NYILATKOZAT

Név: MÁRTON DÉNES

ELTE Természettudományi Kar, szak: MATEMATIKA

NEPTUN azonosító: TW3DC1

Szakdolgozat címe: MONSKY TÉTEL

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

Budapest, 2022.05.31.

Márton Dénes

a hallgató aláírása

Eötvös Loránd Tudományegyetem
Természettudományi Kar

Márton Dénes
Matematika BSc

Monsky tétel

Szakdolgozat

Témavezető: Zábrádi Gergely
Algebra és Számelmélet Tanszék

Budapest, 2022

Köszönetnyilvánítás

Elsősorban szeretném megköszönni témavezetőmnek, Zábrádi Gergelynek, hogy elvállalta a témavezetésemet a BSc szakdolgozatomban, és hogy egy nagyon érdekes témát ajánlott. Az utolsó pillanatos kérdéseimre is rögtön és részletesen válaszolt, nélküle biztosan nem sikerült volna megírnom.

Továbbá szeretném megköszönni a családomnak és a barátaimnak a támogatásukat és motivációjukat.

Tartalomjegyzék

1. Bevezetés

Az American Mathematical Monthly lapban 1967-ben Fred Richman és John Thomas tette fel azt a kérdést, hogy egy négyzetet fel lehet-e bontani páratlan sok azonos területű háromszögre. Thomas egy évvel később megmutatta, hogy ez nem lehetséges, ha a négyzet a $[0,1] \times [0,1]$ és a háromszögelésben előforduló háromszögek csúcsai racionális koordinátájúak páratlan nevezővel. Végül 1970-ben Paul Monsky válaszolta meg a kérdést az általános esetben is. Lényegében azzal egészítette ki Thomas bizonyítását, hogy felhasználta, hogy létezik nemarkhimédeszi, egészen pontosan 2-adikus abszolútérték $\mathbb{R}$-en. Ez fontos része a bizonyításnak, de mint látni fogjuk, ehhez használni kell a Zorn lemmát. Amikor a feladatot kitűzték, akkor azt gondolták, hogy létezik rá egyszerű megoldás, azonban ma sem ismert ennél elemibb. A bizonyítás másik fontos része a Sperner lemma egy alakja. Ebben a szakdolgozatban az algebrai részére fogunk koncentrálni. Bevezetjük az abszolútértékek fogalmát és megvizsgáljuk a tulajdonságaikat különös tekintettel a nemarkhimédeszi abszolútértékre. Természetes a p-adikus számok bevezetése, amikkel bizonyíthatjuk, hogy létezik $\mathbb{R}$-en nemarkhimédeszi abszolútérték. Szükségünk lesz analízisből és topológiából ismert fogalmakra is, hogy le tudjuk írni a p-adikus számokat és tulajdonságaikat. Ezután megnézzük a p-adikus számok bővítéseit. Végül elérjük a $\mathbb{C}_p$ testet, ami a komplex számok testére már hasonlít abban az értelemben, hogy teljes és algebrailag is zárt, ezért nem tudjuk bővíteni Cauchy sorozatok limeszeivel és polinomok gyökeinek hozzávételével. Idáig követjük Gouvêa könyvét [1]. Az 5. fejezetben bebizonyítjuk, hogy létezik $\mathbb{R}$-en is p-adikus abszolútérték, ehhez Lang Algebra [3] és Hungerford ugyancsak Algebra [2] című könyvét használjuk a transzcendens bázis definíciójához és alapvető tulajdonságaihoz. Ehhez a fejezethez szükség van az eddigieknél több halmazelmélet ismeretre, de még bőven elég a BSc-s tudás. Végül az utolsó fejezetben bebizonyítjuk Monsky tételét [5], ami egy szép példája annak, hogy a p-adikus számok váratlanul, sokféle problémánál hasznosak tudnak lenni. Monsky tételének általánosítását n-dimenziós hiperkockára Mead bizonyította be [4], ezt is megnézzük. Itt már nem csak a 2-adikus abszolútértékre lesz szükség, hanem a p-adikus abszolútértékre is minden prímszámra. Végül síkbeli további általánosításokat mondunk ki és néhányat bizonyítunk. Jelenleg is több megválaszolatlan kérdés van a témában, ezek és az általánosítások Stein cikkében találhatóak [6].

2. Abszolútértékek

2.1. Definíciók

Legyen K test és legyen $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$ a nemnegatív valós számok halmaza.

2.1. Definíció. Azt mondjuk, hogy egy $|\cdot| : K \to \mathbb{R}_+$ függvény *abszolútérték*, ha teljesíti a következő tulajdonságokat:

(i) $|x| = 0$ pontosan akkor, ha $x = 0$;

(ii) $|xy| = |x||y|$ minden $x, y \in K$;

(iii) $|x + y| \leq |x| + |y|$ minden $x, y \in K$.

Ha a *(iii)*-nál erősebb

(iv) $|x+y| \leq \max\{|x|,|y|\}$ minden $x, y \in K$

feltételt is teljesíti, akkor azt mondjuk, hogy az abszolútérték *nemarkhimédeszi*, ha nem teljesíti, akkor pedig azt, hogy *arkhimédeszi*.

2.2. Példa. Ha K tetszőleges test, akkor $|x| = \begin{cases} 0 & \text{, ha } x = 0 \\ 1 & \text{, ha } x \neq 0 \end{cases}$ egy nemarkhimédeszi abszolútérték és *triviális abszolútérték*nek hívják.

2.3. Példa. Legyen $K = \mathbb{Q}$. Arkhimédeszi abszolútérték a *szokásos*

$$|x|_\infty = \begin{cases} x & \text{, ha } x \geq 0 \\ -x & \text{, ha } x < 0 \end{cases}$$

abszolútérték.

Egy másik érdekesebb példa a következő:

2.4. Definíció. Legyen $p \in \mathbb{Z}$ egy prímszám. Definiáljuk a $v_p : \mathbb{Q} \to \mathbb{R} \cup \{+\infty\}$ függvényt a következő módon: ha n nemnulla egész szám, akkor $v_p(n)$ legyen az a természetes szám, amire $p^{v_p(n)} \mid n$, de $p^{v_p(n)+1} \nmid n$. (Ez egyértelműen létezik.) Ha adottak r, s nemnulla relatív prím egészek és $x = r/s \in \mathbb{Q}^\times$ racionális szám, akkor $v_p(x) := v_p(r) - v_p(s)$. Illetve $v_p(0) := +\infty$. ($+\infty$ szimbólumot a szokásos módon értelmezzük)

2.5. Állítás. *Minden $x, y \in \mathbb{Q}$ számpárra teljesülnek az alábbiak:*

a) $v_p(xy) = v_p(x) + v_p(y)$;

b) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

Bizonyítás. 1. eset: Tegyük fel, hogy $x \neq 0 \neq y$. Ekkor $x = p^{v_p(x)} \cdot \frac{a}{b}$, ahol $a, b \in \mathbb{Z}$, $p \nmid ab$, illetve $y = p^{v_p(y)} \cdot \frac{c}{d}$, ahol $c, d \in \mathbb{Z}$, $p \nmid cd$.

a) $xy = p^{v_p(x)+v_p(y)} \cdot \frac{ac}{bd}$, ahol $p \nmid abcd$, tehát $v_p(xy) = v_p(x) + v_p(y)$.

b) Tegyük fel az általánosság rovása nélkül, hogy $v_p(x) \leq v_p(y)$. Ekkor

$$x + y = p^{v_p(x)} \left(\frac{a}{b} + p^{v_p(y)-v_p(x)} \cdot \frac{c}{d} \right) = p^{v_p(x)} \cdot \frac{ad + bc \cdot p^{v_p(y)-v_p(x)}}{bd}.$$

A számlálóban és a nevezőben is egész szám van és a nevező nem osztható p-vel, így $v_p(x+y) \geq v_p(x) = \min\{v_p(x), v_p(y)\}$.

2. eset: Valamelyik 0, például $y = 0$.

a) $+\infty = v_p(x) + \infty$,

b) $v_p(x) \geq \min\{v_p(x), +\infty\} = v_p(x)$

mindkettő egyszerűen adódott. □

2.6. Definíció. Tetszőleges $x \in \mathbb{Q}$ racionális számra legyen $|x|_p = p^{-v_p(x)}$, ahol természetesen $|0|_p = 0$ a $+\infty$ szimbólumot értelemszerűen használva. Ezt nevezzük a *p-adikus abszolútérték*nek.

2.7. Következmény. $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ *valóban abszolútérték és nemarkhimédeszi.*

Bizonyítás. Az előző Állításból egyszerűen következik. □

2.2. Alapvető tulajdonságok

2.8. Állítás. *Legyen K tetszőleges test és $|\cdot| : K \to \mathbb{R}_+$ tetszőleges abszolútérték. Ekkor teljesülnek a következők:*

(i) $|1| = 1$*;*

(ii) ha $x \in K$*,* $n \in \mathbb{N}$ *és* $|x^n| = 1$*, akkor* $|x| = 1$*;*

(iii) $|-1| = 1$*;*

(iv) minden $x \in K$*-ra* $|-x| = |x|$*;*

(v) ha K *véges, akkor* $|\cdot|$ *triviális.*

Bizonyítás. *(i)* $|1| = |1^2| = |1|^2$, ezért $|1| = 1$, mert $|1|$ pozitív valós szám.

(ii) $1 = |x^n| = |x|^n$, tehát itt is $|x| = 1$, mert $|x|$ nemnegatív valós szám.

(iii) $1 = |1| = |(-1)^2| = |-1|^2$, innen is $|-1| = 1$ adódik.

(iv) $|-x| = |(-1)x| = |-1||x| = 1|x| = |x|$

(v) Legyen $|K| = q \in \mathbb{N}$ $(q \geq 2)$, ekkor minden $x \neq 0$ elemre teljesül $x^{q-1} = 1$. Az (i) miatt $|x^{q-1}| = 1$ és a (ii) miatt $|x| = 1$, tehát $|\cdot|$ triviális.

□

Tekintsük az $i : \mathbb{Z} \hookrightarrow K$ beágyazást, azaz

$$i : n \mapsto \begin{cases} \underbrace{1 + \cdots + 1}_{n} & , \text{ ha } n > 0 \\ 0 & , \text{ ha } n = 0 \\ -\underbrace{(1 + \cdots + 1)}_{-n} & , \text{ ha } n < 0 \end{cases}.$$

Legyen i képe $A \subset K$. Ha K karakterisztikája 0, akkor $A \simeq \mathbb{Z}$, ha pedig $\mathrm{char}(K) = p$ prím, akkor $A \simeq \mathbb{F}_p$ a K prímteste.

2.9. Tétel. *Legyen $A \subset K$ az előző halmaz. Egy $|\cdot|$ abszolútérték K-n pontosan akkor nemarkhimédeszi, ha $|a| \leq 1$ minden $a \in A$ számra. Speciálisan egy abszolútérték $\mathbb{Q}$-n pontosan akkor nemarkhimédeszi, ha $|n| \leq 1$ minden n egész számra.*

Bizonyítás. Tegyük fel, hogy $|\cdot|$ nemarkhimédeszi, indukcióval bizonyítunk. Mivel $|\pm 1| = 1$ (2.8. Állítás (i), (iii)), ezért $|a \pm 1| \leq \max\{|a|, 1\}$. Ha $a \in A$-ra tudjuk, hogy $|a| \leq 1$, akkor az egyenlőtlenség miatt $|a \pm 1| \leq 1$, ezért minden $a \in A$-ra igaz, mert például $|0| = 0 \leq 1$.

A másik irányhoz tegyük fel, hogy minden $a \in A$-ra $|a| \leq 1$. Azt akarjuk megmutatni, hogy $|x + y| \leq \max\{|x|, |y|\}$. Ha $y = 0$, akkor triviálisan teljesül, ha $y \neq 0$, akkor $|y|$-nal elosztva ekvivalens állítást kapunk és látjuk, hogy elegendő $|x + 1| \leq \max\{|x|, 1\}$ egyenlőtlenséget megmutatni minden $x \in K$-ra. Vegyünk egy tetszőleges m pozitív

egészt, ekkor $\binom{m}{k}$ egész minden $k = 0, 1, \ldots, m$ számra, azaz a feltétel miatt $\left|\binom{m}{k}\right| \leq 1$. Felírhatjuk a következő egyenlőtlenségeket:

$$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq$$

$$\leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x^k| \leq$$

$$\leq \sum_{k=0}^{m} |x^k| = \sum_{k=0}^{m} |x|^k$$

Ha $|x| > 1$, akkor $|x|^0, |x|^1, \ldots, |x|^m$ közül $|x|^m$ a legnagyobb, ha pedig $|x| \leq 1$, akkor $|x|^k \leq 1$ minden $k = 0, 1, \ldots, m$ számra. A két esetet egyszerre felírhatjuk:

$$\sum_{k=0}^{m} |x|^k \leq (m+1) \max\{|x|^m, 1\}.$$

Tehát m-edik gyökvonás után

$$|x+1| \leq \sqrt[m]{m+1} \max\{|x|, 1\}.$$

Most vehetjük az $m \to \infty$ határértéket, és $\lim_{m\to\infty} \sqrt[m]{m+1} = 1$ miatt teljesül a bizonyítandó $|x+1| \leq \max\{|x|, 1\}$. □

Az arkhimédeszi és a nemarkhimédeszi elnevezések a következő definícióból jönnek.

2.10. Definíció. Azt mondjuk, hogy $|\cdot|$ *teljesíti az Arkhimédeszi tulajdonságot*, ha minden $x, y \in K$, $x \neq 0$ esetén létezik n pozitív egész, amire $|nx| > |y|$.

2.11. Állítás. *Legyen K test. A $|\cdot|$ abszolútérték pontosan akkor akhimédeszi, ha teljesíti az Arkhimédeszi tulajdonságot.*

Bizonyítás. Ha teljesül az Arkhimédeszi tulajdonság, akkor $x = 1$, $y = 1$ választással létezik n pozitív egész, amire $|n| > 1$, és ez a 2.9. Tétel alapján éppen azt jelenti, hogy $|\cdot|$ arkhimédeszi. Tegyük fel, hogy $|\cdot|$ arkhimédeszi, ekkor létezik $a \in A$, hogy $|a| > 1$. Ekkor $|a^k| = |a|^k$ tetszőlegesen nagy lehet. Legyen $x, y \in K$, $x \neq 0$ és ehhez $n = a^k$ olyan, hogy $|n| > |y/x|$. Ekkor látjuk, hogy teljesül az Arkhimédeszi tulajdonság, mert $|nx| > |y| \iff |n| > |y/x|$. □

2.12. Következmény. *Legyen K test és $|\cdot|$ abszolútérték K-n. Ekkor*

1) $|\cdot|$ arkhimédeszi $\iff \sup\{|n| : n \in \mathbb{Z}\} = +\infty$;

2) $|\cdot|$ nemarkhimédeszi $\iff \sup\{|n| : n \in \mathbb{Z}\} = 1$;

3) ha $\sup\{|n| : n \in \mathbb{Z}\} = C < +\infty$, akkor $|\cdot|$ nemarkhimédeszi és $C = 1$.

Bizonyítás. Ha $|\cdot|$ arkhimédeszi, akkor 2.9. Tétel miatt létezik $n \in \mathbb{Z}$, hogy $|n| > 1$, tehát $|n^k| = |n|^k$ miatt $\sup\{|n| : n \in \mathbb{Z}\}$ nem lehet korlátos. Ha nemarkhimédeszi, akkor minden $n \in \mathbb{Z}$-re $|n| \leq 1$, illetve $|1| = 1$ miatt $\sup\{|n| : n \in \mathbb{Z}\} = 1$. Ezzel 1)-et és 2)-t, illetve 3)-ban azt a következtetést, hogy $|\cdot|$ nemarkhimédeszi beláttuk. Két lépésben 3) másik következtetése is látszik, mert ha már tudjuk, hogy $|\cdot|$ nemarkhimédeszi, akkor 2) miatt $C = 1$. □

2.3. Topológia

Definiálhatunk K-n egy metrikát a szokásos módon: $d(x,y) = |x-y|$, $x, y \in K$.

2.13. Állítás. *A $d : K \times K \to \mathbb{R}$ függvény valóban metrika.*

Bizonyítás. $d(x,y) = |x-y| \geq 0$
$d(x,y) = |x-y| = 0 \Leftrightarrow x-y = 0 \Leftrightarrow x = y$
$d(x,y) = |x-y| = |-(x-y)| = |y-x| = d(y,x)$
$d(x,y) + d(y,z) = |x-y| + |y-z| \geq |(x-y)+(y-z)| = |x-z| = d(x,z)$ □

2.14. Állítás. *Legyen $|\cdot|$ egy abszolútérték K-n és d a belőle származtatott metrika. Ekkor $|\cdot|$ pontosan akkor nemarkhimédeszi, ha minden $x, y, z \in K$-ra*

$$d(x,y) \leq \max\{d(x,z), d(z,y)\}.$$

Bizonyítás. Tegyük fel, hogy $|\cdot|$ nemarkhimédeszi. Ekkor

$$d(x,y) = |x-y| \leq \max\{|x-z|, |z-y|\} = \max\{d(x,z), d(z,y)\}.$$

A másik irányhoz helyettesítsük be a következőket: $x := x$, $y := -y$, $z := 0$.

$$|x+y| = d(x,-y) \leq \max\{d(x,0), d(0,-y\} = \max\{|x|, |y|\}$$

□

Az Állításban lévő egyenlőtlenséget teljesítő metrikát *ultrametrikának* szokás hívni. Ha egy téren adott egy ultrametrika, akkor azt a teret *ultrametrikus térnek* hívjuk.

2.15. Állítás. *Legyen adott egy $|\cdot|$ nemarkhimédeszi abszolútérték K-n. Ha $x, y \in K$, $|x| \neq |y|$, akkor*

$$|x+y| = \max\{|x|, |y|\}.$$

Bizonyítás. Tegyük fel, hogy $|x| > |y|$. Ekkor teljesül, hogy

$$|x+y| \leq \max\{|x|, |y|\} = |x|.$$

Másrészt $x = (x+y) - y$, ezért

$$|x| \leq \max\{|x+y|, |-y|\} = \max\{|x+y|, |y|\}.$$

Ez csak akkor teljesülhet, ha $\max\{|x+y|, |y|\} = |x+y|$, mert feltettük, hogy $|x| > |y|$. Visszaírva az egyenlőtlenségbe, $|x| \leq |x+y|$. Mindkét irányú egyenlőtlenséget megmutattuk, azaz $|x| = |x+y|$. □

2.16. Következmény. *Ultrametrikus térben minden háromszög egyenlőszárú.*

Bizonyítás. Legyen a háromszög három csúcsa x, y, z, ekkor a háromszög oldalainak hosszai $d(x,y) = |x-y|$, $d(y,z) = |y-z|$, $d(x,z) = |x-z|$. Ha $|x-y| = |y-z|$, akkor a háromszög egyenlőszárú. Ha $|x-y| \neq |y-z|$, akkor viszont az előző Állítás alapján $|(x-y)+(y-z)| = |x-z|$ megegyezik a hosszabbik oldallal. □

Tehát azt kaptuk, hogy ha K testen adott egy nemarkhimédeszi abszolútérték, akkor $|x|$, $|y|$ és $|x+y|$ közül legalább kettő megegyezik.
Nézzük meg a p-adikus abszolútérték esetén:

2.17. Példa. Legyen $p \in \mathbb{Z}$ prím, $x, y \in \mathbb{Z}$ egész számok. Ekkor $x = p^n x'$ és $y = p^m y'$ valamilyen n, m egészekre és $p \nmid x'y'$ egészekre. Tegyük fel, hogy $p^{-n} = |x|_p > |y|_p = p^{-m}$, azaz $n < m$. Ekkor $x + y = p^n(x' + p^{m-n}y')$ és $p \nmid x' + p^{m-n}y'$, mert $p \nmid x'$, így $|x + y|_p = p^{-n} = |x|_p$. Ha pedig $p^{-n} = |x|_p = |y|_p = p^{-m}$, akkkor $n = m$ és $x + y = p^n(x' + y')$. Mivel lehetséges, hogy p osztja $(x' + y')$-t, így annyit tudunk mondani, hogy $|x + y|_p \leq p^{-n} = |x|_p = |y|_p$. Tehát $|x|_p$, $|y|_p$ és $|x + y|_p$ közül legalább kettő megegyezik.

2.18. Definíció. Legyen K testen adott $|\cdot|$ abszolútérték, továbbá $a \in K$, $r \in \mathbb{R}_+$. Az a középpontú r sugarú *nyílt gömb*

$$B(a, r) = \{x \in K : d(x, a) < r\} = \{x \in K : |x - a| < r\}.$$

Az a középpontú r sugarú *zárt gömb*

$$\overline{B}(a, r) = \{x \in K : d(x, a) \leq r\} = \{x \in K : |x - a| \leq r\}.$$

2.19. Állítás. *Legyen a K testen adott $|\cdot|$ nemarkhimédeszi abszolútérték.*

(i) Ha $b \in B(a, r)$, akkor $B(a, r) = B(b, r)$; azaz egy nyílt gömb minden pontja a középpontja.

(ii) Ha $b \in \overline{B}(a, r)$, akkor $\overline{B}(a, r) = \overline{B}(b, r)$; azaz egy zárt gömb minden pontja a középpontja.

(iii) $B(a, r)$ nyílt és zárt halmaz.

(iv) Ha $r \neq 0$, akkor $\overline{B}(a, r)$ nyílt és zárt halmaz.

(v) Ha $r \neq 0 \neq s$, akkor $B(a, r) \cap B(b, s) \neq \emptyset$ pontosan akkor, ha $B(a, r) \subset B(b, s)$ vagy $B(a, r) \supset B(b, s)$; azaz két nyílt gömb vagy diszjunkt vagy tartalmazzák egymást.

(vi) Ha $r \neq 0 \neq s$, akkor $\overline{B}(a, r) \cap \overline{B}(b, s) \neq \emptyset$ pontosan akkor, ha $\overline{B}(a, r) \subset \overline{B}(b, s)$ vagy $\overline{B}(a, r) \supset \overline{B}(b, s)$; azaz két zárt gömb vagy diszjunkt vagy tartalmazzák egymást.

Bizonyítás. *(i)* Definíció szerint $b \in B(a, r) \Leftrightarrow |b - a| < r$. Vegyünk egy $x \in B(a, r)$ pontot, azaz $|x - a| < r$. Ekkor

$$|x - b| \leq \max\{|x - a|, |b - a|\} < r,$$

azaz $x \in B(b, r)$. Vagyis azt kaptuk, hogy $B(a, r) \subset B(b, r)$. Ha $x \in B(b, r)$, akkor $|x - b| < r$ és

$$|x - a| \leq \max\{|x - b|, |b - a|\} < r,$$

tehát $x \in B(a, r)$. Azaz $B(b, r) \subset B(a, r)$, és így $B(a, r) = B(b, r)$.

(ii) Az (i) rész bizonyítása megismételhető ha $<$-t mindenhol $\leq$-re cseréljük.

(iii) $B(a, r)$ minden metrikus térben nyílt halmaz, de most egyszerűbb dolgunk van: legyen $x \in B(a, r)$, ekkor meg kell mutatni, hogy x belső pont. Ezt bizonyítja, hogy $B(x, r) \subset B(a, r)$, mivel az (i) miatt $B(x, r) = B(a, r)$.

$B(a, r)$ zárt: vegyünk egy x pontot $B(a, r)$ határán. Legyen $s \leq r$. Ekkor létezik $y \in B(a, r) \cap B(x, s)$ pont, mert x a $B(a, r)$ határán van, így minden környezetében tartalmaz $B(a, r)$-beli pontot. Tehát $|y - a| < r$, $|y - x| < s$. Így

$$|x - a| \leq \max\{|y - a|, |y - x|\} < \max\{r, s\} \leq r,$$

tehát $x \in B(a, r)$, azaz $B(a, r)$ tartalmazza a határát, vagyis zárt.

(iv) $\overline{B}(a,r)$ nyílt: vegyünk egy $x \in \overline{B}(a,r)$ pontot. Ez a pont belső pont, mivel $B(x,r) \overset{(i)}{=} B(a,r) \subset \overline{B}(a,r)$. (Az $r \neq 0$ feltétel azért kell, hogy $B(x,r)$ ne legyen üres halmaz. Ez a (iii) részben nem okoz gondot, mivel ott $B(a,r)$ is üres halmaz, de itt $\overline{B}(a,r)$ egy pont.)

$\overline{B}(a,r)$ zárt: a (iii) részhez hasonlóan. Legyen x a $\overline{B}(a,r)$ határán és $s \leq r$. Ekkor legyen $y \in \overline{B}(a,r) \cap B(x,s)$, azaz $|y-a| \leq r$, $|y-x| < s$.

$$|x-a| \leq \max\{|y-a|, |y-x|\} \leq r$$

Tehát $x \in \overline{B}(a,r)$, azaz $\overline{B}(a,r)$ tartalmazza a határát, vagyis zárt.

(v) Ha valamelyik tartalmazás fennáll, akkor természetesen nem lehetnek diszjunktak. Tegyük fel, hogy $r \leq s$. Ha $B(a,r) \cap B(b,s) \neq \emptyset$, akkor létezik $c \in B(a,r) \cap B(b,s)$. Azonban (i) miatt $B(a,r) = B(c,r)$ és $B(b,s) = B(c,s)$, tehát

$$B(a,r) = B(c,r) \subset B(c,s) = B(b,s).$$

(vi) Az (v) rész bizonyításában a nyílt gömböket zártakra kell cserélni és a (ii)-t használni.

□

2.20. Állítás. *Legyen K testen adott $|\cdot|$ nemarkhimédeszi abszolútérték. Ekkor K összefüggőségi komponensei az egy elemű pontok.*

Bizonyítás. Tegyük fel, hogy $x, y \in K$ különböző pontok és $S \subset K$ halmaz tartalmazza mindkettőt. Legyen $r = |x-y| \neq 0$ és $U = B(x, r/2)$, $V = K \setminus U$. U nyílt-zárt halmaz, ezért V is nyílt. Ekkor $S \cap U$ és $S \cap V$ az S egy nyílt felbontása, mert S altértopológiájában nyíltak, diszjunktak és nem üresek, mert $x \in S \cap U$ és $y \in S \cap V$. □

3. p-adikus számok

3.1. Abszolútértékek $\mathbb{Q}$-n

3.1. Definíció. Azt mondjuk, hogy két abszolútérték K-n *ekvivalens*, ha ugyanazt a topológiát generálják K-n.

3.2. Állítás. *Legyen $|\cdot|_1$ és $|\cdot|_2$ két abszolútérték K-n. A következők ekvivalensek:*

i) $|\cdot|_1$ *és* $|\cdot|_2$ *ekvivalensek;*

ii) $|x|_1 < 1 \iff |x|_2 < 1$ *minden* $x \in K$*;*

iii) létezik egy $\alpha > 0$ *valós szám, hogy minden* $x \in K$ *esetén* $|x|_1 = |x|_2^\alpha$.

Bizonyítás. Először megmutatjuk $i) \Rightarrow ii)$-t. Ha ugyanazt a topológiát generálják, akkor ha egy sorozat konvergens az egyik szerint, akkor konvergens a másik szerint is és ugyanoda konvergálnak. Továbbá az is igaz, hogy $x \in K$-ra $\lim\limits_{n\to\infty} x^n = 0$ pontosan akkor teljesül egy $|\cdot|$ abszolútérték által generált topológiában, ha $|x| < 1$. Ebből már következik $ii)$.

ii) $\Rightarrow$ *iii)* Vegyünk egy $x_0 \in K$, $x_0 \neq 0$ számot, amire $|x_0|_1 < 1$. (Ha $|x_0|_1 > 1$, akkor x_0^{-1} jó választás, ha pedig minden $x \neq 0$ számra $|x|_1 = 1$, akkor $|\cdot|_1$ triviális. $|x|_1 > 1 \Leftrightarrow |x^{-1}|_1 < 1 \Leftrightarrow |x^{-1}|_2 < 1 \Leftrightarrow |x|_2 > 1$, tehát $|\cdot|_2$ is triviális és $\alpha = 1$.) Mivel $|x_0|_1 < 1$, ezért $|x_0|_2 < 1$ és legyen α az a pozitív valós szám, amire $|x_0|_1 = |x_0|_2^\alpha$, tehát $\alpha = \frac{\log|x_0|_1}{\log|x_0|_2}$.
Vegyünk egy másik $x \in K$, $x \neq 0$ számot. Ha $|x|_1 = |x_0|_1$, akkor $|x/x_0|_1 = 1$ és $|x/x_0|_2 = 1$, különben $|x/x_0|_2 < 1$ esetén $|x/x_0|_1 < 1$, $|x/x_0|_2 > 1$ esetén pedig $|x/x_0|_1 > 1$. Tehát $|x|_2 = |x_0|_2$, és ekkor $|x|_1 = |x|_2^\alpha$. Ha pedig $|x|_1 = 1$, akkor az előzőhöz hasonlóan $|x|_2 = 1$, és itt is igaz $|x|_1 = |x|_2^\alpha$. Feltehetjük, hogy $|x|_1 \neq |x_0|_1$ és $|x|_1 \neq 1$. Ugyanígy feltehetjük $|\cdot|_2$-re is. Legyen β az a pozitív (*ii)* miatt) valós szám, amire $|x|_1 = |x|_2^\beta$. Feltehető $|x|_1 < 1$, mert ha $|x|_1 < 1$ esetén megmutatjuk, hogy $|x|_1 = |x|_2^\alpha$, akkor $|x|_1 > 1$-re $|x^{-1}|_1 < 1$, ekkor $|x^{-1}|_1 = |x^{-1}|_2^\alpha$, azaz $|x|_1 = |x|_2^\alpha$. $|x|_1 < 1$ és *ii)* miatt $|x|_2 < 1$.
Legyenek n és m pozitív egész számok, ekkor

$$|x|_1^n < |x_0|_1^m \Longleftrightarrow \left|\frac{x^n}{x_0^m}\right|_1 < 1 \Longleftrightarrow \left|\frac{x^n}{x_0^m}\right|_2 < 1 \Longleftrightarrow |x|_2^n < |x_0|_2^m.$$

(Ilyen n és m található, például $m = 1$ és n kellően nagy.) Innen

$$n \log|x|_1 < m \log|x_0|_1 \Longleftrightarrow n \log|x|_2 < m \log|x_0|_2,$$

ami $\log|x|_1 < 0$, $\log|x|_2 < 0$ miatt

$$\frac{n}{m} > \frac{\log|x_0|_1}{\log|x|_1} \Longleftrightarrow \frac{n}{m} > \frac{\log|x_0|_2}{\log|x|_2}.$$

Tehát ugyanazok a racionális számok nagyobbak $\frac{\log|x_0|_1}{\log|x|_1}$-nél, mint $\frac{\log|x_0|_2}{\log|x|_2}$-nél, de ez csak akkor lehetséges, ha ez a két valós szám megegyezik, azaz

$$\frac{\log|x_0|_1}{\log|x|_1} = \frac{\log|x_0|_2}{\log|x|_2},$$

amit átrendezve

$$\frac{\log|x_0|_1}{\log|x_0|_2} = \frac{\log|x|_1}{\log|x|_2},$$

azaz $\alpha = \beta$.

Végül megmutatjuk *iii)* $\Rightarrow$ *i)*-t.

$$|x-a|_1 < r \Longleftrightarrow |x-a|_2^\alpha < r \Longleftrightarrow |x-a|_2 < r^{1/\alpha}$$

Tehát $B_1(a,r) = B_2(a, r^{1/\alpha})$, azaz pontosan ugyanazok a nyílt gömbök $|\cdot|_1$ és $|\cdot|_2$ szerint, vagyis a topológia is, mert a nyílt gömbök a topológia egy bázisát adják. □

3.3. Tétel (Ostrowski)**.** *Minden nemtriviális abszolútérték $\mathbb{Q}$-n ekvivalens vagy a $|\cdot|_\infty$ szokásos abszolútértékkel vagy valamilyen p prímszámra a $|\cdot|_p$ p-adikus abszolútértékkel.*

Bizonyítás. Legyen $|\cdot|$ nemtriviális abszolútérték $\mathbb{Q}$-n. A lehetséges két esetet külön vizsgáljuk:

a) Tegyük fel, hogy $|\cdot|$ arkhimédeszi. Legyen n_0 a legkisebb pozitív egész, amire $|n_0| > 1$ (2.9. Tétel). Legyen α az a pozitív valós szám, amire $|n_0| = n_0^\alpha$. Megmutatjuk,

hogy $|x| = |x|_\infty^\alpha$ teljesül minden racionális x-re, mert ekkor $|\cdot|$ és $|\cdot|_\infty$ ekvivalens. Ehhez elég bebizonyítani, hogy $|n| = n^\alpha$ teljesül minden n pozitív egészre ($|x| = |-x|$ és $|r/s| = |r|/|s|$ miatt).

Írjuk fel n-et n_0-s számrendszerben, azaz

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k,$$

ahol $0 \le a_i \le n_0 - 1$ és $a_k \neq 0$. A k szám az $n_0^k \le n < n_0^{k+1}$ egyenlőtlenség által van meghatározva és $|a_i| \le 1$ az n_0 választása miatt.

$$|n| = |a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k| \le$$

$$\le |a_0| + |a_1| n_0^\alpha + |a_2| n_0^{2\alpha} + \cdots + |a_k| n_0^{k\alpha} \le$$

$$\le 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha} =$$

$$= n_0^{k\alpha} \left(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-k\alpha}\right) \le$$

$$\le n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha} =$$

$$= n_0^{k\alpha} \frac{1}{1 - n_0^{-\alpha}} = n_0^{k\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1}$$

Legyen $C = n_0^\alpha / (n_0^\alpha - 1) > 0$ szám ($n_0^\alpha = |n_0| > 1$). Azt kaptuk, hogy

$$|n| \le C n_0^{k\alpha} \le C n^\alpha.$$

Ez minden n-re teljesül, így az n^N alakú számokra is, azaz

$$|n^N| \le C n^{N\alpha}.$$

Ahonnan

$$|n| \le \sqrt[N]{C}\, n^\alpha.$$

Ez minden N-re teljesül, tehát $N \to \infty$ határértéket véve $|n| \le n^\alpha$.

Ismét nézzük n-nek az n_0-s számrendszerbeli felírását, és használjuk ugyanazokat a jelöléseket.

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \le |n| + |n_0^{k+1} - n|$$

$$|n| \ge n_0^{(k+1)\alpha} - |n_0^{k+1} - n| \ge n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha,$$

ahol felhasználtuk az előző részben kijött $|n| \le n^\alpha$ egyenlőtlenséget pozitív egész számokra, mivel $n_0^{k+1} > n$. Azt is tudjuk, hogy $n \ge n_0^k$, ezért

$$n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n\right)^\alpha \ge n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n_0^k\right)^\alpha,$$

így

$$|n| \ge n_0^{(k+1)\alpha} - \left(n_0^{k+1} - n_0^k\right)^\alpha =$$

$$= n_0^{(k+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) =$$

$$= C' n_0^{(k+1)\alpha} > C' n^\alpha,$$

ha bevezetjük $C' = 1 - (1 - 1/n_0)^\alpha > 0$ számot. Ugyanúgy, mint az előbb, n^N alakú számokra felírva, $1/N$ hatványra emelve, majd $N \to \infty$ határértéket véve kapjuk az $|n| \geq n^\alpha$ egyenlőtlenséget. Tehát teljesül $|n| = n^\alpha$, és így $|\cdot|$ és $|\cdot|_\infty$ ekvivalensek.

b) Tegyük fel, hogy $|\cdot|$ nemarkhimédeszi. Most is elegendő egészekre belátni $|n| = |n|_p^\alpha$ egyenlőséget belátni valamilyen α-ra. Ekkor $|n| \leq 1$ minden n egészre (2.9. Tétel). Mivel $|\cdot|$ nemtriviális, ezért létezik egy legkisebb pozitív egész n_0, amire $|n_0| < 1$, és ez az $n_0 \neq 1$, mert $|1| = 1$ minden abszolútértékre. Tegyük fel, hogy $n_0 = ab$ valamilyen a, b pozitív egész számra, amik kisebbek, mint n_0. Tehát n_0 definíciója miatt $|a| = |b| = 1$, mivel 1-nél nagyobbak nem lehetnek. Ez persze nem lehetséges, mert $1 > |n_0| = |ab| = |a||b| = 1$, tehát n_0 prímszám, nevezzük át p-re. Megmutatjuk, hogy $|\cdot|$ ekvivalens $|\cdot|_p$-vel.

Vegyünk egy $p \nmid n$ egész számot. Ekkor $n = rp + s$ valamilyen r egész számra és $0 < s < p$ egész számra. Definíció miatt $|s| = 1$ és $|r| \leq 1$ (2.9. Tétel), tehát $|rp| = |r||p| < 1$. Így 2.15. Állítás miatt

$$|n| = |rp + s| = \max\{|rp|, |s|\} = 1.$$

Vegyünk most egy tetszőleges n egészt. Ekkor $n = p^v n'$, ahol v természetes szám, $p \nmid n'$ egész szám. Ekkor

$$|n| = |p^v n'| = |p|^v |n'| = |p|^v = c^{-v},$$

ahol $c = |p|^{-1}$. Másrészt $|n|_p = p^{-v}$, tehát $\alpha = \log_p(c)$-re $|n| = |n|_p^\alpha$, azaz $|\cdot|$ és $|\cdot|_p$ ekvivalensek. ($\alpha = \log_p(c) > 0 \Leftrightarrow c > 1 \Leftrightarrow |p| < 1$) □

3.4. Állítás. *Minden $x \in \mathbb{Q}^\times$ számra*

$$\prod_{p \leq \infty} |x|_p = 1,$$

ahol $p \leq \infty$ azt jelenti, hogy p prímszám és a p-adikus abszolútértéket vesszük vagy a szokásos $|\cdot|_\infty$ abszolútértéket.

Bizonyítás. Legyen $x = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ az x prímfelbontása, ahol α_i lehet negatív is.

$$\begin{cases} |x|_q = 1, & \text{ha } q \neq p_i \\ |x|_{p_i} = p_i^{-\alpha_i}, & \text{ha } i = 1, \ldots, k \\ |x|_\infty = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \end{cases}$$

Innen pedig látszik az egyenlőség. □

Ez a tétel indokolja, hogy a p-adikus abszolútérték alapja p legyen, hiszen $|x| = c^{-v_p(x)}$ ($c > 1$) is ekvivalens abszolútérték lenne.

3.2. Teljessé tétel

Rögzítsünk le egy $|\cdot| = |\cdot|_p$ p-adikus abszolútértéket $\mathbb{Q}$-n valamilyen p prímszámra.

3.5. Állítás. *Legyen adott K-n egy nemarkhimédeszi abszolútérték. Egy $(x_n) \subset K$ sorozat pontosan akkor Cauchy, ha*

$$\lim_{n \to \infty} |x_{n+1} - x_n| = 0.$$

Bizonyítás. Az egyik irányhoz tegyük fel, hogy (x_n) Cauchy. Legyen $\varepsilon > 0$, ekkor létezik $N \in \mathbb{N}$, hogy minden $n, m \geq N$-re $|x_n - x_m| < \varepsilon$, speciálisan $|x_{n+1} - x_n| < \varepsilon$, tehát $\lim\limits_{n\to\infty} |x_{n+1} - x_n| = 0$.

Másik irány: legyen $\varepsilon > 0$, ekkor létezik $N \in \mathbb{N}$, hogy minden $n \geq N$-re teljesül $|x_{n+1} - x_n| < \varepsilon$. Ha $m = n + r > n \geq N$, akkor

$$|x_m - x_n| = |(x_{n+r} - x_{n+r-1}) + (x_{n+r-1} - x_{n+r-2}) + \cdots + (x_{n+1} - x_n)| \leq$$

$$\leq \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\} < \varepsilon.$$

Tehát (x_n) Cauchy. □

3.6. Tétel. *A racionális számok $\mathbb{Q}$ teste nem teljes semmilyen nemtriviális abszolútérték szerint sem.*

Bizonyítás. Ostrowski tétele miatt (3.3. Tétel) elegendő $|\cdot|_p$-re belátni, ahol $p \leq \infty$. A szokásos abszolútérték szerint ismert, hogy $\mathbb{Q}$ nem teljes, például $\sqrt{2}$ közelíthető racionális számokból álló Cauchy sorozattal, de $\sqrt{2} \notin \mathbb{Q}$.

Tegyük fel, hogy $p \neq 2$ prím. Válasszunk $a \in \mathbb{Z}$ egész számot, amire:

- a semminek sem a négyzete $\mathbb{Q}$-ban;
- $p \nmid a$;
- $X^2 \equiv a \pmod{p}$-nek van megoldása.

(Ilyen a lehet $p + 1$, ha $p \neq 3$, vagy $a = 7$, ha $p = 3$.) Gyártunk egy (x_n) Cauchy sorozatot $|\cdot|_p$ szerint:

- x_0 legyen $X^2 \equiv a \pmod{p}$ valamilyen megoldása;
- x_n $(n \geq 1)$ legyen olyan, hogy $x_n \equiv x_{n-1} \pmod{p^n}$, $x_n^2 \equiv a \pmod{p^{n+1}}$.

Megmutatjuk, hogy (x_n) sorozat létezik: x_0 definíció szerint létezik. Tegyük fel, hogy $x_0, x_1, \ldots, x_{n-1}$ létezik. Ekkor keressük x_n-t $x_n = x_{n-1} + tp^n$ alakban.

$$x_n^2 = (x_{n-1} + tp^n)^2 = x_{n-1}^2 + 2x_{n-1}tp^n + t^2p^{2n}$$

Mivel $x_{n-1}^2 \equiv a \pmod{p^n}$, ezért $x_{n-1}^2 = a + sp^n$.

$$x_n^2 = a + sp^n + 2x_{n-1}tp^n + t^2p^{2n} \equiv a \pmod{p^{n+1}}$$

$$sp^n + 2x_{n-1}tp^n + t^2p^{2n} \equiv 0 \pmod{p^{n+1}}$$

Feltettük, hogy $n \geq 1$, ezért $2n \geq n+1$, tehát az utolsó tagot elhagyhatjuk és oszthatunk p^n-nel.

$$s + 2x_{n-1}t \equiv 0 \pmod{p}$$

Vegyük észre, hogy $x_{n-1} = x_{n-2} + a_{n-1}p^{n-1} = \cdots = x_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1}$, tehát $x_{n-1} \equiv x_0 \pmod{p}$, és $x_0 \not\equiv 0 \pmod{p}$, mert különben a osztható lenne p-vel. Illetve a $p \neq 2$ feltétel miatt oszthatunk 2-vel, ezért

$$t \equiv -s(2x_{n-1})^{-1} \pmod{p},$$

ahol $(2x_{n-1})^{-1}$ a $2x_{n-1}$ inverze $\mod p$. Tehát

$$x_n = x_{n-1} - s(2x_{n-1})^{-1}p^n = x_{n-1} - (2x_{n-1})^{-1}(x_{n-1}^2 - a)$$

rekurzióval megadva a sorozatot teljesülnek a feltételek. Így teljes indukcióval megadtuk az (x_n) sorozatot.

A 3.5. Állítást használva megmutatjuk, hogy (x_n) Cauchy:

$$|x_{n+1} - x_n|_p = |\lambda p^{n+1}|_p \leq p^{-(n+1)} \to 0.$$

Ugyanakkor az is teljesül,hogy

$$|x_n^2 - a|_p = |\mu p^{n+1}|_p \leq p^{-(n+1)} \to 0,$$

tehát ha létezik $\lim x_n = x \in \mathbb{Q}$, akkor $x^2 = a$, ami nem lehet, mert a-t így definiáltuk.

Ha $p = 2$, akkor az előző módszer nem működik, de valami nagyon hasonló igen:

- $\sqrt[3]{3} \notin \mathbb{Q}$;
- $2 \nmid 3$;
- $X^3 \equiv 3 \pmod 2$-nek van megoldása, például $X = 1$.

Definiáljuk a következő (x_n) sorozatot:

- x_0 az $X^3 \equiv 3 \pmod 2$ megoldása;
- x_n $(n \geq 1)$ legyen olyan, hogy $x_n \equiv x_{n-1} \pmod{2^n}$, $x_n^3 \equiv 3 \pmod{2^{n+1}}$.

Indukció: $x_0, x_1, \ldots, x_{n-1}$ létezik. Keressük x_n-t $x_n = x_{n-1} + t2^n$ alakban.

$$x_n^3 = (x_{n-1} + t2^n)^3 = x_{n-1}^3 + 3x_{n-1}^2 t2^n + 3x_{n-1}t^2 2^{2n} + t^3 2^{3n}$$

Tudjuk, hogy $x_{n-1}^3 \equiv 3 \pmod{2^n}$, ezért $x_{n-1}^3 = 3 + s2^n$.

$$x_n^3 = 3 + s2^n + 3x_{n-1}^2 t2^n + 3x_{n-1}t^2 2^{2n} + t^3 2^{3n} \equiv 3 \pmod{2^{n+1}}$$

$$s2^n + 3x_{n-1}^2 t2^n \equiv 0 \pmod{2^{n+1}}$$

Ismét elhagyhattuk az utolsó két tagot $n \geq 1$ miatt. Osszunk le 2^n-nel.

$$s + 3x_{n-1}^2 t \equiv 0 \pmod 2$$

$$s + x_{n-1}^2 t \equiv 0 \pmod 2$$

Megint észrevehetjük, hogy $x_{n-1} = x_0 + a_1 2 + \cdots + a_{n-1}2^{n-1}$, tehát $x_{n-1} \equiv 1 \pmod 2$, mert $x_0^3 \equiv 3 \equiv 1 \pmod 2$. Tehát

$$t \equiv -s \pmod 2,$$

vagyis

$$x_n = x_{n-1} - s2^n = x_{n-1} - (x_{n-1}^3 - 3).$$

Ebben az esetben is létezik az (x_n) sorozat.

A kapott sorozat Cauchy (3.5. Állítás):

$$|x_{n+1} - x_n|_2 = |\lambda 2^{n+1}|_2 \leq 2^{-(n+1)} \to 0.$$

Illetve mint az előbb

$$|x_n^3 - 3|_2 = |\mu 2^{n+1}|_2 \leq 2^{-(n+1)} \to 0,$$

tehát ha létezik $\lim x_n = x \in \mathbb{Q}$, akkor $x^3 = 3$, ami nem lehet. □

3.7. Definíció. Legyen $|\cdot| = |\cdot|_p$ nemarkhimédeszi abszolútérték $\mathbb{Q}$-n. Jelölje $\mathcal{C}$ vagy $\mathcal{C}_p(\mathbb{Q})$ a *Cauchy sorozatok halmazát* $\mathbb{Q}$-ban.

$$\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) = \{(x_n) \subset \mathbb{Q} : (x_n) \text{ Cauchy sorozat } |\cdot|_p \text{ szerint}\}$$

3.8. Állítás. *Legyen*

$$(x_n) + (y_n) := (x_n + y_n)$$
$$(x_n) \cdot (y_n) := (x_n y_n).$$

Ezekkel a műveletekkel ellátva $\mathcal{C}$-t, kommutatív egységelemes gyűrűt kapunk.

Bizonyítás. Azt kell megmutatni, hogy a műveletek nem vezetnek ki a halmazból, a többi könnyen látszik.

$$\limsup_{n\to\infty} |(x_{n+1} + y_{n+1}) - (x_n + y_n)| \le \limsup_{n\to\infty} \big(\max\{|x_{n+1} - x_n|, |y_{n+1} - y_n|\}\big) = 0$$

A 3.5. Állítás miatt tudjuk, hogy $(x_n + y_n)$ Cauchy.

$$\limsup_{n\to\infty} |x_{n+1}y_{n+1} - x_n y_n| = \limsup_{n\to\infty} |x_{n+1}y_{n+1} - x_{n+1}y_n + x_{n+1}y_n - x_n y_n| \le$$

$$\le \limsup_{n\to\infty} \big(\max\{|x_{n+1}||y_{n+1} - y_n|, |y_n||x_{n+1} - x_n|\}\big) = 0$$

Az (x_n) és (y_n) sorozatok Cauchy sorozatok, tehát konvergensek, tehát korlátosak. A különbségsorozatok 0-hoz tartanak, ezért a max-ban lévő mindkét sorozat nullsorozat. Szintén a 3.5. Állítás miatt $(x_n y_n)$ Cauchy. □

3.9. Definíció. Ha $x \in \mathbb{Q}$, akkor legyen

$$(x) := (x, x, x, \dots)$$

az *x-hez tartozó konstans sorozat.*

3.10. Állítás. *Az $x \mapsto (x)$ függvény egy beágyazása $\mathbb{Q}$-nak $\mathcal{C}$-be.*

Bizonyítás. Egyszerűen látszik, hogy (x) Cauchy, akár 3.5. Állításból, akár a definícióból. □

3.11. Definíció. Legyen

$$\mathcal{N} = \{(x_n) \subset \mathcal{C} : x_n \to 0\} = \{(x_n) \subset \mathcal{C} : \lim_{n\to\infty} |x_n|_p = 0\}$$

a *nullsorozatok halmaza.*

3.12. Állítás. *$\mathcal{N}$ egy maximális ideál $\mathcal{C}$-ben.*

Bizonyítás. Legyen $\mathcal{N} \subsetneq J \lhd \mathcal{C}$ ideál. Azt látjuk be, hogy ekkor $J = \mathcal{C}$. Legyen $(x_n) \in J \setminus \mathcal{N}$, és I az $\mathcal{N}$ és (x_n) által generált ideál. Ekkor $I = \mathcal{C}$ teljesül, tehát $J = \mathcal{C}$ is. Ehhez elegendő megmutatni, hogy (1) (csupa 1 sorozat), a $\mathcal{C}$ egységeleme benne van I-ben.

Először vegyük észre, hogy létezik egy $c > 0$ valós szám és egy $N \in \mathbb{N}$ természetes szám, amire $|x_n| \ge c > 0$ minden $n \ge N$-re:

$(x_n) \notin \mathcal{N}$, tehát $x_n \not\to 0$, azaz $\exists \varepsilon > 0\ \forall N \in \mathbb{N}\ \exists n \geq N:\ |x_n|_p \geq \varepsilon$, rögzítsünk egy ilyen ε-t;

$(x_n) \in \mathcal{C}$, ezért $\varepsilon/2$-höz $\exists N \in \mathbb{N}\ \forall n, m \geq N:\ |x_n - x_m|_p < \varepsilon/2$, rögzítsünk egy ilyen N-t. A rögzített ε és N megfelelő lesz.

Az első megállapítás miatt létezik $n \geq N$, hogy $|x_n|_p \geq \varepsilon$. Legyen $m \geq N$, ekkor $|x_n - x_m|_p < \varepsilon/2$, tehát

$$\varepsilon \leq |x_n|_p \leq \max\{|x_n - x_m|_p, |x_m|_p\}$$

miatt $\max\{|x_n - x_m|_p, |x_m|_p\} = |x_m|_p$, mert $|x_n - x_m|_p < \varepsilon/2$, így $|x_m|_p \geq \varepsilon$.

Definiáljuk az (y_n) sorozatot:

$$y_n = \begin{cases} 0, & n < N \\ 1/x_n, & n \geq N \end{cases}.$$

Ez a sorozat Cauchy lesz 3.5. Állítás miatt, mert $n \geq N$-re

$$|y_{n+1} - y_n| = \left|\frac{1}{x_{n+1}} - \frac{1}{x_n}\right| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|} \leq \frac{|x_{n+1} - x_n|}{c^2} \to 0,$$

felhasználva, hogy (x_n) Cauchy. Könnyen látszik, hogy

$$(1) - (x_n)(y_n) = \begin{cases} 1, & n < N \\ 0, & n \geq N \end{cases},$$

ami nullsorozat. Tehát $(1) - (x_n)(y_n) \in \mathcal{N}$, azaz (1) előáll egy $\mathcal{N}$-beli és (x_n) egy többszörösének összegeként, tehát $(1) \in I$. □

3.13. Definíció. Definiálhatjuk a *p-adikus számok* testét:

$$\mathbb{Q}_p = \mathcal{C}/\mathcal{N}.$$

Ez valóban egy test, mivel egy maximális ideállal faktorizáltunk ki. Két különböző konstans sorozat nem esik ugyanabba az ekvivalenciaosztályba, így továbbra is adott egy $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ beágyazás, ami $x \in \mathbb{Q}$ racionális számot (x) ekvivalenciaosztályába viszi. Ki tudjuk terjeszteni a p-adikus abszolútértéket $\mathbb{Q}_p$-re:

3.14. Állítás. *Legyen $(x_n) \in \mathcal{C}$, de $(x_n) \notin \mathcal{N}$. Az $|x_n|_p$ sorozat egy idő után állandó, azaz létezik N, hogy minden $n, m \geq N$ esetén $|x_n|_p = |x_m|_p$.*

Bizonyítás. Ahogy a 3.12. Állításban megmutattuk, létezik $N_1 \in \mathbb{N}$ és $c > 0$ valós szám, amire $|x_n| \geq c$ minden $n \geq N_1$-re. Ugyanakkor mivel (x_n) Cauchy, ezért létezik egy $N_2 \in \mathbb{N}$ is, amire $|x_n - x_m| < c$ minden $n, m \geq N_2$-re. Legyen $N = \max\{N_1, N_2\}$, ekkor mindkettő feltétel teljesül. Legyenek $n, m \geq N$, ekkor $|x_m| \geq c > |x_n - x_m|$, speciálisan $|x_m| \neq |x_n - x_m|$. Használhatjuk a 2.15. Állítást, tehát

$$|x_n| = \max\{|x_n - x_m|, |x_m|\} = |x_m|,$$

vagyis $n, m \geq N$ esetén teljesül $|x_n| = |x_m|$. □

3.15. Definíció. Legyen $\lambda \in \mathbb{Q}_p$ és legyen $(x_n) \in \mathcal{C}$ egy sorozat, ami reprezentálja λ-t. Ekkor legyen

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p.$$

3.16. Állítás. *Az előbb definiált $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_+$ függvény jóldefiniált, nemarkhimédeszi abszolútérték, ami kiterjeszti a $\mathbb{Q}$-n lévő p-adikus abszolútértéket.*

Bizonyítás. Ha $\lambda = 0$, akkor $(x_n) \in \mathcal{N}$, tehát definíció szerint $x_n \to 0$, vagyis a limesz létezik és 0. Ha $\lambda \neq 0$, akkor $(x_n) \notin \mathcal{N}$ és a 3.14. Állítás miatt $|x_n|_p$ sorozat egy idő után konstans, tehát a limesz létezik.

Tegyük fel, hogy a $\lambda \in \mathbb{Q}_p$ számot az (x_n) és az $(\tilde{x}_n)$ sorozat is reprezentálja. Ekkor meg kell mutatni, hogy ugyanazt a limeszt kapjuk. (x_n) és $(\tilde{x}_n)$ ugyanabban az ekvivalenciaosztályban vannak, tehát $(x_n) - (\tilde{x}_n) = (x_n - \tilde{x}_n) \in \mathcal{N}$, azaz $x_n - \tilde{x}_n \to 0$, $\lim\limits_{n\to\infty} |x_n - \tilde{x}_n|_p = 0$. A szokásos abszolútértéket és háromszögegyenlőtlenséget használva $|x_n - \tilde{x}_n|_p \geq \big||x_n|_p - |\tilde{x}_n|_p\big|$, ahonnan $\big||x_n|_p - |\tilde{x}_n|_p\big| \to 0$, azaz $\lim\limits_{n\to\infty} |x_n|_p = \lim\limits_{n\to\infty} |\tilde{x}_n|_p$.

Ha $\lambda \in \mathbb{Q}_p$, akkor $\lambda = 0 \Leftrightarrow (x_n) \in \mathcal{N} \Leftrightarrow \lim\limits_{n\to\infty} |x_n|_p = 0 \Leftrightarrow |\lambda|_p = 0$.

Legyen $\lambda, \mu \in \mathbb{Q}_p$ és reprezentálja őket (x_n) és (y_n). Ekkor $\lambda\mu$-t $(x_n) \cdot (y_n) = (x_n y_n)$ reprezentálja, így

$$|\lambda\mu|_p = \lim_{n\to\infty} |x_n y_n|_p = \lim_{n\to\infty} |x_n|_p |y_n|_p = \lim_{n\to\infty} |x_n|_p \lim_{n\to\infty} |y_n|_p = |\lambda|_p |\mu|_p.$$

Legyen $\lambda, \mu \in \mathbb{Q}_p$ és reprezentálja őket (x_n) és (y_n). Ekkor $(\lambda + \mu)$-t $(x_n) + (y_n) = (x_n + y_n)$ reprezentálja, tehát

$$|\lambda + \mu|_p = \lim_{n\to\infty} |x_n + y_n|_p \leq \limsup_{n\to\infty} \max\{|x_n|_p, |y_n|_p\} =$$

$$= \max\{\lim_{n\to\infty} |x_n|_p, \lim_{n\to\infty} |y_n|_p\} = \max\{|\lambda|_p, |\mu|_p\}.$$

Ezzel beláttuk, hogy nemarkhimédeszi abszolútértéket kaptunk. Már csak azt kell megmutatni, hogy ha veszünk egy $x \in \mathbb{Q}$ számot és egy ezt reprezentáló sorozatot, például (x)-t, akkor a két p-adikus abszolútérték definíció ugyanazt adja, azaz $|x|_p = |(x)|_p$, ami nyilvánvaló. □

3.17. Állítás. *Minden $0 \neq \lambda \in \mathbb{Q}_p$ számra létezik $n \in \mathbb{Z}$, hogy $|\lambda|_p = p^{-n}$.*

Bizonyítás. Legyen $(x_n) \in \mathcal{C}$ sorozat, ami λ-t reprezentálja, azaz $(x_n) \notin \mathcal{N}$, mert $\lambda \neq 0$. A 3.14. Állítás szerint létezik N, hogy $n, m \geq N$ esetén $|x_n|_p = |x_m|_p$. Definíció szerint $|\lambda|_p = \lim\limits_{n\to\infty} |x_n|_p = |x_N|_p$, azaz $x_N \in \mathbb{Q}$ p-adikus abszolútértéke, tehát p egy egész hatványa. □

3.18. Állítás. *A $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ beagyzásnál vett képe $\mathbb{Q}$-nak sűrű $\mathbb{Q}_p$-ben.*

Bizonyítás. Azt kell megmutatni, hogy minden $\mathbb{Q}_p$-beli szám minden környezete tartalmaz pontot $\mathbb{Q}$ képéből. Tehát legyen $\lambda \in \mathbb{Q}_p$ és $\varepsilon > 0$, ekkor elegendő belátni, hogy létezik konstans sorozat $B(\lambda, \varepsilon)$ nyílt gömbben.

Legyen (x_n) Cauchy sorozat, ami λ-t reprezentálja és $\varepsilon' < \varepsilon$. Létezik $N \in \mathbb{N}$ szám, amire $n, m \geq N$ esetén $|x_n - x_m| < \varepsilon'$. Legyen $y = x_N$ és tekintsük az (y) konstans sorozatot. Ekkor teljesül $(y) \in B(\lambda, \varepsilon)$ ((y)-t és (y) ekvivalenciaosztályát ugyanúgy jelöljük, de a szövegkörnyezetből kiderül, hogy mikor melyik), azaz $|\lambda - (y)| < \varepsilon$:

A $\lambda - (y) \in \mathbb{Q}_p$ számot reprezentálja $(x_n) - (y) = (x_n - y) = (x_n - x_N)$. Definíció szerint

$$|\lambda - (y)| = \lim_{n\to\infty} |x_n - x_N|,$$

de mivel $n \geq N$-re $|x_n - x_N| < \varepsilon'$, ezért

$$\lim_{n\to\infty} |x_n - x_N| \leq \varepsilon' < \varepsilon.$$

Tehát beláttuk, hogy $(y) \in B(\lambda, \varepsilon)$. □

3.19. Állítás. *$\mathbb{Q}_p$ teljes metrikus tér.*

Bizonyítás. 1) Legyen $\lambda_1, \lambda_2, \ldots$ $\mathbb{Q}_p$-beli Cauchy sorozat. (Vagyis $\mathbb{Q}$-beli Cauchy sorozatok ekvivalenciaosztályaiból álló Cauchy sorozat.) Mivel $\mathbb{Q}$ képe sűrű $\mathbb{Q}_p$-ben (3.18. Állítás), ezért létezik $y^{(n)} \in \mathbb{Q}$ racionális szám, amire $(y^{(n)}) \in B(\lambda_n, 1/n)$ (most is $(y^{(n)})$ és $(y^{(n)})$ ekvivalenciaosztályát ugyanúgy jelöljük), azaz $|\lambda_n - (y^{(n)})| < 1/n$.

2) $y^{(1)}, y^{(2)}, \ldots$ sorozat Cauchy $\mathbb{Q}$-ban: reprezentálja λ_k számot $(x_n^{(k)})$. Azt kell belátni, hogy minden $\varepsilon > 0$-hoz létezik $N \in \mathbb{N}$, hogy minden $n, m \geq N$ esetén $|y^{(n)} - y^{(m)}| < \varepsilon$. Legyen $\varepsilon > 0$. Mivel a (λ_k) sorozat Cauchy, ezért létezik $N_1 \in \mathbb{N}$, amire minden $n, m \geq N_1$ esetén $|\lambda_n - \lambda_m| < \varepsilon$, azaz $\lim\limits_{k\to\infty} |x_k^{(n)} - x_k^{(m)}| < \varepsilon$. Legyen $N = \max\{N_1, \lceil \frac{1}{\varepsilon} \rceil\}$. Ez bizonyítja, hogy $y^{(k)}$ Cauchy. Legyenek $n, m \geq N$, ekkor $|\lambda_n - (y^{(n)})| < 1/n$ és $|\lambda_m - (y^{(m)})| < 1/m$, azaz $\lim\limits_{k\to\infty} |x_k^{(n)} - y^{(n)}| < 1/n$ és $\lim\limits_{k\to\infty} |x_k^{(m)} - y^{(m)}| < 1/m$, illetve $\lim\limits_{k\to\infty} |x_k^{(n)} - x_k^{(m)}| < \varepsilon$. Létezik egy megfelelően nagy k, amire $|x_k^{(n)} - y^{(n)}| < 1/n$, $|x_k^{(m)} - y^{(m)}| < 1/m$ és $|x_k^{(n)} - x_k^{(m)}| < \varepsilon$ egyszerre teljesül. N választása miatt

$$n, m \geq N \geq \left\lceil \frac{1}{\varepsilon} \right\rceil \geq \frac{1}{\varepsilon},$$

azaz $\varepsilon \geq 1/n, 1/m$, tehát az előbb kiválasztott k-t használva

$$|y^{(n)} - y^{(m)}| \leq \max\{|y^{(n)} - x_k^{(n)}|, |x_k^{(n)} - x_k^{(m)}|, |x_k^{(m)} - y^{(m)}|\} < \varepsilon.$$

Tehát valóban Cauchy sorozat. Legyen $\lambda \in \mathbb{Q}_p$ az $y^{(1)}, y^{(2)}, \ldots$ $\mathbb{Q}$-beli Cauchy sorozat képe a $\mathcal{C}/\mathcal{N}$ faktorleképezésnél.

3) $\lim\limits_{n\to\infty} \lambda_n = \lambda$: azt kell megmutatni, hogy $\lim\limits_{n\to\infty} |\lambda_n - \lambda| = 0$.

$$|\lambda_n - \lambda| \leq \max\{|\lambda_n - (y^{(n)})|, |(y^{(n)}) - \lambda|\}$$

Az $y^{(n)}$ számok választása miatt $|\lambda_n - (y^{(n)})| < 1/n$, tehát $|\lambda_n - (y^{(n)})| \to 0$. Elég belátni, hogy $|(y^{(n)}) - \lambda| \to 0$, azaz $\lim\limits_{n\to\infty} \lim\limits_{m\to\infty} |y^{(n)} - y^{(m)}| = 0$. Legyen $\varepsilon > 0$, ehhez $N \in \mathbb{N}$, hogy $n, m \geq N$ esetén $|y^{(n)} - y^{(m)}| < \varepsilon$. Előbb m-ben, majd n-ben határértéket véve $\lim\limits_{n\to\infty} \lim\limits_{m\to\infty} |y^{(n)} - y^{(m)}| \leq \varepsilon$. Tehát megmutattuk, hogy $\lim\limits_{n\to\infty} \lambda_n = \lambda$.

4) Tetszőleges $\mathbb{Q}_p$-beli Cauchy sorozatra megmutattuk, hogy konvergens $\mathbb{Q}_p$-ben, tehát $\mathbb{Q}_p$ teljes. □

3.20. Tétel. *Minden $p \in \mathbb{Z}$ prímszámra létezik egy $\mathbb{Q}_p$ test és azon egy $|\cdot|_p$ nemarkhimédeszi abszolútérték, amire:*

(i) létezik egy $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ beágyazás, és $\mathbb{Q}$-nak a beágyazásnál vett képén $|\cdot|_p$ éppen a p-adikus abszolútérték;

(ii) $\mathbb{Q}$ képe a beágyazásnál sűrű $\mathbb{Q}_p$-ben;

(iii) $\mathbb{Q}_p$ teljes metrikus tér.

A $\mathbb{Q}_p$ test egyértelműen meghatározott egyértelmű abszolútérték tartó izomorfia erejéig az (i), (ii), (iii) tulajdonságok által.

Bizonyítás. Az egyetlen bizonyítandó az egyértelműség. Tegyük fel, hogy létezik K test ugyanezekkel a tulajdonságokkal. Vagyis létezik $i : \mathbb{Q} \hookrightarrow K$ beágyazás, ami megtartja az abszolútértéket. A beágyazás homomorfizmus és tekinthetjük úgy, mint $\mathbb{Q}_p$ egy sűrű részhalmazán definiált függvény. Ekkor i folytonos függvény, mert ha $\varepsilon > 0$, akkor $|x-y| < \varepsilon \Rightarrow |i(x)-i(y)| < \varepsilon$, mert $i(x-y) = i(x)-i(y)$. Egyértelműen terjeszthetjük ki i-t a teljes $\mathbb{Q}_p$ testre folytonosan, legyen ez $f : \mathbb{Q}_p \to K$.

Ekkor f homomorfizmus: legyen $x, y \in \mathbb{Q}_p$, ekkor léteznek $(x_n), (y_n) \subset \mathbb{Q}$ sorozatok, amikre $x_n \to x$, $y_n \to y$. Mivel i homomorfizmus, ezért

$$f(x_n + y_n) = i(x_n + y_n) = i(x_n) + i(y_n) = f(x_n) + f(y_n),$$

$$f(x_n y_n) = i(x_n y_n) = i(x_n) i(y_n) = f(x_n) f(y_n).$$

Az f függvény folytonos, így határértéket véve mindkét egyenlőségben

$$f(x+y) = \lim_{n\to\infty} f(x_n + y_n) = \lim_{n\to\infty} (f(x_n) + f(y_n)) = f(x) + f(y),$$

$$f(xy) = \lim_{n\to\infty} f(x_n x_n) = \lim_{n\to\infty} (f(x_n) f(y_n)) = f(x) f(y).$$

Megcserélve K és $\mathbb{Q}_p$ szerepét legyárthatunk egy $g : K \to \mathbb{Q}_p$ folytonos függvényt, ami kiterjesztése a $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ beágyazásnak. Ekkor $g \circ f : \mathbb{Q}_p \to \mathbb{Q}_p$ folytonos, mert két folytonos kompozíciója és $\mathbb{Q}$-t, mint $\mathbb{Q}_p$ részhalmazát tekintve $g \circ f$ az identitás függvény $\mathbb{Q}$-n. Mivel sűrű részhalmazon folytonos függvény egyértelműen terjed ki folytonosan, ezért $g \circ f$ az identitás függvény $\mathbb{Q}_p$-n is. Ugyanígy megmutatható, hogy $f \circ g$ pedig az identitás függvény K-n. Tehát f bijekció, mert van inverze, tehát akkor izomorfizmus.

Legyen $x \in \mathbb{Q}_p$, ekkor létezik $(x_n) \subset \mathbb{Q}$ sorozat, amire $x_n \to x$. Az abszolútérték folytonos függvény, mert tetszőleges abszolútértékre $\big||x| - |y|\big| \le |x-y|$, ahol a külső abszolútérték a szokásos abszolútérték $\mathbb{R}$-en. Ekkor $f(x_n) = i(x_n)$ és $|f(x_n)| = |i(x_n)| = |x_n|$, mert i megtartja az abszolútértéket. Mivel az abszolútérték $\mathbb{Q}_p$-n és K-n is folytonos, illetve f is folytonos, ezért $|f(x)| = |x|$, tehát f megőrzi az abszolútértéket.

Az izomorfia egyértelműsége azt jelenti, hogy $\mathbb{Q}_p$-nek nincs nemtriviális abszolútérték tartó automorfizmusa: ha $\varphi : \mathbb{Q}_p \to \mathbb{Q}_p$ nemtriviális abszolútérték tartó automorfizmus, akkor $f \circ \varphi : \mathbb{Q}_p \to K$ egy f-től különböző abszolútérték tartó izomorfia, mert $\varphi(x) \neq x$ valamilyen x-re, de ekkor $f(\varphi(x)) \neq f(x)$, különben f^{-1}-et ráalkalmazva ellentmondásra jutnánk. Ha $f, g : \mathbb{Q}_p \to K$ két különböző abszolútérték tartó izomorfizmus, akkor $g^{-1} \circ f : \mathbb{Q}_p \to \mathbb{Q}_p$ nemtriviális abszolútérték tartó automorfizmus, mert valamilyen x-re $f(x) \neq g(x)$ és ekkor $g^{-1}(f(x)) \neq x$.

Tegyük fel, hogy $\varphi : \mathbb{Q}_p \to \mathbb{Q}_p$ nem triviális abszolútérték tartó automorfizmus. Ekkor $f \circ \varphi : \mathbb{Q}_p \to K$ f-től különböző abszolútérték tartó izomorfizmus. $f \circ \varphi$ a $\mathbb{Q}$-n megegyezik i-vel, mert φ $\mathbb{Q}$-t fixen hagyja: $\varphi(1) = 1 \Rightarrow \varphi(n) = n$, ha $n \in \mathbb{N}$, $\varphi(-1)^2 = \varphi(1) = 1$, tehát $\varphi(-1) = -1$, mert injektív $\Rightarrow \varphi(n) = n$, ha $n \in \mathbb{Z}$, tehát $\varphi(x) = x$, ha $x \in \mathbb{Q}$. Mivel φ abszolútérték tartó, ezért folytonos ($|x-y| = |\varphi(x-y)| = |\varphi(x) - \varphi(y)|$). Tehát $f \circ \varphi$ folytonos függvény, mert két folytonos kompozíciója és $\mathbb{Q}$-n megegyezik i-vel, tehát az egyértelmű folytonos kiterjesztésből $f \circ \varphi = f$, azaz $\varphi = \mathrm{id}$. □

3.3. $\mathbb{Q}_p$ tulajdonságai

A továbbiakban $\mathbb{Q}_p$ konstrukcióját nem vesszük figyelembe, csak a 3.20. Tételben felsorolt tulajdonságok alapján vizsgáljuk, hiszen ezek a tulajdonságok egyértelműen meghatározzák. $\mathbb{Q}$-t azonosítjuk $\mathbb{Q}$ képével $\mathbb{Q}_p$-ben, azaz úgy tekintjük, hogy $\mathbb{Q} \subseteq \mathbb{Q}_p$. Megmutattuk a 3.17. Állításban, hogy $\mathbb{Q}$-n és $\mathbb{Q}_p$-n a $|\cdot|_p$ abszolútérték képe megegyezik, tehát megfogalmazhatjuk a következő állítást:

3.21. Állítás. *Minden $x \in \mathbb{Q}_p$, $x \neq 0$ esetén létezik $v_p(x) \in \mathbb{Z}$, amire $|x|_p = p^{-v_p(x)}$ és v_p a hasonló $\mathbb{Q}$-n lévő v_p függvény kiterjesztése.*

Az egész $\mathbb{Q}_p$-re $v_p(0) = +\infty$-nel ki tudjuk terjeszteni. Ha $x, y \in \mathbb{Q}_p$, akkor a kiterjesztett v_p függvényre is igaz $v_p(xy) = v_p(x) + v_p(y)$, mert $|xy|_p = |x|_p|y|_p$, illetve $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$, mert $|x+y|_p \leq \max\{|x|_p, |y|_p\}$.

3.22. Definíció. A

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

halmazt *p-adikus egészek*nek hívjuk.

$\mathbb{Z}_p$ megegyezik $\mathbb{Q}_p$ 0 középpontú zárt egységgömbjével, tehát $\mathbb{Z}_p$ nyílt-zárt halmaz.

3.23. Definíció. Azt mondjuk, hogy az *A lokális gyűrű*, ha A kommutatív gyűrű és egyetlen maximális ideálja van.

3.24. Állítás. *A p-adikus egészek egy lokális gyűrű, aminek a maximális ideálja $p\mathbb{Z}_p$. Továbbá:*

i) A $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ beágyazás képe sűrű, méghozzá minden $x \in \mathbb{Z}_p$ és $n \geq 1$ esetén létezik $\alpha \in \mathbb{Z}$, $0 \leq \alpha \leq p^n - 1$ egész, amire $|x - \alpha| \leq p^{-n}$. Az α egész ezekkel a tulajdonságokkal egyértelmű.

ii) Minden $x \in \mathbb{Z}_p$ esetén létezik α_n Cauchy sorozat, ami x-hez tart és

- *$\alpha_n \in \mathbb{Z}$ és $0 \leq \alpha_n \leq p^n - 1$;*
- *minden n-re $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.*

Ez az α_n sorozat egyértelműen meghatározott ezekkel a tulajdonságokkal.

Bizonyítás. $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| < 1\}$, mert $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| \leq p^{-1}\}$ és 3.17. Állítás miatt $|x| < 1 \Rightarrow |x| \leq p^{-1}$. $\mathbb{Z}_p$ a $\mathbb{Q}_p$ test részhalmaza, ezért elég megmutatni, hogy a műveletek nem vezetnek ki és akkor $\mathbb{Z}_p$ gyűrű lesz: legyenek $x, y \in \mathbb{Z}_p$, ekkor

$$|x \pm y| \leq \max\{|x|, |y|\} \leq 1,$$

$$|xy| = |x||y| \leq 1,$$

tehát $x \pm y, xy \in \mathbb{Z}_p$. $p\mathbb{Z}_p$ ideál: legyenek $x, y \in p\mathbb{Z}_p$, ekkor

$$|x \pm y| \leq \max\{|x|, |y|\} < 1,$$

tehát $x \pm y \in p\mathbb{Z}_p$, ha pedig $x \in p\mathbb{Z}_p$, $y \in \mathbb{Z}_p$, akkor

$$|xy| = |x||y| < 1,$$

tehát $xy \in p\mathbb{Z}_p$, vagyis $p\mathbb{Z}_p$ ideál. Maximális ideál, ehhez elég az, hogy ha $x \in \mathbb{Z}_p$, de $x \notin p\mathbb{Z}_p$, akkor x invertálható. Speciálisan $x \neq 0$, tehát létezik $x^{-1} \in \mathbb{Q}_p$. Ekkor

$$|x^{-1}| = |x|^{-1} = 1,$$

mert $|x| = 1$, hiszen $x \notin p\mathbb{Z}_p$, tehát $x^{-1} \in \mathbb{Z}_p$, azaz invertálható tetszőleges ilyen elem. Tegyük fel, hogy létezik $p\mathbb{Z}_p$-től különböző maximális ideál, legyen ez I. Ha $I \subset p\mathbb{Z}_p$, akkor I nem lehet maximális, mert $p\mathbb{Z}_p$ egy őt tartalmazó ideál. Tehát létezik $x \in \mathbb{Z}_p$, hogy $x \in I$, de $x \notin p\mathbb{Z}_p$, mert $I \neq p\mathbb{Z}_p$. Ekkor mint ahogy az előbb megmutattuk, $x^{-1} \in \mathbb{Z}_p$, de ekkor $x^{-1}x = 1 \in I$, mert I ideál, viszont ekkor $I = \mathbb{Z}_p$, tehát I nem lehet maximális.

i) Ha $x \in \mathbb{Z}$, akkor $v_p(x) \geq 0$, tehát $|x| \leq 1$, vagyis van értelme $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ beágyazásnak. Ha megmutatjuk *i*) második felét, akkor $\mathbb{Z}$ képe valóban sűrű $\mathbb{Z}_p$-ben, mert tetszőleges $x \in \mathbb{Z}_p$ minden $B(x, r)$ környezete tartalmaz $\mathbb{Z}$-beli pontot: $p^{-n} < r$, ekkor $\alpha \in \overline{B}(x, p^{-n}) \subset B(x, r)$. Tudjuk, hogy $\mathbb{Q}$ sűrű $\mathbb{Q}_p$-ben, tehát létezik $a/b \in \mathbb{Q}$ ($a, b \in \mathbb{Z}$, $(a, b) = 1$) racionális szám, amire

$$\left|x - \frac{a}{b}\right| \leq p^{-n}.$$

Ekkor

$$\left|\frac{a}{b}\right| \leq \max\left\{|x|, \left|x - \frac{a}{b}\right|\right\} \leq 1,$$

tehát $p \nmid b$, különben p osztaná a-t is, hogy teljesüljön $|a/b| \leq 1$, de akkor a és b nem lehetne relatív prím. Ha $p \nmid b$, akkor létezik $b' \in \mathbb{Z}$, amire $bb' \equiv 1 \pmod{p^n}$. Ekkor

$$\left|\frac{a}{b} - ab'\right| \leq p^{-n},$$

mert

$$\left|\frac{a}{b} - ab'\right| = \frac{|a - abb'|}{|b|} = |a - a(tp^n + 1)| = |at||p^n| = |at|p^{-n},$$

ahol t valamilyen egész és $p \nmid b$, ezért $|b| = 1$, illetve $|at| \leq 1$, mert at egész. Továbbá az is igaz, hogy ab' egész, amit redukálhatunk $\pmod{p^n}$, azaz legyen α az az egész, amire $0 \leq \alpha \leq p^n - 1$ és $\alpha \equiv ab' \pmod{p^n}$. Ez bizonyítja *i*)-t:

$$|x - \alpha| \leq \max\left\{\left|x - \frac{a}{b}\right|, \left|\frac{a}{b} - ab'\right|, |ab' - \alpha|\right\} \leq p^{-n},$$

mert $\alpha \equiv ab' \pmod{p^n}$ miatt létezik s egész, amire $ab' - \alpha = sp^n$, $|s| \leq 1$, tehát $|ab' - \alpha| = |sp^n| = |s|p^{-n} \leq p^{-n}$. Tegyük fel, hogy létezik β ugyanezekkel a tulajdonságokkal. Ekkor

$$|\alpha - \beta| \leq \max\{|x - \alpha|, |x - \beta|\} \leq p^{-n},$$

ekkor $p^n \mid \alpha - \beta$, ami csak úgy lehetséges, ha $\alpha = \beta$.

ii) Legyen $\alpha_n \in \mathbb{Z}$ olyan, amit az *i*) pontból kapunk $x \in \mathbb{Z}_p$ és $n \geq 1$-re. Ekkor $0 \leq \alpha_n \leq p^n - 1$, tehát az első pont teljesül. Az $|x - \alpha_n| \leq p^{-n}$ egyenlőtlenségből következik, hogy α_n x-hez tart és mivel konvergens, ezért Cauchy.

$$|\alpha_n - \alpha_{n-1}| \leq \max\{|x - \alpha_n|, |x - \alpha_{n-1}|\} \leq \max\{p^{-n}, p^{-(n-1)}\} = p^{-(n-1)},$$

tehát $p^{n-1} \mid \alpha_n - \alpha_{n-1}$, azaz teljesül a második pont is. (Ebből is következik, hogy Cauchy, mert $\lim\limits_{n\to\infty} |\alpha_n - \alpha_{n-1}| = 0$.) Tegyük fel, hogy létezik $(\beta_n) \subset \mathbb{Z}$ sorozat ugyanezekkel a

tulajdonságokkal, ami különbözik az előbb gyártott (α_n) sorozattól. Speciálisan $\alpha_k \neq \beta_k$ valamilyen k indexre. Ekkor $\alpha_n \not\equiv \beta_n \pmod{p^k}$ minden $n \geq k$-ra, mert ha $a \equiv b \pmod{p^n}$, akkor $a \equiv b \pmod{p^k}$, ha $k \leq n$, ezért $\alpha_n \equiv \alpha_{n-1} \equiv \cdots \equiv \alpha_k \pmod{p^k}$ és ugyanígy β-val, de $\alpha_k \not\equiv \beta_k \pmod{p^k}$. Tehát $p^k \nmid \alpha_n - \beta_n$, így $|\alpha_n - \beta_n| \geq p^{-(k-1)}$.

$$p^{-(k-1)} \leq |\alpha_n - \beta_n| \leq \max\{|x - \alpha_n|, |x - \beta_n|\}$$

Mivel $|x - \alpha_n| \leq p^{-n}$ és $p^{-(k-1)} > p^{-n}$, ezért $\max\{|x - \alpha_n|, |x - \beta_n|\} = |x - \beta_n|$ és így $p^{-(k-1)} \leq |x - \beta_n|$. De ekkor (β_n) nem tarthat x-hez. □

Ebből az állításból látszik, hogy a p-adikus egészek az egészek teljessé tétele, mert egy p-adikus egészhez tudunk tartani egészekből álló Cauchy sorozattal, ha pedig adott egy egészekből álló Cauchy sorozat, (x_n), akkor $|x_n| \leq 1$ és mivel $|\cdot|$ folytonos függvény, ezért ha x_n határértéke $x \in \mathbb{Q}_p$, akkor $|x| \leq 1$, tehát x p-adikus egész. Az is igaz, hogy $\mathbb{Z}_p$ a $\mathbb{Z}$ lezártja $\mathbb{Q}_p$-ben, mert $\mathbb{Z}$ sűrű $\mathbb{Z}_p$-ben.

3.25. Állítás. *$\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, azaz minden $x \in \mathbb{Q}_p$-re létezik $n \geq 0$ egész, amire $p^n x \in \mathbb{Z}_p$. Az $x \mapsto px$ képlettel definiált $\mathbb{Q}_p \to \mathbb{Q}_p$ függvény homeomorfizmus. A $p^n\mathbb{Z}_p$, $n \in \mathbb{Z}$ halmazok a $0 \in \mathbb{Q}_p$ egy környezetbázisát alkotják, amik az egész $\mathbb{Q}_p$-t fedik.*

Bizonyítás. Ha $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, akkor minden $x \in \mathbb{Q}_p$-re létezik $n \geq 0$ egész, illetve $a_0, \ldots, a_n \in \mathbb{Z}_p$ p-adikus egészek, hogy $x = a_n \frac{1}{p^n} + \cdots + a_0$. Tehát $p^n x = a_n + \cdots + a_0 p^n$, vagyis $p^n x \in \mathbb{Z}_p$ valóban. Ha minden $x \in \mathbb{Q}_p$-re $p^n x \in \mathbb{Z}_p$, akkor valamilyen $a_n \in \mathbb{Z}_p$-re $p^n x = a_n$, $x = a_n \frac{1}{p^n}$, tehát $\mathbb{Q}_p \subseteq \mathbb{Z}_p[1/p]$.

Legyen $x \in \mathbb{Q}_p$, ekkor létezik $v_p(x) \in \mathbb{Z}$. Ha $v_p(x) \geq 0$, akkor $x \in \mathbb{Z}_p$, tehát $n = 0$ megfelelő. Ha $v_p(x) < 0$, akkor $n = -v_p(x)$-re $p^n x \in \mathbb{Z}_p$,mert

$$v_p(p^{-v_p(x)} x) = -v_p(x) + v_p(x) = 0.$$

Az $x \mapsto px$ bijekció, az inverze $x \mapsto x/p$. Számmal való szorzás mindig folytonos, mert például p-re $|px - py|_p = |p|_p |x - y|_p = \frac{1}{p}|x - y|_p$.

$\mathbb{Z}_p$ nyílt halmaz, ami tartalmazza a 0-t, tehát környezet. Az $x \mapsto px$ függvény homeomorfizmus, ezért indukcióval belátható, hogy $p^n\mathbb{Z}_p$ nyílt halmaz minden $n \in \mathbb{Z}$-re, amik tartalmazzák 0-t, tehát környezetek. Az első állítás szerint minden $x \in \mathbb{Q}_p$-re létezik $n \geq 0$ egész, amire $p^n x \in \mathbb{Z}_p$, azaz $x \in p^{-n}\mathbb{Z}_p$, tehát

$$\mathbb{Q}_p = \bigcup_{n \in \mathbb{Z}} p^n \mathbb{Z}_p.$$

Legyen $U \ni 0$ nyílt halmaz, ekkor létezik $B(0, r)$ nyílt gömb, hogy $0 \in B(0, r) \subset U$. Legyen $n \in \mathbb{Z}$ olyan, hogy $p^{-n} < r$, ekkor $p^n\mathbb{Z}_p = \overline{B}(0, p^{-n}) \subset B(0, r)$. Tehát teljesül $0 \in p^n\mathbb{Z}_p \subset U$, vagyis valóban környezetbázis. □

3.26. Állítás. *Ha $x \in \mathbb{Q}_p$, akkor vegyük a legkisebb $n \in \mathbb{Z}$ számot, amire $p^n x \in \mathbb{Z}_p$. Ekkor $v_p(x) = -n$.*

Bizonyítás. Tegyük fel, hogy $p^n x \in \mathbb{Z}_p$, de $p^{n-1} x \notin \mathbb{Z}_p$, azaz $|p^n x|_p \leq 1$, de $|p^{n-1} x|_p > 1$. Használva v_p definícióját, $p^{-n - v_p(x)} \leq 1$, $p^{-n+1-v_p(x)} > 1$. Tehát $-n - v_p(x) \leq 0$, $-n + 1 - v_p(x) > 0$, ahonnan $-n \leq v_p(x) < -n + 1$, azaz $v_p(x) = -n$, mert $v_p(x)$ egész. □

3.27. Következmény. *Minden $n \geq 1$-re*

$$0 \to \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_p \xrightarrow{g} \mathbb{Z}/p^n\mathbb{Z} \to 0$$

egzakt, ahol $f(x) = p^n x$ a p^n-nel való szorzás, g pedig a 3.24. Állítás ii) pontjának megfelelően x-hez α-t rendeli. Speciálisan

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Az f és g függvények folytonosak, ha $\mathbb{Z}/p^n\mathbb{Z}$-re diszkrét topológiát rakunk.

Bizonyítás. $\mathrm{Ker}f = 0$, mert $\mathbb{Q}_p$ test nullosztómentes, ezért $p^n x = 0 \Rightarrow x = 0$. Ha $g(x) = 0$, akkor $|x| \leq p^{-n}$, azaz $x \in p^n\mathbb{Z}_p$, tehát $\mathrm{Ker}g = p^n\mathbb{Z}_p$. $\mathrm{Im}f = p^n\mathbb{Z}_p$. $\mathrm{Im}g = \mathbb{Z}/p^n\mathbb{Z}$, mert ha $x \in \mathbb{Z} \subset \mathbb{Z}_p$, akkor $g(x) = x$. A g függvény homomorfizmus: legyen $x, y \in \mathbb{Z}_p$, ekkor az kell, hogy $g(x+y) = g(x) + g(y)$ és $g(xy) = g(x)g(y)$, azaz $|(x+y) - (g(x) + g(y))| \leq p^{-n}$ és $|xy - g(x)g(y)| \leq p^{-n}$.

$$|(x+y) - (g(x) + g(y))| \leq \max\{|x - g(x)|, |y - g(y)|\} \leq p^{-n}$$

$$|xy - g(x)g(y)| \leq \max\{|xy - xg(y) - yg(x) + g(x)g(y)|, |xg(y) + yg(x) - 2g(x)g(y)|\} \leq$$
$$\leq \max\{|x - g(x)||y - g(y)|, |(x - g(x))g(y) + (y - g(y))g(x)|\}$$

Az első tag felülről becsülhető p^{-2n}-nel, a második pedig p^{-n}-nel, mert $g(x)$ és $g(y)$ egészek, tehát $|g(x)| \leq 1$, $|g(y)| \leq 1$ és

$$|(x - g(x))g(y) + (y - g(y))g(x)| \leq \max\{|x - g(x)||g(y)|, |y - g(y)||g(x)|\} \leq p^{-n}.$$

Mivel g homomorfizmus, így használhatjuk a homomorfizmus tételt, $\mathrm{Ker}g = p^n\mathbb{Z}_p$, $\mathrm{Im}g = \mathbb{Z}/p^n\mathbb{Z}$, így

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Az f függvény folytonos, mert számmal való szorzás folytonos. $\mathbb{Z}/p^n\mathbb{Z}$ minden részhalmaza nyílt, ezért azt kell belátni, hogy tetszőleges $U \subset \mathbb{Z}/p^n\mathbb{Z}$ halmazra $g^{-1}(U)$ nyílt $\mathbb{Z}_p$-ben. Ehhez elég, ha az egy elemű halmazok őseiről belátjuk, hogy nyíltak, mert akkor $g^{-1}(U)$ nyílt halmazok uniója lesz. Legyen $\alpha \in \mathbb{Z}/p^n\mathbb{Z}$, ekkor $g^{-1}(\alpha) = \overline{B}(\alpha, p^{-n}) \cap \mathbb{Z}_p$, ami nyílt $\mathbb{Z}_p$-ben, mert $\overline{B}(\alpha, p^{-n})$ nyílt $\mathbb{Q}_p$-ben. □

Az $a + p^n\mathbb{Z}_p$ halmazok, ahol $a \in \mathbb{Q}$, $n \in \mathbb{Z}$ az a középpontú, p^{-n} sugarú zárt gömbök, tehát nyílt-zárt halmazok. Mivel $\mathbb{Q}$ sűrű $\mathbb{Q}_p$-ben, ezért ezek a gömbök lefedik az egész $\mathbb{Q}_p$-t.

3.28. Állítás. *$\mathbb{Z}_p$ kompakt halmaz, $\mathbb{Q}_p$ lokálisan kompakt.*

Bizonyítás. Elég megmutatni, hogy $\mathbb{Z}_p$ kompakt: legyen $x \in \mathbb{Q}_p$, ekkor $x + \mathbb{Z}_p$ kompakt, mert a kompakt $\mathbb{Z}_p$ halmaz folytonos képe (x-szel való eltolás folytonos). Tehát minden $x \in \mathbb{Q}_p$-nek létezik kompakt környezete, $x + \mathbb{Z}_p$.

$\mathbb{Z}_p$ teljes, mert egy teljes tér zárt részhalmaza, tehát elég belátni, hogy teljesen korlátos. Legyen $\varepsilon > 0$ és ehhez $p^{-n} < \varepsilon$. A 3.27. Következmény szerint

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z},$$

azaz az $a + p^n\mathbb{Z}_p = \overline{B}(a, p^{-n})$ gömbök, ahol $a = 0, 1, \ldots, p^n - 1$ lefedik $\mathbb{Z}_p$-t. Ekkor $B(a, \varepsilon)$ gömbök is fedik $\mathbb{Z}_p$-t, ahol $a = 0, 1, \ldots, p^n - 1$, vagyis létezik véges ε-háló. □

Legyen x p-adikus egész. A 3.24.Állítás szerint létezik $(\alpha_n) \in \mathbb{Z}$ x-hez tartó sorozat, amire

- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$;
- $0 \leq \alpha_n \leq p^n - 1$.

Írjuk fel az α_n sorozatot p-es számrendszerben, azaz $\alpha_1 = b_1$ valamilyen $0 \leq b_1 \leq p-1$ egészre. Ekkor $\alpha_2 = \alpha_1 + sp = b_1 + sp$ valamilyen s egészre. Ha $s \geq p$, akkor $\alpha_2 \geq p^2$, ha pedig $s \leq -1$, akkor $\alpha_2 \leq -1$, ami szintén nem lehet, tehát $0 \leq s \leq p-1$. Legyen $s = b_2$. Ezt folytatva azt kapjuk, hogy

$$\begin{aligned} \alpha_1 &= b_1 & 0 \leq b_1 \leq p-1 \\ \alpha_2 &= b_1 + b_2 p & 0 \leq b_2 \leq p-1 \\ \alpha_3 &= b_1 + b_2 p + b_3 p^2 & 0 \leq b_3 \leq p-1 \end{aligned}$$

3.29. Lemma. *Ha $x \in \mathbb{Z}_p$, akkor az előző*

$$b_1 + b_2 p + b_3 p^2 + \dots$$

sorozat tart az x-hez.

Bizonyítás. Ez a sorozat pontosan akkor tart x-hez, ha $b_1 + b_2 p + b_3 p^2 + \dots + b_n p^{n-1}$ tart az x-hez, ez azonban éppen α_n, amiről pedig tudjuk, hogy tart x-hez. □

3.30. Lemma. *Minden x p-adikus egész felírható*

$$x = b_1 + b_2 p + b_3 p^2 + \dots$$

alakban, ahol $0 \leq b_i \leq p-1$ és ez a felírás egyértelmű.

Bizonyítás. Az előző Lemma alapján megkapható a felírás. Ha ez nem lenne egyértelmű, akkor két különböző felírás alapján kapott részletösszeg-sorozatok különböző α_n sorozatok lennének, amik teljesítik 3.24. Állítás *ii)* pontjának feltételeit, ami nem lehet, mert egyetlen ilyen sorozat van. □

3.31. Következmény. *Minden x p-adikus szám felírható*

$$x = b_{-n_0} p^{-n_0} + b_{-n_0+1} p^{-n_0+1} + \dots = \sum_{n \geq -n_0} b_n p^n$$

alakban, ahol $0 \leq b_i \leq p-1$ és $-n_0 = v_p(x)$. Ez az előállítás egyértelmű.

Bizonyítás. Tudjuk, hogy $p^{-v_p(x)} x \in \mathbb{Z}_p$, tehát ez felírható

$$p^{-v_p(x)} x = b_{v_p(x)} + b_{v_p(x)+1} p + b_{v_p(x)+2} p^2 + \dots$$

alakban. Szorozva $p^{v_p(x)}$-nel

$$x = b_{v_p(x)} p^{v_p(x)} + b_{v_p(x)+1} p^{v_p(x)+1} + b_{v_p(x)+2} p^{v_p(x)+2} + \dots \ .$$

Ha ez az előállítás nem lenne egyértelmű, akkor $p^{-v_p(x)} x \in \mathbb{Z}_p$ előállítása sem lenne egyértelmű, ami az előző Lemmának ellentmondana. □

3.32. Definíció. A *p-adikus egységek* a $\mathbb{Z}_p$ gyűrű egységei, azaz a $\mathbb{Z}_p$-ben invertálható elemek. A p-adikus egységek halmazát $\mathbb{Z}_p^\times$-tel jelöljük.

Ha $x \in \mathbb{Z}_p$ invertálható $\mathbb{Z}_p$-ben, akkor $|x| \leq 1$ és $|x^{-1}| = |x|^{-1} \leq 1$, tehát $|x| = 1$. Ha $|x| = 1$, akkor $|x^{-1}| = 1$, azaz $x^{-1} \in \mathbb{Z}_p$. Tehát $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x| = 1\}$.

3.4. Hensel Lemma

$\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$ alapján $\mathbb{Z}_p$-ben is értelmezhetjük a $\pmod{p^n}$ maradékosztályokat. Ha $\alpha, \beta \in \mathbb{Z}_p$, akkor ugyanazt jelentik $\alpha \equiv \beta \pmod{p^n}$, $\alpha \equiv \beta \pmod{p^n\mathbb{Z}_p}$, $\alpha - \beta \in p^n\mathbb{Z}_p$, $|\alpha - \beta| \leq p^{-n}$, hiszen $p^n \mid \alpha - \beta$ azt jelenti, hogy $\frac{\alpha-\beta}{p^n} \in \mathbb{Z}_p$, azaz $\left|\frac{\alpha-\beta}{p^n}\right| = |\alpha - \beta|p^n \leq 1$.

3.33. Tétel (Hensel Lemma I.)**.** *Legyen $F(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}_p[X]$, tegyük fel, hogy létezik $\alpha_1 \in \mathbb{Z}_p$, amire*

$$F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$

és

$$F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

ahol $F'(X)$ az $F(X)$ polinom formális deriváltja. Ekkor egyértelműen létezik $\alpha \in \mathbb{Z}_p$, amire $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ és $F(\alpha) = 0$.

Bizonyítás. Gyártunk egy $\alpha_1, \alpha_2, \ldots$ sorozatot a következő tulajdonságokkal:

i) $F(\alpha_n) \equiv 0 \pmod{p^n}$,

ii) $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$

minden $n \geq 1$-re. Az α_1 a Tétel feltételei szerint létezik, amire $F(\alpha_1) \equiv 0 \pmod{p}$. Keressük α_2-t a *ii)* feltétel miatt $\alpha_2 = \alpha_1 + b_1p$ alakban, ahol $b_1 \in \mathbb{Z}_p$. Az F polinomot formális Taylor sorba fejthetjük, így

$$F(\alpha_2) = F(\alpha_1 + b_1p) = F(\alpha_1) + F'(\alpha_1)b_1p + \ldots,$$

ahol a $\ldots$ tagok oszthatók p^2-tel, ezért

$$F(\alpha_2) \equiv F(\alpha_1) + F'(\alpha_1)b_1p \pmod{p^2}.$$

Mivel $F(\alpha_1) \equiv 0 \pmod{p}$, ezért $F(\alpha_1) = px$ valamilyen $x \in \mathbb{Z}_p$-re és mivel olyan α_2-t keresünk, amire $F(\alpha_2) \equiv 0 \pmod{p^2}$, ezért

$$px + F'(\alpha_1)b_1p \equiv 0 \pmod{p^2}.$$

Osszunk p-vel

$$x + F'(\alpha_1)b_1 \equiv 0 \pmod{p}.$$

Az $F'(\alpha_1)$ invertálható $\mathbb{Z}_p$-ben, mivel $p \nmid F'(\alpha_1)$, azaz $\frac{F'(\alpha_1)}{p} \notin \mathbb{Z}_p$. Ez ekvivalens azzal, hogy $\left|\frac{F'(\alpha_1)}{p}\right| = |F'(\alpha)|p > 1 \Leftrightarrow |F'(\alpha_1)| > 1/p$. Mivel $F'(\alpha_1) \in \mathbb{Z}_p$, ezért $|F'(\alpha_1)| = 1$, tehát invertálható.

$$b_1 \equiv -x(F'(\alpha_1))^{-1} \pmod{p}$$

Egy ilyen b_1-re $\alpha_2 = \alpha_1 + b_1p$ teljesíti *i)*-t és *ii)*-t. $F'(\alpha_2) \not\equiv 0 \pmod{p}$, mert $F'(\alpha_1 + b_1p)$ formális Taylor sorba fejtéséből látszik, hogy $F'(\alpha_2) \equiv F'(\alpha_1) \pmod{p}$.

Tegyük fel, hogy legyártottuk $\alpha_1, \alpha_2, \ldots, \alpha_n$-et *i)* és *ii)* tulajdonságokkal, illetve $F'(\alpha_n) \not\equiv 0 \pmod{p}$. Csináljuk ugyanazt, mint α_2 keresésénél. Legyen $\alpha_{n+1} = \alpha_n + b_np^n$, ekkor

$$F(\alpha_{n+1}) = F(\alpha_n + b_np^n) \equiv F(\alpha_n) + F'(\alpha_n)b_np^n \pmod{p^{n+1}},$$

mert $2n \geq n+1$. $F(\alpha_n) = p^n x$ valamilyen $x \in \mathbb{Z}_p$-re és $F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}}$, ezért

$$p^n x + F'(\alpha_n) b_n p^n \equiv 0 \pmod{p^{n+1}}.$$

Osszunk p^n-nel

$$x + F'(\alpha_n) b_n \equiv 0 \pmod{p}.$$

Invertálható $F'(\alpha_n)$ $\mathbb{Z}_p$-ben, tehát

$$b_n \equiv -x(F'(\alpha_n))^{-1} \pmod{p}.$$

Ha $F'(\alpha_{n+1})$-et Taylor sorba fejtjük, akkor abból látszik, hogy $F'(\alpha_{n+1}) \equiv F'(\alpha_n) \pmod{p}$, tehát $F'(\alpha_{n+1}) \not\equiv 0 \pmod{p}$.

Teljes indukcióval elkészítettük az $\alpha_1, \alpha_2, \ldots$ sorozatot $\mathbb{Z}_p$-ben az $i)$ és $ii)$ tulajdonságokkal. Ez a sorozat Cauchy a $ii)$ miatt, mert $|\alpha_{n+1} - \alpha_n| \leq p^{-n}$. Létezik $\mathbb{Q}_p$-ben limesze, legyen ez α. Mivel $|\alpha_n| \leq 1$ és $|\cdot|$ folytonos, ezért $|\alpha| \leq 1$, tehát $\alpha \in \mathbb{Z}_p$. Az $F(X)$ polinom folytonos függvény, ezért $\lim\limits_{n\to\infty} F(\alpha_n) = F(\alpha)$. Ugyanakkor $|F(\alpha_n)| \leq p^{-n}$, tehát $F(\alpha_n) \to 0$, azaz $F(\alpha) = 0$. A sorozat konstrukciója alapján $\alpha_n = \alpha_1 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1}$, tehát $\alpha_n - \alpha_1 \in p\mathbb{Z}_p$. Az $(\alpha_n - \alpha_1) \subset p\mathbb{Z}_p$ sorozat $(\alpha - \alpha_1)$-hez tart, ezért $\alpha - \alpha_1 \in p\mathbb{Z}_p$, mert $p\mathbb{Z}_p$ zárt halmaz, tehát $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$.

Tegyük fel, hogy létezik $\alpha \neq \beta \in \mathbb{Z}_p$, $\beta \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$, $F(\beta) = 0$ másik megoldás. Ekkor $\alpha - \beta \neq 0$, tehát létezik inverze $\mathbb{Q}_p$-ben

$$0 = \frac{F(\alpha) - F(\beta)}{\alpha - \beta} = a_1 + a_2(\alpha + \beta) + \cdots + a_n(\alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \alpha\beta^{n-2} + \beta^{n-1}).$$

Ez azonban nem lehetséges, mert $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ és $\beta \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$, tehát

$$0 \equiv a_1 + 2a_2\alpha_1 + \cdots + na_n\alpha_1 = F'(\alpha_1) \pmod{p\mathbb{Z}_p},$$

ami ellentmond a Tétel feltételeivel. □

3.34. Definíció. Legyenek $g(X), h(X) \in \mathbb{Z}_p[X]$ polinomok. Ekkor legyenek $\bar{g}(X)$, $\bar{h}(X) \in \mathbb{F}_p[X]$ azok a polinomok, amiket úgy kapunk, hogy redukáljuk $g(X)$-et és $h(X)$-et modulo p. Azt mondjuk, hogy $g(X)$ és $h(X)$ *relatív prímek modulo* p, ha $(\bar{g}, \bar{h}) = 1$ $\mathbb{F}_p[X]$-ben, azaz a legnagyobb közös osztójuk a konstans 1 polinom.

3.35. Megjegyzés. A $g(X)$ és $h(X)$ relatív prímek modulo p pontosan azt jelenti, hogy léteznek $a(X), b(X) \in \mathbb{Z}_p[X]$ polinomok, amikre

$$g(X)a(X) + h(X)b(X) \equiv 1 \pmod{p}.$$

(Polinomok kongruenciáját együtthatónként nézzük.)

3.36. Tétel (Hensel Lemma II.)**.** *Legyen $f(X) \in \mathbb{Z}_p[X]$ polinom és tegyük fel, hogy léteznek $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$ polinomok, amikre*

- *$g_1(X)$ 1-főegyütthatós;*
- *$g_1(X)$ és $h_1(X)$ relatív prímek modulo p;*
- *$f(X) \equiv g_1(X)h_1(X) \pmod{p}$.*

Ekkor léteznek $g(X), h(X) \in \mathbb{Z}_p[X]$ polinomok, amikre

- $g(X)$ 1-*főegyüttható;*
- $g_1(X) \equiv g(X) \pmod{p}$ *és* $h_1(X) \equiv h(X) \pmod{p}$*;*
- $f(X) = g(X)h(X)$.

Bizonyítás. Legyen $\deg f(X) = d$ és $\deg g_1(X) = m$. Ekkor $\deg h_1(X) \leq d - m$. ($f(X)$ főegyüttható lehet osztható p-vel.) Legyártjuk polinomok egy-egy sorozatát, $g_n(X) \in \mathbb{Z}_p[X]$ és $h_n(X) \in \mathbb{Z}_p[X]$ sorozatok úgy, hogy

i) g_n 1-főegyüttható és m-edfokú;

ii) $g_{n+1} \equiv g_n \pmod{p^n}$ és $h_{n+1} \equiv h_n \pmod{p^n}$;

iii) $f \equiv g_n h_n \pmod{p^n}$.

(Nem írjuk ki a polinomok argumentumába X-et, hogy átláthatóbb legyen, de p nem polinomot, hanem a p prímet fogja jelölni.)

Keressük g_2-t és h_2-t *ii)* miatt $g_2 = g_1 + pr_1$ és $h_2 = h_1 + ps_1$ alakban, ahol $r_1(X), s_1(X) \in \mathbb{Z}_p[X]$ polinomok. Az *i)* ponttal később foglalkozunk, oldjuk meg *iii)*-t:

$$f \equiv g_2 h_2 = (g_1 + pr_1)(h_1 + ps_1) =$$

$$= g_1 h_1 + p(g_1 s_1 + h_1 r_1) + p^2 r_1 s_1 \equiv g_1 h_1 + p(g_1 s_1 + h_1 r_1) \pmod{p^2}.$$

Mivel $f \equiv g_1 h_1 \pmod{p}$, ezért létezik $k_1(X) \in \mathbb{Z}_p[X]$ polinom, amire $f - g_1 h_1 = pk_1$. Ezt beírva

$$pk_1 \equiv p(g_1 s_1 + h_1 r_1) \pmod{p^2},$$

osszunk p-vel

$$k_1 \equiv g_1 s_1 + h_1 r_1 \pmod{p}.$$

Ezt kell megoldani r_1-re és s_1-re. Feltettük, hogy g_1 és h_1 relatív prímek modulo p, ezért léteznek $a(X), b(X) \in \mathbb{Z}_p[X]$ polinomok, amikre $g_1 a + h_1 b \equiv 1 \pmod{p}$. Vegyük a következő két polinomot: $\tilde{r}_1 = bk_1$, $\tilde{s}_1 = ak_1$. Ez a pár megoldja a kongruenciát, de az *i)* pontot nem tudjuk biztosan. Osszuk el $\tilde{r}_1$-et g_1-gyel, azaz $\tilde{r}_1 = g_1 q + r_1$, ahol $q(X), r_1(X) \in \mathbb{Z}_p[X]$ polinomok és $\deg r_1 < \deg g_1$. Legyen $s_1 = \tilde{s}_1 + h_1 q$. Az így kapott r_1 és s_1 megfelelő lesz:

$$g_1 s_1 + h_1 r_1 = g_1(\tilde{s}_1 + h_1 q) + h_1(\tilde{r}_1 - g_1 q) = g_1 \tilde{s}_1 + h_1 \tilde{r}_1 \equiv k_1 \pmod{p},$$

illetve mivel $\deg r_1 < \deg g_1$, ezért $g_2 = g_1 + pr_1$ foka megegyezik g_1 fokával, m-mel és g_2 főegyüttható megegyezik g_1 főegyütthatójával, azaz 1. Hogy folytatni tudjuk, g_2 és h_2 relatív prímek modulo p, mert $g_2 \equiv g_1 \pmod{p}$ és $h_2 \equiv h_1 \pmod{p}$.

Tegyük fel, hogy $g_1, g_2, \ldots, g_n$ és $h_1, h_2, \ldots, h_n$ polinomokat legyártottuk *i)*, *ii)*, *iii)* tulajdonságokkal és g_n és h_n relatív prímek modulo p. Legyen *ii)* miatt $g_{n+1} = g_n + p^n r_n$ és $h_{n+1} = h_n + p^n s_n$ valamilyen $r_n(X), s_n(X) \in \mathbb{Z}_p[X]$ polinomokra.

$$f \equiv g_{n+1} h_{n+1} = (g_n + p^n r_n)(h_n + p^n s_n) =$$

$$= g_n h_n + p^n(g_n s_n + h_n r_n) + p^{2n} r_n s_n \equiv g_n h_n + p^n(g_n s_n + h_n r_n) \pmod{p^{n+1}}$$

Valamilyen $k_n(X) \in \mathbb{Z}_p[X]$ polinomra $f - g_n h_n = p^n k_n$, ekkor

$$p^n k_n \equiv p^n(g_n s_n + h_n r_n) \pmod{p^{n+1}},$$
$$k_n \equiv g_n s_n + h_n r_n \pmod{p}.$$

Relatív prímség miatt léteznek $a(X), b(X) \in \mathbb{Z}_p[X]$ polinomok, amikre $g_1 a + h_1 b \equiv 1 \pmod{p}$, ekkor legyen $\tilde{r}_n = bk_n$, $\tilde{s}_n = ak_n$. Osszuk el maradékosan $\tilde{r}_n$-et g_1-gyel, azaz $\tilde{r}_n = g_1 q + r_n$, ahol $\deg r_n < \deg g_1 = m$. Legyen $s_n = \tilde{s}_n + h_1 q$, ekkor r_n, s_n megfelelő:

$$g_n s_n + h_n r_n = g_n(\tilde{s}_n + h_1 q) + h_n(\tilde{r}_n - g_1 q) =$$
$$= g_n \tilde{s}_n + h_n \tilde{r}_n + (g_n h_1 - h_n g_1) q \equiv k_n \pmod{p},$$

mert $g_n \equiv g_{n-1} \pmod{p^n} \Rightarrow g_n \equiv g_{n-1} \pmod{p}$, tehát $g_n \equiv g_1 \pmod{p}$ és $h_n \equiv h_0 \pmod{p}$, illetve $\deg g_{n+1} = \deg(g_n + p^n r_n) = \deg g_n = m$ és ezért g_{n+1} főegyütthatója $= g_n$ főegyütthatója, ami 1. A g_{n+1} és h_{n+1} polinomok relatív prímek modulo p, mert $g_{n+1} \equiv g_n \pmod{p^n} \Rightarrow g_{n+1} \equiv g_n \pmod{p}$ és ugyanígy h-ra és g_n és h_n relatív prímek modulo p. Teljes indukcióval legyárthatóak a $g_1, g_2, \ldots$ és $h_1, h_2, \ldots$ sorozatok az i), ii) és iii) tulajdonságokkal.

Mivel $g_{n+1} \equiv g_n \pmod{p^n}$, ezért (g_n) Cauchy sorozat abban az értelemben, hogy az együtthatók sorozatai Cauchy sorozatok. Legyen a limesze $g(X) \in \mathbb{Z}_p[X]$ (mint az előző bizonyításban $\mathbb{Z}_p$-beliek Cauchy sorozata $\mathbb{Z}_p$-belihez tart). Ekkor g 1-főegyütthatós, m-edfokú, mert mindegyik g_n is ilyen.

A sorozatok legyártásánál valójában s_n-ből elhagyhatjuk a p-vel osztható tagokat, mert csak modulo p fontos, tehát feltehetjük, hogy megegyezik a modulo p fokával. Indukcióval bizonyíthatjuk, hogy $\deg h_n \leq d - m$. Feltétel szerint h_1-re igaz, tegyük fel, hogy n-re igaz. Ekkor mivel $p^n k_n = f - g_n h_n$, ezért $\deg k_n \leq d$, mert $\deg f = d$, $\deg g_n = m$ és $\deg h_n \leq d - m$. Viszont ebben az esetben $\deg(k_n - h_n r_n) \leq d$, mert $\deg k_n \leq d$, $\deg h_n \leq d - m$ és $\deg r_n < \deg g_1 = m$. Igaz a $k_n - h_n r_n \equiv g_n s_n \pmod{p}$ kongruencia, tehát s_n modulo p foka $\leq d - m$, hiszen $\deg g_n = m$ és a főegyütthatója 1. Mivel s_n foka megegyezik a modulo p fokával, ezért $\deg s_n \leq d - m$, tehát $\deg h_{n+1} = \deg(h_n + p^n s_n) \leq d - m$. Indukcióval ezért azt kaptuk, hogy a h_n polinomok véges fokúak, tehát ugyanúgy, mint a g_n polinomokra, vehetjük a limeszt, azaz $\lim h_n(X) = h(X) \in \mathbb{Z}_p[X]$.

A iii) pont miatt $g_n h_n \to f$, mert minden együtthatóra az együtthatók f megfelelő együtthatójához tartanak, illetve $g_n h_n \to gh$, mert a polinomok véges hosszúak, így kibontva egyesével tartanak a megfelelő együttható sorozatok a megfelelő együtthatókhoz. Vagyis $f = gh$, mert nem lehet két limesz.

Kijött, hogy $g_n \equiv g_1 \pmod{p}$, tehát ha g_n X^k változójának együtthatója a_{nk}, g-nek pedig a_k, akkor $|a_{nk} - a_{1k}| \leq p^{-1}$ és határértéket véve $|a_k - a_{1k}| \leq p^{-1}$. Tehát $a_k \equiv a_{1k} \pmod{p}$, azaz $g \equiv g_1 \pmod{p}$ és ezt a h_n sorozatra is elmondhatjuk. Másképpen úgy is látszik, hogy g_n-et úgy gyártjuk le g_1-ből kiindulva, hogy p-vel osztható polinomokat adunk hozzá. □

4. $\mathbb{Q}_p$ bővítései

4.1. Véges bővítések

4.1. Tétel. *Legyen $K \leq L$ szeparábilis véges bővítés. Ekkor létezik egy $L \leq M$ test, amire $K \leq M$ normális bővítés és M a legkisebb ilyen tulajsonságú test, továbbá M egyértelmű izomorfia erejéig.*

Bizonyítás. Mivel L/K szeparábilis véges bővítés, ezért létezik $\alpha \in L$, hogy $L = K(\alpha)$. Legyen $m(X) \in K[X]$ az α minimálpolinomja K fölött. Legyen $\overline{L}$ az L algebrai lezártja, ekkor $m(X)$ minden gyöke benne van $\overline{L}$-ben. Legyenek ezek a gyökök $\beta_1, \ldots, \beta_n$. Legyen $M = L(\beta_1, \ldots, \beta_n)$, ez lesz a megfelelő test:

M/K normális bővítés: Mivel α az m gyöke, ezért α a β-k valamelyike, tehát $L(\beta_1, \ldots, \beta_n) = K(\beta_1, \ldots, \beta_n)$. Vagyis M éppen m polinom felbontási teste és m szeparábilis polinom, mert L/K szeparábilis bővítés, tehát M/K Galois, de akkor normális is.

M legkisebb ilyen tulajdonságú: Tegyük fel, hogy M' egy test, amire $L \leq M'$ és M'/K normális. Mivel $L \leq M'$, ezért $\alpha \in M'$. M'/K normális, tehát m minimálpolinom (ami irreducibilis) minden gyöke benne van M'-ben, mert α, ami az egyik gyöke benne van M'-ben. Ezek a gyökök éppen $\beta_1, \ldots, \beta_n$, tehát $L(\beta_1, \ldots, \beta_n) \leq M'$, azaz $M \leq M'$.

M egyértelmű izomorfia erejéig: A konstrukcióból látszik. Legyen $\tilde{M}$ egy másik test, amire $L \leq \tilde{M}$, $\tilde{M}/K$ normális és ha $L \leq M'$ és M'/K normális, akkor $\tilde{M} \leq M'$. Az eddigi jelölésekkel gyártsuk le M'-t, mint az m polinom egy felbontási teste egy esetleg másik, de izomorf $\overline{L}_1$ algebrai lezárt testben és legyen ez a felbontási test M'. Ekkor α-t tartalmazza $\tilde{M}$, ezért minden gyökét m-nek, tehát M'-t is, de másrészt $\tilde{M}$ minimalitása miatt $\tilde{M} \leq M'$, azaz $\tilde{M} = M'$. Az algebrai lezártak izomorfiája miatt $\tilde{M}$ és M is izomorf, mert a gyökök megfeleltethetők egymásnak. □

4.2. Definíció. A 4.1. Tételbeli M testet az L/K normális lezártjának hívjuk.

Legyen K test a $\mathbb{Q}_p$ egy véges bővítése, azaz K végesdimenziós vektortér $\mathbb{Q}_p$ felett. Szeretnénk kiterjeszteni a p-adikus abszolútértéket K-ra, azaz egy $|\cdot| : K \to \mathbb{R}_+$ függvényt szeretnénk konstruálni, amire

(i) $|x| = 0$ pontosan akkor, ha $x = 0$;

(ii) $|xy| = |x||y|$ minden $x, y \in K$;

(iii) $|x + y| \leq |x| + |y|$ minden $x, y \in K$;

(iv) $|\lambda| = |\lambda|_p$, ha $\lambda \in \mathbb{Q}_p$.

Egy ilyen abszolútérték nemarkhimédeszi lesz a 2.9. Tétel miatt, mivel $\mathbb{Z} \subset \mathbb{Q}_p$ és a *(iv)*-es tulajdonság miatt $\mathbb{Q}_p$-n megegyezik egy nemarkhimédeszi abszolútértékkel. Azt is észrevehetjük, hogy $|\cdot|$ egy norma lesz a K vektortéren, mert a *(ii)*-es tulajdonságban $\lambda \in \mathbb{Q}_p$, $x \in K$-ra $|\lambda x| = |\lambda||x|$.
Ismert a következő tétel:

4.3. Tétel. *Legyen k test, amin adott egy abszolútérték, amire nézve k teljes metrikus tér. Legyen továbbá V végesdimenziós vektortér k felett. Ekkor bármely két norma ekvivalens V-n és V Banach-tér bármely normára nézve.*

4.4. Állítás. *Legyen $K/\mathbb{Q}_p$ véges bővítés. Ha létezik egy $|\cdot|$ abszolútérték K-n, ami kiterjesztése a p-adikus abszolútértéknek $\mathbb{Q}_p$-n, akkor*

(i) K teljes metrikus tér;

(ii) vehetjük a limeszét egy sorozatnak K-ban úgy, hogy vesszük a limeszét az együtthatóknak egy tetszőleges adott $\{x_1, \ldots, x_n\}$ K-beli bázis szerint, mint $\mathbb{Q}_p$-vektortér.

Tehát K topológiája, amit $|\cdot|$ indukál, az az egyértelmű topológia K-n, mint véges $\mathbb{Q}_p$-vektortér, ezért független az abszolútérték választásától.

Bizonyítás. A 4.3. Tétel szerint K teljes metrikus tér. Minden K-beli elem egyértelműen felírható $a_1x_1 + \cdots + a_nx_n$ alakban, ahol $x_1, \ldots, x_n$ a bázis (ii)-ben. Definiálhatunk egy normát K-n:

$$\|a_1x_1 + \cdots + a_nx_n\| = \max_{1\le i\le n} |a_i|_p.$$

Ekkor (ii) azt jelenti, hogy az $|\cdot|$ abszolútérték ekvivalens a $\|\cdot\|$ normával, ami a 4.3. Tétel miatt bármely két normára igaz. □

4.5. Következmény. *Legfeljebb egy abszolútérték van K-n, ami kiterjesztése a $\mathbb{Q}_p$-n lévő p-adikus abszolútértéknek.*

Bizonyítás. Tegyük fel, hogy $|\cdot|$ és $\|\cdot\|$ is abszolútértékek K-n, és mindkettő a $\mathbb{Q}_p$-n lévő p-adikus abszolútérték kiterjesztése. Ekkor $|\cdot|$ és $\|\cdot\|$ nem csak abszolútértékek, hanem normák is K-n. $\mathbb{Q}_p$ teljes metrikus tér a p-adikus abszolútértékre nézve, ezért 4.3. Tétel miatt $|\cdot|$ és $\|\cdot\|$ ekvivalens normák K-n, tehát ugyanazt a topológiát indukálják. De ekkor definíció szerint $|\cdot|$ és $\|\cdot\|$ mint abszolútértékek is ekvivalensek. (A nyílt gömbök norma és abszolútérték értelemben ugyanazok a halmazok.) A 3.2. Állítás miatt tehát létezik $\alpha > 0$ valós szám, amire $|x| = \|x\|^\alpha$ minden $x \in K$-ra. Azonban a $\mathbb{Q}_p$ halmazon megegyeznek, tehát $\alpha = 1$ (például $x = p$ helyettesítéssel adódik), azaz $|\cdot|$ és $\|\cdot\|$ megegyezik az egész K-n. □

Tegyük fel, hogy $\mathbb{Q}_p \le K \le L$ véges bővítések, amiken adott egy $|\cdot|_K$ és $|\cdot|_L$ abszolútérték, amik a $\mathbb{Q}_p$ p-adikus abszolútértékének kiterjesztései. A $|\cdot|_L$ megszorítása K-ra egy abszolútérték K-n, ami $\mathbb{Q}_p$ p-adikus abszolútértékének kiterjesztése. Ha van ilyen abszolútérték, akkor beláttuk, hogy csak egy ilyen lehet, tehát $|x|_K = |x|_L$ ha $x \in K$. Vagyis egy x abszolútértéke nem függ attól, hogy milyen nagyobb testben nézzük.
Elegendő megkonstruálni egy abszolútértéket K-n, ami a p-adikus abszolútérték kiterjesztése és akkor mondhatjuk azt, hogy az lesz *a* p-adikus abszolútérték K-n.

4.6. Definíció. Az

$$N_{K/F} : K \to F$$

függvényt úgy hívjuk, hogy *norma K-ról F-re*, ha teljesíti a következő (később megmutatjuk, hogy ekvivalens) definíciók valamelyikét:

(i) Legyen $\alpha \in K$, és tekintsük K-t, mint véges F-vektortér. Az α-val való szorzás egy $K \to K$ F-lineáris leképezés. Ekkor $N_{K/F}(\alpha)$ legyen az α-val való szorzás determinánsa.

(ii) Legyen $\alpha \in K$, ekkor $F(\alpha)$ a K részteste. Legyen $r = |K : F(\alpha)|$ a bővítés foka, és

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in F[X]$$

az α minimálpolinomja F fölött. Ekkor legyen $N_{K/F}(\alpha) = (-1)^{nr}a_0^r$.

(iii) Tegyük fel, hogy K/F Galois. Ekkor $N_{K/F}(\alpha)$ legyen a $\sigma(\alpha)$ számok szorzata, ahol σ végigfut K/F összes automorfizmusán. (Ha F karakterisztikája 0, akkor K/F szeparábilis és ilyenkor elég feltenni, hogy K/F normális. K/F automorfizmusai alatt $\mathrm{Hom}_F(K, K)$ elemeit értjük, azaz $\mathrm{Gal}(K/F)$ elemeit, amiből pontosan $|K : F|$ van.)

4.7. Megjegyzés. 1. Ha $\alpha \in F$, akkor $N_{K/F}(\alpha) = \alpha^n$, ahol $n = |K : F|$.

2. $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, $\alpha, \beta \in K$

Bizonyítás. 1. Mindhárom definícióból könnyen adódik: *(i)* Bármilyen bázisban a mátrix az αI_n lesz, ahol I_n az $n \times n$-es egységmátrix. $\det(\alpha I_n) = \alpha^n$.

(ii) $F(\alpha) = F$, $r = n$, $f(X) = X - \alpha$, tehát $(-1)^{nn}(-\alpha)^n = (-1)^{n(n+1)}\alpha^n = \alpha^n$.

(iii) σ F-et fixen hagyja, tehát $\sigma(\alpha) = \alpha$ és n darab σ van.

2. *(i)* Ha $\phi, \psi : K \to K$, amikre $\phi(x) = \alpha x$, $\psi(x) = \beta x$, akkor $N_{K/F}(\alpha\beta) = \det(\phi \circ \psi)$. Teljesül $\det(\phi \circ \psi) = \det(\phi)\det(\psi)$, tehát $N_{K/F}$-re is.

(iii) $\prod_\sigma \sigma(\alpha\beta) = \prod_\sigma \sigma(\alpha)\sigma(\beta) = \prod_\sigma \sigma(\alpha) \prod_\sigma \sigma(\beta)$

□

4.8. Állítás. *Ha $K = F(\alpha)$, akkor az (i) és (ii) definíciók ugyanazt adják.*

Bizonyítás. Tegyük fel, hogy $K = F(\alpha)$ és $n = |K : F|$. Ekkor $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ bázisa K-nak F fölött. Legyen ϕ az α-val való szorzás.

$$\phi(1) = \alpha,\ \phi(\alpha) = \alpha^2,\ \phi(\alpha^2) = \alpha^3, \ldots,\ \phi(\alpha^{n-1}) = \alpha^n$$

Az α $f(X) \in F[X]$ minimálpolinomjára $f(\alpha) = 0$, ezért

$$\alpha^n = -a_0 - a_1\alpha - a_2\alpha^2 - \cdots - a_{n-1}\alpha^{n-1}.$$

Tehát ϕ mátrixa ebben a bázisban

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & -a_0 \\ 1 & 0 & 0 & \ldots & -a_1 \\ 0 & 1 & 0 & \ldots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -a_{n-1} \end{pmatrix}.$$

Az (i)-es definíció szerint ennek determinánsa $N_{K/F}(\alpha)$, azaz $(-1)^{n-1}(-a_0) = (-1)^n a_0$, a (ii)-es definíció szerint pedig $r = 1$ és akkor szintén $(-1)^n a_0$. □

4.9. Állítás. *Legyenek $F \leq K \leq L$ véges bővítések. Ekkor minden $\alpha \in L$-re*

$$N_{K/F}(N_{L/K}(\alpha)) = N_{L/F}(\alpha)$$

az (i)-es definíció szerint.

Bizonyítás. Legyen $\alpha_1, \alpha_2, \ldots, \alpha_n$ bázisa K-nak F fölött és $\beta_1, \beta_2, \ldots, \beta_k$ bázisa L-nek K fölött. Ekkor $\{\alpha_i\beta_j : 1 \leq i \leq n,\ 1 \leq j \leq k\}$ bázisa L-nek F fölött.

- lineárisan független: Legyenek $\lambda_{ij} \in F$ és $\sum_{i,j} \lambda_{ij}\alpha_i\beta_j = 0$. Ekkor átrendezve $\sum_j(\sum_i \lambda_{ij}\alpha_i)\beta_j = 0$, ahol $\sum_i \lambda_{ij}\alpha_i \in K$, tehát $\sum_i \lambda_{ij}\alpha_i = 0$, mert $\beta_1, \ldots, \beta_k$ bázis. Tehát $\lambda_{ij} = 0$ minden i, j-re, mert $\alpha_1, \ldots, \alpha_n$ is bázis.

- generátorrendszer: Tetszőleges $z \in L$ elem felírható $\sum_j \mu_j\beta_j$ alakban, ahol $\mu_j \in K$, mert $\beta_1, \ldots, \beta_k$ bázis. Ekkor $\mu_j = \sum_i \lambda_{ij}\alpha_i$ valamilyen $\lambda_{ij} \in F$ együtthatókkal, mert $\alpha_1, \ldots, \alpha_n$ is bázis. Tehát $z = \sum_{i,j} \lambda_{ij}\alpha_i\beta_j$.

Ezekben a bázisokban írjuk fel a normákat. Legyen $M(c) \in F^{n\times n}$ a $c \in K$-val való szorzás mátrixa az $\alpha_1, \dots, \alpha_n$ bázisban és $((a_{ij})) \in K^{k\times k}$ pedig az α-val való szorzás mátrixa a $\beta_1, \dots, \beta_k$ bázisban, azaz

$$\alpha\beta_j = a_{j1}\beta_1 + \dots + a_{jk}\beta_k.$$

Ekkor az α-val való szorzás mátrixa $\alpha_i\beta_j$ bázisban

$$\begin{pmatrix} M(a_{11}) & \dots & M(a_{1k}) \\ \vdots & \ddots & \vdots \\ M(a_{k1}) & \dots & M(a_{kk}) \end{pmatrix},$$

mert szorozzuk be először az első n sort a báziselemekből álló vektorral

$$\begin{pmatrix} M(a_{11}) & \dots & M(a_{1k}) \end{pmatrix} \begin{pmatrix} \alpha_1\beta_1 \\ \vdots \\ \alpha_n\beta_1 \\ \alpha_1\beta_2 \\ \vdots \\ \alpha_n\beta_k \end{pmatrix} = M(a_{11}) \begin{pmatrix} \alpha_1\beta_1 \\ \vdots \\ \alpha_n\beta_1 \end{pmatrix} + \dots + M(a_{1k}) \begin{pmatrix} \alpha_1\beta_k \\ \vdots \\ \alpha_n\beta_k \end{pmatrix} =$$

$$= \beta_1 M(a_{11}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} + \dots + \beta_k M(a_{1k}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \beta_1 a_{11} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} + \dots + \beta_k a_{1k} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} =$$

$$= (a_{11}\beta_1 + \dots + a_{1k}\beta_k) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \alpha\beta_1 \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \alpha \begin{pmatrix} \alpha_1\beta_1 \\ \vdots \\ \alpha_n\beta_1 \end{pmatrix},$$

éppen az első n báziselemből álló vektor α-szorosa. Ezt természetesen bármelyik n sorra meg lehet mutatni 1 helyett j indexet írva. Definíció szerint ennek a mátrixnak a determinánsa $N_{L/F}(\alpha)$. Kiszámoljuk Gauss-eliminációval, de a blokkokat Gauss-eliminájuk. Úgy is gondolhatjuk, mint amikor az LU felbontást csináljuk és balról egy 1 determinánsú mátrixszal szorozzuk be a mátrixunkat (így nem változik a determináns), például ha a második blokksorból le akarjuk vonni az első sor $M(a_{11}^{-1})$-szeresét, akkor

$$\begin{pmatrix} I & & & \\ -M(a_{11}^{-1}) & I & & \\ & & \ddots & \\ & & & I \end{pmatrix}$$

mátrixszal szorozzuk balról. Így például a második sor első blokkjába $M(a_{21}) - I$ kerülne. Ha ki akarjuk nullázni, akkor $-M(a_{11}^{-1})$ helyett $-M(a_{21})M(a_{11}^{-1})$-et kell írni a balról szorzó mátrixba. Ilyen szorzásokkal elérhető, hogy felső blokk-háromszögmátrix maradjon, amit aztán úgy tudunk tovább eliminálni, ha a balról szorzó mátrixokban a főátló felé rakjuk a nem nulla mátrixot. Probléma akkor merül fel, ha a Gauss-elimináció során sort vagy oszlopot kell cserélni, de ekkor az egyik sort beszorozzuk (-1)-gyel, hogy a determináns ne változzon. (A sor és oszlop blokksort és blokkoszlopot jelent, azaz minden sort és oszlopot, amit tartalmaz azt cseréljük vagy szorozzuk (-1)-gyel.) Tehát

elérhető, hogy blokkdiagonális mátrixot kapjunk. Az is elérhető, hogy minden diagonális blokk az egységmátrix legyen az utolsó kivételével.

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & 0 \\ 1 & b \end{pmatrix} \to \begin{pmatrix} a & -ab \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ -a & ab \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}$$

Kivontuk a második sorból az első $1/a$-szorosát, majd a második oszlopból kivontuk az első oszlop b-szeresét. Utána megcseréltük a két sort és szoroztuk a második sort (-1)-gyel. Végül hozzáadtuk a második sorhoz az első sor a-szorosát. Ezzel a módszerrel sorban eggyel lejjebb tudjuk vinni a blokkokat a nagy mátrixunkban, hiszen ezeket a lépéseket mind meg tudjuk csinálni ott is (oszlopok kivonása az egy hasonló mátrix jobbról szorzása). Az a probléma nem merül fel, mint a 2×2-es példában, hogy a vagy b lehet 0, mert a megfelelő $M(a)$ determinánsa nem 0, mert ha 0 lenne, akkor a blokkdiagonális mátrixunk determinánsa is 0 lenne, azaz az α-val való szorzás L-ben nem lenne injektív, tehát $\alpha = 0$. Erre az esetre könnyű az Állítás, így feltehető, hogy $\alpha \neq 0$. Tehát az a-val való szorzás sem injektív, tehát $a \neq 0$, így létezik a^{-1} és így $M(a^{-1})$ is és ennek sem nulla a determinánsa. Az M művelettartó leképezés, mert ha $\underline{\alpha}$ az α_j báziselemekből álló vektor, akkor

$$M(a+b)\underline{\alpha} = (a+b)\underline{\alpha} = a\underline{\alpha} + b\underline{\alpha} = M(a)\underline{\alpha} + M(b)\underline{\alpha},$$

$$M(a)M(b)\underline{\alpha} = M(a)(b\underline{\alpha}) = b(M(a)\underline{\alpha}) = b(a\underline{\alpha}) = (ba)\underline{\alpha} = (ab)\underline{\alpha} = M(ab)\underline{\alpha}.$$

Kihasználva, hogy M művelettartó és a blokkmátrixon elvégezve az eliminációt az olyan, mintha $((a_{ij}))$ mátrixon végeztük volna el, azt kapjuk, hogy a blokkmátrix utolsó diagonális eleme $M\big(\det((a_{ij}))\big)$, hiszen $((a_{ij}))$-re elvégezve annak az utolsó eleme $\det((a_{ij}))$ lenne. Ekkor készen vagyunk, mert a blokkmátrix determinánsa, azaz $N_{L/F}(\alpha)$ megegyezik az utolsó diagonális blokk determinánsával, azaz $\det M\big(\det((a_{ij}))\big)$-vel, ami éppen $N_{K/F}(N_{L/K}(\alpha))$. □

4.10. Következmény. *Az (i) és (ii) definíciók ugyanazt adják és $F \leq K \leq L$-re $N_{K/F} \circ N_{L/K} = N_{L/F}$ a (ii) definíció szerint is.*

Bizonyítás. $F \leq F(\alpha) \leq K$, jelöljük felső indexben, hogy melyik definíció szerint nézzük a normát. Az előző állítás alapján

$$N^{(i)}_{F(\alpha)/F}(N^{(i)}_{K/F(\alpha)}(\alpha)) = N^{(i)}_{K/F}(\alpha).$$

Az első megjegyzést használva, mert $\alpha \in F(\alpha)$

$$N^{(i)}_{F(\alpha)/F}(\alpha^{|K:F(\alpha)|}) = N^{(i)}_{K/F}(\alpha).$$

A második megjegyzés miatt $N^{(i)}$ multiplikatív, tehát

$$N^{(i)}_{F(\alpha)/F}(\alpha)^{|K:F(\alpha)|} = N^{(i)}_{K/F}(\alpha).$$

Korábbi állítás miatt $N^{(i)}_{F(\alpha)/F} = N^{(ii)}_{F(\alpha)/F}$

$$N^{(ii)}_{F(\alpha)/F}(\alpha)^{|K:F(\alpha)|} = N^{(i)}_{K/F}(\alpha).$$

A (ii) definíció szerint $N^{(ii)}_{F(\alpha)/F}(\alpha) = (-1)^n a_0$ és $|K : F(\alpha)| = r$, amit visszaírva az egyenlőségbe

$$(-1)^{nr} a_0^r = N^{(i)}_{K/F}(\alpha),$$

aminek a bal oldala a (ii) definíció szerinti norma. Az állítás második fele nyilvánvaló abból, hogy (i) definícióra igaz és a két definíció ugyanazt adja. □

4.11. Állítás. *Mindhárom definíció ugyanazt adja. Ha $F \leq K \leq L$ véges testbővítések, akkor $N_{K/F} \circ N_{L/F} = N_{L/F}$ a (iii) definíció szerint is.*

Bizonyítás. Elég belátni, hogy a (*ii*) és a (*iii*) definíció ugyanazt adja. Tegyük fel, hogy K/F Galois bővítés és legyen $\alpha \in K$. Ismert, hogy a $\tau \mapsto \tau(\alpha)$ képlettel megadott $\mathrm{Hom}_F(F(\alpha), K) \to \{\beta \in K : f(\beta) = 0\}$ függvény bijekció, ha f az α F feletti minimálpolinomja. Egy $\tau \in \mathrm{Hom}_F(F(\alpha), K)$ homomorfizmust ki tudunk terjeszteni egy $\sigma \in \mathrm{Hom}_F(K, K)$ homomorfizmussá. K/F normális, ezért f minden gyöke benne van K-ban, mert α, az egyik gyöke benne van. Tehát speciálisan ha β az f egy gyöke, akkor létezik $\sigma \in \mathrm{Gal}(K/F)$ homomorfizmus, amire $\sigma(\alpha) = \beta$. A $G = \mathrm{Gal}(K/F)$ csoport hat az f gyökeinek halmazán, mert tetszőleges $\sigma \in G$-re és β gyökére f-nek, $\sigma(\beta)$ is gyöke f-nek:

$$\sigma(\beta)^n + a_{n-1}\sigma(\beta)^{n-1} + \cdots + a_1\sigma(\beta) + a_0 = \sigma(\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0) = \sigma(0) = 0.$$

Az α stabilizátora $\mathrm{Stab}_G(\alpha) = \{\sigma \in G : \sigma(\alpha) = \alpha\}$, a pályája pedig $G\alpha$ az előzőek alapján f gyökeinek halmaza. Írjuk fel a pálya-stabilizátor lemmát:

$$|G : \mathrm{Stab}_G(\alpha)| = |G\alpha|.$$

Ekkor $|G\alpha| = |F(\alpha) : F|$, mert f-nek ennyi gyöke van és $|G| = |K : F|$. Tehát $|\mathrm{Stab}_G(\alpha)| = |K : F(\alpha)| = r$ és $\mathrm{Stab}_G(\alpha)$ minden mellékosztályának is r eleme van. A mellékosztályok éppen azok az elemei G-nek, amik α-t az f különböző gyökeibe viszik: legyen β az f egy gyöke és $\tau \in G$, amire $\tau(\alpha) = \beta$. Ekkor

$$\tau\ \mathrm{Stab}_G(\alpha) = \{\tau\sigma \in G : \sigma(\alpha) = \alpha\} = \{\varrho \in G : \varrho(\alpha) = \tau\sigma(\alpha) = \beta\}$$

éppen az α-t β-ba vivő homomorfizmusok. Vagyis $\sigma(\alpha)$, $\sigma \in G$ az f gyökeit veszi fel és mindegyiket pontosan r-szer. Tehát megegyezik a két definíció, mert

$$(-1)^{nr}a_0^r = ((-1)^n f(0))^r = \left(\prod_{\beta \text{ az } f \text{ gyöke}} \beta\right)^r = \prod_{\sigma \in G} \sigma(\alpha).$$

A norma tranzitivitását csak a (*iii*) definícióra nem láttuk még be, de mivel mindegyik definíció ugyanazt írja le, ezért a (*iii*) definíció szerint is tranzitív. □

Tegyük fel, hogy $K/\mathbb{Q}_p$ normális és legyen σ automorfizmus. ($\mathrm{char}(\mathbb{Q}_p) = 0$) Tegyük fel továbbá, hogy $|\cdot|$ abszolútérték K-n, ami a p-adikus abszolútérték kiterjesztése. Ekkor $x \mapsto |\sigma(x)|$ szintén abszolútérték K-n és kiterjesztése a p-adikus abszolútértéknek:

(i) $|\sigma(x)| = 0 \overset{|\cdot|\text{-ra } (i)}{\iff} \sigma(x) = 0 \overset{\sigma \text{ aut.}}{\iff} x = 0$;

(ii) $x, y \in K : |\sigma(xy)| \overset{\sigma \text{ aut.}}{=} |\sigma(x)\sigma(y)| \overset{|\cdot|\text{-ra } (ii)}{=} |\sigma(x)||\sigma(y)|$;

(iii) $x, y \in K : |\sigma(x+y)| \overset{\sigma \text{ aut.}}{=} |\sigma(x) + \sigma(y)| \overset{|\cdot|\text{-ra } (iii)}{\leq} |\sigma(x)| + |\sigma(y)|$;

(iv) $\lambda \in \mathbb{Q}_p : |\sigma(\lambda)| \overset{\sigma|_{\mathbb{Q}_p} = id}{=} |\lambda| \overset{|\cdot|\text{-ra } (iv)}{=} |\lambda|_p$.

Beláttuk, hogy K-n egyetlen ilyen abszolútérték lehet, ezért $|x| = |\sigma(x)|$ minden $x \in K$-ra. Tudjuk, hogy összesen $n = |K : \mathbb{Q}_p|$ automorfizmus van, ezért

$$|x|^n = \prod_\sigma |\sigma(x)| = \left| \prod_\sigma \sigma(x) \right|.$$

A jobb oldalon éppen a norma *(iii)*-as definícióját kaptuk, azaz

$$|x|^n = |N_{K/\mathbb{Q}_p}(x)|,$$

ahonnan adódik, hogy

$$|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|}.$$

Tehát ezzel beláttuk, hogy ez lehet csak a képlete $|x|$-nek, és ez számolható is, mert $N_{K/\mathbb{Q}_p}(x)$ $\mathbb{Q}_p$-ben van, tehát $|N_{K/\mathbb{Q}_p}(x)| = |N_{K/\mathbb{Q}_p}(x)|_p$.
Az abszolútérték nem függ a testtől, amiben nézzük, amihez szükséges a következő állítás, ami éppen azt mondja, hogy az előbbi képlet jó:

4.12. Állítás. *Legyen K és L a $\mathbb{Q}_p$ véges bővítései, amikre teljesül $\mathbb{Q}_p \leq K \leq L$. Legyen továbbá $x \in K$ és legyen $m = |K : \mathbb{Q}_p|$, $n = |L : \mathbb{Q}_p|$. Ekkor*

$$\sqrt[m]{|N_{K/\mathbb{Q}_p}(x)|_p} = \sqrt[n]{|N_{L/\mathbb{Q}_p}(x)|_p}.$$

Bizonyítás. Egyrészt teljesül $N_{L/\mathbb{Q}_p}(x) = N_{K/\mathbb{Q}_p}(N_{L/K}(x))$, másrészt $N_{L/K}(x) = x^{|L:K|}$. Tehát kihasználva a norma multiplikativitását $N_{L/\mathbb{Q}_p}(x) = N_{K/\mathbb{Q}_p}(x)^{|L:K|}$. Emeljük az egyenlőséget $m = |K : \mathbb{Q}_p|$-dik hatványra, és $|\cdot|_p$-t véve adódik

$$|N_{L/\mathbb{Q}_p}(x)|_p^m = |N_{K/\mathbb{Q}_p}(x)|_p^n,$$

mert $|L : \mathbb{Q}_p| = |L : K||K : \mathbb{Q}_p|$. Innen átrendezve kapjuk az állítást. □

4.13. Következmény. *Ha létezik abszolútérték K-n, ami kiterjesztése a p-adikus abszolútértéknek, akkor azt csak az*

$$|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

formula adhatja, ahol $n = |K : \mathbb{Q}_p|$.

Bizonyítás. Normális bővítésekre megmutattuk, ha viszont nem normális $K/\mathbb{Q}_p$, akkor vegyük a normális lezártját. Erre tudjuk, hogy csak így definiálhatjuk az abszolútértéket és az előző állítás miatt K-ra is csak így definiálhatjuk. (Vegyük észre, hogy a normális lezárt is véges bővítés.) □

4.14. Tétel. *Legyen $K/\mathbb{Q}_p$ véges bővítés, $n = |K : \mathbb{Q}_p|$. Ekkor a $|\cdot| : K \to \mathbb{R}_+$,*

$$|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

függvény egy nemarkhimédeszi abszolútérték K-n, ami a kiterjesztése $\mathbb{Q}_p$ p-adikus abszolútértékének.

Bizonyítás. Ha $|x| = 0$, akkor $N_{K/\mathbb{Q}_p}(x) = 0$, ami az első definíció alapján azt jelenti, hogy az x-szel való szorzás nem injektív. K test, ezért ez csak akkor lehetséges, ha $x = 0$. $N_{K/\mathbb{Q}_p}$ és $|\cdot|_p$ multiplikativitása miatt $|\cdot|$ is multiplikatív. Ha $x \in \mathbb{Q}_p$, akkor $N_{K/\mathbb{Q}_p}(x) = x^n$, tehát $|x| = \sqrt[n]{|x|_p^n} = |x|_p$. Belátjuk az $|x+y| \leq \max\{|x|, |y|\}$ egyenlőtlenséget. Ha $y = 0$, akkor teljesül, ha $y \neq 0$, akkor osztás után elegendő $|x+1| \leq \max\{|x|, 1\}$-t belátni.

Ehhez elég megmutatni, hogy $|x| \leq 1 \Rightarrow |x-1| \leq 1$:

Tegyük fel, hogy ez a következtetés igaz. Ekkor

$$|x| \leq 1 \Rightarrow |-x| \leq 1 \Rightarrow |-x-1| \leq 1 \Rightarrow |x+1| \leq 1$$

Ha $|x| \leq 1$, akkor $\max\{|x|, 1\} = 1$, illetve $|x+1| \leq 1$ a következtetés miatt. Tehát valóban igaz $|x+1| \leq \max\{|x|, 1\}$. Ha $|x| > 1$, akkor $|1/x| < 1$. A feltevés miatt $|1 + 1/x| \leq 1$, tehát $|x+1| \leq |x|$, ami éppen az, amit akartunk, mert $\max\{|x|, 1\} = |x|$.

Tehát elegendő belátni, hogy $x \in K$-ra

$$|x| \leq 1 \Rightarrow |x-1| \leq 1.$$

Ez $|\cdot|$ definíciója alapján

$$|N_{K/\mathbb{Q}_p}(x)|_p \leq 1 \Rightarrow |N_{K/\mathbb{Q}_p}(x-1)|_p \leq 1.$$

Ezt úgy is ki tudjuk fejezni, hogy

$$N_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p \Rightarrow N_{K/\mathbb{Q}_p}(x-1) \in \mathbb{Z}_p.$$

Használjuk a norma (ii) definícióját és legyen

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[X]$$

az x minimálpolinomja. Ekkor $x-1$ minimálpolinomja $g(X) = f(X+1)$, mert $\mathbb{Q}_p(x)$ (a legkisebb $\mathbb{Q}_p$-t és x-t tartalmazó test) és $\mathbb{Q}_p(x-1)$ ugyanazok a testek, tehát a két minimálpolinom foka meg kell, hogy egyezzen, és $g(x-1) = f(x) = 0$.

$$g(0) = f(1) = 1 + a_{n-1} + \cdots + a_0$$

Ekkor ha $r = |K : \mathbb{Q}_p(x)| = |K : \mathbb{Q}_p(x-1)|$, akkor a (ii) definíció szerint

$$N_{K/\mathbb{Q}_p}(x) = (-1)^{nr}a_0^r \text{ és } N_{K/\mathbb{Q}_p}(x-1) = (-1)^{nr}(1 + a_{n-1} + \cdots + a_0)^r.$$

Ha $\lambda \in \mathbb{Q}_p$, $r \in \mathbb{N}$ akkor $\lambda \in \mathbb{Z}_p \iff \lambda^r \in \mathbb{Z}_p$: az "oda" irány látszik, a "vissza" iránynál fontos $\lambda \in \mathbb{Q}_p$, mert írhatjuk $|\lambda^r|_p = |\lambda|_p^r \leq 1$ és vonhatunk r-dik gyököt. ($\lambda^r \in \mathbb{Q}_p \not\Rightarrow \lambda \in \mathbb{Q}_p$) Tehát elegendő megmutatni, hogy

$$a_0 \in \mathbb{Z}_p \Rightarrow 1 + a_{n-1} + \cdots + a_0 \in \mathbb{Z}_p.$$

Ez következik a következő lemmából:

4.15. Lemma. *Ha $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[X]$ irreducibilis polinom, amire $a_0 \in \mathbb{Z}_p$, akkor $f(X) \in \mathbb{Z}_p[X]$.*

Bizonyítás. Azt bizonyítjuk, hogy ha valamelyik együttható nincs $\mathbb{Z}_p$-ben, akkor $f(X)$ nem irreducibilis. Legyen m a legkisebb olyan egész, amire $p^m a_i \in \mathbb{Z}_p$ minden i-re. ($m \geq 1$, mert $m = 0$-ra nem lehet minden a_i $\mathbb{Z}_p$-ben feltétel szerint.) Legyen

$$g(X) = p^m f(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0,$$

azaz $b_i = p^m a_i$. $b_n = p^m$ és $b_0 = p^m a_0$ osztható p-vel (azaz $b_n/p \in \mathbb{Z}_p$, $b_0/p \in \mathbb{Z}_p$, mert $m \geq 1$). Minden $b_i \in \mathbb{Z}_p$ és legalább az egyik nem osztható p-vel, legyen k a legkisebb i index, amire b_i nem osztható p-vel. ($n > k \geq 1$, mert b_n és b_0 osztható.) Ekkor

$$g(X) \equiv (b_n X^{n-k} + \cdots + b_k) X^k \pmod{p},$$

X^k 1-főegyüttható és relatív prímek modulo p. Ha a $b_n X^{n-k} + \cdots + b_k$ polinomot redukáljuk modulo p, akkor a konstans tag nem nulla. Legyen X^k egy nem konstans osztója $d(X)$, ekkor $d(0) \equiv 0 \pmod{p}$, viszont $d(X)$ nem lehet osztója a másik polinomnak, mert akkor az is 0-ban 0-val lenne kongruens, de annak a konstans tagja nem nulla. Tehát csak konstans közös osztójuk lehet, azaz relatív prímek modulo p. Használhatjuk a második Hensel Lemmát (3.36. Tétel), amiből azt kapjuk, hogy $g(X) = p^m f(X)$ reducibilis ($\mathbb{Z}_p$-ben), tehát $f(X)$ is reducibilis ($\mathbb{Q}_p$-ben). (Az ott kapott $g(X)$ polinomra $g(X) \equiv X^k \pmod{p}$ és $g(X)$ 1-főegyüttható, tehát $\deg g(X) = k$, $n > k \geq 1$.) □

Az x minimálpolinomja $f(X) \in \mathbb{Q}_p[X]$ irreducibilis, ezért ha $a_0 \in \mathbb{Z}_p$, akkor minden együtthatója is és azok összege, $1 + a_{n-1} + \cdots + a_0$ is $\mathbb{Z}_p$-ben van. □

4.2. $\mathbb{Q}_p$ algebrai lezártja

4.16. Definíció. $\mathbb{Q}_p$ *algebrai lezártja* $\mathbb{Q}_p$ összes véges bővítésének az uniója, tehát az összes $\mathbb{Q}_p$ együtthatós polinom összes gyöke. $\mathbb{Q}_p$ algebrai lezártját $\overline{\mathbb{Q}}_p$-vel jelöljük.

4.17. Megjegyzés. $\overline{\mathbb{Q}}_p$ algebrailag zárt test.

4.18. Tétel. *Létezik p-adikus abszolútérték $\overline{\mathbb{Q}}_p$-n és ez egyértelmű.*

Bizonyítás. Legyen $x \in \overline{\mathbb{Q}}_p$, ekkor $\mathbb{Q}_p(x)/\mathbb{Q}_p$ véges bővítés és ebben a véges bővítésben egyértelműen létezik p-adikus abszolútértéke x-nek. Ezzel a módszerrel minden $x \in \overline{\mathbb{Q}}_p$-re definiálhatjuk x abszolútértékét. Ha lenne másik p-adikus abszolútérték $\overline{\mathbb{Q}}_p$-n, akkor valamilyen $x \in \overline{\mathbb{Q}}_p$-re a két abszolútérték eltér. De ezt az abszolútértéket megszorítva $\mathbb{Q}_p(x)$-re ez az abszolútérték eltér, ami nem lehet, mert véges bővítésen egyértelmű a p-adikus abszolútérték.

Még azt kell belátni, hogy ez $\overline{\mathbb{Q}}_p$-n valóban abszolútérték. Ha $x \in \overline{\mathbb{Q}}_p$, $|x| = 0$, akkor $N_{\mathbb{Q}_p(x)/\mathbb{Q}_p}(x) = 0$, azaz mint korábban az x-szel való szorzás nem injektív, tehát $x = 0$. Ha $x \in \mathbb{Q}_p$, akkor $|\mathbb{Q}_p : \mathbb{Q}_p| = 1$, $N_{\mathbb{Q}_p/\mathbb{Q}_p}(x) = x$, tehát $|x| = |x|_p$. Legyen $x, y \in \overline{\mathbb{Q}}_p$, ekkor tekintsük az abszolútértéket $\mathbb{Q}_p(x, y) = K$-ban, amire így $K/\mathbb{Q}_p$ véges bővítés. Ahogy 4.14. Tétel bizonyításában is volt $|xy| = |x||y|$ és $|x + y| \leq \max\{|x|, |y|\}$. □

Megmutatjuk, hogy $\overline{\mathbb{Q}}_p$ nem véges bővítés, amihez elég, hogy létezik tetszőlegesen nagy fokú $\mathbb{Q}_p$ együtthatós irreducibilis polinom. Ha létezik n-edfokú irreducibilis polinom, akkor ennek minden gyöke benne van $\overline{\mathbb{Q}}_p$-ben, de egy gyöke egy n-edfokú bővítést generál, tehát $\overline{\mathbb{Q}}_p$ tartalmaz n-edfokú bővítést minden n-re, vagyis $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$ nem lehet véges. (Ha $\mathbb{Q}_p \leq K_n \leq \overline{\mathbb{Q}}_p$ és $|K_n : \mathbb{Q}_p| = n$, akkor $|\overline{\mathbb{Q}}_p : \mathbb{Q}_p| \geq |K_n : \mathbb{Q}_p| = n$.)

4.19. Lemma. *Tegyük fel, hogy $f(X) \in \mathbb{Z}_p[X]$ polinom szorzattá bomlik úgy, hogy*

$$f(X) = g(X)h(X),$$

ahol $g(X), h(X) \in \mathbb{Q}_p[X]$ és egyik sem konstans. Ekkor léteznek $g_0(X), h_0(X) \in \mathbb{Z}_p[X]$ nem konstans polinomok, amikre $f(X) = g_0(X)h_0(X)$, azaz $\mathbb{Z}_p$ fölött is szorzattá bomlik.

Bizonyítás. Ha $k(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Q}_p[X]$ polinom, akkor legyen

$$w(k(X)) = \min_{0 \le i \le n} v_p(a_i).$$

Ekkor $k(X) \in \mathbb{Z}_p[X] \Leftrightarrow w(k(X)) \ge 0$.

1. lépés: Ha $w(f(X)) = 0$ esetben igaz a Lemma, akkor igaz mindig.

Bizonyítás: Létezik $a \in \mathbb{Q}_p$, amire $w(f(X)) = -v_p(a)$, például vegyük annak az együtthatónak a reciprokát, ahol $w(f(X))$ felveszi a minimumot. Ekkor $0 \le -v_p(a)$, ezért $|a^{-1}| \le 1$, tehát $a^{-1} \in \mathbb{Z}_p$, és

$$w(af(X)) = v_p(a) + w(f(X)) = 0.$$

Legyen $\tilde{f}(X) = af(X)$, $\tilde{g}(X) = ag(X)$, ekkor $\tilde{f}(X) = \tilde{g}(X)h(X)$, ahol $\tilde{f}(X) \in \mathbb{Z}_p[X]$, $w(\tilde{f}(X)) = 0$. Ekkor létezik $\tilde{f}(X)$-nek felbontása, azaz létezik $G_0(X), H_0(X) \in \mathbb{Z}_p[X]$, amire

$$\tilde{f}(X) = G_0(X)H_0(X).$$

Legyenek $g_0(X) = a^{-1}G_0(X)$, $h_0(X) = H_0(X) \in \mathbb{Z}_p[X]$ polinomok, ez bizonyítja az állítást, mert

$$f(X) = a^{-1}\tilde{f}(X) = a^{-1}G_0(X)H_0(X) = g_0(X)h_0(X).$$

2. lépés: Igaz a Lemma $w(f(X)) = 0$ esetben.

Bizonyítás: Tegyük fel, hogy $w(f(X)) = 0$. Ugyanazzal az érveléssel megmutatható, hogy léteznek $b, c \in \mathbb{Q}_p$ számok, amikre $w(bg(X)) = 0$, $w(ch(X)) = 0$, $b^{-1}, c^{-1} \in \mathbb{Z}_p$. Legyenek $g_1(X) = bg(X)$ és $h_1(X) = ch(X)$, illetve

$$f_1(X) = bcf(X) = g_1(X)h_1(X).$$

Legyen $\bar{k}(X) \in \mathbb{F}_p[X]$ a $k(X) \in \mathbb{Z}_p[X]$ polinom redukálva modulo p. A $g_1(X)$ és $h_1(X)$ polinomokat úgy gyártottuk le, hogy $\bar{g}_1(X)$ és $\bar{h}_1(X)$ nem nulla polinomok, tehát $\bar{f}_1(X)$ sem nulla (két nem nulla polinom szorzata). Ekkor $w(f_1(X)) = 0$, mert van legalább egy együtthatója, ami nem osztható p-vel.

$$w(f_1(X)) = w(bcf(X)) = v_p(bc) + w(f(X)) = v_p(bc)$$

Tehát $v_p(bc) = 0$, azaz bc p-adikus egység. Tehát

$$f(X) = (bc)^{-1}f_1(X) = (bc)^{-1}g_1(X)h_1(X).$$

Legyen $g_0(X) = (bc)^{-1}g_1(X)$ és $h_0(X) = h_1(X)$, ekkor $g_0(X), h_0(X) \in \mathbb{Z}_p[X]$ bizonyítja a Lemmát. □

4.20. Állítás (Eisenstein Irreducibilitási Kritérium)**.** *Legyen*

$$f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}_p[X]$$

polinom, ami teljesíti a következő feltételeket:

i) $|a_n| = 1$;

ii) $|a_i| < 1$, *ha* $i < n$;

iii) $|a_0| = 1/p$.

Ekkor $f(X)$ *irreducibilis* $\mathbb{Q}_p$ *felett.*

Bizonyítás. Tegyük fel, hogy $f(X)$ reducibilis $\mathbb{Q}_p$ felett, ekkor az előző, 4.19. Lemma miatt $\mathbb{Z}_p$ felett is reducibilis, azaz léteznek $g(X), h(X) \in \mathbb{Z}_p[X]$ nem konstans polinomok, amikre

$$f(X) = g(X)h(X).$$

Legyenek

$$g(X) = b_r X^r + \cdots + b_1 X + b_0$$

és

$$h(X) = c_s X^s + \cdots + c_1 X + c_0,$$

ahol $r + s = n$. Mivel $|a_n| = 1$, $b_r c_s = a_n$ és $b_r, c_s \in \mathbb{Z}_p$, ezért $|b_r| = |c_s| = 1$. Ekkor b_0 és c_0 is osztható p-vel: ha egyik sem osztható p-vel, akkor $b_0 c_0 = a_0$ szintén nem osztható p-vel, ami nem lehet, mert $|a_0| = 1/p$. Tegyük fel, hogy b_0 osztható p-vel, de c_0 nem és tegyük fel, hogy $r \leq s$. Kiszorzás után $a_1 = b_1 c_0 + b_0 c_1$, ahol b_0 és a_1 osztható p-vel, de c_0 nem, tehát b_1 osztható p-vel. X^2 együtthatója miatt $a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2$, ahol $p \mid b_0, b_1, a_2$, de $p \nmid c_0$, tehát b_2 is osztható p-vel. Ezt folytatva $b_0, b_1, \ldots, b_{r-1}$ osztathók p-vel. X^r együtthatója $a_r = b_r c_0 + \cdots + b_0 c_r$, ahol $r < n$ miatt a_r is osztható p-vel, tehát b_r is. Ez azonban ellentmond azzal, hogy $|b_r| = 1$. Ha $r > s$, akkor ugyanezt lehet csinálni, de például X^{s+1} együtthatójánál nem létezik $b_0 c_{s+1}$ tag, viszont itt is következik, hogy b_{s+1} osztható p-vel. Az utolsó együttható, amit meg kell nézni, X^r együtthatója $a_r = b_r c_0 + \cdots + b_{r-s} c_s$, ahol $p \mid a_r$, mert $r < n$ és ezért $p \mid b_r$ megint ellentmondás. Ha b_0 nem osztható p-vel, de c_0 igen, akkor fordítva elmondva megint ellentmondásra jutunk. Tehát $p \mid b_0$ és $p \mid c_0$ is teljesül, azaz $p^2 \mid b_0 c_0 = a_0$, vagyis $|a_0| \leq 1/p^2$, ami nem lehetséges *iii)* miatt. Tehát $f(X)$ valóban irreducibilis. □

4.21. Következmény. $\overline{\mathbb{Q}}_p$ *végtelen bővítése* $\mathbb{Q}_p$*-nek.*

Bizonyítás. Az eddigiek alapján elég mutatni egy n-edfokú, $\mathbb{Q}_p$ együtthatós, irreducibilis polinomot minden n-re. Az Eisenstein kritérium (4.20.Állítás) miatt nagyon könnyű ilyen polinomot mutatni, például $f(X) = X^n - p$ irreducibilis. □

Mivel $\overline{\mathbb{Q}}_p$ nem véges bővítése $\mathbb{Q}_p$-nek, ezért nem teljesül automatikusan, hogy $\overline{\mathbb{Q}}_p$ teljes tér, sőt ez nem is igaz (a bizonyításától eltekintünk a hossza miatt, megtalálható [1]-ben, 5.7.4. Tétel):

4.22. Tétel. $\overline{\mathbb{Q}}_p$ *nem teljes tér.*

A Tétel miatt van értelme teljessé tenni, a következő fejezetben erről lesz szó.

4.3. $\mathbb{C}_p$

4.23. Definíció. Legyen $K \leq \overline{\mathbb{Q}}_p$. Azt mondjuk, hogy a és a' $\overline{\mathbb{Q}}_p$-beli számok *konjugáltak K fölött*, ha ugyanannak az irreducibilis K együtthatós polinomnak a gyökei.

4.24. Tétel (Krasner Lemma)**.** *Legyen K-n adott egy nemarkhimédeszi abszolútérték, amire nézve K teljes és char $(K) = 0$. Legyenek a és b az algebrai lezárt, $\overline{K}$ elemei. Legyenek $a_1 = a, a_2, \ldots, a_n$ a konjugáltjai a-nak K felett. Tegyük fel, hogy b közelebb van a-hoz bármelyik kongultjánál, azaz $|b-a| < |a-a_i|$ minden $i = 2, 3, \ldots, n$ esetén. Ekkor $K(a) \subset K(b)$.*

Bizonyítás. Legyen $L = K(b)$ és tegyük fel, hogy az állítás nem igaz, azaz $a \notin L$. Ekkor $|L(a) : L| = m > 1$ és mivel $\mathrm{Hom}_L(L(a), \overline{K})$ bijekcióban áll a L feletti minimálpolinomjának $\overline{K}$-ba eső gyökeivel, ezért tudjuk, hogy m darab $\sigma : L(a) \to \overline{K}$ homomorfizmus van, ami L-et fixen hagyja, mert minden gyök benne van az algebrai lezártban. Van legalább egy σ, amire $\sigma(a) \neq a$, mert ha $\sigma(a) = a$, akkor a σ fixen hagyja az egész $L(a)$-t, tehát az identitás, de több, mint egy σ van. Legyen σ_0 ilyen. $\overline{K}$ abszolútértékének az egyértelműsége miatt (ugyanúgy véges bővítésekre egyértelmű és $\overline{K}$ a véges bővítések uniója) $|\sigma(x)| = |x|$ minden σ-ra és x-re. Tehát

$$|\sigma_0(b) - \sigma_0(a)| = |b - a|$$

és mivel σ fixen hagyja L-et és $b \in L$, ezért

$$|b - \sigma_0(a)| = |b - a|.$$

Ekkor

$$|a - \sigma_0(a)| \leq \max\{|a - b|, |b - \sigma_0(a)|\} = |b - a|,$$

ami nem lehet, mert b feltétel szerint közelebb van a-hoz, mint bármelyik konjugáltja és $\sigma_0(a)$ az a egy konjugáltja. □

4.25. Következmény. *Legyen K-n adott egy nemarkhimédeszi abszolútérték, amire nézve K teljes és char $(K) = 0$. Legyen*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$$

irreducibilis polinom és legyen λ az f egyik gyöke. Legyen $L = K(\lambda)$. Ekkor létezik egy $\varepsilon > 0$ szám, amire:

ha $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in K[X]$ és $|a_i - b_i| < \varepsilon$ minden $i = 0, 1, \ldots, n-1$ esetén, akkor $g(X)$ irreducibilis K fölött és van gyöke L-ben.

Bizonyítás. Legyenek $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_n$ az $f(X)$ gyökei $\overline{K}$-ban és legyen

$$r = \min_{i \neq j} |\lambda_i - \lambda_j|.$$

Legyenek $\mu_1, \ldots, \mu_n$ a $g(X)$ gyökei $\overline{K}$-ban, ekkor $g(X) = \prod(X - \mu_j)$. Legyen

$$D = \prod_i g(\lambda_i) = \prod_{i,j}(\lambda_i - \mu_j).$$

1. lépés: Ha $|D| < r^{n^2}$, akkor $g(X)$ irreducibilis K fölött és van gyöke L-ben.

Bizonyítás: Ha $|D| < r^{n^2}$, akkor van legalább egy (i, j) pár, amire $|\lambda_i - \mu_j| < r$. Ekkor μ_j közelebb van λ_i-hez, mint bármelyik konjugáltja, ezért a Krasner Lemma (4.24. Tétel) miatt $K(\lambda_i) \subset K(\mu_j)$. Az $f(X)$ a λ_i minimálpolinomja, mert irreducibilis, ezért $n = |K(\lambda_i) : K| \leq |K(\mu_j) : K|$, de μ_j gyöke egy n-edfokú polinomnak, tehát a polinom irreducibilis, $|K(\mu_j) : K| = n$ és ezért $K(\lambda_i) = K(\mu_j)$. Ha $i = 1$, akkor azt is megmutattuk, hogy $g(X)$-nek van gyöke L-ben. Ha nem, akkor létezik $\overline{K}$-nak egy K-t fixáló automorfizmusa, ami λ_i-t λ-ba viszi. Ekkor ez az automorfizmus μ_j-t egy μ-be viszi, ami szintén $g(X)$ gyöke. Alkalmazva $K(\lambda_i) = K(\mu_j)$-re az automorfizmust $L = K(\lambda) = K(\mu)$ adódik, tehát $g(X)$-nek is van gyöke L-ben, μ.

2. lépés: Létezik $\varepsilon > 0$ szám, amire ha $|a_i - b_i| < \varepsilon$, akkor $|D| < r^{n^2}$.

Bizonyítás: Ha $\varphi : (a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}) \mapsto D$ folytonos függvény, akkor igaz a 2. lépés. Tudjuk, hogy $(a_0, \ldots, a_{n-1}, a_0, \ldots, a_{n-1}) \mapsto 0$. Tehát $(a_0, \ldots, a_{n-1}, a_0, \ldots, a_{n-1})$-nek van egy kis környezete, amin belül teljesül $|D| < r^{n^2}$. Ekkor ε-t olyan kicsinek kell választani, hogy ha minden i-re $|a_i - b_i| < \varepsilon$, akkor $(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1})$ benne legyen ebben a környezetben. Ilyet persze tudunk találni.

D a λ_i-k és μ_j-k szimmetrikus polinomja, hiszen bármilyen permutációt alkalmazhatok az indexekre, D nem változik. A szimmetrikus polinomok alaptétele szerint minden szimmetrikus polinom előáll elemi szimmetrikus polinomok polinomjaként. Az elemi szimmetrikus polinomok viszont ebben az esetben a gyökök és együtthatók közti összefüggések miatt éppen f és g együtthatói. Tehát D előáll az $(a_0, \ldots, a_{n-1})$ és $(b_0, \ldots, b_{n-1})$ polinomjaként, azaz φ valójában egy polinom, így természetesen folytonos. □

A Teljessé tétel fejezetben leírtakkal megegyezően teljessé tehetjük $\overline{\mathbb{Q}}_p$-t, ez lesz $\mathbb{C}_p$:

4.26. Állítás. *Létezik egy $\mathbb{C}_p$ test és azon egy $|\cdot|$ abszolútérték, amire*

- *$\overline{\mathbb{Q}}_p \subset \mathbb{C}_p$ és $|\cdot|$ megszorítása $\overline{\mathbb{Q}}_p$-re a p-adikus abszolútérték;*
- *$\mathbb{C}_p$ teljes metrikus tér;*
- *$\overline{\mathbb{Q}}_p$ sűrű $\mathbb{C}_p$-ben.*

Tovább nem kell folytatni, mert ez már algebrailag zárt test.

4.27. Állítás. *$\mathbb{C}_p$ algebrailag zárt.*

Bizonyítás. Legyen $f(X) \in \mathbb{C}_p[X]$ irreducibilis polinom. $\overline{\mathbb{Q}}_p$ sűrű $\mathbb{C}_p$-ben, ezért tetszőlegesen közel vehetünk egy azonos fokú $f_0(X) \in \overline{\mathbb{Q}}_p[X]$ polinom $f(X)$-hez. A 4.25. Következmény szerint, ha elegendően közel vettük a polinomot, akkor $f_0(X)$ irreducibilis $\mathbb{C}_p$ felett, tehát $\overline{\mathbb{Q}}_p$ felett is (hiszen egy felbontás $\overline{\mathbb{Q}}_p$ felett az felbontás lenne $\mathbb{C}_p$ felett is). Mivel $\overline{\mathbb{Q}}_p$ algebrailag zárt, így irreducibilis polinomok csak elsőfokúak lehetnek, ezért $f(X)$ is elsőfokú. Tehát bármely irreducibilis polinom elsőfokú, azaz $\mathbb{C}_p$ algebrailag zárt. □

5. Nemarkhimédeszi abszolútértékek $\mathbb{R}$-en

Két különböző bizonyítást is adunk arra, hogy létezik nemarkhimédeszi abszolútérték $\mathbb{R}$-en. Ostrowski tétele miatt (3.3. Tétel) ennek az abszolútértéknek a megszorítása $\mathbb{Q}$-ra valamelyik p-adikus abszolútértékkel lesz ekvivalens. Ha a megszorítás $\mathbb{Q}$-ra éppen a p-adikus abszolútérték, akkor azt mondjuk, hogy ez *egy* p-adikus abszolútérték $\mathbb{R}$-en. Látni

fogjuk, hogy nagyon sok p-adikus abszolútérték van $\mathbb{R}$-en. A két bizonyítás különböző fontos módszereket használ, és különböző érdekes eredmények is kijönnek közben, de mindkettőben közös, hogy a Zorn-lemma az alapjuk.

5.1. Algebrailag független, transzcendens bázis

Legyen B kommutatív gyűrű és A egy részgyűrűje. Legyenek $x_1, \dots, x_n \in B$. Minden $(v_1, \dots, v_n) = (v) \in \mathbb{N}^n$ szám n-esre és az $(x) = (x_1, \dots, x_n)$ jelölést használva, vezessük be az

$$M_{(v)}(x) = x_1^{v_1} \cdots x_n^{v_n}$$

jelölést.
Minden $f \in A[X_1, \dots, X_n] = A[X]$ polinom előáll $f = \sum a_{(v)} M_{(v)}(X)$ alakban valamilyen $a_{(v)} \in A$ együtthatókkal. Legyen az $\mathrm{ev}_{(x)} : A[X] \to B$ gyűrűhomomorfizmus, amire $f \mapsto f(x)$.

5.1. Definíció. Azt mondjuk, hogy $x_1, \dots, x_n \in B$ *algebrailag független A fölött*, ha az $\mathrm{ev}_{(x)}$ függvény injektív, azaz ha $f \in A[X]$ polinomra $f(x) = 0$, akkor f minden együtthatója 0.

Egy $S \subset B$ halmazt akkor mondunk *algebrailag függetlennek A fölött*, ha bármilyen véges részhalmaza algebrailag független.

5.2. Megjegyzés. A két definíció megegyezik véges halmazokra, hiszen ha $x_1, \dots, x_n$ algebrailag független, akkor ennek egy $\{x_{i_1}, \dots, x_{i_k}\} \subset \{x_1, \dots, x_n\}$ részhalmaza is algebrailag független, mert $A[X_{i_1}, \dots, X_{i_k}] \subset A[X_1, \dots, X_n]$.

Legyen L/K testbővítés. L azon részhalmazai között, melyek algebrailag függetlenek K fölött, be tudunk vezetni egy részbenrendezést. Legyenek $S, T \subset L$ algebrailag függetlenek, ekkor

$$S \preceq T \Leftrightarrow S \subseteq T.$$

5.3. Definíció. Egy $S \subset L$ algebrailag független részhalmazt *transzcendens bázis*nak hívunk, ha a $\preceq$ részbenrendezés szerint maximális.

5.4. Megjegyzés. Ha S egy transzcendens bázis, akkor L algebrai $K(S)$ (a legkisebb test, ami tartalmazza K-t és S-et) fölött. Ha S algebrailag független és $L/K(S)$ algebrai, akkor S transzcendens bázis.

Bizonyítás. Tegyük fel, hogy $L/K(S)$ nem algebrai. Ekkor létezik $\alpha \in L$, aminek nincs minimálpolinomja $K(S)$ fölött. A $T = S \cup \{\alpha\}$ algebrailag független, ami azt mutatja, hogy S nem maximális:

1) Ha $\{x_1, \dots, x_n\} \subset S$, akkor $x_1, \dots, x_n$ algebrailag független, mert S az.

2) Nézzük az $\{x_1, \dots, x_n, \alpha\} \subset T$ halmazt. Ez is algebrailag független:

Tegyük fel, hogy nem az, azaz létezik egy $0 \neq f(X_1, \dots, X_{n+1}) \in K[X_1, \dots, X_{n+1}]$ polinom, amire $f(x_1, \dots, x_n, \alpha) = 0$. Ha f az X_{n+1} változójában nulladfokú lenne, akkor $x_1, \dots, x_n$ nem lenne algebrailag független K fölött. Tehát

$$g(X) = f(x_1, \dots, x_n, X) \in K(S)[X]$$

polinomra $g(\alpha) = 0$ és $g \neq 0$, azaz létezik α-nak minimálpolinomja $K(S)$ fölött, g egyik irreducibilis osztója.

Másik irány: tegyük fel, hogy nem transzcendens bázis, azaz létezik $S \subsetneq T$ algebrailag független halmaz, speciálisan $x \in T$, $x \notin S$ és $S \cup \{x\}$ algebrailag független. Mivel $L/K(S)$ algebrai, ezért létezik $K(S)$ együtthatós minimálpolinomja x-nek. Ez azonban azt jelenti, hogy $S \cup \{x\}$ nem lehet alegbrailag független. □

5.5. Állítás. *Minden testbővítésnek létezik transzcendens bázisa. Minden algebrailag független halmaz kiegészíthető transzcendens bázissá.*

Bizonyítás. Tekintsük az L/K testbővítést. Zorn lemmával bizonyítjuk, hogy létezik transzcendens bázis. Vegyük L algebrailag független részhalmazainak halmazát. (Nem üres, mert a $\emptyset$ üres halmazt tartalmazza.) Ez részbenrendezett halmaz a $\preceq$ rendezéssel. Vegyünk egy láncot, azaz egy $\{S_r : r \in A\}$ halmazt, ahol S_r algebrailag független, A tetszőleges indexhalmaz és bármely kettő rendezett, azaz egyik halmaz tartalmazza a másikat. Ekkor $S = \bigcup_{r \in A} S_r$ algebrailag független K fölött. Legyen $\{x_1, \dots, x_n\} \subset S$, ekkor létezik $r_1, \dots, r_n \in A$, amikre $x_j \in S_{r_j}$. Mivel bármely két halmaz rendezett, ezért feltehetjük, hogy $S_{r_1} \subseteq S_{r_2} \subseteq \dots \subseteq S_{r_n}$, tehát $\{x_1, \dots, x_n\} \subset S_{r_n}$. S_{n_r} algebrailag független, ezért ennek minden részhalmaza is, tehát $x_1, \dots, x_n$ algebrailag független K fölött. Tehát S is az, mivel minden véges részhalmaza az, vagyis minden láncnak van felső korlátja. A Zorn lemma szerint van maximális elem, ez definíció szerint transzcendens bázis.

Legyen S algebrailag független halmaz. Ugyanúgy a Zorn lemmát használjuk. Vegyük L azon algebrailag független részhalmazainak $\mathcal{H}$ halmazát, amik tartalmazzák S-et. (Szintén nem üres, mert S-et tartalmazza.) A láncfeltétel ellenőrzése ugyanúgy működik, kivéve, hogy azt is ellenőrizni kell, hogy a lánc tagjainak az uniója tartalmazza S-et. Ez pedig nyilvánvaló, mert a lánc minden tagja tartalmazza. Vagyis létezik ennek a halmaznak maximális eleme, legyen ez T. Ekkor T transzcendens bázis. Ha lenne őt tartalmazó T_0 algerbrailag független halmaz, akkor T_0 benne lenne $\mathcal{H}$-ban, mert $T_0 \supset T \supset S$, vagyis T_0 is tartalmazza S-et. Ez azonban nem lehet, mert T maximális volt $\mathcal{H}$-ban. □

5.6. Állítás. *Minden transzcendens bázis számossága egyenlő.*

Bizonyítás. Legyen L/K testbővítés. Tegyük fel, hogy létezik véges transzcendens bázis, azaz egy $\{x_1, \dots, x_m\} \subset L$, $m \geq 1$ algebrailag független halmaz, amit nem tartalmaz másik algebrailag független halmaz. Ekkor elég megmutatni, hogy ha $w_1, \dots, w_n \in L$ algebrailag függetlenek, akkor $n \leq m$, mert ha transzcendens bázis is, akkor megcserélve a szerepeket $n \geq m$ is igaz. $w_1, x_1, \dots, x_m$ nem algebrailag független, tehát létezik $0 \neq f_1 \in K[X_1, \dots, X_{m+1}]$ polinom, amire $f_1(w_1, x_1, \dots, x_m) = 0$. (Valójában feltehető az is, hogy f_1 irreducibilis, mert f_1 valamelyik irreducibilis osztója 0, mivel L test nullosztómentes.) Ha f_1 minden X_i változójában nulladfokú $2 \leq i \leq m+1$ esetén, akkor valójában f_1 1-változós, nemnulla polinom, amire $f_1(w_1) = 0$, tehát $w_1, \dots, w_n$ nem lehet algebrailag független. Feltehetjük, hogy X_2 változójában nem nulladfokú f_1. (Esetleg átindexeljük x_i-ket.) Tehát

$$f_1(X_1, \dots, X_{m+1}) = \sum_j g_j(X_1, X_3, \dots, X_{m+1}) X_2^j,$$

ahol legalább az egyik g_N polinom nemnulla valamelyik $N \geq 1$-re. Ekkor g_N semelyik irreducibilis osztója sem tűnhet el $(w_1, x_2, \dots, x_m)$-en. Tegyük fel, hogy van ilyen, legyen ez $h(X_1, X_3, \dots, X_{m+1})$, ekkor $h(X_1, x_2, \dots, x_m) \in K(x_1, \dots, x_m)[X_1]$ és $f_1(X_1, x_1, \dots, x_m) \in K(x_1, \dots, x_m)[X_1]$ két irreducibilis polinom, amik különböznek és

w_1 gyök, ami nem lehetséges. (Relatív prím polinomoknak létezik lineáris kombinációja, ami a konstans 1 polinom.) Tehát x_1 algebrai $K(w_1, x_2, \ldots, x_m)$ fölött, mert $f_1(w_1, X_2, x_2, x_3, \ldots, x_m) \in K(w_1, x_2, \ldots, x_m)[X_2]$ polinom legalább elsőfokú és x_1 gyöke. Ekkor $w_1, x_2, \ldots, x_m$ algebrailag független K fölött, mert ha nem, akkor létezik $0 \neq f(X_1, \ldots, X_m) \in K[X_1, \ldots, X_m]$ polinom, amire $f(w_1, x_2, \ldots, x_m) = 0$ és f az X_1 változójában legalább elsőfokú ($x_2, \ldots, x_m$ algebrailag független). Tehát w_1 algebrai $K(x_2, \ldots, x_m)$ fölött, vagyis $K(x_2, \ldots, x_m) \leq K(w_1, x_2, \ldots, x_m) \leq K(w_1, x_1, \ldots, x_m)$ két véges bővítés egymásutánja. Azaz $K(x_2, \ldots, x_m) \leq K(w_1, x_1, \ldots, x_m)$ véges bővítés, így $K(x_2, \ldots, x_m) \leq K(x_1, \ldots, x_m)$ is véges, de akkor x_1 algebrai $K(x_2, \ldots, x_m)$ fölött. Ez persze nem lehet, mert $x_1, \ldots, x_m$ algebrailag függetlenek. Tehát valóban kijött, hogy $w_1, x_2, \ldots, x_m$ algebrailag függetlenek K fölött, azaz x_1-et lecserélhettük w_1-re. Ekkor transzcendens bázis is lesz, mert $K(w_1, x_1, \ldots, x_m)/K(w_1, x_2, \ldots, x_m)$ algebrai és $L/K(w_1, x_1, \ldots, x_m)$ algebrai. Ezzel a módszerrel egyesével lecserélhetjük az x_i-ket w_i-kre. Ha $n > m$ teljesülne, akkor még maradna w_i, viszont már $w_1, \ldots, w_m$ is transzcendens bázis lenne, ami nem lehet, ha a w_i-k kezdetben algebrailag függetlenek voltak. Tehát azt kaptuk, hogy ha létezik véges transzcendens bázis, akkor minden transzcendens bázis véges és megegyezik az elemszámuk.

Tegyük fel, hogy létezik végtelen transzcendens bázis, ekkor az előzőek miatt nem létezik véges transzcendens bázis. Legyen S egy végtelen transzcendens bázis és T egy másik transzcendens bázis. Ekkor minden $s \in S$ algebrai $K(T)$ felett a megjegyzés miatt. Ha f az s minimálpolinomja $K(T)$ felett, akkor valamilyen véges $T_s \subset T$ halmazra $f \in K(T_s)[X]$ és ekkor s algebrai $K(T_s)$ felett. Vegyünk egy ilyen T_s véges halmazt minden $s \in S$-re. Ekkor $\bigcup_{s\in S} T_s$ transzcendens bázis lesz. Mivel $\bigcup_{s\in S} T_s \subset T$, ezért algebrailag független. S minden eleme algebrai $K(\bigcup_{s\in S} T_s)$ felett, tehát $K(\bigcup_{s\in S} T_s)(S)$ algebrai $K(\bigcup_{s\in S} T_s)$ felett. Ekkor $K(S) \subset K(\bigcup_{s\in S} T_s)(S)$, tehát $K(S)$ minden eleme algebrai $K(\bigcup_{s\in S} T_s)$ felett. S egy transzcendens bázis volt, ezért $L/K(S)$ algebrai, tehát L a $K(\bigcup_{s\in S} T_s)$ felett is algebrai. De mivel $\bigcup_{s\in S} T_s$ algebrailag független, ezért transzcendens bázis. Tartalmazza a T, ami algebrailag független, tehát $\bigcup_{s\in S} T_s = T$. Ebből következik, hogy

$$|T| = \left|\bigcup_{s\in S} T_s\right| \leq \sum_{s\in S} |T_s| \leq |S|\aleph_0 = |S|,$$

ahol kihasználtuk, hogy $|S|$ végtelen halmaz. Megcserélve S és T szerepét $|T| \geq |S|$ adódik, tehát bármely két transzcendens bázisra $|T| = |S|$. □

5.7. Definíció. Egy L/K testbővítés *transzcendenciafokának* nevezzük egy transzcendens bázisának számosságát, $\mathrm{trdeg}(L/K)$-val jelöljük.

5.8. Megjegyzés. Ha a K testet nem adjuk meg, akkor az L test prímtestét értjük alatta.

5.2. $\mathbb{C}$, $\overline{\mathbb{Q}}_p$ és $\mathbb{C}_p$ izomorf

5.9. Tétel. *Minden $p \geq 0$ karakterisztikára és nem megszámolható k számosságra izomorfia erejéig pontosan egy algebrailag zárt test létezik, aminek a karakterisztikája p, a számossága pedig k.*

Bizonyítás. Tegyük fel, hogy K_1 és K_2 két különböző algebrailag zárt test, amikre $|K_1| = |K_2| = k$ és $\mathrm{char}(K_1) = \mathrm{char}(K_2) = p$, azaz K_1 és K_2 prímteste megegyezik, legyen F ez a test.

5.10. Állítás. *Legyen L/K algebrai bővítés. Ha $|K| = \infty$, akkor $|L| = |K|$, ha $|K| < \infty$, akkor $|L| \leq \aleph_0$.*

Bizonyítás. Legyen $\overline{K}$ az algebrai lezártja K-nak, ekkor $|\overline{K}| = |K|$, ha $|K| = \infty$ és $|\overline{K}| = \aleph_0$, ha $|K| < \infty$. Innen könnyen látszik az Állítás, mert $K \leq L \leq \overline{K}$, tehát $|K| \leq |L| \leq |\overline{K}|$. □

5.11. Állítás. *Ha K algebrailag zárt test és F a prímteste, akkor $|K| = trdeg\ (K/F)$, ha K nem megszámolható.*

Bizonyítás. Legyen S a K/F bővítés egy transzcendens bázisa. Ekkor $K/F(S)$ algebrai bővítés. Ha $F(S)$ véges lenne, akkor az előző Állítás miatt $|K| \leq \aleph_0$, ami nem lehet, mert K nem megszámolható. Tehát $F(S)$ végtelen halmaz, de ekkor szintén az előző Állítás miatt $|K| = |F(S)|$. Megmutatjuk, hogy $|S| = |F(S)|$ és ezzel kész lesz az Állítás. Legyen $F[S]$ a legkisebb gyűrű, ami tartalmazza F-et és S-et. Ekkor

$$F(S) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : \{x_1, \ldots, x_n\} \subset S;\ f, g \in F[X_1, \ldots, X_n];\ g(x_1, \ldots, x_n) \neq 0 \right\}$$

és

$$F[S] = \{f(x_1, \ldots, x_n) : \{x_1, \ldots, x_n\} \subset S;\ f \in F[X_1, \ldots, X_n]\}.$$

Tehát $F[S] \subset F(S)$, vagyis $|F[S]| \leq |F(S)|$, illetve megadható egy $F(S) \to F[S] \times F[S]$ injekció. Egy $x \in F(S)$-nek vegyük egy tetszőleges $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ felírását és rendeljük hozzá az $(f(x_1, \ldots, x_n), g(x_1, \ldots, x_n))$ párt. (Több felírása is lehet x-nek, válasszuk ki bármelyiket. Ha x és y képe megegyezik, akkor a megfelelő f-ek és g-k is megegyeznek, tehát a hányadosuk is, x és y.) Vagyis ebből azt kapjuk, hogy $|F(S)| \leq |F[S]|^2 = |F[S]|$, mert $|F[S]| = \infty$, hiszen ha $F[S]$ véges lenne, akkor $|F[S]|^2$ is véges lenne, ami nem lehet, mert $\infty = |K| = |F(S)| \leq |F[S]|^2$.

$$F[S] \subset \bigcup_{n \geq 0} \{f(x_1, \ldots, x_k) : \{x_1, \ldots, x_k\} \subset S;\ f \in F[X_1, \ldots, X_k];\ \deg f = n\}$$

Adjunk felső becslést az unióban lévő halmaz számosságára. Mivel $\deg f = n$, ezért legfeljebb n változója van és feltehetjük, hogy pontosan n változója van. S végtelen halmaz, mert ha S véges lenne, akkor $F[S]$ megszámlálható, mert ugyanúgy szétválogatjuk f foka szerint és mivel $|F| \leq \aleph_0$, ezért $\leq \aleph_0$ n-edfokú polinom van, és $\leq \aleph_0$ számosságú halmazok megszámlálható unióját vesszük, ami megszámolható. Tehát $F[S]$ megszámolható, tehát $|F[S]|^2 \leq \aleph_0$, ami nem lehet, mert K nem megszámolható és már beláttuk, hogy $|K| \leq |F[S]|^2$. Vagyis S valóban végtelen halmaz. Mivel $|F| \leq \aleph_0$, ezért továbbra is $\leq \aleph_0$ n változós, n-edfokú polinom van. Az n változóba $|S|$-féle sok értéket helyettesíthetünk be, tehát legfeljebb $|S|^n = |S|$ sok behelyettesítés van, mert S végtelen halmaz. Vagyis az unióban lévő halmaz számosságára felső becslés $\aleph_0|S|$, ami $|S|$, mert $|S|$ végtelen számosság. Az unió megszámolható, azaz $|F[S]|$-re felső becslés $\aleph_0|S| = |S|$. Összefoglalva

$$|S| \leq |F(S)| = |F[S]| \leq |S|,$$

tehát $|S| = |F(S)|$, amit be akartunk látni. □

Tehát az Állításokat használva azt kapjuk, hogy $\text{trdeg}(K_1/F) = \text{trdeg}(K_2/F) = k$. Legyen S_1 a K_1/F, S_2 a K_2/F egy-egy transzcendens bázisa, ekkor $|S_1| = |S_2| = k$. Tehát létezik egy $\sigma : S_1 \to S_2$ bijekció a két halmaz között. Legyen $\tilde{\sigma} : F(S_1) \to F(S_2)$,

ami F-et fixen hagyja, ha pedig $x \in S_1$, akkor $\tilde{\sigma}(x) = \sigma(x)$. Ekkor $\tilde{\sigma}$ egy izomorfizmus. $K_1/F(S_1)$ algebrai, ezért K_1 az $F(S_1)$ algebrai lezártja, mert ha $x \in K_1$, akkor létezik $F(S_1)$ együtthatós polinom, aminek a gyöke, tehát benne van az algebrai lezártjában, illetve K_1 algebrailag zárt test, ami tartalmazza $F(S_1)$-et, tehát az algebrai lezártját is. K_2 hasonlóan az $F(S_2)$ algebrai lezártja, de $F(S_1)$ és $F(S_2)$ izomorfak, így az elgebrai lezártjuk, K_1 és K_2 is izomorf. □

5.12. Következmény. *$\mathbb{C}$, $\overline{\mathbb{Q}}_p$ és $\mathbb{C}_p$ izomorf testek.*

Bizonyítás. Mindhárom test karakterisztikája 0. $|\mathbb{C}| = \mathfrak{c}$, tehát azt kell belátni, hogy a másik kettő számossága is kontinuum. A 3.30. Lemma egy $\mathbb{Z}_p \to \{0, 1, \dots, p-1\}^{\mathbb{N}}$ hozzárendelést ad, ami injektív és szürjektív is, mivel egy $b_0 + b_1 p + b_2 p^2 + \dots$ felírás a $b_0 + b_1 p + \dots + b_n p^n$ sorozat limesze, ami egy $\mathbb{Z}$-beli Cauchy sorozat, mert $|b_n p^n| = p^{-n} \to 0$, tehát $\mathbb{Z}_p$-ben van és ez a limesz egyértelmű. Azaz minden felíráshoz is tartozik egy egyértelmű p-adikus egész. Tehát $\mathbb{Z}_p$ számossága $p^{\aleph_0} = \mathfrak{c}$. Mivel $\mathbb{Z}_p$-t mindegyik test tartalmazza, ezért csak azt kell belátni, hogy kontinuumnál $\leq$ a számosságuk. A 3.25. Állítás szerint $x \mapsto px$ bijekció, tehát $|p^n \mathbb{Z}_p| = |\mathbb{Z}_p|$ és

$$\bigcup_{n \in \mathbb{Z}} p^n \mathbb{Z}_p = \mathbb{Q}_p,$$

tehát $|\mathbb{Q}_p| \leq \aleph_0 \mathfrak{c} = \mathfrak{c}$. $\overline{\mathbb{Q}}_p$ és $\mathbb{Q}_p$ számossága megegyezik, mert $\mathbb{Q}_p$ végtelen halmaz, tehát $|\overline{\mathbb{Q}}_p| = \mathfrak{c}$.

5.13. Lemma. *Minden szeparábilis metrikus tér számossága $\leq \mathfrak{c}$.*

Bizonyítás. Legyen $A = (a_1, a_2, \dots)$ sűrű megszámlálható halmaz X metrikus térben. Legyen $X \to \mathbb{R}^{\mathbb{N}}$ az a függvény, ami egy $x \in X$ ponthoz hozzárendeli $(r_1, r_2, \dots)$ sorozatot, ahol $r_j = d(x, a_j)$, azaz x-nek az a_j-től mért távolsága. Ez a függvény injektív. Tegyük fel, hogy nem, azaz léteznek $x \neq y$ pontok, amik minden A-beli ponttól ugyanolyan távolságra vannak. Mivel A sűrű, ezért létezik $a \in A$ pont, hogy $d(x, a) < d(x, y)/2$, de y ugyanolyan távolságra van, azaz $d(y, a) < d(x, y)/2$ is teljesül. Ez azonban nem lehet, mert $d(x, y) \leq d(x, a) + d(y, a) < d(x, y)$. Mivel a függvény injektív, ezért $|X| \leq |\mathbb{R}|^{|\mathbb{N}|} = \mathfrak{c}^{\aleph_0} = \mathfrak{c}$. □

Tehát elég belátni, hogy $\mathbb{C}_p$ szeparábilis. A megszámlálható sűrű részhalmaz $\mathbb{Q}$ algebrai lezártja lesz. (Vegyük észre, hogy az megszámlálható.) Legyen $x \in \mathbb{C}_p$, ehhez akarunk közel találni egy $\overline{\mathbb{Q}}$-beli elemet. Legyen $\alpha \in \overline{\mathbb{Q}}_p$, amire $\alpha \in B(x, \varepsilon/2)$, mert $\overline{\mathbb{Q}}_p$ sűrű $\mathbb{C}_p$-ben. Legyen $f(X) \in \mathbb{Q}_p[X]$ az α minimálpolinom. Mivel $\mathbb{Q}$ sűrű $\mathbb{Q}_p$-ben, ezért létezik egy $g(X) \in \mathbb{Q}[X]$ polinom, ami 1-főegyütthatós, a foka megegyezik f fokával és minden együtthatója közel van f megfelelő együtthatójához. Bontsuk fel $g(X)$-et gyöktényezőkre $\overline{\mathbb{Q}}$-ban, azaz $g(X) = \prod(X - \lambda_i)$, ahol $\lambda_i \in \overline{\mathbb{Q}}$ a $g(X)$ gyökei. Ekkor valamelyik λ_i-re $|\alpha - \lambda_i| < \varepsilon/2$, mert ha ez nem lenne igaz, akkor α-t behelyettesítve $|g(\alpha)|$ nagy lenne, ami nem lehet, mert $g(X)$ közel van α minimálpolinomjához. Ekkor azonban $|x - \lambda_i| \leq |\alpha - \lambda_i| + |\alpha - x| < \varepsilon$, tehát tetszőleges $\mathbb{C}_p$-belihez találtunk tetszőlegesen közel $\overline{\mathbb{Q}}$-belit. □

5.14. Következmény. *Létezik p-adikus abszolútérték $\mathbb{R}$-en.*

Bizonyítás. Legyen $\sigma : \mathbb{C} \to \mathbb{C}_p$ izomorfizmus, $|\cdot|_p$ a p-adikus abszolútérték $\mathbb{C}_p$-n. Ekkor $|\cdot| : \mathbb{C} \to \mathbb{R}_+$, $|x| = |\sigma(x)|_p$ p-adikus abszolútérték $\mathbb{C}$-n. Ha $|x| = 0$, akkor

$|\sigma(x)|_p = 0$, tehát $\sigma(x) = 0$, $x = 0$. Ha $x \in \mathbb{Q}$, akkor $\sigma(x) = x$, tehát $|x| = |x|_p$. Legyenek $x, y \in \mathbb{C}$, ekkor $|xy| = |\sigma(xy)|_p = |\sigma(x)\sigma(y)|_p = |\sigma(x)|_p|\sigma(y)|_p = |x||y|$, illetve $|x+y| = |\sigma(x+y)|_p = |\sigma(x)+\sigma(y)|_p \leq \max\{|\sigma(x)|_p, |\sigma(y)|_p\} = \max\{|x|, |y|\}$ □

5.3. Másik bizonyítás

5.15. Állítás. *Minden 0 karakterisztikájú testen létezik p-adikus abszolútérték.*

Bizonyítás. Legyen K egy 0 karakterisztikájú test. Vegyük azon $(L, |\cdot|_L)$ rendezett párok $\mathcal{H}$ halmazát, amire $\mathbb{Q} \leq L \leq K$ test és $|\cdot|_L$ pedig kiterjesztése a $\mathbb{Q}$-n lévő p-adikus abszolútértéknek L-re. Definiáljuk ezen a halmazon a következő részbenrendezést:

$$(L, |\cdot|_L) \preceq (F, |\cdot|_F) \iff L \leq F \text{ és } |x|_L = |x|_F \text{ ha } x \in L.$$

Teljesül a Zorn-lemma feltétele, azaz minden láncnak van közös felső korlátja: vegyünk egy $(L_r, |\cdot|_{L_r})$ ($r \in A$ indexhalmaz) láncot. Ekkor felső korlát lesz $(\cup_{r\in A} L_r, |\cdot|)$, ahol $|\cdot|$ abszolútértéket úgy definiáljuk, hogy $|x| = |x|_{L_r}$, ha $x \in L_r$ valamilyen $r \in A$ indexre.

- $\cup_{r\in A} L_r$ test
  - Ha $x, y \in \bigcup_{r\in A} L_r$, akkor $x \in L_{r_x}$ és $y \in L_{r_y}$ valamilyen $r_x, r_y \in A$-ra. Mivel láncot vettünk, ezért az egyik test tartalmazza a másikat, tehát $x, y \in L_r$, ahol $r = r_x$ vagy $r = r_y$. L_r test, ezért $x + y \in L_r$ és $xy \in L_r$, illetve ebben a testben kommutatívak a műveletek, ezért $x + y, xy \in \bigcup_{r\in A} L_r$ és ebben a testben is kommutatívak. Ha három elemet veszünk, akkor hasonlóan megmutatható, hogy asszociatívak is és a szorzás disztributív az összeadásra. Továbbá $x \in \bigcup_{r\in A} L_r$ esetén létezik $r \in A$, hogy $x \in L_r$, ekkor $-x \in L_r$ és $1/x \in L_r$, ha $x \neq 0$, tehát $-x, 1/x \in \bigcup_{r\in A} L_r$.
- $|\cdot|$ jóldefiniált
  - Minden $x \in \bigcup_{r\in A} L_r$ elemre rendeltünk hozzá abszolútértéket. Ha $x \in L_r$ és $x \in L_s$ is teljesül, akkor mivel láncot vettünk, ezért feltehetjük, hogy $(L_r, |\cdot|_{L_r}) \preceq (L_s, |\cdot|_{L_s})$. Egyrészt $|x| = |x|_{L_r}$, másrészt $|x| = |x|_{L_s}$, de $\preceq$ rendezés miatt $x \in L_r \leq L_s$ és $|x|_{L_r} = |x|_{L_s}$, tehát $|\cdot|$ egyértelmű.
- $|\cdot|$ abszolútérték
  - A nulla elem minden testben benne van. Veszünk egy tetszőlegeset a láncból, ebben a nulla abszolútértéke 0, ezért $|0| = 0$. Ha $x \in \bigcup_{r\in A} L_r$, $|x| = 0$, akkor $x \in L_r$ valamilyen $r \in A$ indexre és $|x| = |x|_{L_r}$. Tehát $|x|_{L_r} = 0$ és $|\cdot|_{L_r}$ abszolútérték, tehát $x = 0$ teljesül. Egy korábbi ponthoz hasonlóan, ha $x, y \in \bigcup_{r\in A} L_r$, akkor $x, y, xy, x + y \in L_r$ valamilyen indexre és mivel $|\cdot|_{L_r}$ abszolútérték, ezért $|x|_{L_r}|y|_{L_r} = |xy|_{L_r}$ és $|x + y|_{L_r} \leq |x|_{L_r} + |y|_{L_r}$, tehát $|x||y| = |xy|$ és $|x + y| \leq |x| + |y|$.
- $(\cup_{r\in A} L_r, |\cdot|) \in \mathcal{H}$
  - Minden $r \in A$ indexre $\mathbb{Q} \leq L_r \leq K$, ezért $\mathbb{Q} \leq \bigcup_{r\in A} L_r \leq K$, illetve ha $x \in \mathbb{Q}$, akkor $|x| = |x|_{L_r}$ akármelyik $r \in A$ indexre. Mivel $|\cdot|_{L_r}$ a p-adikus abszolútérték kiterjesztése, ezért $|x| = |x|_p$.

Tehát $\mathcal{H}$-ban van maximális elem, legyen ez $(L_0, |\cdot|_{L_0})$. Megmutatjuk, hogy $L_0 = K$, azaz K-n valóban létezik $|\cdot|_K$ p-adikus abszolútérték. Tegyük fel, hogy $L_0 \neq K$, azaz létezik $\alpha \in K$, $\alpha \notin L_0$ elem. Ekkor az $L_0(\alpha)$ szigorúan nagyobb testen létezik abszolútérték, ami az $|\cdot|_{L_0}$ kiterjesztése, ami ellentmond annak, hogy $(L_0, |\cdot|_{L_0})$ maximális elem $\mathcal{H}$-ban. Definiáljuk a $|\cdot|$ abszolútértéket $L_0(\alpha)$-n: ha α transzcendens, akkor $|\alpha|$ legyen tetszőleges pozitív valós szám. $L_0(\alpha)$ elemei $f(\alpha)/g(\alpha)$ alakúak, ahol $f, g \in L_0[X]$ polinom, $g(\alpha) \neq 0$. Legyen $f(X) = a_0 + a_1X + \cdots + a_nX^n \in L_0[X]$ polinom, ekkor $|f(\alpha)| = \max_i(|a_i|_{L_0}|\alpha|^i)$. Törtekre pedig $|f(\alpha)/g(\alpha)| = |f(\alpha)|/|g(\alpha)|$. Ha $x \in L_0$, akkor az $f \equiv x$, $g \equiv 1$ konstans polinomokkal kiszámolva x $|\cdot|$ abszolútértékét $|f(\alpha)/g(\alpha)| = |f(\alpha)|/|g(\alpha)| = |x|_{L_0}/|1|_{L_0} = |x|_{L_0}$, tehát $|\cdot|$ valóban $|\cdot|_{L_0}$ kiterjesztése. Ha $|f(\alpha)| = 0$, akkor $|a_i|_{L_0}|\alpha|^i = 0$ minden i-re. Mivel $|\alpha|$ pozitív, ezért ez azt jelenti, hogy $|a_i| = 0$ minden i-re, tehát f az azonosan 0 polinom, $f(\alpha) = 0$. Ha $|f(\alpha)/g(\alpha)| = 0$, akkor szintén $f(\alpha) = 0$. Multiplikativitás: elég bizonyítani, hogy ha $f(X) = a_0 + a_1X + \cdots + a_nX^n$ és $g(X) = b_0 + b_1X + \cdots + b_kX^k$ L_0 együtthatós polinomok, akkor $|f(\alpha)||g(\alpha)| = |f(\alpha)g(\alpha)|$. Tudjuk, hogy $|\cdot|_{L_0}$ a p-adikus abszolútérték kiterjesztése, ezért 2.9. Tétel miatt nemarkhimédeszi.

$$f(X)g(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_nb_kX^{n+k} = c_0 + c_1X + \cdots + c_{n+k}X^{n+k}$$

Definíció szerint $|f(\alpha)g(\alpha)| = \max_{0\leq i\leq n+k}(|c_i|_{L_0}|\alpha|^i)$, illetve $|c_i|_{L_0} \leq \max_j(|a_jb_{i-j}|_{L_0})$, mert $|\cdot|_{L_0}$ nemarkhimédeszi, tehát

$$|f(\alpha)g(\alpha)| \leq \max(|a_j|_{L_0}|\alpha|^j|b_{i-j}|_{L_0}|\alpha|^{i-j}) \leq |f(\alpha)||g(\alpha)|,$$

ahol a második egyenlőtlenséget úgy kapjuk, hogy max-ban minden tag felülről becsülhető a szorzattal. Legyen i a legkisebb index ahol $|f(\alpha)|$ és j a legkisebb index ahol $|g(\alpha)|$ felveszi a maximumát, azaz $|f(\alpha)| = |a_i|_{L_0}|\alpha|^i$, $|g(\alpha)| = |b_j|_{L_0}|\alpha|^j$ és $|a_l|_{L_0}|\alpha|^l < |a_i|_{L_0}|\alpha|^i$, ha $l < i$, illetve $|b_l|_{L_0}|\alpha|^l < |b_j|_{L_0}|\alpha|^j$, ha $l < j$. Ekkor

$$|c_{i+j} - a_ib_j|_{L_0} \leq \max\{|a_0b_{i+j}|_{L_0}, \ldots, |a_{i-1}b_{j+1}|_{L_0}, |a_{i+1}b_{j+1}|_{L_0}, \ldots, |a_{i+j}b_0|_{L_0}\},$$

$$|c_{i+j} - a_ib_j|_{L_0}|\alpha|^{i+j} \leq \max\{|a_0b_{i+j}|_{L_0}, \ldots, |a_{i-1}b_{j+1}|_{L_0}, |a_{i+1}b_{j+1}|_{L_0}, \ldots, |a_{i+j}b_0|_{L_0}\}|\alpha|^{i+j}.$$

(Esetleg a max-ban néhány tag nem létezik, de ez nem fontos.) Bevisszük az max-ba az $|\alpha|^{i+j}$-t és $|a_kb_{i+j-k}|_{L_0}|\alpha|^{i+j} < |a_i|_{L_0}|\alpha|^i|b_j|_{L_0}|\alpha|^j$, mert az egyik $\leq$, a másik pedig szigorúan $<$ az i és j minimalitása miatt. Tehát

$$|c_{i+j} - a_ib_j|_{L_0}|\alpha|^{i+j} < |a_i|_{L_0}|b_j|_{L_0}|\alpha|^{i+j},$$

$$|c_{i+j} - a_ib_j|_{L_0} < |a_i|_{L_0}|b_j|_{L_0} = |a_ib_j|_{L_0}.$$

Használhatjuk a 2.15. Állítást és azt kapjuk, hogy

$$|c_{i+j}|_{L_0} = |(c_{i+j} - a_ib_j) + a_ib_j|_{L_0} = |a_ib_j|_{L_0},$$

$$|c_{i+j}|_{L_0}|\alpha|^{i+j} = |a_ib_j|_{L_0}|\alpha|^{i+j} = |f(\alpha)||g(\alpha)|.$$

Vagyis találtunk egy indexet, $(i + j)$-t, ahol $|f(\alpha)g(\alpha)|$ éppen megegyezik, tehát

$$|f(\alpha)g(\alpha)| = \max_{0\leq l\leq k+n}(|c_l|_{L_0}|\alpha|^l) \geq |c_{i+j}|_{L_0}|\alpha|^{i+j} = |f(\alpha)||g(\alpha)|$$

a fordított irányú egyenlőtlenséget is beláttuk, azaz $|f(\alpha)g(\alpha)| = |f(\alpha)||g(\alpha)|$.

Legyenek $f, g \in L_0[X]$ polinomok, ekkor belátjuk, hogy

$$|f(\alpha) + g(\alpha)| \leq \max\{|f(\alpha)|, |g(\alpha)|\}.$$

Feltehetjük, hogy azonos a polinomok foka, mert a kisebb fokút kipótoljuk 0-s együtthatókkal, legyen $f(X) = a_0 + a_1X + \cdots + a_nX^n$, $g(X) = b_0 + b_1X + \cdots + b_nX^n$. Ekkor

$$|f(\alpha) + g(\alpha)| = \max_{1\leq i\leq n}(|a_i + b_i|_{L_0}|\alpha|^i) \leq \max_{1\leq i\leq n}(\max\{|a_i|_{L_0}, |b_i|_{L_0}\}|\alpha|^i) =$$

$$= \max\left\{\max_{1\leq i\leq n}(|a_i|_{L_0}|\alpha|^i), \max_{1\leq i\leq n}(|b_i|_{L_0}|\alpha|^i)\right\} = \max\{|f(\alpha)|, |g(\alpha)|\}.$$

Törtekre:

$$\left|\frac{f(\alpha)}{g(\alpha)} + \frac{h(\alpha)}{k(\alpha)}\right| \leq \max\left\{\left|\frac{f(\alpha)}{g(\alpha)}\right|, \left|\frac{h(\alpha)}{k(\alpha)}\right|\right\}$$

ezt kell belátni, szorozzuk fel $|g(\alpha)k(\alpha)|$-val és használjuk a multiplikativitást.

$$|f(\alpha)k(\alpha) + h(\alpha)g(\alpha)| \leq \max\{|f(\alpha)k(\alpha)|, |h(\alpha)g(\alpha)|\}$$

Ezt pedig polinomokra már beláttuk. Tehát ha α transzcendens, akkor létezik abszolútérték $L_0(\alpha)$-n, ami a kiterjesztése $|\cdot|_{L_0}$-nak.

Tegyük fel, hogy α algebrai, azaz $L_0(\alpha)/L_0$ véges és $L_0(\alpha)$-ra akarjuk kiterjeszteni $|\cdot|_{L_0}$-t. A Véges bővítések fejezetben leírtak alapján egyetlen ilyen kiterjesztés van és azt $|x| = \sqrt[n]{|N_{L_0(\alpha)/L_0}(x)|_{L_0}}$ képlettel kapjuk, ahol $n = |L_0(\alpha) : L_0|$. Annak a bizonyítása, hogy ez valóban abszolútérték a Hensel lemmán múlik, amihez pedig az kellett, hogy $\mathbb{Q}_p$ teljes. Tegyük teljessé L_0-t a $|\cdot|_{L_0}$ abszolútérték szerint, legyen ez a test L_1. Legyen f az α minimálpolinomja L_0 felett. Ekkor f irreducibilisek szorzatára bomlik L_1 fölött, legyen ez $f = f_1 \dots f_k$. Vegyük f_1 egy gyökét, legyen ez α_1. Ekkor az $L_1(\alpha_1)$ bővítése L_1-nek véges és L_1 teljes, tehát működik a Hensel lemma, ezért a bizonyításunk arra is, hogy $L_1(\alpha_1)$-en létezik abszolútérték, ami a kiterjesztése $|\cdot|_{L_1}$-nek. Az $L_0(\alpha)$ és az $L_0(\alpha_1)$ testek izomorfak, mert α és α_1 konjugáltak. Tehát az $L_1(\alpha_1)$ testen lévő abszolútértéket megszorítva $L_0(\alpha_1)$-re, majd áthúzva $L_0(\alpha)$-ra egy abszolútértéket kapunk $L_0(\alpha)$-n, ami triviálisan az $|\cdot|_{L_0}$ abszolútérték kiterjesztése.

A feltevésünk hibás volt, tehát $L_0 = K$, azaz létezik $\mathcal{H}$-ban $(K, |\cdot|_K)$ pár. Vagyis létezik K testen abszolútérték, ami a $\mathbb{Q}$-n lévő p-adikus abszolútérték kiterjesztése. □

5.16. Következmény. *Létezik p-adikus abszolútérték $\mathbb{R}$-en.*

6. Monsky tétel

Legyen R egy nem üres, zárt, összefüggő halmaz a síkon, aminek a határa egy zárt töröttvonal. Bontsuk fel R-et véges sok zárt háromszöglap uniójára, ahol bármely kettő metszete üres, egy pont vagy egy szakasz. Legyenek ezek a háromszöglapok a T_i-k. Nevezzük *csúcs*nak a T_i háromszögek csúcsait (tehát R csúcsai is csúcsok), illetve *oldal*nak az R sokszög és a T_i háromszögek oldalait. Könnyen előfordulhat, hogy egy oldalon több csúcs is van. Nevezzünk *szomszédos*nak két csúcsot, ha egy oldalon vannak és ezen az oldalon nincs köztük másik csúcs. A két szomszédos csúcs közti szakaszt pedig nevezzük el *egyszerű szakasz*nak. Így T_i és R határai is egyszerű szakaszok uniója, ahol két egymás melletti egy csúcsban találkozik. Az összes csúcsot színezzük ki az $\mathcal{A}$, $\mathcal{B}$ vagy $\mathcal{C}$ színek valamelyikére. Azt mondjuk, hogy egy oldal vagy egy egyszerű szakasz $\mathcal{AB}$ *típusú*, ha az egyik végpontja $\mathcal{A}$-ban, a másik $\mathcal{B}$-ben van.

6.1. Lemma. *Tegyük fel, hogy semelyik oldal sem tartalmaz $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű csúcsot egyszerre, illetve R határa páratlan sok $\mathcal{AB}$ típusú oldalt tartalmaz. Ekkor létezik T_i háromszög, aminek a három csúcsa $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű.*

Bizonyítás. Egy $\mathcal{AB}$ típusú oldal összesen páratlan sok $\mathcal{AB}$ típusú egyszerű szakaszt tartalmaz:

Mivel $\mathcal{C}$ színű csúcs már nem lehet ezen az oldalon, ezért csak $\mathcal{A}$ és $\mathcal{B}$ színű lehet. Ha egymás mellé esik két azonos színű csúcs, akkor a köztük lévő szakasz nem számít, akár össze is húzhatjuk őket, az $\mathcal{AB}$ típusú egyszerű szakaszok számán nem változtat. Tehát feltehetjük, hogy felváltva vannak $\mathcal{A}$ és $\mathcal{B}$ színű csúcsok, az első $\mathcal{A}$ színű, az utolsó $\mathcal{B}$ színű. Ilyenkor nyilvánvalóan páratlan sok $\mathcal{AB}$ típusú egyszerű szakasz van.

Egy nem $\mathcal{AB}$ típusú oldalon páros sok $\mathcal{AB}$ típusú egyszerű szakasz van:

Ha van $\mathcal{C}$ színű pont az oldalon, akkor nem lehet $\mathcal{AB}$ típusú egyszerű szakasz, mivel mindhárom szín nem lehet egyszerre az oldalon. Tehát csak $\mathcal{A}$ és $\mathcal{B}$ színű csúcsok lehetnek. Ekkor az oldal két végpontja azonos színű ($\mathcal{A}$ vagy $\mathcal{B}$). Az előző bekezdéshez hasonlóan húzzuk össze az azonos színű, egymás melletti csúcsokat, így megint felváltva jönnek a pontok. Szintén látszik, hogy ekkor viszont páros sok $\mathcal{AB}$ típusú egyszerű szakasz van.

Egy háromszög pontosan akkor tartalmaz páratlan sok $\mathcal{AB}$ típusú oldalt, ha a három csúcsa $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű:

Ahhoz, hogy legyen $\mathcal{AB}$ színű oldal, kell egy $\mathcal{A}$ és egy $\mathcal{B}$ színű csúcs. Ha a harmadik csúcs $\mathcal{A}$ vagy $\mathcal{B}$ színű, akkor 2 $\mathcal{AB}$ típusú oldal lesz, ha pedig $\mathcal{C}$, akkor 1.

Tehát az is igaz, hogy egy háromszög három oldalán pontosan akkor van páratlan sok $\mathcal{AB}$ típusú egyszerű szakasz, ha a háromszög három csúcsa $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű.

Tegyük fel a Lemma állításával ellentétben, hogy nem létezik ilyen háromszög és számoljuk az $\mathcal{AB}$ típusú egyszerű szakaszokat. Minden T_i háromszögben páros sok $\mathcal{AB}$ típusú egyszerű szakasz van, tehát háromszögenként összeadva az egyszerű szakaszokat páros számot kapunk. Ugyanakkor így minden belső oldalon kétszer számoltuk az $\mathcal{AB}$ típusú egyszerű szakaszokat, R határán viszont egyszer, tehát az összeg paritása megegyezik az R határán lévő $\mathcal{AB}$ típusú egyszerű szakaszok paritásával. Tehát R határán páros sok $\mathcal{AB}$ típusú egyszerű szakasz van. Ez azonban ellentmond azzal, hogy R határán páratlan sok $\mathcal{AB}$ típusú oldal van, mert így páratlan sok $\mathcal{AB}$ típusú egyszerű szakasznak is kell lennie. Vagyis létezik T_i háromszög, aminek a három csúcsa $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű. □

6.2. Tétel (Monsky)**.** *Nem lehet felbontani egy négyzetet páratlan sok azonos területű háromszögre.*

Bizonyítás. Természetesen elegendő megmutatni, hogy nem lehetséges a felbontás, ha $S = [0,1] \times [0,1]$ a felbontandó négyzet. Tegyük fel, hogy mégis felbontottuk a négyzetet m darab egyenlő területű háromszögre. Vegyünk egy 2-adikus $|\cdot|$ abszolútértéket $\mathbb{R}$-en, azaz teljesül $|2| = 1/2 < 1$. Színezzük ki a sík (x, y) koordinátájú pontjait a következőképpen:

$\mathcal{A}$ ha $|x| < 1$ és $|y| < 1$;

$\mathcal{B}$ ha $|x| \geq 1$ és $|x| \geq |y|$;

$\mathcal{C}$ ha $|y| \geq 1$ és $|y| > |x|$.

Ez a színezés partícionálja a síkot, mert

$$\mathcal{A} \cap \mathcal{B} \subset \{(x,y) \in \mathbb{R}^2 : |x| < 1\} \cap \{(x,y) \in \mathbb{R}^2 : |x| \geq 1\} = \emptyset,$$

$$\mathcal{A} \cap \mathcal{C} \subset \{(x,y) \in \mathbb{R}^2 : |y| < 1\} \cap \{(x,y) \in \mathbb{R}^2 : |y| \geq 1\} = \emptyset,$$

$$\mathcal{B} \cap \mathcal{C} \subset \{(x,y) \in \mathbb{R}^2 : |x| \geq |y|\} \cap \{(x,y) \in \mathbb{R}^2 : |y| > |x|\} = \emptyset,$$

tehát $\mathcal{A} \cap \mathcal{B} = \mathcal{A} \cap \mathcal{C} = \mathcal{B} \cap \mathcal{C} = \emptyset$. Tegyük fel, hogy $(x,y) \notin \mathcal{A}$, azaz $|x| \geq 1$ vagy $|y| \geq 1$. Ekkor az kell, hogy $(x,y) \in \mathcal{B} \cup \mathcal{C}$. Tegyük fel, hogy $(x,y) \notin \mathcal{B}$, azaz $|x| < 1$ vagy $|x| < |y|$. Ha $|x| \geq 1$, akkor $|x| < |y|$ is teljesül, hogy $(x,y) \notin \mathcal{B}$ is igaz legyen, de ekkor $1 \leq |x| < |y| \Rightarrow 1 \leq |y|$, azaz $(x,y) \in \mathcal{C}$. Ha viszont $|x| < 1$, akkor $|y| \geq 1$, hogy $(x,y) \notin \mathcal{A}$ igaz legyen, azonban $|x| < 1 \leq |y| \Rightarrow |x| < |y|$, tehát $(x,y) \in \mathcal{C}$. Tehát minden pontot kiszíneztünk valamilyen színűre.

Legyen $P = (x,y)$ és $P' = (x',y')$ két pont, amik egymás eltoltjai egy $\mathcal{A}$ színű ponttal (vektorral), azaz $|x - x'| < 1$ és $|y - y'| < 1$. ($|x| = |-x|$ miatt mindegy, hogy melyik pontot toljuk el.) Ekkor P és P' azonos színűek:

Ha P $\mathcal{A}$ színű, akkor $|x'| \leq \max\{|x - x'|, |x'|\} < 1$ és ugyanígy az y koordinátára, tehát P' is $\mathcal{A}$ színű.

Ha P $\mathcal{B}$ színű, akkor 2.15. Állítás miatt $|x'| = \max\{|x|, |x' - x|\} = |x| \geq 1$, illetve $|x| \geq 1$ és $|x| \geq |y|$ miatt $|x| \geq \max\{1, |y|\}$, ezért

$$|x'| = |x| \geq \max\{1, |y|\} \geq \max\{|y' - y|, |y|\} \geq |y'|,$$

tehát P' is $\mathcal{B}$ színű.

Ha P $\mathcal{C}$ színű, akkor az előzőhöz hasonlóan $|y'| = |y| \geq 1$ és

$$|y'| = |y| \geq \max\{1, |x|\} \geq \max\{|x' - x|, |x|\} \geq |x'|,$$

ahol egyenlőség nem teljesülhet, mert akkor mindenhol egyenlőség kell hogy legyen. Az elsőnél $|y| > |x|$, ezért $\max\{1, |x|\} = 1$ (és $|y| = 1$), de a másodiknál emiatt csak akkor lehet egyenlőség, ha $\max\{|x' - x|, |x|\} = |x| = 1$, mert $1 > |x' - x|$. Tehát egyszerre kell teljesüljön az egyenlőséghez $|x| = 1$ és $|y| = 1$, ami nem lehet, mert $|y| > |x|$. Vagyis P' is $\mathcal{C}$ színű.

Semelyik egyenes sem tartalmazhat egyszerre $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű pontot: legyen e egyenes. Ha e-n nincs $\mathcal{A}$ színű pont, akkor az állítás igaz. Ha tartalmaz $\mathcal{A}$ színű pontot, akkor tegyük fel, hogy $\mathcal{B}$ és $\mathcal{C}$ színű pontot is tartalmaz, és toljuk el az egyenest úgy, hogy az $\mathcal{A}$ színű pont a $(0,0)$-ba menjen. (Ez egy $\mathcal{A}$ színű ponttal való eltolás, mert $|x| = |-x|$.) Az előbbiek alapján így minden pont színe változatlan marad, és ezen az e' egyenesen, ami átmegy az origón, lesz $\mathcal{B}$ és $\mathcal{C}$ színű pont is. Legyen egy $\mathcal{B}$ színű pont (x,y), egy $\mathcal{C}$ színű pedig (x',y'). Egyrészt $xy' = x'y$, mert e' átmegy az origón, másrészt a színezés miatt $|x| \geq |y|$ és $|y'| > |x'|$. Ha $y \neq 0$, akkor valamilyen $\varepsilon > 0$ számra $|y'| = |x'| + \varepsilon$, és így $|x||y'| \geq |y|(|x'| + \varepsilon) = |y||x'| + |y|\varepsilon > |y||x'|$, tehát $|xy'| > |x'y|$, ami nem lehet. Ha pedig $y = 0$, akkor $x'y = 0$, de $x \neq 0$, mert $|x| \geq 1$ és $y' \neq 0$, mert $|y'| \geq 1$, tehát $xy' \neq 0 = x'y$. (Ebben az esetben is $|xy'| > |x'y|$.) Vagyis megmutattuk, hogy nem lehet egyszerre $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű pont is semelyik egyenesen sem.

Legyen T egy háromszög $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű csúcsokkal. Toljuk el a háromszöget, hogy az $\mathcal{A}$ színű pont az origóba kerüljön. A kapott háromszög legyen T'. Ismét $\mathcal{B}$ és $\mathcal{C}$ színű marad a másik kettő csúcs, amik legyenek az (x,y) és az (x',y'). Az előző bekezdéshez hasonlóan $|xy'| > |x'y|$. A T' háromszög területe $t(T') = \pm\frac{1}{2}(xy' - x'y)$,

ahol $\pm$ azt jelöli, hogy a terület pozitív, de az előjelkülönbség úgysem okoz problémát amikor abszolútértéket veszünk. A 2.15. Állítás miatt

$$|xy' - x'y| = \max\{|xy'|, |-x'y|\} = |xy'|,$$

tehát

$$|t(T)| = |t(T')| = \left|\frac{1}{2}(xy' - x'y)\right| = \left|\frac{1}{2}\right| |xy'| \geq 2 > 1.$$

Térjünk vissza az S négyzethez. Könnyen látszik, hogy S határa egyetlen egy $\mathcal{AB}$ típusú oldalt tartalmaz, illetve semelyik oldal sem tartalmaz egyszerre $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű csúcsot, mivel az egész síkon igaz, hogy egy egyenes legfeljebb két színt tartalmazhat. Tehát használhatjuk a 6.1. Lemmát, azaz létezik egy T_i háromszög, aminek $\mathcal{A}$, $\mathcal{B}$ és $\mathcal{C}$ színű csúcsai is vannak. Egyrészt az előző bekezdés szerint $|t(T_i)| > 1$, másrészt mivel minden háromszög egyenlő területű, ezért $t(T_i) = \frac{1}{m}$, azaz $|\frac{1}{m}| > 1$, vagyis m páros. □

6.3. Megjegyzés. Bármilyen páros $m \in \mathbb{N}$ számra felbontható egy négyzet m darab azonos területű háromszögre.

Bizonyítás. Elég a $[0,1] \times [0,1]$ négyzetet felbontani. Legyen $m = 2n$. Húzzuk be a $\frac{k}{n} \times [0,1]$ szakaszokat $k = 1, 2, \ldots, n-1$-re. A kialakuló n darab téglalapot bontsuk fel valamelyik átlója mentén 2 háromszögre. Ez megfelelő felbontás. □

6.1. Általánosítások

Kézenfekvő kérdés, hogy egy n-dimenziós kockát hány darab szimplexre lehet felbontani.

6.4. Tétel (Mead)**.** *Pontosan akkor lehet felbontani egy n-dimenziós kockát m darab azonos térfogatú szimplexre, ha $n! \mid m$.*

Bizonyítás. A bizonyítás nagyon hasonlít a Monsky tétel bizonyításához. Legyen R egy n-dimenziós politóp. Nevezzük *egyszerű* felbontásnak azt, ha az R politópot úgy bontjuk fel n-dimenziós szimplexekre, hogy ha a felbontásban szereplő S szimplex határára esik egy másik szimplex csúcsa, akkor az S-nek is csúcsa. Tehát nem eshet csúcs semelyik szimplex semelyik nem nulla dimenziós lapjának belsejébe, például a két dimenziós esetben a háromszögelés egy háromszögének az oldalára. Színezzük ki a felbontás szimplexeinek csúcsait $n+1$ színnel $p_0, p_1, \ldots, p_n$ színekkel. Egy k-dimenziós S szimplexet *teljes k-as*nak nevezzük, ha a csúcsait a $p_0, p_1, \ldots, p_k$ színekkel színeztük ki.

6.5. Lemma. *Legyen R n-dimenziós politóp, amit felbontottunk egyszerű felbontással szimplexekre. Tegyük fel, hogy a szimplexek csúcsait a $p_0, p_1, \ldots, p_n$ színekkel színeztük ki. Ekkor a teljes n-esek száma a felbontásban pontosan akkor páratlan, ha a teljes $(n-1)$-esek száma R határán páratlan.*

Bizonyítás. Egy teljes $(n-1)$-es az R határán egy n-dimenziós szimplexben van benne, míg minden más teljes $(n-1)$-es kettő n-dimenziós szimplexben van benne. Egy teljes n-es pontosan egy teljes $(n-1)$-est tartalmaz, egy n-dimenziós szimplex, ami viszont nem teljes, az nulla vagy kettő teljes $(n-1)$-est tartalmaz. (Ha tartalmaz egy teljes $(n-1)$-est, akkor a kimaradó csúcsot nem p_n-re kell színezni, de akkor kialakul még egy teljes $(n-1)$-es.) Ezekből következik a Lemma állítása. □

6.6. Lemma. *Legyen R n-dimenziós politóp, amit felbontottunk nem feltétlenül egyszerű felbontással. Tegyük fel, hogy a szimplex csúcsait úgy színeztük ki a $p_0, p_1, \ldots, p_n$ színekkel, hogy bármely k-dimenziós affin altér, ami tartalmaz p_i színű pontot minden $0 \leq i \leq k$-ra, az nem tartalmaz p_i színű pontot, ahol $i > k$. Ekkor a teljes n-esek száma a felbontásban pontosan akkor páratlan, ha a teljes $(n-1)$-esek száma R határán páratlan.*

Bizonyítás. Indukcióval bizonyítjuk n-re. Ha $n = 0, 1$, akkor a felbontás mindenképpen egyszerű és az előző Lemma miatt igaz ez is. Tegyük fel, hogy minden $k < n$-re igaz a Lemma k-dimenziós szimplexekre.

Legyen T egy $(n-1)$-dimenziós politóp, ami R belsejében van és aminek a csúcsai azok csúcsai felbontásban szereplő szimplexeknek T hipersíkjának mindkét oldalán. (Ha veszünk egy tetszőleges $(n-1)$-dimenziós szimplexet R belsejében a felbontásból, akkor az benne lesz egy ilyen $(n-1)$-dimenziós politópban, tehát található egy ilyen.) Tehát T-t kétféleképpen is felbontottuk $(n-1)$-dimenziós szimplexekre ezzel, ezért indukció miatt megegyezik a két felbontásban a teljes $(n-1)$-esek száma (hiszen mindkettő paritása megegyezik a T határán lévő teljes $(n-2)$-esek számával). Ebből az következik, hogy azon n-dimenziós szimplexek száma, amik tartalmaznak teljes $(n-1)$-est, mint lap és ez a lap az R belsejében van, az páros. Működik az előző Lemma bizonyítása, mert ezzel kiküszöböltük azt a lépést az előző bizonyításban, hogy az R belsejében lévő teljes $(n-1)$-esek kettő n-dimenziós szimplexben vannak benne. (Nem egyszerű felbontásra ez nem igaz, mert a másik oldalán nem feltétlenül kell legyen szimplex, de egy T politópban benne van.) □

Legyen $|\cdot|_p$ p-adikus abszolútérték $\mathbb{R}$-en. Színezzük ki az n-dimenziós tér $(x_1, \ldots, x_n)$ pontjait a $P_0, P_1, \ldots, P_n$ színekkel a következőképpen:

$$(x_1, \ldots, x_n) \in P_0, \text{ ha } |x_i|_p < 1 \ \forall\ 1 \leq i \leq n;$$

$$(x_1, \ldots, x_n) \in P_k, \text{ ha } |x_k|_p \geq 1,\ |x_k|_p > |x_i|_p \ \forall\ i < k \text{ és } |x_k|_p \geq |x_i|_p \forall\ i > k.$$

Ez partícionálja a teret. Tegyük fel, hogy $(x_1, \ldots, x_n) \notin P_0$, ekkor $(x_1, \ldots, x_n) \in P_k$, ha $|x_k|_p = \max |x_j|_p$ és k a legkisebb index, ahol felveszi a maximumot. P_0-beli ponttal való eltolás nem változtatja meg egy pont színét, úgy mint a Monsky tétel bizonyításában.

Tegyük fel, hogy egy k-dimenziós affin altér tartalmaz pontokat $P_0, P_1, \ldots, P_k$ és egy ezektől különböző P_l színnel is. Legyenek egy-egy pont koordinátái az adott színből $(x_{1j}, \ldots, x_{nj})$ (P_j színű pont). Ha eltoljuk a pontokat, akkor nem változik meg se a színük, se a kifeszített politóp térfogata, ami persze 0, mert egy affin altérben vannak. Tehát feltehetjük, hogy a P_0 színű pont az origó. A kifeszített politóp így már egy k-dimenziós lineáris altérben van, ennek a politópnak a merőleges vetülete egy $(k+1)$-dimenziós altérre továbbra is 0 térfogatú kell legyen ebben a $(k+1)$-dimenziós altérben is. Vegyük azt, hogy az első k és az l-dik koordináták által feszített altérre vetítjük a poltitópot. Ez könnyen számolható a következő mátrix determinánsával:

$$\begin{pmatrix} x_{11} & x_{21} & \ldots & x_{k1} & x_{l1} \\ x_{12} & x_{22} & \ldots & x_{k2} & x_{l2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{1k} & x_{2k} & \ldots & x_{kk} & x_{lk} \\ x_{1l} & x_{2l} & \ldots & x_{kl} & x_{ll} \end{pmatrix}.$$

Ha kifejtjük a determinánst, akkor a főátlóból kapott $x_{11}x_{22}\ldots x_{kk}x_{ll}$ tag abszolútértéke szigorúan nagyobb, mint bármely más tagé, mert a színezés miatt egy sorban a főátlóban

lévő szám abszolútértéke a legnagyobb és van legalább egy olyan sor, ahol egy szigorúan kisebb abszolútértékűt választunk ki. A 2.15. Állítás miatt tehát a determináns abszolútértéke $|x_{11}x_{22}\dots x_{kk}x_{ll}|_p$, ami nagyobb, mint 0, azaz a determináns nem lehet 0, tehát a vetített politóp térfogata sem lehet 0. Azaz a feltétel nem igaz. Ez éppen azt jelenti, hogy a definiált színezés teljesíti a 6.6. Lemma feltételeit.

Ha adott egy teljes n-es, akkor ugyanúgy felírva a pontok koordinátáit és a hasonló determinánst, azt kapjuk, hogy a teljes n-es $V\big(((x_{ij}))\big)$ térfogata megegyezik $\frac{1}{n!}\det((x_{ij}))$-vel és $|\det((x_{ij}))|_p = |x_{11}\dots x_{nn}|_p \geq 1$. (Most is feltehetjük, hogy a P_0 színű pont az origó, mert az eltolás nem változtatja meg a színezést és a térfogatokat.) Tehát $|V\big(((x_{ij}))\big)|_p \geq 1/|n!|_p = p^{v_p(n!)}$.

Természetesen elég a Tételt az egységkockára bizonyítani, aminek a határán pontosan egy teljes $(n-1)$-es van. Tehát a 6.6. Lemma miatt páratlan sok teljes n-es van van a felbontásban, azaz van legalább egy. Ennek a térfogata is $1/m$, ha az egységkockát fel tudtuk bontani m darab azonos térfogatú szimplexre. Az előző bekezdés miatt ekkor $|1/m| \geq p^{v_p(n!)}$, tehát $v_p(m) \geq v_p(n!)$. Mivel ezt minden p prímre el tudjuk mondani, ezért valóban következik, hogy $n! \mid m$.

Ha $n! \mid m$, akkor fel tudjuk bontani az egységkockát m egyforma térfogatú szimplexre: legyen $m = l \cdot n!$. Bontsuk fel a hiperkockát $n!$ egyenlő térfogatú részre. A felbontásban lévő szimplexeknek vegyük az egyik 1-dimenziós lapját, azaz élét és osszuk fel l egyenlő részre. Ezek a szimplexet l egyenlő térfogatú szimplexre bontják.

Hiperkocka felbontása $n!$ szimplexre: legyen π az $\{1,\dots,n\}$ halmaz permutációja. Definiáljuk az

$$S_\pi = \{x \in \mathbb{R}^n : 0 \leq x_{\pi(1)} \leq \dots \leq x_{\pi(n)} \leq 1\}$$

halmazt. Ez egy n dimenziós szimplex, mert $n+1$ lineárisan független egyenlőtlenség definiálja, azaz $n+1$ féltér metszete. Ezeknek az S_π szimplexnek a belsejük páronként diszjunkt, mert a belsejük azok azok a pontok, ahol minden egyenlőtlenség szigorú és két szigorú egyenlőtlenség nem teljesülhet két irányba egyszerre ($x > y$, $x < y$). Ha pedig van egy pont, aminek a koordinátái páronként különböznek, akkor azok valamilyen sorrendben vannak, így valamelyik S_π belsejébe esnek. Tehát S_π szimplexek, ahol π végigfut az $\{1,\dots,n\}$ halmaz összes permutációján egy felbontása az egységkockának $n!$ szimplexre. Jelölje $\pi : (x_1,\dots,x_n) \mapsto (x_{\pi(1)},\dots,x_{\pi(n)})$ az n-dimenziós tér egy egybevágóságát is. Ekkor π az S_{id} szimplexet az $S_{\pi^{-1}}$ szimplexbe viszi, tehát a két szimplex térfogata megegyezik. Minden π-re ezt el lehet mondani, ezért minden szimplex térfogata megegyezik. Tehát megadtuk az n-dimenziós kocka egy felbontását $n!$ azonos térfogatú szimplexre. □

Egy másik lehetőség az általánosításra, ha két dimenzióban más alakzatokat akarunk azonos területű háromszögekre bontani. Ha valamit fel lehet bontani páratlan sokra, akkor azt páros sokra is lehet, ha minden háromszöget elfelezünk. Az érdekes kérdés, hogy mik azok az alakzatok, amiket nem lehet páratlan sok háromszögre bontani. Monsky bebizonyította, hogy a négyzet ilyen. Könnyű észrevétel, hogy ha két alakzat affin transzformációval egymásba vihető, akkor ez a két alakzat ugyanakkor osztható fel páratlan sok háromszögre, hiszen egy felbontás képe affin transzformációnál szintén egy háromszögelés. Ebből látszik például a következő egyszerű állítás:

6.7. Állítás. *Egy paralelogramma pontosan akkor osztható fel m darab azonos területű háromszögre, ha m páros.*

Az affin transzformációk mellett az általános módszer a Monsky tételbeli színezés és a 6.1. Lemma használata. Ha meg tudjuk mutatni, hogy egy egységnyi területű alakzat határa páratlan sok $\mathcal{AB}$ típusú oldalt tartalmaz, akkor abból már következik, hogy nem lehet felbontani páratlan sok azonos területű háromszögre.

6.8. Tétel (Kasimatis, Stein)**.** *Legyen adott* $(0,0);(0,1);(1,0);(a,a)$ *csúcsokkal egy négyszög.*

- *Ha* $v_2(a) > 0$*, akkor nem lehet páratlan sok azonos területű háromszögre bontani.*
- *Ha* $-1 < v_2(a) \leq 0$*, akkor szintén nem lehet.*
- *Ha* $v_2(a) = -1$*, akkor van olyan* a*, amire lehet.*

Bizonyítás. Ha $v_2(a) > 0$, akkor az $(x,y) \mapsto (x/a, y)$ affin transzformáció után egy $\mathcal{AB}$ típusú oldal lesz. Ha $-1 < v_2(a) \leq 0$, akkor nem kell transzformálni, az eredeti négyszög határán egy $\mathcal{AB}$ típusú oldal van. Ha $a = 3/2$, akkor fel lehet osztani, vegyük a $(0,1)$ és $(1,0)$-t összekötő szakaszt, majd a kialakuló $(0,1);(1,0);(3/2,3/2)$ háromszög $(3/2,3/2)$-ből induló magasságát az $(1/2,1/2)$ pontig. Ezzel a két szakasszal 3 darab $1/2$ területű háromszögre bontottuk a négyszöget. □

A következő Tétel bizonyításában azt is használták, hogy a p-adikus abszolútérték kiterjeszthető a komplex számokra.

6.9. Tétel (Kasimatis)**.** *Ha egy szabályos* n*-szöget* m *egyenlő területű háromszögre bontottunk és* $n \geq 5$*, akkor* $n \mid m$*.*

6.10. Tétel (Monsky)**.** *Nem lehet páratlan sok azonos területű háromszögre bontani semmilyen középpontosan szimmetrikus sokszöget.*

Bármilyen a tengelyekkel párhuzamos egész koordinátájú egység oldalú négyzet pontosan egy $\mathcal{AB}$ típusú oldalt tartalmaz, hiszen egy olyan csúcsa van, aminek mindkét koordinátája páros és mellette az egyik csúcs $\mathcal{B}$ színű, a másik $\mathcal{C}$ színű.

6.11. Következmény (Stein)**.** *Ha egy alakzat páratlan sok egységnégyzet összeragasztásából áll, akkor nem lehet páratlan sok azonos területű háromszögre felbontani.*

Bizonyítás. Az $\mathcal{AB}$ típusú oldalakat jelöljük meg az egységnégyzetekben minden egységnégyzet belsejében. Ha az alakzat belsejében van valamelyik egységnégyzet jelölése, akkor a hozzáragasztott másik egységnégyzetnek is az alakzat belsejében van. Mivel összesen páratlan sok jelölés van, ezért az alakzat határán páratlan sok jelölés kell legyen. □

6.12. Tétel (Praton)**.** *Akkor se lehet felbontani páratlan sok azonos területű háromszögre, ha páros sok egységnégyzetet ragasztunk össze.*

6.13. Következmény. *Nem lehet páratlan sok azonos területű háromszögre felbontani egy olyan alakzatot, aminek minden éle a határán párhuzamos a megfelelő tengellyel és az éleinek a hossza racionális.*

Bizonyítás. Toljuk el, hogy az egyik csúcsa az origó legyen, majd nagyítsuk egy egész számmal való nyújtással, hogy minden éle egész hosszú legyen. Az így kapott alakzat már egységnégyzetek összeragasztása. □

Irányítsuk az alakzat határát valahogy és minden éléből a határnak csináljunk egy ennek megfelelő vektort. Nevezzük az alakzatot *speciális*nak, ha a párhuzamos élek vektorait összeadva minden párhuzamossági osztály szerint 0-t kapunk. Ilyenek például a négyzet, a paralelogramma a középpontosan szimmetrikus sokszögek és az egységnégyzetekből összeragasztott alakzatok.

6.14. Tétel (Stein)**.** *$A \leq 7$ oldalú speciális alakzatokat nem lehet páratlan sok azonos területű háromszögre bontani.*

6.15. Kérdés. Van-e olyan speciális alakzat, amit fel lehet bontani páratlan sok azonos területű háromszögre?

Hivatkozások

[1] F. Gouvea. *p-adic Numbers: An Introduction*. Universitext. Springer Berlin Heidelberg, 2003.

[2] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.

[3] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005.

[4] D. G. Mead. Dissection of the hypercube into simplexes. *Proceedings of the American Mathematical Society*, 76(2):302–304, 1979.

[5] Paul Monsky. On dividing a square into triangles. *The American Mathematical Monthly*, 77(2):161–164, 1970.

[6] Sherman Stein. Cutting a polygon into triangles of equal areas. *The Mathematical Intelligencer*, 26(1):17–21, 2004.