Eötvös Loránd Tudományegyetem
Természettudományi Kar

Galois-elmélet a p-adikusok fölött

Seress Dániel

MSc Szakdolgozat

Témavezető:
Zábrádi Gergely, docens

Algebra és Számelmélet Tanszék

2021

Tartalomjegyzék

Bevezetés

Az 1. fejezetben szerepel a p-adikus számoknak két, az általam eredetileg tanulttól ($\mathbb{Q}$ teljessé tétele a p-adikus abszolútérték szerint) különböző konstrukciója. Az egyik a $(\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}$ sorozatból az inverz limesz képzése, a másik az $\mathbb{F}_p$-ből a Witt-vektorok képzése.

A 2. fejezetben a $p > 0$ karakterisztikájú testek p-adikus Galois-reprezentációinak előkészítéseként szerepelnek a B-reprezentációk, a reguláris G-gyűrűk és az E fölötti étale φ-modulusok.

A 3. fejezetben a Sen-elmélet bevezetéseként szerepel a Krasner-lemma és az Ax-Sen-lemma, majd a $H^1_{\mathrm{cont}}(G, GL_n(C))$ első (folytonos) kohomológiacsoport vizsgálata.

1. Előkészületek

1.1. Inverz limeszek és Galois-elmélet

1.1.1. Inverz limeszek

Ebben az alfejezetben mindig feltesszük, hogy $\mathcal{A}$ végtelen szorzatokkal ellátott Abel-féle kategória. Speciálisan $\mathcal{A}$ lehet a halmazok, a (topologikus) csoportok, (topologikus) gyűrűk, adott A gyűrű fölötti (topologikus) modulusok kategóriája.

1.1.1. Definíció. Az I részbenrendezett halmazt irányított halmaznak nevezzük, ha bármely két elemének van közös felső korlátja.

1.1.2. Definíció. Legyen I irányított halmaz. Legyen $(A_i)_{i\in I}$ $\mathcal{A}$-beli objektumok rendszere. Ezt a rendszert $\mathcal{A}$ egy inverz rendszerének (vagy projektív rendszerének) nevezzük az I indexhalmaz fölött, ha minden $i, j \in I$, $i \leq j$ párra létezik egy ${}_{ji} : A_j \to A_i$ morfizmus úgy, hogy minden $i \in I$-re $\varphi_{ii} = \mathrm{id}_{A_i}$, és minden $i, j, k \in I$, $i \leq j \leq k$-ra $\varphi_{ki} = \varphi_{ji}\varphi_{kj}$.

1.1.3. Definíció. Az $A_\cdot = (A_i)$ inverz rendszer inverz limesze (vagy projektív limesze) egy $\mathcal{A}$-beli objektumként van definiálva:

$$A = \varprojlim_{i\in I} A_i = \{(a_i) \in \prod_{i\in I} A_i : \forall i, j \in I, i \leq j : \varphi_{ji}(a_j) = a_i\}$$

úgy, hogy minden $i \in I$-re a $\varphi : A \to A_i, a = (a_j)_{j\in I} \mapsto a_i$ vetítés morfizmus.

Ha $i \leq j$, akkor $\varphi_i = \varphi_{ji} \circ \varphi_j$.

1.1.4. Állítás. Legyen (A_i) inverz rendszer $\mathcal{A}$-ban, A az inverz limesze. és B $\mathcal{A}$ egy objektuma. Ha minden $i \in I$-re létezik $f_i : B \to A_i$ morfizmus úgy, hogy minden $i \leq j$-re $f_i = \varphi_{ji} \circ f_j$, akkor egyértelműen létezik egy $f : B \to A$ morfizmus úgy, hogy minden $j \in I$-re $f_j = \varphi_j \circ f$.

Bizonyítás. Legyen $f : B \to \prod_{i\in I} A_i, b \mapsto f(b) := (f_i(b))_{i\in I}$ függvény. Tetszőleges $b \in B$ esetén minden $i \leq j$-re $\varphi_{ji}(f_j(b)) = (\varphi_{ji} \circ f_j)(b) = f_i(b)$, vagyis $f(b) \in A$ az inverz limesz definíciója szerint. Tehát $f : B \to A$ függvény.

Tetszőleges $j \in I$ esetén minden $b \in B$-re $(\varphi_j \circ f)(b) = \varphi_j(f(b)) = f_j(b)$. Tehát $\varphi_j \circ f = f_j$.

□

1.1.5. Példa. A pozitív egészek $\mathbb{N}^*$ halmazán tekintjük az oszthatóságot mint részbenrendezést: $n \leq m$, ha $n \mid m$. Legyen a $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathbb{N}^*}$ inverz rendszernél minden $m, n \in \mathbb{N}^*$, $n \mid m$-re a φ_{mn} morfizmus a gyűrűhomomorfizmus. Ekkor

$$\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}^*} \mathbb{Z}/n\mathbb{Z}$$

Legyen l prímszám. Ekkor az $\mathbb{N}^*$ indexhalmaz $\{l^n : n \in \mathbb{N}\}$ részhalmazára

$$\mathbb{Z}_l = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

az l-adikus egészek gyűrűje. A $\mathbb{Z}_l$ gyűrű teljes diszkrét értékelésgyűrű. Az egyetlen maximális ideálja (l), a maradékteste $\mathbb{F}_l$, és a hányadosteste a p-adikus számok teste:

$$\mathbb{Q}_l = \mathbb{Z}_l \left[\frac{1}{l}\right] = \bigcup_{m=0}^{\infty} l^{-m}\mathbb{Z}_l$$

1.1.2. Galois-elmélet

Legyen K test, és L (véges vagy végtelen) Galois-bővítése K-nak. A $\mathrm{Gal}(L/K)$ az L K-automorfizmusainak a csoportja, vagyis

$$\mathrm{Gal}(L/K) = \{g : L \to L, \forall \gamma \in K : g(\gamma) = \gamma\}$$

Jelölje $\mathcal{E}$ a K L-beli véges Galois-bővítéseinek a halmazát a tartalmazással mint részbenrendezéssel. Ekkor bármely $E, F \in \mathcal{E}$ esetén $EF \in \mathcal{E}$ és $E, F \subset EF$, tehát $\mathcal{E}$ irányított halmaz, és $L = \bigcup_{E\in\mathcal{E}} E$.

1.2. Witt-vektorok és teljes diszkrét értékelésgyűrűk

1.2.1. Nemarkhimédeszi testek és lokális testek

1.2.1. Definíció. Legyen A gyűrű. A $v : A \to \mathbb{R} \cup \{\infty\}$ függvény (nemtriviális) (nemarkhimédeszi) értékelés A-n, ha

1. $v(a) = \infty$ pontosan akkor, ha $a = 0$,
2. $v(ab) = v(a) + v(b)$
3. $v(a + b) \geq \min\{v(a), v(b)\}$,

és létezik $a \in A$, amelyre $v(a) \notin \{0, \infty\}$.

v diszkrét értékelés, ha $v(A)$ diszkrét részhalmaza $\mathbb{R}$-nek.

A 2. feltétel $a = 0$ esetén: $v(0) = v(0b) = v(0) + v(b)$, vagyis $v(b) = 0$ vagy $v(0) = \infty$ az 1. feltétel egyik fele.

Az 1. és a 2. feltétel együtt ekvivalensek azzal, hogy $v : (A, \cdot) \to (\mathbb{R}\cup\{\infty\}, +)$ homomorfizmus. Speciálisan $v(1) = 0$, minden $0 \neq a \in A$-ra $v(a^{-1}) = -v(a)$, és $a^n = 1$ esetén $v(a) = 0$. Speciálisan $v(-1) = 0$, és $v(-a) = v(a)$.

A 3. feltételből indukcióval $v(a_1 + ... + a_n) \geq \min\{v(a_1), ..., v(a_n)\}$.

A 3. feltételből $v(a - b) \geq \min\{v(a), v(-b)\} = \min\{v(a), v(b)\}$.

Ha A gyűrű és v értékelés A-n, akkor megad A-n egy topológiát: legyen $\{\{x : v(x) > n\} : n \in \mathbb{Z}\}$ környezetbázis a 0 körül. Ekkor A topologikus gyűrű. v megad A-n egy abszolútértéket: $|a| = e^{-v(a)}$.

$|a| = 0 \Leftrightarrow v(a) = \infty \Leftrightarrow a = 0$.

$|-a| = e^{-v(-a)} = e^{-v(a)} = |a|$.

$|\cdot|$ teljesíti a nemarkhimédeszi abszolútértékeket jellemző ultrametrikus egyenlőtlenséget:

$$|a + b| = e^{-v(a+b)} \leq e^{-\min\{v(a),v(b)\}} = e^{\max\{-v(a),-v(b)\}} =$$

$$= \max\{e^{-v(a)}, e^{-v(b)}\} = \max\{|a|, |b|\} \leq |a| + |b|$$

Ekkor $d(a,b) := |a-b| = e^{-v(a-b)}$ metrika.

Legyen $a \in A$ tetszőleges. Ekkor $\{x : v(x-a) > n\} = \{x : |x-a| < e^{-n}\} = B(a, e^{-n})$.

Ebben a topológiában tetszőleges $a \in A$-ra $\{\{x : v(x-a) > n\} : n \in \mathbb{Z}\}$ környezetbázis az a körül.

Ha A gyűrű és v értékelés A-n, akkor A tartomány (nullosztómentes): ha $ab = 0$ és $b \neq 0$, akkor $v(ab) = \infty$ és $v(b) \neq \infty$, tehát $v(a) = v(ab) - v(b) = \infty$, vagyis $a = 0$.

Legyen K az A hányadosteste. Ekkor a v értékelés kiterjeszthető K-ra: $v(a/b) = v(a) - v(b)$. Ekkor az értékelések gyűrűje (vagy az egészek gyűrűje) "a zárt egységgömb":

$$\mathcal{O}_K := \{a \in K : v(a) \geq 0\} = \{a \in K : |a| \leq 1\}$$

$\mathcal{O}_K$ egyetlen maximális ideálja "a nyílt egységgömb":

$$m_K := \{a \in K : v(a) > 0\} = \{a \in K : |a| < 1\}$$

Tehát $\mathcal{O}_K$ lokális gyűrű.

Ekkor a $k_K := \mathcal{O}_K / m_K$ test a K maradékteste.

1.2.2. Definíció. Egy K testet egy v értékeléssel értékeléstestnek nevezünk.

1.2.3. Definíció. Ha egy test egy értékelésre nézve teljes, akkor teljes nemarkhimédeszi testnek nevezzük.

1.2.4. Állítás. Ha F teljes nemarkhimédeszi test a v értékeléssel, és F' algebrai bővítése F-nek, akkor F'-n egyértelműen létezik az a v' értékelés, amelyre $v'|_F = v$. v' pontosan akkor teljes, ha F' véges bővítése F-nek. Ha $\alpha, \beta \in F'$ konjugáltak F fölött, akkor $v'(\alpha) = v'(\beta)$.

$$v'(a\alpha^k) = v'(a) + kv'(\alpha)$$

Most v'-t is v-vel jelöljük.

1.2.5. Definíció. Egy lokális test olyan teljes diszkrét értékeléstest, amelynek a maradékteste $p > 0$ karakterisztikájú tökéletes test. Tehát minden lokális test teljes nemarkhimédeszi test.

Egy p-adikus test egy 0 karakterisztikájú lokális test.

1.2.6. Állítás. A K lokális test pontosan akkor lokálisan kompakt (ekvivalensen: $\mathcal{O}_K$ kompakt), ha a k maradéktest véges.

Bizonyítás. $\mathcal{O}_K$ kompaktságával dolgozunk.

m_K nyílt gömb. $\mathcal{O}_K$-nak az m_K szerinti mellékosztályai $\mathcal{O}_J$ egy minimális nyílt fedését alkotják. Ha k végtelen, akkor ebből nem választható ki véges fedés, tehát $\mathcal{O}_K$ nem kompakt.

Tegyük fel, hogy k véges. $\mathcal{O}_K$ teljes. A metrikus tér korlátossága és a maradéktest végessége miatt $\mathcal{O}_K$-ban minden $\varepsilon > 0$-ra van véges ε-háló. Tehát $\mathcal{O}_K$ kompakt. □

1.2.7. Állítás. Legyen S a k egy reprezentánsrendszere $\mathcal{O}_K$-ban. Ekkor

minden $x \in \mathcal{O}_K$ elem egyértelműen felírható $x = \sum_{i \geq 0} s_i \pi^i$ alakban, ahol $s_i \in S$.

minden $x \in K$ elem egyértelműen felírható $x = \sum_{i \geq -n} s_i \pi^i$ alakban, ahol $n \in \mathbb{Z}$, és $s_i \in S$.

$p \in m_p$ és a binomiális tétel miatt

$$(a+b)^p \equiv a^p + b^p \mod m_K$$

n szerinti indukcióval

$$(a+b)^{p^n} \equiv (a^p + b^p)^{p^{n-1}} \equiv ... \equiv a^{p^n} + b^{p^n} \mod m_K$$

$$a \equiv b \mod m_K \Rightarrow a - b \in m_K \Rightarrow (a-b)^{p^n} \in m_K^n$$

1.2.8. Állítás. Az $\mathcal{O}_K \to k$ természetes homomorfizmushoz egyértelműen létezik egy természetes $r : k \to \mathcal{O}_K$ multiplikatív szekció.

Bizonyítás. Legyen $a \in k$. Ekkor minden n-re egyértelműen létezik $a_n \in k$, amelyre $a_n^{p^n} = a$ és $a_{n+1}^p = a_n$. Legyen $\widehat{a}_n$ az a_n egy felemelése $\mathcal{O}_K$-ban.

A.5 miatt $\widehat{a}_{n+1}^p \equiv \widehat{a}_n \mod m_K$-ből következik $\widehat{a}_{n+1}^{p^{n+1}} \equiv \widehat{a}_n^{p^n} \mod m_K^{n+1}$. Tehát $r(a) := \lim_{n\to\infty} \widehat{a}_n^{p^n}$ létezik. Ismét A.5 miatt $r(a)$ független az $\widehat{a}_n$ felemelések választásától. r egy szekciója ρ-nak, és multiplikatív. Továbbá, ha t egy másik szekció, akkor mindig választhatunk $\widehat{a}_n = t(a_n)$-t, és ekkor

$$r(a) = \lim_{n\to\infty} \widehat{a}_n^{p^n} = \lim_{n\to\infty} t(a_n)^{p^n} = t(a)$$

tehát az egyértelműség következik. □

Ezt az $r(a)$ elemet az a Teichmüller-reprezentánsának nevezzük, és $[a]$-val jelöljük.

Ha char $K = p$, akkor $r(a+b) = r(a) + r(b)$, mivel $(\widehat{a}_n + \widehat{b}_n)^{p^n} = \widehat{a}_n^{p^n} + \widehat{b}_n^{p^n}$. Tehát $r : k \to \mathcal{O}_K$ gyűrűhomomorfizmus, amellyel k-t azonosíthatjuk $\mathcal{O}_K$ egy résztestével.

1.2.9. Tétel. Ha K p karakterisztikájú lokális test, akkor

$$\mathcal{O}_K = k[[\pi]], K = k((\pi))$$

Ez a tétel pontosan akkor igaz K-ra, ha k ugyanolyan karakterisztikájú, mint K.

Ha K p-adikus test és char $K = 0$, akkor általában $r(a+b) \neq r(a) + r(b)$. Ennek a helyzetnek a leírására a Witt-vektorokat használjuk.

1.2.2. Witt-vektorok

Legyen p prímszám, A kommutatív gyűrű. Legyenek X_i, Y_i változók, ahol $i \in \mathbb{N}$, és

$$A[\underline{X}, \underline{Y}] = A[X_0, X_1, ..., X_n, ...; Y_0, Y_1, ..., Y_n, ...]$$

1.2.10. Lemma. Minden $\Phi \in \mathbb{Z}[X, Y]$-hoz egyértelműen létezik az a $\{\Phi_n\}_{n\in\mathbb{N}}$ sorozat $\mathbb{Z}[\underline{X}, \underline{Y}]$-ban, amelyre

$$\Phi(X_0^{p^n} + pX_1^{p^{n-1}} + ... + p^n X_n, Y_0^{p^n} + pY_1^{p^{n-1}} + ... + p^n Y_n) =$$

$$= (\Phi_0(\underline{X}, \underline{Y}))^{p^n} + p(\Phi_1(\underline{X}, \underline{Y}))^{p^{n-1}} + ... + p^n \Phi_n(\underline{X}, \underline{Y})$$

Továbbá

$$\Phi_n \in \mathbb{Z}[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n]$$

Bizonyítás. Először $\mathbb{Z}[\frac{1}{p}][X, Y]$-ban dolgozunk. Legyen $\Phi_0(\underline{X}, \underline{Y}) = \Phi(X_0, Y_0)$ és definiáljuk Φ_n-et rekurzívan, így:

$$\Phi_n(\underline{X}, \underline{Y}) = \frac{1}{p^n}\left(\Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) - \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}}\right)$$

Φ_n nyilván létezik, egyértelmű $\mathbb{Z}[\frac{1}{p}][X, Y]$-ban, és $\mathbb{Z}[\frac{1}{p}][X_0, ..., X_n; Y_0, ..., Y_n]$-nek is eleme. Csak azt kell bizonyítanunk, hogy Φ_n együtthatói egészek. Ezt n szerinti indukcióval csináljuk. $n = 0$-ra $\Phi_0(\underline{X}, \underline{Y}) = \Phi(X_0, Y_0)$, tehát egész együtthatós.

A rekurzió átalakítása:

$$p^n \Phi_n(\underline{X}, \underline{Y}) = \Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) - \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}}$$

$$\Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) = \sum_{i=0}^{n} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}}$$

Ezt úgy használjuk, hogy n helyett $n-1$-et és minden változó helyett a p-edik hatványát írjuk:

$$\Phi\left(\sum_{i=0}^{n-1} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n-1} p^i Y_i^{p^{n-i}}\right) = \Phi\left(\sum_{i=0}^{n-1} p^i (X_i^p)^{p^{(n-1)-i}}, \sum_{i=0}^{n-1} p^i (Y_i^p)^{p^{(n-1)-i}}\right) =$$

$$= \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}^p, \underline{Y}^p)^{p^{(n-1)-i}}$$

Feltéve, hogy minden $i \leq n-1$-re Φ_i egész együtthatós, annak bizonyításához, hogy Φ_n egész együtthatós, a következőt kell belátnunk:

$$\Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) \equiv \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}}$$

$\mathbb{F}_p$ Frobenius-endomorfizmusát használva $\Phi_i(\underline{X}^p, \underline{Y}^p) \equiv (\Phi_i(\underline{X}, \underline{Y}))^p \mod p$.
$p \mid x - y$ esetén $p^2 \mid x^p - y^p$, és indukcióval $p^n \mid x^{p^{n-1}} - y^{p^{n-1}}$. Ezért

$$\Phi_i(\underline{X}^p, \underline{Y}^p)^{p^{(n-1)-i}} \equiv \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}} \mod p^n$$

Tehát

$$\Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) \equiv \Phi\left(\sum_{i=0}^{n-1} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n-1} p^i Y_i^{p^{n-i}}\right) =$$

$$= \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}^p, \underline{Y}^p)^{p^{(n-1)-i}} \equiv \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}} \mod p^n$$

□

1.2.11. Megjegyzés. A $W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}$ az $(X_0, X_1, ...)$ sorozathoz tartozó Witt-polinomoknak nevezzük. Ekkor minden n-re $X_n \in \mathbb{Z}[p^{-1}][W_0, ..., W_n]$.

$n \geq 1$-re legyen $W_n(A) = A^n$ halmazként. A fenti lemmát használjuk:
Ha $\Phi = X + Y$, akkor legyen $S_i := \Phi_i \in \mathbb{Z}[X_0, ..., X_i; Y_0, ..., Y_i]$.
Ha $\Phi = XY$, akkor legyen $P_i := \Phi_i \in \mathbb{Z}[X_0, ..., X_i; Y_0, ..., Y_i]$.
Ha $a = (a_0, ..., a_{n-1}), b = (b_0, ..., b_{n-1}) \in W_n(A)$, akkor legyen

$$a + b := (s_0, ..., s_{n-1}),\ a \cdot b := (p_0, ..., p_{n-1})$$

ahol

$$s_i = S_i(a_0, ..., a_i; b_0, ..., b_i),\ p_i = P_i(a_0, ..., a_i; b_0, ..., b_i)$$

1.2.12. Megjegyzés. Ekkor

$$S_0 = X_0 + Y_0,\ P_0 = X_0 Y_0$$

$(X_0 + Y_0)^p + pS_1 = X_0^p + pX_1 + Y_0^p + pY_1$-ből kapjuk:

$$S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} X_0^i Y_0^{p-i}$$

$(X_0 Y_0)^p + pP_1 = (X_0^p + pX_1)(Y_0^p + pY_1)$-ből kapjuk:

$$P_1 = X_1 Y_0^p + X_0^p Y_1 + pX_1 Y_1$$

Általános n-re S_n-et és P_n-et túl bonyolult expliciten leírni.

Tekintsük a következő leképezést:

$$\rho : W_n(A) \to A^n, (a_0, ..., a_{n-1}) \mapsto (w_0, ..., w_{n-1})$$

ahol $w_i = W_i(a) = \sum_{j=0}^{i} p^j a_j^{p^{i-j}}$.
Ekkor $w_i(a + b) = w_i(a) + w_i(b)$ és $w_i(ab) = w_i(a) w_i(b)$.

1.2.13. Definíció. $W_n(A)$ az A fölötti n hosszú Witt-vektorok gyűrűje.
$W(A)$ az A fölötti (végtelen hosszú) Witt-vektorok gyűrűje.

1.2.14. Példa. $W(\mathbb{F}_p) = \mathbb{Z}_p$.

1.3. Folytonos kohomológia

1.3.1. Kommutatív kohomológia

1.3.1. Definíció. Legyen G csoport. Egy Abel-csoportot G-nek egy lineáris hatásával G-modulusnak nevezünk. Ha G topologikus csoport, akkor egy topologikus Abel-csoportot G-nek egy lineáris és folytonos hatásával topologikus G-modulusnak nevezünk.

Legyen $\mathbb{Z}[G]$ a G csoport $\mathbb{Z}$ fölötti csoportgyűrűje, vagyis

$$\mathbb{Z}[G] = \left\{ \sum_{i=1}^{n} a_i g_i : n \in \mathbb{N}, a_i \in \mathbb{Z}, g_i \in G \right\}$$

Egy G-modulus tekinthető bal $\mathbb{Z}[G]$-modulusnak a következőképpen: tetszőleges $a_i \in \mathbb{Z}, g_i \in G, x \in X$ esetén

$$\left(\sum_{i=1}^{n} a_i g_i \right)(x) = \sum_{i=1}^{n} a_i g_i(x)$$

A G-modulusok Abel-féle kategóriát alkotnak.

Legyen M topologikus G-modulus és $n \in \mathbb{N}$. A folytonos n-koláncok $C^n_{\text{cont}}(G, M)$ Abel-csoportja $n > 0$-ra a $G^n \to M$ folytonos függvények csoportja, $n = 0$-ra pedig $C^0_{\text{cont}}(G, M) := M$. Legyen $d_n : C^n_{\text{cont}}(G, M) \to C^{n+1}_{\text{cont}}(G, M)$ a következő függvény ($a \in M$):

$$(d_0 a)(g) := g(a) - a$$

$$(d_1 f)(g_1, g_2) := g_1(f(g_2)) - f(g_1 g_2) + f(g_1)$$

$$(d_2 f)(g_1, g_2, g_3) := g_1(f(g_2, g_3)) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2)$$

$$(d_n f)(g_1, ..., g_{n+1}) := g_1(f(g_2, ..., g_{n+1})) +$$

$$+ \sum_{i=1}^{n} (-1)^i f(g_1, ..., g_{i-1}, g_i g_{i+1}, g_{i+2}, ..., g_{n+1}) + (-1)^{n+1} f(g_1, ..., g_n)$$

Ekkor $d_{n+1} d_n = 0$:

$$((d_1 d_0)a)(g_1, g_2) = g_1((d_0 a)(g_2)) - (d_0 a)(g_1 g_2) + (d_0 a)(g_1) =$$

$$= g_1(g_2(a) - a) - (g_1 g_2(a) - a) + (g_1(a) - a) =$$

$$= g_1 g_2(a) - g_1(a) - g_1 g_2(a) + a + g_1(a) - a = 0$$

$$(d_2 d_1 f)(g_1, g_2, g_3) =$$

$$= g_1((d_1 f)(g_2, g_3)) - (d_1 f)(g_1 g_2, g_3) + (d_1 f)(g_1, g_2 g_3) - (d_1 f)(g_1, g_2) =$$

$$= g_1(g_2(f(g_3)) - f(g_2 g_3) + f(g_2)) -$$

$$-(g_1 g_2(f(g_3)) - f(g_1 g_2 g_3) + f(g_1 g_2)) + (g_1(f(g_2 g_3)) - f(g_1 g_2 g_3) + f(g_1)) -$$

$$-(g_1(f(g_2)) - f(g_1 g_2) + f(g_1)) =$$

$$= g_1g_2(f(g_3)) - g_1f(g_2g_3) + g_1f(g_2) -$$
$$-g_1g_2(f(g_3)) + f(g_1g_2g_3) - f(g_1g_2)) + g_1(f(g_2g_3)) - f(g_1g_2g_3) + f(g_1)) -$$
$$-g_1(f(g_2)) + f(g_1g_2) - f(g_1)) = 0$$
$$-g_1(f(g_2)) + f(g_1g_2) - f(g_1)) =$$
$$(d_{n+1}d_nf)(g_1, ..., g_{n+2}) =$$
$$g_1((d_nf)(g_2, ..., g_{n+2})) +$$
$$+\sum_{i=1}^{n+1}(-1)^i(d_nf)(g_1, ..., g_{i-1}, g_ig_{i+1}, g_{i+2}, ..., g_{n+2}) +$$
$$+(-1)^{n+2}(d_nf)(g_1, ..., g_{n+1}) =$$

Az n-edik rekurzív alak $n+2$ tagú, és mindegyik tagban egyszer szerepel az f függvény. Az $n+1$-edik $n+3$ tagú, és mindegyik tagba behelyettesítjük az n-edik rekurzív alak $n+2$ tagját. Így egy $(n+2)(n+3)$ tagú összeget kapunk.

$$=$$

tehát a $C^{\cdot}_{\text{cont}}(G, M)$ sorozat:

$$C^0_{\text{cont}}(G, M) \xrightarrow{d_0} C^1_{\text{cont}}(G, M) \xrightarrow{d_1} ... \xrightarrow{d_{n-1}} C^n_{\text{cont}}(G, M) \xrightarrow{d_n} ...$$

féligegzakt.

1.3.2. Definíció. Legyenek
$Z^n_{\text{cont}}(G, M) =$
$textKerd_n$
$B^n_{\text{cont}}(G, M) = \text{Im}d_n$
$H^n_{\text{cont}}(G, M) = Z^n/B^n = H^n(C^{\cdot}(G, M))$.
Ezeket rendre az M folytonos n-kociklusai csoportjának, a folytonos n-kohatárai csoportjának és az n-edik folytonos kohomológiacsoportjának nevezzük.

1.3.3. Állítás.

$$H^n_{\text{cont}}(G, M) = Z^0 = M^G = \{a \in M | \forall g \in G : g(a) = a\}$$

$$H^1_{\text{cont}}(G, M) = \frac{Z^1}{B^1} = \frac{\{f : G \to M | f \ folytonos, f(g_1g_2) = g_1f(g_2) + f(g_1)\}}{\{\sigma_a = (g \mapsto g \cdot a - a) : a \in M\}}$$

1.3.4. Következmény. Ha G triviálisan hat M-en, akkor $H^0_{\text{cont}}(G, M) = M$ és $H^1_{\text{cont}}(G, M) = \text{Hom}(G, M)$.

1.3.5. Állítás. Ha

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

topologikus G-modulusok egy rövid egzakt sorozata, akkor létezik egy

$$0 \longrightarrow M'^G \longrightarrow M^G \longrightarrow M''^G \xrightarrow{\delta} H^1_{\text{cont}}(G, M') \longrightarrow H^1_{\text{cont}}(G, M) \longrightarrow H^1_{\text{cont}}(G, M'')$$

egzakt sorozat, ahol minden $a \in M''^G$-ra $\delta(a)$ a következőképpen van definiálva: legyen $x \in M$ olyan, hogy $\beta(x) = a$, ekkor legyen $\delta(a)$ a $g \mapsto \alpha^{-1}(g(x) - x)$ folytonos 1-kociklus.

Bizonyítás. Minden $g \in G$-re $\beta(g(x) - x) = \beta(g(x)) - \beta(x) = g(\beta(x)) - \beta(x) = g(a) - a = 0$. Tehát $g(x) - x \in \text{Im } \alpha$, ezért $\alpha^{-1}(g(x) - x)$ értelmes. □

Két speciális eset:

1. Ha G egy csoport a diszkrét topológiával, $H^n(G, M) = H^n_{\text{cont}}(G, M)$ és adott egy hosszú egzakt sorozat.

2. Ha G provéges csoport és M a diszkrét topológiával van ellátva, akkor is adott egy hosszú egzakt sorozat. Ekkor az, hogy G folytonosan hat, azt jelenti, hogy minden $a \in M$-re a $G_a = \{g \in G | g(a) = a\}$ csoport nyílt G-ben. Ebben az esetben M-et diszkrét G-modulusnak nevezzük.

1.3.2. Nemkommutatív kohomológia

Legyen G topologikus csoport. Legyen M topologikus csoport, amely lehet nemkommutatív, multiplikatívan írva. Tegyük fel, hogy M topologikus G-csoport, vagyis M el van látva G-nek egy folytonos hatásával, amelyre $g(xy) = g(x)g(y)$ minden $g \in G$ és $x, y \in M$-re.

$$H^0_{\text{cont}}(G, M) = M^G = \{x \in M | g(x) = x \forall g \in G\}$$

és

$$Z^1_{\text{cont}}(G, M) = \{f : G \to M | f \ folytonos, f(g_1 g_2) = g_1 f(g_2) + f(g_1)\}$$

Ha $f, f' \in Z^n_{\text{cont}}(G, M')$, akkor azt mondjuk, hogy f és f' kohomológok, ha létezik olyan $a \in M$, hogy $f'(g) = a^{-1} f(g) g(a)$ minden $g \in G$-re. Ez egy ekvivalenciarelációt definiál a kociklusok halmazán, és $H^1_{\text{cont}}(G, M)$ az ekvivalenciaosztályok halmaza. $H^1_{\text{cont}}(G, M)$ egy pontozott halmaz, amelyben a kitüntetett pont az $f(g) \equiv 1$ triviális osztály minden $g \in G$-re.

2. $p > 0$ karakterisztikájú testek p-adikus Galois-reprezentációi

2.1. B-reprezentációk és reguláris G-gyűrűk

2.1.1. B-reprezentációk

Legyen G topologikus csoport, és B topologikus kommutatív gyűrű G egy olyan folytonos hatásával ellátva, amely kompatibilis a gyűrű struktúrájával, vagyis minden $g \in G$ és $b, b \in B$ esetén

$$g(b_1 + b_2) = g(b_1) + g(b_2),\ g(b_1 b_2) = g(b_1)g(b_2)$$

2.1.1. Példa. $B = L$ Galois-bővítése a K testnek, $G = \mathrm{Gal}(L/K)$, mindkettő a diszkrét topológiával.

2.1.2. Definíció. Az X a G B-reprezentációja, ha véges típusú B-modulus ellátva G egy szemilineáris és folytonos hatásával, ahol a szemilinearitás azt jelenti, hogy minden $g \in G$, $\lambda \in B$ és $x, x_1, x_2 \in X$ esetén

$$g(x_1 + x_2) = g(x_1) + g(x_2),\ g(\lambda x) = g(\lambda)g(x)$$

Ha G triviálisan hat B-n, akkor ez egy lineáris reprezentáció. Ha $B = \mathbb{F}_p$ a diszkrét topológiával, akkor mod p reprezentációnak nevezzük. Ha $B = \mathbb{Q}_p$ a p-adikus topológiával, akkor p-adikus reprezentációnak nevezzük.

2.1.3. Definíció. G egy B-reprezentációja szabad, ha a B-modulus szabad.

2.1.4. Definíció. Egy szabad B-reprezentáció triviális, ha a következők valamelyikre teljesül:
1. X-nek létezik X^G elemeiből álló bázisa.
$X \simeq B^d$ a G természetes hatásával.

Most megadjuk a G d rangú szabad B-reprezentációinak klasszifikációját, ha $d \in \mathbb{N}$ és $d \geq 1$.

Tegyük fel, hogy X szabad B-reprezentációja G-nek, és $\{e_1, ..., e_d\}$ egy bázisa. Minden $g \in G$-re legyen

$$g(e_j) = \sum_{i=1}^{d} a_{ij}(g)e_i$$

Ekkor kapunk egy $\alpha : G \to GL_d(B)$ leképezést.

$$\alpha(g) = (a_{ij}(g))_{1 \leq i,j \leq d}$$

Ekkor α egy 1-kociklus $Z^1_{\mathrm{cont}}(G, GL_d(B))$-ben. Továbbá, ha $\{e'_1, ..., e'_d\}$ egy másik bázis, és P a bázisok közötti átmenetmátrix, akkor

$$g(e'_j) = \sum_{i=1}^{d} a'_{ij}(g)e'_i,\ \alpha'(g) = (a'_{ij}(g))_{1 \leq i,j \leq d}$$

Ekkor $\alpha'(g) = P^{-1}\alpha(g)g(P)$.

Tehát α és α' kohomológok. Tehát az α osztálya $H^1_{\text{cont}}(G, GL_d(B))$-ben független az X bázisának választásától, és ezt $[X]$-szel jelöljük.

Megfordítva, ha $\alpha \in Z^1_{\text{cont}}(G, GL_d(B))$ 1-kociklus, akkor $X = B^d$-n egyértelműen létezik G egy szemilineáris hatása úgy, hogy minden $g \in G$-re

$$g(e_j) = \sum_{i=1}^{d} a_{ij}(g)e_i$$

és $[X]$ az α osztálya.

2.1.5. Állítás. Legyen $d \in \mathbb{N}$. Az $X \to [X]$ hozzárendelés bijekciót definiál a G d rangú szabad B-reprezentációinak ekvivalenciaosztályai és $H^1_{\text{cont}}(G, GL_d(B))$ között. Továbbá X pontosan akkor triviális, ha $[X]$ a kitüntetett pont $H^1_{\text{cont}}(G, GL_d(B))$-ben.

2.1.2. Reguláris G-gyűrűk

Ebben az alfejezetben legyen B topologikus gyűrű, és G topologikus csoport, amely folytonosan hat B-n. Legyen $E = B^G$, és tegyük fel, hogy ez test. Legyen F zárt részteste E-nek.

Ha B tartomány, akkor a G hatása kiterjed $C = \operatorname{Frac} B$-re: legyen minden $g \in G$ és $b_1, b_2 \in B$ esetén

$$g\left(\frac{b_1}{b_2}\right) = \frac{g(b_1)}{g(b_2)}$$

2.1.6. Definíció. Azt mondjuk, hogy B (F, G)-reguláris, ha a következők teljesülnek:

1. B tartomány.
2. $B^G = C^G$.
3. Ha $0 \neq b \in B$ esetén minden $g \in G$-re létezik olyan $\lambda \in F$, hogy $g(b) = \lambda b$, akkor b invertálható B-ben.

Speciálisan ha B test, akkor (F, G)-reguláris.

2.2. $p > 0$ karakterisztikájú testek mod p Galois-reprezentációi

2.2.1. Étale φ-modulusok E fölött

2.2.1. Definíció. Egy E fölötti φ-modulus egy M E-vektortér egy $\varphi : M \to M$ leképezéssel, amely szemilineáris az abszolút Frobeniusra nézve, vagyis

$$\forall x, y \in M : \varphi(x + y) = \varphi(x) + \varphi(y)$$

$$\forall \lambda \in E, x \in M : \varphi(\lambda x) = \varphi(\lambda)\varphi(x) = \lambda^p \varphi(x)$$

Ha M E-vektortér, akkor legyen $M_\varphi = E||_\varphi \otimes_E M$, ahol E-t E-modulusnak tekintjük a $\varphi : E \to E$ Frobeniussal. Ez azt jelenti, hogy $\lambda, \mu \in E$ és $x \in M$ esetén

$$\lambda(\mu \otimes x) = \lambda\mu \otimes x$$

$$\lambda \otimes \mu x = \mu^p \lambda \otimes x$$

M_φ E-vektortér, és ha $\{e_1, ..., e_d\}$ E fölötti bázisa M-nek, akkor $1 \otimes e_1, ..., 1 \otimes e_d$ E fölötti bázisa M_φ-nek. Tehát $\dim_E M_\varphi = \dim_E M$.

2.2.2. Megjegyzés. Ha M E-vektortér, akkor egy $\varphi : M_\varphi \to M$ szemilineáris leképezés megadása ekvivalens egy

$$\Phi : M_\varphi \to M$$

$$\lambda \otimes x \mapsto \lambda\varphi(x)$$

lineáris leképezés megadásával.

2.2.3. Definíció. Egy M E fölötti φ-modulus étale, ha $\Phi : M_\varphi \to M$ izomorfizmus, és $\dim_E M$ véges.

Legyen $\{e_1, ..., e_d\}$ E fölötti bázisa M-nek, és tegyük fel, hogy

$$\varphi e_j = \sum_{i=1}^{d} a_{ij} e_i$$

Ekkor $\Phi(1 \otimes e_j) = \sum_{i=1}^{d} a_{ij} e_i$. Tehát
M étale $\Leftrightarrow$ Φ izomorfizmus $\Leftrightarrow$ Φ injektív $\Leftrightarrow$ Φ szürjektív $\Leftrightarrow$ $M = E \cdot \varphi(M)$ $\Leftrightarrow$ $A = (a_{ij})$ invertálható E-ben.
Legyen $\mathcal{M}_\varphi^{ét}(E)$ az étale φ-modulusok kategóriája, ahol a morfizmusok az E lineáris leképezések, amelyek felcserélhetők φ-vel.

2.2.4. Állítás. Az $\mathcal{M}_\varphi^{ét}(E)$ kategória Abel-féle.

Bizonyítás. Legyen $E[\varphi]$ az E és egy φ elem által a $\forall \lambda \in E : \varphi\lambda = \lambda^p\varphi$ relációval generált nemkommutatív (ha $E \neq \mathbb{F}_p$) gyűrű. Az E fölötti φ-modulusok kategóriája azonos a bal $E[\varphi]$-modulusok kategóriájával. Ez Abel-kategória. Az állítás bizonyításához elég azt ellenőrizni, hogy ha $\eta : M_1 \to M_2$ étale φ-modulusok közötti E-morfizmus, akkor az η M' magja és az M'' komagja az E fölötti φ-modulusok kategóriájában étale.

□

2.2.5. Definíció. G egy mod p reprezentációja egy V véges dimenziós $\mathbb{F}_p$-vektortér ellátva G-nek egy folytonos lineáris hatásával. Jelölje $\mathrm{Rep}_{\mathbb{F}_p}(G)$ a G mod p reprezentációinak a kategóriáját.

3. C-reprezentációk és Sen módszerei

3.1. A Krasner-lemma és az Ax-Sen-lemma

3.1.1. A Krasner-lemma

3.1.1. Lemma (Krasner-lemma)**.** Legyen F teljes nemarkhimédeszi test, és E zárt részteste F-nek. Legyen $\alpha, \beta \in F$, és α szeparábilis E fölött. Tegyük fel, hogy α minden E fölötti $\alpha' \neq \alpha$ konjugáltja esetén $|\beta - \alpha| < |\alpha' - \alpha|$. Ekkor $\alpha \in E(\beta)$.

Bizonyítás. Legyen $E' = E(\beta)$ és $\gamma = \beta - \alpha$. Ekkor $E'(\gamma) = E'(\alpha)$, és $E'(\gamma)/E'$ szeparábilis. Belátjuk, hogy $E'(\gamma) = E'$. Elég belátni, hogy γ-nak E' fölött nincs más konjugáltja, mint γ. Legyen $\gamma' = \beta - \alpha'$ a γ konjugáltja E' fölött. Ekkor $|\gamma'| = |\gamma|$ (miért?). Tehát $|\gamma' - \gamma| \leq |\gamma| = |\beta - \alpha|$ (miért?). Másrészt $|\gamma' - \gamma| = |\alpha - \alpha'| = |\alpha' - \alpha| > |\beta - \alpha|$. Ellentmondás. □

$\sqrt[4]{2}$ minimálpolinomja $\mathbb{Q}$ fölött: $x^4 - 2$. Gyökei: $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$.
$\sqrt[4]{2}$ minimálpolinomja $\mathbb{Q}(\sqrt{2})$ fölött: $x^2 - \sqrt{2}$. Gyökei: $\pm\sqrt[4]{2}$.
$\sqrt[4]{2}$ minimálpolinomja $\mathbb{Q}(\sqrt[4]{2})$ fölött: $x - \sqrt[4]{2}$. Gyökei: $\sqrt[4]{2}$.

Ha egy elem egy test fölött szeparábilis, akkor minden bővebb test fölött is szeparábilis.

3.1.2. Következmény. Legyen K teljes nemarkhimédeszi test, K^s egy szeparábilis lezártja K-nak, $\overline{K}$ egy K^s-t tartalmazó algebrai lezártja K-nak. Ekkor $\widehat{K^s} = \widehat{\overline{K}}$, és ez algebrailag zárt test.

Bizonyítás. Legyen $C = \widehat{K^s}$. A következőket kell bizonyítanunk:

1. Ha $\mathrm{char}K = p$, akkor $\forall a \in C : \exists \alpha : \alpha^p = a$.
2. C szeparábilisan zárt.

1. Legyen $0 \neq \pi \in m_K$. Legyen $v = v_\pi$, ekkor $v(\pi) = 1$. Ekkor

$$\mathcal{O}_{K^s} = \{a \in K^s | v(a) \geq 0\}, \mathcal{O}_C = \varprojlim \mathcal{O}_{K^s}/\pi^n \mathcal{O}_{K^s}$$

$C = \mathcal{O}_C[1/\pi]$. Tehát $\pi^{mp} a \in \mathcal{O}_C$, ha $m > 0$ elég nagy. Feltehetjük, hogy $a \in \mathcal{O}_C$. Legyen minden n-re $a_n \in \mathcal{O}_{K^s}$ olyan, hogy $a \equiv a_n \mod \pi^n$. Legyen

$$P_n(X) = X^p - \pi^n X - a_n \in K^s[X]$$

Ekkor $P_n'(X) = -\pi^n \neq 0$, és P_n szeparábilis. Legyen α_n K^s-beli gyöke P_n-nek, $\alpha_n \in \mathcal{O}_{K^s}$. Ekkor

$$\alpha_n^p = \pi^n \alpha_n + a_n$$

$$\alpha_{n+1}^p - \alpha_n^p = \pi^{n+1}\alpha_{n+1} - \pi^n \alpha_n + a_{n+1} - a_n$$

$a_{n+1} \equiv a_n \mod \pi^n$ miatt $v(\alpha_{n+1}^p - \alpha_n^p) \geq n$. $(\alpha_{n+1} - \alpha_n)^p = \alpha_{n+1}^p - \alpha_n^p$ miatt $v(\alpha_{n+1} - \alpha_n) \geq n/p$.

Ezért $(\alpha_n)_{n\in\mathbb{N}}$ konvergens $\mathcal{O}_C$-ben. Legyen $\alpha := \lim_{n\to+\infty} \alpha_n$.

$a_n \equiv a \mod \pi^n$ miatt $v(\alpha_n^p - a) = v(\pi^n \alpha_n + a_n - a) \geq n$.

$\alpha^p = \lim_{n\to+\infty} \alpha_n^p = a$.
2. Legyen

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_{d-1}X^{d-1} + X^d \in C[X]$$

tetszőleges szeparábilis polinom. Azt kell bizonyítanunk, hogy $P(X)$-nek van gyöke C-ben. Feltehetjük, hogy $a_i \in \mathcal{O}_C$. Legyen C' a P felbontási teste C fölött, $r = \max v(\alpha_i - \alpha_j)$, ahol α_i és α_j különböző C'-beli gyökei P-nek. Legyen

$$P_1(X) = b_0 + b_1X + b_2X^2 + ... + b_{d-1}X^{d-1} + X^d \in K^s[X]$$

ahol $b_i \in K^s$, és $v(b_i - a_i) > rd$. Az 1. rész miatt $\overline{K} \subset C$, tehát létezik $\beta \in C$, hogy $P_1(\beta) = 0$. Legyen $\alpha \in C'$ gyöke P-nek, amelyre $|\beta-\alpha'| \geq |\beta-\alpha|$ bármely $\alpha' \in C'$ és $P(\alpha') = 0$ esetén. $P(\beta) = P(\beta) - P_1(\beta)$, és $v(\beta) \geq 0$, $v(P(\beta)) > rd$. Másrészt

$$P(\beta) = \prod_{i=1}^{d}(\beta - \alpha_i)$$

$$v(P(\beta)) = \sum_{i=1}^{d} v(\beta - \alpha_i) > rd$$

$v(\beta - \alpha) > r$. A Krasner-lemma szerint $\alpha \in C(\beta) = C$. □

3.1.2. Az Ax-Sen-lemma

Legyen K nemarkhimédeszi test, és E algebrai bővítése K-nak. Ha α eleme E egy szeparábilis bővítésének, akkor legyen

$$\Delta_E(\alpha) := \min\{v(\alpha' - \alpha)\}$$

ahol α' az α konjugáltjai E fölött. Ekkor

$$\Delta_E(\alpha) = \infty \Leftrightarrow \alpha \in E$$

Az Ax-Sen-lemma azt jelenti, hogy ha α minden α' konjugáltja közel van α-hoz, akkor α közel van E egy eleméhez.

3.1.3. Állítás (Ax-Sen-lemma, 0 karakterisztikájú eset)**.** Legyen K, E mint fent, és char $K = 0$. Ekkor létezik $a \in E$, amelyre

$$v(\alpha - a) > \Delta_E(\alpha) - \frac{p}{(p-1)^2}v(p)$$

3.1.4. Lemma. Legyen $R \in E[X]$ olyan $2 \leq d$-edfokú normált polinom, amelyre $\lambda \in \overline{E}, R(\lambda) = 0$ esetén $v(\lambda) \geq r$. Legyen $m \in \mathbb{N}$, $0 < m < d$. Ekkor létezik $\mu \in F$, amelyre μ gyöke $R^{(m)}$-nek, és

$$v(\mu) \geq r - \frac{1}{d-m}v\left(\binom{d}{m}\right)$$

Bizonyítás. Legyen

$$R = (X - \lambda_1)...(X - \lambda_d) = \sum_{i=0}^{d} b_i X^i$$

Ekkor $b_i \in \mathbb{Z}[\lambda_1, ..., \lambda_d]$ $d - i$-edfokú homogén polinom. Ezért $v(b_i) \geq (d - i)r$.

$$\frac{1}{m!} R^m(X) = \sum_{i=m}^{d} \binom{i}{m} b_i X^{i-m} = \binom{d}{m} (X - \mu_1)...(X - \mu_{d-m})$$

Ekkor

$$b_m = \binom{d}{m} (-1)^{d-m} \mu_1 ... \mu_{d-m}$$

Tehát

$$\sum_{i=1}^{d-m} v(\mu_i) = v(b_m) - v\left(\binom{d}{m}\right) \geq (d - m)r - v\left(\binom{d}{m}\right)$$

Tehát létezik i, amelyre

$$v(\mu_i) \geq r - \frac{1}{d-m} v\left(\binom{d}{m}\right)$$

□

Az Ax-Sen-lemma bizonyítása. Tetszőleges $d \geq 1$-re legyen $l(d)$ a legnagyobb olyan l egész, amelyre $p^l \leq d$. Legyen $\varepsilon(d) = \sum_{i=1}^{l(d)} \frac{1}{p^i - p^{i-1}}$. Ekkor $l(d) = 0$ pontosan akkor, ha $d < p$, ill. pontosan akkor, ha $\varepsilon(d) = 0$. Azt szeretnénk bizonyítani, hogy ha $[E(\alpha) : E] = d$, akkor létezik olyan $\alpha \in E$, amelyre

$$v(\alpha - a) > \Delta_E(\alpha) - \varepsilon(d) v(p)$$

Ebből következik az állítás, mert $\varepsilon(d) \leq \varepsilon(d + 1)$ és $\lim_{d \to +\infty} \varepsilon(d) = \frac{p}{(p-1)^2}$.

d szerinti indukció. $d = 1$ könnyű. Legyen $d \geq 2$. Legyen P az α E fölötti normált minimálpolinomja. Legyen

$$R(X) = P(X + \alpha), R^{(m)}(X) = P^{(m)}(X + \alpha)$$

Ha d nem p-hatvány, akkor $d = p^s n$, ahol $p \nmid n \geq 2$. Egyébként legyen $d = p^s p$, $s \in \mathbb{N}$. Legyen $m = p^s$.

Legyen μ olyan, mint a fenti lemmában. R gyökei $\alpha' \alpha$ alakaúak, ahol α' konjugáltja α-nak. Legyen $r = \Delta_E(\alpha)$, és $\beta = \mu + \alpha$. Ekkor

$$v(\beta - \alpha) \geq r - \frac{1}{d-m} v\left(\binom{d}{m}\right)$$

$P^{(m)}(\beta) = 0$, és $P^{(m)}(X) \in E[X]$ $d-m$-edfokú. Ezért β legfeljebb $d-m$-edfokú algebrai elem E fölött. Ha $\beta \in E$, akkor legyen $\alpha = \beta$; ha $\beta \notin E$, akkor legyen

$a \in E$ olyan, hogy $v(\beta - a) \geq \Delta_E(\beta) - \varepsilon(d-m)v(p)$, amelynek a létezése az indukcióból következik. Azt szeretnénk belátni, hogy $v(\alpha - a) > r - \varepsilon(d)$.

1. eset: $d = p^s n$, ahol $p \nmid n \geq 2$. Ekkor

$$v\left(\binom{d}{m}\right) = v\left(\binom{p^s n}{p^s}\right) = 0$$

Ezért $v(\mu) = v(\beta - \alpha) \geq r$. Ha $\beta' = \alpha' + \mu'$ konjugáltja β-nak, akkor

$$v(\beta' - \beta) = v(\alpha' - \alpha + \mu' - \mu) \geq r$$

Ezért $\Delta_E(\beta) \geq r$. Tehát $v(\beta - a) \geq r - \varepsilon(d - p^s)v(p)$, és

$$v(\alpha - a) \geq \min\{v(\alpha - \beta), v(\beta - a)\} \geq r - \varepsilon(d - p^s)v(p)$$

2. eset: $d = p^s p$. Ekkor

$$v\left(\binom{d}{m}\right) = v\left(\binom{p^{s+1}}{p^s}\right) = v(p)$$

Ezért $v(\mu) \geq r - \frac{1}{p^{s+1} - p^s} v(p)$. Ha $\beta' = \alpha' + \mu'$ konjugáltja β-nak, akkor

$$v(\beta' - \beta) = v(\alpha' - \alpha + \mu' - \mu) \geq r - \frac{1}{p^{s+1} - p^s} v(p)$$

Ezért $\Delta_E(\beta) \geq r - \frac{1}{p^{s+1} - p^s} v(p)$. Ekkor

$$v(\beta - a) \geq r - \frac{1}{p^{s+1} - p^s} v(p) - \varepsilon(p^{s+1} - p^s)v(p) = r - \varepsilon(p^{s+1})v(p)$$

Tehát $v(\alpha - a) \geq v(\alpha - \beta + \beta - a) \geq r - \varepsilon(d)v(p)$. □

3.1.5. Állítás (Ax-Sen-lemma, $p > 0$ karakterisztikájú eset)**.** Legyen K, E mint fent, és char $K = p > 0$, K perfekt. Ekkor minden $\varepsilon > 0$-ra létezik $a \in E$, amelyre

$$v(\alpha - a) > \Delta_E(\alpha) - \varepsilon$$

Bizonyítás. Legyen $L = E(\alpha)$, ekkor L/E szeparábilis. Tehát létezik $c \in L$, amelyre $\mathrm{Tr}_{L/E}(c) = 1$. Elég nagy $r > 0$-ra $v(c^{p^{-r}}) > -\varepsilon$. Legyen $c' = c^{p^{-r}}$, ekkor $(\mathrm{Tr}_{L/E}(c'))^{p^r} = \mathrm{Tr}_{L/E}(c) = 1$. c-t c'-vel helyettesítve, feltehetjük, hogy $v(c) > -\varepsilon$. Legyen S az $L \to \overline{E}$ E-beágyazások halmaza, és

$$a := \mathrm{Tr}_{L/E}(c\alpha) = \sum_{\sigma \in S} \sigma(c\alpha) = \sum_{\sigma \in S} \sigma(c)\sigma(\alpha) \in E$$

$\sum_{\sigma \in S} \sigma(c)\alpha = \mathrm{Tr}_{L/E}(c) = 1$ miatt

$$v(\alpha - a) = v\left(\sum_{\sigma \in S} \sigma(c)(\alpha - \sigma(\alpha))\right) \geq \min\{v(\sigma(c)(\alpha - \sigma(\alpha)))\} \geq \Delta_E(\alpha) - \varepsilon$$

□

3.2. A C-reprezentációk osztályozása

Legyen K p-adikus test, $G = G_K = \mathrm{Gal}(\overline{K}/K)$ és $C = \widehat{\overline{K}}$. Legyen $v = v_p$ a K-nak és bővítéseinek az az értékelése, amelyre $v(p) = 1$.

Rögzítjük K_∞-t, a K-nak egy $\overline{K}$-beli elágazó $\mathbb{Z}_p$-bővítését. Legyen $H = G_{K_\infty} = \mathrm{Gal}(\overline{K}/K_\infty)$. Legyen $\Gamma = \Gamma_0 = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Legyen $\Gamma_m = \Gamma^{p^m}$ és $K_m = K_\infty^{\Gamma_m}$ a K_∞-nek a Γ_m által fixált részteste. Legyen γ topologikus generátora Γ-nak, és legyen $\gamma_m = \gamma^{p^m}$, amely topologikus generátora Γ_m-nek.

Bármely $F \subset C$ résztestre legyen $\widehat{F}$ a C-beli lezártja. Ebben a fejezetben feltesszük, hogy a vizsgált testek el vannak látva a p-adikus topológiával.

3.2.1. $H^1_{\mathbf{cont}}(G, GL_n(C))$ vizsgálata

3.2.1. Lemma. Legyen $H_0 \leq H$ nyílt részcsoport, és $U : H_0 \to GL_n(C)$ olyan kociklus, hogy $v(U_\sigma - 1) \geq a$, $a > 0$ minden $\sigma \in H_0$-ra. Ekkor létezik olyan $M \in GL_n(C)$ mátrix, $v(M - 1) \geq a/2$, hogy minden $\sigma \in H_0$-ra

$$v(M^{-1}U_\sigma \sigma(M) - 1) \geq a + 1$$

Bizonyítás. A bizonyítás hasonló Hilbert 90. tételének a bizonyításához.

Legyen $H_1 \subset H_0$ olyan nyílt normálosztó, hogy $v(U_\sigma - 1) \geq a + 1 + a/2$ minden $\sigma \in H_1$-re. Ez a folytonosság miatt lehetséges. Az A.89. következmény miatt van olyan $\alpha \in C^{H_1}$, hogy

$$v(\alpha) \geq -a/2, \sum_{\tau \in H_0 \setminus H_1} \tau(\alpha) = 1$$

Legyen $S \subset H$ reprezentánsrendszere H_0/H_1-nek, és $M_S := \sum_{\sigma \in S} \sigma(\alpha) U_\sigma$. Ekkor $M_S - 1 = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - 1)$. Emiatt $v(M_S - 1) \geq a/2$, sőt

$$M_S^{-1} = \sum_{n=0}^{+\infty} (1 - M_S)^n$$

tehát $v(M_S^{-1}) \geq 0$ és $M_S \in GL_n(C)$.

Ha $\tau \in H_1$, akkor $U_{\sigma\tau} - U_\sigma = U_\sigma(\sigma(U_\tau) - 1)$. Legyen $S' \subset H_0$ egy másik repezrentánsrendszere H_0/H_1-nek. Tehát minden $\sigma' \in S'$-re létezik $\tau \in H_1$ és $\sigma \in S$, hogy $\sigma' = \sigma\tau$. Így kapjuk

$$M_S - M_{S'} = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - U_{\sigma\tau}) = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma (1 - \sigma(U_\tau))$$

$$v(M_S - M_{S'}) \geq a + 1 + a/2 - a/2 = a + 1$$

Bármely $\tau \in H_0$-ra

$$U_\tau \tau(M_S) = \sum_{\sigma \in S} \tau\sigma(\alpha) U_\tau \tau(U_\sigma) = M_{\tau S}$$

Ekkor $M_S^{-1} U_\tau \tau(M_S) \geq a + 1$. Legyen $M = M_S$ tetszőleges S-re, és ezzel megkapjuk az eredményt. □

3.2.2. Következmény. A fenti lemma feltételei mellett létezik olyan $M \in GL_n(C)$, hogy

$$v(M-1) \geq a/2, M^{-1}U_\sigma\sigma(M) = 1, \forall\sigma \in H_0$$

Bizonyítás. Ismételjük meg a lemmát ($a \mapsto a+1 \mapsto a+2 \mapsto ...$), és vegyük a határértékeket. □

3.2.3. Állítás. $H^1_{\text{cont}}(H, GL_n(C)) = 1$.

Bizonyítás. Azt kell megmutatnunk, hogy minden H-n vett $GL_n(C)$-beli értékű kocilus triviális. Legyen $a > 0$. A folytonosság miatt H-ban választhatunk egy H_0 nyílt normálosztót úgy, hogy $v(U_\sigma - 1) > a$ minden $\sigma \in H_0$-ra. A fenti következmény miatt U H_0-ra való megszorítása triviális. Az

infláció-megszorítás sorozat

H/H_0 végessége és Hilbert 90. tétele miatt $H^1_{\text{cont}}(H/H_0, GL_n(C^{H_0}))$ triviális. Következésképpen U is triviális. □

3.2.4. Lemma. Legyen adott $\delta > 0$, $b \geq 2c + 2d + \delta$ és $r \geq 0$. Tegyük fel, hogy $U = 1 + U_1 + U_2$, ahol

$$U_1 \in M_n(K_r), v(U_1) \geq b - c - d$$

$$U_2 \in M_n(C), v(U_2) \geq b' \geq b$$

Ekkor létezik $M \in GL_n(C)$, $v(M-1) \geq b - c - d$ úgy, hogy

$$M^{-1}U\gamma_r(M) = 1 + V_1 + V_2$$

ahol

$$V_1 \in M_n(K_r), v(U_1) \geq b - c - d$$

$$V_2 \in M_n(C), v(U_2) \geq b' + \delta$$

Bizonyítás. $U_2 = R_r(U_2) + (1 - \gamma_r)V$ úgy, hogy

$$v(R_r(U_2)) \geq v(U_2) - c, v(V) \geq v(U_2) - c - d$$

Tehát

$$(1+V)^{-1}U\gamma_r(1+V) = (1 - V + V^2 - ...)(1 + U_1 + U_2)(1 + \gamma_r(V)) =$$

$$= 1 + U_1 + (\gamma_r - 1)V + U_2 + (\text{legalább 2 fokú tagok})$$

Legyen $V_1 = U_1 + R_r(U_2) \in M_n(K_r)$, és W a legalább másodfokú tagok összege. Tehát $v(W) \geq b + b' - 2c - 2d \geq b' + \delta$. Így vehetjük $M = 1 + V, V_2 = W$. □

3.2.5. Következmény. Tegyük fel, hogy a fenti lemma feltételei teljesülnek. Ekkor létezik $M \in GL(n, \widehat{K}_\infty)$, $v(M-1) \geq b - c - d$, hogy $M^{-1}U\gamma_r(M) \in GL_n(K_r)$.

Bizonyítás. Ismételjük meg a lemmát $b \mapsto b+\delta \mapsto b+2\delta \mapsto ...$ és vegyük a határértéket. □

3.2.6. Lemma. Tegyük fel, hogy $B \in GL_n(C)$. Ha létezik $V_1, V_2 \in GL_n(K_i)$, hogy valamilyen $r \geq i$-re

$$v(V_1-1) > d, v(V_2-1) > d, \gamma_r(B) = V_1 B V_2$$

akkor $B \in GL_n(K_i)$.

Bizonyítás. Legyen $C = B - R_i(B)$. Azt kell belátnunk, hogy $C = 0$. C együtthatói $X_i = (1-R_i)\widehat{K}_\infty$-beliek, és R_i K_i-lineáris és felcserélhető γ_r-rel. Tehát

$$\gamma_r(C) - C = V_1 C V_2 - C = ((V_1-1)+1)C((V_2-1)+1) - C =$$
$$= (V_1-1)C(V_2-1) + (V_1-1)C + C(V_2-1) =$$
$$= ((V_1-1)C(V_2-1)+(V_1-1)C)+((V_1-1)C(V_2-1)+C(V_2-1))-(V_1-1)C(V_2-1) =$$
$$= (V_1-1)CV_2 + V_1C(V_2-1) - (V_1-1)C(V_2-1)$$

Tehát $v(\gamma_r(C)-C) > v(C)+d$. Az A.97. állítás miatt ekkor $v(C) = \infty$, vagyis $C = 0$. □

3.2.7. Állítás. A $GL_n(K_\infty) \to GL_n(\widehat{K}_\infty)$ beágyazás indukál egy

$$i : H^1_{\text{cont}}(\Gamma, GL_n(K_\infty)) \to H^1_{\text{cont}}(\Gamma, GL_n(\widehat{K}_\infty))$$

bijekciót.

Továbbá $H^1_{\text{cont}}(\Gamma, GL_n(\widehat{K}_\infty))$ bármely $\sigma \to U_\sigma$ folytonos kociklusára, ha $v(U_\sigma - 1) > 2c+2d$ minden $\sigma \in \Gamma_r$-re, akkor létezik $M \in GL_n(K_\infty)$, $v(M-1) > c+d$, hogy

$$\sigma \to U'_\sigma = M^{-1} U_\sigma \sigma(M)$$

kielégíti $U'_\sigma \in GL_n(K_r)$-et.

Bizonyítás. Először az injektivitást bizonyítjuk. Legyenek U, U' Γ kociklusai $GL_n(K_\infty)$-ben, és tegyük fel, hogy kohomológgá válnak $GL_n(\widehat{K}_\infty)$-ben. Vagyis, van olyan $M \in GL_n(\widehat{K}_\infty)$, hogy $M^{-1}U_\sigma\sigma(M) = U'_\sigma$ minden $\sigma \in \Gamma$-ra. Speciálisan $\gamma_r(M) = U_{\gamma_r}^{-1} M U'_{\gamma_r}$. Válasszuk r-et elég nagynak ahhoz, hogy U_{γ_r} és U'_{γ_r} kielégítsék a fenti lemma feltételeit. Ekkor $M \in GL_n(K_r)$. Tehát U és U' kohomológok $GL_n(K_\infty)$-ben, és ezzel az injektivitást beláttuk.

Most a szürjektivitást bizonyítjuk. Legyen U Γ kociklusa $GL_n(\widehat{K}_\infty))$-ban, ekkor a folytonosság miatt létezik r, hogy minden $\sigma \in \Gamma_r$-re $v(U_\sigma - 1) > 2c+2d$. A fenti következmény szerint létezik $M \in GL_r(C)$, $v(M-1) > 2(c+d)$, hogy $U'_{\gamma_r} = M^{-1} U_{\gamma_r} \gamma_r(M)$. Továbbá a fenti lemma szerint ismét $M \in GL_n(K_\infty)$.

Legyen $U'_\sigma = M^{-1}U_\sigma\sigma(M)$ minden $\sigma \in \Gamma$. Minden ilyen σ-ra

$$U'_\sigma \sigma(U'_{\gamma_r}) = U'_{\sigma\gamma_r} = U'_{\gamma_r\sigma} = U'_{\gamma_r}\gamma_r(U'_\sigma)$$

Emiatt $\gamma_r(U'_\sigma) = U'^{-1}_{\gamma_r} U'_\sigma \sigma(U'_{\gamma_r})$. Használjuk a fenti lemmát $V_1 = U'^{-1}_{\gamma_r}, V_2 = \sigma(U'_{\gamma_r})$-vel. Ekkor $U_\sigma \in GL_n(K_r)$.

Az állítás utolsó része a szürjektivitás bizonyításából következik. □

Hivatkozások

[1] Jean-Marc Fountaine, Yi Ouyang, *Theory of p-adic Galois representations*, Springer