Eötvös Loránd Tudományegyetem
Természettudományi Kar

Nagy Donát
Matematika BSc
Matematikus szakirány

Szemilineáris leképezések lokális testek felett

Szakdolgozat

Témavezető: Zábrádi Gergely egyetemi adjunktus
Algebra és Számelmélet Tanszék

Budapest, 2014

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Zábrádi Gergelynek a témajavaslatot, a szakirodalom ajánlását és a dolgozat alapos átnézését.

Tartalomjegyzék

1. Bevezetés **5**

2. Szemilineáris leképezések **6**

2.1. Szemilineáris leképezések alaptulajdonságai 6

2.2. Klasszifikáció egy speciális esetben 8

3. Diszkrét értékelésgyűrűk **11**

3.1. Diszkrét értékelések tulajdonságai 11

3.2. Diszkrét értékelésgyűrűk bővítései 14

4. Konstrukciók diszkrét értékelésgyűrűkre **23**

4.1. Witt-vektorok 23

4.2. $W(k)$ egyértelműsége 36

4.3. Cohen-részgyűrűk 39

5. A Dieudonné–Manin tétel **44**

5.1. Izokristályok és rácsok 44

5.2. A Dieudonné–Manin tétel 55

Hivatkozások **58**

1. Bevezetés

A szakdolgozatom elsődleges célja a Dieudonné–Manin tétel egy bizonyításának a bemutatása. Ez a tétel az izokristályok (diszkrét értékeléssel ellátott test feletti végesdimenziós vektortér, amit egy bijektív szemilineáris leképezés önmagára képez) szerkezetét írja le (bizonyos feltételek teljesülése esetén). Ennek megfelelően két, alapvetően független témával foglalkozom: a szemilineáris leképezésekkel illetve a diszkrét értékelésekkel.

A dolgozatom elején definiálom a szemilineáris leképezéseket és belátok néhány rájuk vonatkozó tételt és lemmát, majd bevezetem a diszkrét értékelés fogalmát és a diszkrét értékeléssel ellátott gyűrűkkel illetve testekkel foglalkozom. Az ezutáni részben leírok néhány konstrukciót diszkrét értékeléssel ellátott gyűrűkre, amelyek ugyan közvetlenül nem szükségesek a Dieudonné–Manin tétel bizonyításához, de fontos példái olyan struktúráknak, amire a tétel alkalmazható. Végül a dolgozatomat a Dieudonné–Manin tétel bizonyításával zárom. A dolgozatomban a [4] jegyzet felépítését követem, az [1] könyvben szerepel egy tömörebb, más formalizmust használó bizonyítás; tétel eredeti bizonyítása a [3] cikkben található.

Diszkrét értékeléssel ellátott testre talán a legismertebb példa a p-adikus számok $\mathbb{Q}_p$ teste. Számos eredetileg $\mathbb{R}$ vagy $\mathbb{C}$ felett vizsgált témakörnek van a p-adikus számok feletti analógiája, és ezek vizsgálata során gyakran előkerülnek az izokristályok, például (a teljesség igényen nélkül) használják őket p-adikus differenciálegyenletek vizsgálatakor (az [1] könyveben szerepelnek ilyen alkalmazások), p-adikus kohomológiaelméletben (kristályos kohomológiák) és p-adikus Galois-reprezentációk elméletében. Természetesen ahol az izokristályok előkerülnek, ott fontos szerepe van az őket klasszifikáló Dieudonné–Manin tételnek is.

2. Szemilineáris leképezések

2.1. Szemilineáris leképezések alaptulajdonságai

Rögzítsünk egy K testet és egy $\sigma : K \to K$ testhomomorfizmus. Legyen V egy végesdimenziós K-vektortér.

2.1.1. Definíció. *Egy $f : V \to V$ leképezésről azt mondjuk, hogy szemilineáris (pontosabban σ-lineáris), ha*

$$\begin{aligned} f(v_1 + v_2) &= f(v_1) + f(v_2) \quad (\forall v_1, v_2 \in V) \\ f(av) &= \sigma(a) f(v) \quad (\forall a \in K, v \in V) \end{aligned}$$

Legyen $d := dim_K V$ és $v_1, v_2, \ldots, v_d$ egy rögzített bázis V-ben. A lineáris leképezésekhez hasonlóan egy f szemilineáris leképezéshez is rendelhetünk egy $A_f = (a_{ij}) \in M_d(K)$ mátrixot úgy, hogy

$$f(v_j) = a_{1j}v_1 + a_{2j}v_2 + \ldots + a_{dj}v_d$$

legyen.

2.1.2. Lemma. *Az $f \mapsto A_f$ leképezés bijekció a $V \to V$ szemilineáris leképezések halmaza és az $M_d(K)$ halmaz között.*

Bizonyítás. Az inverz létezéséhez az kell, hogy mindend $A = (a_{ij}) \in M_d(K)$ mátrixhoz megadjunk egy $f : V \to V$ leképezést, amire $A = A_f$ lesz. Legyen egy $v = c_1v_1 + c_2v_2 + \ldots + c_dv_d \in V$ vektorra $f(v) = \sum_{i=1}^{d} \left(\sum_{j=1}^{d} a_{ij}\sigma(c_j) \right) v_i$. Erre $\sigma(0) = 0$ és $\sigma(1) = 1$ miatt

$$f(v_k) = \sum_{i=1}^{d} (0 + \ldots + 0 + a_{ik}\sigma(1) + 0 + \ldots + 0)\, v_i = a_{1k}v_1 + a_{2k}v_2 + \ldots + a_{dk}v_d$$

ami éppen azt jelenti, hogy $A = A_f$. □

2.1.3. Megjegyzések. *i. Ha v koordinátái* $\begin{pmatrix} c_1 \\ \vdots \\ c_d \end{pmatrix}$, *$f(v)$ koordinátái* $A_f \cdot \begin{pmatrix} \sigma(c_1) \\ \vdots \\ \sigma(c_d) \end{pmatrix}$ *lesznek.*

ii. A σ-lineáris leképezések halmaza K-vektortér és az $f \mapsto A_f$ leképezés K-vektorterek izomorfizmusa.

iii. Két σ-lineáris leképezés kompozíciója σ^2-lineáris (általában nem σ-lineáris).

iv. Ha σ nem szürjektív, akkor egy σ-lineáris leképezés képe nem feltétlen altér.

Egy $A = (a_{ij}) \in M_d(K)$ mátrixhoz legyen $\sigma(A) = (\sigma(a_{ij})) \in M_d(K)$. Ekkor $\sigma(A+B) = \sigma(A) + \sigma(B)$, $\sigma(AB) = \sigma(A)\sigma(B)$ és az egységmátrixra $\sigma(I) = I$. Így a $\sigma : \mathrm{GL}_d(K) \to \mathrm{GL}_d(K), A \mapsto \sigma(A)$ megszorítás injektív csoporthomomorfizmus (ami bijektív, ha a σ testhomomorfizmus bijektív volt).

Legyen $v'_1, \ldots, v'_d$ egy másik bázis V-ben, amire nézve az f szemilineáris leképezésünknek A'_f a mátrixa. A $B = (b_{kl})$ áttérési mátrix álljon azokból az értékekből, amikre $v'_l = \sum_{k=1}^{d} b_{kl} v_k$. Némi számolással belátható, hogy $A'_f = B^{-1} A \sigma(B)$.

2.1.4. Definíció. $\mathrm{GL}_d(K)$ *definiáljunk egy ekvivalenciarelációt úgy, hogy $A \equiv A'$ pontosan akkor álljon fenn, ha van olyan $B \in \mathrm{GL}_d(K)$, hogy $A' = B^{-1} A \sigma(B)$. Ekkor A-t és A'-t σ-konjugáltaknak nevezzük, az ekvivalenciaosztályok a σ-konjugáltosztályok.*

2.1.5. Lemma. *i. A_f invertálható $\Leftrightarrow \mathrm{im}(f)$ generálja V-t mint K-vektorteret $\Rightarrow$ f injektív*

ii. σ bijektív $\Rightarrow$ (A_f invertálható $\Leftrightarrow$ f szürjektív $\Leftrightarrow$ f bijektív $\Leftrightarrow$ f injektív)

Bizonyítás. i. A_f rangja $d \Leftrightarrow f(v_1), f(v_2), \ldots, f(v_d)$ bázis V-ben $\Leftrightarrow \langle \mathrm{im}(f) \rangle = V$ miatt az ekvivalencia igaz.

Tegyük fel most, hogy $f(v_1), f(v_2), \ldots, f(v_d)$ bázis V-ben. Ekkor ha $v = c_1 v_1 + + \ldots + c_d v_d$-re $f(v) = 0$, akkor $\sigma(c_1) f(v_1) + \ldots + \sigma(c_d) f(v_d) = 0$, így minden i-re $\sigma(c_i) = 0$, $c_i = 0$. Ez azt jelenti, hogy f valóban injektív ($f(a) = f(b) \Rightarrow f(a - - b) = 0 \Rightarrow a - b = 0$ a szemilinearitást kihasználva).

ii. Ha σ bijektív, $\mathrm{im}(f)$ nyilván lineáris altér V-ben. Elegendő tehát az előzőek mellé azt belátnunk, hogy ha f injektív, akkor $f(v_1), \ldots f(v_d)$ K-lineárisan függetlenek. Tegyük fel, hogy $c_1 f(v_1) + \ldots c_d f(v_d) = 0$! Ekkor találhatunk olyan b_i-ket, hogy $\sigma(b_i) = c_i$ és ezekre $f(b_1 v_1 + \ldots + b_d v_d) = c_1 f(v_1) + \ldots c_d f(v_d) = = 0$, $b_1 v_1 + \ldots + b_d v_d = 0$, minden b_i nulla, így minden c_i is nulla, tehát készen vagyunk.

□

2.1.6. Definíció. *Az $f : V \to V$ szemilineáris leképezésre azt mondjuk, hogy étale, ha $V = \langle \mathrm{im}(f) \rangle$.*

2.2. Klasszifikáció egy speciális esetben

Legyen $p > 1$ egy rögzített prím, $q > 1$ egy rögzített p-hatvány és K egy p karakterisztikájú test, ami $\mathbb{F}_q$-t tartalmazza. Ekkor

$$\begin{aligned} \sigma : K &\to K \\ a &\mapsto a^q \end{aligned}$$

egy testhomomorfizmus (a Frobenius-leképezés). Ekkor

– A $K^{\sigma=\mathrm{id}} := \{a \in K | \sigma(a) = a\}$ résztest (az $X^q - X$ polinom gyökeinek a halmaza) izomorf $\mathbb{F}_q$-val, a továbbiakban azonosítjuk vele

– K algebrailag zárt $\Rightarrow \sigma$ bijektív

Legyen V egy $d < \infty$-dimenziós K-vektortér és $f : V \to V$ egy étale szemilineáris leképezés. Legyen

$$V_1 := \{v \in V | f(v) = v\}$$

Ekkor V_1 egy $\mathbb{F}_q$ (azaz $K^{\sigma=\mathrm{id}}$) feletti vektortér.

2.2.1. Tétel. *Ha K szeparábilisan zárt (azaz nincsen valódi szeparábilis bővítése), akkor*

i. $\dim_{\mathbb{F}_q} V_1 = \dim_K V$;

ii. A

$$\begin{aligned} K \otimes_{\mathbb{F}_q} V_1 &\xrightarrow{\cong} V \\ a \otimes v &\mapsto av \end{aligned}$$

K-lineáris leképezés bijektív.

Bizonyítás. Nyilván feltehetjük, hogy $V \neq \{0\}$.

Először belátjuk, hogy $V_1 \neq \{0\}$. Legyen $v_0 \in V_1 \setminus \{0\}$ tetszőleges és $v_i := f^i(v_0)$. Legyen $m \geq 1$ minimális úgy, hogy $v_0, v_1, \ldots, v_m$ lineárisan összefüggő K felett. Ekkor skalárszorzó erejéig egyértelműen léteznek $a_i \in K$ elemek úgy, hogy

$$a_0 v_0 + a_1 v_1 + \ldots + a_m v_m = 0$$

és $a_m \neq 0$. Vegyük észre, hogy $a_0 \neq 0$, hiszen m minimalitása és a 2.1.3 i. és 2.1.5 i. állítások szerint $v_1 = f(v_0), v_2 = f(v_1), \ldots, v_m = f(v_{m-1})$ lineárisan függetlenek.

Legyen $v := c_0 v_0 + \ldots + c_{m-1} v_{m-1}$, ahol $c_0, \ldots, c_{m-1} \in K$ tetszőleges. Ekkor

$$f(v) = c_0^q f(v_0) + \ldots + c_{m-1}^q f(v_{m-1}) = c_0^q v_1 + \ldots c_{m-1}^q v_m$$

így

$$v - f(v) = \sum_{i=0}^{m} (c_i - c_{i-1}^q) v_i, \text{ ahol } c_{-1} = c_m = 0$$

tehát

$$v = f(v) \equiv c_i - c_{i-1}^q = a_i y \text{ egy } y \in K\text{-ra.}$$

Az $a_0^{q^m} Y^{q^m} + a_1^{q^{m-1}} Y^{q^{m-1}} + \ldots + a_{m-1}^q Y^q + a_m Y$ polinom deriváltja $a_m \neq 0$, így a polinom szeparábilis. Mivel K szeparábilisan zárt, így ennek a polinomnak van egy $y \neq 0$ gyöke. Legyen

$$\begin{aligned} c_0 &:= a_0 y \\ c_1 &:= c_0^q + a_1 y = a_0^q y^q + a_1 y \\ &\vdots \\ c_{m-1} &:= a_0^{q^{m-1}} y^{q^{m-1}} + \ldots + a_{m-1} y \end{aligned}$$

ekkor $a_0 \neq 0$ miatt $c_0 \neq 0$ és így $v \neq 0$. A konstrukcióból leolvasható, hogy $v \in V_1$.

Belátjuk, hogy $\dim_{\mathbb{F}_q} V_1 \leq \dim_K V$. Tegyük fel indirekt, hogy $\dim_{\mathbb{F}_q} V_1 > \dim_K V$. Legyen $r \geq 2$ minimális úgy, hogy léteznek $u_1, \ldots u_r \in V$ vektorok, melyek $\mathbb{F}_q$ felett lineárisan függetlenek, de K felett lineárisan összefüggők. Tegyük fel, hogy

$$b_1 u_1 + \ldots + b_r u_r = 0 \quad \text{és} \quad b_1 \in K^\times$$

Feltehetjük, hogy $b_1 = 1$. Ekkor

$$0 = f(0) = u_1 + b_2^q u_2 + \ldots + b_r^q u_r$$

így

$$0 = (b_2 - b_2^q) u_2 + \ldots + (b_r - b_r^q) u_r$$

de így r minimalitása miatt $b_i - b_i^q$ $(2 \leq i \leq r)$, így $b_i \in \mathbb{F}_q$, de így ellentmondást kaptunk.

$d = \dim_K V$ szerinti indukcióval belátjuk, hogy V_1-nek létezik egy $v_1, \ldots, v_d$ $\mathbb{F}_q$-bázisa, mely egyben K-bázisa V-nek. A $d = 1$ esethez már beláttuk, hogy létezik egy $v_1 \in V_1$ nemnulla elem és hogy $\dim_{\mathbb{F}_q} V_1 \leq \dim_K V = d = 1$, így ebben az esetben igaz az állításunk.

Tegyük fel, hogy $d > 1$ és kisebb d értékekre már beláttuk az állításunkat. Legyen $v_1 \in V_1$ egy nemnulla elem. Ekkor

$$\begin{aligned} \tilde{f} : V/Kv_1 &\to V/Kv_1 \\ u + Kv_1 &\mapsto f(u) + Kv_1 \end{aligned}$$

egy jóldefiniált étale szemilineáris leképezés. Az indukciós feltevést $(V/Kv_1, \tilde{f})$-re alkalmazva kaphatunk $v_2', \ldots, v_d' \in V$ vektorokat, melyekre

– $v_1, v_2', \ldots v_d'$ K-bázisa V-nek

– $f(v_i') = v_i' + a_i v_1$ valamely $a_i \in K$-ra, ha $2 \leq i \leq d$

Legyen $c_i \in K$ gyöke az $Y^q - Y + a_i$ szeparábilis polinomnak és legyen $v_i := v_i' + + c_i v_1$, ha $2 \leq i \leq d$. Ekkor $v_1, v_2, \ldots, v_d$ K-bázisa V-nek és

$$f(v_i) = f(v_i') + c_i^q v_1 = v_i' + a_i v_1 + c_i^q v_1 = v_i + (c_i^q - c_i + a_i)v_1 = v_i$$

azaz $v_i \in V_1$. $\dim_{\mathbb{F}_q} V_1 \leq \dim_K V = d$ miatt az $v_1, \ldots v_d$ $\mathbb{F}_q$-független rendszer nyilván $\mathbb{F}_q$-bázis V_1-ben. □

Nyilvánvaló, hogy a

$$\begin{array}{ccc} K \otimes_{\mathbb{F}_q} V_1 & \xrightarrow{\cong} & V \\ \downarrow{\scriptstyle \sigma \otimes \mathrm{id}_{V_1}} & & \downarrow{\scriptstyle f} \\ K \otimes_{\mathbb{F}_q} V_1 & \xrightarrow{\cong} & V \end{array}$$

diagram kommutatív.

2.2.2. Következmény. *Ha K szeparábilisan zárt és f étale, akkor van egy olyan K-bázisa V-nek, melyben f-nek az A_f mátrixa az egységmátrix. (V_1-nek minden $\mathbb{F}_q$-bázisa ilyen lesz.)*

2.2.3. Következmény. *Ha K szeparábilisan zárt, akkor az egész $GL_d(K)$ egyetlen σ-konjugáltosztály.*

3. Diszkrét értékelésgyűrűk

3.1. Diszkrét értékelések tulajdonságai

3.1.1. Definíció. *Az A főideálgyűrűt diszkrét értékelésgyűrűnek nevezzük, ha pontosan egy $\mathfrak{m} \neq \{0\}$ maximális ideálja van. Az $A/\mathfrak{m}$ testet A maradéktestnek nevezzük.*

Legyen A egy diszkrét értékelésgyűrű. Mivel A alaptételes, könnyen láthatóan

1. $A^\times = A \setminus \mathfrak{m}$
2. $\mathfrak{m} = \pi A$ egy $\pi \in A$ prímelemre
3. $\{\pi^n A | n \geq 0\}$ a nemnulla A-beli ideálok halmaza
4. minden $0 \neq a \in A$ egyértelműen írható $a = \pi^{v(a)} u$ alakban, ahol $v(a) \geq 0$ egész és $u \in A^\times$.

Ez megad egy $v : A \setminus 0 \to \mathbb{N}$ leképezést. (Megjegyzés: A szakdolgozatomban $\mathbb{N}$ a nemnegatív egészek halmazát jelöli.) Erre a következők állnak fenn:

(I) v szürjektív és nem függ a π prímelem választásától

(II) $v(ab) = v(a) + v(b)$

(III) $v(a + b) \geq \min(v(a), v(b))$

3.1.2. Definíció. *v-t az A-n lévő diszkrét értékelésnek nevezzük.*

Legyen K az A gyűrű hányadosteste. A $v\left(\frac{a}{b}\right) := v(a) - v(b)$ definícióval v kiterjeszthető egy $K^\times \to \mathbb{Z}$ csoporthomomorfizmussá, amire (II) és (III) továbbra is teljesül (ez a diszkrét értékelés K-n). Néha szerencsés a $v(0) := \infty$ jelölést alkalmazni.

Vegyük észre, hogy $A = \{x \in K | v(x) \geq 0\}$ és $\mathfrak{m} = \{x \in K | v(x) > 0\}$.

3.1.3. Lemma. *Ha $x, y \in K$, $v(x) \neq v(y)$, akkor $v(x + y) = \min(v(x), v(y))$.*

Bizonyítás. Tegyük fel, hogy például $v(x) > v(y)$. Ekkor

$$v(x) > v(y) = v(x + y - x) \geq \min(v(x + y), v(-x)) = \min(v(x + y), v(x))$$

ahonnan $v(x) > v(x + y)$ adódik, majd ezt figyelembe véve $v(y) \geq v(x + y)$ is, de így

$$v(y) \geq v(x + y) \geq \min(v(x), v(y)) = v(y)$$

azaz $v(y) = v(x + y)$ valóban teljesül. □

3.1.4. Lemma. *Legyen L egy test és $v : L^\times \to \mathbb{Z}$ egy szürjektív függvény, amire (II) és (III) teljesül. Ekkor $B := \{x \in L | v(x) \geq 0\}$ egy diszkrét értékelésgyűrű, aminek L a hányadosteste.*

Bizonyítás. B nyilvánvalóan egy gyűrű és $B^\times = \{x \in L | v(x) \geq 0\}$. Rögzítsünk egy $\pi \in B$ elemet, amire $v(\pi) = 1$. Ekkor minden $x \in B$ egyértelműen előáll $x = \pi^{v(x)}u$ alakban, ahol $u \in B^\times$. Innen látható, hogy a B nemnulla ideáljai éppen a $\pi^n B$ halmazok, ahol n nemnegatív egész. □

3.1.5. Példa. *Ha p egy rögzített prímszám. $\mathbb{Q}$-n a következő p-adikus értékelés egy diszkrét értékelés lesz:*

$$\begin{aligned} v_p : \mathbb{Q}^\times &\to \mathbb{Z} \\ x &\mapsto n, \text{ ha } x = p^n \cdot \frac{a}{b}, \text{ ahol } p \nmid ab \end{aligned}$$

Az ehhez tartozó diszkrét értékelésgyűrű $\mathbb{Z}_{(p)} = \left\{\frac{a}{b} | a, b \in \mathbb{Z}, p \nmid b\right\}$, a maradéktest pedig $\mathbb{F}_p$.

Legyen a továbbiakban A egy diszkrét értékelésgyűrű, K a hányadosteste és v a diszkrét értékelés. $x \in K$-ra legyen

$$|x| := \begin{cases} e^{-v(x)} & \text{, ha } x \neq 0 \\ 0 & \text{, ha } x = 0 \end{cases}$$

Ekkor a következők teljesülnek:

(IV) $|x| \geq 0$

(V) $|x| = 0 \Leftrightarrow x = 0$

(VI) $|xy| = |x| \cdot |y|$

(VII) $|x + y| \leq \max(|x|, |y|)$ (ultrametrikus egyenlőtlenség)

Ez azt jelenti, hogy $|.|$ egy abszolútérték (amire a háromszögegyenlőtlenségnek a (VII)-ben szereplő erősebb alakja is teljesül). A $d(x, y) = |x - y|$ távolságfüggvény metrikus térré teszi K-t, így a továbbiakban beszélhetünk K-ban haladó Cauchy- és konvergens sorozatokról illetve a konvergens sorozatok határértékéről.

Ezeket a fogalmakat a diszkrét értékeléssel is jellemezni tudjuk:

- Az (x_n) sorozat pontosan akkor konvergál $x \in K$-hoz, ha minden $C > 0$-hoz van $N \in \mathbb{N}$, hogy $v(x_n - x) > C$ minden $n > N$-re.

- Az (x_n) sorozat pontosan akkor Cauchy-sorozat, ha minden $C > 0$-hoz van $N \in \mathbb{N}$, hogy $v(x_n - x_m) > C$ minden $n, m > N$-re.

Figyelembe véve a diszkrét értékelés (III) tulajdonságát, az utóbbi a következő alakban is felírható:

- Az (x_n) sorozat pontosan akkor Cauchy-sorozat, ha minden $C > 0$-hoz van $N \in \mathbb{N}$, hogy $v(x_n - x_{n+1}) > C$ minden $n > N$-re.

3.1.6. Definíció. *Azt mondjuk, hogy a diszkrét értékeléssel ellátott K test teljes, ha minden benne futó Cauchy-sorozat konvergens.*

3.1.7. Lemma. *Legyen $\pi \in A$ prímelem, $a \in K$ és $n \in \mathbb{Z}$. Ekkor az $a + \pi^n A$ halmaz nyíltzárt K-ban.*

Bizonyítás. Vegyük észre, hogy

$$a + \pi^n A = \{x \in K | v(a - x) \geq n\} = \{x \in K | d(a, x) \leq e^{-n}\}$$

tehát a-nak az e^{-n} sugrú környezete benne van $a + \pi^n A$-ban.

Legyen $b \in a + \pi^n A$ tetszőleges és $n' = \min(n, v(a - b))$, ekkor

$$b + \pi^{n'} A \subseteq b + \pi^{v(a-b)} A + \pi^n A \subseteq b + (a - b) + \pi^n A = a + \pi^n A$$

és így b benne van $a + \pi^n A$ belsejében, $a + \pi^n A$ nyílt.

Legyen $b \notin a + \pi^n A$, ekkor $v(b - a) \leq n - 1$, hiszen különben $b - a = \pi^n u$ lenne egy $u \in A$-ra, ami ellentmondás. Ekkor $(b + \pi^n A) \cap (a + \pi^n A) = \emptyset$, hiszen ha c a metszetükben lenne, akkor $v(c - a) \geq n$ és $v(b - c) \geq n$ miatt $v(b - c) \geq \min(v(c - - a), v(b - c)) \geq n$ lenne, ami ellentmondás. Ezzel beláttuk, hogy b egy környezete is $a + \pi^n A$-n kívülre esik, tehát $a + \pi^n A$ zárt is. □

3.1.8. Tétel. *Távolságtartó izomorfizmus erejéig egyértelműen létezik egy olyan teljes $(\hat{K}, \hat{v})$ diszkrét értékeléssel ellátott test, aminek K sűrű részteste és $\hat{v}|_{K^\times} = v$.*

Bizonyítás. Először az egyértelműséget igazoljuk. Ha $(\hat{K}_1, \hat{v}_1)$ és $(\hat{K}_2, \hat{v}_2)$ két ilyen test, megadunk egy $\varphi : \hat{K}_1 \to \hat{K}_2$ távolságtartó izomorfizmust. Legyen $x \in \hat{K}_1$ tetszőleges; mivel $K \subseteq \hat{K}_1$ sűrű, létezik $(x_n)_{n \in \mathbb{N}}$ K-ban haladó sorozat, aminek a határértéke ($\hat{v}_1$ szerint) x. Ez a sorozat $\hat{v}_1$ szerint Cauchy-sorozat, de így v szerint, sőt $\hat{v}_2$ szerint is az. Mivel $(\hat{K}_2, \hat{v}_2)$ teljes, így létezik pontosan egy $\varphi(x) \in \hat{K}_2$, amihez az (x_n) sorozat $\hat{v}_2$ szerint konvergál. Ez a hozzárendelés nem függ az (x_n) sorozat választásától (ha két sorozat más $\varphi(x)$-et adna, az összefésültjüket tekintve ellentmondást kapnánk). Könnyen átgondolható, hogy φ bijekció (hiszen egy $y \in \hat{K}_2$-höz is kereshetünk $\hat{K}_1$-beli párt). Az, hogy φ tartja a távolságot, az összeadást és a szorzást, következik onnan, hogy azok könnyen átgondolhatóan folytonos függvények.

A létezés igazolásához legyen $\mathcal{C}$ a K-beli Cauchy-sorozatok halmaza, ez a pontonkénti összeadással és szorzással egységelemes gyűrű. K elemeit azonosíthatjuk a $\mathcal{C}$-beli konstans sorozatokkal. Legyen $\mathcal{N}$ a $\mathcal{C}$-beli zérussorozatok halmaza, ez könnyen átgondolhatóan egy maximális ideál lesz. Legyen $\hat{K} := \mathcal{C}/\mathcal{N}$ és $\hat{v}((x_n)_n + \mathcal{N}) := = \lim_{n\to\infty} v(x_n)$.

3.1.9. Állítás. *Ez a $\hat{v}$ valóban jóldefiniált $\hat{K}^\times \to \mathbb{Z}$ függvény lesz.*

Bizonyítás. Ha $(x_n)_n \in \mathcal{C} \setminus \mathcal{N}$, akkor mivel nem nullsorozat, így $\exists C > 0 : \forall N : : \exists \nu(N) > N : v(x_{\nu(N)} - 0) \leq C$ és ehhez a C-hez van N', hogy $\forall m, n > N' : : v(x_m - x_n) < C$, speciálisan minden $n > N'$-re $v(x_{\nu(N')} - x_n) < C$, így $C \geq \geq v(x_{\nu(N')}) \geq \min(v(x_{\nu(N')} - x_m), v(x_m))$ miatt elég nagy n-re $v(x_n) < C$, tehát $v(x_n)$ korlátos.

Mivel $v(x_n - x_{n+1})$ végtelenhez tart (hiszen x_n Cauchy-sorozat), így 3.1.3 szerint elég nagy n-ekre $v(x_n) = \min(v(x_n - x_{n+1}), v(x_{n+1})) = v(x_{n+1})$, tehát $v(x_n)$ egy idő után konstans, azaz a határértéke létezik. Ha $(x_n)_n, (x'_n)_n \in \mathcal{C} \setminus \mathcal{N}$ és a különbségük $\mathcal{N}$-beli, $v(x_n)$ és $v(x'_n)$ korlátosak, míg $v(x_n - x'_n)$ végtelenbe tart, így elég nagy n-ekre $v(x_n) = \min(v(x_n - x'_n), v(x'_n)) = v(x'_n)$ lesz, tehát a definíciónk jobb oldala nem függ a reprezentáns választásától. □

A többi szükséges tulajdonságot könnyű ellenőrizni: $\hat{v}$ nyilván v kiterjesztése lesz, továbbá (II) és (III) igaz marad, hiszen ha $x = (x_n)_n + \mathcal{N} \in \hat{K}^\times$, akkor létezik N, amelyre $\hat{v}(x) = v(x_n)$ minden $n > N$ egészre. K nyilván sűrű lesz $\hat{K}$-ban, $\hat{K}$ teljessége pedig analízisből ismert gondolatmenettel könnyen ellenőrizhető. □

3.1.10. Definíció. *$\hat{K}$-t (illetve $\hat{A} = \{x \in \hat{K} | \hat{v}(x) \geq 0\}$-t) K (illetve A) telítettjének nevezzük.*

3.1.11. Lemma. *1. Minden $\pi \in A$ prímelem $\hat{A}$-ban is prímelem.*

2. A és $\hat{A}$ maradékteste megegyezik.

Bizonyítás. Az első állítás következik abból, hogy a prímelemek éppen az 1 értékelésű elemek. A második állításhoz vegyük észre, hogy az $A \subseteq \hat{A}$ beágyazás indukál egy $A/\pi A \subseteq \hat{A}/\pi\hat{A}$ beágyazást. Legyen $\hat{a} \in \hat{A}$ tetszőleges. Mivel A sűrű $\hat{A}$-ban és 3.1.7 miatt $\hat{a} + \pi\hat{A}$ $\hat{a}$ egy nyílt környezete $\hat{A}$, így $\hat{a} + \pi\hat{A}$-ban található egy $a \in A$ elem, de ez igazolja, hogy a beágyazásunk szürjektív volt. □

3.2. Diszkrét értékelésgyűrűk bővítései

Ebben a részben legyen A egy diszkrét értékelésgyűrű K hányadostesttel, és tegyük fel, hogy K teljes. Legyen v a diszkrét értékelés, $\mathfrak{m} \subseteq A$ a maximális ideál, π egy rögzített prímelem és $k = A/\mathfrak{m}$ maradéktest.

3.2.1. Tétel. *(Hensel-lemma)*
Legyen $f \in A[T]$ egy polinom és tegyük fel, hogy vannak olyan $g_0, h_0 \in k[T]$ polinomok, hogy g_0 normált, g_0 és h_0 relatív prímek és $f \equiv g_0 h_0 \mod \mathfrak{m}$.

Ekkor léteznek $g, h \in A[T]$ polinomok, hogy g normált, $g \equiv g_0 \mod \mathfrak{m}$, $h \equiv h_0 \mod \mathfrak{m}$ és $f = gh$.

Bizonyítás. $n \in \mathbb{N}$ szerinti teljes indukcióval belátjuk, hogy léteznek olyan $g_n, h_n \in \in A[T]$ polinomok, hogy

$1_n)$ $f \equiv g_n h_n \mod \mathfrak{m}^{n+1}$

$2_n)$ g_n normált

$3_n)$ $\deg(h_n) \leq \deg(f) - \deg(g_0)$

$4_n)$ $g_n \equiv g_0 \mod \mathfrak{m}$, $h_n \equiv h_0 \mod \mathfrak{m}$

Az $n = 0$ eset következik a tétel feltételeiből (a tételben adott $g_0, h_0 \in k[T]$ $A[T]$-beli reprezentánsait véve). Tegyük fel, hogy a $g_0, g_1, \ldots, g_n$ és $h_0, h_1, \ldots, h_n$ polinomokat már megkonstruáltuk! g_{n+1}-et illetve h_{n+1}-et $g_{n+1} = g_n + u_n \pi^{n+1}$ illetve $h_{n+1} = h_n + v_n \pi^{n+1}$ alakban keressük, ahol $u_n, v_n \in A[T]$ polinomok. Ekkor $4_{n+1})$ automatikusan teljesülni fog.

Mivel g_0 és h_0 relatív prímek $k[T]$-ben, így $k[T] = \langle g_0, h_0 \rangle$, $4_n)$-et figyelembe véve így $k[T] = \langle g_n \mod \mathfrak{m}, h_n \mod \mathfrak{m} \rangle$. $1_n)$ szerint $\pi^{-(n+1)}(f - g_n h_n) \in A[T]$, így találhatunk $u_n, v_n \in A[T]$-t hogy

$$\frac{f - g_n h_n}{\pi^{n+1}} \equiv g_n v_n + h_n u_n \mod \mathfrak{m} \tag{1}$$

Ekkor

$$\frac{f - g_{n+1} h_{n+1}}{\pi^{n+1}} \equiv 0 \mod \mathfrak{m}$$

tehát $1_{n+1})$ is teljesülni fog. Vegyük észre, hogy ha $\varphi \in A[T]$ és (u_n, v_n)-t lecseréljük $(u_n + \varphi g_0, v_n - \varphi h_0)$-ra, akkor (1) továbbra is teljesülni fog. Keressünk olyan φ-t maradékos osztással (g_0 normált!), amelyre $u_n = (-\varphi) g_0 + r_0$, ahol $\deg(r_0) < \deg(g_0)$. Ezzel a φ választással elérjük, hogy $\deg(u_n) < \deg(g_0)$ legyen. Ekkor $2_{n+1})$ $2_n)$-ből triviálisan következik.

$3_n)$-ből következik, hogy

$$\deg(h_n u_n) = \deg(h_n) + \deg(u_n) \leq (\deg(f) - \deg(g_0)) + \deg(g_0) = \deg(f) \tag{2}$$

v_n $\mathfrak{m}$-beli együtthatóit cseréljük le nullákra, könnyen átgondolhatóan az eddigi összefüggéseink igazak maradnak. Mivel g_n normált, így

$$\begin{aligned}\deg(g_0)+\deg(v_n) &\overset{4_n)}{=} \deg(g_n)+\deg(v_n)=\deg(g_nv_n)=\deg(g_nv_n \mod \mathfrak{m})\\ &\overset{(1)}{\leq} \max\left(\deg\left(\frac{f-g_nh_n}{\pi^{n+1}} \mod \mathfrak{m}\right), \deg(h_nu_n \mod \mathfrak{m})\right)\\ &\leq \max(\deg(f-g_nh_n),\deg(h_nu_n))\\ &\overset{(2)}{\leq} \max(\deg(f-g_nh_n),\deg(f))\\ &\overset{3_n)}{=} \deg(f)\end{aligned}$$

Kihasználva azt is, hogy 3_n)-ből $\deg(h_n) \leq deg(f) - \deg(g_0)$, kapjuk, hogy $\deg(h_{n+1}) = = \deg(h_n+\pi^{n+1}v_n) \leq \max(\deg(h_n),\deg(v_n)) \leq \deg(f)-\deg(g_0)$, tehát 3_{n+1}) is teljesül. Ezzel az indukciós lépés igazolását befejeztük.

Legyen

$$g := \lim_{n\to\infty} g_n = g_0 + \sum_{n\geq 0} u_n\pi^{n+1}, \quad h := \lim_{n\to\infty} h_n = h_0 + \sum_{n\geq 0} v_n\pi^{n+1}$$

Itt a g_n-ek fokszáma korlátos (pontosabban mindnek $\deg(g_0)$ a foka, 2_n) és 4_n) szerint). Könnyen látható, hogy ha j rögzített, az a sorozat, aminek az n-edik eleme T^j együtthatója g_n-ben Cauchy-sorozat. De ekkor ez az együtthatósorozat konvergens (K teljes), sőt a határértéke A-ban van (A zárt 3.1.7 szerint). Így a limesz valóban értelmes és g egy $A[T]$-beli polinom, amire könnyen átgondolhatóan $g \equiv g_0 \mod \mathfrak{m}$. Hasonlóan h is egy $A[T]$-beli polinom lesz (ott 3_n) miatt korlátos a fokszámok sorozata) és $h \equiv h_0 \mod \mathfrak{m}$. Mivel $\deg(u_n) < \deg(g_0)$, így nyilván g normált lesz. 1_n)-ből

$$f - gh \equiv f - g_nh_n \equiv 0 \mod \mathfrak{m}^{n+1}$$

de ez azt jelenti, hogy $f-gh$ együtthatói $\bigcap_{n=1}^{\infty}\mathfrak{m}^n = \{0\}$-ban vannak, de így $f = = gh$. □

3.2.2. Következmény. *Legyen $f \in K[T]$ normált irreducibilis polinom, ekkor $f(0) \in A \Leftrightarrow f \in A[T]$.*

Bizonyítás. Nyilván csak a "⇒" iránnyal kell foglalkoznunk.

Legyen m minimális, hogy $\pi^m f \in A[T]$. Ha $m \leq 0$, akkor az állítás igaz, tehát feltehetjük, hogy $m \geq 1$. Mivel m minimális, így $\pi^m f \not\equiv 0 \mod \mathfrak{m}$, viszont mivel $m \geq 1$ és f normált, $\deg(\pi^m f \mod \mathfrak{m}) < \deg(f)$.

Ha $f(0) \in A$ lenne, akkor $\pi^m f(0) \in \mathfrak{m}$, így $\pi^m f \equiv T^r h_0 \mod \mathfrak{m}$ lenne egy olyan $h_0 \in k[T]$-re, amire $h_0(0)$ már nem 0 és egy $1 \leq r < \deg(f)$-re. A Hensel-lemmát

alkalmazva innen kapnánk a $\pi^m f$ polinom egy nemtriviális szorzatelőállítását, ami ellentmondana f irreducibilitásának. □

Rögzítsünk a továbbiakban egy L/K véges testbővítést.

3.2.3. Tétel. *Egyértelműen létezik egy $e(L/K)$ pozitív egész és L-en egy v_L diszkrét értékelés, amire $v_L|_{K^\times} = e(L/K) \cdot v$. ami osztója $[L : K]$-nak. Ez az $e(L/K)$ osztója $[L : K]$-nak; az L test teljes a v_L diszkrét értékeléssel ellátva.*

Bizonyítás. Legyen $d := [L : K]$ és $N : L^\times \to K^\times$ a normafüggvény. Legyen

$$\tilde{v}_L := v \circ N : L^\times \to \mathbb{Z}$$

Ekkor a (II) tulajdonság nyilvánvalóan teljesül $\tilde{v}_L$-re.

A (III) tulajdonság ellenőrzéséhez először belátjuk, hogy ha $x \in L$-re $\tilde{v}_L(x) \geq 0$, akkor $\tilde{v}_L(1+x) \geq 0$: Legyen $p(T)$ x minimálpolinomja K felett. Ekkor $p(0)^{[L:K(x)]} = = (-1)^d N(x)$. Mivel $\tilde{v}_L(x) \geq 0$, így $0 \leq v(N(x)) = [L : K(x)]v(p(0))$, tehát $p(0) \in \in A$. Így 3.2.2 miatt $p \in A[T]$, így $p(-1) \in A$, $v(p(-1)) \geq 0$. Azonban $p(T-1)$ éppen $x+1$ minimálpolinomja, így $p(0-1)^{[L:K(x)]} = (-1)^d N(x+1)$, de innen $\tilde{v}_L(x+ + 1) = v(N(x+1)) = [L : K(x)] \cdot v(p(-1)) \geq 0$.

Legyen $x, y \in L$, belátjuk hogy (III) teljesül rájuk. Tegyük fel hogy x és y egyik sem 0 (az az eset triviális) és hogy $\tilde{v}_L(y) \geq \tilde{v}_L(x)$ (feltehető mert (III) szimmetrikus). Ekkor $\tilde{v}_L\left(\frac{y}{x}\right) \geq 0$ és így

$$\tilde{v}_L(x+y) = \tilde{v}_L(x) + \tilde{v}_L\left(1 + \frac{y}{x}\right) \geq \tilde{v}_L(x) = \min(\tilde{v}_L(x), \tilde{v}_L(y))$$

így a (III) tulajdonságot ellenőriztük.

Mivel $\tilde{v}_L|_{K^\times} = d \cdot v$, így $d \cdot \mathbb{Z} \subseteq \mathrm{im}(\tilde{v}_L) \subseteq \mathbb{Z}$, de így egyértelműen létezik $c|d$, hogy $\mathrm{im}(\tilde{v}_L) = c \cdot \mathbb{Z}$.

Ekkor $v_L := \frac{1}{c}\tilde{v}_L : L^\times \to \mathbb{Z}$ szürjektív és így 3.1.4 szerint egy diszkrét értékelés. $v_L|_{K^\times} = \frac{d}{c} \cdot v$, így $e(L/K) := \frac{d}{c}$-t választunk.

(L, v_L) teljességének belátásához tekintjük az $|.|$ abszolútértéket K-n és L-en (mint K-vektortéren) definiáljuk az

$$|x|_L := e^{-v_L(x)/e(L/K)}$$

K-vektortérnormát ($|0|_L := 0$).

(Megjegyzés: Ha F egy test ellátva egy $|.| : F \to \mathbb{R}_{\geq 0}$ abszolútértékkel, akkor egy V F-vektortéren megadott F-vektortérnorma egy $\|.\| : V \to \mathbb{R}_{\geq 0}$ leképezés, amelyre

i. $\mathbf{a} \in V$-re $\|\mathbf{a}\| \geq 0$ és egyenőség pontosan $\mathbf{a} = 0$ esetén áll fenn

ii. $\alpha \in F$-re és $\mathbf{a} \in V$-re $\|\alpha V\| = |\alpha| \cdot \|\mathbf{a}\|$

iii. $\mathbf{a}, \mathbf{b} \in V$-re $\|\mathbf{a} + \mathbf{b}\| \leq \|\mathbf{a}\| + \|\mathbf{b}\|$

teljesül.)

Ha L-ben (mint K-vektortérben) fixálunk egy $e_1, e_2, \ldots, e_d$ bázist, akkor

$$\left| \sum_{i=1}^{d} a_i e_i \right|'_L := \max(|a_1|, |a_2|, \ldots, |a_d|)$$

egy másik K-vektortérnorma L-en. K teljességének a triviális következménye, hogy a $|.|'_L$ által megadott topológiával K teljes.

Használjuk fel a következő állítást (az [5] jegyzetben ez a 4.4.6 állítás, ott megtalálható a bizonyítása):

3.2.4. Állítás. *Egy $(F, |.|)$ abszolútértékkel ellátott test feletti véges dimenziós V vektortéren bármely két norma ugyanazt a topológiát generálja.*

Innen kapjuk, hogy a $|.|_L$ által generált topológia teljes, de átgondolhatóan v_L is ezt a topológiát generálja, így (L, v_L) teljes.

Már csak $e(L/K)$ és v_L egyértelműségét kell bizonyítanunk. Legyen w_L egy másik diszkrét értékelés L-en, amihez van olyan $b \in \mathbb{N}$, hogy $w_L|_{K^\times} = b \cdot v$. Ekkor legyen $\|x\|_L := e^{-w_L(x)/b}$, ez egyrészt egy abszolútértékfüggvény L-en (mint testen), másrészt egy $(K, |.|)$-vektortérnorma L-en (mint K-vektortéren). 3.2.4 szerint az $\|.\|_L$ norma azaz ugyanazt a topológiát generálja L-en, mint $|.|_L$.

A következő állítást is felhasználjuk ([5] 4.1.5):

3.2.5. Állítás. *Ha egy testen adott két abszolútérték, $\|.\|$ és $\|.\|'$, amik ugyanazt a topológiát generálják, akkor létezik $\sigma > 0$ valós, amelyre $\|.\|' = \|.\|^\sigma$.*

Emiatt létezik $\sigma > 0$ valós, amelyre $\|.\|_L = |.|_L^\sigma$, és mivel $|.|_L$ és $\|.\|_L$ is $|.|$ kiterjesztése, így $\sigma = 1$. Így $bv_L = e(L/K)w_L$. Mivel a w_L által kijelölt diszkrét értékelésgyűrűben van prímelem (aminek 1 az értékelése), így $b|e(L/K)$, ugyanezt a másik irányban is kihasználva $e(L/K)|b$, $b = e(L/K)$ és így $v_L = w_L$. Ezzel beláttuk az egyértelműséget is. □

Megjegyezzük, hogy $v_L(\pi) = e(L/K)$.

3.2.6. Definíció. *$e(L/K)$ az L/K bővítés elágazási indexe.*

Legyen $A_L \subseteq L$ a v_L által kijelölt értékelésgyűrű, $\pi_L \in A_L$ egy rögzített prímelem és $k_L = A_L/\pi_L A_L$ a maradéktest. Mivel $\pi A_L = \pi_L^{e(L/K)} A_L$, $\mathfrak{m} = \pi A \subseteq \pi_L A_L$. Az $A \subseteq A_L$ beágyazás így indukál egy $k \subseteq k_L$ beágyazást a maradéktestek között.

3.2.7. Lemma. $[k_L : k] < \infty$

Bizonyítás. Legyen $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n \in k_L$ lineárisan függtelen rendszer k felett és $y_i \in$ $\in A_L$ olyan, hogy $\bar{y}_i = y_i + \pi_L A_L$ $(1 \leq i \leq n)$. Elegendő belátni, hogy az y_i-k K felett lineárisan függetlenek, hiszen L végesdimenziós K felett. Tegyük fel indirekt, hogy $a_1y_1 + a_2y_2 + \ldots + a_ny_n = 0$, ahol $a_i \in K$ $(1 \leq i \leq n)$ és nem minden a_i nulla. Legyen $k = \min(v(a_1), v(a_2), \ldots v(a_n))$, ekkor $a_i' = \pi^{-k}a_i \in A \subseteq A_L$ $(v(a_i') = -k +$ $+ v(a_i) \geq 0)$, de valamely i-re $v(a_i') = (-k) + v(a_i) = 0$, tehát nem minden a_i' van benne $\pi_L A_L$-ben. Így a $a_1'y_1 + a_2'y_2 + \ldots + a_n'y_n = 0$ összefüggést $\mod \pi_L A_L$ tekintve kapjuk, hogy $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n$ mégsem lineárisan független, ami ellentmondás. □

3.2.8. Definíció. *$f(L/K) := [k_L : k]$ az L/K bővítés inerciafoka.*

3.2.9. Lemma. *Egy $M/L/K$ véges bővítésláncra*

$$e(M/K) = e(M/L)e(L/K) \text{ és } f(M/K) = f(M/L)f(L/K)$$

Bizonyítás. Ha $X \in \{K, L, M\}$, akkor jelölje v_X az X-en lévő diszkrét értékelést, π_X egy prímelemet az X-beli diszkrét értékelésgyűrűben, k_X az A_X-beli maradéktestet.

A második állítás azt mondja ki, hogy a $k_M/k_L/k_K$ bővítésláncra $[k_M : k_K] =$ $= [k_M : k_L] \cdot [k_L : k_K]$ és ez a fokszámtétel testbővítésekre. Az első állítás azt mondja ki, hogy $v_M(\pi_K) = e(M/L) \cdot v_L(\pi_K)$, de tudjuk, hogy $v_M|_{L^\times} = e(M/L)v_L$, így ez is teljesülni fog. □

3.2.10. Definíció. *Azt mondjuk, hogy az L/K bővítés*

– *elágazásmentes ha $e(L/K) = 1$ és k_L/k szeparábilis,*

– *teljesen elágazó, ha $e(L/K) = [L : K]$.*

Egy elágazásmentes L/K bővítésre K minden prímeleme L-ben is prímelem.

3.2.11. Lemma. *Legyen $R \subseteq A$ egy reprezentánsrendszere $A/\mathfrak{m}$-nek, ami a nullát tartalmazza, továbbá minden $m \in \mathbb{Z}$-hez rögzítsünk egy $\pi_m \in K$-t, amelyre $v(\pi_m) =$ $= m$. Ekkor a következők igazak:*

i. Ha $a_m \in R$, az $x := \sum_{m \geq m_0} a_m\pi_m$ összeg konvergens K-ban és $v(x) = \min\{m | a_m \neq 0\}$.

ii. Minden $x \in K$ egyértelműen írható $x = \sum_{m \geq m_0} a_m\pi_m$ alakban.

Bizonyítás.

i. A konvergencia triviálisan következik az egyszerűsített Cauchy-kritériumból és abból, hogy $v(a_m\pi_m) \geq m$. Vegyük észre, hogy R összes nemnulla eleme egység A-ban, így 0 értékeléssel rendelkezik, így ha $i = \min\{m|a_m \neq 0\}$, akkor minden $j \geq i$-re $v\left(\sum_{m=m_0}^{j} a_m\pi_m\right) = i$ (kihasználva a 3.1.3 összefüggést), így $v(x) = i$ lesz.

ii. $x = 0$-hoz $a_m = 0$ minden m-re jó választás, és megfordítva, ha $x = 0$, azaz $v(x) = \min\{m|a_m \neq 0\} = \infty$, akkor minden a_m-nek nullának kell lennie. Tegyük fel, hogy $x \in K^\times$ és legyen $m_0 = v(x)$. A létezéshez rekurzívan konstruálunk egy $(a_m)_{m\geq m_0}$ R-ben haladó sorozatot, amire minden $m \geq m_0$ esetén

$$v(x - s_m) \geq m, \text{ ahol } s_m := \sum_{m_0 \leq \mu < m} a_\mu\pi_\mu$$

(Ez $m = m_0$-ra teljesülni fog: $v(x - 0) \geq m_0$.) Tegyük fel, hogy $m \geq m_0$ és minden $m_0 \leq \mu < m$-re már megadtuk a_μ-t! Ekkor $v((x - s_m) \cdot \pi_m^{-1}) \geq 0$, így van olyan $a_m \in R$, amelyre $v((x-s_m)\cdot\pi_m^{-1}-a_m) \geq 1$. Ez jó választás lesz, hiszen ekkor $v(x-s_{m+1}) = v(x-s_m-a_m\pi_m) = v(\pi_m)+v((x-s_m)\cdot\pi_m^{-1}-a_m) \geq m+1$. Ezzel a létezést igazoltuk.

Az egyértelműség igazolásához tegyük fel, hogy $x = \sum_{m\geq m_0} a_m\pi_m = \sum_{n\geq n_0} b_n\pi_n$, ahol $a_m, b_n \in R$ és $a_{m_0} \neq 0 \neq b_{n_0}$. Ekkor $v(x) = m_0 = n_0$. Tegyük fel, hogy $a_{m_0} \neq b_{m_0}$ (különben az első néhány összeadandót elhagyhatjuk). Ekkor

$$(a_{m_0} - b_{m_0})\pi_{m_0} = \sum_{m>m_0} (a_m - b_m)\pi_m$$

így $v(a_{m_0} - b_{m_0}\pi_{m_0}) > m_0$, $v(a_{m_0} - b_{m_0}) > 0$ és ez elletmond annak, hogy $a_{m_0}, b_{m_0} \in R$ különböző elemek.

□

3.2.12. Példa. *Ezt $K = \mathbb{Q}_p$-re, $\pi_m = p^m$-re és $R = \{0,1,2,\ldots,p-1\}$-re alkalmazva kapjuk, hogy minden $x \in \mathbb{Q}_p$ egyértelműen előáll a következő alakban:*

$$x = \sum_{m\geq m_0} a_m p^m, \text{ ahol } 0 \leq a_m < p$$

3.2.13. Tétel. *i.* $[L : K] = e(L/K)f(L/K)$

ii. A_L *egy* $[L : K]$ *rangú szabad* A*-modulus*

Bizonyítás. Legyen $e := e(L/K)$ és $f := f(L/K)$. Legyen

$$\pi_m := \pi^n\pi_L^i, \text{ ha } m = ne + i, \text{ ahol } 0 \leq i < e$$

és R egy nullát tartalmazó reprezentánsrendszere $A/\mathfrak{m}$-nek. Jelöljünk ki $y_1, y_2, \ldots, y_f$ elemeket A_L-ben, úgy, hogy a maradékosztályaik egy k-bázisát alkossák k_L-nek. 3.2.11 szerint minden $x \in L$ egyértelműen írható a következő alakban (és minden ilyen alakú összeg konvergens)

$$x = \sum_{m \geq m_0} a_m \pi_m, \text{ ahol } a_m = r_1^{(m)} y_1 + r_2^{(m)} y_2 + \ldots + r_f^{(m)} y_f \text{ és } r_j^{(m)} \in R$$

Behelyettesítve és átrendezve ezt az egyértelmű az összegalakot

$$x = \sum_{i=0}^{e-1} \left(\sum_n a_{ne+i} \pi^n \right) \pi_L^i = \sum_{i=0}^{e-1} \sum_{j=1}^{f} \left(\sum_n r_j^{(ne+i)} \pi^n \right) y_j \pi_L^i$$

A $c_{i,j} := \sum_n r_j^(ne + i)\pi^n$ együtthatók K-ban vannak és minden K-beli elem egyértelműen áll elő ilyen alakban (3.2.11 miatt). Továbbá könnyen meggondolhatóan pontosan akkor van minden $c_{i,j}$ A-ban, ha x A_L-ben van.

Ez azt jelenti, hogy az ef elemű $\{y_j \pi_L^i | 0 \leq i \leq e-1, 1 \leq j \leq f\}$ rendszer egy K-bázisa L-nek és egy A-bázisa A_L-nek. □

Speciálisan kaptuk, hogy L/K pontosan akkor elágazásmentes, ha k_L/k szeparábilis és $[k_L : k] = [L : K]$.

3.2.14. Megjegyzés. *Legyen $p(T)$ az $x \in L$ elem minimálpolinomja K felett. Ekkor $x \in A_L \Leftrightarrow p \in A[T]$.*

Bizonyítás. v_L-ről 3.2.3 bizonyításában belátjuk, hogy $v_L(x) = \langle \text{pozitív érték} \rangle \cdot v(p(0))$ (pontosabban ezt $\tilde{v}_L$-ről látjuk be, ami pozitív konstansszorosa v_L-nek), így $x \in \in A_L \Leftrightarrow p(0) \in A$. Innen 3.2.2 alkalmazásával adódik a megjegyzésünk. □

3.2.15. Tétel. *Legyen $K \leq L_1, L_2 \leq L$ két testbővítéslánc; ekkor ha L_1/K és L_2/K is elágazásmentes, akkor $L_1 L_2/K$ is elágazásmentes.*

Bizonyítás. Mivel a testbővítések foka multiplikatív és a szeparabilitás tranzitív, így elég belátni, hogy $L_1 L_2/L_2$ elágazásmentes. Mivel minden szeparábilis bővítés egyszerű, létezik egy olyan $\bar{\alpha} \in k_{L_1}$, hogy $k_{L_1} = k(\bar{\alpha})$. Rögzítsünk $\alpha \in A_{L_1}$-et, amelyre $\bar{\alpha} = \alpha + \pi_{L_1} A_{L_1}$ és legyen $p(T)$ α-nak a K feletti minimálpolinomja! Az előző megjegyzés szerint $p \in A[T]$.

Ekkor

$$[k_{L_1} : k] \leq \deg(p \mod \mathfrak{m}) \leq \deg(p) = [K(\alpha) : K] \leq [L_1 : K] = [k_{L_1} : k]$$

így $L_1 = K(\alpha)$ és $p \mod \mathfrak{m}$ az $\bar{\alpha}$ k feletti minimálpolinomja. $L_1 = K(\alpha)$-ból $L_1 L_2 = = L_2(\alpha)$. α-nak az L_2 feletti $q(T)$ minimálpolinomja a Gauss-lemma miatt p-nek egy

$A_{L_2}[T]$-beli osztója. Így $q \mod \pi_{L_2} A_{L_2}$ osztója $p \mod \mathfrak{m}$-nek, tehát szeparábilis és így a Hensel-lemma miatt irreducibilis is (különben q is reducibilis lenne). Így kaptuk, hogy

$$\begin{aligned}[k_{L_1L_2} : k_{l_2}] \leq [L_1L_2 : L_2] = \\ = \deg(q) = \deg(q \mod \pi_{L_2} A_{L_2}) = [k_{L_2}(\bar{\alpha}) : k_{L_2}] \leq [k_{L_1L_2} : k_{l_2}]\end{aligned}$$

és innen következik $k_{L_1L_2} = k_{L_2}(\bar{\alpha})$ szeparabilitása k_{L_2} felett és $[k_{L_1L_2} : k_{l_2}] = [L_1L_2 : : L_2]$ is. □

3.2.16. Definíció. *A legnagyobb K felett elágazásmentes részbővítése L/K-nak L/K inerciateste.*

4. Konstrukciók diszkrét értékelésgyűrűkre

A következő fejezetekben megkonstruáljuk a Witt-vektorok $W(B)$ gyűrűjét egy B kommutatív egységelemes gyűrűhöz (amiről legtöbb tételben további tulajdonságokat is fel kell tenni, például azt, hogy test illetve azt, hogy p karakterisztikájú egy $p > 0$ prímre). Amennyiben B perfekt $p > 0$ karakterisztikájú test, akkor $W(B)$ egy teljes diszkrét értékelésgyűrű lesz (4.1.23 tétel). Ha B nem perfekt, akkor ugyan $W(B)$ maga nem diszkrét értékelésgyűrű, de bizonyos részgyűrűi, a Cohen-részgyűrűk már azok lesznek.

(Ez a fejezet nem része a Dieudonné–Manin tétel bizonyításának.)

4.1. Witt-vektorok

A továbbiakban legyen p egy rögzített prímszám. Minden $n \geq 0$-ra legyen

$$\Phi_n(X_0, \ldots, X_n) := \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n$$

az n-edik Wittpolinom. Ekkor $\Phi_0(X_0) = X_0$ és

$$\Phi_{n+1}(X_0, \ldots, X_{n+1}) = \Phi_n(X_0^p, \ldots, X_n^p) + p^{n+1} X_{n+1} = X_0^{p^{n+1}} + p\Phi_n(X_1, \ldots, X_{n+1}) \tag{3}$$

Legyen A egy tetszőleges kommutatív egységelemes gyűrű. Azt mondjuk, hogy $p1_A$ nem nullosztó, ha a p-vel való szorzás $A \to A$ injektív leképezés. (Ha $p1_A \in A^\times$, akkor a p-vel való szorzás természetesen bijektív.)

4.1.1. Lemma. *Ha $m, n \geq 1$ és $a, b \in A$, akkor*

$$a \equiv b \mod p^m A \Rightarrow a^{p^n} \equiv b^{p^n} \mod p^{m+n} A$$

Bizonyítás. Az $n = 1$ esetből a többi következik indukcióval, elég azt igazolni. $a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1})$. A második tényezőben minden tag $\equiv a^{p-1} \mod pA$ ($m \geq 1$) és p tag van, tehát a második tényező pA-ban van, $a - b$ pedig $p^m A$-ban, így valóban kapjuk a kívánt kongruenciát. □

4.1.2. Lemma. *Ha $m \geq 1$, $n \geq 0$ és $a_0, \ldots, a_n, b_0, \ldots, b_n \in A$, akkor*

i. $a_i \equiv b_i \mod p^m A$ *minden* $0 \leq i \leq n$*-re* $\Rightarrow \Phi_i(a_0, \ldots, a_i) \equiv \Phi_i(b_0, \ldots, b_i) \mod p^{m+i} A$ *minden* $0 \leq i \leq n$*-re.*

ii. Ha $p1_A$ nem nullosztó, ennek a megfordítása is teljesül.

Bizonyítás. Mindkét részt indukcióval látjuk be, $n = 0$ mindkét résznél triviális. Tegyük fel, hogy $n \geq 1$.

i. $a_i^p \equiv b_i^p \mod p^{m+1}A$ az előző lemma és a feltevéseink miatt. Az indukciós feltevést alkalmazva az a_i^p-ekre és $m+1$-re, majd a (3) rekurziós formulát alkalmazva

$$\Phi_n(a_0, \ldots, a_n) - p^n a_n \equiv \Phi_n(b_0, \ldots, b_n) - p^n b_n \mod p^{m+n}A$$

és $a_n \equiv b_n \mod p^m A$, $p^n a_n \equiv p^n b_n \mod p^{m+n}A$ miatt így készen vagyunk.

ii. Az indukciós feltevésből $a_i \equiv b_i \mod p^m A$ minden $0 \leq i < n$-re. Ezekből a feltételekből ismét levezethetjük az

$$\Phi_n(a_0, \ldots, a_n) - p^n a_n \equiv \Phi_n(b_0, \ldots, b_n) - p^n b_n \mod p^{m+n}A$$

összefüggést, de most azt tudjuk, hogy a két $\Phi_n(\ldots)$ érték lesz kongruens, így azt kapjuk, hogy $p^n(a_n - b_n) \in p^{m+n}A$, ahonnan a p-vel szorzás injektív volta miatt készen vagyunk.

□

Legyen

$$A^{\mathbb{N}} = \{(a_0, a_1, a_2, \ldots) | a_i \in A\}$$

az A gyűrű megszámlálhatóan végtelen sok példányának a direkt szorzata (az összeadást és szorzást komponensenként értelmezzük). Definiáljuk a következő leképezéseket:

$$\begin{aligned} f_A \quad &: \quad A^{\mathbb{N}} \to A^{\mathbb{N}} \\ (a_0, a_1, a_2, \ldots) &\mapsto (a_1, a_2, \ldots) \end{aligned}$$

(ez egy gyűrűhomomorfizmus),

$$\begin{aligned} v_A \quad &: \quad A^{\mathbb{N}} \to A^{\mathbb{N}} \\ (a_0, a_1, \ldots) &\mapsto (0, pa_1, pa_2, \ldots) \end{aligned}$$

(ez additív, de a szorzást és az egységelemet nem tartja),

$$\begin{aligned} \Phi_n \quad &: \quad A^{\mathbb{N}} \to A \\ (a_0, a_1, \ldots) &\mapsto \Phi_n(a_0, a_1, \ldots, a_n) \end{aligned}$$

és

$$\begin{aligned} \Phi_A \quad &: \quad A^{\mathbb{N}} \to A^{\mathbb{N}} \\ \mathbf{a} &\mapsto (\Phi_0(\mathbf{a}), \Phi_1(\mathbf{a}), \ldots) \end{aligned}$$

4.1.3. Lemma. *i. Ha $p1_A$ nem nullosztó A-ban, akkor Φ_A injektív.*

ii. Ha $p1_A \in A^\times$*, akkor* Φ_A *bijektív.*

Bizonyítás. Legyenek $\mathbf{a} = (a_0, a_1, \ldots)$ és $\mathbf{u} = (u_0, u_1, \ldots)$ $A^{\mathbb{N}}$-beli elemek! A (3) rekurziós formula szerint $\Phi_A(\mathbf{a}) = \mathbf{u}$ ekvivalens a következővel:

$$\begin{aligned} u_0 &= a_0 \\ u_n &= \Phi_{n-1}(a_0^p, a_1^p, \ldots a_{n-1}^p) + p^n a_n \text{ ha } n \geq 1 \end{aligned} \tag{4}$$

A bizonyítandó állítás innen könnyen leolvasható: ha a p-vel szorzás, így a p^n-nel szorzás is injektív, akkor adott u_n-ekhez egyetlen (a_n) sorozat tartozhat, míg ha ez a szorzás bijektív, akkor tetszőleges u_n-ekhez találhatunk $\mathbf{a}$-t. □

A (4) rendszerből leolvasható következő:

4.1.4. Következmény. *Legyen* $\mathbf{a} = (a_n)_n, \mathbf{u} = (u_n)_n \in A^{\mathbb{N}}$ *olyanok, hogy* $\Phi_A(\mathbf{a}) = \mathbf{u}$*. Legyen* $B \leq A$ *olyan egységelemes részgyűrű, hogy a* p*-vel való szorzás, mint az* A/B *Abel-csoportot önmagára képző homomorfizmus injektív. Ekkor minden* $m \geq 0$*-ra*

$$u_0, \ldots, u_m \in B \Leftrightarrow a_0, \ldots, a_m \in B$$

4.1.5. Tétel. *Tegyük fel, hogy* A*-n adott egy* σ *endomorfizmus, amire* $\sigma(x) \equiv x^p \mod pA$ *minden* $x \in A$*-ra. Adott* $n \geq 1$*-hez és* $a_0, a_1, \ldots, a_{n-1}$*-hez legyen minden* $0 \leq i \leq n-1$*-re* $u_i = \Phi_i(a_0, \ldots, a_i)$*; ekkor egy* $u \in A$*-ra*

$$(\exists a_n : u_n = \Phi_n(a_0, \ldots, a_n)) \Leftrightarrow \sigma(u_{n-1}) \equiv u_n \mod p^n A$$

Bizonyítás. A 4.1.2 lemma első részét használva $m = 1$-gyel

$$\sigma(u_{n-1}) = \Phi_{n-1}(\sigma(a_0), \ldots, \sigma(a_{n-1}) \equiv \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \mod p^n A$$

Egy olyan a_n, amelyre $u_n = \Phi_n(a_0, \ldots, a_n) = \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n a_n$, pontosan akkor létezik, ha $u_n - \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \in p^n A$, de $\sigma(u_{n-1}) \equiv \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \mod p^n A$ miatt ez ekvivalens $u_n \equiv \sigma(u_{n-1}) \mod p^n A$-val. □

A tétel állítása alapján jellemezhetjük $\mathrm{im}(\Phi_A)$-t:

4.1.6. Következmény. $A' := \mathrm{im}(\Phi_A)$ *egy részgyűrű* $A^{\mathbb{N}}$*-ben, amire*

$$A' = \{(u_n)_n \in A^{\mathbb{N}} | \sigma(u_n) \equiv u_{n+1} \mod p^{n+1} A \text{ minden } n \geq 0\text{-ra}\}$$

és $v_A(A') \subseteq A'$*,* $f_A(A') \subseteq A'$*.*

Ezeket az eredményeinket a (kétszer) megszámlálhatóan végtelen változós

$$A := \mathbb{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$$

polinomgyűrűre alkalmazzuk, amin $p1_A$ nyilván nem nullosztó. Definiájuk a $\theta : A \to A$ gyűrűendomorfizmust úgy, hogy $\theta|_{\mathbb{Z}} := id_{\mathbb{Z}}$, $\theta(X_i) := X_i^p$ és $\theta(Y_i) := Y_i^p$.

4.1.7. Lemma. $\theta(x) \equiv x^p \mod pA$ *minden* $x \in A$*-ra.*

Bizonyítás. Az $\{x \in A | \theta(x) \equiv x^p \mod pA\}$ halmaz könnyen átgondolhatóan részgyűrű A-ban, ami a kis Fermat-tétel szerint tartalmazza $\mathbb{Z}$-t és θ definíciójából leolvashatóan tartalmazza az X_i-ket és Y_i-ket, így ez a részgyűrű maga A lesz. □

Legyen $\mathbf{X} := (X_n)_n$ és $\mathbf{Y} = (Y_n)_n$ $A^{\mathbb{N}}$-ben. 4.1.6 illetve 4.1.3 szerint léteznek illetve egyértelműek olyan $\mathbf{S} = (S_n)_n$, $\mathbf{P} = (P_n)_n$, $\mathbf{I} = (I_n)_n$ és $\mathbf{F} = (F_n)_n$ elemek $A^{\mathbb{N}}$-ben, hogy

$$\begin{aligned}
\Phi_A(\mathbf{S}) &= \Phi_A(\mathbf{X}) + \Phi_A(\mathbf{Y}) \\
\Phi_A(\mathbf{P}) &= \Phi_A(\mathbf{X}) \cdot \Phi_A(\mathbf{Y}) \\
\Phi_A(\mathbf{I}) &= -\Phi_A(\mathbf{X}) \\
\Phi_A(\mathbf{F}) &= f_A(\Phi_A(\mathbf{X}))
\end{aligned}$$

azaz

$$\begin{aligned}
\Phi_n(S_0, \ldots, S_n) &= \Phi_n(X_0, \ldots, X_n) + \Phi_n(Y_0, \ldots, Y_n) \\
\Phi_n(P_0, \ldots, P_n) &= \Phi_n(X_0, \ldots, X_n) \cdot \Phi_n(Y_0, \ldots, Y_n) \\
\Phi_n(I_0, \ldots, I_n) &= -\Phi_n(X_0, \ldots, X_n) \\
\Phi_n(F_0, \ldots, F_n) &= \Phi_{n+1}(X_0, \ldots, X_{n+1})
\end{aligned} \tag{5}$$

4.1.4 szerint

$$\begin{aligned}
S_n, P_n &\in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n] \\
I_n &\in \mathbb{Z}[X_0, \ldots, X_n] \\
F_n &\in \mathbb{Z}[X_0, \ldots, X_{n+1}]
\end{aligned}$$

Ezek az S_n, P_n, I_n, F_n polinomok a (4) rekurziós képletek segítségével kifejezhetőek:

$$\begin{aligned}
&S_0 = X_0 + Y_0, \quad S_1 = X_1 + Y_1 + \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i Y_0^{p-i} \\
&P_0 = X_0 Y_0, \quad P_1 = pX_1Y_1 + X_0^p Y_1 + X_1 Y_0^p \\
&F_0 = X_0 + pX_1, \quad F_1 = X_1^p + pX_2 - \sum_{i=0}^{p-1} \binom{p}{i} p^{p-i-1} X_0^{pi} X_1^{p-i}
\end{aligned}$$

Ha $p \neq 2$, $I_n = -X_n$ triviálisan ellenőrizhető minden $n > 0$-ra.

4.1.8. Lemma. $S_n - X_n - Y_n \in \mathbb{Z}[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$

Bizonyítás. Az állítás belátásához a

$$\Phi_n(S_0,\dots,S_n)=\Phi_n(X_0,\dots,X_n)+\Phi_n(Y_0,\dots,Y_n)$$

képletből indulunk ki. Ide a (3) rekurziós formulát beírva

$$\Phi_{n-1}(S_0^p,\dots,S_{n-1}^p)-\Phi_{n-1}(X_0^p,\dots,X_{n-1}^p)-\Phi_{n-1}(Y_0^p,\dots,Y_{n-1}^p)=p^n\cdot(S_n-X_n-Y_n)$$

és itt a bal oldalon $\mathbb{Z}[X_0,\dots,X_{n-1},Y_0,\dots,Y_{n-1}]$-beli kifejezés áll, így készen vagyunk. □

Legyen B egy tetszőleges kommutatív egységelemes gyűrű. Erre korábban már definiáltuk a $(B^{\mathbb{N}},+,\cdot)$ gyűrűt. Minden $\rho:B_1\to B_2$ (egységelemet is tartó) gyűrűhomomorfizmusra a $\rho^{\mathbb{N}}:B_1^{\mathbb{N}}\to B_2^{\mathbb{N}},(b_n)_n\mapsto(\rho(b_n))_n$ leképezés egy gyűrűhomomorfizmus.

Definiálunk egy másik gyűrűstruktúrát is a $W(B):=B^{\mathbb{N}}$ halmazon: legyen

$$\begin{aligned}(a_n)_n\oplus(b_n)_n&:=(S_n(a_0,\dots,a_n,b_0,\dots,b_n))_n\\(a_n)_n\odot(b_n)_n&:=(P_n(a_0,\dots,a_n,b_0,\dots,b_n))_n\end{aligned}$$

és

$$\mathbf{0}:=(0,0,\dots),\quad \mathbf{1}:=(1,0,0,\dots)$$

P és **S** definíciójából a $\Phi_B:W(B)\to B^{\mathbb{N}}$ leképezésre

$$\begin{aligned}\Phi_B(\mathbf{a}\oplus\mathbf{b})&=\Phi_B(\mathbf{a})+\Phi_B(\mathbf{b})\\\Phi_B(\mathbf{a}\odot\mathbf{b})&=\Phi_B(\mathbf{a})\cdot\Phi_B(\mathbf{b})\end{aligned}\tag{6}$$

és könnyen láthatóan

$$\Phi_B(\mathbf{0})=0\text{ és }\Phi_B(\mathbf{1})=1\ .\tag{7}$$

Minden $\rho:B_1\to B_2$ gyűrűhomomorfizmusra a $W(\rho):=\rho^{\mathbb{N}}:W(B_1)\to W(B_2)$ függvény nyilvánvalóan megtartja a $\oplus$ és $\odot$ műveleteket, kielégíti az $W(\rho)(\mathbf{1})=\mathbf{1}$ összefüggést és a

$$\begin{array}{ccc}W(B_1) & \xrightarrow{\Phi_{B_1}} & B_1^{\mathbb{N}}\\ \downarrow{\scriptstyle W(\rho)} & & \downarrow{\scriptstyle \rho^{\mathbb{N}}}\\ W(B_2) & \xrightarrow{\Phi_{B_2}} & B_2^{\mathbb{N}}\end{array}\tag{8}$$

diagram kommutatív lesz.

4.1.9. Tétel. *i.* $(W(B),\oplus,\odot)$ *egy kommutatív gyűrű* $\mathbf{1}$ *egységelemmel és* $\mathbf{0}$ *nullelemmel, amiben* $(b_n)_n$ *additív inverze* $(I_n(b_0,\dots,b_n))_n$.

ii. $\Phi_B : W(B) \to B^{\mathbb{N}}$ *gyűrűhomomorfizmus, azaz minden* $m \in \mathbb{N}$*-re* $\Phi_m : W(B) \to B$, $(b_n)_n \mapsto \Phi_m(b_0, \ldots, b_m)$ *gyűrűhomomorfizmus.*

iii. Minden $\rho : B_1 \to B_2$ *gyűrűhomomorfizmusra* $W(\rho) : W(B_1) \to W(B_2)$ *gyűrűhomomorfizmus.*

Bizonyítás. A tétel előtti megjegyzéseink miatt elég az első állítást bizonyítanunk. Tekintsük a $B_1 := \mathbb{Z}[\{X_b | b \in B\}]$ polinomgyűrűt és rajta a $\rho : B_1 \to B$, $X_b \mapsto b$ szürjektív homomorfizmust. A B_1 gyűrűn $\sigma(X_b) := X_b^p$ egy endomorfizmust definiál, amire $\sigma(b) \equiv b^p \mod pB_1$ minden $b \in B_1$-re. Nyilván $p1_{B_1}$ nem nullosztó B_1-ben. Ekkor 4.1.3 i. és 4.1.4 miatt

$$\Phi_{B_1} : W(B_1) \xrightarrow{\cong} B_1'$$

egy $B_1' \leq B_1^{\mathbb{N}}$ részgyűrűre képző bijekció. (6) és (7) miatt így a $B_1^{\mathbb{N}}$-beli asszociativitás, disztriutivitás stb. átvihető $W(B_1)$-re is, így $(W(B_1), \oplus, \odot)$ kommutatív gyűrű $\mathbf{1}$ egységelemmel. Az additív inverzere vonatkozó képlet triviális az I_n-re vonatkozó összefüggéseinkből. Ezután használjuk fel, hogy a $W(\rho) : W(B_1) \to W(B)$ szürjektív leképezés tartja a $\oplus$ és $\odot$ műveleteket, valamint az egységelemet, így vele $W(B)$-re is átvihetőek ugyanezek. □

4.1.10. Definíció. $(W(B), \oplus, \odot)$ *a* B*-beli együtthatós Witt-vektorok gyűrűje.*

A $\Phi_n(b_0, \ldots, b_n)$ elemeket a $(b_n)_n \in W(B)$ Witt-vektor *fantomkomponenseinek* nevezzük.

Ezen felül $W(B)$-n definiálhatjuk a következő leképezéseket:

$$F : W(B) \to W(B), \quad (b_n)_n \mapsto (F_n(b_0, \ldots, b_n))_n$$
$$V : W(B) \to W(B), \quad (b_n)_n \mapsto (0, b_0, b_1, \ldots)$$

Az (5) és (4) összefüggésekből adódik, hogy a

$$\begin{array}{ccc} W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}} \\ \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle f_B} \\ W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}} \end{array} \quad \text{és} \quad \begin{array}{ccc} W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}} \\ \downarrow{\scriptstyle V} & & \downarrow{\scriptstyle v_B} \\ W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}} \end{array} \tag{9}$$

diagramok kommutatívak.

4.1.11. Tétel. *i.* F *gyűrűendomorfizmus* $W(B)$*-n.*

ii. V *Abel-csoport endomorfizmus* $W(B)$ *additív csoportján.*

iii. $F(V(\mathbf{b})) = p\mathbf{b}$ *minden* $\mathbf{b} \in W(B)$*-re.*

iv. $V(\mathbf{a} \odot F(\mathbf{b})) = V(\mathbf{a}) \odot \mathbf{b}$ *minden* $\mathbf{a}, \mathbf{b} \in W(B)$*-re.*

v. $F(\mathbf{b}) \equiv \mathbf{b}^p \mod pW(B)$ *minden* $\mathbf{b} \in B$*-re*

(A tételben $p\mathbf{b}$ és $\mathbf{b}^p$ természetesen a $W(B)$-n megadott új $(W(B), \oplus, \odot)$ gyűrűstruktúra szerint értendő.)

Bizonyítás. Ezeknek az állításoknak a bizonyításához ugyanazt a gondolatmenetet alkalmazhatjuk, mint a 4.1.9 tétel bizonyításában:

Ismét áttérünk a $B_1 := \mathbb{Z}[\{X_b | b \in B\}]$ gyűrűre, ahol tudni fogjuk, hogy

$$\Phi_{B_1} : W(B_1) \overset{\cong}{\to} B_1'$$

egy $B_1' \leq B_1^{\mathbb{N}}$ részgyűrűre képző bijekció. A tétel állításainak triviálisan teljesülnek a $B_1^{\mathbb{N}}$ feletti megfelelői (ahol $W(B)$, F, V, $\oplus$ és $\odot$ helyett rendre $B_1^{\mathbb{N}}$, f_{B_1}, v_{B_1}, $+$ $+$ és $\cdot$ szerepel). Ekkor speciálisan B_1' felett is teljesülnek ezek, azonban mivel a Φ_{B_1} izomorfizmus (9) szerint F-et és V-t f_{B_1}-nek és v_{B_1}-nek felteti meg, így kapjuk, hogy $W(B_1)$ felett igazak a tétel állításai. Ezután ugyanúgy fejezhetjük be a bizonyítást, mint a 4.1.9 tételnél: az ottani $W(\rho) : W(B_1) \to W(B)$ szürjektív leképezés a gyűrűműveletek tartásán kívül könnyen átgondolhatóan kommutál az F és V leképezésekkel is. □

4.1.12. Definíció. *F-et ill V-t a $W(B)$-n lévő Frobeniusnak illetve Verschiebungnak ("eltolás") nevezzük.*

Minden $m \geq 0$-ra legyen

$$V_m(B) := \mathrm{im}(V^m) = \{(b_n)_n \in W(B) | b_0 = \ldots = b_{m-1} = 0\}$$

Ekkor

$$W(B) = V_0(B) \supset V_1(B) \ldots \quad \text{és} \quad \bigcap_m V_m(B) = \{0\}$$

4.1.11 ii. és iv. része szerint $V_m(B) \triangleleft W(B)$ ideál.

4.1.13. Definíció. $W_m(B) := W(B)/V_m(B)$ *az m hosszú B-beli együtthatós Witt-vektorok gyűrűje.*

4.1.14. Lemma. *i. Minden $m \geq 1$-re és $(b_n)_n \in W(B)$-re*

$$(b_n)_n = (b_0, b_1, \ldots, b_{m-1}, 0, 0, \ldots) \oplus (\underbrace{0, 0, \ldots, 0}_{m \text{ darab}}, b_m, b_{m+1}, \ldots)$$

ii. A

$$B^m \to W_m(B)$$
$$(b_0, \ldots, b_{m-1}) \mapsto (b_0, \ldots, b_{m-1}, 0,0, \ldots) \oplus V_m(B)$$

függvény minden $m \geq 1$-re bijektív.

Bizonyítás. i. Ismét a 4.1.9 bizonyításában felhasznált technikát fogjuk alkalmazni. Elegendő belátnunk, hogy

$$\Phi_k((b_n)_n) = \Phi_k(b_0, b_1, \ldots, b_{m-1}, 0, 0, \ldots) + \Phi_k(\underbrace{0, 0, \ldots, 0}_{m \text{ darab}}, b_m, b_{m+1}, \ldots) \quad (10)$$

minden $k \geq 0$, ezt B helyett a B_1 polinomgyűrűre alkalmazva, kihasználva, hogy $W(B_1)$ izomorf $B_1^{\mathbb{N}}$ egy részgyűrűjével, majd a $W(\rho) : W(B_1) \to W(B)$ szürjektív leképezéssel visszatérve $W(B)$-re kapjuk a bizonyítandó állítást.

(10) azért teljesül, mert

$$\Phi_k(b_0, b_1, \ldots, b_{m-1}, 0, 0, \ldots) = \begin{cases} \Phi_k(b_0, \ldots, b_k) & \text{, ha } 0 \leq k < m \\ \sum_{i=0}^{m-1} p^i b_i^{p^{k-i}} & \text{, ha } m \leq k \end{cases}$$

és

$$\Phi_k(\underbrace{0, 0, \ldots, 0}_{m \text{ darab}}, b_m, b_{m+1}, \ldots) = \begin{cases} 0 & \text{, ha } 0 \leq k < m \\ \sum_{i=m}^{k} p^i b_i^{p^{k-i}} & \text{, ha } m \leq k \end{cases}$$

ii. A függvényünk i. miatt szürjektív. Az injektivitáshoz tegyük fel, hogy

$$(c_0, \ldots, c_{m-1},0, \ldots) \oplus V_m(B) = (b_0, \ldots, b_{m-1},0, \ldots) \oplus V_m(B)$$

Ekkor van egy olyan $\mathbf{b}' = (\underbrace{0, 0, \ldots, 0}_{m \text{ darab}}, b_m, b_{m+1}, \ldots) \in V_m(B)$ elem, hogy

$$(c_0, \ldots, c_{m-1},0, \ldots) = (b_0, \ldots, b_{m-1},0, \ldots) \oplus \mathbf{b}'$$

de így i. szerint

$$(c_0, \ldots, c_{m-1},0,0, \ldots) = (b_0, \ldots, b_{m-1}, b_m, b_{m+1}, \ldots)$$

azaz $c_i = b_i$ $0 \leq i < m$ esetén, azaz a függvényünk valóban injektív.

□

4.1.15. Megjegyzés. *Az ii. részben szereplő bijekció az $m = 1$ esetben könnyen láthatóan gyűrűizomorfizmus, a $\Phi_0 : W_1(B) \to B$ leképezés inverze; az általános esetben viszont nem tartja a gyűrűműveleteket.*

4.1.16. Lemma.

$$\begin{aligned} W(B) &\overset{\cong}{\to} \varprojlim_m W_m(B) \\ \mathbf{b} &\mapsto (\mathbf{b} \oplus V_m(B))_m \end{aligned}$$

egy gyűrűizomorfizmus.

Bizonyítás. Mivel $\bigcap_m V_m(B) = \{0\}$, a leképezésünk injektív. Az összeadás, szorzás és egységelem tartása is triviálisan teljesülni fog, mert a $\mathbf{b} \mapsto \mathbf{b} \oplus V_m(B) \in W_m(b)$ leképezésere teljesül. A szürjektivitás belátásához legyen $\hat{\mathbf{b}} = (\hat{\mathbf{b}}_m)_m \in \varprojlim_m W_m(B)$ (azaz $\hat{\mathbf{b}}_m \in W_m(B)$ és $0 \leq k \leq m$ esetén $\hat{\mathbf{b}}_m \oplus V_k(B) = \hat{\mathbf{b}}_k$). Az előző lemma ii. része miatt minden m-re van olyan $b_0^{(m)}, \ldots, b_{m-1}^{(m)}$, hogy

$$\hat{\mathbf{b}}_m = (b_0^{(m)}, \ldots, b_{m-1}^{(m)}, 0, 0, \ldots) \oplus V_m(B)$$

Mivel $0 \leq k \leq m$ esetén $\hat{\mathbf{b}}_m \oplus V_k(B) = \hat{\mathbf{b}}_k$,

$$(b_0^{(k)}, \ldots, b_{k-1}^{(k)}, 0, 0, \ldots) \in (b_0^{(m)}, \ldots, b_{m-1}^{(m)}, 0, 0, \ldots) \oplus V_k(B)$$

és itt

$$(b_0^{(m)}, \ldots, b_{m-1}^{(m)}, 0, 0, \ldots) = (b_0^{(m)}, \ldots, b_{k-1}^{(m)}, 0, 0, \ldots) \oplus (\underbrace{0, 0, \ldots, 0}_{k \text{ darab}}, b_k^{(m)}, \ldots, b_{m-1}^{(m)}, 0, 0, \ldots)$$

így

$$(b_0^{(k)}, \ldots, b_{k-1}^{(k)}, 0, 0, \ldots) \in (b_0^{(m)}, \ldots, b_{k-1}^{(m)}, 0, 0, \ldots) \oplus V_k(B)$$

azaz minden $0 \leq i < k \leq m$ esetén $b_i^{(k)} = b_i^{(m)}$. Ez viszont azt jelenti, hogy $(b_n^{(n+1)})_n \in$ $\in W(B)$ képe a leképezésnél éppen $\hat{\mathbf{b}}$ lesz. □

4.1.17. Lemma. *A*

$$\begin{aligned} \tau : B &\to W(B) \\ b &\mapsto (b, 0, 0, \ldots) \end{aligned}$$

függvény multiplikatív.

Bizonyítás. Legyen

$$\tilde{P}_n = P_n(X_0, \underbrace{0, \ldots, 0}_{n-1 \text{ darab}}, Y_0, \underbrace{0, \ldots, 0}_{n-1 \text{ darab}})$$

Tudjuk, hogy $\tilde{P}_0 = P_0(X_0, Y_0) = X_0Y_0$, azt kell még belátnunk, hogy $\tilde{P}_n = 0$ minden $n \geq 1$-re.

Az (5) egyenletből

$$(X_0Y_0)^{p^n} + \sum_{i=1}^{n} p^i \tilde{P}_i^{p^{n-i}} = \Phi_n(\tilde{P}_0, \dots \tilde{P}_n) = \Phi_n(X_0, 0, \dots)\Phi_n(Y_0, 0, \dots) = X_0^{p^n} Y_0^{p^n}$$

és innen indukcióval adódik, hogy $\tilde{P}_n = 0$ minden $n \geq 1$-re. □

4.1.18. Definíció. *$\tau(b) \in W(B)$ a $b \in B$ elem Teichmüller-reprezentánsa.*

4.1.19. Lemma. *Minden $k \geq 1$-re $V_1(B)^k = p^{k-1}V_1(B)$.*

Bizonyítás. A 4.1.11 tétel rendre iv., iii. és ii. részét használva

$$V(\mathbf{a}) \odot V(\mathbf{b}) = V(\mathbf{a} \odot F(V(\mathbf{b}))) = V(\mathbf{a} \odot p\mathbf{b}) = pV(\mathbf{a} \odot \mathbf{b})$$

és így $V_1(B)^2 = pV_1(B)$, és ebből indukcióval következik a lemma állítása. □

Azt mondjuk, hogy a B gyűrű p karakterisztikájú, ha $p1_B = 0$. Ebben az esetben a $B \to B$, $b \mapsto b^p$ Frobenius-leképezés egy gyűrűendomorfizmus. Ha ez az endomorfizmus bijektív, azt mondjuk, hogy B perfekt.

4.1.20. Tétel. *Amennyiben B p karakterisztikájú*

i. $\mathbf{b} = (b_n)_n \in B$*-re*

$$F(\mathbf{b}) = (b_n^p)_n \quad \text{és} \quad p\mathbf{b} = VF(\mathbf{b}) = FV(\mathbf{b}) = (0, b_0^p, b_1^p, \dots)$$

ii. $V_m(B) \odot V_n(B) \subseteq V_{m+n}(B)$ *minden $m, n \geq 0$-ra.*

iii. $p^k W(B) \subseteq V_1(B)^k \subseteq p^{k-1}W(B)$ *minden $k \geq 1$-re.*

iv. A

$$W(B) \xrightarrow{\cong} \varprojlim_k (W(B)/p^k W(B))$$
$$\mathbf{b} \mapsto (\mathbf{b} \oplus p^k W(B))_k$$

gyűrűhomomorfizmus bijektív.

Bizonyítás. i. Ez az állítás következik a 4.1.7 lemmából és a 4.1.11 tétel iii. részéből.

ii. A 4.1.11 tétel iv. részéből indukcióval adódik, hogy $V^m(\mathbf{a}\odot F^m(\mathbf{b})) = V^m(\mathbf{a})\odot\mathbf{b}$. Innen kaphatjuk, hogy

$$V^m(\mathbf{a}) \odot V^n(\mathbf{b}) = V^m(\mathbf{a} \odot F^m(V^n(\mathbf{b})))$$

és

$$V^n(F^m(\mathbf{b})) \odot \mathbf{a} = V^n(F^m(\mathbf{b}) \odot F^n(\mathbf{a}))$$

Azonban most i. miatt $V^n \circ F^m = F^m \circ V^n$, így

$$V^m(\mathbf{a}) \odot V^n(\mathbf{b}) = V^{m+n}(F^m(\mathbf{b}) \odot F^n(\mathbf{a}))$$

minden $\mathbf{a}, \mathbf{b} \in W(B)$-re

i.-ből $pW(B) = V(F(W(B))) \subseteq V_1(B)$, így a 4.1.19 lemma miatt valóban teljesül az állítás.

i. szerint

$$p^kW(B) = \{(\underbrace{0, \ldots, 0}_{k \text{ darab}}, b_k, b_{k+1}, \ldots) \in W(B) | b_n \in B^{p^k} \text{ minden } n \geq k\text{-ra}\}$$

Innen leolvasható, hogy $\bigcap_{k\geq 1} p^kW(B) = \{\mathbf{0}\}$, ami igazolja a leképezésünk injektív voltát.

Legyen $(\mathbf{b}^{(k)} \oplus p^kW(B))_k \in \varprojlim W(B)/p^kW(B)$. i. és iii. szerint $p^kW(B) \subseteq V_k(B)$, és így $(\mathbf{b}^{(k)} \oplus V_k(B))_k \in \varprojlim W(B)/V_k(B)$. A 4.1.16 lemma szerint van olyan $\mathbf{b} \in \in W(B)$, hogy $\mathbf{b} \oplus V_k(B) = \mathbf{b}^{(k)} \oplus V_k(B)$ minden k-ra. Ekkor minden $j \geq k$-ra

$$\mathbf{b} \oplus V_j(B) \oplus p^kW(B) = \mathbf{b}^{(j)} \oplus V_j(B) \oplus p^kW(B) = \mathbf{b}^{(k)} \oplus V_j(B) \oplus p^kW(B)$$

és így minden k-ra

$$\mathbf{b} \oplus \bigcap_{j\geq k} \big(V_j(B) \oplus p^kW(B)\big) = \mathbf{b}^{(k)} \oplus \bigcap_{j\geq k} \big(V_j(B) \oplus p^kW(B)\big)$$

Belátjuk, hogy $\bigcap_{j\geq k} \big(V_j(B) \oplus p^kW(B)\big) = p^kW(B)$.

Legyen $\mathbf{c} = (\underbrace{0, \ldots, 0}_{k \text{ darab}}, c_k, c_{k+1}, \ldots)$ a metszet egy tetszőleges eleme. Ekkor vannak olyan $a_{j,n} \in B^{p^k}$ elemek ($j \in \mathbb{N}, n \geq k$), hogy

$$\mathbf{c} \in (\underbrace{0, \ldots, 0}_{k \text{ darab}}, a_{j,k}, a_{j,k+1}, \ldots) \oplus V_j(B)$$

A 4.1.14 lemma szerint innen $c_i = a_{j,k} \in B^{p^k}$, ha $k \geq i < j$. Tehát j-t elegendően

nagynak választva kapjuk, hogy minden $i \geq k$-ra $c_i \in B^{p^k}$, azaz $\mathbf{c} \in p^k W(B)$.

Ez azt jelenti, hogy $\mathbf{b} \oplus p^k W(B) = \mathbf{b}^{(k)} \oplus p^k W(B)$ minden $k \geq 1$-re, így a leképezésünk valóban szürjektív. □

4.1.21. Tétel. *Ha a B gyűrű p karakterisztikájú és perfekt, akkor a következők igazak:*

i. Minden $\mathbf{b} = (b_n)_n \in W(B)$-re és $m \geq 1$-re

$$\mathbf{b} \oplus V_m(B) = \tau(b_0) \oplus p\tau(b_1^{p^{-1}}) \oplus \ldots \oplus p^{m-1}\tau(b_{m-1}^{p^{-(m-1)}}) \oplus V_m(B)$$

ii. $V_m(B) = p^m W(B) = V_1(B)^m$ minden $m \geq 0$-ra.

Bizonyítás. i. A 4.1.20 tétel i. része szerint

$$\tau(b_0) \oplus p\tau(b_1^{p^{-1}}) \oplus \ldots \oplus p^{m-1}\tau(b_{m-1}^{p^{-(m-1)}}) \oplus V_m(B) = (b_0, b_1, \ldots, b_{m-1}, 0, 0, \ldots) \oplus V_m(B)$$

így a 4.1.14 lemma szerint készen vagyunk.

ii. A perfektség és 4.1.20 i. szerint F a $W(B)$ gyűrű automorfizmusa. Így

$$p^m W(B) = V^m(F^m(W(B))) = V^m(W(B)) = V_m(B)$$

és így

$$V_1(B)^m = (pW(B))^m = p^m W(B)$$

□

4.1.22. Lemma. *Legyen C egy gyűrű, aminek pontosan egy $\mathfrak{m}$ maximális ideálja van, amire $\bigcap_{i\geq 1} \mathfrak{m}^i = \{0\}$ és $\mathfrak{m} = \pi C$ teljesül (tehát speciálisan főideál). Ekkor minden nem $\{0\}$ ideál C-ben $\pi^k C$ alakú, ahol $k \in \mathbb{N}$.*

Bizonyítás. Egy gyűrű nem egység elemei éppen azok, amik benne vannak valamely maximális ideálban, a mi esetünkben így $C^\times = C \setminus \mathfrak{m}$. Mivel $\bigcap_{i\geq 1} \mathfrak{m}^i = \{0\}$, minden $c \in C \setminus \{0\}$-hez egyértelműen létezik olyan $v(c) \in \mathbb{N}$, hogy $c \in \mathfrak{m}^{v(c)} \setminus \mathfrak{m}^{v(c)+1}$. Ekkor $c = \pi^{v(c)}u$ egy $u \in C$-re. Ekkor $u \notin \pi C = \mathfrak{m}$, így $u \in C^\times$ egység. Legyen $J \neq \{0\}$ egy ideál C-ben. Legyen c J egy olyan eleme, amelyre $k := v(c)$ minimális. Ekkor $J \subseteq \pi^k C$ és másrészt $\pi^k C = cC \subseteq J$. □

4.1.23. Tétel. *Legyen B egy p karakterisztikájú test, ekkor*

i. $W(B)$ egy integritástartomány, amelynek az egyetlen maximális ideálja $V_1(B)$ és $W(B)/W_1(B) \cong B$.

ii. A

$$W(B) \overset{\cong}{\to} \varprojlim_k W(B)/V_1(B)^k$$
$$\mathbf{b} \mapsto (\mathbf{b} \oplus V_1(B)^k)_k$$

gyűrűhomomorfizmus bijektív.

iii. Amennyiben B perfekt is, akkor $W(B)$ egy teljes diszkrét értékelésgyűrű, aminek a maximális ideálja $pW(B)$ és maradékteste B, továbbá minden $\mathbf{b} = (b_n)_n \in \in W(B)$-re

$$\mathbf{b} = \sum_{n=0}^{\infty} p^n \tau(b_n^{p^{-n}})$$

Bizonyítás. iii. A 4.1.20 ii. és iv. része szerint a

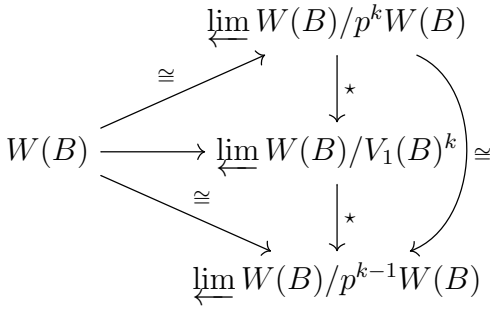

diagram kommutatív, a megjelölt leképezések bijekciók, továbbá a két csillaggal megjelölt leképezés injekció. Ebből azonban következik, hogy a diagramban minden leképezés bijekció.

ii. A 4.1.15 megjegyzés szerint $W(B)/V_1(B) \cong B$. Innen adódik, hogy $V_1(B)$ maximális ideál. Legyen $\mathbf{b} \notin V_1(B)$. Ekkor tudunk találni $\mathbf{a} \in W(B)$-t, amelyre $\mathbf{a} \odot \mathbf{b} = \mathbf{1} + \mathbf{c}$ egy $\mathbf{c} \in V_1(B)$-re. A ii. rész szerint az

$$(\mathbf{1} \oplus \mathbf{c})^{-1} = \sum_{i=0}^{\infty} (-1)^i \mathbf{c}^i$$

összeg létezik, így $\mathbf{b}$ egység $W(B)$-ben. Ez azt jelenti, hogy $V_1(B)$ az egyetlen maximális ideál $W(B)$-ben. $\odot$ definíciójából könnyen átgondolható, hogy ha $\mathbf{a} \odot \mathbf{b} = 0$, akkor $\mathbf{a}$ vagy $\mathbf{b}$ is nulla volt, így $W(B)$ integritástartomány.

iv. A 4.1.21 tétel ii. része miatt $V_1(B) = W(B)$. i., 4.1.20 iv. és 4.1.21 i. szerint elegendő azt belátni, hogy $p\mathbf{1} \neq \mathbf{0}$ és hogy $W(B)$-ben minden ideál főideál. 4.1.20 i. szerint

$$p\mathbf{1} = (0, 1, 0, 0, \ldots) \neq \mathbf{0}$$

Továbbá 4.1.20 iv. szerint $\bigcap k \geq 1 p^k W(B) = \{\mathbf{0}\}$, így a 4.1.22 lemma szerint készen vagyunk.

□

4.1.24. Megjegyzés. *Ha B egy p karakterisztikájú test, akkor $W(B)$ hányadosteste 0 karakterisztikájú.*

Bizonyítás. Tegyük fel, hogy a q prímszámra $qW(B) = \{0\}$. Mivel $B = W(B)/V_1(B)$, innen $qB = \{0\}$, azaz $q = p$. Viszont $p\mathbf{1} = (0, 1, 0, 0, \ldots) \neq \mathbf{0}$. □

A továbbiakban a $W(B)$-n lévő összeadást és szorzást $\oplus$ és $\odot$ helyett a szokásos $+$ és $\cdot$ jelöli.

4.2. $W(k)$ egyértelműsége

Szükségünk lesz két korábbi lemmának a kicsit általánosabb alakjára:

4.2.1. Lemma. *Legyen B tetszőleges gyűrű és $\mathfrak{a} \triangleleft B$ egy tetszőleges $p1_B$-t tartalmazó ideál, ekkor*

i. Minden $m, n \geq 1$ és $a, b \in B$-re

$$a \equiv b \mod \mathfrak{a}^m \Rightarrow a^{p^n} \equiv a^{p^m} \mod \mathfrak{a}^{m+n}$$

ii. Ha $m \geq 1$, $n \geq 0$ és $a_0, \ldots, a_n, b_0, \ldots, b_n \in B$, akkor

$$(\forall 0 \leq i \leq n : a_i \equiv b_i \mod \mathfrak{a}^m) \Rightarrow \Phi_n(a_0, \ldots, a_n) \equiv \Phi_n(b_0, \ldots, b_n) \mod \mathfrak{a}^{m+n}$$

Bizonyítás. Mivel $p1_B \in \mathfrak{a}$, ezen lemmák a 4.1.1 és 4.1.2 lemmákhoz teljesen hasonlóan láthatóak be. □

Legyen k egy perfekt test $p > 0$ karakterisztikával, A egy teljes diszkrét értékelésgyűrű és $\alpha : A \to k$ egy szürjektív gyűrűhomomorfizmus. Legyen $\mathfrak{m} \triangleleft A$ a főideál, ekkor α indukál egy $\bar{\alpha} : A/\mathfrak{m} \to k$ izomorfizmust.

4.2.2. Tétel. *Létezik pontosan egy $s : k \to A$ multiplikatív leképezés amelyre $\alpha \circ \circ s = \mathrm{id}_k$, erre $s(0) = 0$ és $s(1) = 1$*

Bizonyítás. Az egyértelműség onnan következik, hogy ha $\tilde{s}$ egy másik jó leképezés lenne, akkor $x \in k$-ra és $i \in \mathbb{N}$-re $s(x^{p^{-i}}) \equiv \tilde{s}(x^{p^{-i}}) \mod \mathfrak{m}$ lenne, de így 4.2.1 i. szerint $s(x) = s\left((x^{p^{-i}})^{p^i}\right) \equiv s\left((x^{p^{-i}})^{p^i}\right) = \tilde{s}(x) \mod \mathfrak{m}^{i+1}$, és innen $\bigcap_i \mathfrak{m}^i = \{0\}$ miatt következik az egyértelműség.

A létezéshez legyen $x \in k$ tetszőleges. k perfektsége szerint találhatunk olyan $a_1, a_2, \ldots, a_i, \ldots \in A$ sorozatot, amelyre $\alpha(a_1)^p = x$ és $\alpha(a_{i+1})^p = \alpha(a_i)$ minden $i \geq 1$-re. Ekkor minden $i \geq 1$-re

$$a_{i+1}^p \equiv a_i \mod \mathfrak{m} \overset{4.2.1}{\Rightarrow} a_{i+1}^{p^{i+1}} \equiv a_i^{p^i} \mod \mathfrak{m}^{i+1}$$

Ez azt jelenti, hogy $a_i^{p^i}$ egy Cauchy-sorozat, így konvergál egy $s(x) \in A$-hoz. Mivel $\alpha(a_i^{p^i}) = x$, így $\alpha(s(x)) = x$. Az, hogy $s(x)$ nem függ az a_i sorozat választásától, onnan következik, hogy ha $(\tilde{a}_i)_i$ egy másik ilyen sorozat lenne, akkor $\alpha(a_i)^{p^i} = x = \alpha(\tilde{a}_i)^{p^i}$, így $\alpha(a_i) = \alpha(\tilde{a}_i)$, $a_i \equiv \tilde{a}_i \mod \mathfrak{m}$, 4.2.1 i. miatt $a_i^{p^i} \equiv \tilde{a}_i^{p^i} \mod \mathfrak{m}^{i+1}$, és ez azt jelenti, hogy a két sorozat ($a_i^{p^i}$ és $\tilde{a}_i^{p^i}$) határértéke megegyezik. Az, hogy s multiplikatív, $s(0) = 0$ és $s(1) = 1$, könnyen látható alkalmas a_i-k választása mellett. □

4.2.3. Megjegyzés. *Ha $A = W(k)$ és $\alpha = \Phi_0$, akkor $s = \tau$.*

4.2.4. Tétel. *Egyértelműen létezik egy $\gamma : W(k) \to A$ gyűrűhomomorfizmus, amire $\alpha \circ \gamma = \Phi_0$. Ez folytonos és minden $(x_n)_n \in W(k)$-ra*

$$\gamma((x_n)_n) = \sum_{n=0}^{\infty} p^n s(x_n^{p^{-n}}) \tag{11}$$

Ha $p1_A \neq 0$, akkor γ injektív.

Bizonyítás. Először γ létezését látjuk be. A $W(\alpha) : W(k) \to W(A)$ gyűrűhomomorfizmus szürjektív. Legyen $(b_n)_n \in \ker W(\alpha)$, ekkor $b_n \in \mathfrak{m}$ minden $n \geq 0$-ra. Így

$$\begin{aligned}
\Phi_m(b_0, \ldots, b_m) &= b_0^{p^m} + pb_1^{p^{m-1}} + \ldots + p^m b_m \\
&\in \mathfrak{m}^{p^m} + p \cdot \mathfrak{m}^{p^{m-1}} + \ldots + p^m \mathfrak{m} \\
&\subseteq \mathfrak{m}^{m+1} + p\mathfrak{m}^m + \ldots + p^m \mathfrak{m} \\
&\subseteq \mathfrak{m}^{m+1}
\end{aligned}$$

minden $m \geq 0$-ra. Így létezik egy jóldefiniált $\gamma_m : W(k) \to A/\mathfrak{m}^{m+1}$ gyűrűhomomorfizmus, amelyre a

$$\begin{array}{ccc}
W(A) & \xrightarrow{\Phi_m} & A \\
\downarrow{\scriptstyle W(\alpha)} & & \downarrow{\scriptstyle pr} \\
W(k) & \xrightarrow{\gamma_m} & A/\mathfrak{m}^{m+1}
\end{array}$$

diagram kommutatív. (9) szerint $\Phi_m \circ F = \Phi_{m+1}$ és $\gamma_m \circ F \circ W(\alpha) = \gamma_m \circ W(\alpha) \circ F = \gamma_{m+1} \circ F \mod \mathfrak{m}^{m+1}$ és így $W(\alpha)$ szürjektivitásából $\gamma_m \circ F \equiv \gamma_{m+1} \mod \mathfrak{m}^{m+1}$.

A 4.1.20 tétel i.része szerint a $W(k)$ feletti F leképezés bijetív. Ebből és az előző kongruenciából következik, hogy a

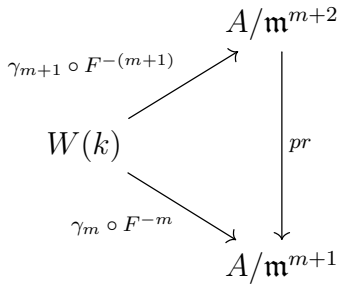

diagram kommutatív. Ez azt jelenti, hogy projektív limeszt véve kaphatunk egy

$$\gamma := \varprojlim(\gamma_m \circ F^{-m}) : W(k) \to \varprojlim(A/\mathfrak{m}^{m+1}) = A$$

gyűrűhomomorfizmust.

Ekkor

$$\alpha \circ \gamma \circ W(\alpha) = \bar{\alpha} \circ \gamma_0 \circ W(\alpha) = \alpha \circ \Phi_0 = \Phi_0 \circ W(\alpha)$$

és így $\alpha \circ \gamma = \Phi_0$.

Az egyérteműség és a többi tulajdonság belátásához legyen $\tilde{\gamma} : W(k) \to A$ tetszőleges gyűrűhomomorfizmus, amire $\alpha \circ \tilde{\gamma} = \Phi_0$. Ebből az összefüggésből következik, hogy $\tilde{\gamma}(pW(k)) \subseteq \mathfrak{m}$ és így $\tilde{\gamma}(p^i W(k)) \subseteq \mathfrak{m}^i$ minden $i \geq 1$-re. Így $\tilde{\gamma}$ folytonos. A 4.1.21 tétel iii. része szerint

$$\tilde{\gamma}((x_n)_n) = \sum_{n=0}^{\infty} p^n \tilde{\gamma}(\tau(x_n^{p^{-n}}))$$

4.2.2 egyértelműségi része szerint $\tilde{\gamma} \circ \tau = s$. De ez azt jelenti, hogy $\tilde{\gamma} = \gamma$ és minden $(x_n)_n \in W(k)$-ra

$$\gamma((x_n)_n) = \sum_{n=0}^{\infty} p^n s(x_n^{p^{-n}})$$

Tegyük fel, hogy $p1_A \neq 0$. $\gamma((x_n)_n) = 0$-ból 3.2.11 szerint következik, hogy $s(x_n^{p^{-n}}) = 0$ és így $x_n = 0$ minden $n \geq 0$-ra. Így $p1_A \neq 0$ esetén γ valóban injektív. □

4.2.5. Következmény. *Ha pA a maximális ideál A-ban, akkor létezik pontosan egy $\gamma : W(k) \overset{\cong}{\to} A$ gyűrűizomorfizmus, amire $\alpha \circ \gamma = \Phi_0$.*

Bizonyítás. Az előző tétel által biztosított γ injektív. Mivel $\mathfrak{m} = pA$, így az (11) egyenletben szereplő hatványsoralak éppen olyan, amilyet a 3.2.11 lemma minden A-beli elemnek garantál, de ez azt jelenti, hogy γ szürjektív is. □

4.2.6. Megjegyzés. $W(\mathbb{F}_p) \cong \mathbb{Z}_p$.

4.3. Cohen-részgyűrűk

Legyen k egy tetszőleges $p > 0$ karakterisztikájú test. Ekkor $k^{p^n} = \{x^{p^n} | x \in k\}$ egy részteste k-nak minden $n \in \mathbb{N}$-re. Azt mondjuk, hogy k elemeinek egy $(x_i)_{i\in I}$ rendszere k egy p-bázisát alkotja, ha a

$$k^p[\{X_i | i \in I\}]/\langle X_i^p - x_i^p | i \in I\rangle \to k$$
$$X_i \mapsto x_i$$

gyűrűhomomorfizmus bijektív. Bizonyítás nélkül megjegyezzük, hogy k-nak létezik p-bázisa.

4.3.1. Lemma. *k-nak minden $(x_i)_{i\in I}$ p-bázisára és minden $n \geq 1$-re*

i. $k = k^{p^n}(\{x_i | i \in I\})$

ii. *k-nak mint k^{p^n} feletti vektortérnek bázisát alkotják a $\prod_{i\in I} x_i^{\mu_i}$ alakú elemek, ahol $0 \leq \mu_i < p^n$ és véges sok i kivételével $\mu_i = 0$.*

Bizonyítás. ii.-ből i. triviálisan következik, elég ii.-t bizonyítani. n szerinti teljes indukciót alkalmazunk.

Az $n = 1$ esethez vegyük észre $k^p[\{X_i | i \in I\}]/\langle X_i^p - x_i^p | i \in I\rangle$ (mint k^p feletti vektortér) egy bázisát alkotják a $\prod_{i\in I} X_i^{\mu_i}$ alakú elemek, ahol $0 \leq \mu_i < p$ és véges sok i kivételével $\mu_i = 0$, hiszen $k^p[\{X_i | i \in I\}]$-nek bázisát alkotják a $\prod_{i\in I} X_i^{\mu_i}$ alakú szorzatok, ahol $\mu_i \in \mathbb{N}$ és véges sok kivételével minden $\mu_i = 0$. A p-bázisok definíciójában szereplő leképezés egy k^p-vektorterek közötti izomorfizmus, ami ezt a bázist éppen az ii. állításban szereplő rendszerbe viszi, de így $n = 1$-re ii. teljesül.

Tegyük fel, hogy $n \geq 1$-re igazoltuk az állításunkat. $(x_i^p)_{i\in I}$ p-bázisa a k^p testnek, hiszen $x \mapsto x^p$ bijekció k és k^p között. Így az indukciós feltevést k^p-re alkalmazva k^p-nek mint k^{p^n} feletti vektortérnek bázisát alkotják a $\prod_{i\in I} x_i^{p\mu_i}$ elemek, ahol $0 \leq$ $\leq \mu_i < p^{n-1}$ és véges sok i kivételével $\mu_i = 0$. k-nak az elemeit az $n = 1$ eset által biztosított k^p feletti bázis eleminek lineáris kombinációiként felírva innen könnyen láthatóan éppen az adódik, hogy ii. igaz $n + 1$-re is. □

4.3.2. Definíció. *Egy $C < W(k)$ részgyűrű Cohen-részgyűrű, ha C teljes diszkrét értékelésgyűrű pC maximális ideállal és $W(k) = V_1(k) + C$.*

Mivel $C/V_1(k) \cap C \cong W(k)/V_1(k) \cong k$, így $V_1(k) \cap C = pC$ és C maradékteste is k.

4.3.3. Tétel. *Legyen $(\mathbf{a}_i)_{i\in I}$ $W(k)$-beli elemek rendszere, amire az $x_i := \Phi_0(\mathbf{a}_i)$ elemek k p-bázisát alkotják, ekkor egyértelműen létezik egy $C < W(k)$ Cohen-részgyűrű, ami minden $\mathbf{a}_i$-t tartalmaz.*

Bizonyítás. Az áttekinthetőség érdekében legyen $A := W(k)$, $\mathfrak{m} := V_1(k)$ és $pr := \Phi(0) : A \to k$. Legyen továbbá $S := \{\mathbf{a}_i | i \in I\} \subseteq A$. Rögzítsünk egy $m \geq 1$-et. Minden $n \geq m-1$-re legyen

$$C_{n,m} := \langle S \cup \Phi_n(W(A)) \cup \mathfrak{m}^m \rangle < A$$

1. lépés: $C_{n,m}$ a legszűkebb olyan $S \cup \mathfrak{m}^m$-et tartalmazó részgyűrűje A-nak, amire $C_{n,m} + \mathfrak{m} = A$.

Mivel $\Phi_n(W(A)) = \{a_0^{p^n} + pa_1^{p^{n-1}} \ldots + p^n a_n | a_0, \ldots, a_n \in A\}$, így $pA \subseteq \mathfrak{m}$-et figyelembe véve $pr(\Phi_n(W(A))) = k^{p^n}$ és $pr(C_{n,m}) = k^{p^n}(pr(S))$. A 4.3.1 lemmából következik, hogy $pr(C_{n,m}) = k$ és így $C_{n,m} + \mathfrak{m} = A$ teljesülni fog. Legyen $A' < A$ egy részgyűrű, amire $A' + \mathfrak{m} = A$ és $S \cup \mathfrak{m} \subseteq A'$. Elegendő belátnunk, hogy $\Phi_n(W(A)) \subseteq \subseteq A'$. Legyenek $a_0, \ldots, a_n \in A$ tetszőleges elemek. $A' + \mathfrak{m} = A$ miatt léteznek olyan $a_0', \ldots, a_n' \in A'$ elemek, hogy $a_i \equiv a_i' \mod \mathfrak{m}$ minden $0 \leq i \leq n$-re. Mivel $n \geq \geq m-1$, így a 4.2.1 lemma szerint $\Phi_n(a_0, \ldots, a_n) = \Phi_n(a_0', \ldots, a_n') \mod \mathfrak{m}^m$. Mivel $\Phi_n(a_0', \ldots, a_n')$ és $\mathfrak{m}^m$ is A'-ben van, így ezek szerint $\Phi_n(a_0, \ldots, a_n)$ is A'-ben van.

Ezzel az 1. lépés bizonyítását befejeztük; vegyük észre, hogy innen következik, hogy $C_m := C_{n,m}$ nem függ n választásától.

2. lépés: $C_m \cap \mathfrak{m} = pC_m + \mathfrak{m}^m$.

$pA \subseteq \mathfrak{m}$ miatt $C_m \cap \mathfrak{m} \supseteq pC_m + \mathfrak{m}^m$. A másik irányú tartalmazás belátásához legyen $\Lambda(m)$ az összes olyan $(\mu_i)_{i\in I}$ rendszer halmaza, ahol $0 \leq \mu_i < p^m$ és véges sok i kivételével $\mu_i = 0$. $\mu \in \Lambda(m)$-re legyen

$$Z_\mu = \prod_{i\in I} \mathbf{a}_i^{\mu_i}$$

Mivel $S^{p^m} = \{\Phi_m(\mathbf{a}_i, 0, 0, \ldots) | i \in I\} \subseteq \Phi_m(W(A))$, így $C_m = C_{m,m}$-et mint a $\Phi_m(W(A)) + \mathfrak{m}^m < C_m$ részgyűrű feletti modulust a Z_μ-k generálják. Mivel $\Phi_m(a_0, \ldots, a_m) = a_0^{p^m} + p\Phi_{m-1}(a_1, \ldots, a_m)$, így $\Phi_m(W(A)) \subseteq A^{p^m} + pC_{m-1,m} = = A^{p^m} + pC_m$. Ezek miatt minden $c \in C_m$ írható olyan alakban, hogy

$$c = \left(\sum_{\mu\in\Lambda(m)} c_\mu^{p^m} Z_\mu \right) + pc' + c'' \quad \text{, ahol } c_\mu \in A, c' \in C_m \text{ és } c'' \in \mathfrak{m}^m$$

Ezért ha $c \in C_m \cap \mathfrak{m}$, akkor

$$0 = pr(c) = \sum_{\mu \in \Lambda(m)} pr(c_\mu)^{p^m} pr(Z_\mu)$$

A 4.3.1 lemma szerint a $pr(Z_\mu)$-k bázisát alkotják k-nak k^{p^m} felett, így minden $pr(c_\mu)$-nek nullának kell lennie, így $c_\mu \in \mathfrak{m}$, $c_\mu^m \in \mathfrak{m}^m$. Tehát $c \in pC_m + \mathfrak{m}^m$. Ezzel a 2. lépés bizonyítását is befejeztük.

C_m minimalitásából következik, hogy minden $m \geq 1$-re

$$C_m = C_{m+1} + \mathfrak{m}^m \tag{12}$$

Legyen

$$C := \bigcap_{m \geq 1} C_m$$

Nyilván ez a C tartalmazza S elemeit. Az $(A/\mathfrak{m}^m)_m$ projektív rendszert alkotó gyűrűknek részgyűrűi a $(C_m/\mathfrak{m}^m)_m$ projektív rendszer megfelelő tagjai. A 4.1.23 tétel ii. része szerint a

$$\begin{array}{ccc} A & \xrightarrow{\cong} & \varprojlim A/\mathfrak{m}^m \\ \subseteq \uparrow & & \uparrow \subseteq \\ C & \xrightarrow{\cong} & \varprojlim C_m/\mathfrak{m}^m \end{array}$$

kommutatív diagramban a vízszintes nyilak izomorfizmusok. (12) szerint a $C_{m+1}/\mathfrak{m}^{m+1} \to C_m/\mathfrak{m}^m$ beágyazások és így a $C \to C_m/\mathfrak{m}^m$ projekciók is szürjektívek. Emiatt létezik

$$C/C \cap \mathfrak{m} \xrightarrow{\cong} C_1/\mathfrak{m} = A/\mathfrak{m} \xrightarrow{\cong} k$$

izomorfizmus, így $C \cap \mathfrak{m}$ maximális ideál C-ben. A 4.1.23 i. rész bizonyításához teljesen hasonlóan (mértani sor konvergenciáját felhasználva) beláthatjuk, hogy $C \setminus \setminus C \cap \mathfrak{m}$ minden eleme egység C-ben, így $C \cap \mathfrak{m}$ az egyetlen maximális ideál C-ben. A második lépés szerint

$$C \cap \mathfrak{m} = \bigcap_{m \geq 1} C_m \cap \mathfrak{m} = \bigcap_{m \geq 1} (pC_m + \mathfrak{m}^m) = \bigcap_{m \geq 1} \bigcap_{j \geq m} \left(pC_m + \mathfrak{m}^j\right)$$

$$\bigcap_{j \geq m} \left(pC_m + \mathfrak{m}^j\right) \subseteq \bigcap_{j \geq m} (pW(k) + V_j(k)) = pW(k)$$

hiszen ezt az egyenlőséget már beláttuk a 4.1.20 tétel bizonyítása közben. Így legyen $p\mathbf{c} \in \bigcap_{j \geq m} (pC_m + \mathfrak{m}^j)$ tetszőleges elem, ekkor $\mathbf{c} \in p\mathbf{c}^{(j)} + \mathfrak{m}^j$ valamely $\mathbf{c}^{(j)} \in C$-re. 4.1.20 iii. szerint $p(\mathbf{c} - \mathbf{c}^{(m+2)}) \in \mathfrak{m}^{m+2} \subseteq p^{m+1}W(k)$. $W(k)$ 4.1.23 i. szerint integritástartomány, így $\mathbf{c} - \mathbf{c}^{(m+2)} \in p^m W(k) \subseteq \mathfrak{m}^m$. Így $\mathbf{c} \in C_m + \mathfrak{m}^m = C_m$. Ez

azt jelenti, hogy

$$\bigcap_{j\geq m} \left(pC_m + \mathfrak{m}^j\right) = pC_m$$

és

$$C \cap \mathfrak{m} = \bigcap_{m\geq 1} pC_m = p\left(\bigcap_{m\geq 1} C_m\right) = pC$$

(itt a középső egyenlőség azért igaz, mert A integritástartomány). Természetesen C is integritástartomány lesz és $p1_C = p\mathbf{1} \neq 0$. Továbbá $\bigcap_{m\geq 1} p^m C \subseteq \bigcap_{m\geq 1} \mathfrak{m}^m = \{0\}$ a 4.1.23 tétel ii. része szerint. Így a 4.1.22 lemma szerint C egy diszkrét értékelésgyűrű (pC maximális ideállal és k maradéktesttel).

Tudjuk, hogy

$$C \cong \varprojlim C/C \cap \mathfrak{m}^m \cong \varprojlim C_m/\mathfrak{m}^m$$

Mivel minden nem $\{0\}$ ideál C-ben $p^j C$ alakú, így minden $m \geq 1$-hez létezik $j(m) \geq 1$, hogy $C \cap \mathfrak{m}^m = p^{j(m)}C$. $\bigcap_{m\geq 1} C \cap \mathfrak{m}^m = \{0\}$ miatt $\lim_{m\to\infty} j(m) = \infty$. Emiatt

$$C \cong \varprojlim_m C/p^{j(m)}C \cong \varprojlim_j C/p^j C$$

és így C teljes. Az egyértelműség belátásához legyen C' egy másik Cohen-részgyűrű, amire $S \subseteq C'$. Mivel $C' + \mathfrak{m} = A$, így $C' \cap \mathfrak{m} = pC'$ a maximális idál C'-ben. Így minden $m \geq 1$-re létezik $j(m) \geq m$, hogy $C' \cap \mathfrak{m}^m = p^{j(m)}C'$. Másfelől az bizonyításunk 1. lépése szerint $C' + \mathfrak{m}^m \supseteq C_m$ minden $m \geq 1$-re. A

$$\begin{array}{ccccc}
C' & \xrightarrow{\cong} & \varprojlim C'/p^{j(m)}C' & \xrightarrow{=} & \varprojlim C'/C' \cap \mathfrak{m}^m \\
 & & & & \downarrow \cong \\
\subseteq\uparrow & & & & \varprojlim C' + \mathfrak{m}^m/\mathfrak{m}^m \\
 & & & & \subseteq\uparrow \\
C & & \xrightarrow{\qquad\cong\qquad} & & \varprojlim C_m/\mathfrak{m}^m
\end{array}$$

kommutatív diagramról leolvasható, hogy $C \subseteq C'$. Azonban $p\mathbf{1}$ C'-ben és C-ben is prímelem. A

$$\begin{array}{ccc}
C'/pC' & & \\
\uparrow & \searrow^{\cong} & \\
\subseteq & & A/\mathfrak{m} \\
 & \nearrow_{\cong} & \\
C/pC & &
\end{array}$$

diagram kommutatív, ahol a függőleges nyíl a $C \subseteq C'$ beágyazás által indukált $C/pC \subseteq C'/pC'$ injekció. Mivel a másik két leképezés izomorfizmus, így ez az injektív leképezés is bijektív lesz. Ekkor azonban a 3.2.11 lemma szerint kapjuk, hogy $C = C'$. □

5. A Dieudonné–Manin tétel

5.1. Izokristályok és rácsok

Legyen A egy diszkrét értékelésgyűrű $\mathfrak{m} = \pi A$ maximális ideállal és K hányadostesttel. Rögzítjük A-nak egy σ gyűrűautomorfizmusát. σ-nak a K-ra való multiplikatív kiterjesztése testautomorfizmus lesz, ezt szintén σ-val jelöljük.

Példa: $A := W(k)$ egy k perfekt $p > 0$ karakterisztikájú testre és $\sigma := F$ (ez 4.1.21 i. szerint automorfizmus).

5.1.1. Definíció. *Legyen $a \in \mathbb{Z}$. Egy σ^a-izokristály egy (V, f) pár, ahol $V \neq \{0\}$ egy véges dimenziós K-vektortér és $f : V \to V$ egy bijektív σ^a-lineáris leképezés. A*

$$h(V, f) := \dim_K V$$

számot (V, f) magasságának nevezzük.

Az $a = 1$ esetben egyszerűen izokristályról beszélünk. Legyen (V, f) egy izokristály.

5.1.2. Definíció. *Egy $M < V$ A-részmodulus V-ben egy rács, ha létezik V-nek egy $v_1, v_2, \ldots, v_h$ K-bázisa, amelyre $M = Av_1 + \ldots + Av_h$. Ekkor M egy h rangú szabad A-modulus.*

5.1.3. Lemma. *Ha M, M' rácsok V-ben*

i. Minden $v \in V$-hez létezik $n \geq 0$ egész, hogy $\pi^n v \in M$.

ii. Létezik $n \geq 0$, hogy $\pi^n M \subseteq M'$.

iii. $M \cap M'$ egy rács V-ben.

iv. $f(M)$ egy rács V-ben.

Bizonyítás. i. Ez triviálisan teljesül.

ii. M-hez van a rács definíciójában szereplő tulajdonságú $v_1, v_2, \ldots, v_h$, i. szerint léteznek olyan n_i-k, hogy $\pi^{n_i} v_i \in M'$. Ekkor $n := \max_{1 \leq i \leq h} n_i$ könnyen láthatóan megfelelő lesz.

iii. Mivel végesen generált szabad modulus minden részmodulusa is szabad, így $M \cap M'$-t szabadon generálja egy $u_1, u_2, \ldots, u_r \in V$ rendszer valamely $0 \leq$ $\leq r$-re. $r \leq h$, hiszen különben az u_i-knek egy nemtriviális K-beli együtthatós lineáris kombinációja 0 lenne, de az együtthatókat π egy hatványával felszorozva

kapnánk egy 0 értékű nemtriviális A-beli együtthatós lineáris kombinációt, ami ellentmond annak, hogy az u_i-k szabad generátprrendszert alkotnak.

Ha $v \in V$ tetszőleges, akkor i. szerint van olyan $n, n' \geq 0$, hogy $\pi^n v \in M$, $\pi^{n'} v \in M'$, ekkor $\pi^{\max(n,n')} v \in M \cap M'$, de így $\pi^{\max(n,n')} v$ és így v is benne van az $u_1, \ldots, u_r$ által generált K-vektortérben. Így $u_1, u_2, \ldots, u_r$ V-nek egy generátorrendszere, speciálisan $r = h$, és ez éppen azt jelenti, hogy $M \cap M'$ rács.

iv. Legyen $M = Av_1 + \ldots + Av_h$. Ekkor $f(M) = \sigma^a(A)f(v_1) + \ldots + \sigma^a(A)f(v_h) = = Af(v_1) + \ldots + Af(v_h)$. Az, hogy $f(v_1), \ldots, f(v_h)$ K-bázisa V-nek következik a 2.1.5 lemmából.

□

Mivel πA az egyetlen maximális ideál A-ban, így $A/\pi A$ izomorfizmus erejéig az egyetlen egyszerű A-modulus. Nyilván minden $n \geq 1$-re az $A/\pi^n A$ A-modulus hossza n. Minden M rácsra V-ben $M/\pi^n M = \bigoplus_{i=1}^{h} A/\pi^n A$ egy hn hosszú A-modulus. Az 5.1.3 szerint így ha M, M' rácsok V-ben, $M/M \cap M'$ egy véges hosszú A-modulus lesz. Legyen

$$[M : M'] := \operatorname{length}_A M/M \cap M' - \operatorname{length}_A M'/M \cap M'$$

(itt length_A egy A-modulushoz a hosszát rendeli).

5.1.4. Lemma. *Ha M, M' és M'' rácsok V-ben, akkor*

$$[M : M''] = [M : M'] + [M' : M'']$$

Bizonyítás. Tudjuk hogy $X \leq Y \leq Z$ A-modulusokra $\operatorname{length}_A Z/X = \operatorname{length}_A Z/Y + + \operatorname{length}_A Y/X$ (és ha az egyik oldalon szerepel ∞, akkor mindkét oldalon szerepel; ez a modulusokra vonatkozó Jordan-Hölder tétel speciális esete). Ezt alkalmazva az összes olyan bővítésláncra, ahol Z M, M' és M'' egyike, Y Z-nek a metszete M, M' és M'' közül a másik kettő valamelyikével és $X = M \cap M' \cap M''$, a kapott összefüggésekből könnyen láthatóan következik a bizonyítandó. □

5.1.5. Lemma. *Az $[M : f(M)]$ nem függ az M rács választásától.*

Bizonyítás. Legyen M' egy másik rács V-ben. Ekkor

$$[M' : f(M')] = [M' : M] + [M : f(M)] + [f(M) : f(M')]$$

de itt $[f(M) : f(M')] = [M : M'] = -[M' : M]$. □

5.1.6. Definíció. *A $d(V, f) := [M : f(M)]$ számot (ahol M tetszőleges rács V-ben) a (V, f) izokristály dimenziójának nevezzük.*

A továbbiakban legyen a rövidség kedvéért $h := h(V,f)$ és $d := d(V,f)$. Egy V-beli M rácsra legyen $\operatorname{ord}_M f = \max\{n \in \mathbb{Z} : f(M) \subseteq \pi^n M\}$ (ez 5.1.3 miatt véges).

5.1.7. Lemma. *Legyen M egy tetszőleges rács V-ben, ekkor*

i. Minden m pozitív egészre $\operatorname{ord}_M f \leq \frac{1}{m} \operatorname{ord}_M f^m \leq \frac{d}{h}$.

ii. Ha van olyan m pozitív egész, hogy $\operatorname{ord}_M f \neq \frac{1}{m} \operatorname{ord}_M f^m$, *akkor* $\operatorname{ord}_M f + \frac{1}{h} \leq$ $\leq \frac{1}{h} \operatorname{ord}_M f^h$

Bizonyítás. $f(M) \subseteq \pi^n M$-ből $f^m(M) \subseteq f^{m-1}(\pi^n \cdot M) = f^{m-1}((\sigma^{-(m-1)}(\pi))^n \cdot M) =$ $= \pi^n f^{m-1}(M)$ és így indukcióval következik, hogy $f^m(M) \subseteq \pi^{mn} M$.

Innen $m \cdot \operatorname{ord}_M(f) \leq \operatorname{ord}_M(f^m)$. Tegyük fel, hogy $f^m(M) \subseteq \pi^n M$. Ekkor

$$\begin{aligned} md &= m[M : f(M)] = [M : f^m(M)] \\ &= [M : \pi^n M] + [\pi^n M : f^m(M)] \geq [M : \pi^n M] = nh \end{aligned}$$

és így $\operatorname{ord}_M f^m \leq m \cdot \frac{d}{h}$.

Legyen $n = \operatorname{ord}_M f$ és tegyük fel, hogy $f^m(M) \subseteq \pi^{mn+1} M$ egy m pozitív egészre. Minden $i \geq 0$-ra legyen $M_i := \{v \in M | f^i(v) \in \pi^{in+1} M\}$. $f(M) \subseteq \pi^n M$-ből következik, hogy

$$\pi M = M_0 \leq M_1 \leq \ldots \leq M_m = M$$

5.1.3 iii. részéhez hasonlóan belátható, hogy minden M_i rács V-ben. Mivel $h = [M : \pi M] = [M_1 : M_0] + [M_2 : M_1] + \ldots + [M_m : M_{m-1}]$, így ezen rácssorozatban legfeljebb h hely kivételével mindenütt egyenlőségek állnak fenn.

Belátjuk, hogy $M_i = M_{i+1}$-ből következik $M_i = M_j$ minden $j \geq i$-re.

Legyen $v \in M_j$, ekkor $v \in M$ és $f^j(v) \in \pi^{jn+1} M$. Ekkor $f^{j-(i+1)}(v) = \pi^{(j-(i+1))n} v'$ egy $v' \in M$-re. Tehát $\pi^{(j-(i+1))n} f^{i+1}(v') \in A^\times \cdot f^j v \subseteq \pi^{jn+1} M$ és így $f^{i+1}(v') \in$ $\in \pi^{(i+1)n+1} M$, $v' \in M_{i+1}$. $M_i = M_{i+1}$-ből következik, hogy $f^i(v') \in \pi^{in+1} M$. és így $f^{j-1}(v) = f^i(f^{j-(i+1)}(v)) = \sigma^{-(j-(i+1)n)}(\pi) \cdot f^i(v') \in \pi^{(j-1)n+1}$, $v \in M_{j-1}$ és innen indukcióval haladva lefelé $M_j = M_i$.

Ebből következik, hogy $M_h = M$, így $f^h(M) \subseteq \pi^{hn+1} M$, azaz $\operatorname{ord}_m f^h \geq$ $\geq h \cdot \operatorname{ord}_M f + 1$. □

5.1.8. Definíció. *A (V,f) izokristály első meredeksége*

$$\operatorname{Newton}(V,f) := \sup \left\{ \frac{1}{m} \operatorname{ord}_M f^m | m \text{ pozitív egész, } M \text{ rács } V\text{-ben} \right\}$$

5.1.7 i. szerint $\operatorname{Newton}(V,f) \leq \frac{d}{h}$.

5.1.9. Lemma. *Tetszőleges V-beli M rácsra*

$$\mathrm{Newton}(V,f) = \lim_{m\to\infty} \frac{1}{m}\,\mathrm{ord}_M(f^m)$$

Bizonyítás. Legyen M' egy tetszőleges másik rács V-ben. Ekkor az 5.1.3 lemma ii. része szerint létezik $n, n' > 0$, hogy $\pi^n M \subseteq M'$ és $\pi^{n'} M' \subseteq M$. Ekkor

$$f(M) \subseteq \pi^{-n} f(M') \subseteq \pi^{\mathrm{ord}_{M'} f - n} M' \subseteq \pi^{\mathrm{ord}_{M'} f - n - n'} M$$

És így $\mathrm{ord}_M f \geq \mathrm{ord}_{M'} f - n - n'$. Minden $i \geq 1$-re

$$\begin{aligned}
\sup_m \frac{1}{m}\,\mathrm{ord}_M f^m &\geq \sup_j \frac{1}{ij}\,\mathrm{ord}_M f^{ij} \\
&\geq \sup_j \frac{1}{ij}(\mathrm{ord}_{M'} f^{ij} - n - n') \\
&\geq \sup_j \left(\frac{1}{i}\,\mathrm{ord}_{M'} f^i - \frac{n+n'}{ij}\right) \\
&= \frac{1}{i}\,\mathrm{ord}_{M'} f^i
\end{aligned}$$

az utolsó előtti lépésben 5.1.7 i.-t használva. Ezzel beláttuk, hogy $\lambda := \sup_m \frac{1}{m}\,\mathrm{ord}_M f^m = \mathrm{Newton}(V,f)$.

Legyen $\varepsilon > 0$. Rögzítsünk egy olyan m_0 pozitív egészt, amire

$$\mathrm{ord}_M f^{m_0} \geq m_0 \left(\lambda - \frac{\varepsilon}{2}\right)$$

Minden $r \geq 1$ és $0 \leq s < m_0$ egészre

$$\mathrm{ord}_M f^{m_0 r + s} \geq m_0 r \left(\lambda - \frac{\varepsilon}{2}\right) + s \cdot \mathrm{ord}_M f$$

Válasszunk egy olyan r_0 pozitív egészt, hogy

$$\mathrm{ord}_M f - \left(\lambda - \frac{\varepsilon}{2}\right) > -\frac{\varepsilon}{2}(r_0 + 1)$$

innen minden $r \geq r_0$ és $0 \leq s < m_0$-ra

$$\frac{s\left(\mathrm{ord}_M f - \left(\lambda - \frac{\varepsilon}{2}\right)\right)}{m_0 r + s} \geq -\frac{\varepsilon}{2}$$

Minden $m \geq m_0 r_0$ írható $m = m_0 r + s$ alakban, ahol $r \geq r_0$ és $0 \leq s < m_0$. Így

$m \geq m_0 r_0$-ra

$$\begin{aligned}\lambda \geq \frac{1}{m}\operatorname{ord}_M f^m &> \frac{m_0 r}{m_0 r + s}\left(\lambda - \frac{\varepsilon}{2}\right) + \frac{s}{m_0 r + s}\operatorname{ord}_M f \\ &> \frac{m_0 r}{m_0 r + s}\left(\lambda - \frac{\varepsilon}{2}\right) + \frac{s}{m_0 r + s}\left(\lambda - \frac{\varepsilon}{2}\right) - \frac{\varepsilon}{2} \\ &= \left(\lambda - \frac{\varepsilon}{2}\right) - \frac{\varepsilon}{2} = \lambda - \varepsilon\end{aligned}$$

Innen következik, hogy $\lambda = \lim_{m\to\infty} \frac{1}{m}\operatorname{ord}_M f^m$. □

5.1.10. Lemma. *Minden s egészre és r pozitív egészre*

$$\operatorname{Newton}(V, \pi^s f^r) = r \operatorname{Newton}(V, f) + s$$

Bizonyítás. Triviális, hogy

$$\operatorname{Newton}(V, \pi^s f) = \operatorname{Newton}(V, f) + s$$

A másik rész azért teljesül, mert

$$\operatorname{Newton}(V, f^r) = \lim_{m\to\infty} \frac{1}{m}\operatorname{ord}_M f^{rm} = \lim_{m\to\infty} \frac{r}{m}\operatorname{ord}_M f^m = r \operatorname{Newton}(V, f)$$

□

5.1.11. Lemma. *Ha létezik egy M rács, amire $f^{h+1}(M) \subseteq \pi^{-1}M$, akkor létezik olyan M'' rács is, amire $f(M'') \subseteq M''$.*

Bizonyítás. A főideálgyűrű (A) feletti végesen generált modulusok alaptétele ([2] 7.4.1 tétel) szerint $M' := M + f(M) + \ldots + f^h(M)$ egy szabad A-modulus lesz. A szabad generátorrendszere nem lehet h-nál több elemű, mivel akkor K-lineárisan összefüggő lenne és abból következik π egy hatványával felszorozva az A-lineáris összefüggőség; de h-nál kevesebb elemű sem lehet, hiszen $M \subseteq M'$, így a szabad generátorrendszer K felett generátorrendszere egész V-nek. Ez azt jelenti, hogy M' egy rács.

Ekkor

$$\sum_{j=0}^{h+1} f^j(M') = \sum_{j=0}^{2h+1} f^j(M) = M' + \sum_{j=0}^{h} f^j(f^{h+1}(M)) \subseteq \pi^{-1}M'$$

Tekintsük a következő, rácsokból álló láncot:

$$M' \subseteq M' + f(M') \subseteq \ldots \subseteq \sum_{j=0}^{h+1} f^j(M') \subseteq \pi^{-1}M'$$

Mivel $\dim_{A/\pi A} \pi^{-1}M'/M' = h$, így ebben nem állhat fenn mindenütt szigorú tartalmazás, így létezik egy $0 \leq i \leq h$, amelyre

$$M'' := \sum_{j=0}^{i} f^j(M') = \sum_{j=0}^{i+1} f^j(M')$$

Ekkor $f(M'') \subseteq M''$. □

5.1.12. Tétel. *Létezik olyan M rács V-ben és olyan $1 \leq r \leq h$ és $s \leq d$ egészek, hogy*

$$\operatorname{ord}_M f^r = s \quad \textit{és} \quad \operatorname{Newton}(V, f) = \frac{s}{r}$$

Bizonyítás. Legyen $\lambda := \operatorname{Newton}(V, f)$.

Először belátjuk, hogy léteznek olyan $1 \leq r \leq h$ és s egészek, hogy

$$\left|\lambda - \frac{s}{r}\right| \leq \frac{1}{r(h+1)}$$

Minden $r \in \mathbb{Z}$-hez megkeressük azt a t_r értéket, amelyre

$$s_r := r\lambda - t_r \in \mathbb{Z} \quad \text{és} \quad -\frac{1}{h+1} \leq t_r < 1 - \frac{1}{h+1}$$

Ha egy $1 \leq r \leq h$-ra $t_r \leq \frac{1}{h+1}$, akkor készen vagyunk azzal az r-rel és $s := s_r$-rel. Egyébként van olyan $1 \leq r_1 < r_2 \leq h$, hogy $|t_{r_1} - t_{r_2}| \leq \frac{1}{h+1}$. Ekkor $r := r_2 - r_1$ és $s := s_{r_2} - s_{r_1}$ könnyen láthatóan megfelelő lesz.

Belátjuk, hogy létezik egy M rács V-ben, amelyre $f^r(M) \subseteq \pi^s M$. Legyen

$$f' := \pi^{-s} f^r \quad \text{és} \quad f'' := \pi^{1+(h+1)} f'^{(h+1)^2}$$

Az 5.1.10 lemma szerint

$$\lambda' := \operatorname{Newton}(V, f') \geq -|\operatorname{Newton}(V, f')| = -|r\lambda - s| \geq -\frac{1}{h+1}$$

és

$$\operatorname{Newton}(V, f'') \geq (h+1)^2\lambda' + 1 + (h+1) \geq 1$$

Így találhatunk egy M_1 rácsot V-ben és egy m pozitív egészt, melyre $f''^m(M_1) \subseteq M_1$. $M_2 := M_1 + f''(M_1) + \ldots + f''^{m-1}(M_1)$-re $f''(M_2) \subseteq M_2$, azaz $(\pi f'^{h+1})^{h+1}(M_2) \subseteq \subseteq \pi^{-1}M_2$. Kétszer alkalmazva az 5.1.11 lemmát, kapunk olyan M' rácsot, amelyre $\pi f'^{h+1}(M') \subseteq M'$, azaz $f'^{h+1}(M') \subseteq \pi^{-1}M'$ és olyan M rácsot, melyre $f'(M) \subseteq M$, azaz $f^r(M) \subseteq \pi^s M$.

$\lambda' \leq \frac{1}{h+1}$ miatt

$$\operatorname{ord}_M f' \geq 0 > \lambda' - \frac{1}{h} \leq \frac{1}{h} \operatorname{ord}_M f'^h - \frac{1}{h}$$

Az 5.1.7 lemma ii. része miatt $\operatorname{ord}_M f' = \frac{1}{m} \operatorname{ord}_M f'^m$ minden $m \geq 1$-re. Így $\lambda' = \operatorname{ord}_M f' \in \mathbb{Z}$, tehát $\lambda' = 0$, $\lambda = \frac{r}{s}$ és $\operatorname{ord}_M f^r = s + \operatorname{ord}_M f' = s$. $\frac{s}{r} = \lambda \leq \frac{d}{h}$ következik onnan, hogy $s \leq \frac{dr}{h} \leq d$. □

A második résznél használt trükk segítségével bizonyítható a következő lemma is:

5.1.13. Lemma. *Legyen r pozitív egész és s egész úgy, hogy* $\operatorname{Newton}(V, f) \geq \frac{s}{r}$, *ekkor létezik egy M rács V-ben, amelyre $f^r(M) \subseteq \pi^s M$.*

Bizonyítás. Legyen $f' := \pi^{1-s(h+1)} f^{r(h+1)}$. Az 5.1.10 lemma szerint

$$\operatorname{Newton}(V, f') = r(h+1) \operatorname{Newton}(V, f) + 1 - s(h+1) \geq 1$$

Így létezik egy M_1 rács V-ben és egy m pozitív egész, melyekre $f'^m(M_1) \subseteq M_1$. $M_2 := M_1 + f'(M_1) + \ldots + f'^{m-1}(M_1)$-re $f'(M_2) \subseteq M_2$, azaz $(\pi^{-s} f^r)^{h+1}(M_2) \subseteq \pi^{-1} M_2$. Az 5.1.11 lemma szerint így létezik egy olyan M rács V-ben, melyre $\pi^{-s} f^r(M) \subseteq M$, azaz $f^r(M) \subseteq \pi^s M$. □

5.1.14. Definíció. *A (V, f) izokristályt izoklinnek nevezzük, ha*

$$\operatorname{Newton}(V, f) = \frac{d(V, f)}{h(V, f)}$$

5.1.15. Lemma. *A következő állítások ekvivalensek:*

i. (V, f) izoklin.

ii. Létezik egy M rács V-ben, melyre $f^h(M) = \pi^d M$.

iii. Létezik egy M rács V-ben, r pozitív egész és s egész úgy, hogy $f^r(M) = \pi^s M$.

Továbbá minden a iii. állítás feltételét kielégítő (r, s) párra $\operatorname{Newton}(V, f) = \frac{s}{r}$.

Bizonyítás. i. ⇒ ii. Az 5.1.13 lemma szerint vegyünk egy M rácsot V-ben, melyre $f^h(M) \subseteq \pi^d M$. Ekkor

$$[\pi^d M : f^h(M)] = [M : f^h(M)] - [M : \pi^d M] = h[M : f(M)] - dh = 0$$

így $f^h(M) = \pi^d M$.

ii. $\Rightarrow$ iii. Ez a következtetés triviálisan teljesül.

iii. $\Rightarrow$ i. Mivel

$$\begin{aligned} 0 &= [\pi^s M : f^r(M)] = [M : f^r(M)] - [M : \pi^s M] \\ &= r[M : f(M)] - hs = rd - hs \end{aligned}$$

így

$$\frac{d}{h} = \frac{s}{r} = \frac{1}{r}\operatorname{ord}_M f^r \leq \operatorname{Newton}(V, f) \leq \frac{d}{h}$$

és így $\operatorname{Newton}(V, f) = \frac{d}{h} = \frac{s}{r}$. □

5.1.16. Definíció. *Ha r pozitív egész és s egész, akkor legyen a hozzájuk tartozó standard izokristály $V_{s,r} = (K^r, f_{s,r})$, ahol*

$$f_{s,r}(e_i) := \begin{cases} e_{i+1} & , \text{ ha } 1 \leq i < r \\ \pi^s e_1 & , \text{ ha } i = r \end{cases}$$

(itt (e_i) a K^r vektortér standard bázisa).

Az $A^r = \sum_{i=1}^r Ae_i$ rácsra $f_{s,r}(A^r) = A\pi^s e_1 + \sum_{i=2}^r Ae_i$, így $h(V_{s,r}) = r$, $d(V_{s,r}) = s$ és $f_{s,r}^r(A^r) = \pi^s A^r$. Így $V_{s,r}$ izoklin és $\operatorname{Newton}(V_{s,r}) = \frac{s}{r}$.

Egy $\alpha : (V, f) \to (V', f')$ σ^a-izokristályok közötti homomorfizmus alatt egy olyan $\alpha : V \to V'$ K-lineáris leképezést értünk, amelyre $f' \circ \alpha = \alpha \circ f$.

5.1.17. Lemma. *i. Legyen $0 \to (V_1, f_1) \xrightarrow{\alpha} (V, f) \xrightarrow{\beta} (V_2, f_2) \to 0$ egy izokristályokból álló rövid egzakt sorozat, ekkor*

$$\operatorname{Newton}(V, f) \leq \min(\operatorname{Newton}(V_1, f_1), \operatorname{Newton}(V_2, f_2))$$

és ha (V, f) izoklin, akkor (V_1, f_1) és (V_2, f_2) is az és

$$\operatorname{Newton}(V_1, f_1) = \operatorname{Newton}(V, f) = \operatorname{Newton}(V_2, f_2)$$

ii. Legyen (V, f) izoklin és legyen (V', f') egy másik izokristály és tegyük fel, hogy $\operatorname{Newton}(V, f) < \operatorname{Newton}(V', f')$. Ekkor (V, f) és (V', f') között egyik irányban sincsen nemnulla homomorfizmus.

Bizonyítás. i. Az 5.1.12 tétel szerint létezik egy M rács V-ben és $r, s \in \mathbb{Z}$, $r > 0$, melyekre $f^r(M) \subseteq \pi^s M$ és $\operatorname{Newton}(V, f) = \frac{s}{r}$.

Belátjuk, hogy $M_1 := \alpha^{-1}(M)$ és $M_2 := \beta(M)$ rácsok V_1-ben illetve V_2-ben. Ismét a főideálgyűrű feletti végesen generált modulusok alaptételére hivatkozva ezek szabad A-modulusok lesznek. Ha $\langle . \rangle_K$ jelöli a generált K-vektorteret, akkor $\langle M \rangle_K = V$,

hiszen M rács és innen $\langle M_2\rangle_K = \mathrm{im}(\beta) = V_2$, tehát M_2 szabad generátorrendszere legalább $\dim_K V_2$ elemű (és annál több elemű nyilván nem lehet). Másfelől $\langle M \cap \mathrm{im}(\alpha)\rangle_K = \mathrm{im}(\alpha)$, hiszen minden $v \in \mathrm{im}(\alpha)$-hoz van olyan n, hogy $\pi^n v \in M$ és mivel $\alpha : V_1 \to \mathrm{im}(\alpha)$ K-lineáris bijekció, így $\langle M_1\rangle_K = V_1$, tehát M_1 szabad generátorrendszere legalább $\dim_K V_1$ elemű (és annál több elemű nyilván nem lehet).

Ezzel beláttuk, hogy M_1 és M_2 rácsok a megfelelő vektorterekben. $i \in \{1,2\}$ esetén $f_i^r(M_i) \subseteq \pi^s M_i$ nyilván fennáll, így $\mathrm{Newton}(V,f) = \frac{s}{r} \leq \frac{1}{r}\mathrm{ord}_{M_i} f_i^r \leq$ $\leq \mathrm{Newton}(V_i, f_i)$.

Ha (V,f) izoklin, akkor az 5.1.15 lemma szerint az is feltehető, hogy $f^r(M) =$ $= \pi^s M$ és így $f_i^r(M) = \pi^s M_i$. Ekkor ismét az 5.1.15 lemmát használva (V_i, f_i) izoklin és $\mathrm{Newton}(V_i, f_i) = \frac{s}{r} = \mathrm{Newton}(V,f)$

ii. Tegyük fel indirekt először azt, hogy $\alpha \neq 0$ egy $(V,f) \to (V',f')$ homomorfizmus. Tekintsük a $(V_1 := \mathrm{im}(\alpha), f_1 := f'|_{V_1})$ izokristályt. Az i. állítást alkalmazzuk a

$$0 \to (\ker(\alpha), f|_{\ker(\alpha)}) \xrightarrow{\mathrm{id}} (V,f) \xrightarrow{\alpha} (V_1, f_1) \to 0$$

és a

$$0 \to (V_1, f_1) \xrightarrow{\mathrm{id}} (V', f') \xrightarrow{pr} (V'/V_1, g_1) \to 0$$

rövid egzakt sorozatokra (az utóbbiban $pr : V' \to V'/V_1$ a projekció, $g_1(u + V_1) :$ $:= f'(u) + V_1$; könnyen átgondolható, hogy ezek valóban izokristályokból álló rövid egzakt sorozatok). Az elsőből, mivel (V,f) izoklin, így ((V_1, f_1) is izoklin és) $\mathrm{Newton}(V,f) = \mathrm{Newton}(V_1, f_1)$, a másodikból $\mathrm{Newton}(V_1, f_1) \geq N(V', f')$, ezek együtt ellentmondást adnak, az indirekt feltevés téves volt.

Tegyük fel most, hogy $\beta \neq 0$ egy $(V', f') \to (V, f)$ homomorfizmus. Tekintsük a $(V_2 := \mathrm{im}(\beta), f_2 := f|_{V_2})$ izokristályt. Most a

$$0 \to (\ker(\beta), f'|_{\ker(\beta)}) \xrightarrow{\mathrm{id}} (V', f') \xrightarrow{\beta} (V_2, f_2) \to 0$$

és a

$$0 \to (V_2, f_2) \xrightarrow{\mathrm{id}} (V, f) \xrightarrow{pr} (V/V_2, g_2) \to 0$$

rövid egzakt sorozatokra fogjuk alkalmazni az i. állítást (ahol $pr : V \to V/V_2$ projekció, $g_2(u + V_2) := f(u) + V_2$). Az elsőből $\mathrm{Newton}(V', f') \leq \mathrm{Newton}(V_2, f_2)$, a másodikból (V,f) izoklin volta miatt $\mathrm{Newton}(V_2, f_2) = \mathrm{Newton}(V,f)$, így ismét ellentmondást kapunk. □

5.1.18. Lemma. *Ha $r, s \in \mathbb{Z}$, $r > 0$ és r és s relatív prímek (azaz $s = 0$ esetén $r = 1$), akkor a $V_{s,r}$ standard izokristálynak nincs valódi részizokristálya.*

Bizonyítás. Legyen (V,f) egy részizokristálya $V_{s,r}$-nek, aminek a magassága $1 \leq$

$\leq h \leq r$ és a dimenziója f. Ekkor 5.1.17 i. szerint (V, f) izoklin és

$$\frac{d}{h} = \text{Newton}(V, f) = \text{Newton}(V_{s,r}) = \frac{s}{r}$$

Mivel r és s relatív prímek, $r|h$, így $r = h$, így $V = V_{s,r}$. □

A továbbiakban feltesszük, hogy A teljes. Ekkor minden V-beli M rácsra az $M \to \varprojlim_n M/\pi^n M$ természetes leképezés izomorfizmus.

5.1.19. Tétel. *Legyen A teljes, ekkor egyértelműen léteznek $(V_1, f_1), \ldots, (V_t, f_t) \leq$ $\leq (V, f)$ izoklin részizokristályok, amelyekre*

$$V = \bigoplus_{i=1}^{t} V_i, \quad f = \bigoplus_{i=1}^{t} f_i$$

és

$$\text{Newton}(V, f) = \text{Newton}(V_1, f_1) < \text{Newton}(V_2, f_2) < \ldots < \text{Newton}(V_t, f_t)$$

Bizonyítás. Elegendő azt belátni, hogy V előáll $V = V_1 \oplus V_1'$ direkt összegként, ahol V_1, V_2 f-invariáns alterek, $(V_1, f|_{V_1})$ izoklin és

$$\text{Newton}(V, f) = \text{Newton}(V_1, f|_{V_1}) < \text{Newton}(V_1', f_{V_1'})$$

Létezés: Legyen $\text{Newton}(V, f) = \frac{s}{r}$, ahol $s, r \in \mathbb{Z}$, $r > 0$ és legyen M egy rács V-ben, melyre $f^r(M) \subseteq \pi^s M$ (5.1.12 miatt van ilyen). A $g := \pi^{-s} f^r$ leképezésre $g(M) \subseteq M$ és így minden k pozitív egészre indukál egy

$$g_k : M/\pi^k M \to M/\pi^k M$$

leképezést. Rögzítsünk egy k-t. Mivel $M/\pi^k M$ véges hosszú, így a

$$\text{im}(g_k) \supseteq \text{im}(g_k^2) \supseteq \ldots \supseteq \text{im}(g_k^i) \supseteq \ldots$$

és

$$\ker(g_k) \subseteq \ker(g_k^2) \subseteq \ldots \subseteq \ker(g_k^i) \subseteq \ldots$$

A-részmodulusláncok $M/\pi^k M$-ben egy idő után stabilizálódnak. Így létezik egy $j = j(k) \geq 1$, amelyre

$$M_{k,1} := \text{im}(g_k^j) = \text{im}(g_k^i) \quad \text{és} \quad M_{k,1}' := \ker(g_k^j) = \ker(g_k^i)$$

minden $i \geq j$-re. Ekkor a következők nyilvánvalóan teljesülnek:

(a) $g_k(M_{k,1}) = g_k(\text{im}(g_k^j)) = \text{im}(g_k^{j+1}) = M_{k,1}$

(b) $g_k^j(M'_{k,1}) = g_k^j(\ker(g_k^j)) = \{0\}$

(c) $g_k(M'_{k,1}) = g_k(\ker(g_k^{j+1})) \subseteq \ker(g_k^j) = M'_{k,1}$

Mivel $M_{k,1}$ véges hosszú, így (a)-ból $g_k : M_{k,1} \overset{\cong}{\to} M_{k,1}$ bijekció. (b) szerint így $M_{k,1} \cap M'_{k,1} = \{0\}$.

Legyen $\bar{v} \in M/\pi^k M$ tetszőleges elem. Ekkor $g_k^j(\bar{v}) = g_k^{2j}(\bar{\bar{v}})$ egy $\bar{\bar{v}} \in M/\pi^k M$ elemre, így

$$v = g_k^j(\bar{\bar{v}}) + (\bar{v} - g_k^j(\bar{\bar{v}})) \in M_{k,1} + M'_{k,1}$$

Ez azt jelenti, hogy $M/\pi^k M = M_{k,1} \oplus M'_{k,1}$. Ahogy k-t változtatjuk, könnyen átgondolható, hogy ez a felbontás kompatibilis a $M/\pi^{k+1}M \to M/\pi^k M$ projekciókkal. Így legyen

$$M_1 := \varprojlim_k M_{k,1} \quad \text{és} \quad M'_1 := \varprojlim_k M'_{k,1}$$

így kapunk egy

$$M = M_1 \oplus M'_1$$

felbontást f-invariáns A-részmodulusok direkt összegére. Könnyen láthatóan

(d) $g(M_1) = M_1$

(e) $g^{j(1)}(M'_1) \subseteq \pi M'_1$

Legyen $V_1 := KM_1$ és $V'_1 := KM'_1$, ekkor

$$V = V_1 \oplus V'_1$$

V felbontása g-invariáns alterek direkt összegére. Nyilvánvalóan M_1 illetve M'_1 rács V_1-ben illetve V'_1-ben. (d) és 5.1.15 szerint $(V_1, g|_{V_1})$ izoklin és 0 meredekségű, (e) szerint

$$\mathrm{Newton}(V'_1, g|_{V'_1}) \geq \frac{1}{j(1)} > 0 = \mathrm{Newton}(V_1, g|_{V_1})$$

Vegyük észre, hogy

$$V = f(V_1) \oplus f(V'_1)$$

egy másik g-invariáns alterekre való felbontás, ahol $(f(V_1), g|_{f(V_1)})$ is izoklin és

$$\mathrm{Newton}(f(V'_1), g|_{f(V'_1)}) > 0 = \mathrm{Newton}(f(V_1), g|_{f(V_1)})$$

Az 5.1.17 lemma ii. része szerint a

$$(V_1, g|_{V_1}) \overset{\subseteq}{\to} (V, g) \overset{pr}{\to} (f(V'_1), g|_{f(V'_1)})$$

illetve

$$(V'_1, g|_{V'_1}) \overset{\subseteq}{\to} (V, g) \overset{pr}{\to} (f(V_1), g|_{f(V_1)})$$

leképezéspárok kompozíciója azonosan nulla. Ebből következik, hogy V_1 illetve V_1' f-invariánsak. (d) és (e) szerint

$$f^r(M_1) = \pi^s M_1 \quad \text{és} \quad f^{rj(1)}(M_1') \subseteq \pi^{sj(1)+1} M_1$$

tehát az 5.1.15 lemma szerint

$$\mathrm{Newton}(V, f) = \frac{s}{r} = \mathrm{Newton}(V_1, f|_{V_1}) < \frac{sj(1)+1}{rj(1)} \leq \mathrm{Newton}(V_1', f|_{V_1'})$$

Egyértelműség: Az egyértelműség az 5.1.17 lemma segítségével ugyanúgy látható be, mint V_1 és V_1' f-invarianciája. □

5.1.20. Definíció. *Az 5.1.19 tétel szerint létező* $\mathrm{Newton}(V_1, f_1), \ldots, \mathrm{Newton}(V_t, f_t)$ *számokat a* (V, f) *izokristály meredekségeinek nevezzük.*

5.2. A Dieudonné–Manin tétel

Az izoklin izokristályok szerkezetének a megértéséhez szükségünk lesz néhány további feltevésre, ezekre együtt (DM)-ként hivatkozunk:

– A teljes és az $A/\mathfrak{m}$ maradékteste algebrailag zárt és $p > 0$ karakterisztikájú;

– $\sigma^a \equiv a^q \mod \mathfrak{m}$ minden $a \in A$-ra, ahol $q > 1$ egy rögzített p-hatvány;

– létezik egy $\pi \in A$ prímelem, melyre $\sigma(\pi) = \pi$.

5.2.1. Tétel. *Tegyük fel, hogy (DM) teljesül és* (V, f) *egy izoklin* σ*-izokristály 0 meredekséggel, ekkor létezik egy* $v_1, \ldots, v_h$ K*-bázis* V*-ben, amelyre* $f(v_j) = v_j$ *minden* $1 \leq j \leq h$*-ra.*

Bizonyítás. Legyen M egy rács V-ben, melyre $f(M) = M$. A kívánt $(v_i)_i$ bázist M A-bázisaként konstruáljuk meg. Mivel $M \cong \varprojlim_k M/\pi^k M$, így $\varprojlim_k M/\pi^k M$ elemeiként kereshetjük a bázisvektorokat. Így konstruálunk rekurzívan egy $\left((v_1^{(k)}, \ldots, v_h^{(k)})\right)_k$ M^h-ban haladó sorozatot, amelyre a következők teljesülnek:

(a) $\left\{v_1^{(k)} \mod \pi M, \ldots, v_h^{(k)} \mod \pi M\right\}$ egy $A/\mathfrak{m}$-bázis $M/\pi M$-ben;

(b) $f\left(v_j^{(k)}\right) \equiv v_j^{(k)} \mod \pi^k M$ minden $1 \leq j \leq h$-ra;

(c) $v_j^{(k+1)} \equiv v_j^{(k)} \mod \pi^k M$ minden $1 \leq j \leq h$-ra.

A kezdőlépés, azaz $v_1^{(1)}, \dots, v_k^{(1)}$ létezése azonnal következik a 2.2.1 tételből.

Tegyük fel, hogy már konstruáltuk (a)-(c)-t kielégítő $v_1^{(k)}, \dots, v_h^{(k)}$ elemeket.

(a)-ból könnyen láthatóan következik, hogy $v_1^{(k)}, \dots, v_h^{(k)}$ egy A-bázisa M-nek. Ezek szerint

$$f\left(v_j^{(k)}\right) - v_j^{(k)} = \pi^k \sum_{i=1}^{h} a_{ij} v_i^{(k)} \quad \text{ahol } a_{ij} \in A$$

Mivel a maradéktest algebrailag zárt, találhatunk $b_{ij} \in A$ elemeket, melyekre

$$a_{ij} + \sigma(b_{ij}) - b_{ij} \equiv a_{ij} + b_{ij}^q - b_{ij} \equiv 0 \mod \mathfrak{m}$$

Legyen

$$v_j^{(k+1)} := v_j^{(k)} + \pi^k \sum_{i=1}^{h} b_{ij} v_i^{(k)}$$

Ekkor a konstrukció láthatóan biztosítja (a) és (c) teljesülését, (b) azért teljesül, mert

$$\begin{aligned} f\left(v_j^{(k+1)}\right) - v_j^{(k+1)} &= f\left(v_j^{(k)}\right) - v_j^{(k)} + \sigma(\pi)^k \sum_{i=1}^{h} \sigma(b_{ij}) f\left(v_i^{(k)}\right) - \pi^k \sum_{i=1}^{h} b_{ij} v_i^{(k)} \\ &= \pi^k \sum_{i=1}^{h} (a_{ij} + \sigma(b_{ij}) - b_{ij}) v_i^{(k)} + \pi^{2k} \sum_{i=1}^{h} \sum \ell = 1^h \sigma(b_{ij}) a_{\ell i} v_\ell^{(k)} \\ &\equiv 0 \mod \pi^{(k+1)} M \end{aligned}$$

(c) szerint a $v_j := \left(v_j^{(k)} + \pi^k M\right)_k$ elemek $M \cong \varprojlim_k M/\pi^k M$-ben jóldefiniáltak, ezek (a) szerint A-bázist alkotnak M-ben és így K-bázist V-ben, végül (b) szerint $f(v_j) = v_j$ is teljesül rájuk. □

5.2.2. Tétel. *(Dieudonné–Manin) Tegyük fel, hogy (DM) teljesül és (V, f) egy izoklin σ-izokristály és* $\mathrm{Newton}(V, f) = \frac{s}{r}$*, ahol $r, s \in \mathbb{Z}$ relatív prímek, $r > 0$. Ekkor (V, f) izomorf $V_{s,r}$ standard izokristályok (véges) direkt összegével.*

Bizonyítás. Az 5.1.13 lemma szerint találhatunk olyan V-beli M rácsot, melyre $f^r(M) \subseteq \pi^s M$. Mivel $\frac{s}{r} = \frac{d}{h}$, így

$$[\pi^s M : f^r(M)] = [M : f^r(M)] - [M : \pi^s M] = rd - sh = 0$$

és így $f^r(M) = \pi^s M$. Az 5.2.1 tételt alkalmazhatjuk a $(V, \pi^{-s} f^r)$ izokristályra, ami az 5.1.15 és 5.1.10 lemmák szerint izoklin 0 meredekséggel, így kaphatunk $v_1, \dots, v_h$

bázist V-ben, melyre $f^r(v_j) = \pi^s v_j$. Legyen $V_j := \sum_{i=0}^{r-1} Kf^i(v_j)$. Ekkor

$$\begin{aligned} V_{s,r} &\to (V_j, f|_{V_j}) \\ e_i &\mapsto f^{i-1}(v_j) \end{aligned}$$

egy szürjektív izokristály-homomorfizmus, ami az 5.1.18 lemma szerint izomorfizmus kell, hogy legyen.

Így kaptunk egy

$$V = \sum_{j=1}^{h} V_j \quad \text{ahol } (V_j, f|_{V_j}) \cong V_{s,r}$$

összeg-előállítást. Az 5.1.18 lemma szerint a V_j-knek nincsen nemtriviális részizokristálya, így ebből az összegből egy egyszerű eljárás szerint kijelölhetünk néhány tagot, amelyeknek már direkt összege lesz V: haladjunk végig az egyes V_j-ken valamilyen sorrendben, amikor tekintünk egy V_j-t, nézzük meg, hogy annak mi a metszete az eddig kiválasztott tagok összegével. Ez a metszet csak $\{0\}$ vagy V_j lehet, az előbbi esetben válasszuk ki V_j-t, az utóbbi esetben pedig ne válasszuk ki. Könnyen átgondolható, hogy a kiválasztott tagok összege mindig direkt összeg és hogy az eljárás során mindig V a már kiválasztott és a még nem vizsgált tagok összege. □

Hivatkozások

[1] Kedlaya, Kiran S., *p-adic Differential Equations*, Cambridge University Press, New York, 2010. Elérhető a `http://kskedlaya.org/papers/p-adic_differential_equations.pdf` címen.

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

[3] Manin, Jurij I., *Kommutatív formális csoportok elmélete véges karakterisztikájú testek felett* (oroszul), Uszpehi Matematicseszki Nauk., 18 (6), 1963.

[4] Schneider, Peter *Die Theorie des Anstieges* előadásjegyzet, elérhető a `http://wwwmath.uni-muenster.de/u/pschnei/publ/lectnotes/Theorie--des-Anstiegs.pdf` címen, 2006/07.

[5] Zábrádi Gergely, *Algebrai számelmélet jegyzet*, elérhető a `http://www.cs.elte.hu/~zger/Jegyzetek/algszamjegyzet.pdf` címen, 2014.