ben az

$$X_t := \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid \sum_\tau |z_\tau| < t\}$$

centrálszimmetrikus konvex tartományt.

3.5.12. Lemma. *Az* X_t *tartomány térfogata* $\mathrm{vol}(X_t) = 2^r\pi^s\frac{t^n}{n!}$.

Bizonyítás. A 3.5.2. Lemma szerint paraméterezzük át $K_{\mathbb{R}}$-et. Ekkor

$$f(X_t) = \{x_\tau \in \prod_\tau \mathbb{R} \mid \sum_\rho |x_\rho| + \sum_\sigma 2\sqrt{x_\sigma^2 + x_{\overline{\sigma}}^2} < t\}$$

és $\mathrm{vol}(X_t) = 2^s\mathrm{vol}_{Leb}(f(X_t))$. (A kettes szorzó $\sum_\sigma 2\sqrt{x_\sigma^2 + x_{\overline{\sigma}}^2}$-ben onnan jön, hogy $|z_\sigma| = |z_{\overline{\sigma}}| = \sqrt{x_\sigma^2 + x_{\overline{\sigma}}^2}$.) A fenti térfogat kiszámolható úgy, ha a σ-típusú koordinátákban áttérünk polárkoordinátákra, és r és s szerinti indukciót alkalmazunk. A részletek kidolgozását az olvasóra hagyjuk. □

Legyen továbbá $\Gamma := j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ rács. Ekkor a 3.5.3. Állítás szerint $\mathrm{vol}(\Gamma) = \sqrt{|d_K|}$, ezért t választása és a Lemma miatt $\mathrm{vol}(X_t) > 2^n\mathrm{vol}(\Gamma)$. Így a 3.4.4. Tétel miatt X_t-ben van az origótól különböző rácspont, azaz van olyan $0 \neq \alpha \in \mathcal{O}_K$, melyre $\sum_\tau |\tau(\alpha)| < t$. Viszont a számtani-mértani közép közti egyenlőtlenség szerint ekkor

$$1 \leq |N_{K/\mathbb{Q}(\alpha)}| = \prod_\tau |\tau(\alpha)| \leq \frac{t^n}{n^n} = \frac{n!\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} + \varepsilon}{n^n} \ .$$

Az állítás adódik $\varepsilon \to 0$-val, hiszen $s \leq \frac{n}{2}$. □

A fenti tétel segítségével effektív becslést is adhatunk az osztályszámra. Ennek illusztrálásaképpen legyen $\mathcal{O}$ a $\mathbb{Q}(\sqrt{-11})$ egészeinek gyűrűje. Belátjuk, hogy $\mathcal{O}$ főideálgyűrű. A 3.5.9. Tétel bizonyításában láttuk, hogy az osztálycsoport minden eleme reprezentálható egy olyan $\mathcal{O}$-beli I ideállal, melynek abszolútnormája $\mathfrak{N}(I) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Mivel K nem valós, ezért $s = 1$, és mivel $-11 \equiv 1 \pmod 4$, ezért $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, speciálisan diszkriminánsa -11. Tehát minden ideálosztályban van egy olyan I ideál, melynek normája $\leq \frac{2\sqrt{11}}{\pi} < 3$. Viszont $\mathcal{O}$-ban egyáltalán nincs 2 normájú ideál: Tegyük fel ugyanis, hogy $\mathcal{O}/I \cong \mathbb{F}_2$. Ekkor $2 \in I$. Viszont $\mathcal{O}/(2) \cong \mathbb{F}_2[x]/(x^2+x+3) \cong \mathbb{F}_4$, hiszen $\frac{1+\sqrt{-11}}{2}$ minimálpolinomja x^2+x+3, ami modulo 2 irreducibilis. Tehát (2) egy maximális ideál $\mathcal{O}$-ban, speciálisan $\mathcal{O}$-ban nincs 2-indexű ideál. Így $\mathcal{O}$ osztálycsoportjának csak 1 eleme lehet, így a 3.3.12. Állítás miatt főideálgyűrű.

3.6. Multiplikatív Minkowski-elmélet, az egységcsoport

A Cl_K osztálycsoport végessége után rátérünk a Minkowski-elmélet másik alkalmazására: belátjuk Dirichlet tételét a K-beli algebrai egészek egységeiről. Ehhez szükségünk lesz a Minkowski-elmélet multiplikatív verziójára, melyet a továbbiakban felépítünk.

A $j\colon K \hookrightarrow K_{\mathbb{C}}$ gyűrűhomomorfizmus indukál egy $j\colon K^\times \to K_{\mathbb{C}}^\times$ leképezést a multiplikatív csoportokon is. Továbbá tekintsük a

$$\begin{aligned} N\colon K_{\mathbb{C}}^\times &\to \mathbb{C}^\times \\ (z_\tau)_\tau &\mapsto \prod_\tau z_\tau \end{aligned}$$

homomorfizmust. Nyilván $N \circ j = N_{K/\mathbb{Q}}$. Legyen továbbá

$$\begin{aligned} \ell = \log|\cdot|\colon K_{\mathbb{C}}^\times &\to \prod_\tau \mathbb{R} \\ (z_\tau)_\tau &\mapsto (\log|z_\tau|)_\tau\ . \end{aligned}$$

Mivel a logaritmus szorzatot összegbe visz, ezért kapunk egy

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{C}}^\times & \xrightarrow{\ell} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{C}^\times & \xrightarrow{\log|\cdot|} & \mathbb{R} \end{array} \tag{3.2}$$

kommutatív diagramot. A (3.2) diagramban minden csoporton hat a komplex konjugálás (azaz $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$) – a hatást $K^\times$-en és $\mathbb{Q}^\times$-en triviálisnak értelmezzük, $K_{\mathbb{C}}$-n a hatást már megadtuk az előző fejezetben, $\prod_\tau \mathbb{R}$-en pedig $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ csak a $\tau\colon K \to \mathbb{C}$ $\mathbb{Q}$-homomorfizmusok permutálja. Azt is könnyű látni, hogy a (3.2) diagramban minden leképezés $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-ekvivariáns, azaz a leképezések felcserélhetők a komplex konjugálással. Tehát ha $[\prod_\tau \mathbb{R}]^+$-szal jelöljük a komplex konjugálás fixpontjainak halmazát $\prod_\tau \mathbb{R}$-en, akkor az alábbi kommutatív diagramot kapjuk:

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{\ell} & [\prod_\tau \mathbb{R}]^+ \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \xrightarrow{\log|\cdot|} & \mathbb{R} \end{array} \tag{3.3}$$

Ha $\rho_1, \dots, \rho_r$-rel jelöljük a valós τ-kat, $\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s}$-tal pedig a komplex konjugált párokat, akkor $[\prod_\tau \mathbb{R}]^+$-t jellemezhetjük a következőképpen:

$$[\prod_\tau \mathbb{R}]^+ = \prod_\rho \mathbb{R} \times \prod_\sigma [\mathbb{R} \times \mathbb{R}]^+ \ ,$$

ahol $[\mathbb{R} \times \mathbb{R}]^+ = \{(x, x) \in \mathbb{R} \times \mathbb{R}\}$. Továbbá $[\mathbb{R} \times \mathbb{R}]^+$-t azonosíthatjuk $\mathbb{R}$-rel is az $(x, x) \mapsto 2x$ leképezésen keresztül, ami egy $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$ azonosítást eredményez. Ennél az azonosításnál és a $K_\mathbb{R} \xrightarrow{f} \mathbb{R}^{r+2s}$ azonosítással az $\ell\colon K_\mathbb{R}^\times \to [\prod_\tau \mathbb{R}]^+$ leképezés

$$\ell(x) = (\log|x_{\rho_1}|, \dots, \log|x_{\rho_r}|, \log|x_{\sigma_1}|^2, \dots, \log|x_{\sigma_s}|^2)$$

alakba írható.

Vegyük észre, hogy ha $\varepsilon \in \mathcal{O}_K^\times$, akkor $N_{K/\mathbb{Q}}(\varepsilon) = \pm 1$. Speciálisan $\ell \circ j(\varepsilon)$ benne van $\mathrm{Tr}\colon [\prod_\tau \mathbb{R}]^+ \to \mathbb{R}$ magjában. Jelölje $H = \mathrm{Ker}(\mathrm{Tr})$ ezt a magot. Ez egy $r + s - 1$-dimenziós hipersík $[\prod_\tau \mathbb{R}]^+$-ban. Jelölje továbbá $S \leq K_\mathbb{R}^\times$ a ± 1 normájú elemek részcsoportját, azaz $S = \ell^{-1}(H)$.

A továbbiakban a célunk az lesz, hogy belássuk, hogy $\Gamma := \ell(j(\mathcal{O}_K^\times))$ egy teljes rács H-ban, továbbá $\ell \circ j$ magja pontosan a $\mathcal{O}_K^\times$-beli véges rendű elemekből áll. Speciálisan $\mathcal{O}_K^\times$ egy $\dim H = r + s - 1$-rangú Abel-csoport. Jelöljük $\mu(K)$-val a K-ban levő egységgyökök csoportját. Ezek mind algebrai egészek, hiszen gyökei az $x^k - 1 \in \mathbb{Z}[x]$ polinomnak alkalmas k pozitív egész számmal.

3.6.1. Lemma. *Az* $1 \to \mu(K) \to \mathcal{O}_K^\times \xrightarrow{\ell \circ j} \Gamma \to 0$ *sorozat egzakt.*

Bizonyítás. Azt kell belátnunk, hogy $\mathrm{Ker}(\ell \circ j) = \mu(K)$. A $\mu(K) \subseteq \mathrm{Ker}(\ell \circ j)$ tartalmazás világos, hiszen ha $\varepsilon \in \mu(K)$ egy egységgyök, akkor $|\tau(\varepsilon)| = 1$, azaz $\ell(j(\varepsilon))_\tau = \log|\tau(\varepsilon)| = 0$ minden $\tau \in \mathrm{Hom}_\mathbb{Q}(K, \mathbb{C})$-re, azaz $\varepsilon \in \mathrm{Ker}(\ell \circ j)$.

Visszafelé, ha $\alpha \in \mathcal{O}_K^\times$ benne van $\ell \circ j$ magjában, akkor $|\tau(\alpha)| = 1$ minden $\tau \in \mathrm{Hom}_\mathbb{Q}(K, \mathbb{C})$. De ekkor $|\tau(\alpha^k)| = 1$ minden $k \geq 1$ egészre. Speciálisan a $j(\alpha^k)$ benne van $K_\mathbb{R}$ egy korlátos tartományában. De mivel $j(\mathcal{O}_K) \subset K_\mathbb{R}$ diszkrét, ezért $j(\alpha)$ hatványai egy véges halmazt alkotnak, speciálisan α egy egységgyök. □

3.6.2. Állítás. *A* $\Gamma \subset H$ *egy teljes rács* H*-ban. Speciálisan* $\Gamma \cong \mathbb{Z}^{r+s-1}$.

Bizonyítás. Először belátjuk, hogy Γ egy rács, azaz egy diszkrét részcsoport H-ban. Azt kell belátni, hogy minden $c > 0$ valós számra az $X_c = \{(x_\tau)_\tau \in \prod_\tau \mathbb{R} \mid |x_\tau| < c \text{ minden } \tau \in \in \mathrm{Hom}_\mathbb{Q}(K, \mathbb{C})\}$ korlátos tartomány metszete Γ-val véges. Node $\ell(j(\alpha)) \in X_c$ azt jelenti, hogy $|\log|\tau(\alpha)|| < c$, azaz $e^{-c} < |\tau(\alpha)| < e^c$. De ez egy korlátos tartomány $K_\mathbb{R}$-ben, ezért véges sok pontot tartalmazhat a $j(\mathcal{O}_K)$ rácsból.

A teljességhez konstruálnunk kell egy olyan $M \subset H$ korlátos halmazt, melynek Γ elemeivel való eltoltjai lefedik H-t. Először válasszunk minden $\tau \in \mathrm{Hom}_\mathbb{Q}(K, \mathbb{C})$-re egy-egy $c_\tau > 0$ valós számot úgy, hogy $c_\tau = c_{\overline{\tau}}$ és $C := \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Tekintsük az

$$X = \{(z_\tau)_\tau \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$$

részhalmazt $K_\mathbb{R}$-ben. A 3.5.9. Tétel bizonyításához hasonlóan asszociáltság erejéig véges sok olyan $\alpha \in \mathcal{O}_K$ elem van, melynek normája $|N_{K/\mathbb{Q}}(\alpha)| < C$, hiszen ideálból is véges sok van,

aminek a normája kisebb, mint C. Legyenek ezek az elemek $\alpha_1, \dots, \alpha_m$ és legyen

$$M = \ell(T) = \ell\left(S \cap (\bigcup_{i=1}^{m} Xj(\alpha_i)^{-1})\right) .$$

Belátjuk, hogy M teljesíti a kívánt feltételeket. Egyrészt mivel X korlátos, ezért véges sok eltoltjának uniója is az, ezért M is korlátos. Másrészt legyen $y = (y_\tau)_\tau \in S$ tetszőleges ($y \in S$ azt jelenti, hogy $\prod y_\tau = \pm 1$). Ekkor

$$Xy^{-1} = \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid |z_\tau y_\tau| < c_\tau\} = \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau |y_\tau^{-1}|\} .$$

Mivel $\prod_\tau c_\tau |y_\tau^{-1}| = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$, ezért az 3.5.8. Lemma miatt van olyan $\alpha \in \mathcal{O}_K$, melyre $j(\alpha) \in Xy^{-1}$. Speciálisan $|N_{K/\mathbb{Q}}(\alpha)| < C$, tehát van olyan $i \in \{1, \dots, m\}$, melyre α és α_i asszociáltak, azaz $\varepsilon := \alpha_i \alpha^{-1} \in \mathcal{O}_K^\times$. Ez viszont azt jelenti, hogy $\alpha \in Xy^{-1}$ miatt $y \in Xj(\alpha)^{-1} = Xj(\alpha_i^{-1})j(\varepsilon)$. Speciálisan $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} Tj(\varepsilon)$, ezért $H = \ell(S) = \bigcup_{\gamma \in \Gamma}(M + \gamma)$. □

A fenti állítás közvetlen következménye az alábbi

3.6.3. Tétel. *Az $\mathcal{O}_K^\times$ egységcsoport a $\mu(K)$ véges csoport és $\mathbb{Z}^{r+s-1}$ direkt szorzatával izomorf.*

3.7. Dedekind gyűrűk és a lokalizálás

Legyen R egy egységelemes integritási tartomány, $0 \notin S \subseteq R$ pedig egy multiplikatívan zárt halmaz, azaz $1 \in S$ és $s_1, s_2 \in S$ esetén $s_1 s_2 \in S$. Ekkor az R gyűrű S-szerinti hányadosgyűrűjének nevezzük az

$$RS^{-1} = (R \times S)/\sim$$

faktorhalmazt, ahol $\sim$ a következő ekvivalenciarelációt jelöli: $(a, s) \sim (b, t)$ akkor és csak akkor, ha $at = bs$. Ez valóban egy ekvivalenciareláció: a reflexivitás és a szimmetria nyilvánvaló, a tranzitivitáshoz pedig legyen $(a, s) \sim (b, t)$ és $(b, t) \sim (c, u)$. Ekkor $atu = bsu = bus = cts$, de mivel R nullosztómentes $au = cs$, azaz $(a, s) \sim (c, u)$. Mostantól jelöljük az (a, s) pár ekvivalenciosztályát RS^{-1}-ben $\frac{a}{s}$-sel és értelmezzük RS^{-1}-en a következő műveleteket:

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &:= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &:= \frac{ab}{st} . \end{aligned}$$

Könnyű számolás mutatja (lsd. pl. $S = R \setminus \{0\}$ esetben az 5.7.2. tétel bizonyítását [7]-ben), hogy ezek a műveletek jóldefiniáltak és RS^{-1} egy integritási tartomány ezekkel a műveletekkel. Továbbá R izomorf RS^{-1} egy részgyűrűjével, mégpedig az $\frac{a}{1}$ alakú törtek részgyűrűjével.

3.7.1. Állítás. *Az*

$$\begin{aligned} RS^{-1} \rhd P &\mapsto P \cap R \lhd R \\ RS^{-1} \rhd QS^{-1} &\leftarrow\!\shortmid Q \lhd R \end{aligned}$$

leképezések kölcsönösen egyértelmű megfeleltetést létesítenek RS^{-1} prímideáljai és R azon Q prímideáljai között, melyekre $Q \cap S = \emptyset$.

Bizonyítás. Mivel R részgyűrű RS^{-1}-ben, ezért ezek a leképezések ideálokhoz ideált rendelnek. Másrészt ha $P \lhd RS^{-1}$ és $Q \lhd R$ prímek, akkor

$$\begin{aligned} P \cap R &= \{a \in R \mid \frac{a}{s} \in P \text{ minden } s \in S\text{-re}\} ; \\ QS^{-1} &= \{\frac{a}{s} \in RS^{-1} \mid a \in Q\} . \end{aligned}$$

A $(P \cap R)S^{-1} = P$ egyenlőség és a $QS^{-1} \cap R \supseteq Q$ tartalmazás világos, ezekhez nem is kell, hogy P, illetve Q prím legyen. Ugyanakkor ha $\frac{a}{s} = r \in R$ úgy, hogy $a \in Q$ és $s \in S$, akkor $sr = a \in Q$, $s \notin Q$ miatt $r \in Q$, hiszen Q prímideál. Továbbá ha $r_1, r_2 \in R$ melyekre $r_1 r_2 \in$ $\in P \cap R$, akkor r_1 és r_2 közül valamelyik P-ben van, de ha pl. $r_1 \in P$, akkor $r_1 \in P \cap R$. Visszafelé legyen $\frac{a}{s}, \frac{b}{t} \in RS^{-1}$ melyekre $\frac{ab}{st} \in QS^{-1}$. Ekkor van olyan $\alpha \in Q$ és $u \in S$, melyre $\frac{ab}{st} = \frac{\alpha}{u}$, azaz $abu = \alpha st \in Q$. De mivel $u \in S$, ezért $u \notin Q$, ezért $ab \in Q$, tehát legalább az egyik a és b közül Q-ban van, hiszen Q prím. □

A legfontosabb példánk az, amikor $S = R \setminus \mathfrak{p}$ egy $\mathfrak{p}$ prímideál komplementere. Ebben az esetben az RS^{-1} gyűrűt $R_\mathfrak{p}$-vel jelöljük, és az R $\mathfrak{p}$-szerinti lokalizáltjának nevezzük.

3.7.2. Állítás. *$R_\mathfrak{p}$ egy* lokális gyűrű*, azaz egyetlen maximális ideálja van, mégpedig $\mathfrak{p}R_\mathfrak{p}$.*

Bizonyítás. Valóban, $\mathfrak{p}R_\mathfrak{p}$ egy ideál $R_\mathfrak{p}$-ben és minden $\frac{a}{s}$ elem, ami nincs benne $\mathfrak{p}R_\mathfrak{p}$-ben invertálható, hiszen $a \notin \mathfrak{p}$ miatt $a \in S$, azaz $\frac{s}{a}$ is egy elem $R_\mathfrak{p}$-ben, ami $\frac{a}{s}$ reciproka. Tehát minden valódi ideálja $R_\mathfrak{p}$-nek benne van $\mathfrak{p}R_\mathfrak{p}$-ben, hiszen egyébként tartalmazna egy invertálható elemet. Speciálisan $\mathfrak{p}R_\mathfrak{p}$ az egyetlen maximális ideál. □

Jelöljük $\mathfrak{m}_\mathfrak{p}$-vel a $\mathfrak{p}R_\mathfrak{p}$ maximális ideált. Ekkor van egy természetes injektív gyűrűhomomorfizmus $R/\mathfrak{p}$-ből $R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$-be. Továbbá az is látszik, hogy $R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ minden eleme előáll $R/\mathfrak{p}$-beli elemek hányadosaként, azaz $R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ nem más, mint $R/\mathfrak{p}$ hányadosteste. Speciálisan ha $\mathfrak{p}$ egy maximális ideál R-ben, akkor $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$. Sőt, igaz az alábbi

3.7.3. Állítás. *Ha $\mathfrak{p}$ egy maximális ideál R-ben, akkor $R/\mathfrak{p}^n \cong R_\mathfrak{p}/{\mathfrak{m}_\mathfrak{p}}^n$ minden $n \geq 1$-re.*

Bizonyítás. Legyen

$$\begin{aligned} f\colon R/\mathfrak{p}^n &\to R_\mathfrak{p}/{\mathfrak{m}_\mathfrak{p}}^n \\ a \mod \mathfrak{p}^n &\mapsto \frac{a}{1} \mod {\mathfrak{m}_\mathfrak{p}}^n \end{aligned}$$

gyűrűhomomorfizmus. Az f injektivitása világos. A szürjektivitáshoz vegyünk egy $\frac{a}{s} + {\mathfrak{m}_\mathfrak{p}}^n \in$ $\in R_\mathfrak{p}/{\mathfrak{m}_\mathfrak{p}}^n$ elemet. Mivel $s \in R \setminus \mathfrak{p}$, ezért $\mathfrak{p}^n + sR = R$, hiszen $\mathfrak{p}^n$-ent csak a $\mathfrak{p}$ maximális ideál tartalmazza, viszont $s \notin \mathfrak{p}$. Tehát $s + \mathfrak{p}^n$ invertálható $R/\mathfrak{p}^n$-ben, így inverzének a-szorosa épp $\frac{a}{s} + {\mathfrak{m}_\mathfrak{p}}^n$-re képződik. □

3.7.4. Definíció. Azt mondjuk, hogy az $\mathcal{O}$ integritási tartomány egy *diszkrét értékelésgyűrű* (DVR), ha lokális főideálgyűrű. Speciálisan a $\mathfrak{p} \lhd \mathcal{O}$ maximális ideált is egyetlen π elem generálja.

Vegyük észre, hogy mivel $\mathcal{O}$ főideálgyűrű, ezért igaz benne a számelmélet alaptétele. Viszont csak egyetlen prímelemünk van: π, azaz minden $a \neq 0$ elem egyértelműen írható $a = \varepsilon\pi^n$ alakban, ahol $\varepsilon \in \mathcal{O}^\times$ egy egység és $n \geq 0$ egész.

3.7.5. Definíció. Ha $a = \varepsilon\pi^n$, akkor a $v_\pi(a) := n$ számot az a (π-adikus) értékelésének hívjuk.

Ekkor nyilván $(a) = \mathfrak{p}^{v_\pi(a)}$. Az értékelés nyilván kiterjed $\mathcal{O}$-ról a K hányadostestre is egy $v_\pi\colon K^\times \to \mathbb{Z}$ csoporthomomorfizmussá. Továbbá legyen $v_\pi(0) := \infty$. Ekkor nyilván $v_\pi(a + b) \geq \min(v_\pi(a), v_\pi(b))$.

A továbbiakban a célunk a következő tétel bizonyítása lesz:

3.7.6. Tétel. *Egy $\mathcal{O}$ noether-féle integritási tartomány pontosan akkor Dedekind gyűrű, ha minden $0 \neq \mathfrak{p} \lhd \mathcal{O}$ prímideálra $\mathcal{O}_\mathfrak{p}$ egy diszkrét értékelésgyűrű.*

A bizonyítás előkészítéséhez szükségünk van a következő – önmagában is érdekes – állításra:

3.7.7. Állítás. *Ha $0 \notin S$ egy multiplikatívan zárt halmaz az $\mathcal{O}$ Dedekind gyűrűben, akkor az $\mathcal{O}S^{-1}$ hányadosgyűrű is Dedekind.*

Bizonyítás. A 3.7.1. Állítás miatt $\mathcal{O}S^{-1}$ minden prímideálja maximális. Másrészt ha $I \lhd \lhd \mathcal{O}S^{-1}$ egy ideál, akkor $I = (I \cap \mathcal{O})S^{-1}$, azaz I-t is generálják $I \cap \mathcal{O}$ generátorelemei, azaz I végesen generált, tehát $\mathcal{O}S^{-1}$ noether. Végül legyen $\alpha \in K$ egész elem $\mathcal{O}S^{-1}$ fölött, ahol K a hányadostest. Ekkor van olyan $\frac{a_0}{s_0}, \ldots, \frac{a_{n-1}}{s_{n-1}} \in \mathcal{O}S^{-1}$, melyekre

$$\alpha^n + \frac{a_{n-1}}{s_{n-1}}\alpha^{n-1} + \cdots + \frac{a_0}{s_0} = 0\ .$$

A fenti egyenletet $(s_0 \ldots s_{n-1})^n$-nel beszorozva azt kapjuk, hogy $s_0 \ldots s_{n-1}\alpha$ egész $\mathcal{O}$ felett, de mivel $\mathcal{O}$ egészre zárt, ezért $\mathcal{O}$-ban van. Ez viszont azt jelenti, hogy $\alpha \in \mathcal{O}S^{-1}$. □

Ha $\mathcal{O}$ egy integritási tartomány, akkor jelöljük $\mathrm{Spec}(\mathcal{O})$-val $\mathcal{O}$ prímideáljainak halmazát.

3.7.8. Lemma. *Ha $\mathcal{O}$ egy tetszőleges integritási tartomány, akkor $\mathcal{O} = \bigcap_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O})} \mathcal{O}_\mathfrak{p}$.*

Bizonyítás. A $\mathcal{O} \subseteq \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p}$ tartalmazás világos. A másik irányhoz legyen $\alpha \in \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p} \setminus \mathcal{O}$ tetszőleges és $A := \{\beta \in \mathcal{O} \mid \alpha\beta \in \mathcal{O}\}$. Ekkor $1 \notin A \lhd \mathcal{O}$. Tehát A benne van egy $\mathfrak{p}$ maximális ideálban. Node a feltevés szerint $\alpha \in \mathcal{O}_\mathfrak{p}$. Tehát $\alpha = \frac{a}{s}$ alakba írható, ahol $a \in \mathcal{O}$ és $s \in \mathcal{O} \setminus \mathfrak{p}$. Viszont ez azt jelenti, hogy $s\alpha \in \mathcal{O}$, azaz $s \in A \subseteq \mathfrak{p}$, ami ellentmondás. □

3.7.6. Tétel bizonyítása. Először legyen $\mathcal{O}$ egy Dedekind gyűrű és $\mathfrak{p} \lhd \mathcal{O}$ egy prímideál. A 3.7.7. Állítás miatt $\mathcal{O}_\mathfrak{p}$ is Dedekind gyűrű. Tehát minden ideálja az $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ ideálnak egy hatványa. Vegyünk egy tetszőleges $\pi \in \mathfrak{m}_\mathfrak{p} \setminus {\mathfrak{m}_\mathfrak{p}}^2$ elemet. Ekkor $(\pi) = {\mathfrak{m}_\mathfrak{p}}^k$ valamilyen $k \geq 1$-re, de $(\pi) \not\subset {\mathfrak{m}_\mathfrak{p}}^2$, ezért $(\pi) = \mathfrak{m}_\mathfrak{p}$ főideál. Viszont ekkor $\mathfrak{m}_\mathfrak{p}$ minden hatványa is főideál, ezért $\mathcal{O}_\mathfrak{p}$ főideálgyűrű.

Megfordítva tegyük fel, hogy $\mathcal{O}$ egy noethergyűrű és tetszőleges $\mathfrak{p} \lhd \mathcal{O}$ prímideálra $\mathcal{O}_\mathfrak{p}$ egy diszkrét értékelésgyűrű. Tegyük fel továbbá, hogy van olyan $0 \neq \mathfrak{p}$ prímideál, ami nem maximális, tehát benne van egy $\mathfrak{p}_2$ maximális ideálban. De ekkor $\mathcal{O}_{\mathfrak{p}_2}$ is diszkrét értékelésgyűrű, speciálisan $\mathfrak{p}\mathcal{O}_{\mathfrak{p}_2}$ egy pozitív egész kitevős hatványa $\mathfrak{p}_2\mathcal{O}_{\mathfrak{p}_2}$-nek, ami ellentmondás, hiszen ez egy $\mathfrak{p}_2\mathcal{O}_{\mathfrak{p}_2}$-től különböző prímideál a 3.7.1. Állítás miatt. Tehát $\mathcal{O}$-ban minden nemnulla prímideál maximális.

Azt kell még belátnunk, hogy $\mathcal{O}$ egészre zárt. Legyen $\alpha \in K$ egy egész elem a hányadostestben. Mivel $\mathcal{O}_\mathfrak{p}$ főideálgyűrű (speciálisan egészre zárt) minden $0 \neq \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$-ra, ezért $\alpha \in \mathcal{O}_\mathfrak{p}$ minden $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$-ra, azaz $\alpha \in \mathcal{O} = \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p}$ a 3.7.8. Lemma miatt. Tehát $\mathcal{O}$ egészre zárt. □

3.7.9. Lemma. *Legyen $\mathcal{O}$ egy Dedekind gyűrű és $A = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r}$ egy törtideál. Ekkor A prímtényezős felbontásában a kitevők leolvashatók „lokálisan": $A\mathcal{O}_{\mathfrak{p}_i} = (\mathfrak{p}_i\mathcal{O}_{\mathfrak{p}_i})^{n_i}$ minden $i = 1, \dots, r$-re, sőt, ha $\mathfrak{p} \neq \mathfrak{p}_i$ semmilyen $i = 1, \dots, r$-re, akkor $A\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$.*

Bizonyítás. Valóban, az $A \mapsto A\mathcal{O}_{\mathfrak{p}}$ nyilván multiplikatív. Másrészt ha $\mathfrak{p}_1 \neq \mathfrak{p}_2$, akkor van olyan $\alpha \in \mathfrak{p}_2$, ami $\mathfrak{p}_1$-ben nincs benne, tehát $\mathcal{O}_{\mathfrak{p}_1}$-ben invertálható, azaz $\mathfrak{p}_2\mathcal{O}_{\mathfrak{p}_1} = \mathcal{O}_{\mathfrak{p}_1}$. □

A következőkben azt fogjuk megvizsgálni, hogy a lokalizálás során hogy változik a Dedekind gyűrű osztálycsoportja. Legye $(0) \notin X \subseteq \mathrm{Spec}(\mathcal{O})$ egy olyan részhalmaz, mely véges sok kivétellel az összes prímideált tartalmazza. Ekkor az

$$\mathcal{O}(X) = \left\{ \frac{f}{g} \in K \mid g \notin \mathfrak{p} \text{ semmilyen } \mathfrak{p} \in X\text{-re} \right\}$$

gyűrű nem más, mint az $\mathcal{O}T^{-1}$ hányadosgyűrű a $T = \mathcal{O} \setminus \left(\bigcup_{\mathfrak{p} \in X} \mathfrak{p} \right)$ multiplikatívan zárt halmazzal. A következő tétel $\mathcal{O}$ és $\mathcal{O}(X)$ osztálycsoportját és egységcsoportját hasonlítja össze:

3.7.10. Tétel. *Van egy kanonikus egzakt sorozat:*

$$1 \to \mathcal{O}^\times \xrightarrow{\varphi_1} \mathcal{O}(X)^\times \xrightarrow{\varphi_2} \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}) \setminus X} K^\times/\mathcal{O}_{\mathfrak{p}}^\times \xrightarrow{\varphi_3} Cl(\mathcal{O}) \xrightarrow{\varphi_4} Cl(\mathcal{O}(X)) \to 1 \ .$$

Továbbá minden $0 \neq \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ prímre $K^\times/\mathcal{O}_{\mathfrak{p}}^\times \cong \mathbb{Z}$.

Bizonyítás. Az összekötő leképezések a következők: az első $\varphi_1 \colon \mathcal{O}^\times \to \mathcal{O}(X)^\times$ a természetes tartalmazás. A másodikban $\varphi_2(\alpha)$ egy $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}) \setminus X$-hez tartozó koordinátája $\varphi_2(\alpha)_{\mathfrak{p}} := \alpha\mathcal{O}_{\mathfrak{p}}^\times \in K^\times/\mathcal{O}_{\mathfrak{p}}^\times$ minden $\alpha \in \mathcal{O}(X)^\times$-re. A harmadik φ_3 leképezés az $\alpha_{\mathfrak{p}} \in K^\times/\mathcal{O}_{\mathfrak{p}}^\times$-hez $\mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$ osztályát rendeli a $Cl(\mathcal{O})$ osztálycsoportban, az utolsóra pedig $\varphi_4([A]) := [A\mathcal{O}(X)]$ ahol $A \lhd \mathcal{O}$ egy tetszőleges ideál az $[A]$ osztályban. Könnyű látni, hogy ezek a csoporthomomorfizmusok mind jóldefiniáltak.

Világos, hogy φ_1 injektív, mint ahogy az is, hogy $\varphi_2 \circ \varphi_1 = 0$. Valóban, $\mathcal{O}^\times$ benne van $\mathcal{O}_{\mathfrak{p}}^\times$-ben minden $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$-ra.

Egzaktság $\mathcal{O}(X)^\times$-nél: Legyen $\alpha \in \mathrm{Ker}(\varphi_2)$. Ekkor $\alpha \in \mathcal{O}_{\mathfrak{p}}^\times$ minden $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}) \setminus X$-re. Viszont ha $\mathfrak{p} \in X$, akkor $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}(X)_{\mathfrak{p}\mathcal{O}(X)}$ tehát mivel $\alpha \in \mathcal{O}(X)^\times$, ezért α benne van $\mathcal{O}_{\mathfrak{p}}$-ben $\mathfrak{p} \in X$ esetén is. Speciálisan a 3.7.8. Lemma miatt $\alpha, \alpha^{-1} \in \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}} = \mathcal{O}$, azaz $\alpha \in \mathcal{O}^\times$.

Egzaktság $\bigoplus_{\mathfrak{p} \notin X} K^\times/\mathcal{O}_{\mathfrak{p}}^\times$-nél: Vegyük észre, hogy ha $\alpha \in \mathcal{O}(X)^\times$, akkor az $\alpha\mathcal{O}$ törtideál prímtényezős felbontásában csak a $\mathfrak{p} \notin X$ prímek szerepelhetnek a 3.7.9. Lemma miatt. Sőt, ha $\alpha\mathcal{O} = \prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$, akkor φ_3 definíciója miatt $\varphi_3(\varphi_2(\alpha)) = [\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}] = [(\alpha)] = 1$ az osztálycsoportban. Másrészt, ha $\beta = (\beta_{\mathfrak{p}})_{\mathfrak{p} \notin X} \in \mathrm{Ker}(\varphi_3)$, akkor $\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_{\mathfrak{p}}(\beta_{\mathfrak{p}})}$ egy (tört)főideál $\mathcal{O}$-ban, azaz van olyan $\alpha \in K^\times$, melyre $\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_{\mathfrak{p}}(\beta_{\mathfrak{p}})} = \alpha\mathcal{O}$. Node ekkor tetszőleges $\mathfrak{p} \notin X$ prímre $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\beta_{\mathfrak{p}})$ és minden $\mathfrak{p}' \in X$ prímre pedig $v_{\mathfrak{p}'}(\alpha) = 0$. De ez pont azt jelenti, hogy $\alpha \in \mathcal{O}(X)$ és $\varphi_2(\alpha) = (\beta_{\mathfrak{p}})_{\mathfrak{p} \notin X}$.

Egzaktság $Cl(\mathcal{O})$-nál: Ha $\beta = (\beta_{\mathfrak{p}})_{\mathfrak{p} \notin X} \in \bigoplus_{\mathfrak{p} \notin X} K^\times/\mathcal{O}_{\mathfrak{p}}^\times$, akkor

$$\varphi_4(\varphi_3(\beta)) = [\prod_{\mathfrak{p} \notin X} (\mathfrak{p}\mathcal{O}(X))^{v_{\mathfrak{p}}(\beta_{\mathfrak{p}})}] \ .$$

Node ha $\mathfrak{p} \notin X$, akkor $\mathfrak{p}\mathcal{O}(X) = \mathcal{O}(X)$, tehát $\varphi_4 \circ \varphi_3 = 0$. Tegyük fel indirekten, hogy egy $[\prod_{\mathfrak{p}\in X} \mathfrak{p}^{n_\mathfrak{p}}] \in Cl(\mathcal{O})$ ($n_\mathfrak{p} \in \mathbb{Z}$ minden $\mathfrak{p} \in X$-re és $n_\mathfrak{p} = 0$ véges sok kivétellel) benne van φ_4 magjában. Ekkor $\prod_{\mathfrak{p}\in X} \mathfrak{p}^{n_\mathfrak{p}}\mathcal{O}(X) = \alpha\mathcal{O}(X)$ alkalmas $\alpha \in K^\times$ elemmel. Ekkor a 3.7.9. Lemma miatt $(\alpha^{-1}) \prod_{\mathfrak{p}\in X} \mathfrak{p}^{n_\mathfrak{p}}$ prímtényezős felbontásában csak $\mathrm{Spec}(\mathcal{O}) \setminus X$-beli prímek szerepelnek, azaz $[(\alpha^{-1}) \prod_{\mathfrak{p}\in X} \mathfrak{p}^{n_\mathfrak{p}}] = [\prod_{\mathfrak{p}\in X} \mathfrak{p}^{n_\mathfrak{p}}]$ benne van φ_3 képében.

Az egzaktság $Cl(\mathcal{O}(X))$-nél következik a 3.7.1. Lemmából. □

3.8. Dedekind gyűrűk bővítései

3.8.1. Állítás. *Legyen $\mathcal{O}_K$ egy Dedekind gyűrű, K a hányadosteste, L/K pedig egy véges szeparábilis bővítés. Ekkor $\mathcal{O}_K$ egész lezártja L-ben is Dedekind gyűrű.*

Bizonyítás. Az világos, hogy az $\mathcal{O}_K$ feletti egészek $\mathcal{O}_L$ gyűrűje egészre zárt.

Legyen $0 \neq P \lhd \mathcal{O}_L$ egy prímideál. Ekkor $\mathfrak{p} := \mathcal{O}_K \cap P$ is prímideál $\mathcal{O}_K$-ban, így maximális. Tehát $\mathcal{O}_L/P$ egy gyűrűbővítés $\mathcal{O}_K/\mathfrak{p}$-nek, mely nullosztómentes. Továbbá minden $\beta \in \mathcal{O}_L/P$-beli elem algebrai $\mathcal{O}_K/\mathfrak{p}$ felett, tehát m_β minimálpolinomja létezik és a nullosztómentesség miatt irreducibilis. Viszont ekkor $\mathcal{O}_K/\mathfrak{p}[\beta] \cong \mathcal{O}_K/\mathfrak{p}[x]/(m_\beta(x))$ egy test, azaz $\mathcal{O}_L/P$ minden eleme invertálható, azaz P maximális ideál $\mathcal{O}_L$-ben.

Azt kell még belátnunk, hogy $\mathcal{O}_L$ noether. Ehhez elég belátnunk, hogy $\mathcal{O}_L$ egy végesen generált $\mathcal{O}_K$-modulus, hiszen ekkor minden részmodulusa is végesen generált $\mathcal{O}_K$ felett (hiszen $\mathcal{O}_K$ noether), de akkor nyilván a nagyobb $\mathcal{O}_L$ gyűrű felett is. Ehhez vegyünk egy $\alpha_1, \ldots, \alpha_n \in \in \mathcal{O}_L$ K-bázist L-ben. A 3.2.4. Állítás miatt $\mathcal{O}_L \subseteq \mathcal{O}_K\alpha_1/d + \ldots \mathcal{O}_K\alpha_n/d$, speciálisan egy végesen generált $\mathcal{O}_K$-modulus részmodulusa, azaz végesen generált. □

3.8.2. Definíció. Legyen most $\mathfrak{p} \lhd \mathcal{O}_K$ egy prímideál. Ekkor mivel $\mathcal{O}_L$ Dedekind gyűrű, ezért létezik egy $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \ldots P_r^{e_r}$ prímfelbontása $\mathfrak{p}$-nek $\mathcal{O}_L$-ben. Ekkor azt mondjuk, hogy P_i ($i = 1, \ldots, r$) egy $\mathfrak{p}$ fölötti prím. Vegyük észre, hogy ekkor $\mathfrak{p} \subseteq P_i \cap \mathcal{O}_K$, de $1 \notin P_i$ és $\mathfrak{p}$ maximalitása miatt $\mathfrak{p} = P_i \cap \mathcal{O}_K$ minden $i = 1, \ldots, r$-re. Speciálisan az $\mathcal{O}_L/P_i$ test egy véges bővítése $\mathcal{O}_K/\mathfrak{p}$-nek. Jelöljük f_i-vel ennek a testbővítésnek a fokát, melyet *inerciafoknak* nevezünk. Az e_i szám pedig a P_i prím *elágazási indexe*.

3.8.3. Állítás (Fundamentális egyenlet)**.** *Ha $|L : K| = n$ szeparábilis, akkor $n = \sum_{i=1}^r e_i f_i$.*

Bizonyítás. Először is a kínai maradéktétel miatt

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \bigoplus_{i=1}^{r} \mathcal{O}_L/P_i^{e_i} \ . \tag{3.4}$$

Legyen $k := \mathcal{O}_K/\mathfrak{p}$ test. Vegyük észre, hogy ekkor (3.4) mindkét oldala vektortér k felett. Valóban, mindkét oldal egy olyan $\mathcal{O}_K$-modulus, melyet $\mathfrak{p}$ annullál. A 3.5.6. Állítás bizonyításához hasonlóan (3.4) jobb oldala $\sum_{i=1}^r e_i f_i$ dimenziós. Valóban, minden egyes P_i^j/P_i^{j+1} részfaktor egy f_i-dimenziós vektortér k felett, hiszen egydimenziós $\mathcal{O}_L/P_i$ felett. Belátjuk, hogy a bal oldal dimenziója n.

Vegyünk egy $\overline{w_1}, \ldots, \overline{w_m}$ bázist $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$-ben, mint k feletti vektortérben. Vegyük továbbá minden $\overline{w_i}$-nek egy-egy w_i reprezentánsát $\mathcal{O}_L$-ben. Belátjuk, hogy $w_1, \ldots, w_m$ egy bázis L/K-ban, azaz $m = \dim_K L = n$.

A függetlenséghez tegyük fel, hogy

$$\sum_{i=1}^{m} a_i w_i = 0$$

valamilyen $a_i \in K$ elemekre ($i = 1, \dots, m$). Mivel $\mathcal{O}_K$ hányadosteste K, a közös nevezővel beszorozva feltehetjük, hogy $a_i \in \mathcal{O}_K$ minden $i = 1, \dots, m$-re. Jelöljük A-val az $a_1, \dots, a_m$ elemek által generált ideált $\mathcal{O}_K$-ban és tegyük fel, hogy $0 \neq A$. Válasszunk továbbá egy $\alpha \in \in A^{-1} \setminus A^{-1}\mathfrak{p}$ elemet. Ekkor $\alpha a_i \in \mathcal{O}_K$ minden $i = 1, \dots, m$-re, de van olyan $1 \leq j \leq m$, amire $\alpha a_j \notin \mathfrak{p}$. Tehát a $\sum_{i=1}^{m} \overline{\alpha a_i} \cdot \overline{w_i} = 0$ egy nemtriviális lineáris kombinációja a $\overline{w_i}$-knek, ami ellentmond annak, hogy a $\overline{w_1}, \dots, \overline{w_m}$ független k fölött. Tehát $A = 0$, azaz $w_1, \dots, w_m$ is független.

Legyen most $M := \mathcal{O}_K w_1 + \dots + \mathcal{O}_K w_m$ és $N = \mathcal{O}_L/M$ (mindkettő végesen generált $\mathcal{O}_K$-modulus). Vegyük N-nek egy $\alpha_1, \dots, \alpha_s$ generátorrendszerét. Vegyük észre, hogy mivel $\overline{w_1}, \dots, \overline{w_m}$ generátorrendszer $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$-ben, ezért $(M + \mathfrak{p}\mathcal{O}_L)/\mathfrak{p}\mathcal{O}_L = M/(M \cap \mathfrak{p}\mathcal{O}_L) = = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, azaz $M + \mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$, és így $\mathfrak{p}N = N$. Tehát vannak olyan $b_{ij} \in \mathfrak{p}$ elemek ($1 \leq i, j \leq s$), melyekre $\alpha_j = \sum_{i=1}^{s} b_{ij}\alpha_i$. Speciálisan a $C = I - ((b_{ij}))_{ij}$ mátrixra

$$C \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix} = 0 \ .$$

Tehát a 3.1.2. Lemma miatt $\det(C)N = 0$, azaz $\det(C)\mathcal{O}_L \subseteq M = \mathcal{O}_K w_1 + \dots + \mathcal{O}_K w_m$. Speciálisan $\det(C)L \subseteq K w_1 + \dots + K w_m$. Viszont $\det(C) \neq 0$, hiszen $\det(C) \equiv 1 \pmod{\mathfrak{p}}$, tehát $w_1, \dots, w_m$ generátorrendszer L-ben. □

3.8.4. Definíció. Azt mondjuk, hogy $\mathfrak{p} \lhd \mathcal{O}_K$ prím *teljesen felbomlik* L-ben, ha $e_i = f_i = 1$ minden $i = 1, \dots, r$-re. Speciálisan ekkor $r = n$. A $\mathfrak{p}$ prím *elágazik*, ha van olyan i, melyre $e_i > 1$ vagy az $\mathcal{O}_L/P_i$ nem szeparábilis bővítése $\mathcal{O}_K/\mathfrak{p}$-nek. Ez utóbbi inszeparábilitás $K/\mathbb{Q}$ véges bővítés esetén nem állhat fenn, hiszen ekkor $\mathcal{O}_K/\mathfrak{p}$ egy véges test, speciálisan tökéletes. Továbbá a $\mathfrak{p}$ prím teljesen elágazik, ha $r = f_1 = 1$. Azt mondjuk, hogy $\mathfrak{p}$ prím marad L-ben, ha $r = 1$ és $e_1 = 1$ (azaz $f_1 = n$).

3.8.5. Példa. Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$, ahol d négyzetmentes, és $p > 2$ prím. Ekkor $p \mid d$ (azaz $\left(\frac{d}{p}\right) = 0$) esetén p elágazik L-ben, $\left(\frac{d}{p}\right) = -1$ esetén p prím marad L-ben, $\left(\frac{d}{p}\right) = 1$ esetén pedig p teljesen felbomlik L-ben.

A továbbiakban a célunk az lesz, hogy belássuk, hogy csak véges sok prím ágazik el minden véges bővítésben. Sőt, azt fogjuk belátni, hogy pontosan azok a prímek ágaznak el, melyek osztói a diszkriminánsnak.

3.8.6. Tétel. *Legyen $\mathbb{Q} \leq K \leq L$ egy véges bővítése számtesteknek. Legyen továbbá A egy Dedekind gyűrű K-ban, melynek K a hányadosteste és B az A egész lezártja L-ben. (Pl. $A = = \mathcal{O}_K$, vagy valamilyen hányadosgyűrűje $\mathcal{O}_K$-nak.) Tegyük fel továbbá, hogy B egy szabad A-modulus. Ekkor B-ben pontosan a $d_{B/A}$ diszkriminánst osztó prímek ágaznak el.*

3.8.7. Megjegyzés. Itt a $d_{B/A}$ diszkrimináns B egy tetszőleges A-bázisának diszkriminánsa. Azért létezik, mert B-ről feltettük, hogy szabad modulus A felett. Továbbá az is világos, hogy a diszkrimináns egységszorzó erejéig egyértelmű, hiszen az áttérési mátrix $\mathrm{GL}_n(A)$-ban van. Viszont B nem mindig szabad modulus A fölött az $A = \mathcal{O}_K$, $B = \mathcal{O}_L$ esetben, de az $A = \mathbb{Z}$ vagy a lokális $A = \mathcal{O}_{K\mathfrak{p}}$ ($\mathfrak{p} \lhd \mathcal{O}_K$ prím) esetben ez automatikus, hiszen ekkor A főideálgyűrű.

3.8.8. Definíció. Egy B kommutatív gyűrűről azt mondjuk, hogy *redukált*, ha B-ben nincsenek nullától különböző nilpotens elemek.

3.8.9. Lemma. *Legyen k egy tökéletes test és B egy kommutatív végesdimenziós k-algebra. Ekkor B pontosan akkor redukált, ha diszkriminánsa $d_{B/k} \neq 0$.*

Bizonyítás. Ha $\beta \neq 0$ egy nilpotens elem, akkor legyen $\beta = e_1, \ldots, e_n$ a B egy bázisa k felett. Ekkor $d_{B/A}$ nem más, mint a $(\mathrm{Tr}(e_i e_j))_{i,j}$ mátrix determinánsa. Node βe_j minden j-re nilpotens, tehát mátrixa is nilpotens, ezért nyoma 0. Így $(\mathrm{Tr}(e_i e_j))_{i,j}$ első sora 0, speciálisan determinánsa is 0.

Megfordítva legyen B redukált. Belátjuk, hogy ekkor B testek direkt szorzata. Az állítás ebből már következik, hiszen ekkor B diszkriminánsa a testek diszkriminánsainak szorzata (blokkdiagonális mátrix determinánsa a blokkok determinánsának szorzata), de mivel k tökéletes, ezért ezek szeparábilis bővítések, diszkriminánsuk nem 0 a 3.2.3. Tétel miatt.

Valóban, a feltétel, hogy B-ben nincs nilpotens elem azt jelenti, hogy B nilradikálja $\mathfrak{N} = \{b \in B \mid b \text{ nilpotens}\} = 0$. Az $\mathfrak{N}$ nilradikál pedig nem más, mint B prímideáljainak metszete. Valóban, ha $b^n = 0$ valamilyen $n \geq 1$-re és $P \lhd B$ egy prímideál, akkor $b^n \in P$ miatt $b \in P$. Megfordítva tegyük fel, hogy $b \in B$ nem nilpotens. Tekintsük B-nek az összes olyan I ideáljának $\mathcal{H}$ halmazát, amiben b-nek semmilyen hatványa nincs benne. Mivel b nem nilpotens, ezért $(0) \in \mathcal{H}$, speciálisan $\mathcal{H}$ nemüres. Másrészt B noether (sőt, artin, hiszen végesdimenziós k-algebra), ezért $\mathcal{H}$-nak van maximális eleme. Belátjuk, hogy I prím, azaz b nincs benne az összes prímideál metszetében, hiszen $b \notin I$. Legyen ugyanis $x, y \notin I$ és tegyük fel, hogy $xy \in I$. Ekkor I maximalitása miatt $b^m \in I + (x)$ és $b^l \in I + (y)$ alkalmas $l, m \geq 1$ egészekkel. De ekkor $b^{l+m} \in (I + (x))(I + (y)) \subseteq I + (xy) \subseteq I$, ami ellentmondás.

Tehát B prímideáljainak metszete 0. Node B minden prímideálja maximális: Valóban, ha $P \lhd B$ egy prímideál, akkor B/P egy végesdimenziós nullosztómentes kommutatív k-algebra, ezért test (lsd. a 3.8.1. Állítás bizonyítása). Tehát P maximális ideál B-ben. Speciálisan B egy olyan artin gyűrű, melyben a maximális (bal)ideálok metszete triviális, azaz $\mathrm{Jac}(B) = 0$. Így a Wedderburn-Artin tétel miatt B ferdetestek feletti mátrixgyűrűk direkt szorzata, de mivel kommutatív, ezért testek direkt szorzata. □

A 3.8.6. Tétel bizonyítása. Vegyük B egy A feletti $\alpha_1, \ldots, \alpha_n$ bázisát és legyen $\mathfrak{p}$ egy prímideál B-ben. Ekkor mivel B egy szabad modulus A felett, ezért $B/\mathfrak{p}B$ is egy szabad modulus $A/\mathfrak{p}$ felett, mégpedig $\alpha_1 + \mathfrak{p}B, \ldots, \alpha_n + \mathfrak{p}B$ generátorokkal. Speciálisan $d_{B/A} = d(\alpha_1, \ldots, \alpha_n)$ pontosan akkor van benne a $\mathfrak{p}$ prímideálban, ha $d_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = 0$ $A/\mathfrak{p}$-ben. Ez pedig a 3.8.9. Lemma miatt (alkalmazhatjuk, hiszen $A/\mathfrak{p}$ egy véges test, ezért tökéletes) pont azt jelenti, hogy $B/\mathfrak{p}B$ nem redukált. Node ha $\mathfrak{p}B = \prod_{i=1}^{r} P_i^{e_i}$ a $\mathfrak{p}$ prímtényezős felbontása B fölött, akkor a kínai maradéktétel szerint

$$B/\mathfrak{p}B \cong \bigoplus_{i=1}^{r} B/P_i^{e_i} \ .$$

Ebben viszont pontosan akkor nincs nilpotens elem, ha $e_i = 1$ minden $i = 1, \dots, r$-re, azaz ha $\mathfrak{p}$ nem ágazik el. □

3.8.10. Következmény. *$\mathbb{Q}$-nak nincs olyan bővítése, ami semelyik prímben sem ágazik el.*

Bizonyítás. Ha K egy tetszőleges véges bővítése $\mathbb{Q}$-nak, akkor a 3.5.11. Tétel alapján $|d_K| > 1$, speciálisan d_K-nak van prímosztója, mely a 3.8.6. Tétel szerint elágazik K-ban. □

A 3.8.6. Tétel állítása akkor is igaz, ha nem tesszük fel, hogy B szabad modulus A felett. Ehhez viszont először értelmeznünk kell B diszkriminánsát A felett az általános esetben. Ezt kétféleképpen tehetjük meg, de a két definíció ekvivalens. Az első definíció a következő: Legyen $\mathfrak{p} \lhd A$ egy tetszőleges prímideál. Ekkor $A_\mathfrak{p}$ egy diszkrét értékelésgyűrű, ezért ennek $B_\mathfrak{p}$ egész lezártja szabad modulus $A_\mathfrak{p}$ felett. Speciálisan értelmezhetjük $B_\mathfrak{p}$ $d_{B_\mathfrak{p}/A_\mathfrak{p}} \in A_\mathfrak{p}$ diszkriminánsát. Legyen $m_\mathfrak{p} := v_\mathfrak{p}(d_{B_\mathfrak{p}/A_\mathfrak{p}})$ és definiáljuk $\mathfrak{d}_{B/A} \lhd A$ diszkriminánst mint $\mathfrak{d}_{B/A} = \prod_\mathfrak{p} \mathfrak{p}^{m_\mathfrak{p}}$ szorzatot. Ahhoz, hogy ez értelmes legyen, be kell látnunk, hogy véges sok kivétellel $m_\mathfrak{p} = 0$, azaz csak véges sok prím ágazik el B-ben. A következő lemma az első lépés ebben az irányban, mely azt is mutatja, hogy az elágazás egy lokális tulajdonság:

3.8.11. Lemma. *Legyen $\mathfrak{p} \lhd A$ egy prím. Ekkor az $A_\mathfrak{p}$ gyűrű egész lezártja L-ben nem más, mint $B_\mathfrak{p} = BS^{-1}$, ahol $S = A \setminus \mathfrak{p}$. Speciálisan $\mathfrak{p}$ pontosan akkor ágazik el B-ben, ha $\mathfrak{p}A_\mathfrak{p}$ elágazik $B_\mathfrak{p}$-ben.*

Bizonyítás. Egyrészt egy $\frac{\beta}{s} \in BS^{-1}$ elem egész $A_\mathfrak{p}$ fölött: Mivel $\beta \in B$, ezért van olyan $f(x) \in \in A[x]$ normált polinom, melyre $f(\beta) = 0$. Viszont $\frac{\beta}{s}$ gyöke ekkor az $s^{-\deg(f)} f(xs) \in A_\mathfrak{p}[x]$ normált polinomnak, tehát egész $A_\mathfrak{p}$ felett.

Visszafelé legyen $\alpha \in L$ egész $A_\mathfrak{p}$ fölött. Ekkor van olyan $a_i \in A$, $s_i \in S$ $(i = 0, \dots, m-1$ alkalmas $m \geq 1$-re), melyekre $\alpha^m + \frac{a_{m-1}}{s_{m-1}}\alpha^{m-1} + \dots + \frac{a_0}{s_0} = 0$. Viszont beszorozva $(s_0 \dots s_{m-1})^m$-nel ez azt jelenti, hogy $s_0 \dots s_{m-1}\alpha$ egész A fölött, tehát B-ben van, speciálisan $\alpha \in BS^{-1}$.

Legyen $\mathfrak{p}B$ prímtényezős felbontása B-ben $\mathfrak{p}B = P_1^{e_1} \dots P_r^{e_r}$. Ekkor $B_\mathfrak{p}$-nek csak véges sok prímideálja van, mégpedig $P_1, \dots, P_r$. Valóban, $B_\mathfrak{p}$ prímideáljai kölcsönösen egyértelműen megfelelnek B S-et nem metsző P prímideáljainak, azaz azoknak, melyekre $P \cap A \subseteq \mathfrak{p}$. Tehát $\mathfrak{p}B_\mathfrak{p} = \prod_{i=1}^r (P_i B_\mathfrak{p})^{e_i}$. □

A következő lépésként belátjuk, hogy véges sok B-ben elágazó prímideál van mindig. Ez egyúttal algoritmust is ad arra, hogy bizonyos speciális esetekben (amikor $B = A[\alpha]$ alkalmas $\alpha \in B$-re) hogyan tudjuk meghatározni a $\mathfrak{p}$ prím felbontását B felett.

3.8.12. Definíció. Legyen A egy Dedekind gyűrű K hányadostesttel és L/K egy szeparábilis bővítés, melyben A egész lezártja B. Legyen továbbá $\alpha \in B$ egy olyan elem, melyre $L = K(\alpha)$. Ekkor az $A[\alpha]$ gyűrű *konduktorának* az $I = I(\alpha) = \{\beta \in B \mid \beta B \subseteq A[\alpha]\} \lhd B$ ideált nevezzük. Mivel B egy végesen generált A-modulus, ezért $I \neq 0$.

3.8.13. Állítás. *Legyen $\mathfrak{p}$ egy $I(\alpha)$-hoz relatív prím prímideál A-ban (azaz $I(\alpha) \cap A \not\subseteq \mathfrak{p}$). Legyen továbbá $f(x) \in A[x]$ az α minimálpolinomja. Bontsuk f-et irreducibilisek szorzatára modulo $\mathfrak{p}$: $f(x) \equiv \overline{f}(x) = \prod_{i=1}^r \overline{f_i}(x)^{e_i} \pmod{\mathfrak{p}}$ és legyen $f_i(x) \in A[x]$ egy-egy normált felemelt, azaz $f_i(x) \equiv \overline{f_i}(x) \pmod{\mathfrak{p}}$. Ekkor a*

$$P_i = \mathfrak{p}B + f_i(\alpha)B$$

ideálok páronként különböző prímideálok, melyekre

$$\mathfrak{p}B = \prod_{i=1}^{r} P_i^{e_i} \ .$$

Speciálisan ha $\mathfrak{p}$ nem osztja a $d(1, \alpha, \ldots, \alpha^{n-1})$ diszkriminánst (és $I(\alpha)$-hoz is relatív prím), akkor nem ágazik el B-ben.

Bizonyítás. Jelöljük $A/\mathfrak{p} = k$-val a $\mathfrak{p}$ maradéktestét. Mivel $\mathfrak{p}$ és $I(\alpha)$ relatív prímek, ezért $B = \mathfrak{p}B + I(\alpha)$. Viszont $I(\alpha)$ definíciója miatt $I(\alpha) \subseteq A[\alpha]$, speciálisan $B = \mathfrak{p}B + A[\alpha]$. Ekkor az I. izomorfizmustétel miatt

$$B/\mathfrak{p}B \cong A[\alpha]/(\mathfrak{p}B \cap A[\alpha]) = A[x]/(\mathfrak{p}A[x], f(x)) \cong k[x]/(\overline{f}(x)) \cong \bigoplus_{i=1}^{r} k[x]/(\overline{f_i}(x)^{e_i}) \ .$$

Tehát a kínai maradéktételt alkalmazva $B/\mathfrak{p}B$-re is azt kapjuk, hogy $\mathfrak{p}B = \prod_{i=1}^{r} Q_i^{e_i}$, ahol $Q_i \lhd B$ a teljes ősképe $(\overline{f_i}(x))$-nek a természetes $\pi_i \colon B \to k[x]/(\overline{f}_i(x))$ homomorfizmusnál. Az világos, hogy $P_i \subseteq Q_i$, hiszen ennél a homomorfizmusnál $\pi_i(\alpha) = x + (\overline{f}_i(x))$. Másrészt $B/P_i \cong k[x]/(\overline{f_i}(x)) \cong B/Q_i$, tehát $P_i = Q_i$. □

Így B-ben csak azok az ideálok ágazhatnak el, amik nem relatív prímek $I(\alpha)$-hoz vagy $d(1, \ldots, \alpha^{n-1})$-hez, speciálisan csak véges sok A-beli prímideál ágazhat el B-ben. Tehát a $\mathfrak{d}_{B/A} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p}}$ szorzat véges, ezt nevezzük a B/A bővítés diszkriminánsának.

3.8.14. Állítás. *A $\mathfrak{d}_{B/A}$ ideált generálják a $d(\alpha_1, \ldots, \alpha_n)$ számok, ahol az $(\alpha_1, \ldots, \alpha_n) \in B^n$ szám n-esek az L test K-feletti B-ben fekvő bázisain futnak végig.*

Bizonyítás. Legyen $\alpha_1, \ldots, \alpha_n \in B$ egy bázisa L-nek K felett és $\mathfrak{p} \lhd A$ egy prímideál. Ekkor mivel $\bigoplus_{i=1}^{n} A_\mathfrak{p}\alpha_i \subseteq B_\mathfrak{p}$, ezért $d(\alpha_1, \ldots, \alpha_n) \in d_{B_\mathfrak{p}/A_\mathfrak{p}} A_\mathfrak{p} = \mathfrak{p}^{m_\mathfrak{p}} A_\mathfrak{p}$. Tehát $d(\alpha_1, \ldots, \alpha_n) \in \in \bigcap_{\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p}} = \mathfrak{d}_{B/A}$. Másrészt jelöljük I-vel a $d(\alpha_1, \ldots, \alpha_n) \in A$ elemek által generált ideált és tekintsük az $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$ prímtényezős felbontást. Azt kell még belátnunk, hogy minden $\mathfrak{p}$ prímre $n_\mathfrak{p} \leq m_\mathfrak{p}$, hiszen az $I \subseteq \mathfrak{d}_{B/A}$ tartalmazásból következik, hogy $n_\mathfrak{p} \geq m_\mathfrak{p}$. Mivel $A_\mathfrak{p}$ főideálgyűrű, ezért $B_\mathfrak{p}$ egy n rangú szabad modulus $A_\mathfrak{p}$ felett. Így a 3.8.11. Lemma miatt választhatjuk $B_\mathfrak{p}$-nek egy B-ben fekvő $\alpha_{1,\mathfrak{p}}, \ldots, \alpha_{n,\mathfrak{p}}$ bázisát (valóban, egy tetszőleges bázis elemeit beszorozhatjuk az $S = A \setminus \mathfrak{p}$-beli nevezőkkel, hiszen azok invertálhatók $B_\mathfrak{p}$-ben). Ekkor viszont $d(\alpha_{1,\mathfrak{p}}, \ldots, \alpha_{n,\mathfrak{p}})A_\mathfrak{p} = \mathfrak{p}^{m_\mathfrak{p}} A_\mathfrak{p}$, speciálisan $n_\mathfrak{p} \leq m_\mathfrak{p}$. □

A fentieket összetéve adódik a következő

3.8.15. Tétel. *Egy $\mathfrak{p} \lhd A$ prímideál pontosan akkor ágazik el B-ben, ha $\mathfrak{d}_{B/A} \subseteq \mathfrak{p}$.*

3.8.16. Példa. Bontsuk $\mathbb{Z}[\sqrt[3]{2}]$-ben prímtényezők szorzatára az (5)-öt.

Megoldás. Mivel $\mathbb{Z}[\sqrt[3]{2}]$ egészre zárt, ezért elég az $x^3 - 2$ polinomot felbontani irreducibilisek szorzatára $\mathbb{F}_5$-ben. $\mathbb{F}_5$ fölött ennek van gyöke ($x = 3$), ezért a felbontás $x^3 - 2 = (x + 2)(x^2 - - 2x - 1)$, ahol $x^2 - 2x - 1$ már irreducibilis, hiszen ennek már nincs gyöke $\mathbb{F}_5$-ben. Tehát a kívánt felbontás: $(5) = (5, \sqrt[3]{2} + 2)(5, \sqrt[3]{4} - 2\sqrt[3]{2} - 1)$. □

3.9. Hilbert-féle elágazáselmélet

A továbbiakban legyen $\mathcal{O} = \mathcal{O}_K$ egy Dedekind gyűrű K hányadostesttel és L/K egy véges *Galois*-bővítés $G = \mathrm{Gal}(L/K)$ Galois-csoporttal, $\mathcal{O}_L$ pedig $\mathcal{O}_K$ egész lezártja L-ben. Ekkor G hat az $\mathcal{O}_L$ gyűrűn, hiszen ha α egész $\mathcal{O}_K$ felett, akkor $\sigma(\alpha)$ is az minden $\sigma \in G$-re, hiszen ugyanazoknak a K-beli együtthatós polinomoknak gyökei. Továbbá ha $\mathfrak{p} \lhd \mathcal{O}_K$ prímideál és $\mathfrak{p} \subseteq P \lhd \mathcal{O}_L$ egy $\mathcal{O}_L$-beli $\mathfrak{p}$-t osztó prím, akkor $P \cap \mathcal{O}_K = \mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(P \cap \mathcal{O}_K) = \sigma(P) \cap \mathcal{O}_K$. Tehát $\sigma(P)$ is egy $\mathfrak{p}$ fölötti prím.

3.9.1. Állítás. *Ha $\mathfrak{p} \lhd \mathcal{O}_K$ egy tetszőleges prím $\mathcal{O}_K$-ban, akkor G tranzitívan hat az L-beli $\mathfrak{p}$ feletti prímeken. Speciálisan ha $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \dots P_r^{e_r}$, akkor $e_1 = \dots = e_r$ és $f_1 = \dots = f_r$.*

Bizonyítás. Legyenek $P' \cap \mathcal{O}_K = \mathfrak{p} = P \cap \mathcal{O}_K$ prímek és tegyük fel, hogy $\sigma(P) \neq P'$ semmilyen $\sigma \in G$-re. A kínai maradéktétel szerint van olyan $\alpha \in \mathcal{O}_L$, melyre $\alpha \equiv 0 \pmod{P'}$ és $\alpha \equiv 1 \pmod{\sigma(P)}$ minden $\sigma \in G$-re. Ekkor egyrészt $N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \in P' \cap \mathcal{O}_K = \mathfrak{p} \subseteq P$ (hiszen $\alpha \in P'$), másrészt $N_{L/K}(\alpha) \notin P$, hiszen $\sigma(\alpha) \in P \Leftrightarrow \alpha \in \sigma^{-1}(P)$. Ez ellentmondás, tehát a G-hatás tranzitív a $\mathfrak{p}$ feletti prímeken.

A második állításhoz alkalmazzuk $\sigma \in G$-t a $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \dots P_r^{e_r}$ egyenletre: $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(P_1)^{e_1} \dots \sigma(P_r)^{e_r}$, tehát a tranzitivitás miatt $e_1 = \dots = e_r$. Másrészt $\sigma \colon \mathcal{O}_L/P \to \mathcal{O}_L/\sigma(P)$ egy izomorfizmus, ezért $f_1 = \dots = f_r$. □

A fenti állítás fényében a fundamentális egyenlet (3.8.3. Állítás) az $n = efr$ alakra egyszerűsödik a Galois-esetben.

3.9.2. Definíció. Ha $P \lhd \mathcal{O}_L$ egy prím, akkor a P elem G-beli G_P stabilizátorát a fenti hatásra nézve P felbontási részcsoportjának nevezzük.

G tranzitivitása miatt a G_P részcsoportok konjugáltak G-ben ($\mathfrak{p} \subseteq P$). Továbbá az orbit-stabilizátor lemma azt mutatja, hogy $|G : G_P| = r$. Jelöljük $L^{G_P} = Z_p$-vel a G_P részcsoport fixtestét L-ben és $P \cap Z_P = P_Z$-vel a P alatti prímet Z_P-ben.

3.9.3. Állítás. *(i) P az egyetlen P_Z feletti prím L-ben;*

(ii) P elágazási indexe az L/Z_P bővítésben e, inerciafoka f;

(iii) P_Z elágazási indexe és inerciafoka K fölött egyaránt 1.

Bizonyítás. Vegyük észre, hogy G_P nem más, mint az L/Z_P bővítés Galois-csoportja, ezért tranzitívan hat a P_Z feletti prímeken. Viszont P egy P_Z feletti prím, és ezt fixálja a G_P csoport, tehát csak ez az egy prím van L-ben P_Z felett. Másrészt ha e'-vel ill. f'-vel jelöljük P elágazási indexét ill. inerciafokát Z_P fölött, továbbá e''-vel ill. f''-vel a P_Z elágazási indexét ill. inerciafokát K fölött, akkor $e = e'e''$ és $f = f'f''$ (azaz az inerciafok és az elágazási index egyaránt összeszorzódik bővítések egymásutánjánál). Valóban, az f inerciafokra ez a (maradéktestekre alkalmazott) fokszámtétel egyenes következménye. Másrészt e' és e'' definíciójából

$$P^e \cdot \dots = \mathfrak{p}\mathcal{O}_L = P_Z^{e''}\mathcal{O}_L \cdot \dots = (P^{e'})^{e''} \cdot \dots = P^{e'e''} \cdot \dots$$

egyenletben összehasonlítva P kitevőjét $e = e'e''$ is adódik. Viszont mivel P_Z felett csak egyetlen prím van L-ben, ezért $e'f' = |L : Z_P| = |G_P| = \frac{n}{r} = ef$, tehát szükségképpen $e = e'$ és $f = f'$, amikoris $e'' = f'' = 1$. □

Legyen most P egy $\mathfrak{p}$ feletti prím az L/K Galois-bővítésben és jelölje $k_P := \mathcal{O}_L/P$, ill. $k_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ a maradéktesteket. Tegyük fel továbbá, hogy a $k_P/k_\mathfrak{p}$ bővítés szeparábilis (speciálisan ha $k_\mathfrak{p}$ egy véges test, akkor ez automatikus). Ha $\sigma \in G_P$, akkor a

$$\begin{aligned} \overline{\sigma}\colon k_P &\to k_P \\ \alpha + P &\mapsto \sigma(\alpha) + P \end{aligned}$$

leképezés jóldefiniált. Sőt, az is világos, hogy ez egy $k_\mathfrak{p}$-t fixáló automorfizmusa k_P-nek, tehát a $\mathrm{Gal}(k_P/k_\mathfrak{p})$ Galois-csoport egy eleme.

3.9.4. Állítás. *A $k_P/k_\mathfrak{p}$ bővítés normális (speciálisan Galois, mivel feltettük, hogy szeparábilis) és a $\bar{\cdot}\colon G_P \to \mathrm{Gal}(k_P/k_\mathfrak{p})$ homomorfizmus szürjektív.*

Bizonyítás. A 3.9.3. Állítás miatt a Z_P felbontási test maradékteste ugyanaz, mint K maradékteste, ezért feltehetjük, hogy $K = Z_P$ és így $G = G_P$.

A normalitáshoz azt kell belátnunk, hogy ha egy $\overline{g}(x) \in k_\mathfrak{p}[x]$ irreducibilis polinomnak van gyöke k_P-ben, akkor k_P fölött lineáris faktorokra bomlik. Vegyünk egy ilyen $\overline{g}$ polinomot és egy $\overline{\alpha} \in k_P$ gyököt. Tekintsük az $\overline{\alpha}$ egy tetszőleges $\alpha \in \mathcal{O}_L$ reprezentánsát. Legyen továbbá $f(x) \in \mathcal{O}_K[x]$ az α minimálpolinomja $\mathcal{O}_K$ fölött (ez normált, hiszen, $\alpha \in \mathcal{O}_L$ egész $\mathcal{O}_K$ fölött). Ekkor ha $\overline{f}$ az f redukciója modulo $\mathfrak{p}$, akkor $\overline{f}(\overline{\alpha}) = \overline{f(\alpha)} = 0$, speciálisan $\overline{g} \mid \overline{f}$, hiszen $\overline{g}$ a minimálpolinom. Viszont mivel L/K Galois, ezért f összes gyöke $\mathcal{O}_L$-ben van, azaz f lineáris faktorokra bomlik $\mathcal{O}_L$ felett. De ekkor a redukciója, $\overline{f}$ is lineáris faktorokra bomlik k_P felett, speciálisan minden osztója, azaz $\overline{g}$ is.

A szürjektivitáshoz legyen $\overline{\alpha}$ egy primitív elem, azaz $k_P = k_\mathfrak{p}(\overline{\alpha})$. Továbbra is jelölje $\overline{g}(x) \in$ $\in k_\mathfrak{p}[x]$ az $\overline{\alpha}$ minimálpolinomját, $\alpha \in \mathcal{O}_L$ egy tetszőleges felemeltet f minimálpolinommal, és legyen $\overline{\sigma} \in \mathrm{Gal}(k_P/k_\mathfrak{p})$ tetszőleges. Ekkor $\overline{\sigma}(\overline{\alpha})$ is gyöke $\overline{g}$-nek, ezért $\overline{f}$-nek is. Node f gyökeinek redukáltjai k_P-ben éppen $\overline{f}$ gyökei, ezért f-nek van egy olyan α' gyöke $\mathcal{O}_L$-ben, melyre $\alpha' \equiv$ $\equiv \overline{\sigma}(\overline{\alpha}) \pmod{P}$. Viszont G tranzitívan hat f gyökein, ezért van olyan $\sigma \in G$, melyre $\sigma(\alpha) =$ $= \alpha'$. De ekkor σ képe éppen $\overline{\sigma}$ a $G_P \to \mathrm{Gal}(k_P/k_\mathfrak{p})$ természetes homomorfizmusnál. □

3.9.5. Definíció. A $G_P \to \mathrm{Gal}(k_P/k_\mathfrak{p})$ homomorfizmus magját a P prím inerciarészcsoportjának nevezzük és I_P-vel jelöljük.

3.9.6. Megjegyzés. A 3.9.4. Állítás szerint $f = |k_P : k_\mathfrak{p}| = |\mathrm{Gal}(k_P/k_\mathfrak{p})|$, tehát $|I_P| = e$. Speciálisan a $\mathfrak{p}$ prím pontosan akkor ágazik el, ha I_P nemtriviális.

3.10. Algebrai geometriai analógiák

Ebben a fejezetben megpróbálunk rámutatni az algebrai geometriai analógiákra. A bizonyítások vázlatosak lesznek, mivel ahhoz, hogy precízzé tegyük őket, szükségünk lenne némi algebrai geometriai bevezetőre, ami jelen esetben nem célunk. A szándékunk sokkal inkább az érdeklődés felkeltése azok számára, akik még nem tanultak algebrai geometriát, illetve a két terület közötti hasonlóságok bemutatása azok számára, akik már tanultak.

Legyen $f(x, y) \in \mathbb{C}[x, y]$ egy irreducibilis polinom. Tekintsük az $\mathcal{O} = \mathbb{C}[x, y]/(f(x, y))$ faktorgyűrűt, azaz a $V(f) = \{(x_0, y_0) \in \mathbb{C}^2 \mid f(x_0, y_0) = 0\}$ komplex görbének koordinátagyűrűjét.

3.10.1. Állítás. *$\mathcal{O}$ pontosan akkor Dedekind gyűrű, ha a $V(f)$ görbe nemszinguláris, azaz ha semmilyen $(x_0, y_0) \in V(f)$ pontra a $(\frac{\partial}{\partial x} f(x_0, y_0), \frac{\partial}{\partial y} f(x_0, y_0))$ érintővektor nem a nullvektor.*

Bizonyítás. Hilbert bázistétele ([7] 5.6.11. Tétel) szerint $\mathbb{C}[x, y]$ noether, ezért $\mathcal{O}$ is noether. Másrészt a Nullstellensatz ([7] 5.6.9. Tétel) miatt $\mathcal{O}$ minden maximális ideálja $\mathfrak{p} = (x - x_0 + \\ + (f(x, y)), y - y_0 + (f(x, y)))$ alakú, speciálisan (legfeljebb) két elemmel generálható. Belátjuk, hogy az $\mathcal{O}_\mathfrak{p}$ lokalizált pontosan akkor diszkrét értékelésgyűrű, ha $V(f)$ nemszinguláris az (x_0, y_0) pontban.

Vegyük észre, hogy

$$\mathfrak{p}/\mathfrak{p}^2 \cong (x - x_0, y - y_0)/((x - x_0)^2, (x - x_0)(y - y_0), (y - y_0)^2, f(x, y)) \ .$$

Tehát ez egy legfeljebb kétdimenziós vektortér $\mathbb{C} \cong \mathcal{O}/\mathfrak{p}$ felett. Másrészt ha az $f(x, y)$ polinomot (x_0, y_0) körül Taylor-sorba fejtjük és észrevesszük, hogy $(x_0, y_0) \in V(f)$ miatt $f(x_0, y_0) = \\ = 0$, akkor $f(x, y)$-t az alábbi alakba írhatjuk:

$$f(x, y) \equiv \frac{\partial}{\partial x} f(x_0, y_0)(x - x_0) + \frac{\partial}{\partial y} f(x_0, y_0)(y - y_0) \pmod{\mathfrak{p}^2} \ .$$

Tehát $\mathfrak{p}/\mathfrak{p}^2$ pontosan akkor egydimenziós, ha $f(x, y)$ nincs benne az $(x - x_0, y - y_0)^2 \lhd \mathbb{C}[x, y]$ ideálban, ami pedig a fentiek szerint azzal ekvivalens, hogy $V(f)$ nemszinguláris az (x_0, y_0) pontban.

A 3.7.3. Állítás értelmében $\mathfrak{p}/\mathfrak{p}^2 \cong \mathfrak{m}_\mathfrak{p}/{\mathfrak{m}_\mathfrak{p}}^2$, ahol $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ a maximális ideál a lokális gyűrűben. Speciálisan, ha $V(f)$-nek van egy (x_0, y_0) szinguláris pontja, akkor a megfelelő $\mathcal{O}_\mathfrak{p}$ lokális gyűrű nem lehet diszkrét értékelésgyűrű, hiszen $\mathfrak{m}_\mathfrak{p}$ nem főideál (különben $\mathfrak{m}_\mathfrak{p}/{\mathfrak{m}_\mathfrak{p}}^2$ is egy elemmel generálható lenne, holott kétdimenziós). Tehát $\mathcal{O}$ nem Dedekind a 3.7.6. Tétel miatt.

Megfordítva ha $V(f)$-nek nincs szinguláris pontja, akkor minden $\mathfrak{p} \lhd \mathcal{O}$ *maximális* ideálra $\dim_\mathbb{C} \mathfrak{m}_\mathfrak{p}/{\mathfrak{m}_\mathfrak{p}}^2 = 1$. Vegyünk tehát egy tetszőleges $\pi \in \mathfrak{m}_\mathfrak{p} \setminus {\mathfrak{m}_\mathfrak{p}}^2$ elemet. Ekkor $(\pi) + {\mathfrak{m}_\mathfrak{p}}^2 = \mathfrak{m}_\mathfrak{p}$, így a Nakayama Lemma miatt $(\pi) = \mathfrak{m}_\mathfrak{p}$ egy főideál. Továbbá ebben a speciális esetben az is világos, hogy $\bigcap_n {\mathfrak{m}_\mathfrak{p}}^n = 0$. Valóban, ha $I = \bigcap_n {\mathfrak{m}_\mathfrak{p}}^n$ akkor nyilván $\pi I \subseteq I$, de ha $\alpha \in I$ tetszőleges, akkor $\alpha = \pi^{n+1}\beta$ alakú, ezért $\frac{\alpha}{\pi} = \pi^n \beta$ alakú, azaz $\frac{\alpha}{\pi} \in I$, azaz $\mathfrak{m}_\mathfrak{p} I = \pi I = I$. Viszont ekkor a Nakayama Lemma szerint $I = 0$. Legyen most $0 \neq J \lhd \mathcal{O}_\mathfrak{p}$ egy tetszőleges ideál. Ekkor mivel $\bigcap_n {\mathfrak{m}_\mathfrak{p}}^n = 0$, ezért van olyan $k \geq 0$, melyre $J \subseteq {\mathfrak{m}_\mathfrak{p}}^k$, de $J \not\subseteq {\mathfrak{m}_\mathfrak{p}}^{k+1}$. Ekkor viszont $J + {\mathfrak{m}_\mathfrak{p}}^{k+1} = {\mathfrak{m}_\mathfrak{p}}^k$, hiszen ${\mathfrak{m}_\mathfrak{p}}^k/{\mathfrak{m}_\mathfrak{p}}^{k+1} = (\pi^k)/(\pi^{k+1})$ egy egydimenziós vektortér $\mathcal{O}/\mathfrak{p}$ felett, melyben $J + {\mathfrak{m}_\mathfrak{p}}^{k+1}/{\mathfrak{m}_\mathfrak{p}}^{k+1}$ egy nemnulla altér. A Nakayama Lemma ismételt alkalmazásával $J = {\mathfrak{m}_\mathfrak{p}}^k = (\pi^k)$ egy főideál, azaz $\mathcal{O}_\mathfrak{p}$ egy diszkrét értékelésgyűrű. Ahhoz, hogy a 3.7.6. Tételt (formálisan) alkalmazhassuk, nemcsak a maximális ideáloknál vett lokalizáltakról kellene tudnunk, hogy diszkrét értékelésgyűrűk, hanem minden prímideálnál. Viszont vegyük észre, hogy a 3.7.6. Tétel bizonyításában csak azt használtuk, hogy a maximális ideáloknál vett lokalizáltak diszkrét értékelésgyűrűk. Valóban, ha $0 \neq \mathfrak{p}_1 \lhd \mathcal{O}$ egy nem maximális prímideál, akkor benne van egy $\mathfrak{p}$ maximális ideálban, viszont ekkor $0 \neq \mathfrak{p}_1\mathcal{O}_\mathfrak{p} \neq \mathfrak{p}\mathcal{O}_\mathfrak{p}$ egy prímideál $\mathcal{O}_\mathfrak{p}$-ben, ami ellentmond annak, hogy $\mathcal{O}_\mathfrak{p}$ diszkrét értékelésgyűrű. □

Ha viszont $V(f)$ szinguláris, azaz a $\mathcal{O} = \mathbb{C}[x, y]/(f(x, y))$ gyűrű nem Dedekind, akkor vehetjük a hányadostestében az egész lezártját. Ennek a spektruma már egy nemszinguláris görbe. Erre tekinthetünk úgy is, mint a $V(f)$ görbe szingularitásainak feloldására. A szingularitások feloldhatósága az algebrai geometria egyik alapkérdése.

A Dedekind gyűrűk bővítéseinek geometriai analógiája a(z elágazó) fedőleképezés. Valóban, ha $\mathcal{O}_K \leq \mathcal{O}_L$ Dedekind gyűrűk egy bővítése, akkor ez indukál egy leképezést $\mathcal{O}_L$ prímideáljainak halmazából $\mathcal{O}_K$ prímideáljainak halmazába: $P \lhd \mathcal{O}_L$ képe $\mathfrak{p} = P \cap \mathcal{O}_K$. Egy adott $0 \neq \mathfrak{p} \lhd \mathcal{O}_K$ prímideál ősképe ennél a leképezésnél nem más, mint a $\{P_1, \ldots, P_r\}$ halmaz, ahol $\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \ldots P_r^{e_r}$. Sőt, a P_i ősép multiplicitását értelmezhetjük e_i-nek. Továbbá, ha az $\mathcal{O}_K/\mathfrak{p}$ maradéktest algebrailag zárt (mint a fenti példában $\mathcal{O}_K/\mathfrak{p} = \mathbb{C}$), akkor $f_i = 1$ minden $i = 1, \ldots, r$-re, hiszen f_i a maradéktest bővítésének foka. Speciálisan a fundamentális egyenlet $n = \sum_{i=1}^{r} e_i$ alakba írható, azaz multiplicitással számolva minden pontnak pontosan n ősképe van. A fedés – akárcsak a Riemann-felületek elméletében – pontosan akkor elágazásmentes, ha minden $\mathfrak{p}$ ősképe n darab *különböző* pont, azaz $e_i = 1$, azaz a $\mathfrak{p}$ prímideál nem ágazik el $\mathcal{O}_L$-ben.

3.10.1. Elliptikus görbék és a Picard-csoport

A továbbiakban legyen $f(x, y) = y^2 - x^3 - ax - b$ egy elliptikus görbe egyenlete, azaz tegyük fel, hogy $V(f)$ nemszinguláris. Ez azzal ekvivalens, hogy az $x^3 + ax + b$ polinomnak nincs többszörös gyöke. Ekkor a 3.10.1. Állítás szerint $\mathcal{O} = \mathbb{C}[x, y]/(f(x, y))$ egy Dedekind gyűrű, melynek nemnulla prímideáljai megfelelnek $V(f) \subseteq \mathbb{C}^2$ pontjainak. Tehát $\mathcal{O}$ osztálycsoportja nem más, mint a $P \in V(f)$ pontokon, mint generátorokon értelmezett szabad Abel csoport egy faktorcsoportja, mégpedig $\sum n_i[P_i] = 0$, akkor és csak akkor, ha a $\prod P_i^{n_i}$ törtideál egy főideál. Mit jelent ez pontosan geometriai szempontból? Ez éppen azzal ekvivalens, hogy van olyan g racionális törtfüggvény a $V(f)$ görbén, melynek éppen n_i-szeres gyöke ($n_i < 0$ esetén $-n_i$-szeres pólusa) van a P_i pontban, és minden ezektől különböző $Q \neq P_i$ pontban g-nek sem pólusa sem gyöke nincs. Ez a definíció tehát nem más, mint az affin $V(f)$ görbe *Picard-csoportja*, mely ezek szerint izomorf az $\mathcal{O}$ Dedekind gyűrű osztálycsoportjával.

Ahhoz, hogy ezt az analógiát pontosabban megértsük (legalább elliptikus görbék esetén), a $V(f)$ görbét a $\mathbb{PC}^2$ projektív síkon kell tekintenünk, és ki kell egészítenünk egy „végtelen távoli" O ponttal. Tehát projektivizáljuk az f polinomot, és tekintsük az

$$f_0(x, y, z) = y^2 z - x^3 - axz^2 - bz^3 = 0$$

egyenletű görbét a projektív síkon. A végtelen távoli egyenes nem más, mint a $z = 0$ nullhelyeinek halmaza, ezen nyilván egyetlen O-val jelölt pontja van az $E := V(f_0) \subseteq \mathbb{PC}^2$ görbének, jelesül $O = [0 : 1 : 0]$.

3.10.2. Definíció. Jelöljük $\mathrm{Div}(E)$-vel az E görbe *divizorjainak* a csoportját, azaz az E pontjai által generált szabad Abel csoportot. Egy $D = \sum n_i[P_i] \in \mathrm{Div}(E)$ divizor *foka* $\deg(D) = \sum n_i \in \mathbb{Z}$ (ez mindig egy véges összeg). Legyen továbbá $\mathrm{Div}^0(E)$ a nulla fokú divizorok részcsoportja $\mathrm{Div}(E)$-ben.

Ha $g \in K(E)^\times$ egy nemnulla racionális törtfüggvény az E görbén (azaz két azonos fokú homogén polinom hányadosa), akkor $g\colon E \to \mathbb{PC}^1$ egy meromorf függvény. Belátható (lsd. pl. Prop. II.3.1 [12]), hogy ekkor g-nek multiplicitással számolva pontosan annyi pólusa van, mint gyöke. (Ebben a speciális esetben ez pl. abból következik, hogy a gyökök száma nem más, mint a 0 ősképének elemszáma (multiplicitással), a pólusok száma pedig ∞ ősképeinek a száma, és ezek mindegyike megegyezik e g leképezés fokával.) Jelöljük $\mathrm{div}(g) \in \mathrm{Div}^0(E)$-vel

a g-hez tartozó divizort, ahol

$$\operatorname{div}(g) := \sum_{P_i \ n_i\text{-szeres gyöke } g\text{-nek}} n_i[P_i] - \sum_{Q_j \ m_j\text{-szeres pólusa } g\text{-nek}} m_j[Q_j] \ .$$

Ekkor $\operatorname{div}\colon K(E)^\times \to \operatorname{Div}^0(E)$ egy csoporthomomorfizmus, hiszen g_1g_2 gyökei és pólusai épp g_1 ill. g_2 gyökeiből és pólusaiból állnak (megfelelő multiplicitással). A div homomorfizmus képének elemeit nevezzük a fődivizoroknak (vagy principális divizoroknak). Az E görbe 0-fokú divizorosztálycsoportja definíció szerint div komagja, azaz $\operatorname{Pic}^0(E) := \operatorname{Div}^0(E)/\operatorname{Im}(\operatorname{div})$. Azt mondjuk, hogy két $D_1, D_2 \in \operatorname{Div}^0(E)$ divizor *lineárisan ekvivalens* (jel.: $D_1 \sim D_2$), ha $D_1 - D_2$ fődivizor, azaz ha D_1-nek és D_2-nek ugyanaz az osztálya $\operatorname{Pic}^0(E)$ csoportban. Vegyük észre, hogy div magja pedig a konstans függvények: hiszen ezek az egyetlen olyan függvények E-n, melyeknek sem gyöke, sem pólusa nincs (lsd. pl. Prop. II.3.1 [12]). összefoglalva a 3.3.11. Állítás analogonja ebben a szituációban, hogy a

$$1 \to \mathbb{C}^\times \to K(E)^\times \stackrel{\operatorname{div}}{\to} \operatorname{Div}^0(E) \to \operatorname{Pic}^0(E) \to 0$$

sorozat egzakt.

3.10.3. Állítás. *A* $\operatorname{Pic}^0(E)$ *csoport izomorf az affin* $\operatorname{Pic}(V(f)) = Cl(\mathcal{O})$ *csoporttal.*

Bizonyítás vázlat. Valóban, ha $\sum n_i[P_i] \in \operatorname{Div}(V(f))$, akkor ehhez hozzárendelhetjük a

$$\sum n_i[P_i] - \sum n_i[O] \in \operatorname{Div}^0(E)$$

divizort. Ez a – továbbiakban φ-vel jelölt – leképezés fődivizorhoz nyilván fődivizort rendel, hiszen ha $g\colon V(f) \to \mathbb{PC}^1$ egy racionális törtfüggvény, akkor azt ki lehet terjeszteni a végtelen távoli O pontba is (ez egyáltalán nem triviális, de igaz). Az O pontban annyiszoros gyöke vagy pólusa lesz a kiterjesztésnek, hogy a kapott divizor foka 0 legyen. Tehát φ megad egy $\overline{\varphi}\colon \operatorname{Pic}(V(f)) \to \operatorname{Pic}^0(E)$ csoporthomomorfizmust. A szürjektivitás világos. Az injektivitáshoz pedig vegyük észre, hogy ha $\sum n_i[P_i] \in \operatorname{Ker}(\overline{\varphi})$, akkor $\sum n_i[P_i] - \sum n_i[O] = \operatorname{div}(g)$ egy $g\colon E \to \mathbb{PC}^1$ függvényre, de ekkor ha $\tilde{g}\colon V(f) \to \mathbb{PC}^1$ a g megszorítása $V(f) \subset E$-re, akkor $\sum n_i[P_i] = \operatorname{div}(\tilde{g})$ is fődivizor (ez viszont lényegében triviális). □

Ha E egy elliptikus görbe, akkor valójában $\operatorname{Pic}^0(E)$ azonosítható az E görbe pontjainak halmazával. Az azonosítás a következő: egy P ponthoz az E görbén rendeljük hozzá a $[P] - [O] \in \operatorname{Div}^0(E)$ divizor osztályát $\operatorname{Pic}^0(E)$-ben. Ahhoz, hogy belássuk, hogy ez a leképezés egy bijekció, szükségünk lesz a Riemann-Roch tételre.

3.10.4. Definíció. Egy $D = \sum n_P[P] \in \operatorname{Div}(E)$ divizorról azt mondjuk, hogy pozitív (vagy effektív), ha $n_P \geq 0$ minden $P \in E$ pontra. Továbbá $D_1, D_2 \in \operatorname{Div}(E)$ esetén $D_1 \geq D_2$ akkor és csak akkor, ha $D_1 - D_2$ pozitív.

Ha D egy divizor, akkor legyen $\mathcal{L}(D) := \{f \in K(E)^\times \mid \operatorname{div}(f) \geq -D\} \cup \{0\}$. Ez egy vektortér $\mathbb{C}$ fölött, mely minden esetben véges dimenziós. Az is világos, hogy ha $0 \neq -D \geq 0$, akkor $\mathcal{L}(D) = \{0\}$, hiszen minden fődivizor 0 fokú.

3.10.5. Tétel (Riemann-Roch elliptikus görbékre)**.** *Ha* $\deg(D) \geq 1$*, akkor* $\dim \mathcal{L}(D) = \deg(D)$.

Bizonyítás. Megtalálható a [6] könyvben (IV. §1). □

3.10.6. Állítás. *A*

$$\begin{aligned} E &\to \mathrm{Pic}^0(E) \\ P &\mapsto [P]-[O] \end{aligned} \tag{3.5}$$

leképezés egy bijekció.

Bizonyítás. A Riemann-Roch tétel speciális esete, hogy ha $D=[P]$, akkor $\dim \mathcal{L}(D)=1$. Viszont a konstans függvények nyilván benne vannak $\mathcal{L}(D)$-ben, hiszen $\mathcal{L}(D)$ elemei azon függvények, melyeknek csak P-ben lehet pólusa, és ott is maximum 1-szeres. Speciálisan ha $P_1\neq P_2$ pontok, akkor $[P_1]-[P_2]$ *nem* lehet fődivizor, hiszen akkor egy $\mathcal{L}([P_2])$-beli függvénynek lenne a divizora, de $\mathcal{L}([P_2])$-ben csak a konstans függvények vannak, melyek divizora nyilván 0. Ez pont azt jelenti, hogy a (3.5) leképezés injektív.

A szürjektivitáshoz azt kell belátnunk, hogy a $\mathrm{Pic}^0(E)$ csoportban minden elem reprezentálható egy $[P]-[O]$ alakú elemmel. Mivel a $[P]-[O]$ alakú elemek nyilván generálják $\mathrm{Pic}^0(E)$-t, ezért elég belátnunk, hogy részcsoportot alkotnak. Ehhez két dolgot kell belátnunk: egyrészt minden $P\in E$-hez van olyan $P'\in E$, melyre $[O]-[P]\sim[P']-[O]$. Ehhez szükségünk van egy olyan $g\in K(E)^\times$ függvényre, melyre $\mathrm{div}(g)=[P]+[P']-2[O]$. Node a Riemann-Roch tétel szerint $\dim\mathcal{L}(2[O]-[P])=1$, tehát van olyan – nem azonosan 0 – $g\in K(E)^\times$ függvény, mely eltűnik P-ben, és legfeljebb 2-szeres pólusa van O-ban, máshol pedig nincs pólusa. Speciálisan ez a függvény nemkonstans (hiszen P-ben 0, de nem mindenhol), ezért az O pontban pontosan kétszeres a pólusa (hiszen a fenti gondolatmenet miatt egyszeres nem lehet). Mivel $\mathrm{div}(g)$ foka 0, ezért pontosan egy zérushelye van még P-n kívül (vagy a P-beli zérushely kétszeres), azaz létezik egy ilyen $P'\in E$. Ezzel azt láttuk be, hogy minden $[P]-[O]$ alakú elem inverze is ilyen alakú $\mathrm{Pic}^0(E)$-ben. Másrészt ha $P_1,P_2\in E$, akkor kell, hogy van olyan $P_3\in E$, melyre $[P_1]-[O]+[P_2]-[O]\sim[P_3]-[O]$. Ehhez vegyük észre, hogy a $D=[P_1]+[P_2]-[O]$ divizor is 1 fokú, tehát van olyan $g\in K(E)^\times$ függvény, melynek maximum 1-szeres pólusa van a P_1 és P_2 pontokban (illetve maximum kétszeres a P_1 pontban, ha $P_1=P_2$), és eltűnik az O pontban. A fenti érveléshez hasonlóan g-nek kell lennie még egy P_3 zérushelyének (lehet persze $P_3=O$ is, ez esetben az O pontban kétszeres gyöke van g-nek). □

A fenti tételt úgy is interpretálhatjuk, hogy az E görbe pontjain értelmeztünk egy Abel-csoport műveletet. Valóban, $\mathrm{Pic}^0(E)$ egy Abel-csoport, melyet azonosítottunk E-vel. Az összeadás nulleleme az O végtelen távoli pont. Vegyük észre, hogy egy egyenes multiplicitással számolva mindig pontosan 3 pontban metszi az E görbét. Ez Bézout tételének speciális esete, de közvetlen számolással is látszik: a metszéspontok meghatározásához egy harmadfokú egyenletet kell megoldanunk.

3.10.7. Állítás. *Két pont (P és Q) összegét a következőképpen kell meghatározni: a P és Q pontokat összekötő egyenes pontosan egy R pontban metszi még az E görbét (multiplicitással számolva). Kössük össze R-et a végtelen távoli O ponttal; ez az egyenes egy harmadik S pontban is metszi a görbét. Ekkor a P és Q pontok összege az S pont, azaz* $([P]-[O])+([Q]-$ $-[O])\sim[S]-[O]$.

Bizonyítás. Legyen L_1 a P, Q, R pontokon átmenő egyenes (homogén) egyenlete, L_2 pedig az O, S, R pontokon átmenő egyenes egyenlete. Ekkor $L_1/L_2 \in K(E)^\times$ egy olyan racionális törtfüggvény a görbén, melynek a P és Q pontban gyöke, az O és S pontban pólusa van – mindenhol máshol pedig nemnulla és reguláris. Tehát $[P] + [Q] \sim [O] + [S]$. □

3.10.8. Megjegyzés. A Riemann-Roch tétel igaz más – nem feltétlen elliptikus – sima görbékre is. Az $\mathcal{L}(D)$ vektortér dimenzióját meghatározó formula ezekre a görbékre bonyolultabb, kimondásához szükségünk lenne a differenciálformák, illetve a görbe génuszának definíciójára. Sőt, ha C egy tetszőleges sima projektív görbe, akkor $\mathrm{Pic}^0(C)$ szintén azonosítható egy algebrai varietással: ez lesz a C görbe Jacobi-varietása, melyen természetes módon van egy Abel-csoport struktúra. Az így kapott algebrai varietásokat Abel-féle varietásoknak nevezzük – ezek az elliptikus görbék magasabb dimenziós általánosításai. Akit érdekel a téma, a [9] jegyzetben olvashat erről többet.

3.10.9. Megjegyzés. Ha E egy esetleg szinguláris, harmadfokú görbe, akkor is értelmezhető egy összeadás E *nemszinguláris* pontjainak halmazán, melyre nézve a nemszinguláris pontok Abel-csoportot alkotnak.

3.11. Miért körosztási testek?

Az algebrai számelméletben rendkívül fontos szerepet játszanak a körosztási testek, azaz a racionális számtest egységgyökökkel való bővítései. Egyrészt – ahogy látni fogjuk – a Fermat-sejtés egyes speciális eseteinek a bizonyítása is ezen bővítések számelméletét használja. Valóban, ha $2 < p$ egy prímszám, akkor az $x^p + y^p = z^p$ egyenletet $\mathbb{Q}(\zeta_p)$ fölött az $\prod_{i=0}^{p-1}(x + \zeta_p^i y) = z^p$ alakba írhatjuk (itt ζ_p egy primitív p-edik egységgyök). A 19. század végén hatalmas áttörésnek számított, hogy Ernst Kummer német matematikus belátta, hogy az $x^p + y^p = z^p$ egyenletnek nincs az egészek körében nemtriviális megoldása, ha p egy ún. *reguláris prím*, azaz ha p nem osztja a $\mathbb{Q}(\zeta_p)$ test osztályszámát. A matematikatörténészek azt valószínűsítik, hogy Fermat „csodálatos bizonyítása", ami nem fért ki a margóra is ezen az ötleten alapulhatott, melynek során Fermat – hibásan – feltette, hogy a számelmélet alaptétele igaz a $\mathbb{Q}(\zeta_p)$ testben is. Sajnos ezt a módszert azóta sem sikerült általánosítani irreguláris prímekre – Wiles bizonyítása a Fermat sejtésre más módszeren alapszik: ha $x^p + y^p = z^p$-nek lenne egy nemtriviális megoldása, akkor létezne egy bizonyos tulajdonságokkal rendelkező elliptikus görbe. Wiles moduláris formák segítségével azt látta be, hogy ilyen nagyon speciális tulajdonságokkal rendelkező elliptikus görbék nem léteznek.

Ami a reguláris prímeket illeti, Jensen 1915-ben belátta, hogy végtelen sok irreguláris prím van (a legkisebb egyébként a 37), speciálisan végtelen sok körosztási testben sérül az elemekre a számelmélet alaptétele. Az viszont máig megoldatlan, hogy végtelen sok reguláris prím van-e. Siegel sejtése, hogy igen, sőt azt sejti Siegel, hogy a reguláris prímek aszimptotikus sűrűsége a prímek között $\frac{1}{\sqrt{e}}$.

Ernst Kummer bámulatos észrevétele volt az is, hogy az, hogy egy p prímszám reguláris-e, leolvasható az úgynevezett B_k Bernoulli számokról. A Bernoulli számoknak több ekvivalens definíciója létezik, a legegyszerűbb talán a következő generátorfüggvényes:

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!} \ .$$

Az már ebből a definícióból is világos, hogy a B_k számok racionálisak. Kummer azt látta be, hogy p pontosan akkor reguláris prím, ha p nem osztja a B_k Bernoulli szám egyszerűsített alakjának számlálóját semmilyen $k = 2,4,\dots,p-3$ páros számra sem. Vegyük észre, hogy

$$\sum_{k=0}^{\infty} B_k(-1)^k \frac{t^k}{k!} = \frac{-t}{e^{-t}-1} = \frac{te^t}{e^t-1} = t + \sum_{k=0}^{\infty} B_k \frac{t^k}{k!} \ .$$

Tehát $B_{2n+1} = 0$, ha $n \geq 1$.

Egy viszonylag mély összefüggés viszont a Bernoulli számok kapcsolata a Riemann-féle ζ-függvénnyel – melyet a ζ-függvény függvényegyenletéből és a Γ-függvény tulajdonságaiból lehet levezetni. Jelöljük $\zeta(s)$-sel a Riemann-féle ζ-függvényt: ha $\mathrm{Re}(s) > 1$, akkor $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Ennek létezik analitikus folytatás az $s = 1$ egyszeres pólustól eltekintve az egész komplex síkra. Ekkor minden $n \geq 1$-re

$$\zeta(1-n) = -\frac{B_n}{n} \ . \tag{3.6}$$

Speciálisan a Riemann ζ-nak zérushelye van a negatív páros számokban. Ezek a ζ-függvény úgynevezett triviális gyökei. A Riemann-sejtés szerint ezeken kívül csak a $\mathrm{Re}(s) = \frac{1}{2}$ függőleges egyenesen vannak a ζ-függvény gyökei. A fenti formulából – a ζ-függvény függvényegyenletének segítségével – az is következik, hogy ha $n \geq 1$ egész, akkor

$$\zeta(2n) = (-1)^{n+1} \frac{(2\pi)^{2n}}{2 \cdot (2n)!} B_{2n} \ .$$

Speciálisan ezek a függvényértékek mind transzcendensek.

A (3.6) formulát kombinálva Kummer észrevételével azt kapjuk, hogy a ζ-függvény speciális értékeiről leolvasható információ a körosztási testek osztályszámáról. Erre a jelenségre épül az Iwasawa-elmélet is, ami a ζ-függvény, vagy általánosabban bizonyos L-függvények speciális értékeiből próbál aritmetikai információt kinyerni. A kiindulópont a következő – szintén Kummer nevéhez fűződő – kongruenciák a Bernoulli-számokra:

$$(1-p^{k-1})\zeta(1-k) = (p^{k-1}-1)\frac{B_k}{k} \equiv (p^{l-1}-1)\frac{B_l}{l} = (1-p^{l-1})\zeta(1-l) \pmod{p^n} \ , \tag{3.7}$$

ha $p-1 \nmid k \equiv l \pmod{\varphi(p^n)}$, ahol $\varphi(p^n) = p^{n-1}(p-1)$ az Euler-féle φ-függvény. Ezt úgy kell érteni, hogy a két oldalon álló racionális számok nevezője nem osztható p-vel, ezért tekinthetjük mindkét oldalt modulo p^n. A fenti kongruenciát úgy is interpretálhatjuk, hogy az $(1-p^{-s})\zeta(s)$-függvényt a negatív egész számokról ki lehet terjeszteni folytonosan

$$(\mathbb{Z}/(p-1) \setminus \{0\}) \times \varprojlim_n \mathbb{Z}/(p^{n-1}) = (\mathbb{Z}/(p-1) \setminus \{0\}) \times \mathbb{Z}_p \text{ -re,}$$

azaz a p-adikus számok $p-2$ példányára. (Ez a $(p-2)$ darab kiterjesztés olyasmi, mint a komplex test fölött a négyzetgyökfüggvény két ága. A p-adikus számok definícióját lásd a következő fejezetben.) Mivel

$$\zeta(s) = \prod_{q \text{ prím}} \frac{1}{1-q^{-s}} \ ,$$

ezért az $(1-p^{-s})\zeta(s)$ szorzat nem más, mint a módosított ζ-függvény, ahol a p-hez tartozó Euler-faktort kihagyjuk a szorzattábontásból. Ez a p-adikus kiterjesztés az úgynevezett p-adikus ζ-függvény, amely rengeteg aritmetikai információt hordoz.

A következő heurisztikus gondolatmenet szigorúan véve teljesen hibás, és nem is lehet ilyen formában precízzé tenni, de mégis rámutat arra, hogyan lehet egy ilyen Kummer-féle kongruenciát megsejteni. Induljunk ki az

$$(1-p^{-s})\zeta(s) = \prod_{q\neq p \text{ prím}} \frac{1}{1-q^{-s}} = \sum_{1\leq n,(n,p)=1} \frac{1}{n^s}$$

formulából. Vegyük észre, hogy az Euler-Fermat tétel értelmében (mivel feltettük, hogy $(n,p) = 1$)

$$\text{ha} \quad k \equiv l \pmod{\varphi(p^n)} \quad , \text{ akkor} \quad n^k \equiv n^l \pmod{p^n} \ .$$

Ha ennek a végtelen sok kongruenciának a reciprokát összeadjuk, akkor

$$(1-p^{-k})\zeta(k) \equiv (1-p^{-l})\zeta(l)$$

adódik. Sajnos ezzel a gondolatmenettel több bökkenő is van:

(1) egyrészt miért lehetne összeadni végtelen sok kongruenciát;

(2) másrészt ha k és l pozitív egészek, akkor $\zeta(k)$, ill. $\zeta(l)$ nem racionális, de még csak nem is algebrai szám – mi értelme lenne akkor egy ilyen kongruenciának?;

(3) harmadrészt ha viszont negatív egész k-t és l-et veszünk (ilyenkor $\zeta(k)$ és $\zeta(l)$ valóban racionális), és az (1)-es számú problémával valamilyen csodával határos módon megbírkózunk, akkor pedig az a baj, hogy a $\sum_{1\leq n,(n,p)=1} \frac{1}{n^k}$ összeg nem konvergál.

Annál inkább bámulatos, hogy a (3.7) kongruenciák mégis teljesülnek (legalábbis, ha $p-1 \nmid k$)! Akit érdekel a téma a [2] könyvben olvashat utána.

3.12. Körosztási testek

3.12.1. Definíció. Az n-edik körosztási testnek a $\mathbb{Q}(\zeta_n)$ testet nevezzük, ahol ζ_n egy primitív n-edik egységgyök.

A következő technikai Lemma készíti elő prímhatvány n-re az n-edik körosztási test egész bázisát.

3.12.2. Lemma. *Legyen ℓ egy prímszám és $\lambda = 1-\zeta_{\ell^r} =: 1-\zeta$. Jelöljük továbbá $\mathcal{O}_{\ell^r}$-nel az egészek gyűrűjét $\mathbb{Q}(\zeta)$-ban. Ekkor*

$$\ell\mathcal{O}_{\ell^r} = (\lambda)^m \ ,$$

ahol $m = \varphi(\ell^r) = (\ell-1)\ell^{r-1} = |\mathbb{Q}(\zeta):\mathbb{Q}|$. Speciálisan ℓ egy prímideál, melynek inerciafoka 1, azaz ℓ teljesen elágazik $\mathbb{Q}(\zeta)$-ban, és $\mathcal{O}_{\ell^r}/(\lambda) = \mathbb{F}_\ell$. Továbbá az $1,\zeta,\ldots,\zeta^{d-1}$ bázis diszkriminánsa $d = \pm\ell^s$, ahol $s = \ell^{r-1}(r\ell-r-1)$.

Bizonyítás. Legyen $\Phi_{\ell^r}(x) = \sum_{j=0}^{\ell-1} x^{\ell^{r-1}j}$ az ℓ^r-edik körosztási polinom. Mivel ez irreducibilis ([7] 3.9.9. Tétel), ezért ez ζ minimálpolinomja $\mathbb{Q}$ fölött. Másrészt

$$\ell = \Phi_{\ell^r}(1) = \prod_{g\in(\mathbb{Z}/\ell^r\mathbb{Z})^\times} (1-\zeta^g) \ ,$$

ahol $1-\zeta^g$ minden g-re λ egységszerese. Valóban, ha $g^{-1}+\ell^r\mathbb{Z} \in (\mathbb{Z}/\ell^r\mathbb{Z})^\times$ a g inverze a multiplikatív csoportban valamilyen $1 \le g^{-1} \in \mathbb{Z}$ számra, akkor

$$\varepsilon_g = \frac{1-\zeta^g}{1-\zeta} = 1+\zeta+\cdots+\zeta^{g-1} \in \mathcal{O}_{\ell^r}$$
$$\varepsilon_g^{-1} = \frac{1-\zeta^{gg^{-1}}}{1-\zeta^g} = 1+\zeta^g+\cdots+\zeta^{g(g^{-1}-1)} \in \mathcal{O}_{\ell^r} \ ,$$

azaz $\varepsilon_g \in \mathcal{O}_{\ell^r}^\times$. Speciálisan azt kaptuk, hogy $\ell\mathcal{O}_{\ell^r} = (\lambda)^{\varphi(\ell^r)}$. Tehát ebben a speciális esetben az e elágazási index megegyezik a $\varphi(\ell^r)$ fokszámmal, ezért a fundamentális egyenlet (3.8.3. Tétel) miatt az ℓ prím teljesen elágazik, azaz $f=1$.

A diszkriminánsról szóló állításhoz vegyük észre, hogy $d(1,\zeta,\dots,\zeta^{m-1})$ egy Vandermonde típusú determináns négyzete, azaz ha $\zeta=\zeta_1,\dots,\zeta_m$ jelöli ζ Galois-konjugáltjait (azaz jelen esetben az összes primitív ℓ^r-edik egységgyököt), akkor

$$d = \prod_{i<j}(\zeta_i-\zeta_j)^2 = \pm\prod_{i\ne j}(\zeta_i-\zeta_j) = \prod_{i=1}^{m}\Phi'_{\ell^r}(\zeta_i) = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\Phi'_{\ell^r}(\zeta)) \ .$$

A $(x^{\ell^{r-1}}-1)\Phi_{\ell^r}(x) = x^{\ell^r}-1$ egyenletet lederiválva és ζ-t behelyettesítve azt kapjuk, hogy

$$(\zeta^{\ell^{r-1}}-1)\Phi'_{\ell^r}(\zeta) = \ell^r\zeta^{-1} \ .$$

Itt ζ^{-1} egy egység, tehát normája ±1, ugyanakkor

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{\ell^{r-1}}-1) = N_{\mathbb{Q}(\zeta^{\ell^{r-1}})/\mathbb{Q}}(\zeta^{\ell^{r-1}}-1)^{|\mathbb{Q}(\zeta):\mathbb{Q}(\zeta^{\ell^{r-1}})|} = \pm\ell^{\ell^{r-1}} \ ,$$

hiszen $\zeta^{\ell^{r-1}}$ egy ℓ-edik egységgyök, ezért $\zeta^{\ell^{r-1}}-1$ normája előjeltől eltekintve $\Phi_\ell(x+1)$ konstans tagja, azaz $\pm\ell$. Behelyettesítve adódik a d-re vonatkozó állítás. □

3.12.3. Állítás. *Ha ℓ^r egy tetszőleges prímhatvány, akkor $\mathcal{O}_{\ell^r}$-ben $1,\zeta,\dots,\zeta^{\varphi(\ell^r)-1}$ egész bázist alkot. Másszóval $\mathcal{O}_{\ell^r} = \mathbb{Z}[\zeta]$.*

Bizonyítás. A 3.12.2. Lemmát kombinálva a 3.2.4. Állítással azt kapjuk, hogy

$$\ell^s\mathcal{O}_{\ell^r} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\ell^r}$$

Másrészt a 3.12.2. Lemma első része szerint $\mathcal{O}_{\ell^r}/\lambda\mathcal{O}_{\ell^r} = \mathbb{Z}/\ell\mathbb{Z}$, azaz $\mathcal{O}_{\ell^r} = \mathbb{Z}+\lambda\mathcal{O}_{\ell^r}$, speciálisan $\mathcal{O}_{\ell^r} = \mathbb{Z}[\zeta]+\lambda\mathcal{O}_{\ell^r}$. Utóbbi egyenletet λ-val szorozva azt kapjuk, hogy $\lambda\mathcal{O}_{\ell^r} = \lambda\mathbb{Z}[\zeta] + \lambda^2\mathcal{O}_{\ell^r} \subseteq \mathbb{Z}[\zeta]+\lambda^2\mathcal{O}_{\ell^r}$. Tehát a két egyenletet összevetve $\mathcal{O}_{\ell^r} = \mathbb{Z}[\zeta]+\lambda^2\mathcal{O}_{\ell^r}$, és így tovább indukcióval $\mathcal{O}_{\ell^r} = \mathbb{Z}[\zeta]+\lambda^{ds}\mathcal{O}_{\ell^r} = \mathbb{Z}[\zeta]+\ell^s\mathcal{O}_{\ell^r} = \mathbb{Z}[\zeta]$. □

A következő célunk annak igazolása, hogy a 3.12.3. Állítás nemcsak prímhatványokra, hanem tetszőleges egész számra igaz. Ehhez szükségünk lesz a következő – szintén technikai – technikai Lemmára.

3.12.4. Lemma. *Legyen $\mathcal{O}_K$ egy Dedekind gyűrű K hányadostesttel és legyenek $K \leq L \leq \overline{K}$ és $K \leq L' \leq \overline{K}$ véges Galois-bővítések, melyek foka n, ill. n', és $L \cap L' = K$. Legyen továbbá $w_1, \ldots, w_n$ egy egész bázis $\mathcal{O}_L$-ben, $w'_1, \ldots, w'_{n'}$ pedig egy egész bázis $\mathcal{O}_{L'}$-ben d, ill. d' diszkriminánssal. Tegyük fel továbbá, hogy $(d, d') = \mathcal{O}_K$ (relatív prímek). Ekkor $\{w_i w'_j \mid 1 \leq i \leq n, 1 \leq j \leq n'\}$ egy egész bázisa $\mathcal{O}_{LL'}$-nek. Továbbá LL'-ben pontosan azok a K-beli prímek ágaznak el, melyek L-ben vagy L'-ben elágaznak.*

Bizonyítás. Először is az LL' kompozíció is egy Galois-bővítés, hiszen normális és szeparábilis. Tehát $\mathrm{Gal}(LL'/L)$ és $\mathrm{Gal}(LL'/L')$ két normálosztó $\mathrm{Gal}(LL'/K)$-ban (hiszen fixtestük Galois), melyek metszete csak az egységelem, hiszen ha egy automorfizmus L-et és L'-t is fixen hagyja, akkor a kompozíciójukat is. Továbbá a Galois-elmélet főtétele szerint ([7] 6.6.7. Tétel) a két normálosztó által generált részcsoportnak $K = L \cap L'$ felel meg, azaz $\mathrm{Gal}(LL'/K) \cong \mathrm{Gal}(LL'/L) \times \mathrm{Gal}(LL'/L')$, speciálisan $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(LL'/L')$, így $|LL' : K| = nn'$. Tehát $\{w_i w'_j\}$ egy bázis LL'-ben, mint K fölötti vektortérben, hiszen triviálisan generátorrendszer, és nn' elemű.

Az is világos, hogy $w_i w'_j$ minden i, j-re egész $\mathcal{O}_K$ fölött, hiszen az egész elemek részgyűrűt alkotnak. Azt kell még belátnunk, hogy $\alpha \in \mathcal{O}_{LL'}$ esetén az

$$\alpha = \sum_{i,j} a_{i,j} w_i w'_j \tag{3.8}$$

előállításban az $a_{i,j} \in K$ számok $\mathcal{O}_K$-ban vannak. Legyen $\beta_j = \sum_i a_{i,j} w_i \in L$ és $\mathrm{Gal}(LL'/L) = \{\sigma'_1, \ldots, \sigma'_{n'}\}$. Tekintsük továbbá az $X = ((\sigma'_l w'_j)) \in L'^{n' \times n'}$ mátrixot, illetve az $a = (\sigma'_1 \alpha, \ldots, \sigma'_{n'} \alpha)^T \in (LL')^n$ és a $b = (\beta_1, \ldots, \beta_{n'}) \in L^{n'}$ vektorokat. Ekkor a (3.8) egyenlet miatt $a = Xb$, hiszen σ'_l fixen hagyja a b vektort. Továbbá a d' diszkrimináns definíciója szerint $\det(X)^2 = d'$. Tehát ha X^* jelöli az előjeles aldeterminánsokból álló mátrixot, akkor $\det(X) b = X^* a \in \mathcal{O}_{LL'}^{n'}$, speciálisan $d' a_{i,j} \in \mathcal{O}_K$, hiszen $\{w_i\}$ egy egész bázis $\mathcal{O}_L$-ben. Hasonlóan $d a_{i,j} \in \mathcal{O}_K$, tehát $a_{i,j} \in \mathcal{O}_K a_{i,j} = (d, d') a_{i,j} \subseteq \mathcal{O}_K$.

A második állításhoz egyrészt ha egy prím elágazik L-ben vagy L'-ben, akkor LL'-ben is, hiszen az elágazási indexek összeszorzódnak. Másrészt vegyük észre, hogy a 3.9.6. Megjegyzés miatt egy $0 \neq \mathfrak{p} \lhd \mathcal{O}_K$ prím pontosan akkor ágazik el LL'-ben, ha egy ($\Rightarrow$ az összes) $P \lhd \mathcal{O}_{LL'}$ prímre az I_P inerciarészcsoport $\mathrm{Gal}(LL'/K)$-ban nemtriviális. Továbbá I_P képe a $\mathrm{Gal}(LL'/K) \to \mathrm{Gal}(L/K)$ faktorleképezésnél nyilván benne van $P \cap \mathcal{O}_L$ inerciarészcsoportjában, hiszen egy $\sigma \in I_P$ elem a maradéktesten triviálisan hat. Viszont ha $\mathfrak{p}$ nem ágazik el L-ben, akkor $P \cap \mathcal{O}_L$ inerciarészcsoportja triviális, speciálisan I_P benne van ennek a faktorleképezésnek a magjában, $\mathrm{Gal}(LL'/L')$-ben. Hasonlóképp $I_P \leq \mathrm{Gal}(LL'/L)$, node $\mathrm{Gal}(LL'/L) \cap \cap \mathrm{Gal}(LL'/L') = \{1\}$, azaz $\mathfrak{p}$ nem ágazik el LL'-ben. □

3.12.5. Tétel. *Ha n egy tetszőleges pozitív egész akkor a $\mathbb{Q}(\zeta_n)$ körosztási test egészeinek gyűrűje $\mathcal{O}_n = \mathbb{Z}[\zeta_n]$. Speciálisan $1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}$ egész bázis.*

Bizonyítás. Legyen $n = \prod_{i=1}^r p_i^{\nu_i}$. Az r szerinti teljes indukcióval bizonyítjuk. Ha $r = 1$, akkor a 3.12.3. Állítás miatt $\mathcal{O}_{p_1^{r_1}}$-ben egész bázis a $\{1, \zeta_{p_1^{\nu_1}}, \ldots, \zeta_{p_1^{\nu_1}}^{\varphi(p_1^{\nu_1})-1}\}$ halmaz $d_1 = \pm \pm p_1^{s_1}$ diszkriminánssal, tehát ebben a bővítésben csak p_1 ágazik el a 3.8.6. Tétel szerint.

Továbbá ha $m = \frac{n}{p_1^{\nu_1}}$, akkor $\mathcal{O}_m$-re alkalmazhatjuk az indukciós feltevést és a 3.12.4. Lemma alkalmazásaként kapjuk, hogy $\mathcal{O}_n$-nek is létezik egységgyökökből álló egész bázisa. Valóban: $\mathcal{O}_m$ és $\mathcal{O}_{p_1^{\nu_1}}$ diszkriminánsai relatív prímek egymáshoz, hiszen d_1-nek csak p_1 a prímosztója, de ez a 3.12.4. Lemma második állítása és a 3.8.6. Tétel szerint nem ágazik el $\mathcal{O}_m$-ben. Speciálisan $\mathcal{O}_n = \mathbb{Z}[\zeta_n]$, hiszen minden n-edik egységgyök ζ_n egy hatványa. □

3.12.6. Következmény. *Egy p páratlan prím pontosan akkor ágazik el $\mathcal{O}_n$-ben, ha $p \mid n$, illetve a $p = 2$ prím pontosan akkor ágazik el $\mathcal{O}_n$-ben, ha $4 \mid n$. Továbbá ha p pontosan a ν-edik hatványon szerepel n prímtényezős felbontásában és f jelöli p rendjét $(\mathbb{Z}/\frac{n}{p^\nu})^\times$-ben, akkor p prímtényezős felbontása*

$$p\mathcal{O}_n = (P_1 \dots P_r)^{\varphi(p^\nu)}$$

szerkezetű, ahol $r = \frac{\varphi(n)}{f\varphi(p^\nu)}$, és $P_1, \dots, P_r$ különböző prímideálok f inerciafokkal.

Bizonyítás. Mivel $\mathcal{O}_n = \mathbb{Z}[\zeta_n]$, ezért elég a $\Phi_n(x)$ körosztási polinomot felbontani irreducibilisek szorzatára modulo p. Ez pedig a 6.7.20. Feladat [7]-ben kombinálva azzal az észrevétellel, hogy $\Phi_n(x) \equiv \Phi_{\frac{n}{p^\nu}}(x)^{\varphi(p^\nu)} \pmod p$. Ez utóbbi kongruencia teljes indukcióval következik a

$$\prod_{u|m} \Phi_u(x)^{p^\nu} = (x^m - 1)^{p^\nu} \equiv x^n - 1 = \prod_{d|n} \Phi_d(x) \pmod p$$

kongruenciából ($m = \frac{n}{p^\nu}$). Valóban, a bal oldalon $\Phi_m(x)$ kitevője p^ν, a jobb oldalon pedig minden $d = mp^k$ ($k < \nu$) esetén az indukciós feltevésből adódik egy $\Phi_m(x)^{\varphi(p^k)}$ tényező. Viszont $p^\nu - \sum_{k=0}^{\nu-1} \varphi(p^k) = \varphi(p^\nu)$.

A $p = 2$ esetet azért kellett különválasztanunk, mivel primitív második egységgyök már $\mathbb{Q}$-ban is van (jelesül a -1). Valóban, ha a $p = 2$ prím pontosan első hatványon szerepel n prímtényezős felbontásában, akkor a P_i prímideálok kitevője $\varphi(2) = 1$. □

3.12.7. Definíció. Egy K algebrai számtestet komplex szorzó testnek, vagy röviden CM testnek hívunk, ha K egy teljesen képzetes másodfokú bővítése egy teljesen valós $K^+ \leq K$ testnek.

3.12.8. Lemma. *A $\mathbb{Q}(\zeta_n)$ n-edik körosztási test egy CM test, ha $n \geq 3$. A teljesen valós részteste $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.*

Bizonyítás. Először is $\mathbb{Q}(\zeta_n)$ valóban teljesen képzetes, hiszen $\mathbb{R}$-ben nincsen n-edik egységgyök $n \geq 3$ esetén. Másrészt $\zeta_n + \zeta_n^{-1} = \zeta_n + \overline{\zeta_n} \in \mathbb{R}$. Sőt, $\zeta_n + \zeta_n^{-1}$ minden Galois-konjugáltja egy n-edik egységgyök és konjugáltjának összege, tehát valós. Tehát $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ minden $\mathbb{C}$-be való beágyazásának képe $\mathbb{R}$-ben van, azaz $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ teljesen valós. Végül ζ_n gyöke az $x^2 - x(\zeta_n + \zeta_n^{-1}) + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$ polinomnak, azaz $|\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})| = 2$. □

Ha K egy CM-test, akkor a K/K^+ bővítés másodfokú, speciálisan Galois. A Galois-csoport egyetlen nemtriviális elemét $\bar{\cdot}$-sal jelöljük a komplex konjugálás mintájára. Ha K-t a komplex számok egy résztestével azonosítjuk, akkor ez valóban a komplex konjugálás.

3.12.9. Állítás. *Ha K egy CM test és $u \in \mathcal{O}_K^\times$ egy egység az egészek gyűrűjében, akkor $u/\overline{u} \in \mathcal{O}_K^\times$ egy egységgyök.*

Bizonyítás. Belátjuk, hogy $u/\overline{u}$ minden Galois-konjugáltja 1 abszolútértékű. Ebből következik, hogy egységgyök, hiszen ekkor ez $u/\overline{u}$ összes hatványára is igaz, azaz a $\{j(u^k/\overline{u^k}) \mid k \in \in \mathbb{Z}\} \subset j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ halmaz korlátos. Node $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ diszkrét, ezért $\{j(\frac{u^k}{\overline{u^k}}) \mid k \in \mathbb{Z}\}$ egy véges halmaz. Speciálisan $u/\overline{u}$-nak csak véges sok hatványa van, azaz egységgyök.

Legyen $\tau\colon K \to \mathbb{C}$ egy tetszőleges injektív testhomomorfizmus. Mivel K egy CM test, ezért $\tau(K) \not\subset \mathbb{R}$, de $\tau(K^+) \subset \mathbb{R}$. Tehát a komplex konjugálás a $\tau(K)/\tau(K^+)$ testbővítés egyetlen nemtriviális automorfizmusa, speciálisan $\overline{\tau(u)} = \tau(\overline{u})$. Így $\tau(u/\overline{u}) = \tau(u)/\overline{\tau(u)}$ egy egységnyi abszolútértékű komplex szám. □

3.12.10. Következmény. *Ha K egy CM test, akkor az $\mathcal{O}_K^\times$ és $\mathcal{O}_{K^+}^\times$ Abel-csoportok rangja megegyezik.*

Bizonyítás. Jelöljük $\mu(K)$-val a K-testben levő egységgyökök csoportját. Az előző állítás szerint létezik egy

$$\begin{aligned} \mathcal{O}_K^\times &\to \mu(K) \\ u &\mapsto u/\overline{u} \end{aligned}$$

csoporthomomorfizmus. Vegyük észre, hogy ennek magja nem más, mint $\mathcal{O}_{K^+}^\times$, hiszen ezek pontosan azok az egységek, melyek megegyeznek a konjugáltjukkal, azaz valósak. Mivel a $\mu(K)$ csoport véges, ezért $\mathcal{O}_{K^+}^\times$ rangja megegyezik $\mathcal{O}_K^\times$ rangjával a végesen generált Abel-csoportok alaptétele miatt ([7] 7.4.1. Tétel). □

3.12.11. Következmény. *Ha p egy páratlan prím, akkor minden $u \in \mathcal{O}_{p^k}^\times$ felírható $u = \zeta^l v$ alakban, ahol $\zeta = \zeta_{p^k}$ egy primitív p^k-adik egységgyök, l egy egész szám, $v \in \mathbb{Z}[\zeta] \cap \mathbb{R}$ pedig valós.*

Bizonyítás. A 3.12.9. Állítás miatt $u/\overline{u}$ egy egységgyök. Node vegyük észre, hogy $\mathbb{Q}(\zeta)$-ban minden egységgyök rendje osztója $2p^k$-nak. Valóban, ha egy ε primitív n-edik egységgyök benne van $\mathbb{Q}(\zeta_{p^k})$-ban, akkor $\mathbb{Q}(\varepsilon) \subseteq \mathbb{Q}(\zeta_{p^k})$. Speciálisan $\mathbb{Q}(\zeta_{p^k})$-ban van $[n, p^k]$-adik (legkisebb közös többszörös) egységgyök is, azaz $\varphi([n, p^k]) \mid \varphi(p^k)$. Ekkor viszont $n \mid 2p^k$ (pl. a φ explicit képletéből).

Belátjuk, hogy valójában $u/\overline{u}$ egy p^k-adik egységgyök. Először is u-t írjuk fel $u = a_0 + a_1\zeta + \\ + \cdots + a_{\varphi(p^k)-1}\zeta^{\varphi(p^k)-1}$ alakban ($a_i \in \mathbb{Z}$, $i = 0,1,\ldots,\varphi(p^k)-1$). Ekkor $\overline{u} = \sum_{i=0}^{\varphi(p^k)-1} a_i\zeta^{-i} \equiv u \pmod{\zeta - 1}$. Speciálisan $u/\overline{u} \equiv 1 \not\equiv -1 \pmod{\zeta - 1}$. Tehát a ha μ_{2p^k} jelöli a $2p^k$-adik egységgyökök csoportját, akkor a -1, azaz az egyetlen másodrendű elem nincs benne a

$$\begin{aligned} \mathcal{O}_{p^k}^\times &\to \mu_{2p^k} \\ u &\mapsto u/\overline{u} \end{aligned}$$

homomorfizmus képében. Tehát a képben nincs másodrendű elem, azaz minden elem p^k-adik egységgyök. Mivel p^k páratlan, ezért minden p^k-adik egységgyök felírható egy p^k-adik egységgyök négyzeteként, azaz alkalmas $l \in \mathbb{Z}$-re $u/\overline{u} = \zeta^{2l} = \zeta^l/\overline{\zeta^l}$. Azaz $v := u/\zeta^l \in \mathbb{R}$. □

3.12.1. A Fermat-sejtés első esete reguláris prímekre

Illusztrációként belátjuk a Fermat-sejtés első esetét reguláris prímekre.

3.12.12. Tétel. *Legyen p egy reguláris prím, azaz p nem osztja $\mathbb{Q}(\zeta_p)$ osztályszámát. Ekkor az $x^p + y^p = z^p$ egyenletnek az egész számok körében nincs olyan megoldása, melyre $p \nmid xyz$.*

3.12.13. Megjegyzés. A fenti egy kissé gyengébb eredmény, mint a Fermat sejtés a p kitevőre, hiszen elvileg lehetne olyan nemtriviális megoldás is, melyben p osztja az x, y, z számok valamelyikét. Hasonló módszerrel ezt is ki lehet zárni, de ettől a jelen jegyzetben eltekintünk, mivel egyrészt sok számolást igényelne, másrészt szükség van Kummer alábbi lemmájára:

3.12.14. Lemma (Kummer)**.** *Legyen p egy reguláris prím és $u \in \mathbb{Z}[\zeta_p]^\times$ egy olyan egység, melyre van olyan $a \in \mathbb{Z}$, hogy $u \equiv a \pmod{p}$. Ekkor u egy p-edik hatvány, azaz van olyan $v \in \mathbb{Z}[\zeta_p]^\times$, amire $u = v^p$.*

A fenti lemmának többféle bizonyítása van. Az egyik [1] azon alapul, hogy ha u p-edik gyökével bővítjük $\mathbb{Q}(\zeta)$-t, akkor az egy olyan Galois-bővítés lesz, melynek Galois-csoportja p-rendű ciklikus (vagy ha u eleve p-edik hatvány, akkor triviális), ráadásul egyetlen $\mathbb{Q}(\zeta_p)$-beli prím sem ágazik el benne (utóbbit belátni nehéz). Viszont az *osztálytest-elmélet* szerint ekkor ennek a bővítésnek a foka osztaná az osztályszámot, ami ellentmond p regularitásának. Az osztálytest-elmélet lényegében a Kronecker–Weber tétel (5.2.1. Tétel) általánosítása $\mathbb{Q}$ véges bővítéseire. Egy másik bizonyítása a Kummer lemmának p-adikus analízist használ és a reguláris prímek Bernoulli számokon keresztüli definícióját [4]. A Fermat-sejtés második esetének bizonyítása a Kummer lemma segítségével hasonló jellegű, mint az első eset bizonyítása és megtalálható Keith Conrad jegyzetében [3].

A $p = 3$ esetben a teljes bizonyítás megtalálható a [5] könyvben (7.7.10. Tétel). Ebben az esetben a $\mathbb{Q}(\zeta_3)$ testben igaz a számelmélet alaptétele, ezért fogalmilag könnyebb a bizonyítás. Ebben a könyvben szintén megtalálható a Fermat-sejtés egy elemi bizonyítása a 4 kitevőre (7.7.2. Tétel – ez utóbbi egyébként valóban Fermat tétele: odafért a margóra a bizonyítás).

Bizonyítás. Először a $p = 3$ és a $p = 5$ eseteket intézzük el. Ha $p = 3$, akkor egy 3-mal nem osztható egész szám köbe csak ± 1 maradékot adhat 9-cel osztva, ezért két köbszám összege csak ± 2 vagy 0 lehet modulo 9, tehát nem lehet ± 1. Hasonlóképp a $p = 5$ esetben egy 5-tel nem osztható egész szám ötödik hatványa $\pm 1, \pm 7$ maradékot adhat 25-tel osztva, ezért két ötödik hatvány összege csak $0, \pm 2, \pm 6, \pm 8$ lehet modulo 25, azaz nem lehet ötödik hatvány.

A továbbiakban legyen $p > 5$. Az esetleges közös osztó p-edik hatványával leosztva feltehetjük, hogy az x, y, z számok páronként relatív prímek, hiszen ha kettőjüknek lenne közös osztója, az osztaná a harmadikat is. Vegyük észre továbbá, hogy esetleges változócsere után feltehetjük, hogy $p \nmid x - y$. Valóban, ha $x \equiv y \pmod{p}$, de $x \not\equiv -z \pmod{p}$, akkor az egyenletet átrendezhetjük úgy, hogy $x^p + (-z)^p = (-y)^p$. Az viszont nem lehet, hogy $x \equiv y \equiv -z \pmod{p}$, hiszen ekkor $p \mid 3z^p$ ellentmond a $p > 3$ és $p \nmid xyz$ feltevéseknek. Az egyenletet $\mathcal{O}_p = \mathbb{Z}[\zeta_p] = \mathbb{Z}[\zeta]$-ban szorzattáalakíthatjuk a következőképpen:

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = z^p \ .$$

Jelöljük $\mathfrak{p} = (1 - \zeta)$-val az egyetlen p fölötti prímet $\mathcal{O}_p$-ben.

3.12.15. Lemma. *Az $x + \zeta^i y$ számok páronként relatív prímek az $\mathcal{O}_p$ gyűrűben.*

Bizonyítás. Tegyük fel, hogy van egy olyan $\mathfrak{q}$ prímideál, melyre $x+\zeta^i y, x+\zeta^j y \in \mathfrak{q}$ valamilyen $0 \leq i \neq j \leq p-1$-re. Ekkor $(x+\zeta^i y)-(x+\zeta^j y) = y(\zeta^i-\zeta^j) \in \mathfrak{q}$ és $\zeta^j(x+\zeta^i y)-\zeta^i(x+\\ +\zeta^j y) = x(\zeta^j-\zeta^i) \in \mathfrak{q}$. Mivel $(x,y)=1$ és $\zeta^i-\zeta^j$ a $\mathfrak{p}$ egy generátoreleme, ezért csak $\mathfrak{q}=\mathfrak{p}$ lehet. Node $x+\zeta^i y \equiv x+y \pmod{\mathfrak{p}}$, de $p \nmid x+y$, hiszen egyébként $p \mid x^p+y^p=z^p$ lenne. □

3.12.16. Lemma. *Minden $\alpha \in \mathcal{O}_p$-re $\alpha^p \in \mathbb{Z}+p\mathcal{O}_p$.*

Bizonyítás. Írjuk α-t $\alpha = a_0+a_1\zeta+\cdots+a_{p-2}\zeta^{p-2}$ alakban. Ekkor modulo p emelhetünk tagonként p-edik hatványra, azaz

$$\alpha^p \equiv a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{p(p-2)} = a_0^p+\cdots+a_{p-2}^p \in \mathbb{Z} \pmod{p\mathcal{O}_p}$$

□

3.12.17. Lemma. *Legyen $\alpha = a_0+a_1\zeta+\ldots a_{p-1}\zeta^{p-1}$, ahol $a_i \in \mathbb{Z}$ $(i=0,\ldots,p-1)$ és legalább az egyik $a_i=0$. Ekkor ha $\alpha \in n\mathcal{O}_p$ alkalmas $n \in \mathbb{Z}$ egész számmal, akkor $n \mid a_i$ minden $i=0,\ldots,p-1$-re.*

Bizonyítás. Mivel $1+\zeta+\cdots+\zeta^{p-1}=0$, ezért bármely $p-1$ ezek közül egy egész bázist alkot. □

Áttérve ideálokra azt kapjuk, hogy az $(x+\zeta^i y)$ páronként relatív prím ideálok szorzata egy ideál p-edik hatványa. Az ideálokra történő egyértelmű prímfelbontás miatt azt kapjuk, hogy minden $i=0,\ldots p-1$-re az $(x+\zeta^i y)$ ideál egy A_i ideál p-edik hatványa. Node $A_i^p=(x+\\ +\zeta^i y)$ egy főideál, ezért A_i osztályának rendje a $Cl(\mathcal{O}_p)$ osztálycsoportban osztója p-nek. De mivel p-ről feltettük, hogy reguláris prím, azaz p nem osztja $Cl(\mathcal{O}_p)$ rendjét, ezért A_i osztálya triviális, azaz $A_i=(\alpha_i)$ egy főideál. Speciálisan $x+\zeta y = u\alpha^p$ alkalmas $u \in \mathcal{O}_p^\times$ egységgel $(\alpha=\alpha_1)$. Sőt, a 3.12.11. Következmény szerint $u=\zeta^l v$ alakba írható, ahol $v \in \mathbb{R}$. Továbbá a 3.12.16. Lemma miatt van olyan $a \in \mathbb{Z}$ egész szám, melyre $\alpha^p \equiv a \pmod{p\mathcal{O}_p}$. Tehát

$$x+\zeta y \equiv \zeta^l v a \pmod{p\mathcal{O}_p}\ .$$

Ezt megkonjugálva

$$x+\zeta^{-1} y \equiv \zeta^{-l} v a \pmod{p\mathcal{O}_p}\ .$$

A kettőt összevetve

$$x+\zeta y-\zeta^{2l}x-\zeta^{2l-1}y = x+\zeta y-\zeta^{2l}(x+\zeta^{-1}y) \equiv 0 \pmod{p\mathcal{O}_p}\ . \tag{3.9}$$

Ha az $1,\zeta,\zeta^{2l-1},\zeta^{2l}$ számok mind különbözők, akkor mivel $p \geq 5$, ezért a 3.12.17. Lemma ellentmond a $p \nmid x$ feltételnek. Tehát szükségképpen van két egyenlő ezek között a számok között.

- Ha $1=\zeta^{2l}$, akkor a (3.9) egyenlet $p \mid \zeta y-\zeta^{-1}y$ alakú, ami – a 3.12.17. Lemma újbóli alkalmazásával – ellentmond annak, hogy $p \nmid y$.
- Ha $1=\zeta^{2l-1}$, akkor $\zeta=\zeta^{2l}$, azaz a (3.9) egyenlet $p \mid (x-y)-(x-y)\zeta$ alakú, ami a $p \nmid x-y$ választásnak mond ellent.
- Ha $\zeta=\zeta^{2l-1}$, akkor a (3.9) egyenlet $p \mid x-\zeta^2 x$ alakú, ami szintén ellentmondás.

□

4. fejezet

Értékelések

4.1. Értékelések, telítés és a p-adikus számok teste

4.1.1. Definíció. Legyen K egy test. Egy $|\cdot|\colon K \to \mathbb{R}^{\geq 0}$ függvényt (multiplikatív) értékelésnek (vagy abszolútértéknek) nevezünk, ha

(1) $|x| = 0 \iff x = 0$;

(2) $|xy| = |x||y|$;

(3) $|x + y| \leq |x| + |y|$ (ez az ún. háromszögegyenlőtlenség).

Az $|\cdot|$ értékelés indukál egy $d(x, y) := |x - y|$ metrikát K-n. Így K egy metrikus tér (speciálisan van rajta egy topológia).

4.1.2. Példa. A *triviális* abszolútérték: $|x| = 1$ ha $x \neq 0$ és $|0| = 0$.

4.1.3. Lemma. *Tetszőleges $|\cdot|$ értékelésre $|1| = |-1| = 1$, és $|1/x| = 1/|x|$ $(x \neq 0)$.*

Bizonyítás. $|1| = |1 \cdot 1| = |1| \cdot |1|$, ahol $|1| \neq 0$. Továbbá $1 = |(-1)^2| = |-1|^2$, ahol $|-1| > 0$. Végül $1 = |x \cdot 1/x| = |x||1/x|$. □

4.1.4. Definíció. $|\cdot|_1$ és $|\cdot|_2$ értékelések a K testen *ekvivalensek*, ha ugyanazt a topológiát indukálják.

4.1.5. Állítás. *$|\cdot|_1$ és $|\cdot|_2$ akkor és csak akkor ekvivalens, ha létezik olyan $s > 0$ valós szám, melyre $|x|_1 = |x|_2^s$ minden $x \in K$-ra.*

Bizonyítás. Az $\Leftarrow$ irány triviális. A másik irányhoz vegyük észre, hogy $|x|_i < 1$ akkor és csak akkor teljesül, ha x hatványai nullához tartanak az $|\cdot|_i$ értékelésben ($i = 1,2$). Tehát ha $|\cdot|_1$ és $|\cdot|_2$ ugyanazt a topológiát indukálja, akkor $|x|_1 < 1$ akkor és csak akkor, ha $|x|_2 < 1$. Ezt x helyett a/b-re és b/a-ra is alkalmazva a 4.1.3. Lemma segítségével azt kapjuk, hogy $|a|_1 \leq |b|_1 \Leftrightarrow |a|_2 \leq |b|_2$ $(a, b \in K)$. Speciálisan ha $|\cdot|_1$ és $|\cdot|_2$ közül az egyik triviális, akkor a másik is, ezért feltehetjük, hogy létezik $y \in K$, melyre $|y|_1 > 1$. Ekkor $|y|_2 > 1$, ezért választhatjuk az $s > 0$ valós számot úgy, hogy $|y|_1 = |y|_2^s$. Tetszőleges $0 \neq x \in K$-ra van olyan $\alpha = \alpha(x) \in \mathbb{R}$, melyre $|x|_1 = |y|_1^\alpha$. Vegyük racionális számoknak egy szigorúan monoton

csökkenő $(\frac{m_i}{n_i})_{i\in\mathbb{N}}$ ($m_i, n_i \in \mathbb{Z}$, $n_i \neq 0$) sorozatát, melynek határértéke α. Ekkor $|x|_1 = |y|_1^\alpha <$ $< |y|_1^{m_i/n_i}$, azaz $|x^{n_i}|_1 < |y^{m_i}|_1$, így $|x^{n_i}|_2 < |y^{m_i}|_2$, azaz $|x|_2 < |y|_2^{m_i/n_i}$. i-vel végtelenhez tartva azt kapjuk, hogy $|x|_2 \leq |y|_2^\alpha$. Másrészt ha α-t alulról közelítjük racionálisakkal, akkor $|x|_2 \geq |y|_2^\alpha$ hasonlóképp adódik, tehát $|x|_1 = |y|_1^\alpha = |y|_2^{s\alpha} = |x|_2^s$ teljesül minden $0 \neq x \in K$-ra (és persze $x = 0$-ra is). □

4.1.6. Definíció. Azt mondjuk, hogy az $|\cdot|$ értékelés *nemarkhimédeszi*, ha a $\{|n\cdot 1| \colon n \in \mathbb{Z}\} \subseteq$ $\subseteq \mathbb{R}$ halmaz korlátos, illetve *arkhimédeszi* ha ez a halmaz nem korlátos (v.ö.: arkhimédeszi axióma, mely szerint minden valósnál van nagyobb egész).

4.1.7. Megjegyzés. Mondhattuk volna azt is, hogy ha a $f \colon \mathbb{Z} \to K$, $f(1) = 1$ gyűrűhomomorfizmus képe *korlátos* K-ban, akkor a $|\cdot|$ nemarkhimédeszi. Viszont ehhez definiálnunk kellett volna a korlátosságot K részhalmazaira.

4.1.8. Példa.

1. A triviális értékelés nemarkhimédeszi.
2. A szokásos (a mostani jegyzetben $|\cdot|_\infty$-nel jelölt) abszolútérték $\mathbb{R}$-en (vagy $\mathbb{C}$-n vagy ezeknek egy résztestén) arkhimédeszi.
3. Legyen p egy prímszám. Vegyük $\mathbb{Q}$-n az $|\cdot|_p$ ún. p-adikus értékelést, melyre $|\frac{a}{b}p^n|_p = p^{-n}$, ahol $p \nmid a, b \in \mathbb{Z}$, és $|0|_p = 0$. Ez nemarkhimédeszi, hiszen ha $\frac{a}{b}p^n \in \mathbb{Z}$, akkor $n \geq 0$, azaz $|\frac{a}{b}p^n|_p = p^{-n} \leq 1$.
4. Általában, ha $v \colon K^\times \to \mathbb{Z}$ egy diszkrét értékelés, akkor $|x| := e^{-v(x)}$ ($x \neq 0$) és $|0| := 0$ egy nemarkhimédeszi abszolútérték a K testen. Ezt nevezzük a v diszkrét értékeléshez tartozó abszolútértéknek. Itt e a természetes alapú logaritmus alapszáma, de helyette választhatnánk bármilyen más 1-nél nagyobb valós számot. Amennyiben K maradékteste véges, akkor szokásos választás ennek a véges testnek az elemszáma e helyett.

4.1.9. Gyakorlat. *Igazoljuk, hogy a fent definiált p-adikus értékelés $\mathbb{Q}$-n valóban teljesíti az* (1) − (3) *axiómákat.*

4.1.10. Állítás. *A $|\cdot|$ értékelés akkor és csak akkor nemarkhimédeszi, ha teljesül az ún.* ultrametrikus *egyenlőtlenség, mely szerint*

(3′) $|x + y| \leq \max(|x|, |y|)$.

Sőt, ha $|\cdot|$ nemarkhimédeszi, akkor $\{|n \cdot 1|, n \in \mathbb{Z}\}$ nemcsak korlátos, hanem $|n \cdot 1| \leq 1$.

Bizonyítás. Ha teljesül az ultrametrikus egyenlőtlenség, akkor nyilván $|n \cdot 1| \leq |1| = 1$. Másrészt ha $k > 0$ egész, $|x| \geq |y|$ és $|n \cdot 1| \leq C$ valamilyen $0 < C \in \mathbb{R}$-re, akkor

$$|x+y|^k = |(x+y)^k| = |\sum_{j=0}^{k} \binom{k}{j} x^j y^{k-j}| \leq \sum_{j=0}^{k} |\binom{k}{j} \cdot 1||x|^j |y|^{k-j} \leq \sum_{j=0}^{k} C|x|^k = (k+1)C|x|^k \ .$$

A fenti egyenletből k-adik gyököt vonva és k-val tartva a végtelenbe adódik az állítás. □

4.1.11. Tétel (Ostrowski)**.** *A racionális számok $\mathbb{Q}$ testén ekvivalencia erejéig csak a triviális, a valós $|\cdot|_\infty$ és a p-adikus $|\cdot|_p$ értékelések vannak (ahol $p \in \mathbb{N}$ végigfut a prímszámokon).*

Bizonyítás. Hogy össze ne keverjük $|\cdot|_\infty$-vel, használjuk inkább a $\|\cdot\|$ jelölést az értékelésre ebben a bizonyításban. Tehát vegyünk egy $\|\cdot\|\colon \mathbb{Q}\to\mathbb{R}^{\geq 0}$ értékelést.

1. eset: $\|\cdot\|$ nemarkhimédeszi. Ha minden p prímszámra $\|p\|=1$, akkor az értékelés triviális (negatívokra lásd 4.1.3. Lemma). Tehát feltehetjük, hogy van olyan p prím, melyre $\|p\|<1$. Vegyük észre, hogy ekkor az $A:=\{a\in\mathbb{Z}\colon \|a\|<1\}$ egy ideál $\mathbb{Z}$-ben, hiszen zárt az összeadásra a $(3')$ ultrametrikus egyenlőtlenség miatt, és (2) miatt a külső elemmel való szorzásra is, hiszen a 4.1.10. Állítás szerint $\|n\|\leq 1$, ha $n\in\mathbb{Z}$. Node $p\in A$, ugyanakkor $1\notin A$, ezért $A=(p)$, hiszen (p) egy maximális ideál $\mathbb{Z}$-ben. Ez viszont azt jelenti, hogy $p\nmid a,b\in\mathbb{Z}$ esetén $\|a\|=\|b\|=1$, azaz $\|\frac{a}{b}p^n\|=\|p\|^n=|\frac{a}{b}p^n|_p^s$, ahol $s:=\log_{1/p}\|p\|$.

2. eset: $\|\cdot\|$ arkhimédeszi. Legyen $1<m,n\in\mathbb{Z}$ tetszőleges.

4.1.12. Lemma. *Ekkor* $\|m\|^{1/\log m}=\|n\|^{1/\log n}$*, ahol* log *a természetes alapú logaritmust jelöli (valójában mindegy, hogy melyik).*

Bizonyítás. Írjuk fel m-et n-es számrendszerben, azaz $m=\sum_{i=0}^r a_i n^i$, ahol $0\leq a_i<n$ $(0\leq \leq i\leq r)$. Ekkor $n^r\leq m$, azaz $r\leq\frac{\log m}{\log n}$, továbbá $\|a_i\|\leq a_i\|1\|=a_i\leq n$. Így

$$\|m\|=\|\sum_{i=0}^r a_i n^i\|\leq\sum_{i=0}^r\|a_i\|\|n\|^i\ . \tag{4.1}$$

Vegyük észre, hogy ha $\|n\|\leq 1$, akkor $\|m\|\leq n(r+1)\leq\frac{n(\log m+\log n)}{\log n}$. Utóbbit m helyett m^k-ra alkalmazva és k-adik gyököt vonva $\|m\|\leq\sqrt[k]{n+\frac{kn\log m}{\log n}}$ adódik, ami $k\to\infty$-vel m-től független korlátot ad $\|m\|$-re. Ez pedig ellentmond annak, hogy $\|\cdot\|$ arkhimédeszi. Tehát $\|n\|>1$, és (4.1) miatt

$$\|m\|\leq\sum_{i=0}^r\|a_i\|\|n\|^i\leq\|n\|^r\sum_{i=0}^r\|a_i\|\leq\|n\|^r n(r+1)\leq\|n\|^{\log m/\log n}n(1+\frac{\log m}{\log n})\ .$$

Ebben m helyére m^k-t írva, k-adik gyököt vonva és k-val tartva a végtelenbe azt kapjuk, hogy $\|m\|\leq\|n\|^{\log m/\log n}$. Az állítás m és n szerepének felcserélésével adódik. □

Legyen $s:=\frac{\log\|n\|}{\log n}$ valamilyen $1<n\in\mathbb{Z}$-re. A fenti Lemma szerint s nem függ n választásától, és pozitív. Így $\|m\|=e^{s\log m}=m^s=|m|_\infty^s$ minden $1<m\in\mathbb{Z}$-re, sőt, a 4.1.3. Lemma miatt $m\leq 1$-re is, tehát hányadost képezve minden racionális m-re is. □

4.1.13. Definíció. Azt mondjuk, hogy a K test *teljes* a $|\cdot|$ értékelésre nézve, ha minden Cauchy-sorozat konvergens.

4.1.14. Példa. $\mathbb{R}$ és $\mathbb{C}$ teljes a $|\cdot|_\infty$ értékelésre nézve, $\mathbb{Q}$ viszont csak a triviális értékelésre nézve teljes, hiszen ebben minden Cauchy sorozat valamilyen indextől kezdve konstans.

A továbbiakban azt mutatjuk meg, hogy lehet egy tetszőleges értékelt testet beágyazni egy teljes testbe. Legyen K tehát egy test, melyen értelmezve van egy $|\cdot|$ értékelés. Definiáljuk

$$R:=\{(a_n)_n\in K^{\mathbb{N}}\colon \forall\varepsilon>0\exists N\in\mathbb{N}\text{, melyre } |a_n-a_m|<\varepsilon \text{ ha } m,n\geq N\}\text{-et}$$

mint a K-beli Cauchy-sorozatok gyűrűjét. Ez valóban gyűrű a koordinátánkénti műveletekre, hiszen Cauchy-sorozatok összege, különbsége és szorzata is Cauchy. Vegyük észre, hogy K

diagonálisan beágyazódik R-be, azaz van egy $\iota\colon K \to R$ injektív gyűrűhomomorfizmus, melyet a $\iota(c) := (c)_n$ képlet definiál, azaz egy $c \in K$ elem esetén $\iota(c)$ a konstans c sorozat. Legyen I_0 azon sorozatok halmaza, amik véges sok tagtól eltekintve azonosan 0-k. Ekkor $I_0 \lhd R$ egy ideál. Jelöljül $R/I_0 =: R_0$-lal a faktorgyűrűt. R_0-ra gondolhatunk úgy is, mint a Cauchy-sorozatok ekvivalencia-osztályainak gyűrűjére, ahol két Cauchy-sorozat ekvivalens, ha véges sok tagtól eltekintve megegyeznek.

4.1.15. Állítás. *R_0 lokális gyűrű, melyben a maximális ideált a nullasorozatok alkotják.*

Bizonyítás. Jelöljük M-mel azt a részhalmazát R-nek, melynek elemei a nullasorozatok (azaz a 0-hoz konvergáló sorozatok). M nyilván zárt a kivonásra és az R-beli elemmel való szorzásra, tehát $M \lhd R$. Sőt, nyilván $I_0 \subseteq M$. Másrészt ha $(a_n)_n$ egy Cauchy-sorozat, melynek tagjai nem tartanak a 0-hoz, akkor $(1/a_n)_{n\geq N}$ is egy Cauchy-sorozat elég nagy N-re (hiszen ha N elég nagy, akkor $N \leq n$ esetén $a_n \neq 0$), tehát $(a_n)_n$ invertálható R_0-ban. Így M valóban maximális ideál. □

4.1.16. Definíció. Legyen K test egy $|\cdot|$ értékeléssel. Ekkor $(K, |\cdot|)$ *telítettje* definíció szerint a $\hat{K} := R/M$ test.

4.1.17. Megjegyzés. $\hat{K}$ valóban test, hiszen R-et egy maximális ideállal faktorizáltuk.

Vegyük észre, hogy a ι beágyazás kompozíciója az $R \to \hat{K} = R/M$ faktorleképezéssel még mindig injektív: ha $0 \neq c \in K$, akkor a konstans c sorozat nem tart nullához, azaz nincs benne M-ben. Tehát innentől K-t úgy tekintjük, mint $\hat{K}$ egy résztestét. Be kell még látnunk, hogy $\hat{K}$ valóban egy telített, azaz teljes. Ehhez legelőször ki kell terjesztenünk az $|\cdot|$ értékelést K-ról $\hat{K}$-ra. Mivel $|a_m| \leq |a_n| + |a_m - a_n| < |a_n| + \varepsilon$, ha $n, m > N = N(\varepsilon)$ elég nagy, ezért ha $(a_n)_n$ Cauchy-sorozat K-ban, akkor $|a_n|$ is Cauchy, tehát konvergens $\mathbb{R}$-ben. Így értelmezhetjük egy $(a_n)_n$ Cauchy-sorozat értékelését az $|(a_n)_n| := \lim_{n\to\infty} |a_n|$ limesszel. Nyilván ha $(a_n)_n$ és $(b_n)_n$ különbsége nullasorozat – azaz $(a_n)_n$ és $(b_n)_n$ M-szerinti mellékosztálya megegyezik –, akkor $|(a_n)_n| = |(b_n)_n|$. Továbbá a konstans c sorozat értékelése nyilván megegyezik c értékelésével. Ily módon kiterjesztettük $|\cdot|$-et $\hat{K}$-ra. Egyszerű számolás mutatja, hogy $|\cdot|$-ra teljesülnek $\hat{K}$-on is az $(1) - (3)$ axiómák.

4.1.18. Állítás. *$\hat{K}$ teljes a kiterjesztett $|\cdot|$ értékelésre nézve.*

Bizonyítás. Be kell látnunk, hogy Cauchy-sorozatok ekvivalenciaosztályainak egy Cauchy-sorozata konvergál egy Cauchy-sorozat ekvivalenciaosztályához. Ha $i \in \mathbb{N}$, akkor jelölje az i-edik Cauchy-sorozat n-edik elemét $a_n^{(i)}$. Az, hogy a Cauchy-sorozataink sorozata Cauchy, azt jelenti, hogy minden $\varepsilon > 0$-ra létezik olyan nagy $N(\varepsilon) \in \mathbb{N}$, hogy ha $i, j \geq N(\varepsilon)$, akkor van olyan $M(i, j, \varepsilon) \in \mathbb{N}$, melyre $|a_m^{(i)} - a_m^{(j)}| < \varepsilon$, ha $m \geq M(i, j, \varepsilon)$. Továbbá minden rögzített $i \in \mathbb{N}$-re az $(a_n^{(i)})_n$ sorozat is Cauchy, így minden i-re van olyan $n_i \in \mathbb{N}$, melyre $|a_{n_i}^{(i)} - a_m^{(i)}| < < 1/2^i$, ha $m \geq n_i$. Belátjuk, hogy az $(a_{n_i}^{(i)})_i$ sorozat Cauchy, és ennek ekvivalenciosztálya lesz a határérték. Rögzített $\varepsilon > 0$-hoz legyen $i, j \geq N(\varepsilon/3)$ olyan, hogy $1/2^i$,$1/2^j < \varepsilon/3$. Tehát ha $m \geq M(i, j, \varepsilon/3)$, akkor $|a_m^{(i)} - a_m^{(j)}| < \varepsilon/3$. Így

$$|a_{n_i}^{(i)} - a_{n_j}^{(j)}| = |(a_{n_i}^{(i)} - a_m^{(i)}) + (a_m^{(i)} - a_m^{(j)}) + (a_m^{(j)} - a_{n_j}^{(j)})| \leq \frac{1}{2^i} + \varepsilon/3 + \frac{1}{2^j} < \varepsilon \ ,$$

azaz az $(a_{n_i}^{(i)})_i$ sorozat Cauchy. Az, hogy ez a határérték, világos, hiszen minden $\varepsilon > 0$ létezik olyan $N \in \mathbb{N}$, hogy $i \geq N$ esetén az i-edik sorozat $(a_n^{(i)})_n$ már ε-nyira közel van ehhez, azaz $|a_n^{(i)} - a_{n_n}^{(n)}| < \varepsilon$ minden elég nagy n-re. □

4.1.19. Megjegyzés. A $\hat{K}$ telítettnek megvan a következő univerzális tulajdonsága: Ha van egy $K \hookrightarrow L$ értékeléstartó testhomomorfizmus egy teljes L testbe, akkor az kiterjed értékeléstartóan K-ról $\hat{K}$-ra, sőt a kiterjesztés egyértelmű.

4.1.20. Definíció. A p-adikus számok $\mathbb{Q}_p$ teste legyen $\mathbb{Q}$ telítettje a p-adikus $|\cdot|_p$ normára nézve.

A p-adikus számok testének fenti definíciója Kürschák Józseftől származik, természetességét Ostrowski tétele is mutatja. Ennek a definíciónak az is az előnye, hogy viszonylag könnyen általánosítható $\mathbb{Q}$ helyett más testekre, sőt akár integritási tartományokra. Utóbbi a nemarkhimédeszi analitikus geometriának a kiindulópontja, melyben egy R integritási tartomány analitikus spektruma az összes rajta értelmezett abszolútérték halmaza – ezen a halmazon természetes módon lehet definiálni topológiát is.

Viszont Cauchy-sorozatok ekvivalenciaosztályaival nehéz számolni, ezért hasznos a p-adikus számoknak az alábbi, p-adikus sorfejtése.

4.1.21. Definíció. Ha $(K, |\cdot|)$ egy – nem feltétlenül teljes – nemarkhimédeszien értékelt test, akkor legyen $\mathcal{O}_K := \{a \in K \colon |a| \leq 1\}$ az *egészek gyűrűje* K-ban, vagy K *értékelésgyűrűje*. Az ultrametrikus egyenlőtlenség miatt ez valóban részgyűrű.

4.1.22. Gyakorlat. *Az $\mathcal{O}_K$ gyűrű egy lokális gyűrű, azaz egyetlen maximális ideálja van. A maximális ideálja $\mathcal{M}_K := \{a \in K \colon |a| < 1\}$. Az $\mathcal{O}_K/\mathcal{M}_K$ testet a maradéktestnek (vagy a maradékosztályok testének) nevezik.*

4.1.23. Megjegyzés. Vegyük észre, hogy az $\mathcal{O}_K$ értékelésgyűrű egészre zárt. Valóban, egy 1-nél nagyobb abszolútértékű elem nem lehet gyöke egy normált, $\mathcal{O}_K$-beli együtthatós polinomnak az ultrametrikus egyenlőtlenség miatt.

4.1.24. Definíció. A p-adikus egészek $\mathbb{Z}_p$ gyűrűje az egészek $\mathcal{O}_{\mathbb{Q}_p}$ gyűrűje a p-adikus számok $\mathbb{Q}_p$ testében.

4.1.25. Lemma. *A $|\cdot|_p$ értékelés értékkészlete $\mathbb{Q}_p$-n ugyanaz, mint $\mathbb{Q}$-n, azaz $\{0\} \cup p^{\mathbb{Z}} \subset \mathbb{R}$.*

Bizonyítás. Definíció szerint $|\mathbb{Q}| = \{0\} \cup p^{\mathbb{Z}}$. Ez a halmaz zárt $\mathbb{R}$-ben, sőt, egyetlen torlódási pontja a 0. Viszont az értékelés nyilvánvalóan folytonos az általa definiált topológiában, és $\mathbb{Q} \subset \mathbb{Q}_p$ sűrű, ezért $|\mathbb{Q}_p| = \{0\} \cup p^{\mathbb{Z}}$. □

4.1.26. Megjegyzés. A fenti bizonyítás azt is mutatja, hogy ha $(a_n)_n$ egy Cauchy-sorozat ($a_n \in \mathbb{Q}$, $n \in \mathbb{N}$) a p-adikus értékelésben, és $(a_n)_n$ nem nullasorozat, akkor $(|a_n|)_n$ sorozat véges sok tagtól eltekintve konstans, hiszen 0-n kívül nincs más torlódási pontja $\{0\} \cup p^{\mathbb{Z}}$-nek.

4.1.27. Állítás. *$\mathbb{Z}_p$-ben a maximális ideál $p\mathbb{Z}_p$, és a faktorgyűrű $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.*

Bizonyítás. Vegyünk egy x elemet $\mathbb{Z}_p$-ben, mely az $(a_n/b_n)_n$ Cauchy-sorozat ekvivalenciaosztálya, ahol $a_n, b_n \in \mathbb{Z}$, $b_n \neq 0$ és $(a_n, b_n) = 1$. Ha n elég nagy, akkor $|a_n/b_n|_p \leq 1$, azaz $p \nmid b_n$. Másrészt mivel a sorozat Cauchy, van olyan $N \in \mathbb{N}$, hogy $n, m \geq N$-re $|a_n/b_n - a_m/b_m|_p \leq p^{-1}$, azaz $a_n/b_n \equiv a_m/b_m \pmod{p}$. Rendeljük hozzá x-hez az $a_n/b_n \pmod{p} \in \mathbb{F}_p$ értéket. Ez egy szürjektív $\mathbb{Z}_p \to \mathbb{F}_p$ gyűrűhomomorfizmus, melynek magja $p\mathbb{Z}_p$. Tehát $p\mathbb{Z}_p$ maximális ideál $\mathbb{Z}_p$-ben (hiszen a faktorgyűrű test), ezért a 4.1.22. Gyakorlat szerint ez az egyetlen maximális ideál. □

4.1.28. Tétel. *$\mathbb{Q}_p$ minden eleme egyértelműen írható $x=\sum_{n=-N}^{\infty} x_n p^n$ konvergens hatványsor alakban, ahol $x_n \in \{0,1,\dots,p-1\}$ $(N \le n \in \mathbb{Z})$. Továbbá ha $x_{-N} \neq 0$, akkor $|x|_p = p^N$.*

Bizonyítás. Ha $x=0$, akkor legyen $x_n=0$ minden $n\in\mathbb{Z}$-re. Ha $x\neq 0$, akkor a 4.1.25. Lemma miatt $|x|=p^N$ valamilyen $N\in\mathbb{N}$-re. Szükség esetén x-et megszorozva p^N-nel feltehetjük, hogy $N=0$. A 4.1.27. Állítás miatt van olyan $x_0\in\{1,\dots,p-1\}$, melyre $x-x_0\in p\mathbb{Z}_p$. Ugyanezt x helyett $(x-x_0)/p$-re elmondva van olyan $x_1\in\{0,\dots,p-1\}$, melyre $(x-x_0)/p-x_1\in p\mathbb{Z}_p$, és így tovább. Vegyük észre, hogy a(z a priori formális) $\sum_{n=0}^{\infty} x_n p^n$ sor konvergens, hiszen tagjai tartanak a 0-hoz a $|\cdot|_p$ értékelésben. Sőt, $p^{k+1} \mid x-\sum_{n=0}^{k} x_n p^n$, azaz $|x-\sum_{n=0}^{k} x_n p^n|_p \le p^{-k-1}$, azaz a határérték épp x. □

4.2. Direkt limesz

Legyen I egy (általában végtelen) részbenrendezett halmaz, melyben bármely két elemnek van közös felső korlátja (azaz I *jobb filtrált*). Ekkor természetesen bármely véges sok elemnek is van közös felső korlátja.

4.2.1. Definíció. Legyenek az A_i halmazok az I részbenrendezett halmazzal indexelve, és minden $i\le j$-re legyen adva egy $f_{ji}\colon A_i\to A_j$ függvény az alábbi tulajdonságokkal: (1) $f_{ii}=$ $=\mathrm{id}_{A_i}$ minden $i\in I$-re; (2) ha $i\le j\le k\in I$, akkor $f_{ki}=f_{kj}\circ f_{ji}$. Az $(A_i)_{i\in I}$ halmazrendszert ekkor *direkt rendszer*nek nevezzük. Az $(A_i)_{i\in I}$ direkt rendszer *direkt limesz*én a

$$\varinjlim_{i\in I} A_i := \dot{\bigcup} A_i/\sim\ ,$$

ahol $\sim$ a következő ekvivalenciareláció a $\dot{\bigcup}_{i\in I}A_i$ diszjunkt unión: $a_i\sim a_j$ ($a_i\in A_i$, $a_j\in A_j$, $i,j\in I$) akkor és csak akkor, ha van olyan $k\in I$, melyre $i\le k$, $j\le k$ és $f_{ki}(a_i)=f_{kj}(a_j)\in$ $\in A_k$. Az $a_i\in A_i$ osztályát a $\varinjlim A_i$ direkt limeszben $[a_i]$-vel jelöljük. A direkt limeszt időnként injektív limesznek, vagy kolimesznek is nevezik.

4.2.2. Megjegyzés. Ha az A_i halmazok topologikus terek, és az f_{ji} leképezések folytonosak, akkor a $\varinjlim_{i\in I} A_i$ is egy topologikus tér lesz (a diszjunkt unión vett ekvivalenciareláció szerinti faktortértopológiával). Ez a topológia $\varinjlim_{i\in I} A_i$-n a *direkt limesz topológia*, mely nem más, mint a legfinomabb olyan topológia, melyre nézve az $A_i\hookrightarrow\dot{\bigcup}A_i\twoheadrightarrow\varinjlim A_i$ leképezések mind folytonosak.

4.2.3. Állítás. *Ha az A_i halmazok csoportok, és az f_{ji} leképezések csoporthomomorfizmusok, akkor $\varinjlim A_i$ is csoport az $[a_i]\cdot[a_j]:=[f_{ki}(a_i)\cdot f_{ji}(a_i)]$ művelettel, ahol $k\in I$ tetszőleges közös felső korlátja $i,j\in I$-nek.*

Bizonyítás. A jóldefiniáltság abból következik, hogy $[a_i]=[f_{ki}(a_i)]$, és ha $a_i\sim a_{i'}$ (melyet egy $i,i'\le k_1\in I$ index bizonyít), $a_j\sim a_{j'}$ (melyet egy $j,j'\le k_2\in I$ index bizonyít) és k,k' egy-egy közös felső korlátja i,j-nek, illetve i',j'-nek rendre, akkor vehetünk egy $k_0\in I$ közös felső korlátot az $i,j,k,i',j',k',k_1,k_2\in I$ elemeknek. Ekkor (többször használva, hogy az f-ek homomorfizmusok, és jól viselkednek a kompozícióra)

$$\begin{aligned} f_{k_0k}(f_{ki}(a_i)f_{kj}(a_j)) = f_{k_0k}\circ f_{ki}(a_i) f_{k_0k}\circ f_{kj}(a_j) = \\ = f_{k_0i}(a_i)f_{k_0j}(a_j) = f_{k_0k_1}\circ f_{k_1i}(a_i) f_{k_0k_2}\circ f_{k_2j}(a_j) = \\ = f_{k_0k_1}\circ f_{k_1i'}(a_{i'}) f_{k_0k_2}\circ f_{k_2j'}(a_{j'}) = f_{k_0i'}(a_{i'})f_{k_0j'}(a_{j'}) = f_{k_0k'}(f_{k'i'}(a_{i'})f_{k'j'}(a_{j'}))\ . \end{aligned}$$

Az asszociativitás egy hasonló számolás és $[a_i]^{-1} = [a_i^{-1}]$. □

A fenti bizonyítás azt is mutatja, hogy ha az A_i-ken tetszőleges műveletek vannak adva, amiket az f_{ji} leképezések megtartanak, akkor a direkt limeszen is értelmezhetők ugyanezek a műveletek. Sőt, ha vannak azonosságaink, melyek az összes A_i-ben teljesülnek, akkor azok az azonosságok a direkt limeszben is teljesülni fognak. Tehát gyűrűk, modulusok, vektorterek direkt limesze is gyűrű, modulus, vektortér. Sőt, ha feltesszük, hogy a leképezések mindig testhomomorfizmusok, melyek az 1-et az 1-be viszik (speciálisan injektívek), akkor testek direkt limesze is test lesz, hiszen minden nem 0 elemnek lesz inverze.

4.2.4. Példa. Ha $I = \mathbb{Z}^{>0}$ az oszthatóságra nézve, és $\mu_n \leq \mathbb{C}^\times$ jelöli az n-edik egységgyökök csoportját, és $n \mid m$ esetén $f_{mn}\colon \mu_n \to \mu_m$ a természetes tartalmazás, akkor $\varinjlim_n \mu_n \cong \mu_\infty$ az összes komplex egységgyök csoportja.

4.2.5. Állítás. *A direkt limesz funktor egzakt (Abel-csoportokon).*

Mielőtt belekezdenénk a fenti állítás bizonyításába, először azt kell megmondanunk, mitől is lesz a „direkt limesz" egy funktor, és melyik kategóriából melyikbe képez. Rögzítsünk egy I jobb filtrált részbenrendezett halmazt, és tekintsük ezzel a részbenrendezett halmazzal indexelt Abel-csoportok direkt rendszereit, mint objektumokat. Egy $(A_i, f_{ji})_{i\leq j\in I}$ és egy $(B_i, g_{ji})_{i\leq j\in I}$ direkt rendszer között egy $\varphi = (\varphi_i)_{i\in I}$ morfizmus alatt $\varphi_i\colon A_i \to B_i$ $(i \in I)$ Abel-csoport homomorfizmusok egy rendszerét értjük, melyekre minden $i \leq j \in I$ esetén a

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_i} & B_i \\ {\scriptstyle f_{ji}}\downarrow & & \downarrow{\scriptstyle g_{ji}} \\ A_j & \xrightarrow{\varphi_j} & B_j \end{array}$$

diagram kommutatív. Vegyük észre, hogy direkt rendszerek közti leképezések magja és képe (sőt, komagja) is direkt rendszer, ezért van értelme direkt rendszerek egzakt sorozatáról beszélni. Továbbá ha φ egy morfizmus az $(A_i)_{i\in I}$ és a $(B_i)_{i\in I}$ direkt rendszer között, akkor φ indukál egy $\varinjlim \varphi_i\colon \varinjlim A_i \to \varinjlim B_i$ Abel-csoport homomorfizmust a direkt limeszek között. Tehát $\varinjlim_{i\in I}$ valóban egy funktor, mégpedig az I-vel indexelt Abel-csoportokból álló direkt rendszerek kategóriájából az Abel-csoportok kategóriájába, és van értelme arról beszélni, hogy egzakt sorozatot egzaktba visz-e.

Bizonyítás. Azt kell belátnunk, hogy ha $(A_i, f_{ji})_{i\leq j\in I} \xrightarrow{\alpha} (B_i, g_{ji})_{i\leq j\in I} \xrightarrow{\beta} (C_i, h_{ji})_{i\leq j\in I}$ direkt rendszerek egy egzakt sorozata, akkor $\varinjlim A_i \xrightarrow{\varinjlim \alpha_i} \varinjlim B_i \xrightarrow{\varinjlim \beta_i} \varinjlim C_i$ is egzakt. Az, hogy $\varinjlim \beta_i \circ \circ \varinjlim \alpha_i = \varinjlim(\beta_i \circ \alpha_i) = \varinjlim 0 = 0$ (vagyis $\operatorname{Im}(\varinjlim \alpha_i) \subseteq \operatorname{Ker}(\varinjlim \beta_i)$), világos. Másrészt legyen $b = [b_i] \in \operatorname{Ker}(\varinjlim \beta_i) \subseteq \varinjlim B_i$. Ez azt jelenti, hogy $(\varinjlim \beta_i)(b) = [\beta_i(b_i)] = [0] = 0$ $\varinjlim C_i$-ben. A $\sim$ ekvivalenciareláció definíciója szerint ez azt jelenti, hogy van olyan $k \geq i \in I$, melyre $h_{ki}(\beta_i(b_i)) = h_{ki}(0) = 0 \in C_k$. Node $0 = h_{ki}(\beta_i(b_i)) = \beta_k(g_{ki}(b_i))$, azaz $g_{ki}(b_i) \in \operatorname{Ker}(\beta_k) = = \operatorname{Im}(\alpha_k)$ (a direkt rendszerek közti sorozat egzaktsága miatt). Ekkor van olyan $a_k \in A_k$, melyre $\alpha_k(a_k) = g_{ki}(b_i)$, azaz $b = [b_i] = [g_{ki}(b_i)] = [\alpha_k(a_k)] = \varinjlim \alpha_i([a_k]) \in \operatorname{Im}(\varinjlim \alpha_i)$. Tehát $\operatorname{Ker}(\varinjlim \beta_i) \subseteq \operatorname{Im}(\varinjlim \alpha_i)$, mivel $b \in \operatorname{Ker}(\varinjlim \beta_i)$ tetszőleges volt. □

4.3. Inverz limesz

4.3.1. Definíció. Legyenek az A_i halmazok ismét egy részben rendezett I halmazzal indexelve (melyben bármely két elemnek van felső korlátja, de ez itt a definícióhoz nem szükséges, csak a későbbi állításokhoz). Az $(A_i)_{i\in I}$ halmazok egy *inverz rendszer*t alkotnak, ha minden $i \leq j \in I$-re adva van egy $f_{ij}\colon A_j \to A_i$ függvény, melyre (1) $f_{ii} = \mathrm{id}_{A_i}$; (2) $i \leq j \leq k$ esetén $f_{ij} \circ f_{jk} = f_{ik}$. Az A_i halmazok inverz limesze a

$$\varprojlim_{i\in I} A_i := \{(a_i)_{i\in I} \in \prod_{i\in I} A_i \mid f_{ij}(a_j) = a_i \text{ minden } i \leq j \in I\text{-re}\}$$

halmaz. Az inverz limeszt időnként projektív limesznek vagy egyszerűen csak limesznek is nevezik.

4.3.2. Megjegyzés. Ha az A_i halmazok topologikus terek, és az f_{ij} $(i \leq j \in I)$ leképezések folytonosak, akkor a $\varprojlim A_i$ halmazon értelmezhetjük a szorzattopológia altértopológiáját, melyre nézve egy topologikus tér lesz. Ez a topológia nem más, mint a legdurvább olyan topológia, melyre nézve a $\varprojlim_{i\in I} A_i \hookrightarrow \prod_{i\in I} A_i \to A_j$ leképezések folytonosak minden $j \in I$-re. Másrészt az is világos, hogy ha az A_i halmazok csoportok (gyűrűk, modulusok, stb.) és az f_{ij} leképezések homomorfizmusok, akkor a $\varprojlim A_i$ részcsoportja (részgyűrűje, részmodulusa, stb.) lesz a direkt szorzatnak.

4.3.3. Példa. A p-adikus egészek gyűrűje felírható inverz limeszként: $\mathbb{Z}_p \cong \varprojlim_{n\geq 1} \mathbb{Z}/(p^n)$. Hasonlóan egy R (kommutatív) gyűrű feletti formálos hatványsorok gyűrűje is: $R[\![x]\!] \cong \varprojlim_{n\geq 1} R[x]/(x^n)$.

4.3.4. Állítás. *Nemüres, kompakt, Hausdorff A_i $(i \in I)$ halmazok (folytonos összekötő leképezésekkel vett) inverz limesze nemüres, kompakt, és Hausdorff.*

Bizonyítás. Hausdorff terekt direkt szorzata is Hausdorff, ezek részhalmaza is az. Másrészt Tyihonov tétele szerint kompakt halmazok szorzata is kompakt. Belátjuk, hogy ha az eredeti A_i halmazok Hausdorffak, akkor $\varprojlim A_i$ egy zárt része $\prod A_i$-nek, speciálisan kompakt. Valóban, minden $i \leq j \in I$ pár esetén a $B_{i,j} := \{(a_i)_{i\in I} \in \prod_{i\in I} A_i \mid f_{ij}(a_j) \neq a_i\}$ halmaz nyílt $\prod A_i$-ben, hiszen A_i Hausdorff, ezért $(a_i)_{i\in I} \in B_{ij}$ esetén a_i-nek és $f_{ij}(a_j)$-nek van egymástól diszjunkt $a_i \in V_i$, $f_{ij}(a_j) \in U_j$ környezetei. Ekkor $V_j := f_{ij}^{-1}(U_j) \subseteq A_j$ is nyílt, tehát $V_i \times V_j \times \times \prod_{k\in I, i\neq k\neq j} A_j \subseteq B_{ij}$, azaz B_{ij} nyílt. Továbbá ha $\varprojlim A_i$ üres lenne, az azt jelentené, hogy a B_{ij} $(i \leq j \in I)$ lefednék a kompakt $\prod A_i$ halmazt, tehát ennek létezne véges részfedése, azaz $i_1 \leq j_1, \ldots, i_n \leq j_n \in I$ n darab pár, melyre $\bigcup_{k=1}^{n} B_{i_k j_k} = \prod A_i$. Node ennek a $2n$ darab indexnek van egy $t \in I$ közös felső korlátja, és tetszőleges $a_t \in A_t$-re az $a_{i_k} := f_{i_k t}(a_t)$, $a_{j_k} := f_{j_k t}(a_t)$, $a_s \in A_s$ tetszőleges $(s \neq i_1, j_1, \ldots, i_n, j_n \in I)$ esetén $(a_i)_{i\in I} \in \prod A_i$ nincs benne egyik $B_{i_k j_k}$-ban sem $(k = 1, \ldots, n)$, ami ellentmondás. □

Vegyük észre, hogy a fenti állítás a Kőnig-lemma messzemenő általánosítása, mely – ezen a nyelven – azt mondja ki, hogy véges nemüres halmazok inverz limesze nemüres. Valóban, minden véges halmaz kompakt a diszkrét topológiában, és minden leképezés folytonos két diszkrét tér között.

A direkt limeszhez hasonlóan adott I részbenrendezett halmazra az inverz limesz is funktor: az Abel-csoport inverz rendszereinek kategóriájából az Abel-csoportok kategóriájába.

4.3.5. Állítás. *Abel-csoportokon az inverz limesz balegzakt, de általában nem jobb egzakt.*

Bizonyítás. Legyen $0 \to A_i \stackrel{\alpha_i}{\to} B_i \stackrel{\beta_i}{\to} C_i$ Abel-csoportok inverz rendszerének egy egzakt sorozata (tehát a

$$\begin{array}{ccccc} 0 & \longrightarrow & A_j & \xrightarrow{\alpha_j} & B_j & \xrightarrow{\beta_j} & C_j \\ & & \downarrow{\scriptstyle f_{ij}} & & \downarrow{\scriptstyle g_{ij}} & & \downarrow{\scriptstyle h_{ij}} \\ 0 & \longrightarrow & A_i & \xrightarrow{\alpha_i} & B_i & \xrightarrow{\beta_i} & C_i \end{array}$$

diagramok minden $i \le j \in I$ esetén kommutatívak). Az, hogy $\varprojlim \alpha_i$ injektív, abból következik, hogy a $\prod \alpha_i \colon \prod A_i \to \prod B_i$ leképezés is injektív. A $(\varprojlim \beta_i) \circ (\varprojlim \alpha_i) = \varprojlim (\beta_i \circ \alpha_i) = \varprojlim 0 = 0$, szintén világos. Másrészt, ha $(b_i)_{i\in I} \in \varprojlim B_i \subseteq \prod B_i$ benne van $\mathrm{Ker}(\varprojlim \beta_i)$-ben, akkor minden $i \in I$-re $\beta_i(b_i) = 0$, azaz $b_i \in \mathrm{Ker}(\beta_i) = \mathrm{Im}(\alpha_i)$, így van olyan $a_i \in A_i$, melyre $\alpha_i(a_i) = b_i$. Ráadásul α_i injektív, ezért ez az a_i egyértelmű is, sőt, $\alpha_i(f_{ij}(a_j)) = g_{ij}(\alpha_j(a_j)) = g_{ij}(b_j) = b_i = \alpha_i(a_i)$ és α_i injektivitása miatt $f_{ij}(a_j) = a_i$, azaz $(a_i)_{i\in I}$ benne van $\varprojlim A_i$-ben. □

4.3.6. Példa. Az inverz limesz általában nem egzakt: A $0 \to p^n\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/(p^n) \to 0$ sorozat minden n-re egzakt, és kompatibilis a természetes leképezésekkel, viszont $\varprojlim_n p^n\mathbb{Z} = 0$, $\varprojlim \mathbb{Z} = \mathbb{Z}$, és $\varprojlim \mathbb{Z}/(p^n) = \mathbb{Z}_p$, és a $0 \to 0 \to \mathbb{Z} \to \mathbb{Z}_p \to 0$ sorozat nem egzakt.

Variációk egy témára:

4.3.7. Következmény. *Kompakt Hausdorff Abel-csoportokon az inverz limesz egzakt.*

Bizonyítás. Azt kell belátnunk, hogy anélkül, hogy feltennénk, hogy az $\alpha_i \colon A_i \to B_i$ leképezések injektívek, következik az egzaktság $\varprojlim B_i$-nél. A fenti bizonyításban ezt ott használtuk ki, hogy mivel a_i egyértelmű volt, ezért az $(a_i)_{i\in I}$ sorozat szükségképpen kompatibilis az A_i-k közötti összekötőleképezésekkel. Viszont most az A_i-k kompaktak, ezért az $\alpha_i^{-1}(b_i) \subset A_i$ részhalmazok is kompaktak, nemüresek, és Hausdorffak (zárt őse zárt, kompaktnak zárt része kompakt). Ráadásul ezen halmazok is inverz rendszert alkotnak, tehát inverz limeszük nemüres a 4.3.4-es állítás miatt. Ez pedig azt bizonyítja, hogy a $(b_i)_{i\in I}$ elem benne van $\varprojlim \alpha_i$ képében. □

4.3.8. Következmény. *Legyen $0 \to A_i \stackrel{\alpha_i}{\to} B_i \stackrel{\beta_i}{\to} C_i \to 0$ Abel-csoportok inverz rendszerének egy egzakt sorozata, és tegyük fel, hogy $I = \mathbb{N}$ a szokásos $\le$ részbenrendezéssel. Tegyük fel, hogy az $(A_i)_{i\in I}$ inverz rendszer teljesíti a Mittag-Leffler feltételt: Minden $i \in \mathbb{N}$-re van olyan $i \le m = m(i) \in \mathbb{N}$ index, melyre minden $j \ge m$-re $\mathrm{Im}(f_{im}) = \mathrm{Im}(f_{ij})$ (azaz valamilyen indextől kezdve a képterek stabilizálódnak). Ekkor a $0 \to \varprojlim A_i \to \varprojlim B_i \to \varprojlim C_i \to 0$ sorozat is egzakt. Speciálisan ha az $f_{ij} \colon A_j \to A_i$ leképezések minden $i \le j \in I$-re szürjektívek, akkor a Mittag-Leffler feltétel triviálisan teljesül $m = i$-vel.*

Bizonyítás. Az általános eset bizonyítását az olvasóra hagyjuk. Ha az f_{ij} leképezések szürjektívek, akkor be kell látnunk, hogy a $\varprojlim \beta_i \colon \varprojlim B_i \to \varprojlim C_i$ leképezés szürjektív. Legyen $(c_i)_{i\in I} \in \varprojlim C_i$. Ekkor a $D_i := \beta_i^{-1}(c_i) \subseteq B_i$ halmazok $\mathrm{Ker}(\beta_i) = \mathrm{Im}(\alpha_i)$-szerinti mellékosztályok, melyekre $g_{ij}(D_j) \subseteq D_i$. Belátjuk, hogy itt egyenlőség van, azaz $g_{ij} \colon D_j \to D_i$ is szürjektív. Legyen $d_i \in D_i$, vegyünk egy tetszőleges $d'_j \in D_j$-t. Ekkor $g_{ij}(d'_j) \in D_i$, azaz $d_i - g_{ij}(d'_j) \in \mathrm{Im}(\alpha_i)$. Mivel α_i injektív, ezért egyértelműen létezik egy $a_i \in A_i$, melyre $\alpha_i(a_i) = d_i - g_{ij}(d'_j)$. Másrészt $f_{ij} \colon A_j \to A_i$ szürjektív, azaz van olyan $a_j \in A_j$, melyre $f_{ij}(a_j) = a_i$.

Ekkor viszont $d_i = \alpha_i(a_i) + g_{ij}(d'_j) = \alpha_i(f_{ij}(a_j)) + g_{ij}(d'_j) = g_{ij}(\alpha_j(a_j) + d'_j) \in g_{ij}(D_j)$, hiszen $\alpha_j(a_j) + d'_j$ ugyanabban az $\mathrm{Im}(\alpha_j)$-szerinti mellékosztályban van, mint d'_j, azaz D_j-ben van. Tehát rekurzívan meg tudjuk konstruálni a $\varprojlim D_i$ halmaz egy elemét: ha $d_i \in D_i$ már megvan, akkor vesszük egy tetszőleges ősképét D_{i+1}-ben, és így tovább. □

Az alábbi példában megmutatjuk, hogyan lehet a fenti Mittag-Leffler feltételt alkalmazni.

4.3.9. Feladat. *Igazoljuk, hogy* $\mathbb{Z}[\![x]\!]/(x-p) \cong \mathbb{Z}_p$.

Megoldás. Írjuk a $\mathbb{Z}[\![x]\!]$ formális hatványsorgyűrűt $\mathbb{Z}[\![x]\!] \cong \varprojlim \mathbb{Z}[x]/(x^n)$ alakba. Vegyük észre, hogy az $x-p$-vel való szorzás injektív a $\mathbb{Z}[x]/(x^n)$ gyűrűn. Valóban, ha valamely $f(x) \in$ $\in \mathbb{Z}[x]$-re $f(x)(x-p)$ osztható x^n-nel, akkor $f(x)$ is osztható x^n, mivel x^n-nek és $x-p$-nek nincs közös irreducibilis osztója, és $\mathbb{Z}[x]$-ben igaz a számelmélet alaptétele. Tehát minden $n \geq 1$-re kapunk egy

$$0 \to \mathbb{Z}[x]/(x^n) \overset{(x-p)\cdot}{\to} \mathbb{Z}[x]/(x^n) \to \mathbb{Z}[x]/(x^n, x-p) \to 0$$

rövid egzakt sorozatot. Ráadásul ezek a rövid egzakt sorozatok kompatibilisek a $\mathbb{Z}[x]/(x^{n+1}) \twoheadrightarrow$ $\mathbb{Z}[x]/(x^n)$ természetes szürjektív faktorleképezésekkel, azaz a

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}[x]/(x^{n+1}) & \xrightarrow{(x-p)\cdot} & \mathbb{Z}[x]/(x^{n+1}) & \longrightarrow & \mathbb{Z}[x]/(x^{n+1}, x-p) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}[x]/(x^n) & \xrightarrow{(x-p)\cdot} & \mathbb{Z}[x]/(x^n) & \longrightarrow & \mathbb{Z}[x]/(x^n, x-p) & \longrightarrow & 0
\end{array}$$

diagram kommutatív minden $n \geq 1$-re. Vegyük észre, hogy $\mathbb{Z}[x]/(x^n, x-p) \cong \mathbb{Z}[x]/(p^n, x-$ $-p) \cong \mathbb{Z}/(p^n)$, ráadásul a természetes $\mathbb{Z}[x]/(x^{n+1}, x-p) \to \mathbb{Z}[x]/(x^n, x-p)$ faktorleképezés ennél az izomorfizmusnál a $\mathbb{Z}/(p^{n+1}) \to \mathbb{Z}/(p^n)$ természetes faktorleképezést indukálja. Így a 4.3.8-as Következmény szerint a

$$0 \to \varprojlim \mathbb{Z}[x]/(x^n) \overset{(x-p)\cdot}{\to} \varprojlim \mathbb{Z}[x]/(x^n) \to \varprojlim \mathbb{Z}/(p^n) \to 0$$

sorozat is egzakt, azaz $\mathbb{Z}_p \cong \mathbb{Z}[\![x]\!]/(x-p)$. □

4.4. Értékelések kiterjesztése

4.4.1. Definíció. Legyen K egy $|\cdot|$ nemarkhimédeszi értékelésre nézve teljes test, $\mathcal{O}_K$ az egészek gyűrűje, $\mathfrak{p} \lhd \mathcal{O}_K$ a maximális ideál, és $k = \mathcal{O}_K/\mathfrak{p}$ a maradéktest. Egy $f(x) \in \mathcal{O}_K[x]$ polinomról azt mondjuk, hogy *primitív*, ha az együtthatók legnagyobb közös osztója 1, vagyis van olyan együttható, ami nincs benne $\mathfrak{p}$-ben. Ez persze egy $f(x) = a_n x^n + \cdots + a_1 x + a_0$ polinomra azzal ekvivalens, hogy $1 = \max_{0 \leq i \leq n}(|a_i|)$.

A következő tétel alapvető fontosságú az értékelések kiterjesztésében. A későbbi alkalmazások kedvéért – és mivel az általánosabb bizonyítás nem igényel különösebb extra erőfeszítéseket – az állítást nemcsak lokális testekre mondjuk ki és bizonyítjuk be, hanem tetszőleges teljes nemarkhimédeszi testre.

4.4.2. Tétel (Hensel Lemma)**.** *Tegyük fel, hogy az $f(x) \in \mathcal{O}_K[x]$ primitív polinom modulo $\mathfrak{p}$ felbomlik $f(x) \equiv \overline{g}(x)\overline{h}(x) \pmod{\mathfrak{p}}$ szorzatra, ahol a $\overline{g}, \overline{h} \in k[x]$ polinomok relatív prímek. Ekkor az f polinom is felbomlik $f(x) = g(x)h(x)$ szorzatra ($g, h \in \mathcal{O}_K[x]$), ahol $g(x) \equiv \overline{g}(x) \pmod{\mathfrak{p}}$ és $h(x) \equiv \overline{h}(x) \pmod{\mathfrak{p}}$, továbbá $\deg(g) = \deg(\overline{g})$.*

Bizonyítás. Legyen $d = \deg(f)$ és $m = \deg(\overline{g})$. Ekkor $d - m \geq \deg(\overline{h})$. Emeljük fel $\overline{g}$-t $\mathcal{O}_K[x]$-be (azaz vegyük minden együttható egy-egy reprezentánsát $\mathcal{O}_K$-ban) úgy, hogy a kapott $g_0(x) \in \mathcal{O}_K[x]$ polinom foka megegyezzen $\overline{g}$ fokával. Hasonlóképp emeljük fel a $\overline{h}$ polinomot is egy $h_0(x) \in \mathcal{O}_K[x]$ polinommá úgy, hogy $\deg(h_0) \leq d - m$.

Mivel $(\overline{g}, \overline{h}) = 1$, ezért van olyan $a(x), b(x) \in \mathcal{O}_K[x]$ polinom, melyekre

$$ag_0 + bh_0 \equiv 1 \pmod{\mathfrak{p}} .$$

Tehát az $f - g_0h_0$ és az $ag_0 + bh_0 - 1$ polinomok $\mathfrak{p}$-beli együtthatósak. Speciálisan minden, a két polinom valamelyikében fellépő együttható abszolútértéke kisebb, mint 1. Vegyünk az összes ilyen együttható közül egy maximális abszolútértékűt, melyet π-vel jelölünk. Ekkor persze $|\pi| < 1$. A g és h polinomokat

$$\begin{aligned} g &= g_0 + p_1\pi + \cdots + p_n\pi^n + \dots , \qquad \text{ill.} \\ h &= h_0 + q_1\pi + \cdots + q_n\pi^n + \dots \end{aligned} \tag{4.2}$$

alakban keressük. Ahhoz, hogy a (4.2) végtelen összegek konvergáljanak egy polinomhoz arra lesz szükségünk, hogy a p_i, illetve q_i ($1 \leq i$) polinomok foka korlátos legyen. Valóban, ekkor a fenti végtelen polinomösszeget definiálhatjuk együtthatónként, és mivel $|\pi^n| \to 0$, ezért K teljessége miatt valóban kapunk két $\mathcal{O}_K[x]$-beli polinomot. A p_i, q_i polinomokat rekurzívan konstruáljuk. Legyen $n \geq 1$, és tegyük fel, hogy a

$$\begin{aligned} g_{n-1} &= g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1} , \qquad \text{ill.} \\ h_{n-1} &= h_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1} \end{aligned}$$

polinomokra $f \equiv g_{n-1}h_{n-1} \pmod{\pi^n}$ (azaz $\frac{f - g_{n-1}h_{n-1}}{\pi^n} \in \mathcal{O}_K[x]$) és $\deg(g_{n-1}) = m$, $\deg(h_{n-1}) \leq \leq d - m$. A $p_n, q_n \in \mathcal{O}_K[x]$ polinomokat úgy fogjuk választani, hogy

$$g_0q_n + h_0p_n \equiv \frac{f - g_{n-1}h_{n-1}}{\pi^n} \pmod{\pi} \tag{4.3}$$

és $\deg(p_n) < m$, $\deg(q_n) \leq d - m$. Legyen tehát $g_n = g_{n-1} + p_n\pi^n$ és $h_n = h_{n-1} + q_n\pi^n$. Ilyen választással ugyanis

$$\begin{aligned} f - g_nh_n = f - (g_{n-1} + p_n\pi^n)(h_{n-1} + q_n\pi^n) = \\ = \pi^n \left(\frac{f - g_{n-1}h_{n-1}}{\pi^n} - g_{n-1}q_n - h_{n-1}p_n - \pi^n p_nq_n \right) \equiv \\ \equiv \pi^n \left(\frac{f - g_{n-1}h_{n-1}}{\pi^n} - g_0q_n - h_0p_n \right) \equiv 0 \pmod{\pi^{n+1}} . \end{aligned}$$

Mivel g_0 és h_0 relatív prímek, ezért ha a fokszámra vonatkozó feltételt egy pillanatra elfelejtjük, akkor könnyen találhatunk a (4.3) egyenletet kielégítő p_n-et és q_n-et: például $p_n = b\frac{f - g_{n-1}h_{n-1}}{\pi^n}$ és $q_n = a\frac{f - g_{n-1}h_{n-1}}{\pi^n}$ megfelel. Viszont vegyük észre, hogy $p_n = b\frac{f - g_{n-1}h_{n-1}}{\pi^n}$ helyett bármilyen

más, vele modulo g_0 kongruens polinom is jó. Osszuk el tehát a $b\frac{f-g_{n-1}h_{n-1}}{\pi^n}$ polinomot maradékosan a g_0 polinommal és legyen a maradék p_n:

$$b\frac{f-g_{n-1}h_{n-1}}{\pi^n} = qg_0 + p_n \qquad \text{és} \qquad \deg(p_n) < \deg(g_0)\ .$$

Ezzel a választással

$$h_0p_n + g_0\left(h_0q + a\frac{f-g_{n-1}h_{n-1}}{\pi^n}\right) \equiv \frac{f-g_{n-1}h_{n-1}}{\pi^n} \pmod{\pi}\ ,$$

viszont $h_0q+a\frac{f-g_{n-1}h_{n-1}}{\pi^n}$ fokszáma lehet nagyobb, mint $d-m$. Legyen q_n az a polinom, melyet úgy kapunk, hogy $h_0q + a\frac{f-g_{n-1}h_{n-1}}{\pi^n}$-ből elhagyjuk a π-vel osztható együtthatójú tagokat. Ekkor nyilván

$$g_0q_n + h_0p_n \equiv h_0p_n + g_0\left(h_0q + a\frac{f-g_{n-1}h_{n-1}}{\pi^n}\right) \equiv \frac{f-g_{n-1}h_{n-1}}{\pi^n} \pmod{\pi}\ ,$$

sőt, mivel $\deg(h_0p_n) < d-m+m$ és $\deg(\frac{f-g_{n-1}h_{n-1}}{\pi^n}) \le d$, ezért $\deg(q_n) \le d - \deg(g_0) = d - - m$, hiszen modulo π egyenlőség van és a választás miatt q_n foka megegyezik a modulo π redukciójának fokával.

Tehát a (4.2) egyenletben konstruált polinomokkal $\deg(g) = m = \deg(g_0)$, $\deg(h) \le d-m$, és $gh = (\lim_{n\to\infty} g_n)(\lim_{n\to\infty} h_n) = \lim_{n\to\infty} g_nh_n = f$. □

4.4.3. Következmény. *Az $x^{p-1}-1$ polinom $\mathbb{Z}_p$-ben gyöktényezők szorzatára bomlik. Speciálisan $\mathbb{Q}_p$-ben van primitív $p-1$-edik egységgyök.*

Bizonyítás. Az $x^{p-1}-1$ polinom $\mathbb{F}_p$-ben különböző gyöktényezők szorzatára bomlik, ezért alkalmazhatjuk a Hensel lemmát. □

Hasonlóképp, ha K egy lokális test, akkor $k = \mathcal{O}_K/\mathfrak{p}$ egy véges test, speciálisan $\mathbb{F}_{p^f}$-fel izomorf alkalmas p^f prímhatványra. Node $\mathbb{F}_{p^f}$-ben az $x^{p^f-1}-1$ polinom különböző gyöktényezők szorzatára bomlik, tehát a Hensel lemma miatt $\mathcal{O}_K$-ban is. Speciálisan minden $0 \neq \overline{\alpha} \in \mathbb{F}_{p^f}$-hez van olyan α p^f-1-edik egységgyök $\mathcal{O}_K$-ban, melyre $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{p}}$. Ezt az α-t nevezzük az $\overline{\alpha}$ *multiplikatív reprezentánsának*, vagy egyes szakirodalmakban Teichmüller reprezentánsának.

4.4.4. Következmény. *Legyen K egy teljes, nemarkhimédeszi test és $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ egy irreducibilis polinom. Ekkor $|f| := \max_{0\le i\le n}(|a_i|) = \max(|a_0|, |a_n|)$.*

Bizonyítás. Megfelelő konstanssal szorozva feltehetjük, hogy $|f| = 1$, speciálisan $f(x) \in \in \mathcal{O}_K[x]$. Indirekten tegyük fel, hogy $0 < r < n$ a legkisebb, amire $|a_r| = 1$. Ekkor $f(x) \equiv \equiv x^r(a_r + \cdots + a_nx^{n-r}) \pmod{\mathfrak{p}}$, ahol x^r relatív prím $a_r + \cdots + a_nx^{n-r}$-hez modulo $\mathfrak{p}$, hiszen a 0 nem gyöke az utóbbinak modulo $\mathfrak{p}$ se, hiszen $a_r \notin \mathfrak{p}$. Ez viszont a Hensel lemma miatt ellentmondás. □

4.4.5. Tétel. *Legyen K egy teljes, nemarkhimédeszi test, L/K pedig egy véges, n-edfokú bővítés. Ekkor $|\cdot|$ egyértelműen kiterjed egy L-en értelmezett értékeléssé. Mégpedig a kiterjesztés a következő: ha $\alpha \in L$, akkor $|\alpha| := \sqrt[n]{|N_{L/K}(\alpha)|}$. Erre az értékelésre nézve L teljes.*

Bizonyítás. Először belátjuk, hogy a tételben definiált kiterjesztés valóban értékelés. Először is ez tényleg kiterjesztése a K-n levő értékelésnek, hiszen ha $\alpha \in K$, akkor $N_{L/K}(\alpha) = \alpha^n$. Legyen $\mathcal{O}_K$ a K értékelésgyűrűje, $\mathcal{O}_L$ pedig ennek egész lezártja L-ben. Ekkor $\mathcal{O}_L = \{\alpha \in \in L \mid N_{L/K}(\alpha) \in \mathcal{O}_K\}$. Valóban, ha $\alpha \in \mathcal{O}_L$ egy $\mathcal{O}_K$ felett egész elem, akkor $N_{L/K}(\alpha)$ is egész $\mathcal{O}_K$ fölött, és K-ban van, ezért $N_{L/K}(\alpha) \in \mathcal{O}_K$. Visszafelé, ha $N_{L/K}(\alpha) \in \mathcal{O}_K$ és α minimálpolinomja $m_\alpha(x) = x^d + \cdots + a_0$, akkor $\pm a_0^{n/d} = N_{L/K}(\alpha) \in \mathcal{O}_K$, azaz $|a_0| \leq 1$. Így a 4.4.4. Következmény szerint m_α minden együtthatója $\mathcal{O}_K$-beli (hiszen abszolútértéke maximum 1), speciálisan $\alpha \in \mathcal{O}_L$. Az, hogy a $|\cdot| = \sqrt[n]{|N_{L/K}(\cdot)|}\colon L \to \mathbb{R}^{\geq 0}$ leképezés nyilván multiplikatív és csak a 0-t képzi a 0-ba. Az ultrametrikus egyenlőtlenséghez pedig azt kell belátnunk, hogy $|\alpha + \beta| \leq \max(|\alpha|, |\beta|)$. A nagyobb abszolútértékűvel leosztva elég belátni, hogy ha $|\alpha| \leq 1$, akkor $|\alpha + 1| \leq 1$. Ez pedig világos, hiszen $\mathcal{O}_L$ részgyűrű.

Az egyértelműséghez szükségünk lesz az alábbi lemmára.

4.4.6. Lemma. *Legyen K egy teljes test, V pedig egy n-dimenziós vektortér K fölött, $\|\cdot\|$ pedig egy vektortérnorma V-n. Ekkor tetszőleges $v_1, \ldots, v_n$ bázisra V-ben a*

$$\begin{array}{rcl} K^n & \to & V \\ (x_1, \ldots, x_n) & \mapsto & x_1 v_1 + \cdots + x_n v_n \end{array}$$

egy homeomorfizmus. Speciálisan V teljes. Más szavakkal véges dimenzióban minden vektortérnorma ekvivalens.

Bizonyítás. Legyen $|x| := \max_{1 \leq i \leq n}(|x_i|)$, ahol $x = x_1 v_1 + \cdots + x_n v_n$. Azt kell belátnunk, hogy van olyan ρ és ρ' konstans, melyre $\rho|x| \leq \|x\| \leq \rho'|x|$. Nyilván $\rho' = \|v_1\| + \cdots + \|v_n\|$ jó lesz. Teljes indukciót alkalmazunk ρ megkonstruálásához. Az $n = 1$ esetben $\rho = \|v_1\|$ nyilván jó lesz. Minden $1 \leq i \leq n$-re legyen $V_i = Kv_1 + \cdots + Kv_{i-1} + Kv_{i+1} + \cdots + Kv_n$. Ekkor $V = V_i \oplus Kv_i$. Az indukciós feltevésből következően a V_i $n-1$-dimenziós vektortér teljes a $\|\cdot\|$ normában. Speciálisan benne minden Cauchy-sorozat konvergál, ezért V_i zárt altér V-ben.Mivel az eltolás folytonos, ezért $V_i + v_i$ affin altér is zárt V-ben. Zártak véges uniója zárt, ezért a 0-nak van olyan ρ-sugarú környezete, mely diszjunkt $\bigcup_{i=1}^n (V_i + v_i)$-től. Belátjuk, hogy ez a ρ jó lesz. Legyen ugyanis $x = x_1 v_1 + \cdots + x_n v_n$ tetszőleges, és $1 \leq r \leq n$ olyan, amire $|x_r|$ maximális, azaz $|x_r| = |x|$. Ekkor

$$\|x_r^{-1} x\| = \left\| \frac{x_1}{x_r} v_1 + \cdots + v_r + \cdots + \frac{x_n}{x_r} v_n \right\| > \rho \ ,$$

hiszen $x_r^{-1} x \in V_r + v_r$. Beszorozva x_r-rel kapjuk, hogy $|x|\rho < \|x\|$. □

Legyen $|\cdot|'$ egy másik kiterjesztés. Ekkor a fenti lemma szerint $|\cdot| \sim |\cdot|'$, tehát a 4.1.5. Állítás miatt van olyan $s \in \mathbb{R}^{>0}$, amire $|x|' = |x|^s$ minden $x \in L$-re. Speciálisan ha $|\cdot|$ triviális K-n, akkor L-en is, ezért $|\cdot|'$ is triviális. Ha pedig $|\cdot|$ nemtriviális, akkor van olyan $x \in K$, melyre $|x| > 1$. Node $|\cdot|'$ is kiterjesztés, azaz K-n megegyezik $|\cdot|$-kel, tehát $|x| = |x|' = |x|^s$, azaz $s = 1$.

A teljesség ugyancsak következik a fenti Lemmából, hiszen a maximum normára nézve L teljes. □

4.4.7. Megjegyzés. Ha L egy nem feltétlenül véges, de algebrai bővítése K-nak, akkor a K-n levő abszolútérték még mindig egyértelműen terjeszthető ki L-re. Valóban, L ekkor a véges részbővítések uniója, és minden véges részbővítésre létezik és egyértelmű a kiterjesztés a 4.4.5. Tétel miatt. Viszont a teljesség már nem marad igaz végtelen algebrai bővítésekre.

4.5. Lokális testek klasszifikációja

A $|\cdot|$ nemarkhimédeszi abszolútértékről azt mondjuk, hogy *diszkrét*, ha a $|\cdot|\colon K^\times \to \mathbb{R}^{>0}$ homomorfizmus képe $\mathbb{Z}$-vel izomorf. Ez a homomorfizmus tétel alapján azzal ekvivalens, hogy $K^\times/\mathcal{O}_K^\times \cong \mathbb{Z}$. Ez a feltétel pedig épp azt jelenti, hogy $|\cdot|$ egy diszkrét additív értékelésből ered, azaz $\mathcal{O}_K$ egy DVR.

4.5.1. Definíció. Egy K testet egy $|\cdot|$ diszkrét értékeléssel *lokális testnek* nevezünk, ha K teljes és a maradékteste véges.

4.5.2. Példa. $\mathbb{Q}_p$ egy lokális test. Továbbá ha $K/\mathbb{Q}$ egy véges bővítés és $\mathfrak{p} \lhd \mathcal{O}_K$ egy prímideál, akkor K telítése a $\mathfrak{p}$-ből származó diszkrét értékelésre nézve is egy lokális test.

4.5.3. Állítás. *Legyen K egy teljes test egy diszkrét értékelésre nézve, melyben $\mathcal{O}_K$ az egészek gyűrűje, $(\pi) = \mathfrak{p} \lhd \mathcal{O}_K$ pedig az egyetlen maximális ideál. Ekkor $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n$. Hasonlóképp az $\mathcal{O}_K^\times$ egységcsoportot is felírhatjuk inverz limeszként: $\mathcal{O}_K^\times \cong \varprojlim_n \mathcal{O}_K^\times/U^{(n)}$, ahol $U^{(n)} := 1 + \mathfrak{p}^n\mathcal{O}_K$. Ez az izomorfizmus egyben homeomorfizmus is, ha $\mathcal{O}_K$-n és $\mathcal{O}_K^\times$-en a $|\cdot|$ által indukált topológiát vesszük, a $\varprojlim \mathcal{O}_K/\mathfrak{p}^n$, ill. $\varprojlim_n \mathcal{O}_K^\times/U^{(n)}$-n pedig a diszkrét topológiák inverz limeszét. Speciálisan ha K egy lokális test, akkor $\mathcal{O}_K$ és $\mathcal{O}_K^\times$ kompakt.*

Bizonyítás. Jelöljük f_n-nel a természetes $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}^n$ faktorleképezést. Ezeket összefűzve kapunk egy $f := \varprojlim f_n\colon \mathcal{O}_K \to \varprojlim \mathcal{O}_K/\mathfrak{p}^n$ gyűrűhomomorfizmust. Azt kell belátnunk, hogy f izomorfizmus.

Az injektivitáshoz legyen $x \in \mathrm{Ker}(f)$. Ekkor $x \in \mathfrak{p}^n$ minden $n \geq 1$-re, azaz $\pi^n \mid x$, így $x = 0$, hiszen $\mathcal{O}_K$ főideálgyűrű, speciálisan igaz benne a számelmélet alaptétele. A szürjektivitáshoz rögzítsük egy tetszőleges $J \subset \mathcal{O}_K$ reprezentánsrendszerét az $\mathcal{O}_K/\mathfrak{p}$-beli mellékosztályoknak. Vegyük észre, hogy minden $x_n + \mathfrak{p}^n \in \mathcal{O}_K/\mathfrak{p}^n$ elem $x_n + \mathfrak{p}^n = a_{0,n} + a_{1,n}\pi + \cdots + a_{n-1,n}\pi^{n-1} + \mathfrak{p}^n$ alakba írható, ahol $a_i \in J$. Valóban, $n = 1$-re ez világos, egyébként pedig indukció: van olyan $a_0 \in J$, melyre $x_n \equiv a_0 \pmod{\mathfrak{p}}$, és az indukciós feltevéssel $(x_n - a_0)/\pi$-t felírhatjuk a kívánt alakban. Továbbá az $(x_n + \mathfrak{p}^n)_n \in \prod \mathcal{O}_K/\mathfrak{p}^n$ sorozat kompatibilitása pontosan azt jelenti, hogy minden $n \leq m$-re és $i \leq n-1$-re $a_{i,n} = a_{i,m} =: a_i$. Ekkor az $x := \sum_{i=0}^\infty a_i\pi^n$ sor konvergens $\mathcal{O}_K$-ban (hiszen Cauchy és $\mathcal{O}_K$ teljes) és $f(x) = (x_n + \mathfrak{p}^n)_n \in \in \varprojlim \mathcal{O}_K/\mathfrak{p}^n$.

Ahhoz, hogy belássuk, hogy a fenti leképezés egy homeomorfizmus, elegendő megmutatnunk, hogy a 0 egy környezetbázisa a 0 egy környezetbázisába képződik. Valóban, az eltolás egy $a \in \mathcal{O}_K$ számmal egy homeomorfizmus mindkét oldalon, tehát a leképezés az a elem egy környezetbázisát is a képének egy környezetbázisába viszi. $\mathcal{O}_K$-ban a 0 egyik környezetbázisa a $\mathfrak{p}^n$ alakú részhalmazokból áll. Másrészt a $\prod_{n\geq 1} \mathcal{O}_K/\mathfrak{p}^n$-n levő szorzattopológiában a 0-nak egy környezetbázisát alkotják a

$$P_n = \underbrace{\{0\} \times \ldots \{0\}}_{n} \times \prod_{\nu \geq n+1} \mathcal{O}_K/\mathfrak{p}^\nu$$

alakú halmazok. Viszont $P_n \cap \varprojlim_\nu \mathcal{O}_K/\mathfrak{p}^\nu$ éppen $\mathfrak{p}^n$-nek felel meg a fenti izomorfizmusnál.

A multiplikatív csoportra vonatkozó izomorfizmus és homeomorfizmus következik az $\mathcal{O}_K$-ra vonatkozóból: gyűrűizomorfizmus izomorfizmust indukál a multiplikatív csoportokon is, sőt,

a részhalmaztopológiákban ez homeomorfizmus is. Másrészt vegyük észre, hogy $(\mathcal{O}_K/\mathfrak{p}^n)^\times = \mathcal{O}_K^\times/U^{(n)}$, ezért

$$\mathcal{O}_K^\times \cong (\varprojlim_n \mathcal{O}_K/\mathfrak{p}^n)^\times \cong \varprojlim_n (\mathcal{O}_K/\mathfrak{p}^n)^\times \cong \varprojlim \mathcal{O}_K^\times/U^{(n)} \ .$$

Ha most K lokális test, akkor $\mathcal{O}_K$, illetve $\mathcal{O}_K^\times$ véges halmazok inverz limesze, speciálisan a 4.3.4. Állítás miatt kompakt, hiszen minden véges halmaz kompakt a diszkrét topológiában. □

Speciálisan azt kaptuk, hogy $\mathbb{Z}_p$ is kompakt a p-adikus abszolútérték által indukált topológiában.

4.5.4. Következmény. *Ha K egy lokális test, akkor* lokálisan kompakt.

Bizonyítás. Valóban, minden $a \in K$-nak van olyan környezete, melynek lezárása kompakt: jelesül $a + \mathcal{O}_K$ (ami eleve nemcsak nyílt, hanem zárt is). □

4.5.5. Megjegyzés. A lokális testeket definiálhatnánk a fenti következmény segítségével úgy is, hogy egy K test lokális, ha lokálisan kompakt egy $|\cdot|$ abszolútértékre nézve (vö. [8] Def. 7.48). Ez a definíció nem teljesen ekvivalens: ha még azt is feltesszük, hogy $|\cdot|$ nemarkhimédeszi, akkor már ekvivalens. Viszont ez az utóbbi definíció magában foglalja az arkhimédeszi lokális testeket is: ezekből csak kettő van: $\mathbb{R}$ és $\mathbb{C}$.

4.5.6. Tétel. *A lokális testek éppen $\mathbb{Q}_p$ és $\mathbb{F}_p((t))$ véges bővítései.*

Bizonyítás. Először is $\mathbb{Q}_p$ és $\mathbb{F}_p((t))$ lokális testek, hiszen teljesek a p-adikus, illetve a t-adikus diszkrét értékelésre nézve, maradéktestük pedig $\mathbb{F}_p$ véges. Továbbá ha K egy n-edfokú $\mathbb{Q}_p$-nek vagy $\mathbb{F}_p((t))$-nek, akkor K teljes lesz a kiterjesztett értékelésre nézve a 4.4.5. Tétel miatt. Továbbá vegyük észre, hogy a kiterjesztett értékelés is diszkrét lesz: valóban, a $|\cdot|\colon K^\times \to \mathbb{R}^{>0}$ képe benne lesz $p^{\frac{1}{n}\mathbb{Z}}$-ben. Sőt, ha k-val jelöljük K maradéktestét, akkor $\dim_{\mathbb{F}_p} k \leq n < \infty$. Valóban, ha $\overline{\alpha_1}, \ldots, \overline{\alpha_r}$ lineárisan függetlenek $\mathbb{F}_p$ felett, akkor tetszőleges felemeltjeik is lineárisan függetlenek $\mathbb{Z}_p$ ill. $\mathbb{F}_p[\![t]\!]$ felett, azaz $r \leq n$.

Megfordítva legyen K egy lokális test. Mivel $|\cdot|$ diszkrét, ezért van olyan $\pi \in K$ elem, melyre $|\pi| < 1$, de ezen belül $|\pi|$ maximális. Ekkor $\mathfrak{p} = (\pi)$. Vegyük k egy J teljes reprezentánsrendszerét $\mathcal{O}_K$-ban. A 4.1.28. Tételhez hasonlóan ekkor K minden $x \neq 0$ eleme egyértelműen írható $x = \sum_{n=-N}^{\infty} a_n \pi^n$ alakba, ahol $a_n \in J$ $(n \geq -N)$.

Két esetet különböztetünk meg: $\mathrm{char}(K) = 0$ vagy $\mathrm{char}(K) = p$ valamilyen p prímre. Utóbbi esetben $\mathbb{F}_p$ résztest K-ban, speciálisan $\mathbb{F}_p[x]$ is részgyűrű $\mathcal{O}_K[x]$-ben. Ha most $\alpha \in k$ tetszőleges és $m_\alpha \in \mathbb{F}_p[x]$ a minimálpolinomja, akkor a Hensel lemma miatt m_α-nak van gyöke $\mathcal{O}_K$-ban is. Speciálisan ha $k = \mathbb{F}_p(\alpha)$, akkor azt kapjuk, hogy $\mathcal{O}_K$-nak van k-val izomorf részteste. Így a J reprezentánsrendszer választható ennek a résztestnek, speciálisan $K \cong k((\pi)) \cong k((t))$, azaz $\mathbb{F}_p((t))$-nek véges bővítése.

A másik esetben $\mathrm{char}(K) = 0$, tehát $\mathbb{Q} \leq K$. Szorítsuk meg a $|\cdot|$ abszolútértéket $\mathbb{Q}$-ra. Mivel $|\cdot|$ nemarkhimédeszi, ezért Ostrowski Tétele (4.1.11) szerint $|\cdot|$ ekvivalens $\mathbb{Q}$-n a p-adikus $|\cdot|_p$ abszolútértékkel valamilyen p prímszámra. Mivel K teljes, ezért $\mathbb{Q}_p$ is résztest K-ban. Már csak azt kell belátnunk, hogy a $K/\mathbb{Q}_p$ bővítés véges. Ehhez tekintsük a $v\colon K^\times \twoheadrightarrow \mathbb{Z}$ diszkrét értékelést, melyet – megfelelően normálva – a $|\cdot|$ logaritmusaként kapunk. Ekkor $v(\mathbb{Q}_p^\times) \leq \mathbb{Z}$ egy nemnulla részcsoport, speciálisan véges indexű. Legyen tehát $e := |v(K^\times) : v(\mathbb{Q}_p^\times)|$ az

index, ezt nevezzük a K test abszolút elágazási indexének. Sőt, mivel $v(\mathbb{Q}_p^\times)$-t generálja a $0 < < v(p) \in \mathbb{Z}$ elem, ezért $e = v(p)$. Másrészt $k/\mathbb{F}_p$ egy véges bővítés, hiszen K lokális, speciálisan k véges test. Legyen $f := |k : \mathbb{F}_p|$ az abszolút inerciafok. A továbbiakban megmutatjuk, hogy $|K : \mathbb{Q}_p| = ef$ véges. Vegyünk egy $\overline{b_1} = 1, \overline{b_2}, \ldots, \overline{b_f}$ $\mathbb{F}_p$-bázist k-ban, emeljük fel őket $\mathcal{O}_K$-ba $b_1 = 1, b_2, \ldots, b_f$ elemekkel. Legyen továbbá $\pi \in \mathcal{O}_K$ egy prímelem, azaz $v(\pi) = 1$. Belátjuk, hogy az

$$1, \pi, \ldots, \pi^{e-1}, b_2, b_2\pi, \ldots, b_2\pi^{e-1}, \ldots, b_f, \ldots, b_f\pi^{e-1} \tag{4.4}$$

elemek bázist alkotnak K-ban $\mathbb{Q}_p$ felett. Vegyük észre, hogy $v(\pi^e) = v(p)$, azaz $\frac{\pi^e}{p} \in \mathcal{O}_K^\times$ egység. Tehát K elemeinek $x = \sum_{n=-N}^{\infty} x_n\pi^n$ alakú felírásához hasonlóan, minden $x \neq 0$ elemet egyértelműen írhatunk a (4.4) elemek $\mathbb{Q}_p$-lineáris kombinációjaként. Valóban, mivel $v(\pi)$ generálja $v(K^\times)$-et, ezért van olyan $N \in \mathbb{Z}$, melyre $v(\pi^N x) = 0$, azaz $\pi^N x \in \mathcal{O}_K^\times$. N-et elosztva maradékosan e-vel kapunk egy $M \in \mathbb{Z}$ és egy $0 \leq j \leq e-1$ számot, melyekre $\pi^j p^M x \in \mathcal{O}_K^\times$. Mivel $\overline{b_1}, \ldots, \overline{b_f}$ bázis k-ban $\mathbb{F}_p$ fölött, ezért modulo π felírhatjuk $\pi^j p^M x$-et a $b_1, \ldots, b_f$ elemek egész együtthatós lineáris kombinációjaként. Ezt folytatva kapunk egy

$$x = \sum_{j=1}^{e-1} \pi^j \sum_{i=1}^{f} b_i \sum_{n=-M}^{\infty} a_{i,j,n} p^n$$

kifejtést, ahol $a_{i,j,n} \in \mathbb{Z}$, speciálisan rögzített i-re és j-re a $\sum_{n=-M}^{\infty} a_{i,j,n}p^n$ összeg konvergens $\mathbb{Q}_p$-ben. A felírás létezéséből és egyértelműségéből következik, hogy (4.4) bázis K-ban $\mathbb{Q}_p$ fölött. □

A fenti bizonyítás kísértetiesen hasonlít a fundamentális egyenletre (3.8.3. Állítás). Ez nem véletlen, hiszen ha K egy lokális test, akkor $\mathcal{O}_K$ egy diszkrét értékelésgyűrű, speciálisan Dedekind gyűrű. Ha pedig L/K egy véges bővítés, akkor 4.4.5. Tétel szerint L is egy lokális test, speciálisan az $\mathcal{O}_K$ Dedekind gyűrű egész lezártja L-ben éppen $\mathcal{O}_L$. Ha még az L/K bővítés szeparábilis is, akkor alkalmazható a 3.8.3. Állítás ebben a szituációban is, azaz $|L : K| = ef$, hiszen ebben az esetben $\mathcal{O}_L$ is egy lokális gyűrű, tehát egyetlen prímszám van. Sőt, ebben az esetben, amikor K teljes egy diszkrét értékelésre nézve, a szeparábilitást nem is kell feltenni. Ez lényegében következik a 4.5.6. Tétel bizonyításából.

4.5.7. Definíció. Ha L/K egy véges bővítése lokális testeknek, akkor az $e := |v(L^\times) : v(K^\times)|$ számot nevezzük a bővítés elágazási indexének, az $f := |l : k|$ számot pedig az inerciafoknak (l az L maradékteste). Azt mondjuk, hogy L/K elágazásmentes, vagy nem ágazik el, ha $e = 1$, vagyis ha $f = |L : K|$.

4.5.8. Következmény. *Legyen K egy lokális test. Ekkor $K^\times \cong \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)}$, ahol $\pi \in \mathcal{O}_K$ egy prímelem, $q = |k|$ a maradéktest elemszáma, $U^{(1)} = 1 + \mathfrak{p}$ az 1-egységcsoport (principal units, Einseinheiten).*

Bizonyítás. A $v\colon K^\times \twoheadrightarrow \mathbb{Z}$ homomorfizmus magja épp $\mathcal{O}_K^\times$, képét generálja $v(\pi)$. Így, mivel $\mathbb{Z}$ egy szabad Abel-csoport, ezért $K^\times \cong \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times$. Másrészt a k véges test multiplikatív csoportja $q-1$ rendű ciklikus, és a 4.4.3. Következmény miatt ez felemelhető $\mathcal{O}_K^\times$-be, a felemeltek nyilván $q-1$-edik egységgyökök. Ez azt jelenti, hogy az

$$1 \to U^{(1)} \to \mathcal{O}_K^\times \to k^\times \to 1$$

rövid egzakt sorozat hasadó. □

Ahogy azt később látni fogjuk, az $U^{(1)}$ csoport nem feltétlenül torziómentes, tartalmazhat p-hatványrendű egységgyököket is.

4.6. Elágazási részcsoportok

Legyen L/K egy véges Galois bővítése egy diszkrét értékelésre nézve teljes testeknek (azt nem tesszük fel, hogy a maradéktest véges). Jelöljük továbbá G-vel a $\mathrm{Gal}(L/K)$ Galois-csoportot. Ebben az esetben $\mathcal{O}_K$ és $\mathcal{O}_L$ diszkrét értékelésgyűrűk, speciálisan Dedekind gyűrűk. Tehát alkalmazhatjuk a 3.9. fejezetben tanultakat. Mivel csak egyetlen prím van, ezért G megegyezik a felbontási részcsoporttal. Továbbá $\mathcal{O}_L$ és $\mathfrak{p}_L$ nyilván G-invariáns, ami azt jelenti, hogy a G csoport hatása L-en megőrzi az abszolútértéket (ez egyébként a kiterjesztés konkrét megadásából is látszik: $N_{L/K}(\alpha) = N_{L/K}(g\alpha)$, ha $g \in G$, $\alpha \in L$). Speciálisan létezik egy $G \twoheadrightarrow \mathrm{Gal}(l/k)$ szürjektív homomorfizmus. Jelöljük ennek magját G_0-lal. Ekkor

$$G_0 = \{g \in G \mid g\alpha \equiv \alpha \pmod{\mathfrak{p}_L} \text{ minden } \alpha \in \mathcal{O}_L\text{-re}\} \ .$$

Ennek mintájára legyen

$$G_i := \{g \in G \mid g\alpha \equiv \alpha \pmod{\mathfrak{p}_L^{i+1}} \text{ minden } \alpha \in \mathcal{O}_L\text{-re}\} \ .$$

Ez nyilván részcsoport G-ben, hiszen ha $g, h \in G_i$, akkor $gh\alpha \equiv h\alpha \equiv \alpha \pmod{\mathfrak{p}_L^{i+1}}$, azaz $gh \in G_i$.Sőt, ha $g \in G_i$ és $h \in G$ tetszőleges, akkor h is megtartja az abszolútértéket, ezért

$$hgh^{-1}\alpha - \alpha = h(g(h^{-1}\alpha) - h^{-1}\alpha) \in h(\mathfrak{p}_L^{i+1}) = \mathfrak{p}_L^{i+1} \ ,$$

azaz $hgh^{-1} \in G_i$. Tehát $G_i \lhd G$ normálosztó minden $i \geq 0$-ra.

4.6.1. Definíció. A $G_0 \lhd G$ részcsoportot inerciarészcsoportnak, a G_1 részcsoportot pedig elágazási részcsoportnak nevezzük. A G_i részcsoportok ($i > 1$) a magasabb elágazási részcsoportok.

4.6.2. Állítás. *Ha i elég nagy, akkor $G_i = \{1\}$.*

Bizonyítás. Nyilván $G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i \supseteq \ldots$. Ha $1 \neq g \in G$ tetszőleges, akkor van olyan $\alpha \in \mathcal{O}_L$, melyre $g\alpha \neq \alpha$, speciálisan ha i elég nagy, akkor $g\alpha - \alpha \notin \mathfrak{p}_L^{i+1}$, hiszen $\bigcap \mathfrak{p}_L^{i+1} = \{0\}$. Speciálisan $g \notin G_i$, ha i elég nagy. Az állítás következik abból, hogy G véges. □

Legyen $\pi = \pi_L$ egy prímelem L-ben, azaz $\mathfrak{p}_L = (\pi)$. Valójában azt, hogy $g \in G_0$ benne van-e G_i-ben viszonylag könnyen el lehet dönteni: nem kell g hatását az összes $\alpha \in \mathcal{O}_L$-en megvizsgálni, elég csak π-n.

4.6.3. Lemma. *Ha L/K egy teljesen elágazó bővítés és $\pi \in L$ egy prímelem, akkor $L = K(\pi)$ és $\mathcal{O}_L = \mathcal{O}_K[\pi]$.*

Bizonyítás. Mivel L/K teljesen elágazó, ezért $l = k$. A 4.5.6. Tétel bizonyításához hasonlóan azt kapjuk, hogy $1, \pi, \ldots, \pi^{e-1}$ egy bázis L-ben K felett, illetve $\mathcal{O}_L$-ben is $\mathcal{O}_K$ felett. □

4.6.4. Állítás. *Ha $i \geq 1$, akkor $G_i = \{g \in G_0 \mid g\pi \equiv \pi \pmod{\pi^{i+1}}\}$.*

Bizonyítás. A $\subseteq$ tartalmazás világos, hiszen $\pi \in \mathcal{O}_L$. A másik irányhoz K-ról áttérve G_0 fixtestére feltehetjük, hogy $G = G_0$, azaz L/K teljesen elágazik. Tehát a 4.6.3. Lemma miatt $\mathcal{O}_L = \mathcal{O}_K[\pi]$. Így minden $\alpha \in \mathcal{O}_L$ elem felírható $f(\pi)$ alakban, ahol $f \in \mathcal{O}_K[x]$. Tehát ha egy $g \in G_0$ elemre teljesül, hogy $g\pi \equiv \pi \pmod{\pi^{i+1}}$, akkor $gf(\pi) = f(g\pi) \equiv f(\pi) \pmod{\pi^{i+1}}$. □

Jelöljük $U^{(i)} = 1 + \mathfrak{p}_L^i$-vel a modulo $\mathfrak{p}_L^i$ 1-gyel kongruens egységek részcsoportját $\mathcal{O}_L^\times$-ben. Speciálisan legyen $U^{(0)} = \mathcal{O}_L^\times$.

4.6.5. Tétel. *Minden $i \geq 0$ egész számra a*

$$\begin{aligned} \Theta_i \colon G_i/G_{i+1} &\to U^{(i)}/U^{(i+1)} \\ g &\mapsto \frac{g\pi}{\pi} \mod U^{(i+1)} \end{aligned}$$

homomorfizmus injektív és nem függ a $\pi \in L$ prímelem választásától.

Bizonyítás. Ha π fix prímelem, akkor a 4.6.4. Állítás szerint $g \in G_i$ esetén valóban $\frac{g\pi}{\pi} \equiv 1 \pmod{\pi^i}$, azaz benne van $U^{(i)}$-ben. Sőt, pontosan akkor van benne $U^{(i+1)}$-ben is, ha $g \in G_{i+1}$. Továbbá ha $u\pi$ egy másik prímelem ($u \in \mathcal{O}_L^\times$) és $g \in G_i$, akkor

$$\frac{g(u\pi)}{u\pi} = \frac{gu}{u} \cdot \frac{g\pi}{\pi} \equiv \frac{g\pi}{\pi} \pmod{U^{(i+1)}} ,$$

hiszen $u \in \mathcal{O}_L$ miatt $gu \equiv u \pmod{\pi^{i+1}}$, de mivel u egység, ezért eloszthatunk vele, azaz $\frac{gu}{u} \equiv 1 \pmod{\pi^{i+1}}$. Tehát Θ_i nem függ π választásától. Ez pedig azt jelenti, hogy $g, h \in G_i$ esetén

$$\Theta_i(gh) = \frac{gh\pi}{\pi} U^{(i+1)} = \frac{g(h\pi)}{h\pi} \cdot \frac{h\pi}{\pi} U^{(i+1)} = \Theta_i(g)\Theta_i(h) ,$$

hiszen $h\pi$ is egy prímelem L-ben. □

4.6.6. Következmény. *Ha L/K egy Galois-bővítése lokális testeknek, akkor* $\mathrm{Gal}(L/K)$ *feloldható.*

Bizonyítás. Ez esetben $G/G_0 \cong \mathrm{Gal}(l/k)$ véges testek bővítésének a Galois-csoportja, speciálisan ciklikus ([7] 6.7.8. Tétel). A 4.6.5. Tétel szerint viszont minden $i \geq 0$-ra G_i/G_{i+1} izomorf $U^{(i)}/U^{(i+1)}$ egy részcsoportjával, speciálisan Abel. Tehát G-nek van olyan normállánca, melyben a faktorok kommutatívak, azaz feloldható. □

4.6.7. Lemma. *Ha L egy tetszőleges diszkréten értékelt teljes test l maradéktesttel, akkor $U^{(0)}/U^{(1)} \cong l^\times$ és minden $i \geq 1$-re $U^{(i)}/U^{(i+1)} \cong l$. Speciálisan ha l egy p-karakterisztikájú véges test, akkor $U^{(1)}$ egy pro-p csoport (véges p-csoportok inverz limesze), $U^{(0)}/U^{(1)}$ rendje pedig relatív prím p-hez.*

Bizonyítás. Az $\mathcal{O}_L^\times \to l^\times$ homomorfizmus szürjektív, magja épp $U^{(1)}$. Másrészt ha π egy prímelem és $i \geq 1$, akkor $U^{(i)}$ minden eleme felírható $1 + a\pi^i$ alakban, ahol $a \in \mathcal{O}_L$. Ekkor a

$$\begin{aligned} U^{(i)} &\to l \\ 1 + a\pi^i &\mapsto a \pmod{\pi} \end{aligned}$$

egy szürjektív homomorfizmus, melynek magja épp $U^{(i+1)}$. Valóban, $(1 + a\pi^i)(1 + b\pi^i) \equiv 1 + {} + (a + b)\pi^i \pmod{\pi^{i+1}}$. □

4.6.8. Következmény. *Ha K egy lokális test, akkor $U^{(1)}$ egy pro-p csoport, azaz véges p-csoportok inverz limesze.*

Bizonyítás. Ha $i \geq 1$, akkor $U^{(i)}/U^{(i+1)}$ izomorf a maradéktest additív csoportjával, speciálisan elemi Abel p-csoport, hiszen a maradéktest egy p-karakterisztikájú véges test. Így indukcióval $U^{(1)}/U^{(i+1)}$ is p-hatvány rendű, a 4.5.3. Állítás miatt pedig $U^{(1)} = \varprojlim_i U^{(1)}/U^{(i+1)}$ pro-p csoport. □

4.6.9. Következmény. *Ha K egy lokális test, akkor G_1 egy véges p-csoport, G_0/G_1 egy p-hez relatív prím rendű ciklikus, G/G_0 pedig ciklikus.*

Bizonyítás. Véges test multiplikatív csoportja ciklikus és rendje p-hez relatív prím. Továbbá véges testek bővítésének Galois csoportja ciklikus. □

4.6.10. Tétel (Puiseux)**.** *A $\bigcup_{n=1}^{\infty} \mathbb{C}((t^{1/n}))$ test algebrailag zárt. Speciálisan ez a $\mathbb{C}((t))$ test algebrai lezártja.*

Bizonyítás. Legyen $K/\mathbb{C}((t))$ egy véges, n-edfokú Galois-bővítés, továbbá legyen $L = K\mathbb{C}((t^{1/n}))$ és $G = \mathrm{Gal}(L/\mathbb{C}((t)))$ a Galois csoport. Tekintsük a $\mathbb{C}((t))$ testen a következő abszolútértéket: $|0| := 0$, ill.

$$\left| \sum_{n=-N}^{\infty} a_n t^n \right| := e^N \ .$$

Ez egy nemarkhimédeszi értékelés, melyre nézve $\mathbb{C}((t))$ teljes, az egészek gyűrűje $\mathbb{C}[[t]]$, t egy prímelem, és $\mathbb{C}$ a maradéktest. A 4.4.5. Tétel miatt ez az abszolútérték kiterjeszthető L-re is. Tekintsük G-ben a G_i elágazási részcsoportokat ($i \geq 0$). Mivel $\mathbb{C}$ algebrailag zárt, és G/G_0 izomorf a maradéktestek bővítésének Galois-csoportjával, ezért $G = G_0$. Továbbá G_0/G_1 izomorf $\mathbb{C}^\times$ egy részcsoportjával izomorf, de mivel véges, ezért ciklikus. Végül ha $i \geq 1$, akkor G_i/G_{i+1} izomorf $\mathbb{C}$ additív csoportjának egy részcsoportjával, de mivel $\mathrm{char}(\mathbb{C}) = 0$ és G_i/G_{i+1} véges, ezért $G_i = G_{i+1}$ ha $i \geq 1$. Tehát $G_1 = \{1\}$, azaz G ciklikus. Viszont ciklikus csoportnak csak egyetlen adott rendű faktorcsoportja lehet, speciálisan mivel $|K : \mathbb{C}((t))| = n = |\mathbb{C}((t^{1/n})) : \mathbb{C}((t))|$, tehát a Galois-elmélet főtétele miatt $K = \mathbb{C}((t^{1/n}))$. Speciálisan $\bigcup_{n=1}^{\infty} \mathbb{C}((t^{1/n}))$ nem más, mint $\mathbb{C}((t))$ összes véges bővítésének az uniója, azaz az algebrai lezártja. □

4.7. A lokális Kronecker-Weber tétel

Ebben a fejezetben belátjuk a Kronecker-Weber tétel lokális változatát.

4.7.1. Tétel (Lokális Kronecker-Weber)**.** *Ha $K/\mathbb{Q}_p$ egy véges Galois-bővítés, melynek Galois csoportja Abel, akkor van olyan $n \geq 1$ egész, melyre $K \leq \mathbb{Q}_p(\mu_n)$.*

Bizonyítás. A bizonyítás több lépésben, lemmákon keresztül fog történni. A fő lépés az lesz, hogy klasszifikáljuk az összes olyan Abel-csoportot, mely előáll $\mathbb{Q}_p$ egy bővítésének Galois csoportjaként. Ha elhisszük a lokális Kronecker-Weber tételt, akkor nem nehéz megsejteni mi lesz a válasz. Először az elágazásmentes bővítéseket osztályozzuk. Ez jóval könnyebb feladat, hiszen ebben az esetben a Galois-csoport izomorf a maradéktestek Galois-csoportjával, speciálisan ciklikus.

4.7.2. Lemma. *Legyen $\mathbb{Q}_p \leq L \leq K$ két tetszőleges véges bővítése a p-adikus számok testének úgy, hogy K/L elágazásmentes. Ekkor K/L Galois,* $\mathrm{Gal}(K/L)$ *ciklikus, és van olyan p-hez relatív prím n egész szám, melyre $K = L(\mu_n)$. Megfordítva, tetszőleges $m \geq 1$ egész számhoz és $L/\mathbb{Q}_p$ véges bővítéshez létezik pontosan egy olyan K/L elágazásmentes bővítés, melyre* $\mathrm{Gal}(K/L) \cong Z_m$ *(m-edrendű ciklikus csoport).*

Bizonyítás. Először tegyük fel, hogy K/L Galois. Legyen $\mathcal{O}_L$ (ill. $\mathcal{O}_K$) az egészek gyűrűje L-ben (ill. K-ban), $\mathfrak{p}_L$ (ill. $\mathfrak{p}_K$) a maximális ideál, l (ill. k) pedig a maradéktest, és $G = \mathrm{Gal}(K/L)$ a Galois-csoport. Mivel K/L elágazásmentes, ezért $G_0 = \{1\}$, azaz $G \cong \mathrm{Gal}(k/l)$ ciklikus. Sőt, mivel k egy véges test, ezért minden 0-tól különböző eleme egységgyök, azaz egy véges hatványa 1. Ráadásul $|k^\times| = |k| - 1$, tehát nem osztható p-vel. Legyen $\overline{\alpha} \in k$ olyan, hogy $k = l(\overline{\alpha})$ és legyen $p \nmid n$ az $\overline{\alpha}$ rendje $k^\times$-ben. Speciálisan az $x^n - 1 = (x - \overline{\alpha})h(x)$, és mivel $x^n - 1$-nek nincs többszörös gyöke p karakterisztikában, ezért alkalmazhatjuk a Hensel Lemmát (4.4.2), mely szerint van olyan $\alpha \in \mathcal{O}_K$, melyre $\alpha + \mathfrak{p}_K = \overline{\alpha}$ és $\alpha^n = 1$. Sőt, ha $0 < d < n$, akkor $\alpha^d \neq 1$, hiszen akkor $\overline{\alpha}^d$ is 1 lenne, de $\overline{\alpha}$ rendje n. Node ha $f(x) \in \mathcal{O}_L[x]$ az α minimálpolinomja és $\overline{f}(x) \in l[x]$ a modulo $\mathfrak{p}_L$ redukció, akkor $\overline{f}(\overline{\alpha}) = 0$, speciálisan $\deg(f) = \deg(\overline{f}) \geq |k : l| = |K : L|$, hiszen $|k : l|$ nem más, mint $\overline{\alpha}$ minimálpolinomjának a foka. Így $K = L(\alpha) = L(\mu_n)$.

Vegyük észre, hogy ha K/L egy tetszőleges elágazásmentes bővítés, akkor K normális lezártja M is elágazásmentes (hiszen az K-val izomorf testek uniója), tehát $\mathrm{Gal}(M/L)$ ciklikus, speciálisan Abel. Így $\mathrm{Gal}(M/K)$ normálosztó $\mathrm{Gal}(M/L)$-ben, azaz K/L is normális bővítés, azaz Galois.

Megfordítva ha $m \geq 1$ tetszőleges, akkor létezik pontosan egy olyan k véges bővítése az l testnek, melynek foka m. Legyen $k = l(\overline{\alpha})$, ahol $\overline{\alpha}$ minimálpolinomja $\overline{f}$ és emeljük fel $\overline{f}$-et egy normált $f \in \mathcal{O}_L[x]$ polinommá. Nyilván f irreducibilis $\mathcal{O}_L$ (és így L) felett, ezért $K := L[x]/(f(x))$ egy $|k : l|$-edfokú bővítés L-nek. Másrészt K maradékteste nyilván k, hiszen $\overline{f}$-nek van benne gyöke. Tehát K/L elágazásmentes és m-edfokú.

Az egyértelműséghez legyen K_1 és K_2 két m-edfokú elágazásmentes bővítés. Ekkor K_1K_2 is elágazásmentes, ezért $\mathrm{Gal}(K_1K_2/L)$ ciklikus. Viszont ebben $\mathrm{Gal}(K_1K_2/K_1)$ és $\mathrm{Gal}(K_1K_2/K_2)$ két azonos rendű részcsoport, viszont ciklikus csoportnak csak egyetlen adott rendű részcsoportja van. Így a Galois-elmélet főtétele szerint $K_1 = K_2$. □

A fenti lemma osztályozza az elágazásmentes bővítéseket, speciálisan mindegyik egy körosztási bővítés. A következő lépésben rátérünk a teljesen elágazó bővítésekre. Először megvizsgáljuk az ún. *szelíden elágazó* (tamely ramified, zahmverzweigt) bővítéseket. Ezek azok a bővítések, melyek elágazási indexe relatív prím p-hez.

4.7.3. Lemma. *Legyen $\mathbb{Q}_p \leq L \leq K$ véges bővítés úgy, hogy K/L teljesen elágazik és $|K : L| = e$ relatív prím p-hez. Ekkor van olyan $\pi \in L$ prímelem és $\alpha \in K$, melyre $K = L(\alpha)$ és $\alpha^e = \pi$.*

Bizonyítás. Vegyünk egy β prímelemet K-ban és jelöljük $v\colon K^\times \to \mathbb{Z}$-vel a diszkrét értékelést, melyre $v(\beta) = 1$. Mivel K/L teljesen elágazik, ezért $|K : L| = |v(K^\times) : v(L^\times)|$, ezért ha π_0 egy tetszőleges prímelem L-ben, akkor $v(\pi_0) = e = v(\beta^e)$. Speciálisan $\beta^e = \pi_0 u$ valamely $u \in \mathcal{O}_K^\times$ egységre. Mivel K/L teljesen elágazik, ezért a maradéktestük megegyezik. Speciálisan van olyan $u_1 \in \mathcal{O}_L^\times$, melynek redukciója megegyezik u-éval, azaz $u = u_1\varepsilon$, ahol $\varepsilon \in 1 + \mathfrak{p}_K$. Node az $x^e - \varepsilon$ polinomnak van gyöke modulo $\mathfrak{p}_K$ (jelesül az 1), és mivel $(e, p) = 1$, ezért az

$x^e - 1$ polinomnak nincs többszörös gyöke p-karakterisztikában. Tehát használhatjuk ismét a Hensel Lemmát (4.4.2): van egy olyan $\gamma \in \mathcal{O}_K$, melyre $\gamma^e = \varepsilon$. Viszont ekkor $\alpha := \frac{\beta}{\gamma}$ és $\pi := \pi_0 u_1 \in \mathcal{O}_L$ választással $\alpha^e = \pi$. Mivel $L(\alpha)/L$ elágazási indexe is (legalább) e, hiszen $v(\alpha) = 1$, ezért $L(\alpha) = K$. □

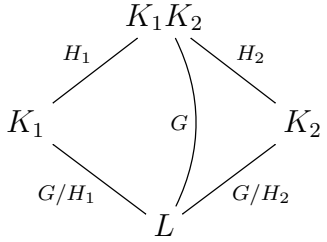
4.7.4. Lemma. $\mathbb{Q}_p(\mu_p) = \mathbb{Q}_p((-p)^{1/(p-1)})$.

Bizonyítás. Legyen ζ_p egy primitív p-edik egységgyök. Ekkor $\zeta_p - 1$ gyöke az $\frac{(x+1)^p-1}{x}$ polinomnak, ahol $px \mid \frac{(x+1)^p-1}{x} - x^{p-1} - p$. Speciálisan $u := \frac{(\zeta_p-1)^{p-1}}{-p} \equiv 1 \pmod{\zeta_p - 1}$. Viszont ekkor $u_1 = u^{-(1+p+\cdots+p^n+\dots)}$ limesz létezik $\mathbb{Q}_p(\zeta_p)$-ben, ez pedig u-nak $p-1$-edik gyöke. Speciálisan $-p$ is $p-1$-edik hatvány $\mathbb{Q}_p(\zeta_p)$-ben, de mivel az $x^{p-1} + p$ polinom irreducibilis (Schönemann-Eisenstein) $\mathbb{Q}_p$ fölött, ezért $\mathbb{Q}_p((-p)^{1/(p-1)}) \leq \mathbb{Q}_p(\zeta_p)$ azonos fokú bővítések, ezért megegyeznek. □

Legyen most $K/\mathbb{Q}_p$ Abel-féle, melynek foka egy q^m prímhatvány egy $q \neq p$ prímre. Legyen L a maximális elágazásmentes részbővítés K-ban, azaz az inerciarészcsoport fixteste és $e := |K : L|$. A 4.7.2. Lemma szerint ekkor van olyan $p \nmid n$ egész, melyre $L \leq \mathbb{Q}_p(\mu_n)$. Mivel e is q-hatvány, speciálisan p-hez relatív prím, ezért alkalmazhatjuk a 4.7.3. Lemmát: $K = L(\pi^{1/e})$ alkalmas $\pi \in L$ prímelemre. Node $L/\mathbb{Q}_p$ elágazásmentes, azaz p is prím L-ben. Speciálisan van egy olyan $u \in \mathcal{O}_L^\times$ egység, melyre $-p = \pi u$. Vegyük észre, hogy az $x^e - u$ egy gyökével való bővítés elágazásmentes. Valóban, az $x^e - u$ polinomnak nincs többszörös gyöke modulo $\mathfrak{p}_L$, tehát a Hensel Lemma (4.4.2) miatt van egy olyan elágazásmentes bővítése L-nek, melyben van gyöke. Viszont itt ismét alkalmazhatjuk a 4.7.2. Lemmát, mely szerint van olyan $M \geq 1$ egész, melyre $L(u^{1/e}) = L(\mu_M) \leq \mathbb{Q}_p(\mu_{Mn})$. Azt kaptuk, hogy $\mathbb{Q}_p((-p)^{1/e}) \leq K(\mu_{Mn})$.

4.7.5. Lemma. *Legyen K_1 és K_2 két Abel-féle bővítése egy tetszőleges L testnek. Ekkor* $\mathrm{Gal}(K_1K_2/L)$ *is Abel.*

Bizonyítás. Két Galois bővítés kompozíciója is Galois, legyen tehát $G := \mathrm{Gal}(K_1K_2/L)$. Mivel K_i/L Galois, ezért $H_i := \mathrm{Gal}(K_1K_2/K_i)$ normálosztó G-ben ($i = 1,2$).



Sőt, a feltétel miatt $G/H_i \cong \mathrm{Gal}(K_i/L)$ Abel ($i = 1,2$), azaz $[G,G] \leq H_1 \cap H_2$. Node $H_1 \cap H_2$ fixteste épp K_1K_2, hiszen $H_1 \cap H_2$ elemei K_1 és K_2 elemeit is helybenhagyják. A Galois-elmélet főtétele szerint ekkor $H_1 \cap H_2 = \{1\}$, ezért G Abel, hiszen kommutátora az $\{1\}$. □

A fenti Lemma szerint $K(\mu_{Mn}) = K\mathbb{Q}_p(\mu_{Mn})$ is Abel-féle bővítése $\mathbb{Q}_p$-nek. Viszont Abel csoportban minden részcsoport normálosztó, tehát minden közbülső test Galois. Speciálisan $\mathbb{Q}_p((-p)^{1/e})$ egy Galois-bővítése $\mathbb{Q}_p$-nek. Node $x^e + p$ irreducibilis $\mathbb{Q}_p$ fölött, tehát ha egyik gyökével vett bővítés Galois, akkor tartalmazza az összes többi gyököt is. Viszont $x^e + p$ többi gyöke a fix gyök ζ-szorosai, ahol ζ egy e-edik egységgyök. Speciálisan a ζ_e primitív e-edik egységgyök benne van $\mathbb{Q}_p((-p)^{1/e})$-ben. Node ez egy teljesen elágazó bővítése $\mathbb{Q}_p$-nek, $\mathbb{Q}_p(\zeta_e)$

viszont elágazásmentes (hiszen $(e,p)=1$). Ez viszont azt jelenti, hogy $\zeta_e \in \mathbb{Q}_p$. Node $\mathbb{Q}_p$-ben csak $p-1$-edik egységgyökök vannak. Valóban, ζ_e modulo p egy e-rendű elem az $\mathbb{F}_p$ testben (hiszen gyöke a $\Phi_e(x)$ polinomnak, ahol $p \nmid e$), speciálisan $e \mid p-1$. Azt kaptuk tehát, hogy $K \leq \mathbb{Q}_p((-p)^{1/e}, \mu_{nM}) \leq \mathbb{Q}_p(\mu_{pnM})$. Összefoglalva

4.7.6. Állítás. *Ha q^m egy p-től különböző q prím hatványa és $\mathrm{Gal}(K/\mathbb{Q}_p) \cong Z_{q^m}$, akkor van olyan $N \geq 1$, melyre $K \leq \mathbb{Q}_p(\mu_N)$.*

4.7.7. Lemma. *Legyen $K = \mathbb{Q}_p(\mu_p)$. Ekkor*

$$\begin{aligned} K^\times &= (1-\zeta_p)^{\mathbb{Z}} \times \mu_{p-1} \times U^{(1)} \ ; \\ (K^\times)^p &= (1-\zeta_p)^{p\mathbb{Z}} \times \mu_{p-1} \times U^{(p+1)} \ . \end{aligned}$$

Bizonyítás. Az első állítás következik a 4.5.8. Következményből, hiszen $(1-\zeta_p)$ egy prímelem K-ban és K maradékteste $\mathbb{F}_p$, aminek a multiplikatív csoportja $p-1$ rendű. A második állításhoz azt kell belátnunk, hogy $(U^{(1)})^p = U^{(p+1)}$. Egyrészt mivel $U^{(1)}/U^{(2)}$ izomorf $\mathbb{F}_p$ additív csoportjával, ezért minden $u \in U^{(1)}$ elem $u \equiv 1 + b(\zeta_p - 1) \pmod{(\zeta_p-1)^2}$ alakba írható, ahol $b \in \{0,1,\ldots,p-1\}$. Viszont $\zeta_p^b = (1+\zeta_p-1)^b \equiv 1 + b(\zeta_p-1) \pmod{(\zeta_p-1)^2}$. Speciálisan $u = \zeta_p^b u_1$ alakú, ahol $u_1 = 1 + \beta(\zeta_p-1)^2 \in U^{(2)}$. Így

$$u^p = \zeta_p^{pb} u_1^p = u_1^p = (1+\beta(\zeta_p-1)^2)^p \equiv 1 \pmod{(\zeta_p-1)^{p+1}} \ ,$$

hiszen $(\zeta_p-1)^{p-1}$ és p asszociáltak. Tehát $u^p \in U^{(p+1)}$. Visszafelé egy tetszőleges $1+\gamma(\zeta_p-1)^{p+1}$ alakú elemből kellene p-edik gyököt vonnunk. Ehhez használjuk az

$$(1+x)^{1/p} = \sum_{n=0}^{\infty} \binom{1/p}{n} x^n$$

binomiális sort, melyről megmutatjuk, hogy $v_p(x) \geq v_p((\zeta_p-1)^{p+1}) = \frac{p+1}{p-1}$ esetén konvergál. Ehhez vegyük észre, hogy

$$\begin{aligned} v_p\left(\binom{1/p}{n}\right) = v_p\left(\frac{1/p(1/p-1)\ldots(1/p-n+1)}{n!}\right) = \\ = v_p\left(\frac{(1-p)(1-2p)\ldots(1-(n-1)p)}{p^n n!}\right) = -n - v_p(n!) = -n - \frac{n-s}{p-1} \geq -n\frac{p}{p-1} \ , \end{aligned}$$

ahol s az n jegyeinek összege p-es számrendszerben. Node mivel $v_p(x) \geq \frac{p+1}{p-1}$, ezért

$$v_p\left(\binom{1/p}{n} x^n\right) \geq n\frac{p+1}{p-1} - n\frac{p}{p-1} = \frac{n}{p-1} \to \infty \quad (n \to \infty) \ .$$

Ez pedig azt jelenti, hogy az $(1+x)^{1/p}$ binomiális sor konvergál, ráadásul egy $U^{(1)}$-beli elemhez, hiszen $n \geq 1$ esetén $\binom{1/p}{n}x^n$ p-adikus értékelése pozitív. □

4.7.8. Lemma. *Legyen F egy p-től különböző karakterisztikájú test és $L = F(\zeta_p, \alpha^{1/p})$ valamilyen $\alpha \in F(\zeta_p)$ elemre. Tekintsük továbbá a $\chi\colon \mathrm{Gal}(F(\zeta_p)/F) \to \mathbb{F}_p^\times$ karaktert, melyre $g\zeta_p = \zeta_p^{\chi(g)}$ (ezt hívják a modulo p körosztási karakternek). Ha a $\mathrm{Gal}(L/F)$ Galois-csoport Abel, akkor minden $g \in \mathrm{Gal}(F(\zeta_p)/F)$ elemre $g\alpha \equiv \alpha^{\chi(g)} \pmod{(F(\zeta_p)^\times)^p}$.*

Bizonyítás. Legyen $G = \mathrm{Gal}(L/F)$ és $H = \mathrm{Gal}(L/F(\mu_p))$. Ekkor nyilván $H \lhd G$, hiszen $F(\mu_p)/F$ normális. Speciálisan G hat H-n a konjugálással, és mivel H Abel (azaz triviálisan hat saját magán a konjugálással), ezért ez a hatás átfaktorizálódik G/H-n, tehát a G/H csoport is hat H-n a konjugálással. G pontosan akkor Abel, ha ez a hatás triviális. Válasszunk egy $\beta \in L$ elemet, melyre $\beta^p = \alpha$. Ha $h \in H$, akkor van olyan $\omega(h) := \zeta$ p-edik egységgyök, melyre $h\beta = \omega(h)\beta$, hiszen $(h\beta)^p = h\alpha = \alpha$. Ekkor $\omega\colon H \to \mu_p$ egy csoporthomomorfizmus, mely nem függ β választásától. Legyen $g \in G/H$ tetszőleges. Ekkor

$$\frac{h\beta^{\chi(g)}}{\beta^{\chi(g)}} = \omega(h)^{\chi(g)} = g(\omega(h)) = g\left(\frac{h\beta}{\beta}\right) = \frac{ghg^{-1}(g\beta)}{g\beta} \ .$$

Ha G Abel, akkor $ghg^{-1} = h$, speciálisan a $\frac{\beta^{\chi(g)}}{g\beta}$ elemet fixálja H, azaz benne van $F(\zeta_p)$-ben. Speciálisan p-edik hatványa

$$\frac{\alpha^{\chi(g)}}{g\alpha} = \left(\frac{\beta^{\chi(g)}}{g\beta}\right)^p \in (F(\zeta_p)^\times)^p \ .$$

□

4.7.9. Megjegyzés. A 4.7.8. Lemma megfordítása is igaz, de erre nem lesz szükségünk a Kronecker-Weber tétel bizonyításához.

4.7.10. Állítás. *Ha p páratlan prím, akkor nincs olyan $L/\mathbb{Q}_p$ véges Galois-bővítés, melyre* $\mathrm{Gal}(L/\mathbb{Q}_p) \cong Z_p \times Z_p \times Z_p$.

Bizonyítás. Tegyük fel, hogy $L/\mathbb{Q}_p$ ilyen bővítés. A 2.3.9. Következmény szerint ekkor $L(\mu_p) = \mathbb{Q}_p(\mu_p)(\sqrt[p]{\alpha_1}, \sqrt[p]{\alpha_2}, \sqrt[p]{\alpha_3})$ alkalmas $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}_p(\mu_p)^\times$ elemekkel. Sőt, az

$$\alpha_1(\mathbb{Q}_p(\zeta_p)^\times)^p, \alpha_2(\mathbb{Q}_p(\zeta_p)^\times)^p, \alpha_3(\mathbb{Q}_p(\zeta_p)^\times)^p$$

elemek lineárisan függetlenek $\mathbb{F}_p$ felett a $\mathbb{Q}_p(\zeta_p)^\times/(\mathbb{Q}_p(\zeta_p)^\times)^p$ vektortérben. A 4.7.5. Lemma miatt $\mathrm{Gal}(L(\mu_p)/\mathbb{Q}_p)$ egy Abel csoport. Így a 4.7.8. Lemma szerint minden $g \in \Gamma := \mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$-re

$$g\alpha_i \equiv \alpha_i^{\chi(g)} \pmod{(\mathbb{Q}_p(\mu_p)^\times)^p} \ (i = 1,2,3) \ .$$

Speciálisan $i = 1,2,3$-ra

$$v_p(\alpha_i) = v_p(g\alpha_i) \equiv \chi(g)v_p(\alpha_i) \pmod{p} \ .$$

Node $\chi\colon \Gamma \to \mathbb{F}_p^\times$ egy izomorfizmus, speciálisan van olyan $g \in \Gamma$, melyre $\chi(g) \not\equiv 1 \pmod{p}$, ezért $p \mid v_p(\alpha_i)$. Tehát az α_i-ket leosztva egy-egy alkalmas p-edik hatvánnyal a 4.7.7. Lemma miatt feltehetjük, hogy $\alpha_i \in U^{(1)}$. Jelöljük B-vel az $\alpha_1, \alpha_2, \alpha_3$ elemek mellékosztályai által generált részcsoportot $U^{(1)}/U^{(p+1)}$-ben. A 4.7.7. Lemma szerint ez egy elemi Abel p-csoport, melyen hat a Γ ($p-1$ rendű ciklikus) csoport. A 4.7.8. Lemma szerint ez a hatás a B részcsoporton a χ körosztási karakteren keresztül történik.

4.7.11. Lemma. *Minden $j \geq 1$-re a Γ csoport az $U^{(j)}/U^{(j+1)}$ faktorcsoporton a χ körosztási karakter j-edik hatványán keresztül hat.*

Bizonyítás. Vegyük, hogy $\zeta_p - 1$ egy prímelem, és $U^{(j)}/U^{(j+1)}$ minden elemének van egy $1 + + b(\zeta_p - 1)^j$ alakú reprezentánsa, ahol $b = \{0,1,\ldots,p-1\}$. Viszont

$$g(\zeta_p - 1) = \zeta_p^{\chi(g)} - 1 = (\zeta_p - 1 + 1)^{\chi(g)} - 1 \equiv \chi(g)(\zeta_p - 1) \pmod{(\zeta_p - 1)^2},$$

így

$$g(1 + b(\zeta_p - 1)^j) \equiv 1 + b\chi(g)^j(\zeta_p - 1)^j \pmod{(\zeta_p - 1)^{j+1}}.$$

Tehát a hatás a χ^j karakteren keresztül történik. □

Mivel χ egy $p-1$-edrendű karakter, ezért $U^{(1)}/U^{(p+1)}$-nek két olyan részfaktora van, melyen Γ χ-n keresztül hat: $U^{(1)}/U^{(2)}$ és $U^{(p)}/U^{(p+1)}$. Mindkettő p-rendű az 4.6.7. Lemma miatt, tehát $U^{(1)}/U^{(p+1)}$-nek nincs p^3-rendű B részcsoportja, melyen Γ a χ karakteren keresztül hat. □

A fenti állításból következik a lokális Kronecker-Weber tétel minden $p > 2$ prímre a következő elemi csoportelméleti Lemma segítségével:

4.7.12. Lemma. *Legyen $1 \leq m \leq n_1, n_2$ egész számok. Ekkor a $G = Z_{p^{n_1}} \times Z_{p^{n_2}}$ Abel-csoportnak pontosan egy $H_m = Z_{p^m} \times Z_{p^m}$-nel izomorf faktorcsoportja van. Továbbá H_m-nek megvan a következő univerzális tulajdonsága: minden A Abel csoportra, melynek exponense osztója p^m-nek, és minden $\varphi\colon G \to A$ csoporthomomorfizmusra φ átfaktorizálódik H_m-en, azaz minden* $\mathrm{Ker}(\varphi)$ *tartalmazza a $G \twoheadrightarrow H_m$ csoporthomomorfizmus N_m magját.*

Bizonyítás. Jelöljük $Z_{p^{n_i}}$ (egyik) generátorelemét e_i-vel ($i = 1,2$). Mivel A-ban minden elem p^m-edik hatványa az egységelem, ezért $e_i^{p^m}$ benne van tetszőleges $\varphi\colon G \to A$ csoporthomomorfizmus magjában. Node $G/\langle e_1^{p^m}, e_2^{p^m}\rangle \cong Z_{p^m} \times Z_{p^m} = H_m$, tehát $N_m = \langle e_1^{p^m}, e_2^{p^m}\rangle \leq \mathrm{Ker}(\varphi)$. Sőt, ugyanezt $A = H_m$-re alkalmazva azt is megkapjuk, hogy H_m pontosan egyféleképpen áll elő G faktorcsoportjaként (hiszen ekkor $\mathrm{Ker}(\varphi) = N_m$). □

Legyen tehát $K/\mathbb{Q}_p$ egy tetszőleges Galois-bővítés, melyre $A = \mathrm{Gal}(K/\mathbb{Q}_p)$ Abel. Ekkor a véges Abel-csoportok alaptétele miatt G felírható prímhatványrendű ciklikus csoportok direkt szorzataként. Speciálisan K előáll olyan testek uniójaként, melyek $\mathbb{Q}_p$ feletti Galois-csoportja prímhatványrendű ciklikus, elég tehát feltenni, hogy már maga $A \cong Z_{q^m}$ valamilyen q prímre. Ha $q \neq p$, akkor a 4.7.6. Állítás miatt K benne van egy körosztási bővítésben. Legyen tehát $q = p > 2$ és $A = \mathrm{Gal}(K/\mathbb{Q}_p) \cong Z_{p^m}$. Már van egy teljesen elágazó K_r bővítésünk p^m-rendű ciklikus Galois csoporttal, mégpedig a $\mathbb{Q}_p(\mu_{p^{m+1}})$ testbeli fixteste a $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^{m+1}})/\mathbb{Q}_p) \cong Z_{p-1} \times Z_{p^m}$ csoport Z_{p-1}-gyel izomorf részcsoportjának. Továbbá a 4.7.2. Lemma miatt van egy K_u elágazásmentes bővítésünk is Z_{p^m}-nel izomorf Galois-csoporttal, sőt, $K_u = \mathbb{Q}_p(\mu_n)$ alkalmas n egész számmal.

4.7.13. Állítás. *Ekkor $K \leq K_rK_u$, azaz K benne van egy körosztási bővítésben.*

Bizonyítás. Tegyük fel, hogy $K \not\leq K_rK_u$ és legyen $L = KK_rK_u$, valamint $G := \mathrm{Gal}(L/\mathbb{Q}_p)$. Ekkor a 4.7.5. Lemma szerint G egy p-hatványrendű Abel csoport, amit legfeljebb 2 elem generál a 4.7.10. Állítás miatt, hiszen különben lenne G-nek $Z_p \times Z_p \times Z_p$-vel izomorf faktorcsoportja, ami a Galois-elmélet főtétele alapján $\mathbb{Q}_p$ egy alkalmas bővítésének lenne a Galois csoportja. Legyen tehát $G \cong Z_{p^{n_1}} \times Z_{p^{n_2}}$. Másrészt a 4.7.5. Lemma ismételt alkalmazásával $\mathrm{Gal}(K_rK_u/\mathbb{Q}_p) \cong Z_{p^m} \times Z_{p^m}$, mely előáll G faktorcsoportjaként. Speciálisan $m \leq n_1, n_2$. Viszont A exponense p^m, ezért a 4.7.12. Lemma szerint a $G \twoheadrightarrow A$ faktorleképezés magja tartalmazza a $G \twoheadrightarrow \mathrm{Gal}(K_rK_u/\mathbb{Q}_p)$ faktorleképezés magját. Ez pedig a Galois elmélet főtétele szerint pont azt jelenti, hogy $K \leq K_rK_u$ ellentmondva a feltevésünknek. □

Tehát a lokális Kronecker-Weber tétel bizonyításából csak a $p = q = 2$ eset maradt meg. Ehhez legyen $\mathrm{Gal}(K/\mathbb{Q}_2) \cong Z_{2^m}$. A $p > 2$ esethez hasonlóan van már egy K_u elágazásmentes bővítésünk, melyre $\mathrm{Gal}(K_u/\mathbb{Q}_2) \cong Z_{2^m}$. Másrészt van egy $K_r = \mathbb{Q}_2(\mu_{2^{m+2}})$ bővítésünk $\mathrm{Gal}(K_r/\mathbb{Q}_2) \cong Z_2 \times Z_{2^m}$ Galois-csoporttal. Mivel $K_u \cap K_r = \mathbb{Q}_2$, ezért $\mathrm{Gal}(K_uK_r/\mathbb{Q}_2) \cong Z_2 \times$ $\times Z_{2^m} \times Z_{2^m}$. Tegyük fel, hogy $K \not\leq K_rK_u$. Ekkor $G := \mathrm{Gal}(KK_rK_u/\mathbb{Q}_2)$ egy 2-hatványrendű Abel-csoport, amit legfeljebb 4 elem generál, és $Z_2 \times Z_{2^m} \times Z_{2^m}$ előáll G egy faktorcsoportjaként. Most alkalmazzuk a 4.7.12. Lemma következő variánsát:

4.7.14. Lemma. *Legyen $2 \leq m \leq n_1, n_2$ egész számok. Ekkor a $G = Z_2 \times Z_{2^{n_1}} \times Z_{2^{n_2}}$ Abel-csoportnak pontosan egy $H_m = Z_2 \times Z_{2^m} \times Z_{2^m}$-nel izomorf faktorcsoportja van. Továbbá H_m-nek megvan a következő univerzális tulajdonsága: minden A Abel csoportra, melynek exponense osztója 2^m-nek, és minden $\varphi\colon G \to A$ csoporthomomorfizmusra φ átfaktorizálódik H_m-en, azaz minden $\mathrm{Ker}(\varphi)$ tartalmazza a $G \twoheadrightarrow H_m$ csoporthomomorfizmus N_m magját.*

Bizonyítás. A 4.7.12. Lemma bizonyításához hasonlóan H_m a G legnagyobb 2^m-exponensű faktora, hiszen ez nem más, mint a generátorok 2^m-edik hatványai általa generált részcsoport szerinti faktor. □

A 4.7.14. Lemma miatt tehát ha K nincs benne K_rK_u-ban, azaz a Galois csoportja nem faktorizálódik át H_m-en, akkor G nem lehet $Z_2 \times Z_{2^{n_1}} \times Z_{2^{n_2}}$ alakú. Mivel G-t legfeljebb 4 elem generálja, ezért vagy ténylegesen 4 elemű a minimális generátorrendszere, amikor előáll $(Z_2)^4$ a G-nek egy faktorcsoportjaként, vagy ha 3 elem generálja, akkor mindegyik tényező legalább 4-rendű ciklikus (különben $G \cong Z_2 \times Z_{2^{n_1}} \times Z_{2^{n_2}}$ alakú lenne). Belátjuk, hogy egyik sem lehetséges.

4.7.15. Állítás. *$\mathbb{Q}_2$-nek nincs olyan K Galois bővítése, melynek Galois csoportja $(Z_2)^4$-nel izomorf.*

Bizonyítás. Minden másodfokú bővítése $\mathbb{Q}_2$-nek egy nemnégyzet $\alpha \in \mathbb{Q}_2^\times$ gyökével való bővítés. Tehát egy $(Z_2)^4$-nel izomorf Galois-csoportú bővítéshez szükségünk lenne négy

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{Q}_2^\times$$

elemre, amik lineárisan függetlenek $\mathbb{F}_2$ fölött a $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ vektortérben (elemi Abel 2-csoportban). Node $\mathbb{Q}_2(\mu_2) = \mathbb{Q}_2$ multiplikatív csoportját jellemzi a 4.7.7. Lemma. Eszerint $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong$ $Z_2 \times U^{(1)}/U^{(3)} \cong Z_2^3$, viszont ez csak 3-dimenziós, ezért nincs 4 lineárisan független eleme. □

4.7.16. Állítás. *$\mathbb{Q}_2$-nek nincs olyan N bővítése, melynek Galois-csoportja $(Z_4)^3$-nal izomorf.*

Bizonyítás. Tegyük fel, hogy $G = \mathrm{Gal}(N/\mathbb{Q}_2) \cong Z_4^3$ valamilyen N testre. Ekkor $i = \sqrt{-1} \in$ $\in N$, hiszen egyébként kapnánk egy olyan 2-hatvány fokú Abel-féle bővítést, melynek Galois csoportja nem generálható 3 elemmel, ez pedig az előző eset miatt nem lehetséges. Mivel G minden 2-indexű részcsoportja tartalmaz egy $Z_4 \times Z_4$-gyel izomorf részcsoportot (véges Abel-csoportok alaptétele), ezért van egy olyan $\mathbb{Q}_2(i) \leq L \leq N$ résztest, melyre $\mathrm{Gal}(L/\mathbb{Q}_2) \cong Z_4 =$ $= \langle\sigma\rangle$. Írjuk L-et $L = \mathbb{Q}_2(i, \alpha)$ alakba, ahol $\alpha^2 \in \mathbb{Q}_2(i)$. Ekkor σ^2 generálja $\mathrm{Gal}(L/\mathbb{Q}_2(i))$-t és $\sigma(i) = -i$. Sőt, $\sigma^2(\alpha) = -\alpha$, hiszen $(\sigma^2(\alpha))^2 = \sigma^2(\alpha^2) = \alpha^2$. Hasonlóan $\sigma^2(\sigma(\alpha)) = -\sigma(\alpha)$, hiszen $\sigma(\alpha)$ négyzete is $\mathbb{Q}_2(i)$-ben van. Azt kaptuk, hogy σ^2 fixálja $\frac{\sigma(\alpha)}{\alpha}$-t, ezért az $\mathbb{Q}_2(i)$-ben van. Írjuk tehát $\frac{\sigma(\alpha)}{\alpha}$-t

$$\frac{\sigma(\alpha)}{\alpha} = a + bi$$

alakba, ahol $a, b \in \mathbb{Q}_2$. Ekkor

$$\frac{\sigma^2(\alpha)}{\sigma(\alpha)} = \sigma(\frac{\sigma(\alpha)}{\alpha}) = \sigma(a+bi) = a - bi \ .$$

Azt kaptuk, hogy

$$-1 = \frac{\sigma^2(\alpha)}{\alpha} = (a+bi)(a-bi) = a^2 + b^2 \ .$$

Ez pedig ellentmond az alábbi lemmának:

4.7.17. Lemma. *A $a^2 + b^2 = -1$ egyenletnek nincs megoldása $\mathbb{Q}_2$-ben.*

Bizonyítás. A közös nevező négyzetével beszorozva a fenti egyenlet az $x^2+y^2+z^2 = 0$ egyenlet egy nemtriviális megoldásához vezetne. Mivel ez az egyenlet már homogén, feltehetjük, hogy $x, y, z \in \mathbb{Z}_2$ és legalább az egyikük nem osztható 2-vel. Viszont ennek az egyenletnek nincs nemtriviális megoldása modulo 8, tehát $\mathbb{Z}_2$-ben sem lehet. □

Tehát $\mathbb{Q}_2$-nek nincs olyan bővítése sem, melynek Galois-csoportja $Z_4 \times Z_4 \times Z_4$-gyel izomorf. □

Ezzel a lokális Kronecker-Weber tételt a $p = 2$ esetben is igazoltuk. □

5. fejezet

Globális testek

5.1. Értékelések és prímideálok kapcsolata

Legyen $K/\mathbb{Q}$ egy véges bővítés (azaz K egy *globális számtest*). Jelöljük $\mathcal{O}_K$-val az egészek gyűrűjét K-ban. Legyen továbbá $\mathfrak{p} \lhd \mathcal{O}_K$ egy tetszőleges prímideál. Ekkor $\mathfrak{p}$-hez tartozik egy $v_\mathfrak{p}\colon K^\times \to \mathbb{Z}$ diszkrét értékelés: $0 \neq \alpha \in K$ esetén $v_\mathfrak{p}(\alpha)$ legyen $\mathfrak{p}$ kitevője az $\alpha\mathcal{O}_K$ törtideál prímtényezős felbontásában. Ehhez a diszkrét értékeléshez pedig tartozik egy nemarkhimédeszi abszolútérték: $|\alpha|_\mathfrak{p} := |N_{K/\mathbb{Q}}(\mathfrak{p})|^{-v_\mathfrak{p}(\alpha)}$. (Itt $|N_{K/\mathbb{Q}}(\mathfrak{p})|$ helyett bármely más 1-nél nagyobb valós számot választva ekvivalens abszolútértéket kapunk.) Visszafelé legyen $|\cdot|\colon K \to \mathbb{R}^{\geq 0}$ egy tetszőleges nemtriviális nemarkhimédeszi abszolútérték és $\alpha \in \mathcal{O}_K$. Mivel α algebrai egész, ezért gyöke egy egész együtthatós normált polinomnak, azaz létezik $a_0, \ldots, a_{n-1} \in \mathbb{Z}$, melyekre $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Az ultrametrikus egyenlőtlenséget használva azt kapjuk, hogy

$$|\alpha|^n \leq \max_{0\leq i\leq n-1}(|a_i||\alpha|^i) \leq \max_{0\leq i\leq n-1}(|\alpha|^i)\ ,$$

hiszen egész számok abszolútértéke legfeljebb 1 a 4.1.10. Állítás miatt. Ez pedig azt jelenti, hogy $|\alpha| \leq 1$. Továbbá $|\cdot|$ nemtrivialitása miatt $\mathfrak{p} := \{\alpha \in \mathcal{O}_K \mid |\alpha| < 1\}$ egy nemnulla prímideál $\mathcal{O}_K$-ban. Ez viszont Ostrowski Tételének (4.1.11) bizonyításához hasonlóan azt jelenti, hogy $|\cdot|$ ekvivalens a $|\cdot|_\mathfrak{p}$ abszolútértékkel. Így egy kölcsönösen egyértelmű megfeleltetést létesítettünk a K-n lévő nemarkhimédeszi abszolútértékek ekvivalenciaosztályai és $\mathcal{O}_K$ prímideáljai között (a triviális abszolútérték a (0) prímideálhoz tartozik). K telítését a $|\cdot|_\mathfrak{p}$ abszolútértékre nézve $K_\mathfrak{p}$-vel jelöljük.

Legyen most L/K egy véges bővítés. Vegyük észre, hogy ha $P \lhd \mathcal{O}_L$ egy prímideál, akkor $|\cdot|_P$ megszorítása K-ra ekvivalens $|\cdot|_\mathfrak{p}$-vel, ha $\mathfrak{p} = P \cap \mathcal{O}_K$. Tehát $|\cdot|_\mathfrak{p}$ kiterjesztései L-re az L-beli $\mathfrak{p}$ fölötti prímeknek felelnek meg. Hogy ezt a kapcsolatot mélyebben is megértsük, írjuk L-et $L = K(\alpha)$ alakba alkalmas $\alpha \in L$-lel. Legyen $f(x) \in K[x]$ az α minimálpolinomja, amit bontsunk $f(x) = f_1(x)\cdots f_r(x)$ irreducibilisek szorzatára a bővebb $K_\mathfrak{p}$ test fölött (az $f_i \in K_\mathfrak{p}[x]$ polinomok mind különbözők, hiszen f-nek nincs többszörös gyöke). Ekkor

$$L \otimes_K K_\mathfrak{p} \cong K[x]/(f(x)) \otimes_K K_\mathfrak{p} \cong K_\mathfrak{p}[x]/(f(x)) \cong \bigoplus_{i=1}^{r} K_\mathfrak{p}[x]/(f_i(x)) =: \prod_{i=1}^{r} L_i\ .$$

Vegyük észre, hogy $K_\mathfrak{p}$ teljessége miatt az L_i testekre egyértelműen terjed ki $|\cdot|_\mathfrak{p}$, sőt, a kiterjesztésre nézve L_i teljes. Másrészt a fenti azonosításnál $L \otimes 1 \leq L \otimes_K K_\mathfrak{p}$ vetülete L_i-re

egy L-lel izomorf sűrű résztest L_i-ben. Speciálisan L_i az L telítése a $|\cdot|_\mathfrak{p}$ abszolútérték egyik kiterjesztésére nézve. Megfordítva, ha L_P az L telítése a $|\cdot|_\mathfrak{p}$ értékelés egy $|\cdot|_P$ L-re való kiterjesztésére nézve, akkor a természetes tartalmazások indukálnak egy

$$\begin{array}{ccc} L & \hookrightarrow & L_P \\ \uparrow & & \uparrow \\ K & \hookrightarrow & K_\mathfrak{p} \end{array}$$

kommutatív diagrammot, ahol $L_P = K_\mathfrak{p}(\alpha)$, hiszen utóbbi teljes és tartalmazza $L = K(\alpha)$-t. Viszont ekkor $L_P \cong L_i$ valamilyen $i = 1, \ldots, r$-re, hiszen α minimálpolinomja az f_i polinomok egyike. Összefoglalva azt kaptuk, hogy

5.1.1. Állítás. *Ha L/K globális számtestek egy véges bővítése és $0 \neq \mathfrak{p} \lhd \mathcal{O}_K$ egy prímideál, akkor*

$$L \otimes_K K_\mathfrak{p} \cong \prod_{i=1}^{r} L_i \ ,$$

ahol az L_i testek az L telítettjei a $|\cdot|_\mathfrak{p}$ abszolútérték különböző kiterjesztéseire nézve.

Tegyük fel a továbbiakban, hogy L/K egy Galois-bővítés $G = \mathrm{Gal}(L/K)$ Galois-csoporttal. Ekkor az $L = K(\alpha)$ test normális bővítése K-nak, azaz az $f(x)$ minimálpolinomja α-nak gyöktényezők szorzatára bomlik L-ben. Viszont mivel L résztest L_i-ben, ezért L_i-ben is gyöktényezők szorzatára bomlik f, speciálisan f_i is. Tehát az $L_i/K_\mathfrak{p}$ bővítés is Galois minden $i = 1, \ldots, r$-re. Jelöljük G_P-vel a P prím felbontási részcsoportját G-ben. Vegyük észre, hogy G nemcsak a $\mathfrak{p}$ feletti prímek halmazán, hanem $|\cdot|_\mathfrak{p}$ kiterjesztésein is tranzitívan hat, hiszen ezek egymásnak felelnek meg. Ha most $g \in G_P$, akkor g stabilizálja a $|\cdot|_P$ kiterjesztést, azaz minden $\beta \in L$-re $|g\alpha|_P = |\alpha|_P$. Speciálisan g Cauchy-sorozatot Cauchy-sorozatba visz, ezért folytonosan kiterjed az L_P test egy testautomorfizmusává, azaz a $\mathrm{Gal}(L_P/K_\mathfrak{p})$ Galois-csoport egy elemévé.

5.1.2. Állítás. *A fenti leképezés izomorfizmust létesít G_P és $\mathrm{Gal}(L_P/K_\mathfrak{p})$ között.*

Bizonyítás. Az injektivitás világos, hiszen ha g fixen hagyja L_P minden elemét, akkor nyilván L minden elemét is. A szürjektivitáshoz vegyük észre, hogy $|\mathrm{Gal}(L_P/K_\mathfrak{p})| = \dim_{K_\mathfrak{p}} L_P$. Mivel G tranzitívan hat a $|\cdot|_\mathfrak{p}$ kiterjesztésein, ezért az L_i testeken is, azaz $\dim_{K_\mathfrak{p}} L_P = \dim_{K_\mathfrak{p}} L_i$ minden i-re. Tehát

$$r|G_P| = |G| = \dim_K L = \dim_{K_\mathfrak{p}} L \otimes_K K_\mathfrak{p} = \sum_{i=1}^{r} \dim_{K_\mathfrak{p}} L_i = r \dim_{K_\mathfrak{p}} L_P = r|\mathrm{Gal}(L_P/K_\mathfrak{p})| \ ,$$

speciálisan a leképezés szürjektív, hiszen injektív és a két oldal rendje megegyezik. □

Tehát G_P nem más, mint a megfelelő lokális bővítés Galois-csoportja. Sőt, a 3.9.5. és 4.6.1. Definíciók kompatibilisek egymással, hiszen igaz a következő:

5.1.3. Állítás. *Az $\mathcal{O}_K/\mathfrak{p}$ maradéktest izomorf a telített $K_\mathfrak{p}$ test maradéktestével. Speciálisan az e elágazási indexet és az f inerciafokot is le lehet olvasni lokálisan.*

Bizonyítás. Jelöljük $\mathcal{O}_\mathfrak{p}$-vel az $\mathcal{O}_K$ gyűrű lokalizáltját a $\mathfrak{p}$ prímideálnál (tehát invertálunk minden $\mathfrak{p}$-n kívüli elemet $\mathcal{O}_K$-ban, speciálisan $\mathcal{O}_\mathfrak{p} \leq K$) és $\mathfrak{m}_\mathfrak{p}$-vel a maximális ideált $\mathcal{O}_\mathfrak{p}$-ben. Legyen továbbá $\hat{\mathcal{O}}_\mathfrak{p}$ az értékelésgyűrű $K_\mathfrak{p}$-ben, és $\hat{\mathfrak{m}}_\mathfrak{p}$ a maximális ideál. A 3.7.3. Állítás szerint $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$. Másrészt minden $\beta \in \hat{\mathcal{O}}_\mathfrak{p}$-beli elemhez van egy hozzá konvergáló K-beli sorozat, speciálisan van egy olyan $\alpha \in K$, melyre $\alpha \equiv \beta \pmod{\hat{\mathfrak{m}}_\mathfrak{p}}$. Viszont ekkor $|\alpha|_\mathfrak{p} \leq 1$, azaz $\alpha \in \mathcal{O}_\mathfrak{p}$. Ez viszont azt jelenti, hogy $\beta + \hat{\mathfrak{m}}_\mathfrak{p}$ benne van a természetes $\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} \hookrightarrow \hat{\mathcal{O}}_\mathfrak{p}/\hat{\mathfrak{m}}_\mathfrak{p}$ homomorfizmus képében. □

5.2. A globális Kronecker-Weber tétel

5.2.1. Tétel (Kronecker–Weber)**.** *Ha $L/\mathbb{Q}$ egy olyan Galois-bővítése a racionális számtestnek, melynek Galois-csoportja Abel, akkor van olyan $n \geq 1$ egész szám, melyre L benne van a $\mathbb{Q}(\mu_n)$ n-edik körosztási testben.*

Bizonyítás. Legyen S az L-ben elágazó (racionális) prímek véges halmaza, és minden $p \in S$-re válasszunk egy $\mathfrak{p} \mid p$ prímet L-ben. Ekkor a 5.1.2. Állítás szerint $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$ izomorf a $\mathrm{Gal}(L/\mathbb{Q})_\mathfrak{p}$ felbontási részcsoporttal, speciálisan Abel. Tehát a 4.7.1. Tétel szerint van olyan n_p egész szám, melyre $L_\mathfrak{p} \leq \mathbb{Q}_p(\mu_{n_p})$. Legyen e_p a p prím kitevője az n_p prímtényezős felbontásában, azaz $n_p = p^{e_p} n_p'$, ahol $p \nmid n_p'$. Belátjuk, hogy $L \leq \mathbb{Q}(\mu_n)$, ahol $n = \prod_{p \in S} p^{e_p}$. Legyen ugyanis $M = L(\mu_n)$, azt kell belátnunk, hogy $M = \mathbb{Q}(\mu_n)$.

Először is vegyük észre, hogy $G := \mathrm{Gal}(M/\mathbb{Q})$ is Abel a 4.7.5. Lemma miatt. Továbbá ha P egy tetszőleges prím M-ben $\mathfrak{p}$ fölött, akkor $M_P = L_\mathfrak{p}(\mu_n) = \mathbb{Q}_p(\mu_n) = \mathbb{Q}_p(\mu_{n'})(\mu_{p^{e_p}})$, ahol $p \nmid n'$. Viszont ekkor a 3.12.6. Következmény és az 5.1.3. Állítás szerint az $M_P/\mathbb{Q}_p$ bővítés elágazási indexe pontosan $\varphi(p^{e_p})$. Legyen $I_p \leq G_P \leq G$ az inerciarészcsoport minden $p \in S$-re, ennek rendje tehát $|I_p| = \varphi(p^{e_p})$. Jelöljük továbbá I-vel az I_p ($p \in S$) részcsoportok által generált részcsoportot G-ben. Mivel az elágazási index összeszorzódik bővítések egymásutánjában, ezért az M^I fixtest semmilyen prímben sem ágazhat el, hiszen minden $p \in S$-re az M/M^I-beli és az $M/\mathbb{Q}$-beli elágazási index megegyezik. Viszont ekkor a 3.8.10. Következmény szerint $M^I = \mathbb{Q}$, azaz $I = G$ (Galois-elmélet főtétele). Tehát

$$|M : \mathbb{Q}| = |I| \leq \prod_{p \in S} |I_p| = \prod_{p \in S} \varphi(p^{e_p}) = \varphi(n) = |\mathbb{Q}(\mu_n) : \mathbb{Q}| \ ,$$

de mivel $\mathbb{Q}(\mu_n) \leq M$, ezért $L \leq M = \mathbb{Q}(\mu_n)$. □

5.3. A lokál-globál elv

Megírandó. ***

A függelék

Végtelen Galois-bővítések

A.1. Algebrai lezárt létezése

A.1.1. Lemma. *Legyenek $f_1(x), \dots, f_n(x) \in K[x]$ nemkonstans polinomok. Ekkor van olyan $K \leq L$ véges bővítése K-nak, melyben mindegyik f_i $(i = 1, \dots, n)$ polinomnak van gyöke.*

Bizonyítás. Indukció n szerint. Ha $n = 1$, akkor vesszük f_1-nek egy g_1 irreducibilis osztóját, és az $L_1 := K[x]/(g_1(x))$ testet, melyben g_1-nek és így f_1-nek van gyöke. □

A következő bizonyítás megegyezik Pelikán József Algebra [11] jegyzetében található bizonyítással, de az olvasó kényelmének kedvéért megismételjük.

A.1.2. Tétel. *Minden K testnek izomorfia erejéig egyértelműen létezik algebrai lezártja, azaz olyan $K \leq \overline{K}$ test, mely algebrai bővítése K-nak és algebrailag zárt.*

Bizonyítás. Létezés: Legyen $S := \{f(x) \in K[x] \mid f \text{ nem konstans }\}$ a K feletti nemkonstans polinomok halmaza, és $R := K[x_f \mid f \in S]$ sokváltozós polinomgyűrű (minden $f \in S$ polinomra veszünk egy-egy x_f változót). Legyen továbbá $I := (f(x_f) \mid f \in S) \lhd R$ az $f(x_f)$ polinomok által generált ideál. Azt állítjuk, hogy $I \neq R$. Valóban, tegyük fel indirekten, hogy $1 \in I$, azaz van olyan $g_1, \dots, g_n \in R$ és $f_1, \dots, f_n \in S$, melyekre

$$1 = g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n}) \ . \tag{A.1}$$

A A.1.1-es Lemma szerint van olyan $K \leq L$ véges bővítés és $\alpha_1, \dots, \alpha_n \in L$ elemek, melyekre $f_i(\alpha_i) = 0$ $(i = 1, \dots, n)$. Az (A.1)-es egyenletbe x_{f_i} helyére α_i-t helyettesítve, a többi változó helyére pedig tetszőleges (pl. 0) számokat írva egy olyan $R \to L$ gyűrűhomomorfizmust kapunk, ami a bal oldalt 1-be, a jobb oldalt pedig 0-ba viszi. Ez ellentmondás, tehát $I \neq R$.

Így van I-t tartalmazó $M \lhd R$ maximális ideál R-ben Krull tétele szerint (itt kihasználjuk a Zorn lemmát). Ekkor $K_1 := R/M$ test. Vegyük észre, hogy K_1-et generálják az $x_f + M \in$ $\in K_1$ elemek K felett $(f \in S)$, hiszen R-et is generálják az x_f elemek. Viszont az $x_f + M$ elemek algebraiak K fölött, hiszen $f(x_f + M) = 0$. Tehát K_1 egy olyan algebrai bővítése K-nak, melyben minden K feletti nemkonstans polinomnak van gyöke. Vegyük észre, hogy az egyáltalán nem nyilvánvaló (lsd. A.1.4. Megjegyzés), hogy K_1 algebrailag zárt, hiszen elvileg előfordulhat, hogy egyes K_1-beli polinomoknak nincs gyökük K_1-ben, sőt, az is, hogy egy $f \in K[x]$ polinomnak csak egyetlen gyöke van K_1-ben, nem az összes. Viszont ezt megkerülhetjük úgy, hogy K helyett K_1-gyel elismételhetjük a fenti konstrukciót, mellyel kapunk

egy $K \leq K_1 \leq K_2$ algebrai bővítést, melyben minden K_1 feletti polinomnak van gyöke. És így tovább, legyen $\overline{K} := \bigcup_{n=1}^{\infty} K_n$ felszálló unió. Ekkor a $\overline{K}$ testnek minden eleme algebrai K felett (hiszen algebrai bővítések egymásutánja is algebrai), továbbá $\overline{K}$ már algebrailag zárt: ha $g(x) \in \overline{K}[x]$ nemkonstans, akkor van olyan $n \geq 1$, melyre g minden együtthatója benne van K_n-ben, azaz g-nek van gyöke $K_{n+1} \subset \overline{K}$-ban.

Egyértelműség: Legyen F egy másik algebrai lezártja K-nak. A Zorn-lemma segítségével megadunk egy $\overline{K} \to F$ izomorfizmust. Legyen $\mathcal{H}$ az (L, φ) rendezett párok halmaza, ahol $K \leq L \leq \overline{K}$ egy közbülső test, $\varphi\colon L \to F$ pedig egy K-homomorfizmus. Értelmezzük $\mathcal{H}$-n a következő részbenrendezést: $(L_1, \varphi_1) \leq (L_2, \varphi_2)$ akkor és csak akkor, ha $L_1 \leq L_2$ résztest és φ_2 megszorítása L_1-re megegyezik φ_1-gyel. $\mathcal{H}$ egy nemüres halmaz, hiszen $K \leq F$, ezért $(K, \iota) \in \mathcal{H}$, ahol $\iota\colon K \to F$ a természetes tartalmazás. Továbbá $\mathcal{H}$ zárt a felszálló unióra, ezért alkalmazható a Zorn lemma: legyen (L_0, φ_0) a $\mathcal{H}$ egy maximális eleme. Tegyük fel először, hogy $L_0 \neq \overline{K}$, azaz van egy $\alpha \in \overline{K}$, melyre $\alpha \notin L_0$. Legyen α minimálpolinomja L_0 felett $m_\alpha(x) \in$ $\in L_0[x]$. A 2.1.9-es Állítás szerint φ_0 kiterjesztései $L_0(\alpha)$-ra bijekcióban vannak $\varphi_0(m_\alpha(x))$ F-beli gyökeivel. Mivel F algebrailag zárt, ezért $\varphi_0(m_\alpha)$-nak van gyöke F-ben, tehát létezik egy $\psi\colon L_0(\alpha) \to F$ K-homomorfizmus kiterjesztése φ_0-nak, ami ellentmond (L_0, φ_0) maximalitásának. Tehát $L_0 = \overline{K}$ és $\varphi_0\colon \overline{K} \to L$ egy K-homomorfizmus, speciálisan injektív. A szürjektivitáshoz legyen $\beta \in F$ tetszőleges. Mivel F/K algebrai, ezért β-nak van egy $m_\beta(x) \in$ $\in K[x]$ minimálpolinomja K felett, melynek különböző gyökei F-ben $\beta_1 = \beta, \ldots, \beta_n$. Ekkor m_β-nak $\overline{K}$-ban is n különböző gyöke van: $\beta_1', \ldots, \beta_n'$ (valóban, a különböző gyökök száma leolvasható a polinomról többszörös deriválással). Node $\beta_1', \ldots, \beta_n'$ mind $\beta_1, \ldots, \beta_n$-be mehet csak a φ_0 testhomomorfizmusnál, speciálisan β is benne van φ_0 képében, azaz φ_0 izomorfizmus. □

A.1.3. Megjegyzés. Az algebrai lezárt fenti konstrukcióját másképp is végrehajthatjuk: Konstruálhatunk egy olyan algebrai bővítését K-nak, melyben minden K-beli együtthatós polinom gyöktényezők szorzatára bomlik. Ezt legkényelmesebben *transzfinit rekurzióval* tehetjük meg: jólrendezzük a $K[x]$ halmazt, azaz megindexeljük az elemeit egy α rendszámmal. Legyen $K_0 = K$, és az első lépésben legyen K_1 az első polinom felbontási teste K felett. Általában ha $\beta = \gamma + 1 \leq \alpha$ egy rákövetkező rendszám, akkor legyen K_β az $f_\beta(x) \in K[x]$ polinom felbontási teste K_γ fölött, ha pedig β limeszrendszám, akkor legyen $K_\beta := \bigcup_{\gamma<\beta} K_\gamma$ felszálló unió. Ekkor K_α lesz az algebrai lezárt: Egyrészt ennek minden eleme algebrai K fölött. Másrészt K_α algebrailag zárt, hiszen ha létezne egy nemtriviális véges F bővítése, akkor tetszőleges $\lambda \in F$ esetén λ algebrai lenne K fölött is, viszont a K feletti minimálpolinomja K_α-ban már gyöktényezők szorzatára bomlik, azaz $\lambda \in K_\alpha$.

A.1.4. Megjegyzés. Az A.1.2. Tétel bizonyításában valójában már K_1 is algebrailag zárt lesz, de ezt egy kicsit nehezebb meggondolni. Továbbá ennek bizonyításához felhasználjuk, hogy minden véges szeparábilis bővítés egyszerű, amihez viszont kellett az algebrai lezárt létezése (vagy, ha nem is kellett, de használtuk). Az előző megjegyzést használva azt kell ugyanis belátnunk, hogy ha $f(x) \in K[x]$ egy tetszőleges (irreducibilis) polinom, akkor létezik véges sok $f_1, \ldots, f_k \in K[x]$ irreducibilis polinom azzal a tulajdonsággal, hogy ha egy K-t tartalmazó L testben az $f_1, \ldots, f_k$ polinomok mindegyikének van gyöke, akkor $f(x)$ gyöktényezők szorzatára bomlik L-ben. Ha f szeparábilis, akkor f felbontási teste K fölött egyszerű bővítése K-nak, ezért találunk egyetlen ilyen polinomot. Ha viszont f nem szeparábilis, akkor $\mathrm{char}(K) = p$ prím és $f(x) = g(x^{p^r})$ valamilyen irreducibilis g polinomra és $r > 0$ egész számra. Ekkor van egy olyan $h(x) = a_0 + a_1 x + \cdots + a_n x^n$ polinom, melynek egyetlen gyökével való $K(\alpha) := K[x]/(h(x)), \alpha \leftrightarrow x + (h(x))$ bővítés izomorf a g polinom K_g felbontási

testével. Legyenek a $g(x)$ polinom gyökei $K_g \cong K(\alpha)$-ban $\beta_1, \dots, \beta_k$ ($k := \deg(g)$). Ekkor minden $1 \le j \le k$-ra $\beta_j = \sum_{i=0}^{n-1} a_{ij}\alpha^i$ alakba írható, ahol $a_{ij} \in K$ minden $0 \le i \le n-1$-re. Vegyük észre, hogy f-nek is pontosan k darab különböző gyöke van, melyek mindegyike az egyik β_j p^r-edik gyöke. Tekintsük tehát a $h(x^{p^r})$ és $x^{p^r} - a_{ij}$ polinomokat, ahol $0 \le i \le n-1$ és $1 \le j \le k$. Ha L egy olyan test, amelyben ezek mindegyikének van egy-egy gyöke, akkor γ-val jelölve $h(x^{p^r})$ egy gyökét L-ben, δ_{ij}-vel pedig az $x^{p^r} - a_{ij}$ polinom egy gyökét, akkor az $\alpha_j := \sum_{i=0}^{n-1} \delta_{ij}\gamma^i$ elemek ($j = 1, \dots, k$) az $f(x)$ polinom L-beli gyökei, és ezek páronként különbözők. Valóban, a γ^{p^r} elem gyöke a $h(x)$ polinomnak, és mivel ez irreducibilis K felett, ez is a minimálpolinom. Tehát a $K(\gamma^{p^r})$ test izomorf K_g-vel, és ezeket azonosíthatjuk úgy, hogy $\alpha = \gamma^{p^r}$. Viszont ezzel az azonosítással $\alpha_j^{p^r} = \sum_{i=0}^{n-1} \delta_{ij}^{p^r}\gamma^{p^r i} = \sum_{i=0}^{n-1} a_{ij}\alpha^i = \beta_j$, tehát ezek tényleg az f különböző gyökei.

A.1.5. Állítás. *Legyen K egy tökéletes test. Ekkor*

$$\overline{K} \cong \varinjlim_{K \le L \le \overline{K}, L/K \text{ véges}} L \cong \varinjlim_{K \le L \le \overline{K}, L/K \text{ véges Galois}} L \ ,$$

ahol az összekötőleképezések és a részbenrendezés a tartalmazás.

Bizonyítás. Ha L_1, L_2 két véges bővítése K-nak $\overline{K}$-ban, akkor L_1-nek és L_2-nek van közös felső korlátja (bővítünk mindkettő generátoraival), tehát a direkt limesznek van értelme. Másrészt, ha $\alpha \in \overline{K}$, akkor van olyan $K \le L_0 \le \overline{K}$ véges közbülső test, melyben α benne van, sőt, ha K tökéletes, akkor még Galois-bővítés is van ilyen. Tehát α-hoz hozzárendelhetjük $\alpha \in L_0$ osztályát a $\varinjlim L$ direkt limeszben, mely hozzárendelés egy K-homomorfizmus. Ez a K-homomorfizmus nyilvánvalóan bijektív. □

A.1.6. Definíció. Egy F/K végtelen algebrai bővítést Galois-bővítésnek nevezünk, ha szeparábilis és normális. A fenti bizonyítással analóg érvelés miatt ez azzal ekvivalens, hogy F véges Galois-bővítések direkt limesze.

A.1.7. Állítás. *Ha F/K Galois-bővítés, akkor*

$$\mathrm{Gal}(F/K) := \mathrm{Hom}_K(F,F) \cong \varprojlim_{K \le L \le F, L/K \text{ véges Galois}} \mathrm{Gal}(L/K) \ ,$$

ahol a jobb oldalon $K \le L_1 \le L_2$ véges Galois bővítések esetén a $\mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$ összekötő leképezések a megszorítás által indukált faktorleképezések.

Bizonyítás. Ha $\tau \in \mathrm{Hom}_K(F,F)$, akkor τ nyilván injektív, és a A.1.2-es Tétel bizonyításának végéhez hasonló gondolatmenet miatt szürjektív is, azaz invertálható. Tehát $\mathrm{Gal}(F/K)$ egy csoport. Továbbá ha $\tau \in \mathrm{Hom}_K(F,F)$, akkor τ-t megszoríthatjuk minden L véges Galois közbülső testre, így a $\tau \mapsto (\tau_L)_L$ egy $\mathrm{Gal}(F/K) \to \varprojlim \mathrm{Gal}(L/K)$ csoporthomomorfizmus lesz, hiszen $(\tau_{L_2})_{L_1} = \tau_{L_1}$. Az injektivitás világos, hiszen ha $\tau \neq \mathrm{id}$, akkor van olyan $\alpha \in F$, melyre $\tau(\alpha) \neq \alpha$, de α benne van egy véges bővítésben is. A szürjektivitás szintén világos, hiszen ha van τ_L-eknek egy kompatibilis rendszere, akkor ez megad egy $\tau\colon F \to F$ K-homomorfizmust a következőképpen: ha $\alpha \in F$, akkor van olyan L véges bővítés, mely tartalmazza α-t. Ekkor $\tau(\alpha) := \tau_L(\alpha)$ legyen, és ez nyilván nem függ L választásától, mivel $(\tau_L)_L$ kompatibilis volt. □

A.1.8. Definíció. A K tökéletes test abszolút Galois-csoportján a $\mathrm{Gal}(\overline{K}/K)$ csoportot értjük. Ezen értelmezhető az inverz limesz topológia (a $\mathrm{Gal}(L/K)$ véges csoportokon a diszkrét topológiát választva), melyre nézve egy kompakt csoport, hiszen véges (spec. kompakt) csoportok inverz limesze. Véges csoportok inverz limeszeit *provéges* csoportoknak nevezzük. Ha K nem tökéletes, akkor $\overline{K}$ nem Galois-bővítése K-nak. Ebben az esetben $\overline{K}$ helyett K maximális szeparábilis K^{sep} bővítését („szeparábilis lezárt") kell venni az abszolút Galois csoport definíciójában.

Híres megoldatlan probléma az inverz Galois-probléma, mely ebben a kontextusban azzal ekvivalens, hogy minden véges csoport előáll-e a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ csoport folytonos homomorf képeként, azaz $\mathbb{Q}$ véges bővítésének Galois-csoportjaként.

A.2. Tökéletes lezárt létezése

Ebben a fejezetben azt igazoljuk, hogy ha K egy p karakterisztikájú test, akkor létezik egy K-t tartalmazó legszűkebb K^{perf} test, ami tökéletes. Kicsit precízebben ezt a fogalmat is az univerzális tulajdonságával lehet megfogni: a $K \hookrightarrow K^{perf}$ bővítés a K tökéletes lezártja, ha tetszőleges F tökéletes testre és $K \hookrightarrow F$ testbeágyazásra létezik és egyértelmű egy olyan $K^{perf} \hookrightarrow F$ beágyazás, mely a

$$\begin{array}{ccc} K & \hookrightarrow & K^{perf} \\ & \searrow & \downarrow \\ & & F \end{array} \tag{A.2}$$

diagrammot kommutatívvá teszi. Az elképzelés K^{perf} megkonstruálására a következő: ha K nem tökéletes, akkor van olyan α eleme, ami nincs benne a Frob_p Frobenius endomorfizmus képében, azaz α-nak nincs K-ban p-edik gyöke. Ekkor adjungálnunk kell K-hoz $\sqrt[p]{\alpha}$-t. Továbbá ezt meg kell tennünk K többi elemével is, sőt, $K(\sqrt[p]{\alpha})$ elemivel is (pl. $\sqrt[p]{\alpha}$-val), és így tovább. Ezt elegánsan a következő módon tehetjük meg: Tekintsük a

$$\mathrm{Frob}_p \colon K^{(0)} \hookrightarrow K^{(1)}$$

injektív testhomomorfizmustmorfizmust, ahol $K^{(0)}$-t és $K^{(1)}$-et is azonosítjuk K-val. Speciálisan Frob_p egy izomorfizmus $K^{(0)}$ és $\mathrm{Frob}_p(K^{(0)}) \leq K^{(1)}$ között. Ha most $K^{(0)}$-at azonosítjuk ezen izomorfizmus mentén $\mathrm{Frob}_p(K^{(0)})$-lal, akkor tekinthetünk $K^{(1)}$-re úgy is, mint $K^{(0)}$ egy bővítésére, melyben minden $K^{(0)}$-beli elemnek van p-edik gyöke, hiszen a p-edik hatványra emelés képtere $K^{(1)}$-ben épp $K^{(0)}$. Ezt iterálva az n-edik lépésben $K^{(n)}$-et azonosítjuk $\mathrm{Frob}_p(K^{(n)})$-nel $K^{(n+1)}$-ben. Ekkor testeknek ez a sorozata a Frob_p-vel, mint összekötő leképezésekkel egy direkt rendszert alkot. Vegyük észre, hogy a $K^{(n)}$ test minden $n \geq 0$-ra izomorf K-val, de a direkt rendszerben az összekötő leképezések nem izomorfizmusok (hacsak K nem volt eleve tökéletes), hanem a p-Frobenius endomorfizmusok.

A.2.1. Tétel. *A fenti összekötő leképezésekkel a direkt limesz* $K^{perf} := \varinjlim_n K^{(n)} = \bigcup_n K^{(n)}$ *és a* $K \cong K^{(0)} \hookrightarrow K^{perf}$ *testbeágyazás teljesíti a tökéletes lezártat definiáló* (A.2) *univerzális tulajdonságot.*

Bizonyítás. Először belátjuk, hogy K^{perf} tökéletes. A direkt limeszben az összekötő leképezések injektívek, ezért $K^{(n)}$-et azonosíthatjuk a K^{perf}-beli képével, és K^{perf} =. Legyen

$\alpha \in K^{perf}$ tetszőleges. Ekkor α benne van $K^{(n)}$-ben valamilyen $n \geq 0$-ra. Ha $\alpha \in K^{(n)}$ a $K^{(n)} \cong K \cong K^{(n+1)}$ azonosításnál $\beta \in K^{(n+1)}$-nek felel meg, akkor $\beta^p = \mathrm{Frob}_p(\alpha)$ mint $K^{(n+1)}$-beli elemek, azaz α-nak van p-edik gyöke K^{perf}-ben.

Másrészt ha F egy tökéletes bővítése K-nak, akkor a $\mathrm{Frob}_p\colon F \to F$ leképezés bijektív, speciálisan van inverze. Így $\mathrm{Frob}_p^{-1}(K) \leq F$ egy K-t tartalmazó résztest F-ben (a $\mathrm{Frob}_p(K) \leq \leq K$ tartalmazásra alkalmazzuk a Frob_p^{-1} bijekciót). Továbbá $K^{(1)}$ konstrukciója miatt a $K \leq \leq K^{(1)}$ bővítés izomorf a $K \leq \mathrm{Frob}_p^{-1}(K)$ bővítéssel. Ezt iterálva az n-edik lépésben kapunk egy izomorfizmust a $K \leq K^{(n)}$ és a $K \leq \mathrm{Frob}_p^{-n}(K)$ bővítés között. Direkt limeszt véve kapunk egy izomorfizmust K^{perf} és $\bigcup_n \mathrm{Frob}_p^{-n}(K) \leq F$ között. A p-edik gyökvonás egyértelműsége miatt ez az izomorfizmus is egyértelmű. □

A.2.2. Megjegyzés. A tökéletes lezártat definiáló direkt limeszre a szakirodalomban a $\varinjlim_{\mathrm{Frob}_p} K$ jelölést használják.

Irodalomjegyzék

[1] Borevich, Z. I. és Shafarevich, I. R., *Number Theory*, Academic Press, New York, 1966.

[2] Coates, John és Sujatha, Ramdorai, *Cyclotomic fields and zeta values*, Springer, Heidelberg, 2006.

[3] Conrad, Keith, Fermat's Last Theorem for regular primes, internetes jegyzet.

[4] Conrad, Keith, Kummer's lemma, internetes jegyzet.

[5] Freud Róbert és Gyarmati Edit, *Számelmélet*, Nemzeti tankönyvkiadó, Budapest, 2000.

[6] Hartshorne, Robin, *Algebraic Geometry*, Springer, 1977.

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

[8] Milne, James, *Algebraic Number Theory*, internetes jegyzet.

[9] Milne, James, *Abelian Varieties*, internetes jegyzet.

[10] Neukirch, Jürgen, *Algebraische Zahlentheorie*, Springer, Heidelberg, 2007.

[11] Pelikán József, *Algebra jegyzet*, Testbővítések fejezet

[12] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Heidelberg, 1986.

[13] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer, Heidelberg, 1982.