TARTALOMJEGYZÉK

1. Véges test feletti irreducibilis polinomok

Azok az összefüggések, amelyek általában egy test feletti irreducibilis polinomra vonatkoznak, természetesen most is érvényben vannak, így ebben a fejezetben főleg olyan tulajdonságokat vizsgálunk, amelyek specifikusak a véges test feletti felbonthatatlan polinomokra. A továbbiakban $\hat{f}$ az *f* polinomhoz tartozó polinomfüggvény.

1.1. Tétel

Ha K egy *q*-elemű véges test, akkor tetszőleges $\varphi: \mathsf{K} \to \mathsf{K}$ leképezéshez van olyan egyértelműen meghatározott, azonosan nulla, vagy legfeljebb $q-1$-edfokú K feletti *f* polinom, hogy a *K* minden *u* elemére $\varphi(u) = \hat{f}(u)$. Ez az *f* polinom megadható az $f = \sum_{u \in K} \varphi(u)\left(e - (x-u)^{q-1}\right)$ alakban, továbbá ha $g \in \mathsf{K}[x]$-re is igaz, hogy $\hat{g} = \varphi$, akkor $g = f + t \cdot \left(x^q - x\right)$ valamilyen $t \in \mathsf{K}[x]$ polinommal.

Δ

Bizonyítás:

Nézzük a felírt polinomot. Az összeg minden tagja – egymástól függetlenül – nulla, vagy pontosan $q-1$-edfokú, igy az összegük vagy a nullpolinom, vagy legfeljebb $q-1$-edfokú. Legyen *b* a *K* tetszőleges eleme. *x* helyére *b*-t írva, $u \neq b$ esetén $(b-u)^{q-1} = e$, és minden ilyen tag nulla lesz az összegben. Ha viszont $u = b$, akkor a megfelelő tag $\varphi(b)$, tehát $\hat{f}(b) = \varphi(b)$ a test minden elemére.

Ha *h* egy másik olyan K feletti polinom, amely vagy 0, vagy a foka legfeljebb $q-1$, és *K* minden *u* elemére $\hat{h}(u) = \varphi(u)$, akkor az $f - h$ polinomhoz tartozó $\hat{f} - \hat{h}$ leképezés *K* valamennyi elemét a 0-ba viszi, vagyis a különbségpolinomnak *K* minden eleme gyöke, ami azt jelenti, hogy van *q* különböző gyök. Viszont polinomok különbsége vagy a nullpolinom, vagy a fokszám nem nagyobb a fokszámmal rendelkező tagok fokainak maximumánál, így $f - h$ is vagy a nullpolinom, vagy legfeljebb $q-1$-edfokú. De test feletti nem nulla polinomnak még multiplicitással számolva sem lehet több gyöke, mint amekkora a fokszáma, így $f - h = 0$, $f = h$, ami azt jelenti, hogy *f* egyértelmű.

Most legyen *g* olyan K feletti polinom, hogy minden *K*-beli *u*-ra $\hat{g}(u) = \varphi(u)$. Mivel *g* egyértelműen írható $g = t \cdot \left(x^q - x\right) + r$ alakban, ahol $r = 0$, vagy *r* foka kisebb, mint *q*, ezért áttérve a megfelelő leképezésre, $\varphi(u) = \hat{g}(u) = \hat{t}(u)\left(u^q - u\right) + \hat{r}(u) = \hat{r}(u)$ (mert *q*-elemű test minden *u* elemére érvényes az $u^q = u$ egyenlőség), és ilyen *r* pontosan egy van, nevezetesen *f*, tehát $r = f$.

□

1.2. Kiegészítés

Legyen $\varphi: \mathbf{F}_q^n \to \mathbf{F}_q$, ahol $n \in \mathbf{N}$. Ekkor $f = \sum_{(u_1,\ldots,u_n) \in \mathbf{F}_q^n} \left(\varphi(u_1,\ldots,u_n) \prod_{i=1}^{n} \left(e - (x_i - u_i)^{q-1}\right)\right)$ egy minden határozatlanban legfeljebb $q-1$-edfokú *n*-határozatlanú polinom, amelyhez tartozó $\hat{f}$ polinomfüggvény megegyezik φ-vel, és nincs más ilyen polinom.

Δ

Bizonyítás:

f-ről az előbbiek alapján könnyű belátni, hogy minden határozatlanban legfeljebb $q-1$-edfokú, és a polinom bármely $(a_1,\ldots,a_n) \in \mathbf{F}_q^n$ helyen vett helyettesítési értéke $\varphi(a_1,\ldots,a_n)$.

Az egyértelműséget kissé általánosabb formában bizonyítjuk. Legyen $\mathbf{N}_r := \{k \in \mathbf{N}_0 \mid r > k\}$, és $\mathbf{N}_{r_1,\ldots,r_s} := \mathbf{N}_{r_1} \times \ldots \times \mathbf{N}_{r_s}$, ahol $r \in \mathbf{N}$, $s \in \mathbf{N}$, $s \geq i \in \mathbf{N}$-re $r_i \in \mathbf{N}$, és legyen $f^{(1)}$ és $f^{(2)}$ az R integritási tartomány feletti *m*-határozatlanú polinom. Ha $m \geq i \in \mathbf{N}$-re $n_i^{(j)}$ az $f^{(j)}$ fokszáma x_i-ben, $\max\{n_i^{(1)}, n_i^{(2)}\} < n_i \in \mathbf{N}$, és $T^{(m)} = \left\{\left(u_{k_1}^{(i)},\ldots,u_{k_m}^{(m)}\right) \in R^m \middle| (k_1,\ldots,k_m) \in \mathbf{N}_{n_1,\ldots,n_m}\right\}$ $n_1 \cdots n_m$ számú páronként különböző olyan pont, amelyekben a két függvény értéke azonos, akkor a két polinom is azonos. Ez ekvivalens azzal, hogy amennyiben az R fölötti *m*-határozatlanú polinom az *i*-edik határozatlanban legfeljebb $n_i - 1$-edfokú, és az előbb megadott pontok mindegyike gyöke a polinomnak, akkor *f* a nullpolinom. Ezt a határozatlanok száma szerinti indukcióval bizonyítjuk. Ez $m = 1$-re igaz. Tegyük fel, hogy $m \in \mathbf{N}$-re is igaz az állítás, és legyen $f = \sum_{(i_1,\ldots,i_m,i_{m+1}) \in \mathbf{N}_{n_1,\ldots,n_m,n_{m+1}}} c_{i_1,\ldots,i_m,i_{m+1}} \prod_{j=1}^{m+1} x_j^{i_j}$, továbbá $T^{(m+1)} = T^{(m)} \times T^{(1)} = \left\{\left(u_{k_1}^{(i)},\ldots,u_{k_m}^{(m)},u_{k_{m+1}}^{(m+1)}\right) \in R^{m+1} \middle| (k_1,\ldots,k_m,k_{m+1}) \in \mathbf{N}_{n_1,\ldots,n_m,n_{m+1}}\right\}$ a polinom $n_1 \cdots n_m n_{m+1}$ különböző gyökének halmaza. *f* minden $m+1 \geq i \in \mathbf{N}$ indexre legfeljebb $n_i - 1$-edfokú x_i-ben, és $f = \sum_{i=0}^{n_{m+1}-1} f_i x_{m+1}^i$, ahol $f_i = \sum_{(i_1,\ldots,i_m) \in \mathbf{N}_{n_1,\ldots,n_m}} c_{i_1,\ldots,i_m,i} \prod_{j=1}^{m} x_j^{i_j}$. Bármely $\left(u_{k_1}^{(1)},\ldots,u_{k_m}^{(m)}\right) \in T^{(m)}$ pontban $f^{\left(u_{k_1}^{(i)},\ldots,u_{k_m}^{(m)}\right)} = \sum_{i=0}^{n_{m+1}-1} \hat{f}_i\left(u_{k_1}^{(1)},\ldots,u_{k_m}^{(m)}\right) x_{m+1}^i$ egyhatározatlanú polinom, amelynek $T^{(1)}$ valamennyi eleme gyöke. Ez a polinom pontosan akkor lesz valamennyi megadott $u_i^{(m+1)} \in T^{(1)}$ helyen 0, ha minden együtthatója 0, azaz ha minden $i \in \mathbf{N}_{m+1}$-re $\hat{f}_i\left(u_{k_1}^{(1)},\ldots,u_{k_m}^{(m)}\right) = 0$. Ez azt jelenti, hogy minden rögzített *i*-re az f_i polinom a $T^{(m)}$ minden pontjában, azaz $n_1 \cdots n_m$ pontban 0. Ez viszont az indukciós feltevés alapján pontosan akkor igaz, ha f_i a nullpolinom, azaz valamennyi együtthatója, tehát minden $c_{i_1,\ldots,i_m,i_1}$ értéke 0, és ezt akartuk bizonyítani.

Az egyértelműségre adunk egy másik, kombinatorikus bizonyítást is. A *q*-elemű testet önmagába képező *m*-változós függvények száma q^{q^m}, és ugyanennyi a *q*-elemű test fölötti, minden határozatlanjában legfeljebb $q-1$-edfokú *m*-határozatlanú polinomok száma. Egy ilyen polinomhoz pontosan egy előbb említett leképezés tartozik, és minden érintett leképezéshez találtunk olyan, minden határozatlanjában legfeljebb $q-1$-edfokú *m*-határozatlanú polinomot, amelyhez tartozó polinomfüggvény megegyezik az adott leképezéssel, vagyis az a megfeleltetés, amely a polinomhoz hozzárendeli a leképezést, szürjektív a leképezések halmazára. Mivel a leképezések halmazában és a *q*-elemű test fölötti, minden határozatlanjában legfeljebb $q-1$-edfokú *m*-határozatlanú polinomok halmazában ugyanannyi elem van, ezért a szürjektivitásból következik az injektivitás is, ami éppen az egyértelműséget jelenti.

□

1.3. Megjegyzés

A tétel szerint véges test feletti tetszőleges függvény lényegében véve polinomfüggvény.

Ha R gyűrű, és φ illetve ψ egyaránt *R*-et *R*-be képező függvény, vagyis *R* transzformációja, akkor az $u \mapsto \varphi(u) + \psi(u)$ és $u \mapsto \varphi(u)\psi(u)$, ahol $u \in R$, szintén *R* feletti transzformáció, amelyeket $\varphi + \psi$ és $\varphi\psi$, továbbá könnyen lehet ellenőrizni, hogy ezzel gyűrűt kapunk, ahol a nullelem az a transzformáció, amely minden elemhez a 0-t rendeli, a φ ellentettje pedig az, amely *u*-t $-\varphi(u)$-ra képezi. Jelöljük ezt a gyűrűt T_R-el. Ennek P_R részhalmazát képezik az $u \mapsto \sum_{i=0}^{n} a_i u^i$ alakú leképezések, ahol $n \in \mathbf{N}_0$, és valamennyi *i*-re a_i az R gyűrű eleme, vagyis a polinomfüggvények. Látható, hogy $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} a_i u^i$ szürjekció $R[x]$-ről P_R-be, és összegtartó, továbbá ha R kommutatív, akkor teljesül a szorzattartás is, így kommutatív gyűrűben az előbbi megfeleltetés egyben homomorf-

izmus is (amiből a szürjektivitással együtt az is következik, hogy a polinomfüggvények P_R halmaza részgyűrűt alkot T_R-ben). Mármost az előbbi tétel azt jelenti, hogy véges test esetén T_R azonos P_R-el, így az előbbi szabály $\mathsf{R}[x]$ szürjektív homomorfizmusa T_R-re. Ez a leképezés viszont biztosan nem injektív. *q*-elemű test esetén a test bármely *u* elemére $u^q - u = 0$, ezért tetszőleges $f \in R[x],\ g \in R[x]$ esetén *f* és $f + g \cdot (x^q - x)$ képe azonos polinomfüggvény. Ugyanakkor végtelen elemű *R* esetén a szürjektivitás biztosan nem igaz. Ezt két módon is bizonyítjuk.

Tekintsük azt a $\sigma : R \to R$ leképezést, amely a 0 kivételével *R* minden eleméhez a 0-t rendeli, míg a 0-ban az értéke az *R* egy nem nulla *u* eleme. Ha lenne egy R feletti *f* polinom, amelyre $\hat{f} = \sigma$, akkor ennek a polinomnak a 0 kivételével valamennyi *R*-beli elem gyöke lenne, vagyis *f*-nek végtelen sok gyöke lenne. Ilyen polinom csak egy van, a nullpolinom. Viszont a nullpolinomhoz tartozó polinomfüggvény értéke mindenütt 0, tehát a 0-ban is. Ugyanakkor $\sigma(0) = u \neq 0$, a nullpolinomhoz tartozó polinomfüggvény sem lehet σ-val egyenlő, így nincs olyan polinom, amelyhez tartozó polinomfüggvény megegyezik σ-val, ami azt jelenti, hogy az $f \mapsto \hat{f}$ leképezés végtelen gyűrű esetén nem szürjektív.

Az előző bizonyításban csak annyit mutattunk meg, hogy az a $\varphi : R[x] \to T_R$ leképezés, ahol *f* képe $\hat{f}$, nem szürjektív. Ez még nem zárná ki, hogy valamilyen más hozzárendeléssel szürjektíven képezzük le a polinomgyűrűt a gyűrűt önmagába képező leképezések halmazába. A második bizonyítással azonban kimutatjuk, hogy T_R számossága nagyobb, mint a polinomgyűrű számossága, ami kizárja, hogy létezzen a polinomgyűrűnek T_R-re való bármilyen szürjektív leképezése.

Az R feletti polinomok lényegében véve *R* feletti véges hosszúságú sorozatok. Egy halmaz fölötti *n* hosszúságú sorozatok halmaza R^n, ahol a szorzás a Descartes-szorzat, és ha *R* végtelen, akkor $|R^n| = |R|$. A polinomgyűrű az összes véges sorozat halmaza, vagyis ekvivalens az $\bigcup_{n=1}^{\infty} R^n$ halmazzal. Viszont megszámlálható sok azonos számosságú végtelen halmaz uniója megegyezik az unióban szereplő tagok számosságával, így $|R[x]| = \left|\bigcup_{n=1}^{\infty} R^n\right| = |R|$. Ezzel szemben viszont legalább kételemű halmaz esetén $|T_R| = |R^R| > |R|$, így ezt az eredményt egybevetve az előzővel kapjuk, hogy $|R[x]| < |T_R|$.

Végtelen gyűrű esetén tehát az $f \mapsto \hat{f}$ leképzés nem szürjekció $R[x]$-ről T_R-be. Ha viszont R végtelen elemszámú integritási tartomány, akkor az előbbi megfeleltetés injektív homomorfizmus. Egyrészt a kommutativitás következtében a leképezés művelettartó. Másrészt integritási tartomány feletti nem nulla polinom gyökeinek száma nem haladhatja meg a polinom fokát, ezért két polinomfüggvény csak úgy lehet egyenlő, ha maga a két polinom is azonos (polinomok egyenlősége ekvivalens azzal, hogy minden együtthatójuk azonos, míg két polinomfüggvény, mint tetszőleges két leképezés is, pontosan akkor egyenlő, ha az értelmezési tartomány minden eleméhez azonos elemet rendel).

Δ

A továbbiakban sokszor felhasználjuk az $x^q - x = \prod_{u \in \mathbf{F}_q} (x - u)$ egyenlőséget, valamint az ehhez hasonló $x^{q-1} - e = \prod_{u \in \mathbf{F}_q^*} (x - u)$ összefüggést. Lényeges lesz a továbbiakban az is, hogy ha R kommutatív gyűrű, amelyben minden *u* elemre $pu = 0$, ahol *p* egy rögzített prímszám, akkor a $\varphi_n : u \mapsto u^{p^n}$ leképezés minden nem negatív egész *n*-re az R endomorfizmusa, vagyis összeg- és szorzattartó, továbbá ha a gyűrű nullosztómentes, akkor ez a leképezés injektív is, és így véges testen automorfizmus. Ebből következik, hogy q^m-elemű testen az $u \mapsto u^{q^n}$ leképezés automorfizmus, hiszen *q* a test karakterisztikájának, azaz egy prímnek a pozitív egész kitevős hatványa.

Az $x^q - x = \prod_{u \in \mathbf{F}_q} (x - u)$ egyenlőségnél valamivel általánosabb az alábbi állítás:

1.4. Tétel

Ha $f \in \mathbf{F}_q[x]$, akkor $f^q - f = \prod_{u \in \mathbf{F}_q} (f - u)$.

Δ

Bizonyítás:
$(fg) \circ h = (f \circ h)(g \circ h)$, és ha $f = g$, akkor $f \circ h = g \circ h$ tetszőleges *h* polinommal, így

$$f^q - f = (x^q - x) \circ f = \left(\prod_{u \in \mathbf{F}_q} (x - u) \right) \circ f = \prod_{u \in \mathbf{F}_q} ((x - u) \circ f) = \prod_{u \in \mathbf{F}_q} (f - u)$$

□

A fenti bizonyításban – és a későbbiekben is – $f \circ g := \sum_{i=0}^{n} f_i g^i$, ahol $f = \sum_{i=0}^{n} f_i x^i$.

Egy későbbi bizonyításban felhasználjuk az alábbi tétel eredményét:

1.5. Tétel

$t \in \mathbf{N}$-re $f \in \mathbf{F}_{q^t}[x]$ akkor és csak akkor eleme $\mathbf{F}_q[x]$-nek, ha $f^q = f \circ x^q$.

Δ

Bizonyítás:

Legyen $f = \sum_{i=0}^{n} a_i x^i \in \mathbf{F}_q{}^t[x]$. a_i eleme $\mathbf{F}_{q^t}$-nak, így $f^q = \left(\sum_{i=0}^{n} a_i x^i \right)^q = \sum_{i=0}^{n} a_i^q \left(x^q \right)^i$, míg $f \circ x^q = \sum_{i=0}^{n} a_i \left(x^q \right)^i$. De két polinom pontosan akkor egyenlő, ha minden indexre az együtthatójuk azonos, azaz ha $0 \le i \le n$-re $a_i = a_i^q$, és ez $\mathbf{F}_{q^t}$ elemei közül pontosan $\mathbf{F}_q$ elemeire igaz.

□

1.6. Tétel

Ha $\mathsf{L} \supseteq \mathbf{F}_q$, $f \in \mathbf{F}_q[x]$, és $\alpha \in L$ gyöke *f*-nek, akkor α^q is gyöke *f*-nek.

Δ

Bizonyítás:

Legyen $n \in \mathbf{N}_0$, $f = \sum_{i=0}^{n} a_i x^i \in \mathbf{F}_q[x]$. Ekkor minden $n \ge i \in \mathbf{N}_0$-ra $a_i \in \mathbf{F}_q$, és így $a_i^q = a_i$, továbbá $\mathbf{F}_q$-ban és annak bármely L bővítésében $(a+b)^q = a^q + b^q$, $(ab)^q = a^q b^q$ *L*-beli *a* és *b* elemekkel. A feltétel szerint $\hat{f}(\alpha) = 0$, és így $0 = 0^q = \left(\hat{f}(\alpha) \right)^q = \left(\sum_{i=0}^{n} a_i \alpha^i \right)^q = \sum_{i=0}^{n} a_i \left(\alpha^q \right)^i = \hat{f}\left(\alpha^q \right)$, ami igazolja a tételben megfogalmazott állításunkat.

□

1.7. Következmény

Ha az $f \in \mathbf{F}_q[x]$ polinomnak van gyöke az $\mathbf{F}_q$ egy L bővítésében, és α egy ilyen gyök, akkor α^{q^n} tetszőleges $n \in \mathbf{N}_0$-ra is gyöke ugyanezen polinomnak.

Δ

Bizonyítás:

$n=0$-ra $\alpha^{q^n}=\alpha$, és erre a feltétel szerint igaz a dolog, és ha egy $n\in\mathbf{N}_0$-ra $\hat{f}\left(\alpha^{q^n}\right)=0$, akkor az előző tétel szerint $\left(\alpha^{q^n}\right)^q=\alpha^{q^{n+1}}$ is gyöke *f*-nek.

□

Látható, hogy *q*-elemű test bővítésében nem nulla α elem q^i kitevős hatványai fontos szerepet játszanak, ezért röviden foglalkozunk az ilyen hatványokkal, ám előtte összefoglalunk a kongruenciával kapcsolatos néhány ismertnek feltételezett tényt, amelyeket a későbbiekben felhasználunk.

1.8. Definíció

Legyen $m\in\mathbf{N}$, és $i\in\mathbf{Z}$. $\min\left\{k\in\mathbf{N}\middle|ki\equiv 0\ (m)\right\}$ az *i* **additív rendje** modulo *m*, feltéve, hogy létezik minimum; ekkor ezt a rendet $o_m^+(i)$ jelöli.

Δ

1.9. Tétel

Minden $m\in\mathbf{N}$ és $i\in\mathbf{Z}$ esetén létezik és egyértelmű $o_m^+(i)$, továbbá $o_m^+(i)=\frac{m}{(i,m)}$.

Δ

Bizonyítás:

$mi\equiv 0\ (m)$, ezért $\varnothing\neq K=\left\{k\in\mathbf{N}\middle|ki\equiv 0\ (m)\right\}\subseteq\mathbf{N}$. **N** jólrendezett, így *K*-ban van legkisebb elem, a rend létezik és egyértelmű. Ha $t=o_m^+(i)$, és $d=\frac{m}{(i,m)}$, akkor $di=\frac{m}{(i,m)}i=m\frac{i}{(i,m)}\equiv 0\ (m)$, és $m\neq 0$, tehát $d>0$, így $t\le d$. Fordítva: $ti\equiv 0\ (m)$, ebből $t\equiv 0\ (d)$, vagyis $d\middle|t$, és mivel *d* és *t* pozitív egész, ezért az előbbi oszthatóságból $d\le t$, vagyis a rendezés antiszimmetriája következtében $d=t$.

□

1.10. Következmény

Legyen *m* természetes szám, *i*, *j* és *k* egész számok. Ekkor

1. $ji\equiv ki\ \left(m\Leftrightarrow j\equiv k\ \left(o_m^+(i)\right)\right)$
2. $ji\equiv 0\ (m)\Leftrightarrow o_m^+(i)\middle|j$
3. $o_m^+(i)\middle|m$, és $o_m^+(i)=m$ akkor és csak akkor, ha $(i,m)=1$
4. $o_m^+(ki)\middle|\left(o_m^+(k),o_m^+(i)\right)$
5. pontosan akkor lesz minden $u\in\mathbf{Z}$-vel $o_m^+(ku)=o_m^+(u)$, ha $(k,m)=1$.

Δ

Bizonyítás:

1. $ki\equiv ji\ (m)\Leftrightarrow k\equiv j\ \left(\frac{m}{(i,m)}\right)$ a kongruencia osztási szabálya szerint
2. az előző pont alapján $0\cdot i=0\equiv ji\ (m)\Leftrightarrow 0\equiv j\ \left(o_m^+(i)\right)\Leftrightarrow o_m^+(i)\middle|j$

3. $\frac{m}{(i,m)}\Big|m$, és $\frac{m}{(i,m)}=m \Leftrightarrow (i,m)=1$

4. ha $o_m^+(k)=s$, $o_m^+(i)=t$ és $o_m^+(ki)=r$, akkor $0=0\cdot i\equiv(sk)i=s(ki)\ (m)$, vagyis $r|s$, és teljesen hasonlóan kapjuk, hogy $r|t$, ami együtt azt jelenti, hogy $r|(s,t)$

5. ha $(k,m)=1$, akkor $(u,m)=(uk,m)$, így $\frac{m}{(u,m)}=\frac{m}{(uk,m)}$, míg ha ez az egyenlőség minden u-ra igaz, akkor $u=1$ mellett $1=(1,m)=(1\cdot k,m)=(k,m)$

□

1.11. Definíció

$n\in\mathbf{Z}$ modulo m (**multiplikatív**) **rendje**, ha létezik, $o_m(n):=\min\{k\in\mathbf{N}|n^k\equiv 1\ (m)\}$.

Δ

1.12. Tétel

Tetszőleges $m\in\mathbf{N}$ és $n\in\mathbf{Z}$ esetén akkor és csak akkor létezik n modulo m rendje, ha $(m,n)=1$. Ekkor a j és k nem negatív egészre $n^j\equiv n^k\ (m)$ pontosan akkor igaz, ha $j\equiv k\ (o_m(n))$ (speciálisan $n^i\equiv 1\ (m)$ pontosan akkor teljesül, ha $o_m(n)$ osztója i-nek), végül $o_m(n)|\varphi(m)$.

Δ

Bizonyítás:

Ha $a\equiv b\ (c)$, akkor $(a,c)=(b,c)$, és mivel minden pozitív egész k-ra $d=(m,n)|(m,n^k)$, ezért $n^k\equiv 1\ (m)$ esetén d osztója $(m,1)=1$-nek, vagyis $d>1$ esetén nem létezik n-nek olyan pozitív egész kitevős hatványa, amely 1-gyel kongruens modulo m, ebben az esetben nincs n-nek modulo m rendje.

Legyen most n relatív prím m-hez, akkor $n^{\varphi(m)}\equiv 1\ (m)$, tehát $\{k\in\mathbf{N}|n^k\equiv 1\ (m)\}$ az $\mathbf{N}$ nem üres részhalmaza, így $\mathbf{N}$ jólrendezettsége következtében létezik $o_m(n)$. Legyen $t\in\mathbf{N}$ olyan, hogy $n^t\equiv 1\ (m)$, és jelöljük a rövidség kedvéért $o_m(n)$-t r-rel. $r>0$, így alkalmas $q\geq 0$ és $r>s\in\mathbf{N}_0$ egészekkel $t=qr+s$. Ezzel $1\equiv n^t=n^{qr+s}=(n^r)^q n^s\equiv n^s\ (m)$, és mivel r a legkisebb pozitív egész, amellyel ez a kongruencia teljesül, ezért $s=0$, tehát $r|t$. De akkor ez igaz $\varphi(m)$-re is, $r|\varphi(m)$. Végül ha $k\in\mathbf{N}_0$, $k\geq j\in\mathbf{N}_0$, és $n^j\equiv n^k\ (m)$, akkor $(m,n)=1$ következtében $n^{k-j}\equiv 1\ (m)$, tehát az előzőek szerint $r|k-j$, azaz $j\equiv k\ (r)$. Visszafelé tegyük fel, hogy $k\in\mathbf{N}_0$, $k\geq j\in\mathbf{N}_0$ és $j\equiv k\ (r)$, akkor $k=j+qr$ alkalmas q nem negatív egésszel, ahonnan kapjuk, hogy $n^k=n^{j+qr}=n^j(n^r)^q\equiv n^j\ (m)$.

□

Most visszatérünk az α^{q^i} hatványokra.

1.13. Tétel

Legyen $\alpha\in\mathbf{F}_{q^t}$, továbbá $s=1$, ha $\alpha=0$, egyébként $s=o_n(q)$, ahol n az α rendje. Ekkor $\alpha^{q^0},\alpha^{q^1},\ldots,\alpha^{q^{s-1}}$ páronként különböző, bármely $j\in\mathbf{N}_0$-ra α^{q^j} az előbbi hatványok valamelyikével azonos, és a $j\in\mathbf{N}_0$, $j\geq i\in\mathbf{N}_0$ egészekre $\alpha^{q^i}=\alpha^{q^j}$ pontosan akkor igaz, ha $i\equiv j\ (s)$.

Δ

Bizonyítás:

$\alpha = 0$-ra az állítás nyilvánvaló, ezért áttérünk a többi esetre. Legyen $j \in \mathbf{N}_0$, és $j \geq i \in \mathbf{N}_0$. Ekkor $\alpha^{q^i} = \alpha^{q^j}$ akkor és csak akkor igaz, ha $q^i \equiv q^j \ (n)$. Mivel *n* osztója az L multiplikatív csopotja rendjének, azaz $q^t - 1$-nek, így relatív prím *q*-hoz, ezért az előbbi kongruencia ekvivalens a $q^{j-i} \equiv 1 \ (n)$ kongruenciával, ez utóbbi viszont az $i \equiv j \ (s)$ kongruenciával, ahol $s = o_n(q)$. Innen viszont az is látszik, hogy $s > i \in \mathbf{N}_0$ kitevőkkel az α^{q^i} hatványok páronként különbözőek, és bármely α^{q^j} egy *s*-nél kisebb nemnegatív egész *i* kitevős α^{q^i}-vel azonos.

□

1.14. Definíció

$\alpha \in \mathbf{F}_{q^t}$ (**$\mathbf{F}_q$-ra vonatkozó**) **ciklikus rendje** $s_\alpha^{(q)} = \min\left\{k \in \mathbf{N} \middle| \alpha^{q^k} = \alpha\right\}$, ahol $t \in \mathbf{N}$.

Δ

Az előző tételben azt láttuk be, hogy véges test minden elemének létezik és egyértelmű a test bármely K résztestére vonatkozó ciklikus rendje. Az is látszik, hogy ez a rend – eltekintve a prímtest elemeitől – attól is függ, hogy L mely résztestére vonatkoztatjuk. Erről is szól az alábbi tétel.

1.15. Tétel

1. Ha L a K véges test *t*-edfokú bővítése, és $\alpha \in L$, úgy α K feletti ciklikus rendje osztója *t*-nek, és a ciklikus rend akkor és csak akkor 1, ha $\alpha \in K$.

2. Ha *f* a *q*-elemű K test feletti *n*-edfokú polinom, α az *f* egy gyöke a K valamely bővítésében, és α K-ra vonatkozó ciklikus rendje *s*, akkor $s \leq n$.

3. Ha az M véges test az L test m_2-edfokú bővítése, és L a *q*-elemű K test m_1-edfokú bővítése, továbbá az *M* valamely $u \neq 0$ elemének K feletti ciklikus rendje $s_u^{(q)} = s$, akkor *u* L feletti ciklikus rendje $s_1 = s_u^{\left(q^{m_1}\right)} = \dfrac{s}{(s, m_1)} = o_s^+(m_1)$.

Δ

Bizonyítás:

1. Legyen *K* elemeinek száma *q*. L a K *t*-edfokú bővítése, ezért *L* elemeinek száma q^t, és $\alpha^{q^t} = \alpha$. Ez az előző tétel értelmében azt jelenti, hogy $t \equiv 0 \ (s)$, azaz $s \mid t$, ahol $s = s_\alpha^{(q)}$. Az *L*-beli α akkor és csak akkor eleme *K*-nak, ha az előbbi oszthatóság $t = 1$ esetén is teljesül, és ez ekvivalens azzal a feltétellel, hogy *s* maga is 1.

2. Mivel $0 \leq i < s$-re az α^{q^j}-k páronként különböző gyökei *f*-nek, és test fölötti polinomnak nem lehet a fokszámát meghaladó számú gyöke, ezért *s* valóban legfeljebb *n* lehet.

3. *s* a *q* modulo *n* rendje, így $q^r \equiv 1 \ (n)$ akkor és csak akkor igaz egy pozitív egész *r*-rel, ha *r* osztható *s*-sel. Ha s_1 az *u* ciklikus rendje a q^{m_1}-elemű test fölött, akkor s_1 a legkisebb pozitív egész, amellyel $\left(q^{m_1}\right)^k \equiv 1 \ (n)$, vagyis s_1 a legkisebb *k* pozitív egész, amelyre km_1 osztható *s*-sel. Ha $s \mid km_1$, akkor $\dfrac{s}{(s, m_1)} \middle| k$, és a kegkisebb ilyen *k* pozitív egész szám maga az osztó, azaz $\dfrac{s}{(s, m_1)}$.

□

Most rátérünk az irreducibilis polinomok vizsgálatára.

1.16. Tétel

Legyen $f \in \mathbf{F}_q[x]$ *m*-edfokú polinom. *f* akkor és csak akkor irreducibilis $\mathbf{F}_q$ fölött, ha van $\mathbf{F}_q$-nak olyan L bővítése, és *L*-ben olyan α, hogy $\hat{f}(\alpha)=0$, és $s = s_\alpha^{(q)} \geq m$.

Δ

Bizonyítás:

Mivel *f*-nek van foka, ezért *f* nem a nullpolinom.

1. Tegyük fel, hogy *f*-nek $\mathbf{F}_q$ valamely bővítésében van gyöke. Mivel *f* nem a nullpolinom, ezért a gyök létezése azt jelenti, hogy a polinom legalább elsőfokú, így nem egység. Legyen a gyök α, és $s \geq m$, továbbá $f = uv$ $\mathbf{F}_q$ fölötti *u* és *v* polinomokkal. Mivel $f \neq 0$, ezért $u \neq 0 \neq v$. A feltétel szerint $\hat{u}(\alpha)\hat{v}(\alpha) = \hat{f}(\alpha) = 0$, és test nullosztómentes, ezért $\hat{u}(\alpha)$ és $\hat{v}(\alpha)$ közül legalább az egyik 0. Az általánosság csorbítása nélkül feltehető, hogy például $\hat{u}(\alpha)$=0. Ekkor α-val együtt $m > i \in \mathbf{N}_0$-re α^{q^i} is gyöke *u*-nak, és $s \geq m$ következtében ezek a gyökök páronként különbözőek, így *u* legalább *m*-edfokú, ennél magasabb fokú viszont nem lehet, hiszen osztója a nem nulla *f*-nek. Test fölötti nem nulla polinomok szorzatának foka a tényezőpolinomok fokának összege, így *v* foka 0, vagyis *v* konstans, és nem nulla, ezért egység $\mathbf{F}_q$ fölött. Ez $m \geq 1$ következtében azt jelenti, hogy *f* felbonthatatlan.

2. Most legyen *f* felbonthatatlan $\mathbf{F}_q[x]$-ben. Ekkor $\deg(f) = m \geq 1$, és van $\mathbf{F}_q$-nak olyan L bővítése, amelyben van *f*-nek gyöke, mondjuk α. Ha α $\mathbf{F}_q$ fölötti ciklikus rendje *s*, akkor $\hat{f}(\alpha)=0$-ból az $s > i \in \mathbf{N}_0$ egészekkel α^{q^i} páronként különböző gyöke *f*-nek. Legyen $g = \prod_{i=0}^{s-1}\left(x - \alpha^{q^i}\right)$. Ez a *g* L feletti polinom, és mivel *s* gyöke van, ezért a foka *s*, tehát $g = \sum_{i=0}^{s} a_i x^i$ egy L feletti polinom az a_i együtthatókkal. Írjuk fel *g* *q*-adik hatványát (nem feledve, hogy *L* elemeinek száma *q* egy pozitív egész kitevős hatványa, és hogy α q^s-edik hatványa azonos a q^0-adik hatvánnyal):

$$g^q = \left(\prod_{i=0}^{s-1}\left(x - \alpha^{q^i}\right)\right)^q = \prod_{i=0}^{s-1}\left(x^q - \alpha^{q^{i+1}}\right) = \prod_{i=0}^{s-1}\left(x^q - \alpha^{q^i}\right) = g \circ x^q.$$

Korábban láttuk, hogy ebből $g \in \mathbf{F}_q[x]$ következik. Mivel α gyöke *f*-nek, és *f* felbonthatatlan, ezért egy esetleges nem nulla konstans szorzótól eltekintve *f* az α $\mathbf{F}_q$ fölötti minimálpolinomja. Egy $\mathbf{F}_q$ fölötti *h* polinomnak α akkor és csak akkor gyöke, ha α $\mathbf{F}_q$ fölötti minimálpolinomja osztója *h*-nak, így *f* osztója *g*-nek. Ebből viszont következik, hogy $m = \deg(f) \leq \deg(g) = s$.

□

1.17. Következmény

1. $\mathbf{F}_q$ fölött ireducibilis *m*-edfokú polinom gyökének $\mathbf{F}_q$ fölötti ciklikus rendje *m*, így egy elemnek az őt tartalmazó test valamely résztestére vonatkozó ciklikus rendje megegyezik ugyanezen résztest fölötti minimálpolinomjának fokával
2. $\mathbf{F}_q$ valamely bővítésében egy primitív elem ciklikus rendje azonos a bővítés fokával
3. Véges test feletti irreducibilis polinom gyökei egyszeresek.

Δ

Bizonyítás:

1. Korábban láttuk, hogy *m*-edfokú polinom gyökének ciklikus rendje nem nagyobb a polinom fokánál, az előző tételben pedig kiderült, hogy irreducibilis polinom gyökének ciklikus rendje

legalább akkora, mint a polinom foka. A kettő együtt azt jelenti, hogy adott test felett irreucibilis polinom foka megegyezik egy gyökének ugyanezen testre vonatkozó ciklikus rendjével.

2. Primitív elem minimálpolinomjának foka azonos a bővítés fokával, így ez 1. alapján igaz.
3. A tétel szerint ha *f* az $\mathbf{F}_q$ test fölött *m*-edfokú ireducibilis polinom, és $\mathbf{F}_q$ egy alkalmas bővítésében α a polinom gyöke, akkor az α^{q^i} elemek $m > i \in \mathbf{N}_0$ esetén páronként különböző gyökök, a polinomnak van *m* különböző gyöke. De test fölötti nem nulla polinom gyökeinek száma multiplicitásukkal számolva megegyezik a polinom fokszámával, így ha valamelyik gyök többszörös lenne, akkor a gyököket multiplicitásukkal számolva *f*-nek több gyöke lenne *m*-nél, ami lehetetlen.

□

Az előbbi tételnek egy további igen fontos következménye az alábbi

1.18. Tétel

Véges test egyszerű algebrai bővítése a bővítő elem minimálpolinomjának felbontási teste.

Δ

A tétel azt állítja, hogy véges testet irreducibilis polinom egyetlen gyökével bővítve, a bővített test tartalmazza a polinom valamennyi gyökét. Ez például a racionális számok teste esetén korántsem igaz: az $x^3 - 2$ polinomnak három gyöke, egy valós és két komplex gyöke van, ám a valós gyökkel bővítve biztosan olyan testet kapunk, amely nem tartalmazza a másik két gyököt.

Δ

Bizonyítás:

Ha α az f $\mathbf{F}_q$ fölött felbonthatatlan *m*-edfokú polinom gyöke, akkor $\mathbf{F}_q(\alpha)$ tartalmazza α minden nemnegatív egész kitevős hatványát, tehát $m > i \in \mathbf{N}_0$-re valamennyi α^{q^i}-t is. De éppen a felsorolt elemek az *f* gyökei, így *f* felbontási teste része $\mathbf{F}_q(\alpha)$-nak. Ugyanakkor szűkebb nem lehet a felbontási test, hiszen tartalmaznia kell mind $\mathbf{F}_q$-t, mind *f* gyökeit, de akkor legalábbis α-t és innen $\mathbf{F}_q(\alpha)$-t, ezért a felbontási test megegyezik $\mathbf{F}_q(\alpha)$-val.

□

1.19. Definíció

Ha $\alpha \in \mathrm{F}_{q^t}$, akkor α, α^q, α^{q^2},…, $\alpha^{q^{t-1}}$ az α $\mathbf{F}_q$**-ra vonatkozó konjugáltjai**.

Δ

1.20. Tétel

A konjugáltság ekvivalenciareláció F_{q^t}-en, és a konjugáltjak $\mathrm{F}_{q^t}^*$-beli rendje azonos. α egymással azonos konjugáltjainak száma $\frac{t}{s}$, ahol *s* az α $\mathbf{F}_q$ fölötti ciklikus rendje.

Δ

Bizonyítás:

Legyen α ciklikus rendje *s*, ekkor $s \le t$, hiszen *s* osztója *t*-nek.

1. Jelölje az F_{q^t}-beli α-ra és β-ra $\alpha \sim \beta$, hogy β az α konjugáltja. Ez bármely F_{q^t}-beli rendezett párra vagy igaz, vagy nem, így ~ binér reláció F_{q^t}-en.

A konjugáltság definíciójából közvetlenül látszik, hogy $\alpha \sim \alpha$, tehát ~ reflexív.

Amennyiben $\alpha \sim \beta$ és $\beta \sim \gamma$, akkor $\beta = \alpha^{q^u}$ és $\gamma = \beta^{q^v}$, ahol *u* és *v* egyaránt *t*-nél kisebb nem negatív egész, és helyettesítés után $\gamma = \left(\alpha^{q^u}\right)^{q^v} = \alpha^{q^{u+v}}$. De ha α $\mathbf{F}_q$ fölötti ciklikus rendje *s*, és $w = (u+v \mod s)$, ahol a jobb oldal az a legkisebb nemnegatív egész, amellyel $u+v \equiv w \ (s)$, akkor $0 \le w < s \le t$ és $\gamma = \alpha^{q^{u+v}} = \alpha^{q^w}$, és ekkor γ az α $\mathbf{F}_q$ fölötti konjugáltja, $\alpha \sim \gamma$, a reláció tranzitív.

Az előbbi α-val és β-val legyen $(-u \mod s)$. Ekkor $0 \le v < s \le t$ és $u+v \equiv 0 \ (s)$, így $\beta^{q^v} = \left(\alpha^{q^u}\right)^{q^v} = \alpha^{q^{u+v}} = \alpha$, vagyis a reláció szimmetrikus is, tehát valóban ekvivalencia.

2. A rendek egyenlőségének bizonyításához a szimmetria miatt elegendő megmutatni, hogy ha $\alpha \neq 0$, és $\alpha \sim \beta$, akkor β rendje osztója α rendjének. De ha α rendje *n*, akkor tetszőleges $r \in \mathbf{N}_0$-ra $\left(\alpha^r\right)^n = \left(\alpha^n\right)^r = e$, vagyis α^u rendje osztja *n*-et, és $\beta = \alpha^{q^u}$, így β rendje osztója *n*-nek, azaz α rendjének.

3. *s* osztója *t*-nek, és tetszőleges nemnegatív egész *i*-re és *k*-ra $\alpha^{q^i} = \alpha^{q^{i+ks}}$.

□

1.21. Következmény

Legyen α és β az F_{q^t} két eleme, és $\alpha \sim \beta$. Ekkor

1. $f \in \mathbf{F}_q[x]$-re α pontosan akkor gyöke *f*-nek, ha β is gyöke a polinomnak.
2. α és β $\mathbf{F}_q$ fölötti minimálpolinomja azonos.
3. α pontosan akkor primitív elem F_{q^t}-ben, ha β is az.

Δ

Bizonyítás:

1. Azt láttuk, hogy amennyiben α gyök, akkor α^q is az, innen pedig indukcióval kaptuk, hogy α^{q^i} is gyök, tehát α-val együtt valamennyi konjugáltja, így β is gyök. Mivel a konjugáltság ekvivalencia, és így szimmetrikus, ezért visszafelé is áll az állítás.

2. Ha α minimálpolinomja $\mathbf{F}_q$ fölött *m*, α^{q^i}-é m', akkor *m*-nek gyöke α^{q^i} és m'-nek α, vagyis a minimálpolinom egyik tulajdonsága alapján $m \mid m'$ és $m' \mid m$, és mindkettő főpolinom, így megegyeznek.

3. Nem nulla elem konjugáltja sem nulla. Konjugált elemek rendje megegyezik, és egy elem pontosan akkor primitív elem, ha a rendje $q^t - 1$, így ha α primitív elem, akkor β is az, és fordítva.

□

1.22. Definíció

Ha L a K test bővítése, akkor az L egy K **feletti relatív automorfizmus**a az L-nek önmagára való olyan izomorfizmusa, amely *K* elemeit helyben hagyja.

Δ

1.23. Tétel

Legyen L a *q*-elemű K véges test *t*-edfokú bővítése. Az *L* α és β eleme akkor és csak akkor konjugált K fölött, ha van L-nek olyan K fölötti σ relatív automorfizmusa, amellyel $\beta = \sigma(\alpha)$.

Δ

Bizonyítás:

Ha α és β konjugáltak K fölött, akkor $\beta = \alpha^{q^k}$ egy $0 \le k < t$ egésszel. De *q*-elemű test bármely bővítésében $\alpha \mapsto \alpha^{q^k}$ automorfizmus, amely az alaptest elemein az identikus leképezés.

Fordítva, legyen σ az L K feletti relatív automorfizmusa, és $\beta = \sigma(\alpha)$, továbbá az α K feletti minimálpolinomja $f = \sum_{i=0}^{n} c_i x^i$. Ekkor

$$0 = \sigma(0) = \sigma\left(\hat{f}(\alpha)\right) = \sigma\left(\sum_{i=0}^{n} c_i \alpha^i\right) = \sum_{i=0}^{n} c_i (\sigma(\alpha))^i = \hat{f}(\sigma(\alpha))$$

így $\sigma(\alpha)$ is gyöke *f*-nek. Mivel *f* irreducibilis (mert minden minimálpolinom felbonthatatlan), ezért a korábbi eredmények alapján β az α egy q^k-kitevős hatványa, ahol $0 \le k < s$, és $s = \deg(f)$. De *f* foka egyben az α ciklikus rendje, amely osztója a bővítés fokának, *t*-nek, így $s \le t$, vagyis $0 \le k < t$, β az α K fölötti konjugáltja.

□

A bizonyításban hivatkoztunk rá, hogy *q*-elemű K test bármely L bővítésében minden $k \in \mathbf{N}_0$-ra $\alpha \mapsto \alpha^{q^k}$ az L K feletti relatív automorfizmusa. Belátjuk, hogy véges *L*-re nincs is más lehetőség.

1.24. Tétel

Legyen az L véges test a *q*-elemű K test *t*-edfokú bővítése, és $\sigma : \alpha \mapsto \alpha^q$ az *L* elemeire. Ekkor az L K feletti relatív automorfizmusai *t*-rendű ciklikus csoportot alkotnak a σ generátorelemmel.

Δ

Bizonyítás:

$\sigma : \alpha \mapsto \alpha^q$ automorfizmusa L-nek, és ha $\alpha \in K$, akkor $\alpha^q = \alpha$, ezért σ az L egy K feletti relatív automorfizmusa. Test relatív automorfizmusainak szorzata szintén relatív automorfizmus, és automorfizmusnak létezik inverze, amely ismét relatív automorfizmus, végül az identikus leképezés relatív automorfizmus, így ezek csoportot alkotnak. Legyen α az *L* tetszőleges eleme, és *u* a test egy primitív eleme. Definíciószerűen $\sigma^0 = \varepsilon$, és $\varepsilon(\alpha) = \alpha = \alpha^{q^0}$. Mivel $\alpha^{q^{k+1}} = \left(\alpha^{q^k}\right)^q$ minden $k \in \mathbf{N}_0$-ra, ezért, ha egy nem negatív egész *k*-ra $\sigma^k(\alpha) = \alpha^{q^k}$, akkor $\sigma^{k+1}(\alpha) = \sigma\left(\sigma^k(\alpha)\right) = \left(\alpha^{q^k}\right)^q = \alpha^{q^{k+1}}$, vagyis minden nem negatív egész *k*-val $\sigma^{k+1} : \alpha \mapsto \alpha^{q^{k+1}}$.

Legyen *u* az L primitív eleme, és τ az L egy K feletti relatív automorfizmusa. Az 1.23. Tétel szerint $\tau(u) = u^{q^k}$ egy $k \in \mathbf{N}_0$-lal. Amennyiben $\alpha \ne 0$, akkor $\alpha = u^i$ egy $q^t - 1 > i \in \mathbf{N}_0$ egésszel, és $\tau(\alpha) = \tau\left(u^i\right) = (\tau(u))^i = \left(u^{q^k}\right)^i = \left(u^i\right)^{q^k} = \alpha^{q^k}$, továbbá $\tau(0) = 0 = 0^{q^k}$, vagyis $\tau = \sigma^k$, így beláttuk, hogy az L bármely K feletti relatív automorfizmusa eleme a σ által generált ciklikus csoportnak.

u ciklikus rendje *t*, hiszen primitív elem ciklikus rendje azonos a bővítés fokával, így a *t*-nél kisebb kitevőkre $\sigma^i(u) = u^{q^i}$ páronként különböző, és a megfelelő σ^i automorfizmusok is páronként különbözőek, a σ által generált ciklikus csoport rendje legalább *t*. Másrészt az *L* bármely α elemével $\sigma^t(\alpha) = \alpha^{q^t} = \alpha = \sigma^0(\alpha)$, így $\sigma^t = \sigma^0 = \varepsilon$, ahol ε az identikus leképezés, azaz a csoport egységeleme, ami mutatja, hogy a csoport rendje legfeljebb *t*, tehát ez a rend pontosan *t*, így az L K feletti relatív automorfizmusai egy *t*-edrendű ciklikus csoportot alkotnak a σ generátorrendszerrel.

□

1.25. Definíció

Ha $\alpha = \mathbf{F}_{q^t}$, akkor $f = \prod_{k=0}^{t-1}\left(x - \alpha^{q^k}\right)$ az $\mathbf{F}_q$ **feletti karakterisztikus polinomja**.

Δ

A definícióból közvetlenül látszik, hogy $\deg(f) = t$, bármely elem gyöke a karakterisztikus polinomjának, és két elem karakterisztikus polinomja akkor és csak akkor azonos, ha konjugáltak.

1.26. Tétel

Legyen L a *q*-elemű K test *t*-edfokú bővítése, $\alpha \in L$, *m* az α K feletti minimálpolinomja, és *f* az α K feletti karakterisztikus polinomja. Ekkor $f \in \mathsf{K}[x]$, és $f = m^{\frac{t}{s}}$, ahol $s = \deg(m)$.

Δ

Bizonyítás:
α K feletti ciklikus rendje *s*, és $s \mid t$, ezért

$$f = \prod_{k=0}^{t-1}\left(x - \alpha^{q^k}\right) = \prod_{j=0}^{\frac{t}{s}-1}\prod_{i=0}^{s-1}\left(x - \alpha^{q^{i+js}}\right) = \prod_{j=0}^{\frac{t}{s}-1}\left(\prod_{i=0}^{s-1}\left(x - \alpha^{q^i}\right)\right) = m^{\frac{t}{s}}$$

amiből következik, hogy *f* K feletti polinom.

□

1.27. Következmény

Ha L|K, *L* véges, és $\alpha \in L$, akkor α K feletti konjugáltjainak összege és szorzata K-beli.

Δ

Bizonyítás:
A gyökök összege és szorzata a karakterisztikus polinom együtthatója, tehát *K*-beli.

□

1.28. Tétel

Az $\mathbf{F}_q$ fölött irreducibilis *m*-edfokú *f* polinom pontosan akkor osztója $x^{q^n} - x \in \mathbf{F}_q[x]$-nek, ha $m \mid n$, ahol $n \in \mathbf{N}_0$.

Δ

Bizonyítás:
Ha $n = 0$, akkor $m \mid n$, másrészt $x^{q^n} - x$ a nullpolinom, amelynek osztója minden *f* polinom, ekkor igaz az állítás. Nézzük az $n \in \mathbf{N}$ esetet, figyelembevéve, hogy irreducibilis polinom fokszáma, tehát *m*, nagyobb, mint 0. Legyen *f* $\mathbf{F}_q$ feletti felbontási testében α az *f* egy gyöke. $f \mid x^{q^n} - x$ pontosan akkor teljesül, ha α gyöke az $x^{q^n} - x$ polinomnak, tehát ha $\alpha^{q^n} - \alpha = 0$, vagyis ha $\alpha^{q^n} = \alpha$. De ez az egyenlőség akkor és csak akkor igaz, ha $s \mid n$, ahol *s* az α $\mathbf{F}_q$ fölötti ciklikus rendje, és ha *f* irreducibilis $\mathbf{F}_q$ fölött, akkor $s = m$.

□

1.29. Tétel

Legyen *P* azon $\mathbf{F}_q$ fölötti irreducibilis főpolinomok halmaza, amelyek fokszáma egy rögzített *n* természetes szám osztója. Ekkor $x^{q^n} - x = \prod_{f \in P} f$.

Δ

Bizonyítás:

$x^{q^n} - x \in \mathbf{F}_q[x]$, és mint minden polinom, ez is faktorizálható. $\left(x^{q^n} - x\right)' = q^n x^{q^n - 1} - e = -e$, mivel $\mathbf{F}_q$ karakterisztikája osztja *q*-t és így q^n-t, ezért $x^{q^n} - x$-nek nincs többszörös gyöke, tehát többszörös faktora sem lehet. Az előbbi tétel szerint *P* minden eleme osztója $x^{q^n} - x$-nek, és mivel ezen polinomok mindegyike irreducibilis, tehát páronként relatív prím, ezért a szorzatuk, *g* is osztója az $x^{q^n} - x$ polinomnak. Ha most *t* az $x^{q^n} - x$ valamely irreducibilis főpolinom faktora $\mathbf{F}_q$ fölött, akkor *t* csak egyszeres faktor lehet, és az előző tétel szerint eleme *P*-nek, vagyis a *t*-k szorzata, $x^{q^n} - x$, osztója, de akkor asszociáltja *g*-nek. De mindkét polinom főpolinom, így meg is egyeznek.

□

1.30. Következmény

Az $\mathbf{F}_q$ fölött irreducibilis *n*-edfokú főpolinomok száma $\frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

Δ

A tételben μ a Moebius-függvény: $\mu(n) = \begin{cases} 1, & \text{ha } n = 1 \\ 0, & \text{ha } \exists p : p^2 \mid n \\ (-1)^r, & \text{ha } n = \prod_{i=1}^{r} p_i \wedge 1 \le i < j \le r \in \mathbf{N} : p_i \neq p_j \end{cases}$,

ahol *n* pozitív egész szám, és *p* illetve $r \ge i \in \mathbf{N}$-re p_i prímszám.

Bizonyítás:

$q^n = \deg\left(x^{q^n} - x\right) = \deg\left(\prod_{f \in P} f\right) = \sum_{f \in P} \deg(f)$, ahol a szereplő valamennyi *f*-re érvényes, hogy $\deg(f) \mid n$. Jelöljük a P-beli *n*-edfokú polinomok számát N_n-el. Ekkor $q^n = \sum_{d|n} dN_d$, vagyis q^n az $f(n) = nN_n$ számelméleti függvény összegzési függvénye, és így a Moebius-féle megfordítási összefüggéssel visszakapjuk *f*-et, ahonnan *n*-el való osztás után a felírt egyenlőségre jutunk.

□

1.16. megad egy szükséges és elégséges feltételt egy polinom irreducibilitására, ám ez inkább csak elvileg használható, hiszen a döntéshez ismerni kellene a polinom egy gyökét. Az alábbi tételben olyan feltételt adunk, amely a gyakorlatban is alkalmazható a felbonthatóság eldöntésére.

1.31. Tétel

Az $\mathbf{F}_q$ fölötti *n*-edfokú *f* polinom, ahol $2 \le n \in \mathbf{N}$, akkor és csak akkor irreducibilis $\mathbf{F}_q$ fölött, ha $\left(f, x^{q^i} - x\right) = e$ minden $\left\lfloor \frac{n}{2} \right\rfloor \ge i \in \mathbf{N}$-re (*e* az $\mathbf{F}_q$ egységeleme).

Δ

Bizonyítás:

Ha *f* legalább másodfokú polinom, akkor vagy felbontható vagy felbonthatatlan, és csak az egyik tulajdonság lehet igaz, így az eredeti kérdés helyett vizsgálhatjuk azt is, hogy mi a szükséges és elégséges feltétel a felbonthatósághoz.

Tételezzük fel, hogy *f* felbontható $\mathbf{F}_q[x]$-ben. Ekkor van olyan $\mathbf{F}_q$ fölött irreducibilis faktora, amelynek a fokszáma legfeljebb $\left\lfloor \frac{n}{2} \right\rfloor$. Ha *g* ilyen faktor, és $\deg(g)=u$, akkor *g* osztója *f*-nek és $x^{q^u}-x$-nek, így ezek legnagyobb közös osztójának is, a legnagyobb közös osztó nem konstans.

Ha viszont a tételbeli korlátok közé eső *u*-ra a legnagyobb közös osztó nem konstans, akkor van felbonthatatlan osztója, mondjuk *g*, ennek foka osztója *u*-nak, ami biztosan kisebb *n*-nél, tehát *g* valódi osztója *f*-nek, *f* felbontható.

□

1.32. Következmény

Az $\mathbf{F}_q$ fölötti *n*-edfokú *f* polinom, ahol $2 \le n \in \mathbf{N}$, akkor és csak akkor irreducibilis $\mathbf{F}_q$ fölött, ha $\hat{f}(0) \neq 0$, és $\left(f, x^{q^i-1}-e\right)=e$ minden $\left\lfloor \frac{n}{2} \right\rfloor \ge i \in \mathbf{N}$-re (*e* az $\mathbf{F}_q$ egységeleme).

Δ

Bizonyítás:

A legalább másodfokú *f* polinom csak úgy lehet felbonthatatlan, ha *x* nem osztója, vagyis ha $\hat{f}(0) \neq 0$. Ekkor *f* és *x* relatív prímek, és mivel $x^{q^u}-x=x\left(x^{q^u-1}-e\right)$, ezért $\left(f, x^{q^i}-x\right)=\left(f, x^{q^i-1}-e\right)$.

□

1.31.-ben és 1.32.-ben $\deg(f) \ge 2$ nem jelent lényeges megszorítást, hiszen a nulladfokú polinomok egységek egy test fölötti polinomgyűrűben, míg az elsőfokú polinomok felbonthatatlanok. Hasonló a helyzet 1.32.-ben $\hat{f}(0) \neq 0$-val, mert ha 0 gyöke a polinomnak, akkor $f = xg$, és ha *f* legalább másodfokú, akkor *g* legalább elsőfokú, vagyis *f* felbontható.

Mivel a felbonthatóság mindig adott testre vonatkozik, ezért érdemes megvizsgálni, hogy ha egy polinom felbonthatatlan egy test fölött, akkor hogyan viselkediik egy másik testhez viszonyítva.

1.33. Tétel

Ha *f* *n*-edfokú irreducibilis polinom a *q*-elemű K test fölött, L a K bővítése és $[\mathsf{L}:\mathsf{K}]=m$, akkor *f* *d* számú, páronként különböző, $\mathsf{L}[x]$-ben irreducibilis polinom szorzata, ahol $d=(m,n)$, és valamennyi faktor $\frac{n}{d}$-edfokú. Amennyiben $\alpha \in L$ az előbbi irreducibilis *f* gyöke, akkor α^{q^u} és α^{q^v} pontosan akkor gyöke ugyanazon faktornak, ha $u \equiv v \ (d)$, így $d > i \in \mathbf{N}_0$-re az α^{q^i} gyökök a felbontásban szereplő páronként különböző polinom gyökei.

Δ

Bizonyítás:

Legyen M az *f* K fölötti felbontási teste, és tegyük fel, hogy *f* a K test fölött irreducibilis, *n*-edfokú főpolinom (ez utóbbi feltétel semmiben nem korlátozza az általánosságot, hiszen a főegyüttható nem nulla, és így egység a test feletti polinomgyűrűben), továbbá α az *f* egyik *M*-beli gyöke. Mivel *f* *n*-edfokú, $\mathbf{F}_q$ fölött felbonthatatlan főpolinom, ezért M fölött $f=\prod_{i=0}^{n-1}\left(x-\alpha^{q^i}\right)$, és $j > i \in \mathbf{N}_0$ egé-

szekre $\alpha^{q^i}=\alpha^{q^j} \Leftrightarrow i \equiv j \ (n)$. Legyen f felbontása L fölött $f=\prod_{i=0}^{r-1} g_i$. Nyilván teljesül, hogy f gyökeinek halmaza megegyezik a g_i faktorok *M*-beli gyökei halmazának uniójával. f irreducibilis K fölött, így gyökei egyszeresek, amiből következik, hogy a g_i polinomok páronként különbözőek, tehát *M*-ben gyökeik halmaza páronként diszjunkt, másrészről egyik ilyen halmaz sem üres, hiszen irreducibilis polinom legalább elsőfokú, azaz összefoglalóan a g_i polinomok gyökeinek halmazai f gyökei halmazát partícionálják. Legyen u az $r > i \in \mathbf{N}_0$ indexek bármelyike, és β a g_u gyöke. Ekkor $\beta=\alpha^{q^k}$ alkalmas $n > k \in \mathbf{N}_0$ egésszel. g_u L fölött felbonthatatlan polinom, ezért g_u valamennyi gyöke a β valamely $\left(q^m\right)^i = q^{mi}$ kitevős hatványa, vagyis $\alpha^{q^{k+mi}}$ alakú, és g_u foka a legkisebb pozitív egész *t*, amelyre teljesül a $k \equiv k+mt \ (n)$ kongruencia, ahonnan $\deg(g_u)=\frac{n}{d}$. Mivel ez független *u*-tól, ezért valamennyi faktor foka azonos, ahonnan azt is kapjuk, hogy a faktorok száma, *r*, éppen *d*.

A fentiek alapján α^{q^i} és α^{q^j} pontosan akkor gyöke ugyanazon faktornak, ha egy *w* egésszel $j \equiv i+mw \ (n)$. Ilyen *w* akkor és csak akkor van, ha $i-j$ osztható *m* és *n* legnagyobb közös osztójával, azaz ha $i \equiv j \ (d)$, és így $d > i \in \mathbf{N}_0$-ra az α^{q^i} gyökök páronként különböző faktorhoz tartoznak.

□

1.34. Következmény

A K véges test felett irreducibilis *n*-edfokú polinom pontosan akkor irreducibilis a K *m*-edfokú L bővítése fölött, ha $(m,n)=1$, és akkor és csak akkor elsőfokú polinomok szorzata L felett, ha $n \mid m$.

Δ

Bizonyítás:

Az előző tétel alapján a polinom akkor és csak akkor felbonthatatlan a bővebb test felett, ha $d=1$, vagyis ha *m* és *n* relatív prímek, míg a második esetben $d=n$, azaz *n* osztója legyen *m*-nek.

□

1.35. Definíció

A K test feletti *n*-edfokú f polinom **reciproka**, illetve **duálisa**, $f^* := x^n\left(f \circ x^{-1}\right)$, míg $0^* := 0$.

Δ

1.36. Tétel

Ha $f \in \mathsf{K}[x]$, akkor f^* is K feletti polinom. Amennyiben f^* K felett felbontható, akkor f is felbontható K felett, míg ha f felbontható $\mathsf{K}[x]$-ben, és $\hat{f}(0) \neq 0$, akkor f^* is reducibilis K fölött.

Δ

Bizonyítás:

a. $f=0$ -ra igaz az állítás. Legyen most $\deg(f)=n$ és $f=\sum_{i=0}^{n} a_i x^i$, akkor

$$f^* = x^n\left(f \circ x^{-1}\right) = x^n \sum_{i=0}^{n} a_i x^{-i} = \sum_{i=0}^{n} a_i x^{n-i} = \sum_{i=0}^{n} a_{n-i} x^i = \sum_{i=0}^{n} b_i x^i \ ,$$

ahol $b_i = a_{n-i}$, így látható, hogy f^* valóban K feletti polinom.

b. Legyen $f = gh$, és *f, g* és *h* foka rendre *n, m* és *r*, akkor $n = m + r$. A határozatlan felcserélhető az együtthatókkal, ezért $f^* = x^n\left(f \circ x^{-1}\right) = x^{m+r}\left((gh)\circ x^{-1}\right) = \left(x^m\left(g\circ x^{-1}\right)\right)\left(x^r\left(h\circ x^{-1}\right)\right) = g^*h^*$.

c. Ha $c \in K^*$, akkor $f = c$-re $\deg(f) = 0$, és $f^* = c^* = x^0\left(c\circ x^{-1}\right) = c$, míg ha $f = x$, akkor $\deg(f) = 1$, és így $f^* = (x)^* = x\left(x\circ x^{-1}\right) = e$.

d. a. szerint f^* legfeljebb *n*-edfokú, és akkor és csak akkor *n*-edfokú, ha $0 \neq b_n = \hat{f}(0)$.

e. $\hat{f}^*(0) = b_0 = a_n \neq 0$.

f. Ha $f = x^r g$, ahol $\hat{g}(0) \neq 0$, akkor b. és c. alapján $f^* = g^*$, ezért $\left(f^*\right)^* = \left(g^*\right)^*$. Most d.-ből g^* foka azonos *g* fokával, és így az a. ponthoz hasonlóan eljárva, és figyelembevéve e.-t kapjuk, hogy $\left(f^*\right)^* = g$. Ebből következik, hogy $\left(f^*\right)^* \Big| f$.

g. Legyen f^* felbontható K felett, és $f^* = uv$, ahol *u* és *v* egyaránt legalább elsőfokú. Az e. pont alapján $\hat{f}^*(0) \neq 0$, és így $\hat{u}(0) \neq 0$ és $\hat{v}(0) \neq 0$, vagyis u^* és v^* is legalább elsőfokú. Viszont $u^*v^* = \left(f^*\right)^* \Big| f$, ami mutatja, hogy *f* is felbontható K fölött.

h. Ha *f* felbontható, és $\hat{f}^*(0) \neq 0$, akkor $f = uv$ úgy, hogy *u* és *v* foka legalább 1, és $\hat{u}(0) \neq 0$, $\hat{v}(0) \neq 0$. Innen $f^* = u^*v^*$, és *u* valamint *v* egyaránt legalább elsőfokú, ami azt jelenti, hogy *f* reciproka felbontható.

□

1.37. Tétel

$0 \neq f \in \mathsf{K}[x]$-nek $\alpha \neq 0$ akkor és csak akkor *k*-szoros gyöke, ha α^{-1} az f^* *k*-szoros gyöke.

Δ

Bizonyítás:

Legyen először a nem nulla α az f *k*-szoros gyöke, akkor $f = (x-\alpha)^k g$, $\hat{g}(\alpha) \neq 0$, és α-nak létezik inverze, így $f^* = (e-\alpha x)^k g^* = (-\alpha)^k\left(x-\alpha^{-1}\right)^k g^*$, α inverze legalább *k*-szoros gyöke *f* duálisának. Amennyiben viszont $g^*\left(\alpha^{-1}\right) = 0$, akkor $f^* = \left(x-\alpha^{-1}\right)^{k+1} h$, innen az előbbi átalakításhoz hasonlóan eljárva kapjuk, hogy $\left(f^*\right)^* = (-\alpha)^{k+1}(x-\alpha)^{k+1}h^*$, és mivel $\left(f^*\right)^*$ osztója *f*-nek, ezért $f = (x-\alpha)^{k+1}u$, ami lehetetlen, hiszen ez azt jelentené, hogy α legalább $k+1$-szeres gyöke *f*-nek.

Fordítva, ha α^{-1} f^* *k*-szoros gyöke, akkor az előbbiek szerint α pontosan *k*-szoros gyöke $\left(f^*\right)^*$-nak. De $f = x^r\left(f^*\right)^*$, ahol *r* nemnegatív egész, és $\alpha \neq 0$ (reciprok polinomnak a 0 nem gyöke), így α nem gyöke x^r-nek, α multiplicitása *f*-ben és $\left(f^*\right)^*$-ban, de akkor *f*-ben és f^*-ban megegyezik.

□

Érdekesek és fontosak azok a polinomok, amelyek duálisa saját asszociáltjuk.

1.38. Definíció

A K test feletti *f* polinom **önduális** vagy **reciprok**, ha $f^* = cf$ egy K^*-beli *c* elemmel.

Δ

1.39. Tétel

A K test feletti nem nulla *f* polinomra az alábbi állitások ekvivalensek:

a. *f* önduális

b. $f^* = f$ vagy $f^* = -f$.

c. az f K feletti felbontási testének egy α eleme pontosan akkor *r*-szeres gyöke *f*-nek, ahol *r* egy pozitív egész, ha α^{-1} is pontosan *r*-szeres gyöke *f*-nek.

Δ

Bizonyítás:

1. Legyen *f* önduális. Ha f *n*-edfokú, és a_0 illetve a_n a konstans tagja és főegyüttható ja, akkor a duális polinomban a_n a konstans tag és a_0 az *n*-edfokú tag együtthatója, ezért a feltétel alapján $a_n = ca_0$ és $a_0 = ca_n$, vagyis $a_n = c^2 a_n$, és mivel $a_n \neq 0$, ezért $c^2 = e$, vagyis *c* gyöke a K feletti $x^2 - e$ polinomnak. De ennek a polinomnak pontosan két megoldása van: *e* és $-e$ (ha a test karakterisztikája 2, akkor ez a két gyök azonos, vagyis ekkor egy darab kétszeres gyök van).

2. Ha $f^* = f$ vagy $f^* = -f$, és *f* nem a nullpolinom, akkor *f* konstans tagja nem nulla, így a 0 nem gyöke a polinomnak. Azt viszont az előző tételben bebizonyítottuk, hogy egy polinom nem nulla gyökének multiplicitása, és a gyök inverzének multiplicitása a reciprok polinomban azonos, az pedig nyilvánvaló, hogy egy polinomnak és ellentettjének a gyökei azonosak és ugyanolyan multiplicitásúak.

3. Most legyen *f* olyan polinom, amelynek bármely α gyökére igaz, hogy α és α^{-1} azonos multiplicitású gyök. Ebből következik, hogy a nulla nem lehet gyöke a polinomnak, vagyis $\hat{f}(0) \neq 0$, és ha $f = c(x-e)^r (x+e)^s \prod_{i=1}^{m} \left((x-\alpha_i)\left(x-\alpha_i^{-1}\right)\right)^{r_i}$ az *f* gyöktényezős felírása, akkor a duális polinom definícióját alkalmazva

$$f^* = \left(c(x-e)^r (x+e)^s \prod_{i=1}^{m} \left((x-\alpha_i)\left(x-\alpha_i^{-1}\right)\right)^{r_i} \right)^* =$$

$$= (-1)^{r+\sum_{i=1}^{m} r_i} \prod_{i=1}^{m} \left(\alpha_i^{r_i} \left(\alpha_i^{-1}\right)^{r_i} \right) c(x-e)^r (x+e)^s \prod_{i=1}^{m} \left((x-\alpha_i)\left(x-\alpha_i^{-1}\right)\right)^{r_i} =$$

$$= (-1)^r c(x-e)^r (x+e)^s \prod_{i=1}^{m} \left((x-\alpha_i)\left(x-\alpha_i^{-1}\right)\right)^{r_i} = (-1)^r f$$

ami viszont éppen $\pm f$.

□

Végül meghatározzuk a duálisok legnagyobb közös osztóját és legkisebb közös többszörösét.

1.40. Tétel

Ha $d = \left(f_i \middle| n \geq i \in \mathbf{N}\right)$ és $t = \left[f_i \middle| n \geq i \in \mathbf{N}\right]$, akkor az f_i -k duálisainak legnagyobb közös osztója d^*, és legkisebb közös többszöröse t^*.

Δ

Bizonyítás:

Ha minden *i*-re f_i a nullpolinom, akkor a legnagyobb közös osztó a nullpolinom, és ekkor igaz a legnagyobb közös osztóra vonatkozó állítás. Amennyiben a megadott polinomok között van nem nulla, akkor a legnagyobb közös osztó értékét nem befolyásolja nullpolinomok hozzávétele vagy elhagyása, így feltehetjük, hogy a megadott polinomok egyike sem nulla. Legyen δ a reciprok polinomok legnagyobb közös osztója. Mivel nem nulla polinom duálisa a nullában nem nulla, és δ osztója a

duálisoknak, ezért $\hat{\delta}(0) \neq 0$, és így $\left(\delta^*\right)^* = \delta$. $n \geq i \in \mathbf{N}$-re δ osztója f_i^*-nak, így δ^* osztója $\left(f_i^*\right)^*$-nak, ami viszont osztója f_i-nek, amiből következik, hogy δ^* osztója az f_i-k legnagyobb közös osztójának, azaz *d*-nek, innen pedig kapjuk, hogy δ^* reciproka, vagyis δ osztója d^*-nak. Másrészről minden $n \geq i \in \mathbf{N}$-re *d* osztója f_i-nek, ezért d^* osztója f_i^*-nak, ami csak úgy lehetséges, ha egyben osztója az utóbbi polinomok legnagyobb közös osztójának, azaz δ-nak. Ez az előbbi oszthatósággal kiadja, hogy δ és d^* asszociáltak, és ha mindkettőt főpolinomnak választjuk, akkor meg is egyeznek.

Amennyiben az adott polinomok között előfordul a nullpolinom, akkor a legkisebb közös többszörös is nulla, másrészt a reciprokok között is fellép a nullpolinom, így a két legkisebb közös többszörös egybeesik. Legyen most az f_i-k halmaza olyan, amelyben nem szerepel a nullpolinom; a legkisebb közös többszörösre vonatkozó állítást indukcióval bizonyítjuk. Ha $n = 1$, akkor nyilvánvaló az egyenlőség. Ha $n = 2$, akkor $td = f_1 f_2$, ahonnan $t^* d^* = f_1^* f_2^*$, amiből már adódik az állítás, hiszen d^* az f_1^* és f_2^* legnagyobb közös osztója. Végül $n \geq 2$-nél $\left[f_i \middle| n \geq i \in \mathbf{N}\right] = \left[\left[f_i \middle| n > i \in \mathbf{N}\right], f_n\right]$, és ebből kiadódik az állítás.

□

2. Egységgyökök

2.1. Definíció

A K test feletti $x^n - e$ polinom K feletti $\mathsf{K}^{(n)}$ felbontási teste, ahol e a K egységeleme, és $n \in \mathbf{N}$, **a** K **fölötti** *n*-**edik körosztási test**. A polinom $\mathsf{K}^{(n)}$-beli gyökei a K **feletti** *n*-**edik egységgyökök**, ezek halmaza $E^{(K,n)}$.

Δ

2.2. Megjegyzés

Mivel a körosztási test egy adott polinom felbontási teste, és egy rögzített test feletti adott polinom felbontási teste izomorfizmustól eltekintve létezik és egyértelmű, így adott K test és n pozitív egész esetén a K fölötti n-edik körosztási test létezik, és izomorfizmustól eltekintve egyértelmű.

Δ

2.3. Tétel

Legyen K p-karakterisztikájú test, ahol $p = 0$, vagy p prímszám, $n \in \mathbf{N}$, és $n = pm$, ahol $m \in \mathbf{N}$. Ekkor $E^{(K,n)} = E^{(K,m)}$, és $\mathsf{K}^{(n)} = \mathsf{K}^{(m)}$.

Δ

Bizonyítás:

$n \in \mathbf{N}$-ből $n \neq 0$, ezért, ha $n = pm$, akkor p sem lehet 0, vagyis p prímszám, a test prímkarakterisztikájú. Prímkarakterisztikájú K test bármely a és b elemére érvényes az $(a-b)^p = a^p - b^p$ összefüggés, ezért ha a gyöke $x^n - e \in \mathsf{K}[x]$-nek, ahol e a test egységeleme, akkor

$$0 = a^n - e = a^{pm} - e = \left(a^m\right)^p - e^p = \left(a^m - e\right)^p$$

és mivel test nullosztómentes, ezért $a^m - e = 0$, a gyöke a K feletti $x^m - e$ polinomnak. Mindez a másik irányban is igaz: ha a gyöke $x^m - e$-nek, akkor $a^m - e = 0$, és ebből

$$0 = 0^p = \left(a^m - e\right)^p = a^{pm} - e = a^n - e$$

tehát a gyöke a K feletti $x^n - e$ polinomnak. Azt kaptuk, hogy K valamely bővítésének a eleme pontosan akkor gyöke $x^n - e$-nek, ha gyöke $x^m - e$-nek is, így a két polinom gyökeinek halmaza, de akkor a két felbontási test is azonos.

□

2.4. Következmény

Legyen K p-karakterisztikájú test, e a test egységeleme, $n \in \mathbf{N}$. Ha $n = p^r m$, ahol $r \in \mathbf{N}_0$, és m a p-vel nem osztható pozitív egész, akkor $E^{(K,n)} = E^{(K,m)}$, $\mathsf{K}^{(n)} = \mathsf{K}^{(m)}$, és $x^n - e$ minden gyöke p^r-szeres, $x^m - e$ valamennyi gyöke egyszeres a megfelelő felbontási test bármely bővítésében.

Δ

Bizonyítás:

Az első állítás az előző tételből adódik, ha ott *p*-t p^r-rel helyettesítjük, hiszen a bizonyításban alkalmazott összefüggés p^r esetén is érvényes, amennyiben *r* nem negatív egész. Ha $x^m - e$ gyökei egyszeresek a polinom felbontási testében, akkor egyrészt egyszeresek lesznek annak minden bővítésében, továbbá a tétel első fele szerint $x^n - e$ valamennyi gyöke p^r-szeres ugyanezen testekben (hiszen a két polinom felbontási teste K felett egybeesik). Az egyszeres gyökök esete maradt hátra. Egy polinomnak csak akkor van többszörös gyöke, ha valamely gyöke egyben a derivált polinomnak is gyöke. Elsőfokú polinomnak nincs többszörös gyöke, így feltehetjük, hogy $m \geq 2$. $x^m - e$ deriváltja mx^{m-1}. Ha *p* nem osztója *m*-nek, akkor ennek a polinomnak csak a nullelem a gyöke, és a nulla nem gyöke az eredeti polinomnak, viszont *m* a feltétel alapján nem osztható *p*-vel.

□

2.5. Tétel

Ha G kommutatív csoport az *e* egységelemmel, és $n \in \mathbf{N}$, akkor a $H := \{g \in G \mid g^n = e\}$ halmaz a szorzás *H*-ra való megszorításával részcsoport G-ben.

Δ

Bizonyítás:

$e^n = e$, így $H \neq \emptyset$. Ha *a*, *b* a *H* elemei, akkor $a^n = e = b^n$, $(ab^{-1})^n = a^n (b^n)^{-1} = e \cdot e^{-1} = e$, tehát ab^{-1} is eleme *H*-nak, H≤G.

□

2.6. Tétel

Ha K *p*-karakterisztikájú test, $n \in \mathbf{N}$, $n = p^r m$ a nem negatív *r* és *p*-vel nem osztható *m* pozitív egésszel, akkor $E^{(K,n)}$ *m*-edrendű ciklikus csoport a $\mathsf{K}^{(n)}$-beli szorzással.

Δ

Bizonyítás:

$E^{(K,n)} = E^{(K,m)}$, és mivel $x^m - e$ test feletti olyan polinom, amelynek minden gyöke egyszeres $\mathsf{K}^{(n)} = \mathsf{K}^{(m)}$-ben és annak minden bővítésében, ezért $E^{(K,n)}$-nek pontosan *m* eleme van, továbbá az előző tétel szerint csoport a testbeli szorzással (*e* a K egységeleme). Ha egy csoport rendje *m*, akkor minden elemének rendje osztója *m*-nek, és persze a csoport minden elemének van rendje, így $E^{(K,n)}$ tetszőleges *a* elemére $|a| = d \mid m$, és *d* pozitív egész. Legyen *a* a csoport *d*-edrendű eleme, és $k \in \mathbf{N}_0$. $(a^k)^t = e$ akkor és csak akkor, ha $kt \equiv 0 \ (d)$, amihez szükséges és elégséges, hogy $o_d^+(k) = \frac{d}{(k,d)} \mid t$. Ebből a^k rendje $\frac{d}{(k,d)}$, vagyis pontosan olyan *k*-ra lesz a^k *d*-edrendű, amelyre *k* relatív prím *d*-hez. A $d > k \in \mathbf{N}_0$ feltételt kielégítő egész kitevőkkel az *a* hatványai páronként különbözőek, és minden egész kitevős hatványa *a*-nak ezek egyikével azonos, ezért pontosan ezek az elemek adják az $x^d - e$ polinom gyökeit, továbbá ezek közül éppen $\varphi(d)$ számú lesz *d*-edrendű (φ az Euler-függvény). Az előbbiek együtt azt adják, hogy $E^{(K,n)}$ elemeinek rendje csak *m* pozitív egész osztói lehetnek, és egy ilyen *d* osztóra vagy nincs *d*-edrendű elem $E^{(K,n)}$-ben, vagy ha van, akkor pontosan $\varphi(d)$. Legyen $\psi(k)$ a pozitív egészeken értelmezett függvény, amely a *k* helyen 1, ha van $E^{(K,n)}$-ben *k*-adrendű

elem, egyébként 0. Ekkor $m=\sum_{d|m}\psi(d)\varphi(d)\le\sum_{d|m}\varphi(d)=m$, tehát ψ az m minden d osztóján, tehát m-nél is 1, van $E^{(K,n)}$-ben m-edrendű elem, mondjuk u. Az u által generált ciklikus csoport része $E^{(K,n)}$-nek, és m eleme van, ezért $E^{(K,n)}=[u]=\left\{u^k\middle|m>k\in\mathbf{N}_0\right\}$, $E^{(K,n)}$ m-edrendű ciklikus csoport.

□

2.7. Definíció

Legyen $n\in\mathbf{N}$. Az $E^{(K,n)}$ u eleme **primitív** n**-edik** (**egység**)**gyök** K **fölött**, ha a rendje n.

Δ

2.8. Tétel

Legyen $n\in\mathbf{N}$, és $u\in E^{(K,n)}$. u pontosan egy pozitív egész m-re K feletti primitív egységgyök, és ez az m nem osztható a test karakterisztikájával. Az előbbi u akkor és csak akkor K feletti s-edik egységgyök, ha $m|s$.

Δ

Bizonyítás:

Legyen $n=p^rt$, ahol p a test karakterisztikája, r nemnegatív egész, és t a p-vel nem osztható pozitív egész, ekkor $u\in E^{(K,t)}$, és $E^{(K,t)}$ t-edrendű ciklikus csoport. Legyen g generátoreleme ennek a ciklikus csoportnak, akkor $u=g^k$ egy $t>k\in\mathbf{N}_0$ egésszel. u rendje a csoportban $\frac{t}{(k,t)}$, jelöljük ezt m-el. Ekkor $u^m=e$, és $u\in\mathsf{K}^{(n)}$, tehát u gyöke a K feletti x^m-e polinomnak, vagyis u egy K feletti m-edik egységgyök, $u\in E^{(K,m)}$. Másrészt az előbbiek szerint u rendje ebben a csoportban m, és így u primitív m-edik egységgyök K fölött. Mivel elem rendje egyértelmű, u más kitevővel nem primitív egységgyök. Az is látható, hogy m osztója t-nek, ezért nem lehet osztható p-vel.

u pontosan akkor K feletti s-edik egységgyök, ha gyöke a K feletti x^s-e polinomnak, ami ekvivalens $u^s=e$-vel, ez pedig az $s\equiv 0\ (m)$ kongruenciával, azaz az $m|s$ feltétellel.

□

2.9. Tétel

Legyen K p-karakterisztikájú test, $n\in\mathbf{N}$, és $n=p^rm$ a nem negatív r és p-vel nem osztható m pozitív egésszel. u akkor és csak akkor primitív m-edik egységgyök K fölött, ha u m-edik egységgyök K fölött, de semmilyen m-nél kisebb t pozitív egészre nem K feletti t-edik egységgyök. A K fölötti primitív m-edik egységgyökök száma $\varphi(m)$, és ha u egy K feletti primitív m-edik egységgyök, akkor $\mathsf{K}^{(n)}=\mathsf{K}(u)$, és $x^m-e=\prod_{k=0}^{m-1}\left(x-u^k\right)$.

Δ

Bizonyítás:

Ha u primitív m-edik egységgyök K fölött, akkor a rendje m, tehát m-nél kisebb t pozitív egész kitevős hatványa nem lehet egyenlő az egységelemmel; a fordított eset viszont azt jelenti, hogy a rendje éppen m, és így m-edik primitív egységgyök.

$E^{(K,m)}$ ciklikus csoport, ezért van m-edrendű eleme, például u. Ekkor u mindazon hatványa is generálja a csoportot, amelynek a kitevője relatív prím m-hez. Ezek a hatványok különbözőek, ha $m>k\in\mathbf{N}_0$, és más, ezektől különböző ilyen tulajdonságú elem nincs a csoportban, ezért a megfelelő

tulajdonságú *u*-hatványok száma éppen $\varphi(m)$. $x^m - e$ gyökei egyszeresek és *u* hatványai, így igaz a szorzatalak. $\mathsf{K}^{(n)} = \mathsf{K}^{(m)}$, ez utóbbi viszont a legszűkebb olyan test, amely tartalmazza K-t, és a K feletti $x^m - e$ valamennyi gyökét. Ám $E^{(K,m)}$ ciklikus, így ha K egy L bővítése tartalmazza $E^{(K,m)}$ egy *g* generátorelemét, akkor *g* minden hatványát, tehát $x^m - e$ valamennyi gyökét is, ezért $\mathsf{K}^{(n)} = \mathsf{K}(u)$.

□

A fenti bizonyatásból kiemeljük az alábbi következményt.

2.10. Következmény

Legyen *u* primitív *n*-edik egységgyök a K test felett. Ekkor $\mathsf{K}^{(n)}$ valamely *v* eleme akkor és csak akkor primitív *n*-edik egységgyök $\mathsf{K}^{(n)}$-ben, ha $v = u^k$ egy egész *k*-val, és *k* relatív prím *n*-hez.

Δ

Most megnézzük, hogy különböző testek fölötti egységgyökök között milyen kapcsolat van.

2.11. Tétel

Legyen $n \in \mathbf{N}$, és $\mathsf{M}|\mathsf{K}_1 \cong \mathsf{K}_2$. Ekkor létezik olyan L test, hogy $\mathsf{M}^{(n)}|\mathsf{L}|\mathsf{K}_1$, és L izomorf $\mathsf{K}_2^{(n)}$-nel, továbbá ha $\varphi: E^{(K_2,n)} \to (M^{(n)};\cdot)$ injektív homomorfizmus, akkor $\mathrm{Im}(\varphi) = E^{(M,n)}$.

Δ

Bizonyítás:

Jelölje e_M és 0_M az M test egységelemét és nullelemét, és hasonlóan e_K és 0_K a K_2 megfelelő elemét. $E^{(M,n)}$ az M feletti $x^n - e_M$ polinom gyökeinek, vagyis az M feletti *n*-edik egységgyököknek a halmaza, és mivel K_1 részteste M-nek, és az $x^n - e_M$ polinom valamennyi együtthatója 0_M és e_M, és ezek az elemek K_1-ben is benne vannak, ezért $\mathsf{K}_1(E^{(M,n)})$ az $x^n - e_M$ mint K_1 feletti polinom K_1 feletti felbontási teste; hasonlóan $\mathsf{K}_2^{(n)}$ a K_2 feletti $x^n - e_K$ polinom K_2 feletti felbontási teste. De K_1 és K_2 izomorf, az izomorfizmusnak a polinomgyűrűkre való kiterjesztésénél $x^n - e_M$-nek $x^n - e_K$ felel meg, és izomorf testek feletti, egymásnak megfelelő polinomok felbontási teste izomorf, ezért $\mathsf{K}_1(E^{(M,n)})$ és $\mathsf{K}_2^{(n)}$ izomorf testek, az pedig a konstrukcióból nyilvánvaló, hogy $\mathsf{M}^{(n)}|\mathsf{K}_1(E^{(M,n)})|\mathsf{K}_1$.

M a K_1 bővítése, ez pedig izomorf K_2-vel, ezért a három test karakterisztikája azonos, mondjuk *p*. Ha $n = p^r m$, és *m* már nem osztható *p*-vel, akkor $E^{(K_2,n)}$ és $E^{(M,n)}$ *m*-edrendű ciklikus csoport a megfelelő test multiplikatív csoportjában. Legyen *u* generátoreleme $E^{(K_2,n)}$-nek, akkor $m > k \in \mathbf{N}_0$-ra az u^k-k páronként különbözőek, és kimerítik az $E^{(K_2,n)}$ halmazt. $\varphi(u^k) \in M^{(n)}$, továbbá $(u^k)^m = (u^m)^k = e_K^k = e_K$, és φ művelettartó, ezért $(\varphi(u^k))^m = \varphi((u^k)^m) = \varphi(e_K) = e_L = e_M$, így $\varphi(u^k) \in E^{(M,n)}$, és mivel φ injektív, ezért az előbbi képelemek páronként különbözőek, így ki is adják a teljes $E^{(M,n)}$ halmazt, hiszen ennek is pontosan *m* eleme van.

□

2.12. Következmény

1. Ha L *p*-karakterisztikájú test, és $\mathsf{K}_P = \mathbf{Q}$, ha $p = 0$, míg $\mathsf{K}_P = \mathbf{Z}_p$, amennyiben *p* prím, akkor létezik olyan $\varphi : \mathsf{K}_P^{(n)} \to \mathsf{L}^{(n)}$ injektív homomorfizmus, hogy *u* akkor és csak akkor *s*-edik egységgyök K_P felett, ha $\varphi(u)$ *s*-edik egységgyök L fölött.

2. Ha $\mathsf{M} | \mathsf{K}$, akkor $\mathsf{K}^{(n)} = \mathsf{K}\left(E^{(M,n)}\right)$.

3. Legyen $n \in \mathbf{N}$, M a K test olyan bővítése, amely tartalmazza $\mathsf{K}^{(n)}$-t, és σ az M K feletti relatív automorfizmusa. Ekkor K feletti *n*-edik egységgyök képe K feletti *n*-edik egységgyök, és primitív egységgyök képe is primitív egységgyök ugyanazon renddel.

Δ

Bizonyítás:

1. K_P izomorf az L prímtestével, L_P-vel, és ha φ az izomorfizmus, akkor injektív, és a magja csak a nullát tartalmazza, így alkalmazható az előző tétel.

2. Legyen $\mathsf{K}_1 = \mathsf{K} = \mathsf{K}_2$, ekkor az előző tétel alapján $\mathsf{L} = \mathsf{K}\left(E^{(M,n)}\right) = \mathsf{K}_1\left(E^{(M,n)}\right) \cong \mathsf{K}_2^{(n)} = \mathsf{K}^{(n)}$, és az identikus leképezéssel $E^{(K,n)} = E^{(M,n)}$.

3. $E^{(K,n)} \subseteq K^{(n)} \subseteq M$, így $E^{(M,n)} = E^{(K,n)}$, és $E^{(K,n)} \cong E^{(\sigma(M),n)}$, hiszen $\sigma(\mathsf{M}) | \mathsf{K}$.

□

Az előbbi következmény 1. pontja azt jelenti, hogy tetszőleges test feletti bármely (primitív) *n*-edik egységgyök a prímtest felett is (primitív) *n*-edik egységgyök, tehát ismerve a $\mathbf{Q}$ és a $\mathbf{Z}_p$ feletti egységgyököket, már minden *p*-karakterisztikájú test fölött is rendelkezünk az egységgyökökkel.

2.13. Tétel

Legyen K *q*-elemű test, *n* a *q*-hoz relatív prím természetes szám, és *u* egy K fölötti primitív *n*-edik egységgyök. Ekkor

1. u^k pontosan akkor eleme *K*-nak, ha $\dfrac{n}{(q-1,n)} \Big| k$
2. a *K*-beli *n*-edik egységgyökök száma $(q-1,n)$.

Δ

Bizonyítás:

u^k pontosan akkor eleme *K*-nak, ha *q*-adik hatványa önmaga, vagyis ha $u^{qk} = u^k$. Mivel *u* primitív *n*-edik egységgyök, ezért a rendje *n*, így $u^{qk} = u^k$ ekvivalens a $qk \equiv k \ (n)$ kongruenciával, vagy másként írva, ha $(q-1)k \equiv 0 \ (n)$. Ez pontosan azokra a *k* egészekre teljesül, amelyek oszthatóak $o_n^+(q-1)$-el, vagyis $\dfrac{n}{(q-1,n)}$-el, és az $n > k \in \mathbf{N}_0$ feltétellel az ilyen egészek száma $(q-1,n)$.

□

2.14. Tétel

Ha L *q*-elemű véges test, és K az L részteste, akkor $\mathsf{K}^{(q-1)} = \mathsf{L}$ és $E^{(K,q-1)} = L^*$, továbbá L minden primitív eleme, és csak ezek, $q-1$-edik primitív egységgyök K fölött.

Δ

Bizonyítás:

L^* elemei, és csak ezek, gyökei az L feletti $x^{q-1}-e$ polinomnak, így $E^{(L,q-1)}=L^*$, és a legszűkebb test, amely tartalmazza L^*-ot, maga L, amiből következik az $\mathsf{L}^{(q-1)}=\mathsf{L}$ egyenlőség. Ekkor $E^{(K,q-1)}=E^{(L,q-1)}=L^*$, és mivel L a K bővítése, és így L tartalmazza K-t, $\mathsf{K}^{(q-1)}=\mathsf{L}$ is igaz.

u akkor és csak akkor $q-1$-edik primitív egységgyök K fölött, ha egyben L fölött is hasonló tulajdonságú, tehát ha a rendje L^*-ban $q-1$. Ezek az elemek viszont éppen L primitív elemei.

□

A tétel azt fejezi ki, hogy minden véges test valamennyi nem nulla eleme valamilyen n-re n-edik, és így alkalmas m-re primitív m-edik egységgyök a test prímteste fölött.

Az alábbiakban egy fontos polinomot definiálunk.

2.15. Definíció

Legyen K tetszőleges test, és m a p-vel nem osztható egész szám, ahol p a K test karakterisztikája. A $Q^{(K,m)}=\prod_{\substack{k=0\\(k,m)=1}}^{m-1}\left(x-u^k\right)$ polinom a K **fölötti** m**-edik körosztási polinom**.

Δ

2.16. Tétel

Legyen K p-karakterisztikájú test, és m a p-vel nem osztható nem negatív egész. Ekkor $Q^{(K,m)}$ egy K_P feletti $\varphi(m)$-edfokú főpolinom, és $x^m-e=\prod_{d|m}Q^{(K,d)}$, ahol K_P K prímteste.

Δ

Bizonyítás:

$\varphi(m)$ a K feletti m-edik primitív egységgyökök, tehát a polinom gyökeinek száma, és így a körosztási polinom fokszáma, és a körosztási polinom főpolinomok szorzata, tehát maga is főpolinom.

Mivel m nem osztható p-vel, ezért x^m-e gyökei egyszeresek, továbbá mindegyikük egy és csak egy pozitív egészre primitív egységgyök K fölött, és a megfelelő egész osztója m-nek, ami igazolja x^m-e szorzatfelbontását. Azt kell még belátni, hogy a körosztási polinom együtthatói a prímtest elemei. Ezt indukcióval bizonyítjuk. 1 a p-vel nem osztható nem negatív egész, tehát megfelel a tétel követelményeinek. Ekkor $x^m-e=x-e\in K_P[x]$, és $x-e=Q^{(K,1)}$, vagyis $m=1$ esetén igaz az állítás. Tegyük fel, hogy már beláttuk a tétel igazságát minden, az $m>k\in\mathbf{N}$ feltételt kielégítő k egészre. Ekkor igaz lesz az állítás az m valamennyi valódi osztójára, így az x^m-e és $\prod_{\substack{d|m\\d<m}}Q^{(K,d)}$ K_P feletti polinomok, de akkor a hányadosuk, $Q^{(K,m)}$ is $K_P[x]$-beli.

□

2.17. Megjegyzés

Ha $\mathrm{char}(\mathsf{K})=0$, akkor $\mathsf{K}_P\cong\mathbf{Q}$, és így tartalmaz **Z**-vel izomorf részgyűrűt. A körosztási polinom főpolinom, így a bizonyításból látható, hogy az együtthatói benne vannak ebben a gyűrűben. Például az n-edik komplex egységgyökök esetén a körosztási polinom egy egész együtthatós főpolinom.

Δ

2.18. Tétel

Legyen S a $\mathsf{G}=(G;+)$ kommutatív csoport részfélcsoportja. Ha f az **N**-et S-be képezi, akkor $F(n)=\sum_{d|n} f(d)$ az **N**-et S-be képező függvény, és $\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$ a G-beli műveletekkel. Fordítva, ha $F:\mathbf{N}\to S$, akkor $\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)=f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)$ egy $f:\mathbf{N}\to G$ függvény, és $F(n)=\sum_{d|n} f(d)$ a G-beli művelettel (μ a Moebius-függvény).

Δ

Bizonyítás:

$f(d)$ minden $d\in\mathbf{N}$-re S-beli, és mivel S félcsoport az összeadással, ezért $F(n)$ is eleme S-nek. A kifejezés minden természetes számra értelmezett, továbbá az S-beli művelet egyértelmű, ezért valóban függvényt definiál az összeg, egy olyan függvényt, amely **N**-et képezi S-be.

Legyen d a pozitív egész n osztója. $\frac{n}{d}=m$ jelöléssel m is az n osztója, $d=\frac{n}{m}$, és különböző d-hez különböző m tartozik, ezért $\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$ teljesül, így még azt kell belátni, hogy $f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$, ha $F(n)=\sum_{d|n} f(d)$. De

$$\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)=\sum_{d|n}\left(\mu\left(\frac{n}{d}\right)\sum_{d'|d} f(d')\right)=\sum_{d'|n}\left(f(d')\sum_{d\left|\frac{n}{d'}\right.}\mu\left(\frac{n}{d}\right)\right)=f(n),$$

ugyanis a Moebius-függvényt egy adott n természetes szám osztóin kiszámítva és ezeket az értékeket összeadva, az összeg akkor és csak akkor különbözik 0-tól, ha $n=1$, és ekkor az összeg értéke 1, ez pedig esetünkben pontosan akkor teljesül, ha $d'=n$.

Az ellenkező irány esetén azt, hogy f a természetes számokat G-be képező függvény, hasonlóan láthatjuk be, mint az előbb F-ről, hogy **N**-et képezi S-be, míg ha $f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$, akkor

$$\sum_{d|n} f(d)=\sum_{d|n}\left(\sum_{d'|d}\mu\left(\frac{d}{d'}\right)F(d')\right)=\sum_{d'|n}\left(F(d')\sum_{d\left|\frac{n}{d'}\right.}\mu(d)\right)=F(n)$$

azaz F-ből indulva, f-en keresztül visszajutunk F-hez.

□

Összeadás helyett szorzást, együttható helyett kitevőt írva kapjuk az alábbi következményt.

2.19. Következmény

Legyen S részfélcsoportja a $\mathsf{G}=(G;\cdot)$ kommutatív csoportnak. Ha f az **N**-et S-be képezi, akkor $F(n)=\prod_{d|n} f(d)$ egy $F:\mathbf{N}\to S$ függvény, és $f(n)=\prod_{d|n}(F(d))^{\mu\left(\frac{n}{d}\right)}=\prod_{d|n}\left(F\left(\frac{n}{d}\right)\right)^{\mu(d)}$ a G-

beli szorzással, míg ha $F:\mathbf{N}\to S$, akkor $f(n)=\prod_{d|n}\left(F\left(\frac{n}{d}\right)\right)^{\mu(d)}\left(=\prod_{d|n}(F(d))^{\mu\left(\frac{n}{d}\right)}\right)$ egy $f:\mathbf{N}\to G$ függvény, és $F(n)=\prod_{d|n}f(d)$ a G műveletével.

Δ

2.20. Megjegyzés

Az előző következmény megfelelő része szerint az $u=\prod_{\substack{d|n\\ \mu\left(\frac{n}{d}\right)=1}}F(d)$ és $v=\prod_{\substack{d|n\\ \mu\left(\frac{n}{d}\right)=-1}}F(d)$ jelöléssel az *S* bármely ilyen *u* és *v* elemére a $vx=u$ egyenletnek van *S*-ben megoldása (és akkor S regularitása miatt csupán egy megoldása), és ez éppen $f(n)$, és hasonló a helyzet az additív esetben is, ha a produktumjelet szummajelre cseréljük, és $vx=u$ helyett $v+x=u$ -t írunk. R integritási tartományban a K hányadostesttel mind az additív, mind a multiplikatív alakok érvényesek a megfelelő műveletekkel.

Δ

2.21. Definíció

Az előző tételben és következményben szereplő *F* függvény az *f* **összegzési** illetve **szorzatfüggvénye**, míg *f* az *F* (**additív** illetve **multiplikatív**) **Moebius-transzformáltja**. *f*-nek az összegzési vagy szorzatfüggvényből való kifejezése a **megfordítási képlet**.

Δ

2.22. Tétel

Ha K *p*-karakterisztikájú test, és $p\nmid n\in\mathbf{N}$, akkor $Q^{(K,n)}=\prod_{d|n}\left(x^d-e\right)^{\mu\left(\frac{n}{d}\right)}$.

Δ

Bizonyítás:

Ez $x^n-e=\prod_{d|n}Q^{(K,d)}$ -ből a megfordítási képlet multiplikatív alakjával adódik.

□

2.23. Tétel

Legyen K *q*-elemű test, $n\in\mathbf{N}$, $(n,q)=1$. Ekkor $Q^{(K,n)}$ $\frac{\varphi(n)}{r}$ -számú, páronként különböző, *r*-edfokú, K fölött irreducibilis polinom szorzata, ahol $r=o_n(q)$.

□

Bizonyítás:

Ha K karakterisztikája *p*, akkor *p* prím, és *q* a *p* pozitív egész kitevős hatványa, ezért $(n,q)=1$ következtében *n* és *p* relatív prímek, $Q^{(K,n)}$ létezik, és a fokszáma pozitív egész. Legyen $Q^{(K,n)}$ K feletti felbontása irreducibilis polinomok szorzatára $Q^{(K,n)}=\prod_{i=1}^{s}m_i^{(K,n)}$. Az előzőek szerint $s\geq 1$. $Q^{(K,n)}$ gyökei egyszeresek, ezért az m_i faktorok páronként különbözőek. m_i legalább elsőfokú, így van gyöke, és ez a gyök csak $Q^{(K,n)}$ valamelyik gyöke, tehát egy K felett primitív *n*-edik egységgyök lehet. Ha ez a gyök *u*, akkor m_i gyökei pontosan azok az *u*-hatványok, amelyeknél a kitevő q^j alakú,

ahol $o_n(q) > j \in \mathbf{N}_0$, így a megfelelő faktor foka $o_n(q)$. Valamennyi primitív egységgyök gyöke egy és csak egy faktornak, ezért az előbbi megállapítás minden tényezőre érvényes, tehát ezek mindegyike $o_n(q)$-adfokú. $Q^{(K,n)}$ foka $\varphi(n)$, így a tényezők száma $\frac{\varphi(n)}{r}$, ahol *r* az egyes polinomok fokszáma.

□

2.24. Megjegyzés

Ebben a tételben lényeges az, hogy K karakterisztikája nem 0: bizonyítható ugyanis (de nem bizonyítjuk), hogy ha $\mathrm{char}(\mathsf{K}) = 0$, akkor a körosztási polinom irreducibilis a prímtest fölött (tehát a komplex egységgyökök esetén minden *n* természetes számra az *n*-edik körosztási polinom egy egész együtthatós, a **Z** fölött felbonthatatlan, $\varphi(n)$-edfokú főpolinom).

□

2.25. Következmény

Ha K egy *q*-elemű test, $n = p^r m$, ahol *r* nemnegatív egész, és *m* a *p*-vel nem osztható pozitív egész, akkor $\mathsf{K}^{(n)}$ a K $o_m(q)$-fokú egyszerű bővítése.

Δ

Bizonyítás

$\mathsf{K}^{(n)} = \mathsf{K}^{(m)} = \mathsf{K}(u)$ az *u* K feletti primitív *m*-edik egységgyökkel. Ez a K felett felbonthatatlan $o_m(q)$-adfokú polinom gyöke, ebből következik az állítás.

□

2.26. Tétel

Körosztási polinom önduális.

Δ

Bizonyítás

Ha *k* relatív prím *n*-hez, akkor $-k$ is az, így a körosztási polinom bármely gyökének inverze is gyök, továbbá minden gyök egyszeres.

□

3. Diszkrét Fourier-transzformáció

3.1. Definíció

Legyen $\mathsf{M}=(M;+)$ Abel-csoport, $\mathsf{R}=(R;+,\cdot)$ gyűrű. M egy R **fölötti bal oldali modulus**, vagy **bal oldali** R**-modulus**, ha

1. minden $(\rho,a)\in R\times M$ -hez van egy egyértelmű, $\rho\times a$ -val jelölt M-beli elem
2. és ha σ az R-nek, b az M-nek további eleme, akkor teljesülnek az alábbi azonosságok:

a. $(\rho\sigma)\times a=\rho\times(\sigma\times a)$
b. $(\rho+\sigma)\times a=\rho\times a+\sigma\times a$
c. $\rho\times(a+b)=\rho\times a+\rho\times b$

Jobb oldali R-modulus definíciója hasonló az értelemszerű módosítással. Ha S is gyűrű, M egyszerre bal oldali R-modulus az $\times_b$ és jobb oldali S-modulus a $\times_j$ művelettel, és minden R-beli ρ, S-beli σ és M-beli a-val fennáll a $(\rho\times_b a)\times_j\sigma=\rho\times_b(a\times_j\sigma)$ egyenlőség, akkor M-et R-S **modulus**nak, vagy röviden **két oldali modulus**nak mondjuk. Az M R fölötti bal oldali, jobb oldali valamint R-S modulust ${}_{\mathsf{R}}\mathsf{M}$-el, M_{S}-el és ${}_{\mathsf{R}}\mathsf{M}_{\mathsf{S}}$-el jelöljük.

Ha R egységelemes az ε egységelemmel, és az előbbi feltételeken túl $\varepsilon\times_b a=a$ illetve $a\times_j\varepsilon=a$, akkor a bal oldali modulust **unitér bal oldali** R**-modulus**nak, a jobb oldali modulust **unitér jobb oldali** R**-modulus**nak, és a kétoldali modulust **unitér** R-S **modulus**nak mondjuk.

Amennyiben K ferdetest, a K feletti unitér bal oldali modulus K **feletti vektortér**. Ha a K feletti M vektortér egyben gyűrű a $\cdot$ szorzással, és teljesül a $\rho\times(a\cdot b)=(\rho\times a)\cdot b=a\cdot(\rho\times b)$ feltétel, akkor M egy K **feletti algebra**, és a vektortér dimenziója az algebra **rangja**.

Az M valamely N részcsoportja illetve részgyűrűje részmodulus, unitér részmodulus, altér illetve részalgebra, ha M az előbbi tulajdonságú, és minden N-beli a-val $\rho\times_b a$ illetve $a\times_j\sigma$ eleme N-nek.

Δ

3.2. Definíció

Az S félcsoport centruma $C:=\{s\in S\,|\,\forall(u\in S):su=us\}$. Csoport centruma a csoport mint félcsoport centruma, míg gyűrű centruma a gyűrű multiplikatív félcsoportjának centruma.

Δ

3.3. Tétel

Félcsoport centruma zárt a félcsoport műveletére. Egységelem és zéruselem – ha létezik – mindig eleme a centrumnak. Csoport centruma a félcsoport-művelet megszorításával normális részcsoport, míg gyűrű centruma a gyűrűműveletek megszorításával részgyűrű.

Δ

Bizonyítás:

a. Ha u és v eleme C-nek, akkor $(uv)s=u(vs)=u(sv)=(us)v=(su)v=s(uv)$ a félcsoport tetszőleges s elemével, ami mutatja C műveleti zártságát.

b. Ha *e* egységelem, és *z* zéruselem a félcsoportban, akkor $es = s = se$ és $zs = z = sz$ a félcsoport bármely *s* elemével, vagyis *e* és *z* eleme a centrumnak.

c. Az előző pont alapján csoport illetve gyűrű centruma nem üres, így a. alapján a művelet (gyűrű esetén a multiplikatív művelet) megszorításával *C* részfélcsoport. Ha S csoport, akkor *u*-nak van u^{-1} inverze, és $us = su$ -ból $su^{-1} = u^{-1}s$, így u^{-1} is eleme a centrumnak, C részcsoport. Ezen túl $sus^{-1} = (su)s^{-1} = (us)s^{-1} = u(ss^{-1}) = ue = u$, így $s\mathsf{C}s^{-1} = \mathsf{C}$, C normális részcsoport S-ben. Ha viszont S gyűrű, akkor $(u-v)s = us - vs = su - sv = s(u-v)$ a gyűrű valamennyi *s* elemével, tehát $u - v$ is a centrumban van, így *C* mind a szorzásra, mind a kivonásra zárt, ennél fogva a műveletek *C*-re való megszorításával részgyűrű.

□

A továbbiakban sokszor alkalmazzuk az alábbi tétel megállapításait.

3.4. Tétel

Ha $\mathsf{T} = (T;+,\cdot)$, valamint $i \in \{b, j\}$-re $\mathsf{R}^{(i)}$ gyűrű, $\varphi^{(i)} : \mathsf{R}^{(i)} \to \mathsf{T}$ gyűrűhomomorfizmus, továbbá az $a^{(i)} \in R^{(i)}$ elemre $\varphi^{(i)}(a^{(i)}) = \alpha^{(i)}$, akkor $\beta \in T$ -re az $a^{(b)} \times_b \beta := \alpha^{(b)}\beta$ és $\beta \times_j a^{(j)} := \beta\alpha^{(j)}$ szabállyal T egy egy $\mathsf{R}^{(b)} - \mathsf{R}^{(j)}$ modulus.

Ha $\mathsf{R}^{(b)}$ egységelemes, és az egységelem képe egységelem T-ben, akkor T unitér bal oldali $\mathsf{R}^{(b)}$ modulus, és hasonlóan, ha $\mathsf{R}^{(j)}$ egységelemes, és az egységelem képe egységelem T-ben, akkor T unitér jobb oldali $\mathsf{R}^{(j)}$ modulus, végül, ha T unitér bal oldali $\mathsf{R}^{(b)}$ modulus és unitér jobb oldali $\mathsf{R}^{(j)}$ modulus, akkor T unitér $\mathsf{R}^{(b)} - \mathsf{R}^{(j)}$ modulus.

Ha $\mathsf{R}^{(b)}$ ferdetest, T unitér bal oldali $\mathsf{R}^{(b)}$ modulus, és $\mathrm{Im}(\varphi^{(b)}) = T^{(b)}$ része T centrumának, akkor T algebra $\mathsf{R}^{(b)}$ fölött, és ha T test, akkor az algebra rangja azonos a $\mathsf{T}\big|\mathsf{T}^{(b)}$ bővítés fokával.

Δ

Bizonyítás:

$\mathrm{Im}(\varphi^{(i)}) = T^{(i)}$ részgyűrű T-ben, így a definiált műveletek a gyűrű műveletei, és ekkor a modulusra megfogalmazott kritériumok a T-ben a műveletekre szükségszerűen teljesülnek. Az algebránál tett kikötés azért kell, hogy teljesüljön az $\alpha^{(b)}(\beta\gamma) = a^{(b)} \times_b (\beta\gamma) = \beta(a^{(b)} \times_b \gamma) = \beta(\alpha^{(b)}\gamma)$ feltétel, ahol $\gamma$is a *T* egy eleme. Ami az algebra rangját illeti, ez a bővítés fokának definíciójából adódik.

□

A tétel szerint minden gyűrű additív része kétoldali modulus bármely részgyűrűje fölött, és ha a gyűrű egységelemes, és a részgyűrű tartalmazza ezt az egységelemet, akkor unitér is a modulus. Ha még a részgyűrű ferdetest is, és benne van a gyűrű centrumában (és ekkor test), akkor a teljes gyűrű algebra a részgyűrű fölött. Speciális esetként kapjuk, hogy minden (egységelemes) gyűrű két oldali (unitér) modulus önmaga fölött, és ha ez a gyűrű test, akkor 1-rangú algebra (ismét önmaga fölött).

3.5. Tétel

Legyen $\mathsf{R} = (R;+,\cdot)$ gyűrű, $n \in \mathbf{N}$, $S = R^n$ és $\mathbf{u} \in S$, $\mathbf{v} \in S$. Ekkor az $(\mathbf{u} +_n \mathbf{v})_i := u_i + v_i$, $(\mathbf{u} \cdot_n \mathbf{v})_i := u_i \cdot v_i$ szabályokkal, ahol $n > i \in \mathbf{N}_0$, $\mathsf{S} = (S;+_n,\cdot_n)$ gyűrű. R és S egyszerre (bal oldali) egységelemes illetve kommutatív, és S pontosan akkor nullosztómentes, ha $n = 1$ és R nullosztómentes, vagy ha R a nullgyűrű.

Δ

Bizonyítás:

A gyűrűaxiómák minden komponensre külön-külön teljesülnek, mert ezeket a műveleteket egy gyűrűben végezzük, de akkor a teljes vektorra is teljesülnek, hiszen ezekre a műveletet komponensenként alkalmazzuk. A nullvektor minden komponense R nulleleme, míg az ellentett vektor *i*-edik komponense az *i*-edik komponens ellentettje.

Legyen $e^{(b)}$ bal oldali egységelem R-ben, $\mathbf{e}^{(b)} \in R^n$ olyan, hogy minden lehetséges *i*-re $e_i^{(b)} = e_i$. Ekkor az *S* bármely **u** elemére $\left(\mathbf{e}^{(b)} \cdot_n \mathbf{u}\right)_i = e_i^{(b)} \cdot u_i = e^{(b)} \cdot u_i = u_i$, $\mathbf{e}^{(b)}$ bal oldali egységelem az S gyűrűben. Ha viszont az *S* $\mathbf{e}^{(b)}$ eleme bal oldalról egységelem, akkor tetszőleges *R*-beli *u*-ra tekintve egy olyan *S*-beli **u** vektort, amelyben $u_0 = u$, kapjuk, hogy $e_0^{(b)} \cdot u = \left(\mathbf{e}^{(b)} \cdot_n \mathbf{u}\right)_0 = (\mathbf{u})_0 = u$, $e_0^{(b)}$ az R-ben bal oldali egységelem.

Ha R kommutatív, akkor tetszőleges *S*-beli **u**, **v** vektorral $(\mathbf{u} \cdot_n \mathbf{v})_i = u_i \cdot v_i = v_i \cdot u_i = (\mathbf{v} \cdot_n \mathbf{u})_i$, az új gyűrű is kommutatív. Fordítva, ha S kommutatív, és *u*, *v* az *R* elemei, akkor tekintve tetszőleges olyan **u** és **v** vektort, ahol $u_0 = u$ és $v_0 = v$, írhatjuk, hogy $u \cdot v = (\mathbf{u} \cdot_n \mathbf{v})_0 = (\mathbf{v} \cdot_n \mathbf{u})_i = v \cdot u$, ami mutatja, hogy az eredeti gyűrűben is felcserélhető bármely pár.

Nézzük az utolsó állítást. Ha $n = 1$, akkor *R* és *S* lényegében azonosak, így R és S egyszerre nullosztómentes, míg ha *S*-ben egyetlen elem van, akkor ez a nullelem, és most *S* is egyetlen elemből áll, S is nullgyűrű. A többi esetben $n > 1$, és *R*-ben van nullától különböző elem, mondjuk *a*. Legyen **u** az a vektor, amelyben $u_0 = a$, az összes többi komponens 0, míg **v** olyan, amelyben $v_0 = 0$, $v_1 = a$, és minden más *i*-re v_i tetszőleges, ekkor láthatóan sem **u**, sem **v** nem a nullvektor, vagyis nem nullák S-ben, viszont a szorzatvektor valamennyi komponense 0, azaz maga $\mathbf{u} \cdot_n \mathbf{v}$ is **0**.

□

3.6. Definíció

$\mathsf{S} = \left(R^n; +_n, \cdot_n\right)$ az R gyűrű *n*-**szeres direkt összege**.

Δ

3.7. Tétel

Legyen $\mathsf{R} = (R; +, \cdot)$ gyűrű, $n \in \mathbf{N}$, $\mathsf{S} = \left(R^n; +_n, \cdot_n\right)$, és $\tilde{R} := \left\{\tilde{r} \in R^n \middle| \forall (n > i \in \mathbf{N}_0) : \tilde{r}_i = r\right\}$. Ekkor $\tilde{R}$ egy $R \to \tilde{R}$ izomorfizmus, és ha $\mathbf{u} \in R^n$, akkor $(\tilde{r} \cdot_n \mathbf{u})_i = r \cdot u_i$ és $(\mathbf{u} \cdot_n \tilde{r})_i = u_i \cdot r$ minden $n > i \in \mathbf{N}_0$-re. Amennyiben R egységelemes, akkor az egységelem képe egységelem S-ben.

Δ

Bizonyítás:

φ az *R* minden eleméhez $\tilde{R}$-nek pontosan egy elemét rendeli, így φ *R*-nek $\tilde{R}$-be való leképezése. Ha $r \neq s$, akkor $\varphi(r) \neq \varphi(s)$, tehát φ injektív, és bármely $\tilde{R}$-beli elem képelem, φ szürjektív. $\tilde{R} \subseteq R^n$, és $(\varphi(r+s))_i = r + s = (\varphi(r))_i + (\varphi(s))_i$, továbbá $(\varphi(r \cdot s))_i = r \cdot s = (\varphi(r))_i \cdot (\varphi(s))_i$, ami igazolja a művelettartást, és így a bijektivitással az izomorfizmust, amiből adódik a műveleti zártság is.

A definíció alkalmazásával kapjuk, hogy $(\tilde{r} \cdot_n \mathbf{u})_i = \tilde{r}_i \cdot u_i = r \cdot u_i$, és hasonlóan a másik egyenlőséget. A direkt összeg egyszerre egységelemes a gyűrűvel, és ha *e* az R egységeleme, akkor $\varphi(e)$ minden komponense *e*, így az előbbi bekezdés alapján minden *i*-re $(\varphi(e) \cdot_n \mathbf{u})_i = e \cdot u_i = (\mathbf{u})_i$. Hasonló igaz a másik oldali szorzatra is, így $\varphi(e)$ egységelem S-ben.

□

3.8. Következmény

Legyen $\mathsf{R}=(R;+,\cdot)$ gyűrű, $n\in\mathbf{N}$, és $\mathsf{S}=(R^n;+,\cdot)$. Ekkor az $r\times_b\mathbf{u}:=\tilde{r}\cdot\mathbf{u}$, $\mathbf{u}\times_j r:=\mathbf{u}\cdot\tilde{r}$ szabállyal, ahol $r\in R$ és $\mathbf{u}\in R^n$, S kétoldali R-modulus, amely pontosan akkor unitér, ha R egységelemes. S akkor és csak akkor algebra R fölött, ha R test, és ekkor az algebra rangja *n*.

Δ

Bizonyítás:

Az előbbiek szerint R és $\tilde{\mathsf{R}}\le\mathsf{S}$ izomorf az $r\mapsto\tilde{r}$ megfeleletetéssel, így a 3.4. Tétel szerint S két oldali R modulus a tételben megfogalmazott szabályokkal. S és R egyszerre egységelemes, és ha R egységeleme *e*, akkor $\tilde{e}$ egységelem S-ben, a modulus unitér.

Ha R test, akkor egységelemes, tehát a modulus unitér. A szorzás kommutatív a testben, így a direkt összegben is teljesül a szorzás kommutativitása, így algebrát kapunk, ha viszont R csak ferdetest, akkor nem minden elemmel teljesül a felcserélhetőség. Legyen $n>i\in\mathbf{N}_0$-ra $\mathbf{e}^{(i)}\in R^n$ olyan, hogy $e_j^{(i)}=\delta_{i,j}e$, ahol $n>j\in\mathbf{N}_0$. Ekkor $\mathbf{u}\in R^n$-nel $\mathbf{u}=\sum_{i=0}^{n-1}c_i\times_b\mathbf{e}^{(i)}$ pontosan akkor teljesül, ha minden $n>j\in\mathbf{N}_0$ indexre $u_j=\left(\sum_{i=0}^{n-1}c_i\times_b\mathbf{e}^{(i)}\right)_j=\sum_{i=0}^{n-1}\delta_{i,j}c_i=c_j$, vagyis $\left\{\mathbf{e}^{(i)}\middle|n>i\in\mathbf{N}_0\right\}$ $(R;+)$-nak mint R fölötti vektortérnek bázisa, így az algebra rangja *n*.

□

3.9. Definíció

Legyen $a\in\mathbf{R}$, $b\in\mathbf{R}^*$. Ekkor $a^{(b)}=(a\ \mathrm{mod}\ b):=a-b\left\lfloor\frac{a}{b}\right\rfloor$.

Δ

Könnyen ellenőrizhető, hogy $0\le\frac{a^{(b)}}{b}<1$, továbbá ha $i\in\mathbf{Z}$ és $n\in\mathbf{N}$, akkor $n>i^{(n)}\in\mathbf{N}_0$, és $i^{(n)}\equiv i\ (n)$, vagyis $i^{(n)}$ az *i* *n*-el való osztásakor keletkező nem negatív maradéka.

3.10. Definíció

Legyen R gyűrű, $n\in\mathbf{N}$, **u** és **v** az R^n elemei, és $w_i:=\sum_{j=0}^{n-1}u_jv_{(i-j)^{(n)}}$ a **w** *i*-edik komponense. Ekkor $\mathbf{w}=\mathbf{u}*\mathbf{v}$ az **u és v** (**ciklikus**) **konvolúciója**. Ha **a** és **b** az R^{2n} olyan elemei, amelyek legalacsonyabb indexű *n* komponense azonos **u**-val illetve **v**-vel, és a többi komponens 0, akkor **a** és **b** – R^{2n}-beli – ciklikus konvolúciója az **u és v** (**lineáris**) **konvolúciója**, ezt $\mathbf{w}=\mathbf{u}\circ\mathbf{v}$ jelöli.

Δ

Látható, hogy a lineáris konvolúció az R^n-beli párokhoz R^{2n} egy elemét rendeli.

3.11. Tétel

Ha $\mathsf{R}=(R;+,\cdot)$ gyűrű, és $n\in\mathbf{N}$, akkor $\mathsf{T}=(R^n;+,*)$ is gyűrű, ahol a T-beli + a komponensenkénti R-beli összeadás. Az $\overline{R}:=\left(\bar{r}\in R^n\middle|r_0=r\wedge(n>i\in\mathbf{N}_0:r_i=0)\right)$ halmaz a T-nek R-rel izomorf részgyűrűje, és ha $\mathbf{u}\in T$, akkor $(\bar{r}*\mathbf{u})_i=r\cdot u_i$, $(\mathbf{u}*\bar{r})_i=u_i\cdot r$.

Δ

Bizonyítás:

Az összeadásra teljesülnek a feltételek. $*$ az R^n bármely két elemére értelmezett, az eredmény is *n*-komponensű, és valamennyi komponens az *R* egyértelműen meghatározott eleme, hiszen R-beli szorzással és összeadással áll elő, így $*$ binér művelet R^n-en.

$$\big((\mathbf{u}*\mathbf{v})*\mathbf{v}\big)_i = \sum_{j=0}^{n-1}\big(\mathbf{u}*\mathbf{v}\big)_j\, w_{(i-j)^{(n)}} = \sum_{j=0}^{n-1}\left(\sum_{k=0}^{n-1} u_k v_{(j-k)^{(n)}}\right) w_{(i-j)^{(n)}} =$$

$$= \sum_{k=0}^{n-1}\left(u_k \sum_{j=0}^{n-1} v_j\, w_{((i-k)-j)^{(n)}}\right) = \sum_{k=0}^{n-1} u_k \big(\mathbf{v}*\mathbf{w}\big)_{(i-k)^{(n)}} = \big(\mathbf{u}*\big(\mathbf{v}*\mathbf{w}\big)\big)_i$$

$$\big((\mathbf{u}+\mathbf{v})*\mathbf{w}\big)_i = \sum_{j=0}^{n-1}\big(\mathbf{u}+\mathbf{v}\big)_j\, w_{(i-j)^{(n)}} = \sum_{j=0}^{n-1}\big(u_j + v_j\big) w_{(i-j)^{(n)}} =$$

$$= \sum_{j=0}^{n-1} u_j\, w_{(i-j)^{(n)}} + \sum_{j=0}^{n-1} v_j\, w_{(i-j)^{(n)}} = \big(\mathbf{u}*\mathbf{w} + \mathbf{v}*\mathbf{w}\big)_i$$

így $*$ asszociatív, és disztributív az összeadás fölött (a bal oldali disztributivitás bizonyítása hasonló).

Az nyilvánvaló, hogy $\overline{R} \subseteq R^n$, és $\varphi: r \mapsto \bar{r}$ bijekció *R* és $\overline{R}$ között, másrészt könnyen belátható, hogy $\overline{r+s} = \bar{r} + \bar{s}$ és $\overline{r \cdot s} = \bar{r} * \bar{s}$, tehát φ művelettartó, azaz T műveleteinek $\overline{R}$-re való megszorításával R-rel izomorf részgyűrűt kapunk T-ben. $\big(\bar{r} * \mathbf{u}\big)_i = \sum_{j=0}^{n-1} \bar{r}_j u_{(i-j)^{(n)}} = \bar{r}_0 \cdot u_i = r \cdot u_i$, hiszen $\bar{r}_j$ legfeljebb csak $j = 0$ esetén nem 0, és a másik egyenlőség ugyanígy igazolható.

□

3.12. Tétel

$n \in \mathbf{N}$-re az $\mathsf{R} = (R; +, \cdot)$ és $\mathsf{T} = \big(R^n; +, *\big)$ gyűrű egyszerre (bal oldali) egységelemes illetve kommutatív, és T pontosan akkor nullosztómentes, ha $n = 1$ és R nullosztómentes, vagy R nullgyűrű.

Δ

Bizonyítás:

Ha $e^{(b)}$ bal oldali egységelem R-ben, akkor $\overline{e^{(b)}}_j v_{(i-j)^{(n)}}$ csupán $j = 0$ esetén különbözhet nullától, és ekkor az értéke v_i, tehát a konvolúció eredménye az eredeti **v** vektor, $\overline{e^{(b)}}$ balról egységelem. Most tegyük fel, hogy $\boldsymbol{\varepsilon}^{(b)}$ bal oldali egységelem T-ben. Ekkor $\delta_{0,i} v = \bar{v}_i = \big(\boldsymbol{\varepsilon}^{(b)} * \bar{v}\big)_i = \varepsilon_i^{(b)} v$, vagyis $\varepsilon_0^{(b)}$ bal oldali egységelem R-ben.

Kommutatív R esetén $\big(\mathbf{u}*\mathbf{v}\big)_i = \sum_{j=0}^{n-1} u_j v_{(i-j)^{(n)}} = \sum_{j=0}^{n-1} v_{(i-j)^{(n)}} u_j = \sum_{j=0}^{n-1} v_j u_{(i-j)^{(n)}} = \big(\mathbf{v}*\mathbf{u}\big)_i$, mert mialatt a *j* szummációs index 0-tól $n-1$-ig minden értéket egyszer és csak egyszer felvesz, ez alatt $(i-j)^{(n)}$ is ugyanezt teszi, és amikor *v* indexe *j*, akkor *u* indexe $i - j$ modulo *n* maradéka, tehát T is kommutatív. Ha viszont $*$ kommutatív, akkor ez igaz $\overline{\mathsf{R}}$-ben, és így a vele izomorf R-ben is.

Az $n = 1$ illetve $|R| = 1$ eset hasonló a direkt összegnél látottakhoz. Most legyen $n > 1$ és $|R| > 1$, továbbá $a \in R^*$. Ha **u** minden komponense *a*, míg **v** első két komponense *a* és $-a$, a többi 0, akkor a két vektor egyaránt különbözik T nullelemétől, viszont a konvolúciójuk valamennyi komponense 0 lesz, tehát két nem nulla vektor szorzata nulla, az új gyűrű nem nullosztómentes.

□

A bizonyításban $\delta_{0,i} v = \overline{v}_i = \left(\boldsymbol{\varepsilon}^{(b)} * \overline{v}\right)_i = \varepsilon_i^{(b)} v$ biztosan 0, ha $n > i \in \mathbf{N}$, vagyis $i \neq 0$, bármelyik eleme is legyen *v* az R gyűrűnek. Ebből azonban általában nem következik, hogy a nem nulla *i* indexekre $\varepsilon_i^{(b)} = 0$. Legyen $m = u^{t+1} v$, ahol *t* és *v* pozitív egész, míg *u* egynél nagyobb egész szám, és tekintsük az $u\mathbf{Z}_m$ gyűrűt (könnyen ellenőrizhető, hogy ez valóban gyűrű). Ha ennek a gyűrűnek α tetszőleges eleme, akkor $\alpha = u\overline{r} = \overline{ur}$, és $\overline{u^t v} \cdot \alpha = \overline{u^t v} \cdot \overline{ur} = \overline{u^t vur} = \overline{u^{t+1} vr} = \overline{mr} = r\overline{m} = r\overline{0} = \overline{0}$, de $\overline{u^t v} \neq \overline{0}$, vagyis lehet egy nem zérógyűrűnek olyan nem nulla eleme, amellyel a gyűrű bármely elemét szorozva a nullát kapjuk. Általában, ha $\varnothing \neq X \subseteq R$, és *b* a gyűrű olyan eleme, hogy minden $r \in X$ -re $br = 0$, akkor *b* **bal oldali annullátor**a *X*-nek. Hasonlóan definiáljuk a **jobb oldali annullátor**t, és ha a gyűrű egy *a* eleme egyszerre bal és jobb oldali annullátora az *X* halmaznak, akkor *a* **annullátor**a *X*-nek. Az *X* bal oldali annullátorainak *B* halmaza bal oldali ideálja a gyűrűnek, és ha *X* maga is bal oldali ideál, akkor *B* ideálja R-nek. Ha a gyűrűben van jobb oldali egységelem, akkor az *R* olyan részhalmazának, amely tartalmaz legalább egy jobb oldali egységelemet, nem lehet a 0-n kívül más bal oldali annullátora, hiszen ha *b* bal oldali annullátor, és $e^{(j)}$ egy jobb oldali egységelem, akkor $0 = be^{(j)} = b$.

Visszatérve a fenti tételhez, ha R-ben van bal oldali egységelem, és van a nullától különböző bal oldali annullátor is, akkor R egy bal oldali egységeleméhez több különböző bal oldali egységelem tartozik T-ben. Ha viszont R egységelemes, akkor az egyetlen bal oldali annullátor a 0, és így egy és csak egy bal oldali egységelem lesz T-ben, amely egyben egységelem is, nevezetesen *e*, vagyis az az elem, amelynek a nulla indexű komponense R egységeleme, és valamennyi további komponense 0.

3.13. Következmény

Legyen R gyűrű, $n \in \mathbf{N}$, és $r \times_b \mathbf{u} := \overline{r} * \mathbf{u}$, $\mathbf{u} \times_j r := \mathbf{u} * \overline{r}$, ahol $r \in R$ és $\mathbf{u} \in R^n$. Ekkor T kétoldali R modulus, amely akkor és csak akkor unitér, ha R egységelemes, és ez a modulus pontosan akkor algebra, ha R test, és ekkor az algebra rangja *n*.

Δ

Bizonyítás:

$\mathsf{R} \cong \overline{\mathsf{R}} \leq \mathsf{T}$ a $\varphi : r \mapsto \overline{r}$ szabállyal, így a 3.4. Tétel szerint T R-R modulus. T pontosan akkor egységelemes, ha R egységelemes, és ekkor az R *e* egységelemének képe egységelem a T gyűrűben, a modulus unitér. Ha R ferdetest, és része T centrumának, akkor R kommutatív, vagyis test, és algebrát kapunk. Legyen $n > i \in \mathbf{N}_0$-ra $\mathbf{e}^{(i)} \in R^n$ úgy, hogy $e_j^{(i)} = \delta_{i,j} e$, ahol $n > j \in \mathbf{N}_0$. Ekkor $\mathbf{u} \in R^n$-nel $\mathbf{u} = \sum_{i=0}^{n-1} c_i \times_b \mathbf{e}^{(i)}$ akkor és csak akkor teljesül, ha $u_j = \left(\sum_{i=0}^{n-1} c_i \times_b \mathbf{e}^{(i)}\right)_j = \sum_{i=0}^{n-1} \delta_{i,j} c_i = c_j$ minden $n > j \in \mathbf{N}_0$-ra, vagyis $\left\{\mathbf{e}^{(i)} \middle| n > i \in \mathbf{N}_0\right\}$ az $(R; +)$ R fölötti vektortérnek bázisa, így az algebra rangja *n*.

□

3.14. Tétel

Legyen $n \in \mathbf{N}$, K test, továbbá $\mathbf{A}_z^{(K,n)}$ a $\mathsf{K}^{(n)}$ fölötti olyan *n*-edrendű kvadratikus mátrix, amelyben az $n > i \in \mathbf{N}_0$ és $n > j \in \mathbf{N}_0$ indexekre $a_{i,j}^{(z)} = \left(z^{-i}\right)^j$, ahol $z \in E^{(K,n)}$. $\mathbf{A}_z^{(K,n)}$-nek pontosan akkor van inverze, ha $|z| = n$, és ekkor $\mathbf{A}_z^{(K,n)^{-1}} = (ne)^{-1} \mathbf{A}_{z^{-1}}^{(K,n)}$ a test *e* egységelemével.

Δ

Ha nyilvánvaló, hogy melyik testről van szó, és mi az *n* értéke, akkor $\mathbf{A}_z^{(K,n)}$ helyett egyszerűen $\mathbf{A}_z$-t írunk, valamint a továbbiakban $\mathbf{A}_z^{(K,n)}$ mindig a fentebb definiált mátrixot jelöli.

Bizonyítás:

$\mathbf{A}_z$ -ben a 0 indexű sor minden eleme *e*. Ha $t < n$, és *z* *t*-edik egységgyök, akkor $\mathbf{A}_z$ -ben a *t*-edik sor megegyezik a 0. sorral, így a mátrix nem reguláris, tehát biztosan nem invertálható.

Legyen most $t = n$, azaz *z* primitív *n*-edik egységgyök. Ekkor

$$\left(\mathbf{A}_z \cdot \mathbf{A}_{z^{-1}}\right)_{i,k} = \sum_{j=0}^{n-1} a_{i,j}^{(z)} a_{j,k}^{(z^{-1})} = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j \left(z^j\right)^k = \sum_{j=0}^{n-1} \left(z^{k-i}\right)^j = \sum_{j=0}^{n-1} \left(z^{(k-i)^{(n)}}\right)^j .$$

Jelöljük $(k-i)^{(n)}$-et *m*-mel. *i* és *k* korlátjaiból $-(n-1) \le k-i \le n-1$, így *m* akkor és csak akkor 0, ha $i = k$, vagyis $z^m = e$ pontosan akkor teljesül, ha $i = k$, és ekkor az összeg éppen ne. $i \neq k$ esetén $z^m - e \neq 0$, ugyanakkor $\sum_{j=0}^{n-1} \left(z^{(k-i)^{(n)}}\right)^j = \frac{\left(z^m\right)^n - e}{z-e} = 0$, vagyis $\mathbf{A}_z \cdot \mathbf{A}_{z^{-1}}$ főátlójában ne, azon kívül 0 áll, $\mathbf{A}_z \cdot \mathbf{A}_{z^{-1}} = (ne)\mathbf{I}_n$, ahol $\mathbf{I}_n$ a $\mathsf{K}^{(n)}$ fölötti *n*-edrendű egységmátrix. Végül, ha *z* primitív *n*-edik egységgyök, akkor *n* nem osztható a test karakterisztikájával, így ne nem nulla, tehát van inverze, és akkor $\mathbf{A}_z\left((ne)^{-1}\mathbf{A}_{z^{-1}}\right) = \mathbf{I}_n$, ami éppen azt jelenti, hogy $(ne)^{-1}\mathbf{A}_{z^{-1}}$ inverze az eredeti $\mathbf{A}_z$ mátrixnak.

□

Most $\mathbf{A}_z$ segítségével kapcsolatot keresünk a K^n felett korábban konstruált két gyűrű között. Előtte azonban nézzük meg, hogy mi lesz az $\left\{\mathbf{A}_z\mathbf{u} \middle| \mathbf{u} \in K^n\right\}$ halmaz. Legyen először **u** olyan, hogy valamennyi komponense 0, kivéve a 0-indexűt, amely a *K* test egy tetszőleges *c* elemével egyenlő. Ekkor $U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = u_0 = c$, így $K \subseteq \left\{\left(\mathbf{A}_z\mathbf{u}\right)_i \middle| \mathbf{u} \in K^n\right\}$. Másodszor tekintsük azt a vektort, amelynek ismét minden komponense 0, kivéve most az utolsót, az $n-1$ indexhez tartozót, amely ezúttal legyen a test egységeleme, azaz *e*. Ebben az esetben $U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = \left(z^{-i}\right)^{n-1} u_{n-1} = z^i e = z^i$, ami viszont azt mutatja, hogy $z^i \in \left\{\left(\mathbf{A}_z\mathbf{u}\right)_i \middle| \mathbf{u} \in K^n\right\}$, így egy olyan test, amely tartalmazza a képvektorok *i*-indexű komponenseit, biztosan tartalmazza $K\left(z^i\right)$-t. Ugyanakkor ebben a testben bármilyen $\mathbf{u} \in K^n$ esetén benne van $\sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j$, tehát $\mathsf{K}\left(z^i\right)$ a legszűkebb test, amely a képvektorok *i*-indexű komponeseit tartalmazza. Ez igaz $i = 1$ esetén is, és mivel tetszőleges *i* egész szám esetén $K\left(z^i\right) \subseteq K(z)$, ezért minden olyan L testre, amellyel $\left\{\mathbf{A}_z\mathbf{u} \middle| \mathbf{u} \in K^n\right\} \subseteq L^n$, L a $\mathsf{K}(z)$ bővítése, amely lehet éppen $\mathsf{K}(z)$ is.

Most legyen $|z| = m$, ekkor $m \mid n$, továbbá tetszőleges $n > i \in \mathbf{N}_0$ -hoz van olyan egyértelműen meghatározott $m > i_0 \in \mathbf{N}_0$ és $\frac{n}{m} > i_1 \in \mathbf{N}_0$, hogy $i = i_0 + i_1 m$. Ekkor

$$U_{i_0+i_1m} = U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = \sum_{j=0}^{n-1} \left(z^{-(i_0+i_1m)}\right)^j u_j =$$
$$= \sum_{j=0}^{n-1} \left(z^{-i_0}\right)^j \left(\left(z^m\right)^{-i_1}\right)^j u_j = \sum_{j=0}^{n-1} \left(z^{-i_0}\right)^j u_j = U_{i_0}$$

Ebből az eredményből látszik, hogy ha $m < n$, akkor az eredményvektorban az első *m* komponens ismétlődik a további komponensekben. Hasonlóan, minden $n > j \in \mathbf{N}_0$ -hoz létezik egyértelműen meghatározott $m > j_0 \in \mathbf{N}_0$ és $\frac{n}{m} > j_1 \in \mathbf{N}_0$, hogy $j = j_0 + j_1 m$, és így

$$U_{i_0+i_1m}=U_{i_0}=\sum_{j=0}^{n-1}\left(z^{-i_0}\right)^j u_j=$$

$$=\sum_{j_0=0}^{m-1}\sum_{j_1=0}^{\frac{n}{m}-1}\left(z^{-i_0}\right)^{j_0+j_1m}u_{j_0+j_1m}=\sum_{j_0=0}^{m-1}\sum_{j_1=0}^{\frac{n}{m}-1}\left(z^{-i_0}\right)^{j_0}\left(\left(z^m\right)^{-i_0}\right)^{j_1}u_{j_0+j_1m}=$$

$$=\sum_{j_0=0}^{m-1}\sum_{j_1=0}^{\frac{n}{m}-1}\left(z^{-i_0}\right)^{j_0}u_{j_0+j_1m}=\sum_{j_0=0}^{m-1}\left(z^{-i_0}\right)^{j_0}\sum_{j_1=0}^{\frac{n}{m}-1}u_{j_0+j_1m}$$

ami láthatóan megfelel egy *m*-dimenziós vektor transzformációjának, ahol a transzformálandó vektor egy komponense az eredeti vektor $\frac{n}{m}$ darab, egymástól *m* távolságra lévő komponensének az összege.

3.15. Tétel

Legyen $n\in\mathbf{N}$, K test, $z\in E^{(K,n)}$, és $\mathsf{L}\,|\,\mathsf{K}(z)$. Ekkor $\mathbf{u}\overset{\varphi}{\mapsto}\mathbf{A}_z\mathbf{u}$ egy $\varphi:\left(K^n;+,*\right)\to\left(L^n;+,\cdot\right)$ algebrahomomorfizmus, amely pontosan akkor izomorfizmus, ha $|z|=n$, és $L\subseteq K$.

Δ

Bizonyítás:

Azt már a tétel kimondása előtt beláttuk, hogy $\mathrm{Im}(\varphi)\subseteq K(z)^n$, és az is nyilván igaz, hogy K^n minden elemére $\mathbf{A}_z\mathbf{u}$ egyértelműen meghatározott, így φ valóban K^n-nek L^n-be való leképezése.

Nézzük először a művelettartást. $\mathbf{A}_z(a\mathbf{u}+b\mathbf{v})=a(\mathbf{A}_z\mathbf{u})+b(\mathbf{A}_z\mathbf{v})$, ahol *a* és *b* *K*, **u** és **v** K^n elemei, így φ modulushomomorfizmus. Speciális esetként φ összegtartó, és

$$\left(\mathbf{A}_z(\mathbf{u}*\mathbf{v})\right)_i=\sum_{j=0}^{n-1}\left(z^{-i}\right)^j(\mathbf{u}*\mathbf{v})_j=\sum_{j=0}^{n-1}\left(\left(z^{-i}\right)^j\sum_{k=0}^{n-1}u_k v_{(j-k)^{(n)}}\right)=$$

$$=\sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\left(\left(z^{-i}\right)^k u_k\right)\left(\left(z^{-i}\right)^{(j-k)^{(n)}}v_{(j-k)^{(n)}}\right)=$$

$$=\left(\sum_{j=0}^{n-1}\left(z^{-i}\right)^k u_k\right)\left(\sum_{j=0}^{n-1}\left(z^{-i}\right)^j v_j\right)=(\mathbf{A}_z\mathbf{u})_i(\mathbf{A}_z\mathbf{v})_i=\left((\mathbf{A}_z\mathbf{u})\cdot(\mathbf{A}_z\mathbf{v})_i\right)$$

így φ szorzattartó is, tehát a φ leképezés valóban algebrahomomorfizmus.

Legyen $|z|=m$. Izomorfizmushoz szükséges a bijekció, így *L* nem lehet bővebb $K(z)=K^{(m)}$-nél, hiszen láttuk, hogy $\mathrm{Im}(\varphi)\subseteq K(z)^n$. Azt is láttuk, hogy ha $m<n$, akkor a képvektorban lesz legalább két azonos komponens, ezért a képvektorok halmaza nem a teljes $K^{(m)^n}$, a leképezés nem szürjektív, és így nem is izomorfizmus. Ha viszont $m=n$, akkor létezik $\mathbf{A}_z$ inverze. Amennyiben a leképezésünk izomorfizmus, akkor lesz olyan **u** vektor, amelynek a képe az a $\mathbf{v}\in K(z)^n$ vektor, amelyben minden komponens 0, kivéve az $i=1$-hez tartozót, amely *ne*. Ekkor $\mathbf{v}=\mathbf{A}_z\mathbf{u}$, tehát $\mathbf{u}=\mathbf{A}_z^{-1}\mathbf{v}$. De $\mathbf{A}_z^{-1}\mathbf{v}$-ben az $i=1$-hez tartozó komponens *z*, így *K*-nak tartalmaznia kell *z*-t, vagyis izomorfizmushoz szükséges az $L\subseteq K(z)\subseteq K$ feltétel. Most tegyük fel, hogy $m=n$, és $L\subseteq K(z)\subseteq K$. Ekkor *z* primitív *n*-edik egységgyök, $\mathbf{A}_z$-nek van inverze, és $\mathbf{A}_z\mathbf{u}=\mathbf{A}_z\mathbf{v}$-ből $\mathbf{u}=\mathbf{A}_z^{-1}(\mathbf{A}_z\mathbf{u})=\mathbf{A}_z^{-1}(\mathbf{A}_z\mathbf{v})=\mathbf{v}$, a leképezés injektív. Mivel $K\subseteq K(z)$ mindig teljesül, továbbá a tételben tett kikötés szerint $K(z)\subseteq L$, és

most a feltétel szerint $L \subseteq K(z) \subseteq K$, ezért $L = K(z) = K$. Most legyen **w** egy tetszőleges vektor K^n-ből. Ekkor $\mathbf{A}_z^{-1}\mathbf{w} = (ne)^{-1}\mathbf{A}_{z^{-1}}\mathbf{w}$ is benne van K^n-ben, és így $\mathbf{w} = \mathbf{A}_z\left(\mathbf{A}_z^{-1}\mathbf{w}\right)$, a hozzárendelés szürjektív is, és akkor φ bijektív, és a művelettartással együtt izomorfizmus.

□

3.16. Kiegészítés

Ha $z \in K$ primitív *n*-edik egységgyök, akkor $\mathbf{A}_z^{-1}(\mathbf{u} \cdot \mathbf{v}) = \mathbf{A}_z^{-1}(\mathbf{u}) * \mathbf{A}_z^{-1}(\mathbf{v})$.

Δ

Bizonyítás:

Ha *z* primitív *n*-edik egységgyök, akkor létezik $\mathbf{A}_z^{-1}$, és a tételben megadott leképezés bijektív és művelettartó, így a képelemek szorzatának egyértelmű őse a szintén egyértelmű ősök konvolúciója.

□

A továbbiakban általában $\mathbf{A}_z\mathbf{u}$-t **U**, és ha $\mathbf{A}_z$-nek van inverze, akkor $\mathbf{A}_z^{-1}\mathbf{U}$-t **u** jelöli, továbbá ha a K^n-beli **u** vektorra $u^T = (u_0, \ldots, u_{n-2}, u_{n-1})$, akkor $\mathbf{u}_{\rightarrow}$ az $u^T = (u_{n-1}, u_0, \ldots, u_{n-1})$ által meghatározott vektor, $\mathbf{U}^{\rightarrow} := \mathbf{A}_z\mathbf{u}_{\rightarrow}$, és ha *z* primitív *n*-edik egységgyök, akkor $\mathbf{u}^{\rightarrow} := \mathbf{A}_z^{-1}\mathbf{U}_{\rightarrow}$.

3.17. Tétel

Legyen K test, $z \in E^{(K,n)}$ és $\mathbf{u} \in K^n$. Ekkor

1. $\sum_{i=0}^{n-1} u_i = U_0$, és $\sum_{i=0}^{n-1} U_i = nu_0$, ha $|z| = n$.
2. Ha $\mathbf{U} = \mathbf{A}_z\mathbf{u}$, akkor $\left(\mathbf{U}^{\rightarrow}\right)_i = z^{-i}U_i$, és ha $|z| = n$, akkor $\left(\mathbf{u}^{\rightarrow}\right)_i = z^i u_i$.

Δ

Bizonyítás:

1. $\sum_{i=0}^{n-1} u_i = \sum_{i=0}^{n-1}\left(z^{-0}\right)^i u_i = U_0$, ami igazolja az első állítást. Ha viszont *z* primitív *n*-edik egységgyök, akkor $\sum_{i=0}^{n-1} U_i = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j\right) = \sum_{j=0}^{n-1}\left(u_j \sum_{i=0}^{n-1}\left(z^{-j}\right)^i\right) = nu_0$.

2. Közvetlenül látszik, hogy K^n-beli **v** vektorra $(\mathbf{v}_{\rightarrow})_i = v_{(i-1)^n}$. Ebből és a definícióból

$$\left(\mathbf{U}^{\rightarrow}\right)_i = \left(\mathbf{A}_z\, \mathrm{u}_{\rightarrow}\right)_i = \sum_{j=0}^{n-1}\left(z^{-i}\right)^j (\mathbf{u}_{\rightarrow})_j = \sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_{(j-1)^{(n)}} =$$

$$= \sum_{j=0}^{n-1}\left(z^{-i}\right)^{(j+1)} u_j = z^{-i}\sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j = z^{-i}U_i$$

A másik összefüggés igazolása hasonló, figyelembe véve, hogy a megadott feltétellel $ne \neq 0$.

□

Az eddigiekben egy konkrét egységgyökkel végeztük a transzformációt. Kérdés, hogyan változik $\mathbf{A}_z\mathbf{u}$, ha *z* helyett egy másik egységgyököt alkalmazunk. Ez különösen azért fontos kérdés, mert egy absztrakt testben az azonos rendű egységgyökök között semmi különbség nincs, így elvárható, hogy a transzformáció lényegében véve azonos marad, ha egy egységgyök helyett vele azonos rendű egységgyököt alkalmazunk.

3.18. Jelölés

Legyen $n \in \mathbf{N}$, $k \in \mathbf{N}_0$ és $\mathbf{u} \in K^n$. Ekkor az $\mathbf{u}^{(k)} \in K^n$ vektor *i*-indexű komponense, ahol $n > i \in \mathbf{N}_0$, $u_i^{(k)} = \left(\mathbf{u}^{(k)}\right)_i := u_{(ki)^{(n)}}$.

Δ

3.19. Tétel

Tetszőleges egész *k*-ra $\mathbf{A}_{z^k}\mathbf{u} = \left(\mathbf{A}_z\mathbf{u}\right)^{(k)}$, és ha *z* primitív *n*-edik egységgyök, akkor bármely *y* *n*-edik egységgyökhöz van olyan $n > k \in \mathbf{N}_0$, hogy $\mathbf{A}_y\mathbf{u} = \left(\mathbf{A}_z\mathbf{u}\right)^{(k)}$.

Δ

Bizonyítás:
A transzformáció definícióját alkalmazva

$$\left(\mathbf{A}_{z^k}\mathbf{u}\right)_i = \sum_{j=0}^{n-1}\left(\left(z^k\right)^{-i}\right)^j u_j = \sum_{j=0}^{n-1}\left(z^{-ki}\right)^j u_j =$$
$$= \sum_{j=0}^{n-1}\left(z^{-(ki)^{(n)}}\right)^j u_j = \left(A_z\ \mathrm{u}\right)_{(ki)^{(n)}} = \left(\left(A_z\ \mathrm{u}\right)^{(k)}\right)_i .$$

Ha *z* primitív *n*-edik egységgyök, akkor minden *n*-edik egységgyök *z* egy *n*-nél kisebb nem negatív egész kitevős hatványa, így alkalmas $n > k \in \mathbf{N}_0$-val $y = z^k$, és a fenti részből következik a második állítás.

□

3.20. Kiegészítés

Legyen $n \in \mathbf{N}$, és *k* az *n*-hez relatív prím egész. Ekkor $\mathbf{A}_z\mathbf{u}^{(k)} = \left(\mathbf{A}_z\mathbf{u}\right)^{(k')}$, ahol $kk' \equiv 1\ (n)$.

Δ

Bizonyítás:
Ha *k* az *n*-hez relatív prím egész szám, akkor a $kx \equiv 1\ (n)$ kongruencia megoldható, tehát k' létezik, és

$$\left(\mathbf{A}_z\mathbf{u}^{(k)}\right)_i = \sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_{(kj)^{(n)}} = \sum_{j=0}^{n-1}\left(z^{-i}\right)^{(k'j)^{(n)}} u_j =$$
$$= \sum_{j=0}^{n-1}\left(z^{-(k'i)^{(n)}}\right)^j u_j = \left(\mathbf{A}_z\mathbf{u}\right)_{(k'i)^{(n)}} = \left(\left(\mathbf{A}_z\mathbf{u}\right)^{(k')}\right)_i$$

Ez a transzformált vektor minden komponensére igaz, tehát $\mathbf{A}_z\mathbf{u}^{(k)} = \left(\mathbf{A}_z\mathbf{u}\right)^{(k')}$.

□

Amennyiben *k* relatív prím *n*-hez, akkor $n > i \in \mathbf{N}_0$-ra az $i \mapsto (ki)^{(n)}$ szabály az indexek permutációja, így a tétel azt jelenti, hogy különböző primitív *n*-edik egységgyökökkel végezve a leképezést, csupán a kép komponenseinek sorrendje más. Az alábbi következményre jutunk:

3.21. Következmény

Legyen $n \in \mathbf{N}$, és L olyan test, hogy $L^{(n)} \subseteq L$, σ az L automorfizmusa, és K az L legbővebb részteste, amelyen σ az identikus leképezés, $\boldsymbol{\sigma}$ a σ L^n-re való komponensenkénti kiterjesztése, és z primitív n-edik egységgyök. Ekkor van olyan, az n-hez relatív prím, $n > k \in \mathbf{N}_0$, hogy L^n-beli $\mathbf{u}$-ra $\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = \mathbf{A}_{z^k}\boldsymbol{\sigma}(\mathbf{u})$, és $\mathbf{u} \in K^n$ akkor és csak akkor, ha $\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = (\mathbf{A}_z\mathbf{u})^{(k)}$. Ha $\mathsf{L} = \mathbf{C}$ és $\sigma : a \mapsto \overline{a}$, úgy $\mathsf{K} = \mathbf{R}$, és $\mathbf{u} \in \mathbf{R}^n$-hez szükséges és elégséges a $\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = (\mathbf{A}_z\mathbf{u})^{(-1)}$ egyenlőség, míg ha $\mathsf{L} \cong \mathbf{F}_{q^m}$, ahol $m \in \mathbf{N}$, és $\sigma : a \mapsto a^q$, akkor $\mathsf{K} \cong \mathbf{F}_q$, és $\mathbf{u} \in \mathbf{K}^n$ akkor és csak akkor, ha $\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = (\mathbf{A}_z\mathbf{u})^{(q)}$ (**R** a valós, **C** a komplex számok teste, és $\overline{a}$ az a konjugáltja).

Δ

Bizonyítás:

Automorfizmusnál n-edik egységgyök képe n-edik egységgyök, primitív n-edik egységgyöké primitív n-edik egységgyök, így van olyan $n > k \in \mathbf{N}_0$, hogy $\sigma(z) = z^k$ és $(k, n) = 1$. Ekkor

$$(\boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}))_i = \sigma((\mathbf{A}_z\mathbf{u})_i) = \sigma\left(\sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j\right) =$$

$$= \sum_{j=0}^{n-1}\left((\sigma(z))^{-i}\right)^j\left(\sigma(u_j)\right) = \sum_{j=0}^{n-1}\left(\left(z^k\right)^{-i}\right)^j\left(\sigma(u_j)\right) = \left(\mathbf{A}_{z^k}\boldsymbol{\sigma}(\mathbf{u})\right)_i ,$$

és az előző tételből kapjuk az első állítást.

$\mathbf{A}_{z^k}\boldsymbol{\sigma}(\mathbf{u}) = \boldsymbol{\sigma}(\mathbf{A}_z\mathbf{u}) = (\mathbf{A}_z\mathbf{u})^{(k)} = \mathbf{A}_{z^k}\mathbf{u}$ akkor és akkor teljesül, ha $\boldsymbol{\sigma}(\mathbf{u}) = \mathbf{u}$, mert z^k primitív n-edik egységgyök, tehát $\mathbf{A}_{z^k}$ invertálható. Ekkor $\mathbf{u}$ minden komponensére $\sigma(u_i) = u_i$, ami K maximalitásával csak úgy lehetséges, ha $u_i \in K$, de akkor $\mathbf{u} \in K^n$.

Most rátérünk a speciális esetekre. $z \mapsto \overline{z}$ bijektív és műveletartó **C**-n, tehát automorfizmus, és **R** a **C** legbővebb olyan részteste, amelyben a konjugálás az identikus leképezés. z most n-edik komplex egységgyök, tehát $\overline{z} = z^{-1} = z^{n-1}$, ezért $k = n-1$, és $(\mathbf{A}_z\mathbf{u})^{(n-1)} = (\mathbf{A}_z\mathbf{u})^{(-1)}$. A második eset viszont azért igaz, mert q-elemű test bármely bővítésén $a \mapsto a^q$ automorfizmus, és ez z-t z^q-ba viszi, továbbá ez a leképezés pontosan K elemeit hagyja helyben, vagyis K az L-ben foglalt maximális olyan résztest, amelyen a transzformáció megszorítása az identikus leképezés.

□

A speciális esetek jelentését közelebbről is megnézzük. Valós vektor transzformáltjának konjugáltjában a k-adik komponens ugyanaz, mint a transzformált $(-k)^{(n)}$-edik komponense, azaz $\overline{(\mathbf{A}_z\mathbf{u})_k} = (\mathbf{A}_z\mathbf{u})_{(-k)^{(n)}}$. Ebből következik, hogy $(\mathbf{A}_z\mathbf{u})_0$ valós, és $\overline{(\mathbf{A}_z\mathbf{u})_k} = (\mathbf{A}_z\mathbf{u})_{n-k}$ a 0-nál nagyobb k-ra (tehát ha n páros, mondjuk $n = 2m$, akkor az m-edik komponens is valós), ami azt jelenti, hogy csupán $\left\lceil \frac{n+1}{2} \right\rceil$ komponens lehet független (esetleg még ennyi sem). Ez visszafelé is igaz, vagyis ha az $\mathbf{u}$ komplex vektor $\mathbf{U}$ transzformáltjának konjugáltja azonos $\mathbf{U}^{(-1)}$-gyel, akkor $\mathbf{u}$ valós.

A véges testre vonatkozó eset azt jelenti, hogy ha a vektor komponensei a q-elemű testből vannak, akkor a transzformált vektorban a $(qi)^{(n)}$ indexű komponens az i indexhez tartozó komponens q-adik hatványa. Legyen r a legkisebb olyan pozitív egész, amelyre teljesül az $iq^r \equiv i \ (n)$ kongruencia (q és n relatív prímek, mert a test karakterisztikája nem osztója n-nek, így van ilyen r, konkrétan $r = o_{o_n^+(i)}(q)$). Ekkor $(\mathbf{A}_z\mathbf{u})_i$ meghatározza $\mathbf{A}_z\mathbf{u}$ $(q^k i)^{(n)}$-indexű komponenseit, ahol $r > k \in \mathbf{N}_0$.

Visszafelé, ha $\mathbf{A}_z\mathbf{u}$-ban valamennyi $n > i \in \mathbf{N}_0$ indexre teljesül, hogy a $(qi)^{(n)}$ indexű komponens megegyezik $(\mathbf{A}_z\mathbf{u})_i$ q-adik hatványával, akkor **u** a q-elemű K test n-szeres direkt összegéhez tartozó vektor.

3.22. Definíció

Legyen K test, **u** és **v** a K^n két eleme, ahol $n \in \mathbf{N}$. Ekkor **u** és **v** **belső szorzata** vagy **skalárszorzata** $(\mathbf{u},\mathbf{v}) := \sum_{i=0}^{n-1} u_i v_i = \mathbf{u}^T \cdot \mathbf{v}$.

Δ

3.23. Tétel

Legyen K test, n természetes szám, z K feletti primitív n-edik egységgyök, **u** és **v** a K^n két eleme, $\mathbf{w} = \mathbf{uv}$, k az n-hez relatív prím egész, és k' olyan egész, amelyre $kk' \equiv 1 \ (n)$. Ekkor

a. $\left(\mathbf{u} * \mathbf{v}^{(-1)}\right)_0 = (\mathbf{u},\mathbf{v}) = W_0$
b. $\left(\mathbf{u}^{(k)},\mathbf{v}\right) = \left(\mathbf{u},\mathbf{v}^{(k')}\right)$
c. $(\mathbf{U},\mathbf{v}) = (\mathbf{A}_z\mathbf{u},\mathbf{v}) = (\mathbf{u},\mathbf{A}_z\mathbf{v}) = (\mathbf{u},\mathbf{V})$

Δ

Bizonyítás:

a. A definíciókból közvetlenül kapjuk.

b. $\left(\mathbf{u}^{(k)},\mathbf{v}\right) = \sum_{i=0}^{n-1} u_{(ki)^{(n)}} v_i = \sum_{i=0}^{n-1} u_i v_{(k'i)^{(n)}} = \left(\mathbf{u},\mathbf{v}^{(k')}\right)$, hiszen ha k relatív prím az n-hez, akkor mialatt i végigfut 0-tól $n-1$-ig a nemnegatív egész számokon, azalatt ki is pontosan egyszer egyenlő lesz az előbbi elemek egyikével és csak egyikével, és hasonló igaz $k'i$-re, továbbá $i = ((kk')i \mod n)$.

c.

$$(\mathbf{A}_z\mathbf{u},\mathbf{v}) = \sum_{i=0}^{n-1} (\mathbf{A}_z\mathbf{u})_i v_i = \sum_{i=0}^{n-1} \left(\left(\sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j \right) v_i \right) =$$

$$= \sum_{j=0}^{n-1} \left(u_j \left(\sum_{i=0}^{n-1} \left(z^{-j}\right)^i v_i \right) \right) = \sum_{j=0}^{n-1} u_j (\mathbf{A}_z\mathbf{v})_i = (\mathbf{u},\mathbf{A}_z\mathbf{v})$$

□

A tételből következik, hogy $(\mathbf{U},\mathbf{V}) = n\left(\mathbf{u},\mathbf{v}^{(-1)}\right)$, ugyanis

$$(\mathbf{U},\mathbf{V}) = (\mathbf{U},\mathbf{A}_z\mathbf{v}) = (\mathbf{u},\mathbf{A}_z(\mathbf{A}_z\mathbf{v})) = \left(\mathbf{u},\mathbf{A}_z\left(\mathbf{A}_{z^{-1}}\mathbf{v}^{(-1)}\right)\right) =$$
$$= \left(\mathbf{u},\left(\mathbf{A}_z\mathbf{A}_{z^{-1}}\right)\mathbf{v}^{(-1)}\right) = \left(\mathbf{u},n\mathbf{v}^{(-1)}\right) = n\left(\mathbf{u},\mathbf{v}^{(-1)}\right)$$

és ebből speciális esetként kapjuk, hogy $(\mathbf{U},\mathbf{U}) = n\left(\mathbf{u},\mathbf{u}^{(-1)}\right)$.

Legyen $\mathbf{v} = \bar{e}$. Ekkor $\mathbf{V} = \tilde{e}$, és $(\mathbf{U},\mathbf{V}) = \sum_{i=0}^{n-1} U_i$, míg $(\mathbf{u},\mathbf{v}) = u_0$, vagyis $\sum_{i=0}^{n-1} U_i = nu_0$, amint korábban már láttuk.

Test fölötti legfeljebb $n-1$-edfokú polinomok n-dimenziós vektorteret alkotnak az összeadással és a test elemeivel való szorzással. A továbbiakban ezt a tényt alkalmazzuk.

3.24. Jelölés

Legyen $n \in \mathbf{N}$, R tetszőleges gyűrű, és $\mathbf{u} \in R^n$. Ekkor $u^{(\circ)} := \sum_{i=0}^{n-1} u_i x^i$.

Δ

3.25. Tétel

Legyen $n \in \mathbf{N}$, K test, és $\mathbf{u} \in K^n$. Ekkor $U_i = \hat{u}^{(\circ)}\left(z^{-i}\right)$, és ha z primitív n-edik egységgyök, akkor $u_i = (ne)^{-1}\hat{U}^{(\circ)}\left(z^i\right)$.

Δ

Bizonyítás:

$U_i = \sum_{j=0}^{n-1}\left(z^{-i}\right)^j u_j = \sum_{j=0}^{n-1} u_j \left(z^{-i}\right)^j = \hat{u}^{(\circ)}\left(z^{-i}\right)$. Ha z primitív n-edik egységgyök, akkor létezik $\mathbf{A}_z$ inverze, és az előbbihez hasonlóan kapjuk, hogy $u_i = (ne)^{-1}\hat{U}^{(\circ)}\left(z^i\right)$.

□

3.26. Következmény

Legyen $n \in \mathbf{N}$. $U_i = 0$ pontosan akkor igaz, ha $\hat{u}^{(\circ)}\left(z^{-i}\right) = 0$, és $|z| = n$ esetén $u_i = 0$ ekvivalens $\hat{U}^{(\circ)}\left(z^i\right) = 0$ -val.

Δ

Bizonyítás:

Ez az előző tétel közvetlen következménye.

□

A fenti 3.26. Következmény azt az igen fontos tényt mutatja, hogy egy vektor transzformáltjának *i*-edik komponense akkor és csak akkor 0, ha a vektorhoz tartozó polinomnak gyöke z^{-i}, illetve, ha létezik az inverz transzformáció, úgy az eredeti vektorban akkor és csak akkor 0 az *i*-indexű tag, ha a transzformált vektorhoz tartozó polinomnak gyöke z^i. Ezeknek az eredményeknek az alkalmazásokban igen lényeges szerepük van.

3.27. Tétel

Legyen $n \in \mathbf{N}$. Ekkor $\hat{U}^{(\circ)}(0) = \hat{u}^{(\circ)}(e)$ és $U^{\rightarrow(\circ)} = U^{(\circ)} \circ \left(z^{-1}x\right)$, és ha z primitív n-edik egységgyök, akkor $\hat{U}^{(\circ)}(e) = n\hat{u}^{(\circ)}(0)$ és $u^{\rightarrow(\circ)} = u^{(\circ)} \circ (zx)$.

Δ

Bizonyítás:

Tetszőleges $f = \sum_{i=0}^{n} f_i x^i$ polinomra $f_0 = \hat{f}(0)$ és $\hat{f}(e) = \sum_{i=0}^{n} f_i e^i = \sum_{i=0}^{n} f_i$, másrészt $\sum_{i=0}^{n}\left(f_i c^i\right)x^i = \sum_{i=0}^{n} f_i (cx)^i = f \circ (cx)$.

□

Most megvizsgáljuk, hogy mit jelent a ciklikus konvolúció a polinomokkal kapcsolatban.

3.28. Tétel

Legyen $n \in \mathbf{N}$, R egységelemes gyűrű, $\mathbf{u} \in R^n$, $\mathbf{v} \in R^n$, $\mathbf{w} = \mathbf{u} * \mathbf{v}$ és $\mathbf{g} = \mathbf{u} \circ \mathbf{v}$. Ekkor $g^{(\circ)} = u^{(\circ)} v^{(\circ)}$, és $w^{(\circ)} = \left(g^{(\circ)} \mod x^n - e\right)$.

Δ

Bizonyítás:

$g^{(\circ)} = u^{(\circ)} v^{(\circ)}$ legfeljebb $2n-2$-edfokú, tehát egyben legfeljebb $2n-1$-edfokú polinom. Legyen a két polinom $u^{(\circ)} = \sum_{i=0}^{n-1} u_i x^i$ és $v^{(\circ)} = \sum_{i=0}^{n-1} v_i x^i$, akkor írható, hogy $g_i = \sum_{j=0}^{i} u_j v_{i-j}$, ahol $2n > i \in \mathbf{N}_0$, és 0-nál kisebb illetve *n*-nél nem kisebb indexekre az $u^{(\circ)}$ illetve $v^{(\circ)}$ együtthatóit 0-nak tekintjük. Ekkor viszont $g_i = \sum_{j=0}^{i} u_j v_{i-j} = \sum_{j=0}^{2n-1} u_j v_{(i-j)^{(2n)}}$, azaz g_i **u** és **v** lineáris konvolúciójának *i*-edik komponense, így fennáll a $\mathbf{g} = \mathbf{u} \circ \mathbf{v}$ egyenlőség. Ugyanakkor

$$u^{(\circ)} v^{(\circ)} = \sum_{i=0}^{2n-1} g_i x^i = \sum_{i=0}^{n-1} g_i x^i + \sum_{i=n}^{2n-1} g_i x^i = \sum_{i=0}^{n-1} g_i x^i + x^n \sum_{i=0}^{n-1} g_{n+i} x^i = a + x^n b$$

ahol $a = \sum_{i=0}^{n-1} g_i x^i$ és $b = \sum_{i=0}^{n-1} g_{n+i} x^i$. Innen látható, hogy $u^{(\circ)} v^{(\circ)} = a + x^n b = b \cdot \left(x^n - e\right) + (a+b)$, vagyis $w^{(\circ)} = a + b$, és $w^{(\circ)}$ is maximum $n-1$-edfokú polinom, tehát az *n*-nél kisebb *i* indexekre $w_i = a_i + b_i = \left(u^{(\circ)} v^{(\circ)}\right)_i + \left(u^{(\circ)} v^{(\circ)}\right)_{n+i}$. Beírva $g^{(\circ)}$ megfelelő együtthatóit,

$$w_i = \sum_{j=0}^{i} u_j v_{i-j} + \sum_{j=0}^{n+i} u_j v_{(n+i)-j} = \sum_{j=0}^{i} u_j v_{i-j} + \sum_{j=i+1}^{n-1} u_j v_{n+i-j} = \sum_{j=0}^{n-1} u_j v_{(i-j)^{(n)}},$$

ugyanis ha $j \geq n$, akkor $u_j = 0$, és ha $j \leq i$, akkor $v_{(n+i)-j} = 0$, másrészt, ha $n > i \in \mathbf{N}_0$, akkor egyben $i \geq j \in \mathbf{N}_0$-ra $n > i - j \in \mathbf{N}_0$, így $i - j = (i-j)^{(n)}$, és $i+1 \leq j < n$-re $n > n + i - j \in \mathbf{N}_0$, tehát ebben az esetben $n + i - j = (i-j)^{(n)}$. $\sum_{j=0}^{n-1} u_j v_{(i-j)^{(n)}}$ viszont $\mathbf{u} * \mathbf{v}$ *i*-edik komponense.

□

A következő tételben $\mathbf{A}_z$ felhasználásával meghatározzuk, hogy egy *q*-elemű test fölötti polinomnak hány gyöke van a testben.

3.29. Tétel (Kőnig-Rados)

Legyen $f \in \mathbf{F}_q[x]$, $h = x^{q-1} - e \in \mathbf{F}_q[x]$, *h* nem osztója *f*-nek, és $(f,h) = g = \sum_{i=0}^{q-2} g_i x^i$. Ha a $(q-1) \times (q-1)$-es **G** mátrixban a $q-1 > i \in \mathbf{N}_0$ és $q-1 > j \in \mathbf{N}_0$ indexekre $G_{i,j} = g_{(j-i)^{(q-1)}}$, akkor *f* $\mathbf{F}_q$-beli, páronként különböző nem nulla gyökeinek száma $(q-1) - r$, ahol *r* a **G** mátrix rangja.

Δ

Bizonyítás:

Mivel $x^{q-1} - e$-nek a test valamennyi nem nulla eleme gyöke, és más gyöke nem lehet, hiszen az előbbi gyökök száma azonos a polinom fokával, továbbá *g* osztója $x^{q-1} - e$-nek, ezért *g* minden gyöke egyszeres, és benne van $\mathbf{F}_q^*$-ban, ami egyben azt is jelenti, hogy *g* foka megegyezik $\mathbf{F}_q$-beli páronként különböző gyökeinek számával. $f = t \cdot g$, így *g* gyöke egyben *f*-nek is gyöke. De

$g = u \cdot f + v \cdot \left(x^{q-1} - e\right)$ alkalmas $\mathbf{F}_q$ fölötti *u* és *v* polinomokkal, és ha $\alpha \in \mathbf{F}_q^*$ gyöke *f*-nek, akkor $\hat{g}(\alpha) = \hat{u}(\alpha)\hat{f}(\alpha) + \hat{v}(\alpha)\left(\alpha^{q-1} - e\right) = 0$, hiszen α $x^{q-1} - e$-nek is gyöke, tehát $\mathbf{F}_q$ valamely nem nulla eleme akkor és csak akkor gyöke *f*-nek, ha egyben *g*-nek is gyöke, így *f* helyett vizsgálhatjuk *g*-t.

Legyen *z* $\mathbf{F}_q$ primitív eleme. Ekkor a $q-1$-edrendű $\mathbf{A}_z$ reguláris, így **G** és $\mathbf{H} = \mathbf{A}_z\mathbf{G}$ rangja azonos. Erre a **H**-ra

$$H_{i,k} = \sum_{j=0}^{q-2} \left(\mathbf{A}_z\right)_{i,j} G_{j,k} = \sum_{j=0}^{q-2} \left(z^{-i}\right)^j g_{(k-j)^{(q-1)}} =$$
$$= \sum_{j=0}^{q-2} \left(z^{-i}\right)^{k-j} g_j = \left(z^{-i}\right)^k \sum_{j=0}^{q-2} \left(z^i\right)^j g_j = g\left(z^i\right) \cdot \left(z^{-i}\right)^k,$$

vagyis **H**-t úgy kapjuk $\mathbf{A}_z$-ből, hogy ez utóbbi *i*-edik sorának minden elemét megszorozzuk $\hat{g}\left(z^i\right)$-vel. Legyen *g* *t*-edfokú, ahol $q-1 > t \in \mathbf{N}_0$ (*g* nem lehet a nullpolinom, így van foka), és tegyük fel, hogy a gyökök a $0 \le i_0 < \ldots < i_{t-1} < q-1$ kitevőkhöz tartoznak. Ekkor **H** ugyanezen indexű, és csak ezekhez az indexekhez tartozó sorai a nullvektorok. A többi sornak vegyük az első $q-1-t$ elemét. Ezek együttesen **H**-nak egy $(q-1-t)\times(q-1-t)$-szeres részmátrixát alkotják. Ha *D* ennek a mátrixnak a determinánsa, és ennek *u*-adik sora az eredeti mátrixban az i_u indexű sor kezdő szakasza, akkor *D* akkor és csak akkor 0, ha D' is 0, ahol D'-t úgy kapjuk *D*-ből, hogy az *u*-adik sorából kiemeljük a nem nulla $\hat{f}\left(z^{i_u}\right)$-t. A kiemelés után viszont az *u*-adik sor *v*-edik eleme $\left(z^{-i_u}\right)^v$, azaz D' Vandermonde-típusú, és mivel *z* primitív $q-1$-edik egységgyök, és az i_u-k páronként különböző, $q-1$-nél kisebb, nem negatív egészek, ezért $D' \neq 0$. Ez viszont pontosan azt jelenti, hogy a **H** mátrix rangja $q-1-t$, és $(q-1)-r = t$, megegyezésben a gyökök számával.

□

Az előbbi tételnek az a kikötése, hogy *h* ne legyen osztója *f*-nek, nem jelent lényeges megszorítást. Ha ugyanis fennáll az oszthatóság, akkor az éppen azt jelenti, hogy *h* minden $\mathbf{F}_q$-beli gyöke, vagyis $\mathbf{F}_q$ valamennyi eleme gyöke *f*-nek, és akkor természetesen más $\mathbf{F}_q$-beli gyöke nem lehet, vagyis eleve ismerjük *f* összes $\mathbf{F}_q$-beli gyökét.

Az alábbiakban definiáljuk a diszkrét Fourier-transzformációt, és néhány egyéb fogalmat.

3.30. Definíció

Legyen $n \in \mathbf{N}$, és K olyan test, hogy $K^{(n)} \subseteq K$, **u** és **U** K^n elemei, továbbá *z* egy K fölötti primitív *n*-edik egységgyök. Ekkor $\mathbf{A}_z\mathbf{u}$ az **u** (*z*-**vel vett**) **diszkrét Fourier-transzformáltja**, míg $\mathbf{A}_z^{-1}\mathbf{U}$ az **U** (*z*-**vel vett**) **inverz diszkrét Fourier-transzformáltja**, az előbbit $\boldsymbol{F}_z(\mathbf{u})$, az utóbbit $\boldsymbol{F}_z^{-1}(\mathbf{U})$ jelöli. Magát a transzformációt és inverzét **diszkrét Fourier-transzformáció**nak és **inverz diszkrét Fourier-transzformáció**nak mondjuk, és általában **DFT**-nek és **IDFT**-nek rövidítjük.

Amennyiben **U** az **u** diszkrét Fourier-transzformáltja, akkor $U^{(\circ)}$ **az** $u^{(\circ)}$ **polinomhoz tartozó Mattson-Solomon polinom**.

Δ

Mivel a diszkrét Fourier-transzformáció speciális esete az eddig tárgyalt problémáknak, ezért a korábbi tételek alapján összefoglaljuk a diszkrét Fourier-transzformáció és inverzének legfontosabb tulajdonságait:

1. $\boldsymbol{F}_z^{-1}(\boldsymbol{F}_z(\mathbf{u}))=\mathbf{u}$ és $\boldsymbol{F}_z(\boldsymbol{F}_z^{-1}(\mathbf{U}))=\mathbf{U}$
2. $\boldsymbol{F}_z(a\mathbf{u}+b\mathbf{v})=a\boldsymbol{F}_z(\mathbf{u})+b\boldsymbol{F}_z(\mathbf{v})$
3. $\boldsymbol{F}_z(\mathbf{u}*\mathbf{v})=\boldsymbol{F}_z(\mathbf{u})\cdot\boldsymbol{F}_z(\mathbf{v})$ és $\boldsymbol{F}_z(\mathbf{u}\cdot\mathbf{v})=(ne)^{-1}(\boldsymbol{F}_z(\mathbf{u})*\boldsymbol{F}_z(\mathbf{v}))$.

A felsorolt összefüggések közül csupán az első új, ez viszont nyilvánvaló tényt fejez ki, hiszen a definíció alapján $\boldsymbol{F}_z^{-1}(\boldsymbol{F}_z(\mathbf{u}))=\mathbf{A}_z^{-1}(\mathbf{A}_z\mathbf{u})=(\mathbf{A}_z^{-1}\mathbf{A}_z)\mathbf{u}=\mathbf{u}$, és a másik kifejezés ehhez hasonló.

3.31. Megjegyzés

A diszkrét Fourier-transzformáció többek között azt a kapcsolatot fejezi ki, amely szerint egy test feletti legfeljebb $n-1$-edfokú polinomot egyrészt megadhatjuk *n* együtthatójával, másrészt *n* páronként különböző helyen felvett helyettesítési értékével.

Ha megadunk egy polinomot a K test fölött, az egyértelműen meghatározza *K* bármely pontjában a helyettesítési értéket. Legyen $n\in\mathbf{N}$, $\mathbf{f}$ és $\mathbf{g}$ K^n, a és b *K* elemei, $\mathbf{h}=a\mathbf{f}+b\mathbf{g}$ és $\mathbf{w}=\mathbf{f}*\mathbf{g}$, továbbá $t^{(\circ)}=f^{(\circ)}g^{(\circ)}$. Ekkor a K feletti bármely *z* *n*-edik egységgyökkel és $n>i\in\mathbf{N}_0$ egésszel

$$(\mathbf{A}_z(a\mathbf{f}+b\mathbf{g}))_i=(\mathbf{A}_z\mathbf{h})_i=\hat{h}^{(\circ)}(z^{-i})=$$
$$=a\hat{f}^{(\circ)}(z^{-i})+b\hat{g}^{(\circ)}(z^{-i})=a(\mathbf{A}_z\mathbf{f})_i+b(\mathbf{A}_z\mathbf{g})_i$$

$$(\mathbf{A}_z(\mathbf{f}*\mathbf{g}))_i=(\mathbf{A}_z\mathbf{w})_i=\hat{w}^{(\circ)}(z^{-i})=$$
$$=\hat{t}^{(\circ)}(z^{-i})=\hat{f}^{(\circ)}(z^{-i})\hat{g}^{(\circ)}(z^{-i})=(\mathbf{A}_z\mathbf{f})_i\cdot(\mathbf{A}_z\mathbf{g})_i$$

Ha *z* egy *n*-nél kisebb *m*-re primitív *m*-edik egységgyök, akkor az $n>i\in\mathbf{N}_0$-ra vett z^{-i} hatványok száma csak *m*, és *m* helyettesítési érték nem határozza meg az eredeti polinom *n* együtthatóját, ha viszont $m=n$, akkor *n* különböző helyen ismerjük a polinom helyettesítési értékét, és ebből az interpolációs polinom egyértelműsége következtében megkapjuk a polinomot. A diszkrét Fourier-transzformáció tehát többek között azt jelenti, hogy ha egy legfeljebb $n-1$-edfokú polinom helyettesítési értékeit egy primitív *n*-edik egységgyök hatványainál adjuk meg, akkor az interpolációs polinomot egyszerűen egy mátrixszal való szorzás útján is megkapjuk, hiszen ha **U** az a vektor, amelynek *i*-edik komponense $\hat{u}^{(\circ)}(z^{-i})$, akkor a korábbi eredmények alapján $\mathbf{u}=\mathbf{A}_z^{-1}\mathbf{U}$.

Δ

A diszkrét Fourier-transzformált meghatározásához nagyjából n^2 szorzásra és nagyjából ugyanennyi összeadásra van szükség. Létezik olyan algoritmus, amellyel az elvégzendő műveletek száma $n\log n$ nagyságrendű, ezt **gyors Fourier-transzformáció**nak nevezik, jele **FFT**; ezzel majd a következő tétel foglalkozik.

A Fourier-transzformáció lényeges szerepet játszik jelanalízisben, digitális jelfeldolgozásban (**DSP**=**D***igital* **S***ignal* **P***rocessing*), mint például hang és kép feldolgozásában, valamint jelátvivő berendezések vizsgálatában, de például az FFT alkalmazásával sokjegyű számok szorzásának gyors algoritmusa létezik. Egy további konkrét felhasználásával találkozunk bizonyos hibajavító kódok dekódolása során.

3.32. Tétel

Ha $n=n_1n_2$, akkor az *n*-komponensű vektor diszkrét Fourier-transzformációja elvégezhető $n((n_1-1)+(n_2-1))$ nagyságrendű szorzással, és $\max(n_1,n_2)$ tárigénnyel.

Δ

Bizonyítás:

Minden $n > i \in \mathbf{N}_0$ és $n > j \in \mathbf{N}_0$ egyértelműen írható $i = qn_2 + r$ és $j = sn_1 + t$ alakban, ahol $n_1 > q \in \mathbf{N}_0$, $n_2 > r \in \mathbf{N}_0$, $n_2 > s \in \mathbf{N}_0$ és $n_1 > t \in \mathbf{N}_0$. Ekkor

$$U_{qn_2+r} = U_i = \sum_{j=0}^{n-1} \left(z^{-i}\right)^j u_j = \sum_{s=0}^{n_2-1}\sum_{t=0}^{n_1-1} \left(z^{-(qn_2+r)}\right)^{sn_1+t} u_{sn_1+t} =$$

$$= \sum_{t=0}^{n_1-1} \left(\left(z^{n_2}\right)^{-q} z^{-r} \right)^t \sum_{s=0}^{n_2-1} \left(\left(z^{n_1}\right)^{-r} \right)^s u_{sn_1+t} = \sum_{t=0}^{n_1-1} \left(\left(z^{n_2}\right)^{-q} z^{-r} \right)^t \tilde{u}_{rn_1+t} \quad ,$$

ahol $\tilde{u}_{rn_1+t} = \sum_{s=0}^{n_2-1} \left(\left(z^{n_1}\right)^{-r} \right)^s u_{sn_1+t}$. Számítsuk ki egymás után rögzített *t* mellett minden minden *r*-re $\tilde{u}_{rn_1+t}$-t. Ehhez egy-egy adott *t* mellett legfeljebb $n_2(n_2-1)$ szorzás kell, és az eredeti tárolóhelyen túl még n_2 helyre van szükség. Ám a képletből látható, hogy miután az n_2 számú $\tilde{u}_{rn_1+t}$-t kiszámoltuk, a szintén n_2 darab eredeti u_{sn_1+t}-re már nincs szükség, így ezek helyére tehetjük az új $\tilde{u}_{rn_1+t}$ komponenseket. Amikor minden *t*-re meghatároztuk az új komponenseket, akkor az addigi szorzások száma összesen $n_1 n_2 (n_2 - 1)$, és van egy új *n*-méretű vektorunk. Most az előzőhöz hasonlóan rögzített *r*-re kiszámítjuk az n_1 számú *q*-ra az n_1 darab U_{qn_2+r}-t. Ehhez n_1 helyre és $(n_1-1)n_1$, tehát az összes *r*-re számolva $(n_1-1)n_1 n_2$ szorzás kell, így az előbbiekkel együtt összesen körülbelül $n((n_1-1)+(n_2-1))$ szorzást végeztünk.

$n-1 = n_1 n_2 - 1 \geq 2n_1 - 1 > (n_1-1)+(n_1-1) \geq (n_1-1)+(n_2-1)$, ha $n_1 \geq n_2 \geq 2$, azaz ha $n = n_1 n_2$ az *n* valódi felbontása, tehát a fenti algoritmussal kevesebb szorzásra van szükség, mint az eredeti transzformációnál.

□

Az előző eredményből indukcióval kapjuk, hogy ha $n = \prod_{i=0}^{m-1} n_i$, ahol *m* pozitív egész, és a szorzat tényezői egynél nagyobb egész számok, akkor az *n*-dimenziós Fourier-transzformáció elvégezhető $n\sum_{i=0}^{m-1}(n_i - 1)$ szorzással, és a szükséges tárolóhely mérete $\max\{n_i \,|\, m > i \in \mathbf{N}_0\}$, amint az alábbi tétel mutatja.

3.33. Tétel

Legyen K test, $m \in \mathbf{N}$, $\prod_{l=0}^{m-1} n_l = n \in \mathbf{N}$, $m \geq t \in \mathbf{N}_0$-ra $N_t = \prod_{l=0}^{t-1} n_l$ és $N^{(t)} = \prod_{l=m-t}^{m-1} n_l$, továbbá az $n > i^* \in \mathbf{N}_0$ és $n > j \in \mathbf{N}_0$ indexekre $i^* = \sum_{k=0}^{m-1} i_k^* N^{(k)}$ és $j = \sum_{k=0}^{m-1} j_k N_k$, ahol $m > k \in \mathbf{N}_0$-ra $n_{m-1-k} > i_k^* \in \mathbf{N}_0$ és $n_k > j_k \in \mathbf{N}_0$, végül $\mathbf{u} \in K^n$, és $n > j \in \mathbf{N}_0$-ra $u_j^{(m)} = u_j$. Ekkor $m > t \in \mathbf{N}_0$-ra az $u^{(t)}_{J_t + i^*_{m-1-t} N_t + I_{t+1} N_{t+1}} = \sum_{j_t=0}^{n_t-1} \left(\left(z^{\frac{n}{n_t}} \right)^{-i^*_{m-1-t}} \left(z^{N_t}\right)^{-I^{(t+1)}} \right)^{j_t} u^{(t+1)}_{J_t + j_t N_t + I_{t+1} N_{t+1}}$ rekurziós szabállyal $U_{i^*} = u^{(0)}_{\overline{i^*}}$, ahol $J_t = \sum_{k=0}^{t-1} j_k N_k$, $I_t = \sum_{k=t}^{m-1} i_k^* \frac{N_k}{N_t}$, $I^{(t)} = \sum_{k=0}^{m-1-t} i_k^* N^{(k)}$ és $\overline{i^*} = \sum_{k=0}^{m-1} i_k^* N_k$, és a transzformációhoz $n\sum_{i=0}^{m-1}(n_i - 1)$ szorzásra és $\max\{n_i \,|\, m > i \in \mathbf{N}_0\}$ memóriára van szükség.

Δ

Bizonyítás:

Az n_i tényezők a megadott sorrenddel egyértelműen meghatározzák az $i^* = \sum_{k=0}^{m-1} i_k^* N^{(k)}$ és $j = \sum_{k=0}^{m-1} j_k N_k$ felírásban az $n_{m-1-k} > i_k^* \in \mathbf{N}_0$ és $n_k > j_k \in \mathbf{N}_0$ jegyeket. A tételben megadott definíció szerint $U_{i^*} = \sum_{j=0}^{n-1} \left(z^{-i^*}\right)^j u_j = \sum_{j=0}^{n-1} z^{-\left(i^* j\right)} u_j$, és

$$i^* j = \left(\sum_{k=0}^{m-1} i_k^* N^{(k)}\right)\left(\sum_{l=0}^{m-1} j_l N_l\right) = \sum_{l=0}^{m-1}\sum_{k=0}^{m-1} i_k^* j_l N^{(k)} N_l =$$

$$= \sum_{l=0}^{m-1}\sum_{k=0}^{m-1} i_k^* j_l N^{(k)} N_l = \sum_{l=0}^{m-1}\sum_{k=0}^{m-1-l} i_k^* j_l N^{(k)} N_l + n\sum_{l=0}^{m-1}\sum_{k=m-l}^{m-1} i_k^* j_l \frac{N_l}{N_{m-k}} =$$

$$= \sum_{l=0}^{m-1}\left(j_l N_l \sum_{k=0}^{m-1-l} i_k^* N^{(k)}\right) + n\sum_{l=0}^{m-1}\sum_{k=m-l}^{m-1} i_k^* j_l \frac{N_l}{N_{m-k}}$$

Ha most tekintetbe vesszük, hogy z n-edik egységgyök, tehát $z^n = e$, és $z^{r+s} = z^r z^s$, akkor

$$z^{-\left(i^* j\right)} = z^{-\sum_{l=0}^{m-1}\left(j_l N_l \sum_{k=0}^{m-1-l} i_k^* N^{(k)}\right) + n\sum_{l=0}^{m-1}\sum_{k=m-l}^{m-1} i_k^* j_l \frac{N_l}{N_{m-k}}} = z^{-\sum_{l=0}^{m-1}\left(j_l N_l \sum_{k=0}^{m-1-l} i_k^* N^{(k)}\right)} =$$

$$= \prod_{l=0}^{m-1} z^{-j_l N_l \sum_{k=0}^{m-1-l} i_k^* N^{(k)}} = \prod_{l=0}^{m-1}\left(z^{-N_l \sum_{k=0}^{m-1-l} i_k^* N^{(k)}}\right)^{j_l} =$$

$$= \prod_{l=0}^{m-1}\left(z^{-i_{m-1-l}^* \frac{n}{n_l} - N_l \sum_{k=0}^{m-1-(l+1)} i_k^* N^{(k)}}\right)^{j_l} = \prod_{l=0}^{m-1}\left(\left(z^{\frac{n}{n_l}}\right)^{-i_{m-1-l}^*} \left(z^{N_l}\right)^{-\sum_{k=0}^{m-1-(l+1)} i_k^* N^{(k)}}\right)^{j_l}$$

vagyis

$$U_{\sum_{k=0}^{m-1} i_k^* N^{(k)}} = U_{i^*} = \sum_{j=0}^{n-1}\left(z^{-i^*}\right)^j u_j =$$

$$= \sum_{j_0=0}^{n_0-1}\cdots\sum_{j_l=0}^{n_l-1}\cdots\sum_{j_{m-1}=0}^{n_{m-1}}\prod_{l=0}^{m-1}\left(\left(z^{\frac{n}{n_l}}\right)^{-i_{m-1-l}^*} \left(z^{N_l}\right)^{-\sum_{k=0}^{m-1-(l+1)} i_k^* N^{(k)}}\right)^{j_l} u_{\sum_{l=0}^{m-1} j_l N_l} =$$

$$= \sum_{j_0=0}^{n_0-1}\left(\left(z^{\frac{n}{n_0}}\right)^{-i_{m-1}^*} \left(z^{N_0}\right)^{-\sum_{k=0}^{m-2} i_k^* N^{(k)}}\right)^{j_0} \cdots \sum_{j_l=0}^{n_l-1}\left(\left(z^{\frac{n}{n_l}}\right)^{-i_{m-1-l}^*} \left(z^{N_l}\right)^{-\sum_{k=0}^{m-1-(l+1)} i_k^* N^{(k)}}\right)^{j_l} \cdots \sum_{j_{m-1}=0}^{n_{m-1}}\left(\left(z^{\frac{n}{n_{m-1}}}\right)^{-i_0^*}\right)^{j_{m-1}} u_{\sum_{l=0}^{m-1} j_l N_l}$$

Az utolsó sorban álló kifejezésből a rekurzió közvetlenül leolvasható. Most meghatározzuk a rekurzió egy-egy lépésében elvégzett szorzások számát, valamint az algoritmushoz szükséges minimális memória méretét. $u^{(t)}_{J_t + i_{m-1-t}^* N_t + I_{t+1} N_{t+1}} = \sum_{j_t=0}^{n_t-1}\left(\left(z^{\frac{n}{n_t}}\right)^{-i_{m-1-t}^*} \left(z^{N_t}\right)^{-I^{(t+1)}}\right)^{j_t} u^{(t+1)}_{J_t + j_t N_t + I_{t+1} N_{t+1}}$ kiszámítását végezzük úgy, hogy rögzített J_t és I_{t+1} mellett egymás után mindenegyes $n_t > i_{m-1-t}^* \in \mathbf{N}_0$-ra meghatá-

rozzuk $\tilde{u}_{i^*_{m-1-t}} = \sum_{j_t=0}^{n_t-1}\left(\left(z^{\frac{n}{n_t}}\right)^{-i^*_{m-1-t}}\left(z^{N_t}\right)^{-I^{(t+1)}}\right)^{j_t} u^{(t+1)}_{J_t+j_tN_t+I_{t+1}N_{t+1}}$ értékét. Egy-egy ilyen komponens kiszámításhoz n_t-1 szorzás, tehát valamennyi i^*_{m-1-t}-re együttesen $n_t(n_t-1)$ szorzás kell, és amikor minden i^*_{m-1-t}-re meghatároztuk $\tilde{u}_{i^*_{m-1-t}}$-t, akkor többé már nincs szükség az $u^{(t+1)}_{J_t+j_tN_t+I_{t+1}N_{t+1}}$ komponensekre, tehát $u^{(t+1)}_{J_t+j_tN_t+I_{t+1}N_{t+1}}$ helyére beírható $\tilde{u}_{i^*_{m-1-t}}$. Ez utóbbiból következik, hogy a szükséges memória az n_i faktorok maximuma. Mivel J_t és I_{t+1} együtt összesen $\frac{n}{n_t}$ különböző értéket vehet fel, ezért a rekurzió *t*-hez tartozó fordulójában az elvégzett szorzások száma $\frac{n}{n_t}n_t(n_t-1)=n(n_t-1)$, innen pedig kiadódik, hogy a teljes transzformáció elvégzéséhez $n\sum_{l=0}^{m-1}(n_l-1)$ szorzásra van szükség.

□

A tételből következik, hogy ha *n* a *k* darab – nem feltétlenül különböző – p_i prím szorzata, akkor a diszkrét Fourier-transzformáció elvégezhető $n\sum_{i=0}^{k-1}(p_i-1)$ szorzással, és a szükséges tároló mérete $\max\{p_i \mid k \geq i \in \mathbf{N}\}$. Ha $n=p^k$, akkor a szükséges szorzások száma $kn(p-1)=(p-1)n\log_p n$, és a többletmemória nagysága *p*, így a futási idő $\frac{n}{(p-1)\log_p n}$-szeres faktorral csökken, és ennek csupán egy *p*-méretű többletmemória az ára. $p=2$ esetén a szorzások száma $n\log_2 n$, és ez már viszonylag kis *k* esetén is lényegesen kisebb, mint $n(n-1)$. Például $k=10$ mellett $n=1024$, így az arány kisebb, mint 1 százalék (10 az 1023-hoz).

A gyors Fourier-transzformáció lehetővé teszi a konvolúció gyors kiszámítását is. Egy korábbi tétel alapján $\mathbf{u}*\mathbf{v}=\boldsymbol{F}_z^{-1}(\boldsymbol{F}_z(\mathbf{u})\boldsymbol{F}_z(\mathbf{v}))$. A bal oldal meghatározásához nagyságrendileg n^2 szorzás kell, míg a jobb oldal kiszámításához körülbelül $3n\sum_{i=0}^{m-1}(n_i-1)+n=n\left(3\sum_{i=0}^{m-1}(n_i-1)+1\right)$ szorzásra van szükség, amely $3\sum_{i=0}^{m-1}(n_i-1)<n-1$ esetén n^2-nél kisebb. A $t=\prod_{i=0}^{m-1}n_i-3\sum_{i=0}^{m-1}(n_i-1)$ jelöléssel a kérdés az, hogy mikor teljesül a $t>1$ feltétel.

Ha $m=1$, akkor $t=-2n+3$, és ez minden pozitív egész *n*-re legfeljebb 1. A továbbiakban tegyük fel, hogy az n_i faktorok mindegyike legalább 2, és a szorzat legalább két faktort tartalmaz.

Ha $\prod_{i=0}^{m-1}n_i-3\sum_{i=0}^{m-1}(n_i-1)$-ben bármely $m>k\in\mathbf{N}_0$-ra n_k-t eggyel megnöveljük, akkor *t* értéke $\prod_{\substack{i=0\\ i\neq k}}^{m-1}n_i-3$-mal nő, és ez $m\geq 3$, illetve $m=2$ és $n_0>3$, $n_1>3$ esetén biztosan pozitív, vagyis ilyen feltételek mellett *t* értéke minden n_k-ban szigorúan monoton nő. Amennyiben minden tényező értéke 2, akkor $t=\prod_{i=0}^{m-1}n_i-3\sum_{i=0}^{m-1}(n_i-1)=2^m-3m$, és ez $m\geq 3$ esetén *m*-nek szigorúan monoton növekvő függvénye, ugyanis ekkor $\left(2^{m+1}-3(m+1)\right)-\left(2^m-3m\right)=2^3\cdot 2^{m-3}-3\geq 2^3-3=5>0$. Mivel $2^4-3\cdot 4$ nagyobb 1-nél, ezért minden olyan esetben, amikor *n* legalább négy nem triviális tényező szorzata, akkor $t>1$, vagyis $m\geq 4$ esetén a gyors Fourier-transzformációval a konvolúció gyorsítható. Háromtényezős szorzat esetén $2^3-3\cdot 3=-1\leq 1$, de $3^3-3\cdot 3\cdot 2=9>1$, vagyis ha mindhárom tényező 2, akkor még jobb az eredeti konvolúció, de ha már mindhárom faktor 3, akkor célszerűbb a

közvetett módon történő számítás. Mivel $2^2 \cdot 3 - 3(2 \cdot 1 + 2) = 0 \le 1 < 3 = 2 \cdot 3^2 - 3(1 + 2 \cdot 2)$, ezért már akkor is az FFT-vel történő konvolúció a gyorsabb, ha a három tényező közül legalább kettő értéke minimum 3, de ha két tényező értéke 2, és a harmadiké 3, akkor még a hagyományos számítást érdemes elvégezni. $2^2 \cdot 4 - 3(2 \cdot 1 + 3) = 1 \le 1 < 2 = 2^2 \cdot 5 - 3(2 \cdot 1 + 4)$, ami viszont azt mutatja, hogy ha két tényező a lehető legkisebb, akkor a harmadik tényező nagyobb kell, hogy legyen négynél ahhoz, hogy a gyors Fourier-transzformáció gyorsabb konvolúciót eredményezzen.

Legyen végül $m = 2$. Ekkor $\prod_{i=0}^{m-1} n_i - 3\sum_{i=0}^{m-1}(n_i - 1) = (n_0 - 3)(n_1 - 3) - 3$, és ez akkor és csak akkor nagyobb egynél, ha az egyik tényező legalább 5, és a másik minimum 6, vagy az egyik tényező 4, és a másik 7-nél nagyobb.

Összefoglalva, ha *n* szorzatfelírásában legalább négy tényező szerepel, vagy három faktor van, és vagy a legnagyobb minimum 5, vagy legalább kettő 3, vagy a kéttényezős szorzatban vagy az egyik tényező legalább 5, és a másik minimum 6, vagy a kisebbik faktor 4, és a nagyobbik nem kisebb 8-nál, akkor a gyors Fourier-transzformáció alkalmazásával a konvolúció gyorsítható. Ha az előbbi esetek egyike sem teljesül, akkor a közvetlen konvolúció legalább olyan jó, mint az FFT-vel végrehajtott konvolúció.

A fenti gondolatoknál mindenütt a szorzások számát becsültük, de a szükséges összeadások, valamint értékadások száma is hasonló nagyságrendű, és a szorzás időigénye általában lényegesen meghaladja a másik két művelet elvégzéséhez szükséges időt.

4. Polinomok rendje

4.1. Tétel

Ha $f \in \mathbf{F}_q[x]$, $\deg(f) = m$, ahol $m \in \mathbf{N}$ és $\hat{f}(0) \neq 0$, akkor van olyan $q^m - 1 \geq r \in \mathbf{N}$ egész, hogy $f \mid x^r - e$.

Δ

Bizonyítás:

$\mathbf{F}_q[x]/(f)$ nullától különböző elemeinek száma $q^m - 1$. Mivel $\hat{f}(0) \neq 0$, ezért *x* nem osztója *f*-nek, *x* irreducibilis polinom $\mathbf{F}_q$ fölött, tehát *x* és *f*, következésképpen tetszőleges $i \in \mathbf{N}_0$-ra x^i és *f* relatív prímek, így $x^i \not\equiv 0 \ (f)$, $\mathbf{F}_q[x]/(f)$ x^i-vel reprezentált osztálya nem a nullelem a maradékosztálygyűrűben. Ha $q^m - 1 \geq i \in \mathbf{N}_0$, akkor az ilyen kitevőjű *x*-hatványok száma q^m, több, mint a nem nulla elemek száma, ezért kell, hogy legyen legalább egy olyan *i* és *j* egész számpár, hogy $q^m - 1 \geq j > i \in \mathbf{N}_0$, és amelyre $x^i \equiv x^j \ (f)$, vagyis amelyre $f \mid x^j - x^i = x^i\left(x^{j-i} - e\right)$ teljesül. Mivel x^i és *f* relatív prímek, ezért $f \mid x^{j-i} - e$, és a korlátokat figyelembe véve $q^m - 1 \geq j - i \in \mathbf{N}$.

□

4.2. Definíció

Legyen $f = x^i g \in \mathbf{F}_q[x]$, ahol $i \in \mathbf{N}_0$ és $\hat{g}(0) \neq 0$, továbbá $u := \min\left\{k \in \mathbf{N} \,\middle|\, g \mid x^k - e\right\}$. Ekkor *u* az *f* **polinom rendje**, **periódusa** vagy **exponense**, jele $o(f)$.

Δ

4.3. Tétel

Tetszőleges $0 \neq f \in \mathbf{F}_q[x]$ polinomnak van egyértelműen meghatározott rendje. Ha $f = x^i g$, ahol $i \in \mathbf{N}_0$, akkor $o(f) = o(g)$, és ha $\hat{g}(0) \neq 0$ valamint $\deg(g) = m$, akkor $r \geq o(f) \in \mathbf{N}$, ahol $r = \max\{1, q^m - 1\}$.

Δ

Bizonyítás:

Az $\mathbf{F}_q[x]$-beli tetszőleges nem nulla polinom felírható $x^i g$ alakban alkalmas nem negatív egész *i*-vel és $\mathbf{F}_q$ fölötti *g* polinommal, amelyre $\hat{g}(0) \neq 0$. Az első tétel szerint van olyan pozitív egész *r*, amelyre *g* osztója az $x^r - e$ polinomnak, ezért a definícióban megadott halmaz a természetes számok halmazának nem üres részhalmaza, amelyben **N** jólrendezettsége folytán van egyértelműen meghatározott legkisebb elem, így *f*-nek van egyértelmű rendje. A következő állítás a definíció közvetlen következménye, az utolsó pedig a definíciónak és az első tételnek azzal a kiegészítéssel, hogy amennyiben *g* egy nem nulla konstans polinom, akkor a foka 0, viszont a rend definíciójában pozitív egészek minimuma áll, és a test tetszőleges nem nulla eleme osztója az $x - e$ polinomnak, ekkor tehát a rend 1.

□

4.4. Tétel

Legyen $f \in \mathbf{F}_q[x]$, és $\hat{f}(0) \neq 0$. Ekkor $f \mid x^c - e$, ahol $c \in \mathbf{N}$, akkor és csak akkor teljesül, ha $o(f) \mid c$.

Δ

Bizonyítás:

$\hat{f}(0) \neq 0$-t azért kell kikötni, mert ellenkező esetben vagy $f = 0$, és így $o(f)$ nem definiált, vagy nem lehet osztója $x^c - e$-nek egyetlen pozitív egész *c*-re sem. Legyen $o(f) = r$. Ha $r \mid c$, akkor $c = sr$ egy pozitív egész *s*-sel, és $x^r - e$ osztója $x^c - e = (x^r)^s - e^s$-nek, így *f* is osztója $x^c - e$-nek. Fordítva, legyen *f* osztója $x^c - e$-nek, és legyen $c = ur + s$, ahol *u* egész szám, és $r > s \in \mathbf{N}_0$, ekkor $x^c - e = x^{ur+s} - e = x^s(x^{ur} - e) + (x^s - e)$. Mivel a feltétel szerint *f* osztója a bal oldalnak, továbbá éppen most bizonyítottuk, hogy az első zárójelben álló kifejezésnek, tehát a jobb oldal első tagjának is, ezért osztója $x^s - e$-nek is, de ez $s < r$ miatt csak $s = 0$ esetén lehet, tehát *r* osztója *c*-nek.

□

4.5. Tétel

Ha *f* egy *m*-edfokú irreducibilis polinom a *q*-elemű test fölött, $\hat{f}(0) \neq 0$, és α az *f* egy gyöke a felbontási testben, akkor *f* rendje megegyezik α rendjével a q^m-elemű test multiplikatív csoportjában.

Δ

Bizonyítás:

$\hat{f}(0) \neq 0$ biztosítja, hogy $\alpha \neq 0$, ezért van olyan pozitív egész *i* kitevő, amellyel $\alpha^i = e$. Legyen *f* rendje *r*, α multiplikatív rendje *s*. $\alpha^s = e$ következtében α gyöke az $x^s - e$ polinomnak, tehát $f \mid x^s - e$, így az előző tétel szerint $r \mid s$. Másrészről $f \mid x^r - e$ maga után vonja, hogy α gyöke az $x^r - e$ polinomnak, így $\alpha^r - e = 0$, azaz $\alpha^r = e$, ami pedig akkor és csak akkor teljesül, ha $s \mid r$. Mivel *r* és *s* egyaránt pozitív egész, a kölcsönös oszthatóság pontosan azt jelenti, hogy $r = s$.

□

4.6. Következmény

A *p*-karakterisztikájú $\mathbf{F}_q$ fölött irreducibilis, *m*-edfokú *f* polinomra $r \mid q^m - 1$, és $(r, p) = 1$, ahol $r = o(f)$.

Δ

Bizonyítás:

$\hat{f}(0) = 0$ az irreducibilitás miatt csupán $f = cx$ esetén lehetséges, ahol $c \in \mathrm{F}_q^*$. Ekkor $r = 1$, és 1 minden egésznek osztója, és minden egészhez relatív prím. *f* $\mathbf{F}_q$ fölötti felbontási teste $\mathbf{F}_{q^m}$, ezért $f \mid x^{q^m} - x$, és ha $\hat{f}(0) \neq 0$, akkor $f \mid x^{q^m-1} - e$, innen pedig $r \mid q^m - 1$, tehát most is teljesül az oszthatóság. De $q = p^n$ egy *n* pozitív egésszel, ezért $q^m - 1$ relatív prím *p*-hez, de akkor $q^m - 1$ minden osztója is relatív prím *p*-hez.

□

4.7. Tétel

Az $\mathbf{F}_q$ fölötti normált *m*-edfokú, *r*-edrendű irreducibilis polinomok száma $r \geq 2$ és $m = o_r(q)$ esetén $\varphi(r)/m$, $m = 1 = r$ mellett 2, egyébként 0.

Δ

Normált polinom a főpolinom más megnevezése, azaz olyan polinom, amelynek főegyütthatója, vagyis legmagasabb fokú tagjának együtthatója a test (vagy gyűrű) egységeleme.

Bizonyítás:

Legyen *f* tetszőleges nem nulla polinom, akkor ez egyértelműen írható $x^i g$ alakban nem negatív egész *i*-vel és olyan *g*-vel, amelyre $\hat{g}(0) \neq 0$. Amennyiben *f* irreducibilis, akkor ez csak úgy lehet, ha $i = 1$ és $g = c \neq 0$ egy $\mathbf{F}_q$-beli nem nulla *c*-vel , vagy $i = 0$, tehát $f = g$, $\hat{f}(0) \neq 0$, és $\deg(f) \geq 1$. $\hat{f}(0) \neq 0$ és $\deg(f) > 1$ esetén *f* rendje legalább 2, hiszen legalább másodfokú polinom nem lehet osztója $x - e$-nek, ezért elsőrendű polinom nem lehet elsőfokúnál magasabb fokú. Konstans polinom nem irreducibilis, így $o(f) = 1$ irreducibilis polinommal csak $\deg(f) = 1$ esetén lehetséges. Minden elsőfokú polinom irreducibilis; az elsőfokú normált polinomok $x - c$ alakúak, ahol *c* a test tetszőleges eleme. Ha $c = 0$, akkor $f = x$, és *x* rendje 1, és ekkor $m = 1 = r$. $x - e = e(x - c) + (c - e)$, ezért $x - e$ akkor és csak akkor osztható $x - c$-vel, ha $c = e$, és így $x - e$ az egyetlen olyan polinom, amelyre $r = 1$ és $\hat{f}(0) \neq 0$, ezért $r = 1$ csak $m = 1$ mellett lehetséges irreducibilis normált polinomokkal, és ilyen tényleg 2 van (mármint olyan irreducibilis normált polinom, amelynek a rendje 1). A továbbiakban legyen $r \geq 2$. Ha *f* egy *r*-edrendű irreducibilis főpolinom, akkor bármely α gyöke $\mathbf{F}_q$ fölötti primitív *r*-edik egységgyök, *f* osztója az $\mathbf{F}_q$ fölötti *r*-edik körosztási polinomnak, és fordítva, ezen körosztási polinom minden irreducibilis főpolinom osztója egy $\mathbf{F}_q[x]$-beli *r*-edrendű normált irreducibilis polinom. Ezek foka egységesen $m = o_r(q)$, és a számuk $\varphi(r)/m$, ugyanakkor, ha egy 2-nél nem kisebb *r* természetes számra $m \neq o_r(q)$, akkor látjuk, hogy nincs olyan $\mathbf{F}_q$ fölötti polinom, amelynek rendje *r* és a foka *m*.

□

4.8. Tétel

Ha *g* a *p* karakterisztikájú $\mathbf{F}_q$ test fölötti irreducibilis polinom, $\hat{g}(0) \neq 0$, és $f = g^n$, ahol *n* egy pozitív egész szám, továbbá *t* olyan egész szám, hogy $p^{t-1} < n \leq p^t$, akkor $o(f) = p^t o(g)$.

Δ

Bizonyítás:

Az nyilvánvaló, hogy $t \geq 0$, hiszen $p > 1$ miatt $p^{-1} < 1 \leq n$. Legyen $o(g) = v$ és $o(f) = u$. $\hat{g}(0) \neq 0$-ból következik, hogy $\hat{f}(0) \neq 0$, tehát $f \mid x^u - e$. Mivel $g \mid f$, ezért $g \mid x^u - e$, amiből következik, hogy $v \mid u$. $f = g^n \mid (x^v - e)^n \mid (x^v - e)^{p^t} = x^{vp^t} - e$, ezért $u \mid vp^t$, és ez $v \mid u$-val azt adja, hogy $u = vp^s$ egy $t \geq s \in \mathbf{N}_0$ egésszel. Mivel *g* irreducibilis, ezért $(v, p) = 1$, ennél fogva $x^v - e$ gyökei egyszeresek, de akkor $x^u - e = (x^v - e)^{p^s}$ mindenegyes gyöke pontosan p^s-szeres. Mivel g^n osztója $x^u - e$-nek, ezért $x^u - e$ gyökei legalább *n*-szeresek, tehát $n \leq p^s$, ami *t* választása folytán azonos a $t \leq s$ feltétellel, így a korábbi egyenlőtlenséggel együtt $s = t$, és $u = p^t v$.

□

4.9. Tétel

Ha g_1, ..., g_s nem nulla polinomok a *q*-elemű test fölött, és $s \geq i \in \mathbf{N}$-re $\hat{g}_i(0) \neq 0$, akkor legkisebb közös többszörösük rendje megegyezik a rendek legkisebb közös többszörösével.

Δ

Bizonyítás:

Legyen $o(g_i) = n_i$, a polinomok legkisebb közös többszöröse *g*, ennek rendje *n*, és a rendek legkisebb közös többszöröse *t*. Ekkor valamennyi lehetséges *i* indexre $n_i \mid t$, és akkor $g_i \mid x^t - e$, így $g \mid x^t - e$, és $n \mid t$. Viszont megint minden $s \geq i \in \mathbf{N}$-re $g_i \mid g \mid x^n - e$, ahonnan az $n_i \mid n$ oszthatóságot, ebből pedig a $t \mid n$ oszthatóságot kapjuk, és *t* és *n* pozitív egész, tehát $t = n$.

□

4.10. Következmény

Ha g_1, ..., g_s páronként relatív prím nem nulla polinomok a *q*-elemű test fölött, és *g* szorzatukra $\hat{g}(0) \neq 0$, akkor *g* rendje megegyezik a g_i-k rendjének legkisebb közös többszörösével.

Δ

Bizonyítás:

$\hat{g}(0) \neq 0$-ból $\hat{g}_i(0) \neq 0$, és relatív prímek legkisebb közös többszöröse a szorzatuk.

□

4.11. Tétel

Ha $char(\mathbf{F}_q) = p$, és $f = ax^k \prod_{i=1}^{s} f_i^{n_i}$ az $\mathbf{F}_q$ fölötti $f \neq 0$ polinom kanonikus alakja, akkor $o(f) = p^t r$, ahol $t \in \mathbf{Z}$-re $p^{t-1} < \max\{n_i \mid s \geq i \in \mathbf{N}\}$, és *r* az $o(f_i) = r_i$-k legkisebb közös többszöröse.

Δ

Bizonyítás:

t-ről tudjuk, hogy nem negatív egész. $a \in \mathbf{F}_q^*$, ezért egység $\mathbf{F}_q[x]$-ben, tehát $a^{-1} f$ és *f* ugyanazon polinomok osztói, így a rendjük megegyezik, továbbá a rend nem függ x^k-tól sem. Az f_i-k páronként relatív prímek, a hatványaik is azok, továbbá a 0 nem gyökük, ezért a szorzatuk rendje megegyezik a rendjeik legkisebb közös többszörösével. Mindegyik rend *p* egy hatványának és a megfelelő f_i rendjének a szorzata. Ez utóbbi relatív prím *p*-hez, így a legkisebb közös többszörös *p* maximális kitevőjű hatványának és az f_i-k rendje legkisebb közös többszörösének szorzata, a *p* kitevője viszont a polinom kitevőjének monoton növekvő függvénye.

□

4.12. Tétel

Nem nulla polinom rendje megegyezik reciprokának rendjével.

Δ

Bizonyítás:

Legyen $f = x^i g$, ahol $i \in \mathbf{N}_0$ és $\hat{g}(0) \neq 0$. Ekkor $f^* = g^*$ és $o(f) = o(g)$, így elég azt belátni, hogy *g* és g^* rendje azonos. Ha *g* rendje *r*, akkor $g \mid x^r - e$, azaz $x^r - e = ug$ egy *u* polinommal, és

innen $u^* g^* = (ug)^* = \left(x^r - e\right)^* = e - x^r = -e\left(x^r - e\right)$, tehát g^* osztja $x^r - e$-t, és így g^* rendje, r^* is osztója *r*-nek. Hasonlóan kapjuk, hogy $\left(g^*\right)^*$ rendje osztója r^*-nak, és mivel $\left(g^*\right)^* = g$, ezért $r \mid r^*$, vagyis *r* és r^* kölcsönösen osztják egymást, ami pozitív egészek esetén csak egyenlőséggel lehetséges, márpedig *r* és r^* egyaránt pozitív egész, így $r = r^*$.

□

4.13. Definíció

Ha *f* az F_{q^m} egy primitív elemének $\mathbf{F}_q$ fölötti minimálpolinomja, akkor *f* **primitív polinom $\mathbf{F}_q$ fölött**.

Δ

4.14. Tétel

Az $\mathbf{F}_q[x]$-beli *m*-edfokú *f* főpolinom rendje pontosan akkor $q^m - 1$, ha $q = 2$ és $f = x$, vagy *f* primitív polinom $\mathbf{F}_q$ fölött.

Δ

Bizonyítás:

Ha $q = 2$ és $f = x$, akkor $o(f) = 1$ és $m = 1$, vagyis $q^m - 1 = 1$, míg *m*-edfokú primitív polinom egyben *m*-edfokú irreducibilis polinom is, így a rendje megegyezik bármely gyökének rendjével, amely a definíció alapján $q^m - 1$, hiszen a gyök a test primitív eleme.

Nézzük a fordított irányt. Nem nulla konstans polinom esetén $m = 0$ és $o(f) = 1 \neq 0 = q^m - 1$. Legyen a továbbiakban $f = x^k g$, ahol $k \in \mathbf{N}_0$ és $\hat{g}(0) \neq 0$, és legyen $m \in \mathbf{N}$. Amennyiben $k = m$, akkor $o(f) = o(g) = 1 < q^m - 1$, kivéve, ha $q = 2$ és $m = 1$, vagyis amikor *f* a kételemű test fölötti polinom, és $f = x$. Hasonlóan kapjuk, hogy $m > k \in \mathbf{N}$ esetén $o(f) = o(g) \leq q^{m-k} - 1 < q^m - 1$, ezért a továbbiakban feltesszük, hogy $k = 0$. Ha $f = f_1 f_2$, ahol f_1 foka $m > m_1$, f_2 foka $m > m_2$, és a két polinom relatív prím, akkor

$$o(f) = [o(f_1), o(f_2)] \leq o(f_1) o(f_2) \leq$$
$$\leq \left(q^{m_1} - 1\right)\left(q^{m_2} - 1\right) < \left(q^{m_1} - 1\right) q^{m_2} = q^{m_1 + m_2} - q^{m_2} = q^m - q^{m_2} \leq q^m - 2 < q^m - 1,$$

míg ha *f* egy *g* irreducibilis, a nullában nem 0 polinom *r*-edik hatványa, ahol $1 < r \in \mathbf{N}$, és *p* a test karakterisztikája, akkor $p \mid o(f) \leq q^m - 1$, ám *p* nem osztója $q^m - 1$-nek, így *f* rendje ismét kisebb, mint $q^m - 1$. Végül, ha *f* irreducibilis, de nem primitív, akkor a rendje a gyökének a q^m-elemű testbeli rendjével azonos, ami ismét kisebb, mint $q^m - 1$, hiszen ez a gyök nem primitív elem.

□

5. Elem nyoma

5.1. Definíció

Legyen L a *q*-elemű K test *m*-edfokú bővítése, és $\alpha \in L$. Ekkor $\sum_{i=0}^{m-1} \alpha^{q^i}$ az α K **feletti nyoma**, amit $\mathrm{Tr}_{L|K}(\alpha)$ vagy $\mathrm{S}_{L|K}(\alpha)$ jelöl. Ha K prímtest, akkor egyszerűen $\mathrm{Tr}_L(\alpha)$-t vagy $\mathrm{S}_L(\alpha)$-t írunk, ez α **abszolút nyoma**. Ha nyilvánvaló, hogy mely testekről van szó, akkor röviden $\mathrm{Tr}(\alpha)$-t vagy $\mathrm{S}(\alpha)$-t írunk.

Δ

S a német *Spur*, míg Tr az angol *trace* szó alapján jelöli a testbeli elem nyomát. Mi a továbbiakban a rövidebb S jelölést alkalmazzuk.

5.2. Tétel

Legyen L a *q*-elemű K test *m*-edfokú bővítése, α és β az *L*, *c* a *K* tetszőleges eleme. Ekkor

1. $\mathrm{S}(\alpha+\beta)=\mathrm{S}(\alpha)+\mathrm{S}(\beta)$
2. $\mathrm{S}(c\alpha)=c\mathrm{S}(\alpha)$
3. $\mathrm{S}(c)=mc$
4. $\mathrm{S}(\alpha^q)=\mathrm{S}(\alpha)$
5. S az L mint K feletti vektortér K-ra mint K feletti vektortérre való lineáris leképezése.

Δ

Bizonyítás:

A $\sigma_i : L \to L$ leképezés, ahol $\sigma_i(\alpha) := \alpha^{q^i}$, bármely nem negatív egész *i*-re az L test automorfizmusa, amely *K* elemein az identikus leképezés, ezért igaz 1., 2. és 3. $\alpha^{q^m} = \alpha$, innen $\sum_{i=0}^{m-1}\left(\alpha^q\right)^{q^i} = \sum_{i=1}^{m}\alpha^{q^i} = \sum_{i=0}^{m-1}\alpha^{q^i}$, ami igazolja 4.-et.

Az első két állítás biztosítja, hogy a nyom az L vektortérnek L vektortérbe való lineáris leképezése. Ismét $\alpha^{q^m} = \alpha$-ra hivatkozva $(\mathrm{S}(\alpha))^q = \left(\sum_{i=0}^{m-1}\alpha^{q^i}\right)^q = \sum_{i=1}^{m}\alpha^{q^i} = \sum_{i=0}^{m-1}\alpha^{q^i} = \mathrm{S}(\alpha)$ mutatja, hogy ez a leképezés valójában *K*-ba történik. Azt kell még bizonyítani, hogy ez a leképezés egyben szürjektív is. Ehhez elegendő azt belátni, hogy van olyan *L*-beli α elem, amelynek nem 0 a nyoma, ebből már következik a szürjektivitás. Valóban, 0 nyoma 0. Most tegyük fel, hogy létezik olyan α elem *L*-ben, amelynek nem nulla a nyoma. Legyen $\mathrm{S}(\alpha)=a\in K^*$, és *b* a K^* tetszőleges eleme. Mivel K^* csoport a szorzással, így biztosan van olyan K^*-beli *c* elem, amellyel fennáll a $ca=b$ egyenlőség, és így $\mathrm{S}(c\alpha)=c\mathrm{S}(\alpha)=ca=b$, azaz *b* is egy *L*-beli elem nyoma, *b* is benne van a leképezés képterében. Lássuk tehát be ilyen α létezését. Legyen $\beta\in L$, és $\mathrm{S}(\beta)=0$. Ekkor $0=\sum_{i=0}^{m-1}\beta^{q^i}$, tehát β gyöke a q^{m-1}-edfokú $f=\sum_{i=0}^{m-1}x^{q^i}$ polinomnak. Ennek a polinomnak legfeljebb q^{m-1} különböző gyöke van, ugyanakkor *L* elemeinek száma q^m, és mivel $q>1$, ezért $q^m > q^{m-1}$, van olyan *L*-beli elem, amely nem gyöke az *f* polinomnak, tehát amelynek a nyoma nem a test nulleleme.

□

5.3. Tétel

Legyen az L véges test a K test bővítése, $\alpha \in L^*$ tetszőleges rögzített elem, és T_α az L elemein értelmezett olyan szabály, hogy az L bármely β elemére $\mathrm{T}_\alpha(\beta) := \mathrm{S}(\alpha\beta)$. Ekkor T_α az L-nek mint K test feletti vektortérnek a K vektortérre való lineáris leképezése, különböző L-beli α-hoz az L különböző, K-ra való lineáris leképezése tartozik, és az L vektortér bármely, a K vektortérre való lineáris leképezéséhez van olyan L^*-beli α, hogy $\mathrm{T} = \mathrm{T}_\alpha$.

Δ

Bizonyítás:

$\alpha\beta$ az L eleme, a nyom az L minden elemére értelmezett, egyértelmű, és értéke K-beli, tehát T_α valóban L-nek K-ba való leképezése, továbbá ha β végigfut L elemein, akkor $\alpha\beta$ is felveszi L minden elemét, ezért a leképezés K-ra történik. A nyom lineáris leképezés, így K-beli b, c és L-beli β, γ elemekkel $\mathrm{T}_\alpha(b\beta + c\gamma) = \mathrm{S}(\alpha(b\beta + c\gamma)) = b\mathrm{S}(\alpha\beta) + c\mathrm{S}(\alpha\gamma) = b\mathrm{T}_\alpha(\beta) + c\mathrm{T}_\alpha(\gamma)$, tehát T_α egy $\mathsf{L} \to \mathsf{K}$ lineáris szürjektív leképezés. Ha $\alpha \neq \beta$, akkor létezik $\alpha - \beta$ inverze. Legyen $\delta \in L^*$ olyan, hogy $\mathrm{S}(\delta) \neq 0$, és legyen $\gamma = (\alpha - \beta)^{-1}\delta$. Ekkor $\mathrm{T}_\alpha(\gamma) - \mathrm{T}_\beta(\gamma) = \mathrm{S}(\alpha\gamma) - \mathrm{S}(\beta\gamma) = \mathrm{S}((\alpha - \beta)\gamma) = \mathrm{S}(\delta) \neq 0$, vagyis $\mathrm{T}_\alpha(\gamma) \neq \mathrm{T}_\beta(\gamma)$, és így T_α és T_β különböző leképezések. Végül nézzük az utolsó állítást. Legyen K elemeinek száma q, a bővítés foka m, ekkor L-nek van m elemű bázisa K fölött. Egy lineáris transzformációt egyértelműen meghatároz, ha megadjuk egy bázis elemeinek a képét. Bármely bázis-elemnek egymástól függetlenül q különböző képe lehet, tehát összesen q^m különböző lineáris $\mathsf{L} \to \mathsf{K}$ leképezés definiálható. Elhagyva a nulltranszformációt, $q^m - 1$ $\mathsf{L} \to \mathsf{K}$ lineáris transzformáció van. De éppen ennyi a T_α-k száma is, tehát ez a rész is igaz.

□

5.4. Tétel

Ha M véges test, $\mathsf{M}|\mathsf{L}|\mathsf{K}$, és $\alpha \in M$, akkor $\mathrm{S}_{M|K}(\alpha) = \mathrm{S}_{L|K}\left(\mathrm{S}_{M|L}(\alpha)\right)$.

Δ

Bizonyítás:

$S_{M|L}(\alpha) \in L$, ezért alkalmazható rá a külső nyom. Ha $[\mathsf{L}:\mathsf{K}] = m$ és $[\mathsf{M}:\mathsf{L}] = n$, akkor $[\mathsf{M}:\mathsf{K}] = mn$, és

$$\mathrm{S}_{L|K}\left(\mathrm{S}_{M|L}(\alpha)\right) = \sum_{i=0}^{m-1}\left(\sum_{j=0}^{n-1}\alpha^{(q^m)^j}\right)^{q^i} = \sum_{j=0}^{n-1}\sum_{i=0}^{m-1}\alpha^{q^{mj+i}} = \sum_{k=0}^{mn-1}\alpha^{q^k} = \mathrm{S}_{M|K}(\alpha),$$

ahol q a K elemeinek száma, ugyanis mialatt i 0-tól $m-1$-ig, és j 0-tól $n-1$-ig megy, $k = mj + i$ pontosan egyszer felveszi a $0 \le t < mn$ intervallum minden egész elemét.

□

5.5. Tétel

Ha L_1 a K véges test n_1-edfokú, L_2 az n_2-edfokú bővítése, n_1 és n_2 relatív prímek, és M a K $n = n_1 n_2$-edfokú bővítése, továbbá $\alpha_1 \in L_1$ és $\alpha_2 \in L_2$, akkor $\mathrm{S}_{M|K}(\alpha_1\alpha_2) = \mathrm{S}_{L_1|K}(\alpha_1)\mathrm{S}_{L_2|K}(\alpha_2)$.

Δ

Bizonyítás:

Mivel n_1 és n_2 relatív prím, ezért tetszőleges $0 \le k < n_1 n_2$ egészhez van pontosan egy olyan $(i_1, i_2) \in \mathbf{N}_0^2$ pár, hogy $i_1 < n_1$, $i_2 < n_2$, $i_1 \equiv k \ (n_1)$ és $i_2 \equiv k \ (n_2)$. Ekkor $\alpha_1^{q^{i_1}} = \alpha_1^{q^k}$ és $\alpha_2^{q^{i_2}} = \alpha_2^{q^k}$, tehát $\alpha_1^{q^{i_1}} \alpha_2^{q^{i_2}} = \alpha_1^{q^k} \alpha_2^{q^k} = (\alpha_1 \alpha_2)^{q^k}$. Ezt felhasználva

$$\mathrm{S}_{L_1|K}(\alpha_1)\mathrm{S}_{L_2|K}(\alpha_2) = \left(\sum_{i_1=0}^{n_1-1} \alpha_1^{q^{i_1}}\right)\left(\sum_{i_2=0}^{n_2-1} \alpha_2^{q^{i_2}}\right) = \sum_{i_1=0}^{n_1-1}\sum_{i_2=0}^{n_2-1} \alpha_2^{q^{i_2}} \alpha_1^{q^{i_1}} = \sum_{k=0}^{mn-1} (\alpha_1\alpha_2)^{q^k} = \mathrm{S}_{M|K}(\alpha_1\alpha_2).$$

□

5.6. Következmény

Legyen $i = 1, 2$-re L_i a K test n_i-edfokú bővítése, $n = [n_1, n_2]$, $d = (n_1, n_2)$, továbbá M_n és M_d a K n-ed és d-edfokú bővítése úgy, hogy $\mathsf{M}_n | \mathsf{L}_i | \mathsf{M}_d | \mathsf{K}$, és végül legyen $\alpha_i \in L_i$. Ekkor $\mathrm{S}_{M_n|K}(\alpha_1\alpha_2) = \mathrm{S}_{M_d|K}\left(\mathrm{S}_{L_1|M_d}(\alpha_1)\mathrm{S}_{L_2|M_d}(\alpha_2)\right)$.

Δ

Bizonyítás:

Mivel $d | n_i | n$, így létezik a K-nak olyan M_n és M_d bővítése, amellyel $\mathsf{M}_n | \mathsf{L}_i | \mathsf{M}_d | \mathsf{K}$. L_i az M_d $\frac{n_i}{d}$-edfokú bővítése. $\frac{n_1}{d}$ és $\frac{n_2}{d}$ relatív prímek, és M_n az M_d $\frac{n}{d} = \frac{\frac{n_1 n_2}{d}}{d} = \frac{n_1}{d} \cdot \frac{n_2}{d}$-edfokú bővítése, így így az 5.5. tétel szerint $\mathrm{S}_{M_n|M_d}(\alpha_1\alpha_2) = \mathrm{S}_{L_1|M_d}(\alpha_1)\mathrm{S}_{L_2|M_d}(\alpha_2)$. 5.4.-et alkalmazva pedig azt kapjuk, hogy $\mathrm{S}_{M_n|K}(\alpha_1\alpha_2) = \mathrm{S}_{M_d|K}\left(\mathrm{S}_{M_n|M_d}(\alpha_1\alpha_2)\right) = \mathrm{S}_{M_d|K}\left(\mathrm{S}_{L_1|M_d}(\alpha_1)\mathrm{S}_{L_2|M_d}(\alpha_2)\right)$.

□

6. Formális hatványsorok

6.1. Definíció

Legyen *S* egy nem üres halmaz, és $f:\mathbf{N}_0 \to S$. Ekkor $f(i)$-t f_i-vel jelölve $(f_i \in S | i \in \mathbf{N}_0)$ egy *S* **fölötti** (**végtelen**) **sorozat**, amit röviden (f_i) vagy **f** jelöl. $f_i = (\mathbf{f})_i$ **a sorozat** *i*-**edik tagja**, és két sorozat akkor és csak akkor azonos, ha minden $i \in \mathbf{N}_0$-ra a megfelelő tagjuk egyenlő.

Δ

6.2. Tétel

Legyen $\mathsf{R} = (R;+,\cdot)$ gyűrű, és az *R* fölötti $\mathbf{a} = (a_i)$ és $\mathbf{b} = (b_i)$ sorozatra $u_i = a_i + b_i$, valamint $v_i = \sum_{j=0}^{i} a_j b_{i-j}$. Ekkor az $(\mathbf{a} \oplus \mathbf{b})_i := (\mathbf{u})_i = u_i$ és $(\mathbf{a} \otimes \mathbf{b})_i := (\mathbf{v})_i = v_i$ szabállyal $\mathsf{PS}_R = (R^{\mathbf{N}_0};\oplus,\otimes)$ gyűrű. $P_R := \{\mathbf{u} \in R^{\mathbf{N}_0} | \exists (n_u \in \mathbf{N}_0) \forall (n_u < i \in \mathbf{N}_0): u_i = 0\}$ $R^{\mathbf{N}_0}$-nak a PS_R-beli műveletekre zárt részhalmaza, és ha $\oplus_P$ és $\otimes_P$ a $\oplus$ és $\otimes$ műveletek P_R-re való megszorításai, akkor $\mathsf{P}_R = (P_R;\oplus_P,\otimes_P)$ tartalmaz R-rel izomorf részgyűrűt.

Δ

P_R a definíció alapján azokat a sorozatokat tartalmazza, amelyeknek minden komponense egy adott (sorozatonként nem feltétlenül azonos) indextől kezdve 0.

Bizonyítás:

Mivel a_i, b_j, a_j és b_{i-j} gyűrű elemei, és gyűrűben az összeg és szorzat egyértelmű és benne van a gyűrűben, ezért mind u_i, mind v_i minden nemnegatív egész *i*-re az *R* egyértelműen meghatározott eleme, és ekkor maguk a sorozatok is $R^{\mathbf{N}_0}$ egyértelműen meghatározott elemei. A fenti operációkat bármely sorozatpár esetén elvégezhetjük, így a bevezetett $\oplus$ és $\otimes$ szabály egyaránt binér műveletet definiál $R^{\mathbf{N}_0}$-on.

Legyen $\mathbf{c} = (c_i)$ egy további sorozat. $(a_i + b_i) + c_i = a_i + (b_i + c_i)$ az R gyűrűben igaz, így $(\mathbf{a} \oplus \mathbf{b}) \oplus \mathbf{c} = \mathbf{a} \oplus (\mathbf{b} \oplus \mathbf{c})$, az összeadás asszociatív. Ha $\mathbf{0}$ az a sorozat, amelyben minden $i \in \mathbf{N}_0$-ra az *i*-edik tag 0, és $\mathbf{a}'$ *i*-edik tagja $-a_i$, akkor $\mathbf{0} \oplus \mathbf{a} = \mathbf{a}$, $\mathbf{a}' \oplus \mathbf{a} = \mathbf{0}$, PS_R az összeadással csoport, és mivel $a_i + b_i = b_i + a_i$, ezért $\mathbf{a} \oplus \mathbf{b} = \mathbf{b} \oplus \mathbf{a}$, az összeadás kommutatív is. A szorzás is asszociatív:

$$((\mathbf{a} \otimes \mathbf{b}) \otimes \mathbf{c})_i = \sum_{j=0}^{i} (\mathbf{a} \otimes \mathbf{b})_j c_{i-j} = \sum_{j=0}^{i} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} =$$

$$= \sum_{j=0}^{i} \sum_{k=0}^{j} (a_k b_{j-k}) c_{i-j} = \sum_{j=0}^{i} \sum_{k=0}^{j} a_k (b_{j-k} c_{i-j}) =$$

$$\sum_{k=0}^{i} \sum_{j=k}^{i} a_k (b_{j-k} c_{i-j}) = \sum_{k=0}^{i} a_k \left(\sum_{j=k}^{i} b_{j-k} c_{i-j} \right) =$$

$$= \sum_{k=0}^{i} a_k \left(\sum_{j=0}^{i-k} b_j c_{(i-k)-j} \right) = \sum_{k=0}^{i} a_k (\mathbf{b} \otimes \mathbf{c})_{i-k} = (\mathbf{a} \otimes (\mathbf{b} \otimes \mathbf{c}))_i$$

minden értelmes *i*-re teljesül. Nézzük végül a disztributivitást.

$$((\mathbf{a}\oplus\mathbf{b})\otimes\mathbf{c})_i=\sum_{j=0}^{i}(\mathbf{a}\oplus\mathbf{b})_j c_{i-j}=\sum_{j=0}^{i}(a_j+b_j)c_{i-j}=$$
$$=\sum_{j=0}^{i}(a_j c_{i-j}+b_j c_{i-j})=\sum_{j=0}^{i}a_j c_{i-j}+\sum_{j=0}^{i}b_j c_{i-j}=$$
$$=(\mathbf{a}\otimes\mathbf{c})_i+(\mathbf{b}\otimes\mathbf{c})_i=((\mathbf{a}\otimes\mathbf{c})\oplus(\mathbf{b}\otimes\mathbf{c}))_i$$

és a másik oldali disztributivitás hasonló módon igazolható, így valamennyi gyűrűaxióma teljesül.

P_R minden **u** eleméhez van olyan n_u index, hogy valamennyi ennél nagyobb indexre a sorozat megfelelő tagja nulla. Ha **b** additív inverzét **b′**-vel jelöljük, $\mathbf{a}\oplus\mathbf{b}'$-ben és $\mathbf{a}\otimes\mathbf{b}$-ben legfeljebb $\max\{n_a,n_b\}$ illetve n_a+n_b kielégíti ezt a feltételt, így az összeg- és szorzatsorozatban is csupán véges sok nem nulla tag található, ami mutatja, hogy a P_R halmaz zárt a kivonásra és szorzásra. Ugyanakkor P_R nem üres, hiszen a csupa nullából álló sorozat biztosan benne van, ezért $\mathsf{P}_R\le\mathsf{PS}_R$.

Legyen $\overline{R}$ azon PS_R-beli sorozatok halmaza, amelyekben legfeljebb csak a 0-indexű tag nem nulla. Ez mindenesetre részhalmaza P_R-nek, és mivel most az $\overline{R}$-beli **a** és **b** sorozatra $n_a<1$ és $n_b<1$, tehát $\max\{n_a,n_b\}<1$ és $n_a+n_b<1$, ezért mind a különbség, mind a szorzat benne lesz $\overline{R}$-ban, $\overline{\mathsf{R}}\le\mathsf{P}_R$, ahol $\overline{\mathsf{R}}$ az $\overline{R}$ elemeiből álló részgyűrű. Definiáljunk egy szabályt. Legyen az *R* tetszőleges *r* elemére $\bar{r}\in PS_R$ olyan, hogy $(\bar{r})_i=\delta_{i,0}r$, ahol $\delta_{i,j}:=\begin{cases}0, \text{ha } i\neq j\\ 1, \text{ha } i=j\end{cases}$ a Kronecker-szimbólum. *R* minden eleméhez tartozik egy és csak egy ilyen sorozat, különböző *R*-beli elem által meghatározott sorozat különböző, és ezek a sorozatok valamennyien $\overline{R}$-hoz tartoznak, ezért a $\varphi(r)\mapsto\bar{r}$ szabály *R*-et $\overline{R}$-ba képezi, és ez a leképezés injektív. De φ szürjektív is, hiszen $\overline{R}$ bármely $\bar{r}$ eleme olyan, amelyben legfeljebb csak $r_0=(\bar{r})_0$ nem nulla, és ez az r_0 *R*-nek eleme, így φ bijekció a két halmaz között. Ha *u* és *v* az *R* két eleme, akkor a megfelelő két $\overline{R}$-beli sorozatban minden tag nulla a nullás indexűeket leszámítva, amelyek rendre *u* és *v*. Ekkor az összegsorozatban is csupán a 0-indexű tag lehet nullától különböző, és ez $u+v$, vagyis $\varphi(u)\oplus_P\varphi(v)=\varphi(u+v)$. A szorzatban $u_j v_{i-j}$ csak akkor különbözhet nullától, ha mindkét index 0, vagyis ha $j=0$ és $i=i-j=0$, ezért a szorzatban sem lehet 0-nál nagyobb indexű tag nem nulla, ami azt jelenti, hogy a szorzatsorozat is benne van $\overline{R}$-ban. Ugyanakkor a 0-indexű tag uv, így $\varphi(u)\otimes_P\varphi(v)=\varphi(uv)$, tehát ismét teljesül a művelettartás. Mivel φ bijektíven és művelettartó módon képezi le R-et $\overline{\mathsf{R}}$-ra, ezért $\overline{\mathsf{R}}\cong\mathsf{R}$

□

6.3. Definíció

PS_R a(z R **fölötti**) **formális hatványsorok gyűrűje**, míg P_R a(z R **fölötti**) (**egy határozatlanú**) **polinomok gyűrűje**.

Ha az **f** polinomban minden $n<i\in\mathbf{N}$ indexre, ahol *n* nem negatív egész szám, $f_i=0$, akkor **f legfeljebb** *n*-**edfokú** (**polinom**). Ha még az is teljesül, hogy $f_n\neq0$, akkor **f foka** *n*, és **f** *n*-**edfokú** (**polinom**). Az **f** polinom fokát (amennyiben létezik) $\deg(\mathbf{f})$ jelöli.

f_0 a formális hatványsor illetve polinom **konstans tag**ja. Legfeljebb 0-adfokú polinomot, azaz $\overline{R}$ elemeit, **konstans polinom**nak mondunk, és ha egy konstans polinom konstans tagja 0, akkor a polinom **nullpolinom**.

Δ

Mivel $\mathsf{R} \cong \overline{\mathsf{R}} \leq \mathsf{P}_R \leq \mathsf{PS}_R$, ezért R beágyazható P_R-be, és akkor egyúttal PS_R-be is, így a továbbiakban úgy tekintjük, hogy R részgyűrűje a polinomok illetve a formális hatványsorok gyűrűjének, és a továbbiakban mindhárom struktúrában + és · jelöli a műveleteket. A beágyazás után kapott gyűrűkben az *R* bármely *r* elemére $\bar{r} = r$.

6.4. Tétel:

Legyen $\mathsf{R} = (R;+,\cdot)$ gyűrű. Ekkor tetszőleges *R*-beli *r*-rel és PS_R-beli **a**-val $(r\mathbf{a})_i = (\bar{r}\mathbf{a})_i = ra_i$ és $(\mathbf{a}r)_i = (\mathbf{a}\bar{r})_i = a_i r$ minden $i \in \mathbf{N}_0$-ra.

Δ

Bizonyítás:

Az állítás a szorzás definíciójából közvetlenül adódik, hiszen az $\bar{r}$ sorozatnak csak a 0. indexű komponense különbözhet nullától, és ez a komponens éppen *r*.

□

6.5. Tétel

A nullpolinomnak nincs foka, míg a nullpolinom kivételével minden polinomnak van egyértelműen meghatározott foka, és ez nemnegatív egész. Az **f** polinom akkor és csak akkor legfeljebb *n*-edfokú, ha vagy a nullpolinom és $n \geq 0$, vagy $\deg(\mathbf{f}) \leq n$.

Δ

Bizonyítás:

A fokszámot a sorozat egy indexével definiáltuk, és ez nemnegatív egész. Ismét a definíció szerint a nullpolinom az a polinom, amelyben valamennyi tag 0, így a nullpolinomban nincs olyan *i* index, amelyre teljesülne az $f_i \neq 0$ feltétel, ezért ennek a polinomnak nem lehet foka. Ha viszont **f** nem a nullpolinom, akkor van benne nullától különböző tag, és mivel polinom, ezért csak véges sok ilyen tag van benne, így az ilyen tagokhoz tartozó indexek halmaza a nemnegatív egészek halmazának nem üres véges részhalmaza. Egy ilyen halmaznak van legnagyobb eleme, és ha ez *n*, akkor *n* egyértelmű. Ha $i > n$, akkor $f_i = 0$, tehát **f** legfeljebb *n*-edfokú, ugyanakkor $f_n \neq 0$, tehát $\deg(\mathbf{f}) = n$.

A nullpolinomban minden nem negatív egész *n*-re igaz, hogy az *n*-nél nagyobb indexű tagok nullák, vagyis minden nem negatív egész *n*-re a polinom legfeljebb *n*-edfokú. Ha **f** *n*-edfokú, akkor az előbbiek alapján minden $i > n$-re $f_i = 0$, de akkor $m \geq n$ esetén az is igaz, hogy valamennyi $i > m$ indexre $f_i = 0$, tehát **f** legfeljebb *m*-edfokú. Amennyiben viszont $m < n$, akkor van olyan, *m*-nél nagyobb *i* index, nevezetesen *n*, amelyre nem igaz, hogy $f_i = 0$, így az sem igaz, hogy **f** legfeljebb *m*-edfokú. Innen kapjuk az utolsó állítást.

□

Az előbbiek alapján tehát a nullpolinomnak és csak a nullpolinomnak nincs foka, ám ha azt mondjuk, hogy az **f** polinom foka legfeljebb *n* (ahol *n* valamilyen nemnegatív egész), akkor ebbe beleértjük azt a lehetőséget is, hogy **f** esetleg a nullpolinom (hiszen ebben az esetben is teljesül az a kritérium, hogy a polinom valamennyi tagja nulla, ha az indexük nagyobb *n*-nél). Bevezetünk egy célszerű jelölést.

6.6. Jelölés

Ha $\mathbf{f} \in P_R$ nem a nullpolinom, akkor legyen $\delta(\mathbf{f}) := \deg \mathbf{f}$, míg a nullpolinomra $\delta(\mathbf{f}) := -\infty$. $n \in \mathbf{N}_0$-ra $P_R^{(n)} := \{\mathbf{f} \in P_R \mid \delta(\mathbf{f}) \leq n\}$.

Δ

Nyilván igaz, hogy deg egy $\deg : P_R \setminus \{\mathbf{0}\} \to \mathbf{N}_0$ leképezés míg δ egy $\delta : P_R \to \mathbf{N}_0 \cup \{-\infty\}$ leképezés, továbbá minden nem negatív egész *i*-re és *k*-ra $P_R^{(i)} \subseteq P_R^{(i+k)} \subseteq \bigcup_{n=0}^{\infty} P_R^n = P_R$. Azt is láthatjuk, hogy $P_R^{(0)} = \overline{R} = R$.

6.7. Tétel:

R, P_R és PS_R egyszerre kommutatív, egyszerre (bal oldali) egységelemes, és egyszerre nullosztómentes. Nullosztómentes R esetén PS_R (bal oldali) egységeleme – ha létezik – benne van *R*-ben.

Δ

Bizonyítás:

1. Kommutatív gyűrű bármely részgyűrűje kommutatív, így ha PS_R kommutatív, akkor hasonló tulajdonságú P_R, míg P_R kommutativitása esetén kommutatív R. Ha viszont R kommutatív, akkor $(\mathbf{ab})_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j=0}^{i} b_{i-j} a_j = \sum_{j=0}^{i} b_j a_{i-j} = (\mathbf{ba})_i$, tehát kommutatív a PS_R gyűrű.

2. Legyen *e* az R (bal oldali) egységeleme, és $\mathbf{a} \in PS_R$. Ekkor $(e\mathbf{a})_i = ea_i = a_i$, tehát $e\mathbf{a} = \mathbf{a}$, *e* (bal oldali) egységelem a sorozatok gyűrűjében, és mivel $e \in R \subseteq P_R \subseteq PS_R$, így a polinomok gyűrűjében is (bal oldali) egységelem.

Most tegyük fel, hogy az $\mathbf{e} = (e_i)$ sorozat (bal oldali) egységelem PS_R-ben illetve P_R-ben. Ekkor tetszőleges $b \in R$-re $\mathbf{e}b = b$, vagyis $e_0 b = (\mathbf{e}b)_0 = (b)_0 = b$, és az $e = e_0$ jelöléssel $b = eb$, azaz *e* bal oldali egységelem R-ben. Ekkor viszont az eddigiek alapján a harmadik gyűrű is (bal oldali) egységelemes. $i > 0$-ra $0 = b_i = (\mathbf{e}b)_i = e_i b$-ből e_i bal oldali annullátora az eredeti gyűrűnek, és nullosztómentes gyűrűben ez csak a 0 lehet, tehát ekkor **e** konstans sorozat, vagyis eleme *R*-nek.

3. Végül a nullosztómentesség. Nullosztómentes gyűrű részgyűrűje is nullosztómentes, tehát ha PS_R nullosztómentes, akkor nullosztómentes P_R, míg P_R nullosztómentessége esetén nullosztómentes R. Ha viszont R nullosztómentes, és sem **a**, sem **b** nem **0**, akkor van mindkettőben nem nulla tag. Legyen n_a és n_b a legkisebb ilyen index. Ekkor

$$(\mathbf{ab})_{n_a+n_b} = \sum_{i=0}^{n_a+n_b} a_i b_{(n_a+n_b)-i} = \sum_{i=0}^{n_a-1} a_i b_{n_b+(n_a-i)} + a_{n_a} b_{n_b} + \sum_{i=n_a+1}^{n_a+n_b} a_i b_{n_b-(i-n_a)} =$$
$$= \sum_{i=0}^{n_a-1} a_i b_{n_b+(n_a-i)} + a_{n_a} b_{n_b} + \sum_{i=0}^{n_b-1} a_{n_a+(n_b-i)} b_i \quad ,$$

és a jobb oldalon az első összegben valamennyi *i*-re a_i, az utolsóban pedig minden *i*-re b_i értéke 0, így az összeg a középső taggal egyenlő. De R nullosztómentessége alapján $a_{n_a} b_{n_b} \neq 0$, így viszont **ab**-ben van nullától különböző komponens, **ab** nem nulla, tehát PS_R nullosztómentes.

□

6.8. Tétel

Legyen **f** és **g** két R fölötti polinom. Ekkor

1. $\delta(\mathbf{f} \pm \mathbf{g}) \leq \max\{\delta(\mathbf{f}), \delta(\mathbf{g})\}$, és ha $\delta(\mathbf{f}) < \delta(\mathbf{g})$, akkor $\delta(\mathbf{f} \pm \mathbf{g}) = \delta(\mathbf{g}) = \max\{\delta(\mathbf{f}), \delta(\mathbf{g})\}$
2. $\delta(\mathbf{fg}) \leq \delta(\mathbf{f}) + \delta(\mathbf{g})$, és $\delta(\mathbf{fg}) = \delta(\mathbf{f}) + \delta(\mathbf{g})$ akkor és csak akkor, ha **f** és **g** legalább egyike **0**, vagy egyik sem **0**, és $f_{\deg(f)} g_{\deg(g)} \neq 0$.

Δ

Bizonyítás:

1. Minden $\max\{\delta(\mathbf{f}),\delta(\mathbf{g})\} < i \in \mathbf{N}_0$-ra $f_i = 0 = g_i$, de akkor valamennyi ilyen i-re $(\mathbf{f} \pm \mathbf{g})_i = 0$, és így $\delta(\mathbf{f} \pm \mathbf{g}) \le \max\{\delta(\mathbf{f}),\delta(\mathbf{g})\}$. Ha $\delta(\mathbf{f}) < \delta(\mathbf{g})$, akkor $\delta(\mathbf{g}) \neq -\infty$, tehát $\delta(\mathbf{g}) \in \mathbf{N}_0$, és $f_{\delta(\mathbf{g})} = 0 \neq g_{\delta(\mathbf{g})}$, így $(\mathbf{f} \pm \mathbf{g})_{\delta(\mathbf{g})} = f_{\delta(\mathbf{g})} + g_{\delta(\mathbf{g})} = g_{\delta(\mathbf{g})} \neq 0$, tehát $\delta(\mathbf{f} \pm \mathbf{g}) \ge \delta(\mathbf{g}) = \max\{\delta(\mathbf{f}),\delta(\mathbf{g})\}$. Ez viszont, az előbbi egyenlőtlenséggel együtt azt jelenti, hogy $\delta(\mathbf{f} \pm \mathbf{g}) = \delta(\mathbf{g}) = \max\{\delta(\mathbf{f}),\delta(\mathbf{g})\}$.

2. Azt már korábban beláttuk, hogy a $\delta(\mathbf{f}) + \delta(\mathbf{g})$-nél nagyobb indexekre a szorzat minden tagja nulla, tehát $\delta(\mathbf{fg}) \le \delta(\mathbf{f}) + \delta(\mathbf{g})$. Ha $\min\{\delta(\mathbf{f}),\delta(\mathbf{g})\} = -\infty$, akkor legalább az egyik polinom a nullpolinom, de akkor a szorzatuk is az, márpedig $-\infty$-hez önmagát vagy egy véges számot adva ismét $-\infty$-t kapunk. Ha viszont egyik polinom sem a nullpolinom, azaz $\delta(\mathbf{f})$ és $\delta(\mathbf{g})$ egyaránt nem negatív egész szám, akkor a már említett bizonyítás szerint a szorzatban a $\delta(\mathbf{f}) + \delta(\mathbf{g})$ indexhez tartozó tag éppen $f_{\deg(f)} g_{\deg(g)}$, ami most a feltétel szerint nem nulla, így a szorzatpolinom foka legalább $f_{\deg(f)} g_{\deg(g)}$, de nagyobb nem lehet, amint azt már beláttuk.

□

A tételből következik, hogy nullosztómentes gyűrű feletti polinomgyűrűben bármely **f** és **g** polinom esetén $\delta(\mathbf{fg}) = \delta(\mathbf{f}) + \delta(\mathbf{g})$.

6.9. Tétel

Legyen $\mathsf{R} = (R;+,\cdot)$ gyűrű, és P_R és PS_R az R fölötti polinomok illetve sorozatok gyűrűje. Ekkor PS_R a PS_R-beli műveletekkel R fölötti két oldali modulus, amely akkor és csak akkor unitér, ha R egységelemes, akkor és csak akkor R feletti lineáris tér, ha R ferdetest, és pontosan akkor algebra, ha R test, és ez utóbbi esetben az algebra rangja végtelen. P_R az előbbi modulus részmodulusa, amely akkor és csak akkor unitér, vagy lineáris tér, vagy algebra, ha PS_R rendelkezik a megfelelő tulajdonsággal, és az utolsó esetben ez a részmodulus is végtelen rangú. Az R fölötti legfeljebb $n-1$-edfokú polinomok halmaza részmodulus P_R-ben, és ha P_R lineáris tér, akkor a legfeljebb $n-1$-edfokú polinomok halmaza n-dimenziós altér a polinomok R fölötti lineáris terében.

Δ

Bizonyítás:

Bármely gyűrű két oldali modulus tetszőleges részgyűrűje fölött, és mivel a modulusszorzást a sorozatok szorzásával definiáltuk, ezért a részgyűrűk egyben részmodulusok is. Mivel a három gyűrű egyszerre egységelemes, és a három gyűrű egységeleme azonos, ezért igaz az unitérségre és lineáris térre vonatkozó állítás is, és a modulus pontosan akkor lesz algebra, ha a modulus unitér, és a részgyűrű része a teljes gyűrű centrumának, vagyis ha R test.

Ha **a** és **b** legfeljebb $n-1$-edfokú polinom, akkor ez igaz $r\mathbf{a}$-ra és $\mathbf{a} - \mathbf{b}$-re is, ezért a legfeljebb $n-1$-edfokú polinomok (unitér) részmodulust illetve alteret alkotnak P_R-ben.

Még a rangra illetve dimenzióra vonatkozó állításokat kell igazolni. Most R test, tehát egységelemes, legyen e az egységelem. Ha adott nemnegatív egész i-re $\mathbf{x}_i$ jelöli azt a sorozatot, amelyben az i-edik komponens e, az összes többi viszont 0, és t egy nemnegatív egész, akkor $\sum_{i=0}^{t} a_i \mathbf{x}_i$ is P_R-beli sorozat, jelöljük **a**-val. **a** definíciójából látjuk, hogy $t \ge j \in \mathbf{N}_0$-ra **a** j-edik komponense a_j, míg minden más komponens 0 az **a** sorozatban. A definíció alapján P_R két eleme akkor és csak akkor azonos, ha minden komponensük egyenlő, ezért **a** pontosan akkor lesz a nullsorozat, vagyis a vektortér nulleleme, ha minden, t-nél nem nagyobb j-re $a_j = 0$, így az $\mathbf{x}_i$ vektorok halmazában bármilyen nagy pozitív t-re van t lineárisan független vektor, de akkor ez még inkább igaz a teljes PS_R-re, ami mutatja, hogy a test fölötti polinomok és formális hatványsorok valóban végtelen rangú algebrát képeznek.

Algebra egyben vektortér is, tehát $(P_R;+)$ lineáris tér R fölött. Az előbbiek szerint $n>i\in\mathbf{N}_0$-ra az $\mathbf{x}_i$-k lineárisan függetlenek. Legyen most **a** legfeljebb $n-1$-edfokú polinom. A $\sum_{i=0}^{n-1}a_i\mathbf{x}_i$ sorozat minden komponense azonos **a** hasonló indexű komponensével, így az $n>i\in\mathbf{N}_0$ indexű $\mathbf{x}_i$-k lineáris kombinációjaként bármely legfeljebb $n-1$-edfokú polinom előáll. Másfelől a nevezett $\mathbf{x}_i$ sorozatok lineáris kombinációjaként csak olyan sorozatot kapunk, amelyben az *n*-nél nem kisebb indexű komponensek mindegyike 0, azaz legfeljebb $n-1$-edfokú polinomot, ami összefoglalóan azt jelenti, hogy az $\{\mathbf{x}_i|n>i\in\mathbf{N}_0\}$ által generált altér éppen a legfeljebb $n-1$-edfokú polinomok halmaza, és ebben az altérben az előbbi halmaz bázis, tehát ez az altér pontosan *n*-dimenziós.

□

6.10. Tétel

Ha az R gyűrű egységelemes az *e* egységelemmel, és a nemnegatív egész *i*-re $\mathbf{x}_i$ az a sorozat, amelyben az *i*-edik komponens *e*, az összes többi komponens pedig 0, továbbá $\mathbf{x}=\mathbf{x}_1$, akkor $\mathbf{x}_i=\mathbf{x}^i$, és $\mathbf{x}^i$ minden sorozattal felcserélhető. Ha $k\in\mathbf{N}_0$, akkor $(\mathbf{x}^k\mathbf{s})_i=0$, ha $k>i\in\mathbf{N}_0$, és $(\mathbf{x}^k\mathbf{s})_i=s_{i-k}$, amikor $k\le i\in\mathbf{N}_0$. Amennyiben **s** P_R eleme, és **s** legfeljebb *t*-edfokú polinom, akkor $\mathbf{s}=\sum_{i=0}^{t}s_i\mathbf{x}^i$.

Δ

Bizonyítás:

Megmutatjuk, hogy $\mathbf{x}^u$-ban $(\mathbf{x}^u)_v=\delta_{u,v}e$. R egységelemes az *e* egységelemmel, így PS_R is egységelemes, és az egységelem az a sorozat, amelyben minden komponens 0, kivéve a 0. indexhez tartozót, amely az eredeti gyűrű egységeleme, vagyis a sorozatok gyűrűjének egységeleme éppen $\mathbf{x}_0$, és mivel egységelemes gyűrűben minden elem nulladik hatványa a gyűrű egységeleme, ezért $\mathbf{x}_0=\mathbf{x}^0$. Most tegyük fel, hogy ha *u* egy nemnegatív egész, akkor minden, *u*-nál nem nagyobb nemnegatív egész *i*-vel teljesül az $\mathbf{x}_i=\mathbf{x}^i$ egyenlőség. Ekkor $\mathbf{x}^{u+1}=\mathbf{x}^u\mathbf{x}$ alapján csak olyan *j* indexre kapunk $\mathbf{x}^{u+1}$-ben nem nulla tagot, ahol az első tényező indexe $j=u$, a másodiké $i-j=1$. Ennek egyetlen megoldása $i=u+1$, ekkor mindkét tényező az egységelem, a szorzatuk is az, így $\mathbf{x}^{u+1}$ valóban $\mathbf{x}_{u+1}$-el azonos.

$\mathbf{x}^i$-ben csak *e* és 0 áll, ezek *R* minden elemével felcserélhetőek, így igaz a felcserélhetőség.

Ha $k=0$, akkor $\mathbf{x}^k$ az egységelem, és igaz az állítás. $(\mathbf{x}\cdot\mathbf{s})=\sum_{j=0}^{i}x_js_{i-j}$. Ha $i=0$, akkor ez az összeg x_0s_0, és $x_0=0$, tehát a szorzat is nulla, míg ha $i>0$, akkor $j=1$-re $x_js_{i-j}=x_1s_{i-1}=s_{i-1}$, és minden más *j*-re 0, így maga az összeg is s_{i-1}, $k=1$-re is beláttuk a tétel ezen részét, innen pedig indukcióval kapjuk az állítást tetszőleges pozitív egész *k*-ra.

Az utolsó állítás is igaz, hiszen $\mathbf{x}^i=\mathbf{x}_i$, és azt már beláttuk korábban, hogy $\sum_{i=0}^{t}s_i\mathbf{x}^i$ olyan sorozat, amelyben a $t\ge i\in\mathbf{N}_0$ indexekre az *i*-edik komponens s_i, míg *t*-nél nagyobb *i*-re $s_i=0$, azaz $\sum_{i=0}^{t}s_i\mathbf{x}^i$ éppen **s**.

□

6.11. Definíció

Legyen *x* az R gyűrűhöz nem tartozó szimbólum, az $\mathbf{s}=(s_i)$ sorozatra $\sum_{i=0}^{\infty}s_ix^i:=\mathbf{s}$, ahol $s_0x^0:=s_0$, valamint minden nem negatív egész *i*-re $0\cdot x^i:=0$ és $sx^i=x^is$. Ekkor *x* **határozatlan**, és

az R feletti formális hatványsorok és (egyhatározatlanú) polinomok halmazát rendre $R[[x]]$ és $R[x]$, a megfelelő gyűrűket $\mathsf{R}[[x]]$ illetve $\mathsf{R}[x]$ jelöli.

Ha $\mathbf{s} = \sum_{i=0}^{t} s_i x^i$ a nem negatív egész *t*-vel, akkor *t* a polinom **formális foka**.

Δ

6.12. Tétel

Ha R egységelemes gyűrű az *e* egységelemmel, akkor $ex = \mathbf{x}$, ahol **x** az az R fölötti sorozat, amelyben csak az $i = 1$ indexű komponens nem nulla, és ez éppen *e*.

Δ

Bizonyítás:

ex az előbb megadott definíció alapján olyan sorozat, amelyben egyetlen, mégpedig az 1-indexhez tartozó komponens különbözik nullától, és ez a komponens *e*, tehát az *ex* formális hatványsor valóban **x**-el azonos.

□

6.13. Megjegyzés

A fenti tétel szerint *x* pontosan akkor sorozat illetve polinom az eredeti gyűrű fölött, ha ez a gyűrű egységelemes.

Δ

6.14. Tétel

Az R gyűrű feletti **s** formális hatványsor akkor és csak akkor (bal oldali) egység $\mathsf{R}[[x]]$ben, ha s_0 (bal oldali) egység R-ben; ha egy $R[[x]]$-beli sorozat 0. tagja felbonthatatlan R-ben, akkor maga a sorozat felbonthatatlan $\mathsf{R}[[x]]$-ben.

Δ

Bizonyítás:

Legyen *s* bal oldali egység R-ben, és **s** olyan sorozat, amelyben $s_0 = s$. Ha **a** tetszőleges sorozat, akkor van olyan b_0, amellyel $sb_0 = a_0$. Tegyük fel, hogy $n > i \in \mathbf{N}_0$-ra van olyan b_i, hogy $\sum_{j=0}^{i} s_j b_{i-j} = a_i$. Innen az $a_0 = \sum_{j=0}^{n} s_j b_{n-j} = s_0 b_n + \sum_{j=1}^{n} s_j b_{n-j} = sb_n + t$ egyenlőségnek kell teljesülnie, ahol b_n ismeretlen, azaz olyan b_n-t keresünk, amellyel $sb_n = a_n - t = u$. De *s* bal oldali egység, ezért van ilyen elem *R*-ben, vagyis **b** olyan sorozat lesz, amellyel $\mathbf{s} \cdot \mathbf{b} = \mathbf{a}$, és így **s** bal oldali egység a formális hatványsorok gyűrűjében. Ugyanígy kapunk egy olyan **c** sorozatot, amellyel $\mathbf{c} \cdot \mathbf{s} = \mathbf{a}$, ha *s* egység, vagyis ekkor **s** is egység $\mathsf{R}[[x]]$-ben. Fordítva, tegyük fel, hogy az **s** sorozat bal oldali egység az R fölötti formális hatványsorok gyűrűjében, és *a* az *R* tetszőleges eleme. Mivel **s** bal oldali egység, van olyan $\mathbf{b} = R[[x]]$, hogy $\mathbf{s} \cdot \mathbf{b} = a$, ami csak úgy lehetséges, ha $(\mathbf{s} \cdot \mathbf{b})_0 = s_0 b_0 = a$, vagyis s_0 bal oldali egység R-ben. Ha **s** egyben egység, akkor az előbbiekhez hasonlóan láthatjuk be, hogy s_0 egyben jobb oldali egység is az alapgyűrűben, vagyis egység R-ben.

Amennyiben c_0 az R felbonthatatlan eleme, és $\mathbf{c} = \mathbf{a} \cdot \mathbf{b}$, akkor $c_0 = a_0 b_0$-ban a_0 és b_0 egyike szükségszerűen a megfelelő oldalról egység R-ben. Ekkor az adott sorozat is hasonló tulajdonságú a hatványsorok gyűrűjében, így **c** az $\mathsf{R}[[x]]$ felbonthatatlan eleme.

□

6.15. Következmény

Ferdetest feletti formális hatványsor pontosan akkor egység, ha konstans tagja nem nulla.

Δ

Bizonyítás:
Ferdetest nem nulla elemének van inverze, vagyis egység, ellenben a 0 nem egység.

□

6.16. Megjegyzés

Az előbbi tétel és következmény $\mathsf{R}[x]$-re nem igaz: ha R a racionális számok teste, akkor $(1,-1)$ nem osztója $(1,1)$-nek mint polinomnak, tehát $(1,-1)$ nem egység, jóllehet 1 egység **Q**-ban, ugyanakkor 5 felbonthatatlan **Z**-ben, ám az $(5,-6,1)$ polinom előáll $(1,-1)(5,-1)$ alakban.

Δ

6.17. Tétel

Amennyiben R egységelemes gyűrű, akkor $R[[x]]$ minden nem nulla eleme $x^u\mathbf{s}$ alakú, ahol $u \in \mathbf{N}_0$ és $s_0 \neq 0$. Ha R ferdetest, akkor **s** egység $\mathsf{R}[[x]]$-ben, és ha test, akkor $\mathsf{R}[[x]]$ euklideszi gyűrű.

Δ

Bizonyítás:
R egységelemessége alapján x minden nemnegatív egész kitevős hatványa eleme $R[[x]]$-nek, és $x = \mathbf{x}$. Legyen $0 \neq \mathbf{t}$-ben az r-edik tag az első nullától különböző (ilyen létezik, mert feltettük, hogy a sor különbözik 0-tól), és **s** az a sorozat, amelyben $s_i = t_{r+i}$. Korábban már bizonyítottuk, hogy $(\mathbf{x}^r\mathbf{s})_i$ nulla, ha $r > i \in \mathbf{N}_0$, egyébként $s_{i-r} = t_{(r+i)-r} = t_i$ az értéke, így minden $i \in \mathbf{N}_0$-ra $(\mathbf{x}^r\mathbf{s})_i = t_i$, tehát $\mathbf{x}^r\mathbf{s} = \mathbf{t}$. $s_0 \neq 0$, ezért ha R ferdetest, akkor egy korábbi tétel alapján **s** egység $R[[x]]$.

A $\mathbf{t} = \mathbf{x}^r\mathbf{s}$ alakú felírásban **s** konstans tagja nem nulla, ezért ha R test, akkor **s** egység az $\mathsf{R}[[x]]$ gyűrűben. $\varphi(\mathbf{t}) = r$ az R feletti nem nulla formális hatványsorokat képezi le $\mathbf{N}_0$-ba. Ha $\mathbf{a} = x^u\mathbf{a}_1$ és $\mathbf{b} = x^v\mathbf{b}_1$, ahol $\mathbf{a}_1$ és $\mathbf{b}_1$ egység, akkor $u \geq v$ esetén $\mathbf{a} = x^u\mathbf{a}_1 = (x^{u-v}\mathbf{q}_1)(x^v\mathbf{b}_1) = \mathbf{q}\cdot\mathbf{b}$, ahol $\mathbf{q}_1$ az $\mathbf{a}_1$ és $\mathbf{b}_1$ (asszociálttól eltekintve egyértelmű) hányadosa. Ez a hányados létezik, hiszen most $\mathbf{b}_1$ egység. Ha viszont $u < v$, akkor $\mathbf{a} = 0\cdot\mathbf{b} + \mathbf{a}$, és $\varphi(\mathbf{a}) = u < v = \varphi(\mathbf{b})$.

□

6.18. Megjegyzés

Ha az előbbi bizonyításban **a** és **b** polinomok, akkor **q** általában nem polinom, tehát ezzel a φ függvénnyel a test feletti polinomgyűrű nem euklideszi (nem azt mondtuk, hogy a test feletti polinomgyűrű nem euklideszi – hiszen tudjuk, hogy az $-$, hanem, hogy ezzel a φ függvénnyel nem az).

Δ

6.19. Tétel

Ha K test, akkor létezik $\mathsf{K}[[x]]$ hányadosteste, és ennek nem nulla elemei $x^u\mathbf{s}$ alakúak, ahol $u \in \mathbf{Z}$, és **s** egy $\mathsf{K}[[x]]$-beli egység.

Δ

Bizonyítás:

Mivel test kommutatív és nullosztómentes, ezért $\mathsf{K}[[x]]$ is kommutatív és nullosztómentes, így létezik a hányadostest. Test feletti nem nulla hatványsorok $x^u\mathbf{a}$ alakúak nem negatív egész *u*-val és olyan **a** hatványsorral, amelynek konstans tagja nullától különböző, tehát egység K-ban, és így **a** egység $\mathsf{K}[[x]]$-ben. A hányadostest elemei az $(x^u\mathbf{a}, x^v\mathbf{b})$ alakú párok valamint a $(0, x^v\mathbf{b})$ pár által reprezentált osztályok, ahol két ilyen pár, $(x^u\mathbf{a}, x^v\mathbf{b})$ és $(x^w\mathbf{c}, x^z\mathbf{d})$ pontosan akkor van egy osztályban, ha $x^{u+z}\mathbf{ad} = x^{v+w}\mathbf{bc}$. A műveleteket a hányadostestekben megszokott módon definiáljuk, vagyis az $(x^u\mathbf{a}, x^v\mathbf{b})$ és $(x^w\mathbf{c}, x^z\mathbf{d})$ párokkal reprezentált osztályok összege $(x^{u+z}\mathbf{ad} + x^{v+w}\mathbf{bc}, x^{v+z}\mathbf{bd})$ és szorzata $(x^{u+w}\mathbf{ac}, x^{v+z}\mathbf{bd})$ osztálya, illetve, ha az egyik elem 0-val reprezentált osztály, akkor az összeg a másik elemet, a szorzat pedig a 0-t tartalmazó osztály. Legyen *e* $\mathsf{K}[[x]]$ egységeleme. A hányadostestben az $(x^u\mathbf{a}, e)$ alakú elemekkel és a $(0, e)$-vel reprezentált osztályok részgyűrűt alkotnak, amely izomorf $\mathsf{K}[[x]]$-szel, ahol az izomorfizmus az előbbi $(x^u\mathbf{a}, e)$-hoz tartozó osztálynak a $K[[x]]$-beli $x^u\mathbf{a}$-t, a $(0, e)$-hez tartozó osztálynak 0-t felelteti meg. A hányadostest egységelemét azon párok osztálya alkotja, amelyek két komponense azonos, és az $(e, x^u\mathbf{a})$ alakú elemmel reprezentált osztály láthatóan inverze az $(x^u\mathbf{a}, e)$ alakú elemmel reprezentált osztálynak; ezt az inverzet jelölhetjük $x^{-u}\mathbf{c}$-vel, ahol **c** az **a** $\mathsf{K}[[x]]$-beli inverze (ami létezik, mivel **a** mint hatványsor egység). Ha egy osztályt olyan $(x^u\mathbf{a}, x^v\mathbf{b})$ pár reprezentál, amelynél $u \geq v$, akkor ugyanezen osztályt reprezentálja az $(x^{u-v}\mathbf{c}, e)$ pár, ahol $\mathbf{c} = \mathbf{ab}^{-1}$ (**b** egység, így van inverze), vagyis ekkor az $(x^u\mathbf{a}, x^v\mathbf{b})$ párhoz tartozó osztály $x^{u-v}\mathbf{c}$, míg $u < v$-nél az $(x^u\mathbf{a}, x^v\mathbf{b})$ és $(e, x^{v-u}\mathbf{c}^{-1})$ párok lesznek azonos osztályban, vagyis ez az osztály ismét megegyezik $x^{u-v}\mathbf{c}$-vel, ami mutatja, hogy a hányadostest minden nem nulla eleme $x^w\mathbf{c}$ alakú, ahol $w \in \mathbf{Z}$, és **c** egység $\mathsf{K}[[x]]$-ben.

□

6.20. Definíció

Ha K test, akkor $\mathsf{K}[[x]]$ hányadosteste a K **feletti Laurent-sorok teste**, amit $\mathsf{K}\langle x \rangle$ jelöl.

Δ

6.21. Tétel

Ha R egységelemes gyűrű az *e* egységelemmel, akkor $e - x$ inverze $\mathsf{R}[[x]]$-ben $\sum_{i=0}^{\infty} x^i$.

Δ

Bizonyítás:

Legyen $\mathbf{s} = \sum_{i=0}^{\infty} x^i$, ekkor $(e-x)\sum_{i=0}^{\infty} x^i = (e-x)\mathbf{s} = \mathbf{s} - x\cdot\mathbf{s} = \mathbf{s} - \mathbf{t}$, ahol $\mathbf{t} = x\cdot\mathbf{s}$. **s** minden eleme *e*, míg **t**-ben $t_0 = 0$, és $i \geq 1$-re $t_i = s_{i-1} = e = s_i$, így $(\mathbf{s}-\mathbf{t})_0 = s_0 - t_0 = e$, és ha $i \neq 0$, akkor $(\mathbf{s}-\mathbf{t})_i = s_i - t_i = 0$, azaz $(e-x)\mathbf{s} = e$. A másik oldali szorzás hasonló eredményt ad.

□

6.22. Következmény

Ha $p \in \mathbf{N}$ és $\mathbf{f} = \sum_{i=0}^{p-1} a_i x^i \in R[x]$ az R egységelemes gyűrűvel, akkor

1. $\mathbf{f}\cdot\left(e-x^p\right)^{-1}=\sum_{i=0}^{\infty}c_i x^i=\left(e-x^p\right)^{-1}\cdot\mathbf{f}$, ahol $c_i=a_{(i \bmod p)}$.
2. $(e-x)^{-n}=\sum_{k=0}^{\infty}\binom{n+k-1}{n-1}x^k$.

Δ

Bizonyítás

1. Az előbbi tétel alapján $\mathbf{u}=\left(e-x^p\right)^{-1}=\sum_{i=0}^{\infty}\left(x^p\right)^i=\sum_{i=0}^{\infty}x^{pi}=\sum_{i=0}^{\infty}u_i x^i$, ahol $u_i=e$, ha $i=kp$, egyébként 0. Ezzel $\mathbf{f}\left(e-x^p\right)^{-1}=\mathbf{f}\cdot\mathbf{u}=\left(\sum_{i=0}^{p-1}a_i x^i\right)\cdot\mathbf{u}=\sum_{i=0}^{p-1}a_i\left(x^i\mathbf{u}\right)=\sum_{i=0}^{p-1}a_i\mathbf{u}^{(i)}$, és $\mathbf{u}^{(i)}$ j-edik komponense 0, ha $i>j\in\mathbf{N}_0$, egyébként pedig u_{j-i}. Mivel $p>i\in\mathbf{N}_0$, ezért ha $i>j\in\mathbf{N}_0$, akkor $-p<j-i<0$, tehát $u_{j-i}=0$, ami azt jelenti, hogy minden nemnegatív egész j-re $\left(\mathbf{u}^{(i)}\right)_j=u_{j-i}$. Ezt alkalmazva $\left(\mathbf{f}\cdot\mathbf{u}\right)_j=\left(\sum_{i=0}^{p-1}a_i\mathbf{u}^{(i)}\right)_j=\sum_{i=0}^{p-1}a_i\left(\mathbf{u}^{(i)}\right)_j=\sum_{i=0}^{p-1}a_i u_{j-i}$, és mivel a $j-p<k\le j$ intervallum pontosan p egészt tartalmaz, ezért van egy és csak egy olyan i, nevezetesen $(j \bmod p)$, amelyre $j-i$ osztható p-vel, vagyis erre az i-re és csak erre az i-re $u_{j-i}=e$, a többi i indexre $u_{j-i}=0$. Ebből kapjuk, hogy $\left(\mathbf{f}\cdot\mathbf{u}\right)_j=\sum_{i=0}^{p-1}a_i u_{j-i}=a_{(j \bmod p)}$, és $\mathbf{f}\left(e-x^p\right)^{-1}=\sum_{i=0}^{\infty}a_{(i \bmod p)}x^i$. $\mathbf{f}$-fel a másik oldalról szorozva ugyanezt kapjuk, hiszen test kommutatív.

2. Szintén az előbbi tétel szerint $(e-x)^{-n}=\left(\sum_{i=0}^{\infty}x^i\right)^n=\sum_{i_1=0}^{\infty}\cdots\sum_{i_n=0}^{\infty}x^{i_1+\ldots+i_n}=\sum_{i=0}^{\infty}t_i x^i$, ahol t_k az összes olyan $i_1+\ldots+i_n$ összeg száma, amelynek az értéke k, és minden tag nem negatív. Ez éppen a $k+1$ elemből választott $n-1$-edrendű ismétléses kombináció. Egy ilyen kombináció ugyanis kölcsönösen egyértelmű módon megfeleltethető a $\{0,1,\cdots,k\}$ halmaz elemeiből álló $n-1$ hosszúságú monoton növekvő sorozatoknak. Nézzük az $s_j=i_1+\ldots+i_j$ összegeket $j=1,\ldots,n-1$-re. Mivel minden tag nem negatív, ezért ez a sorozat monoton növekszik, a legkisebb érték $i_1=0$ esetén 0, a legnagyobbat pedig akkor kapjuk, ha $i_n=0$, ekkor ugyanis s_{n-1} értéke k kell, hogy legyen. Az ilyen kombinációk számát viszont tudjuk: $\binom{n+k-1}{n-1}$.

□

7. Rekurzív sorozatok

7.1. Definíció

A nem üres *S* halmaz fölötti **s** sorozat **periodikus *t*-től a *p* periódussal**, ha $p \in \mathbf{N}$, $t \in \mathbf{N}_0$, és $\forall (i \in \mathbf{N}_0): s_{t+i+p} = s_{t+i}$. k_p **a *p*-hez tartozó küszöbindex**, ha **s** k_p-től *p* szerint periodikus, és $k_p = 0$ vagy $s_{k_p-1+p} \neq s_{k_p-1}$, az előbbi esetben **a sorozat tisztán periodikus a *p* periódussal**. Az **s** sorozat **periodikus**, ha van legalább egy periódusa. A periodikus **s** sorozat **minimális periódus**a *p*, ha periódusa a sorozatnak, és a sorozat bármely p' periódusára $p \leq p'$.

Δ

7.2. Tétel

Periodikus sorozatnak van egyértelműen meghatározott minimális periódusa, és minden periódushoz egyértelműen meghatározott küszöbindexe. $p' \in \mathbf{N}$ akkor és csak akkor periódusa a sorozatnak, ha $p \mid p'$, ahol *p* a minimális periódus, és ekkor a *p*-hez és p'-höz tartozó *k* illetve k' küszöbindex megegyezik.

Δ

Bizonyítás:

Periodikus sorozatnak van periódusa és ez pozitív egész szám, vagyis ekkor a periódusok halmaza a természetes számok halmazának nem üres részhalmaza. **N** jólrendezett, ezért bármely nem üres részhalmazában van legkisebb elem, ami – ha létezik – egyértelmű, ez igazolja, hogy periodikus sorozatnak van egyértelműen meghatározott minimális periódusa.

Most legyen *p* egy periódus. Ez azt jelenti, hogy van olyan nem negatív egész *t*, hogy minden $i \in \mathbf{N}_0$-ra $s_{t+i+p} = s_{t+i}$. Legyen $K := \left\{ j \in \mathbf{N}_0 \,\middle|\, \forall (i \in \mathbf{N}_0): s_{j+i+p} = s_{j+i} \right\}$. *K* nem üres, hiszen $t \in K$, így $\varnothing \neq K \subseteq \mathbf{N}_0$, ezért létezik *K*-ban legkisebb elem, mondjuk *k*. Ekkor minden nem negatív egész *i*-re $s_{k+i+p} = s_{k+i}$, és ha *k* nem nulla, akkor, így *k* küszöbindex és egyértelmű.

Legyen az **s** periodikus sorozat minimális periódusa *p* a *k* küszöbindexszel. Ekkor tetszőleges *i* nem negatív egészre $s_{k+i+2p} = s_{k+(i+p)+p} = s_{k+(i+p)} = s_{k+i+p} = s_{k+i}$, hiszen $i + p$ is nem egatív egész, ezért a sorozat $2p$ szerint is periodikus. Ha minden, $u \geq 2$-nél nem nagyobb *j* pozitív egészre igaz, hogy jp periódusa a sorozatnak, akkor $s_{k+i+(u+1)p} = s_{k+(i+up)+p} = s_{k+i+up} = s_{k+i}$ bármilyen nem negatív egész *i*-vel, ezért $(u+1)p$ is periódusa **s**-nek, ami mutatja, hogy amennyiben p' a *p*-vel osztható pozitív egész, akkor p' is periódusa a sorozatnak. Fordítva, tegyük fel, hogy p' egy periódus, a hozzá tartozó küszöbindex k', és legyen *t* a *k* és k' maximuma. Ekkor *t* is nemnegatív egész, és $p \leq p'$, hiszen *p* minimális a periódusok halmazában. $p' = qp + r$, ahol *q* pozitív egész, míg *r* *p*-nél kisebb nem negatív egész. Most bármely nem negatív egész *i*-re $s_{t+i} = s_{t+i+p'} = s_{t+i+qp+r} = s_{t+(i+r)+qp} = s_{t+i+r}$, mert a sorozat *t*-től biztosan periodikus mind *p*, mind p' szerint, és $i + r$ nem negatív egész. Azt látjuk, hogy vagy $r = 0$, és ekkor az egyenletsor két végén azonos elem áll, amikor természetes az egyenlőség, vagy *r* is periódusa a sorozatnak. De a második eset $r < p$ miatt lehetetlen, hiszen *p*-nél kisebb periódusa nincs a sorozatnak, így $r = 0$, és ebből $p' = qp$, azaz $p \mid p'$.

Ha $p' = qp$, akkor $s_{k+i+p'} = s_{k+i+qp} = s_{k+i}$, a sorozat *k*-tól biztosan periodikus a p' periódussal, ezért $k' \leq k$. Másrészt biztosan létezik olyan q' pozitív egész, amellyel érvényes a $k' + q'p' \geq k$

egyenlőtlenség. Ekkor $s_{k'+i+p} = s_{k'+i+p+q'p'} = s_{(k'+q'p')+i+p} = {}_{(k'+q'p')+i+p}\, s_{k'+i}$, és így $k' \geq k$. A két egyenlőtlenség alapján $k = k'$.

□

7.3. Következmény

Ha **s** periodikus *k*-tól a *p* periódussal, és a nem negatív egész *i*-vel és *j*-vel $i \equiv j \quad (p)$, akkor $s_{k+i} = s_{k+j}$.

Δ

Bizonyítás:

Az általánosság csorbítása nélkül tekinthetjük úgy, hogy $i \leq j$. Ha $i \equiv j \quad (p)$, akkor alkalmas *q* nemnegatív egész *i*-vel $j = i + qp$, és ekkor $s_{k+j} = s_{k+i+qp} = s_{k+i}$.

□

7.4. Definíció

Egy periodikus sorozat **tisztán periodikus**, ha a küszöbindexe 0.

Δ

Az előzőek szerint egy periodikus sorozat a periódustól függetlenül vagy tisztán periodikus vagy nem tisztán periodikus.

7.5. Definíció

Legyen $b \in \mathbf{N}_0$, és $d \in \mathbf{N}$. $\mathbf{t} = \mathbf{s}^{(b)}$ sorozat az **s** sorozat *b*-**eltoltja**, ha minden *i* indexre $t_i = s_{i+b}$, és $\mathbf{u} = {}^{(d)}\mathbf{s}$ az **s** *d*-**decimáltja**, ha valamennyi nem negatív egész *i*-re $u_i = s_{di}$.

Δ

7.6. Tétel

Legyen *k* és *b* nem negatív egész és *p* pozitív egész. Ha **s** a *k* küszöbtől periodikus a *p* minimális periódussal, akkor $\mathbf{s}^{(b)}$ periodikus a $k' = \max\{0, k-b\}$ küszöbtől a *p* minimális periódussal. Fordítva, ha $\mathbf{s}^{(b)}$ a *k* küszöbtől periodikus a *p* minimális periódussal, akkor **s** periodikus $k+b$-től a *p* minimális periódussal, és ha $k > 0$, akkor $k+b$ az **s** sorozat küszöbindexe.

Δ

Bizonyítás:

a) $k' \geq k-b$, így $k'+b \geq k$. Ekkor $s^{(b)}_{k'+i+p} = s_{k'+i+p+b} = s_{(k'+b)+i+p} = s_{(k'+b)+i} = s_{k'+i+b} = s^{(b)}_{k'+i}$ minden nem negatív egész *i*-vel, tehát $\mathbf{s}^{(b)}$ periodikus k'-től a *p* periódussal.

b) Ha $\forall(i \in \mathbf{N}_0)$-ra $s^{(b)}_{k+i+p} = s^{(b)}_{k+i}$, akkor $s_{(k+b)+i+p} = s_{k+i+p+b} = s^{(b)}_{k+i+p} = s^{(b)}_{k+i} = s_{k+i+b} = s_{(k+b)+i}$, ami pontosan azt jelenti, hogy **s** $k+b$-től periodikus a *p* periódussal.

Az előző két pont alapján egy periodikus sorozatnak és bármely eltoltjának a minimális periódusa megegyezik (ha valamelyiké kisebb, akkor a másik is periodikus ezzel a kisebb periódussal, ami azt jelentené, hogy periodikus egy olyan periódussal, ami kisebb, mint a minimális periódusa).

Ha $k' = 0$, akkor k' nyilván küszöbindex, míg ha $k' = k-b$, és az eltolt sorozat küszöbindexe, $k^{(b)}$, kisebb, mint k', akkor **s** periodikus $k^{(b)} + b < k' + b = k - b + b = k$-tól, ami nem lehetséges.

Az ellenkező irány bizonyításához legyen az eltolt sorozat küszöbindexe pozitív. Ez azt jelen-

ti, hogy $s_{(k+b)-1+p} = s_{k-1+p+b} = s^{(b)}_{k-1+p} \neq s^{(b)}_{k-1} = s_{k-1+b} = s_{(k+b)-1}$, és így az eredeti sorozat küszöbindexe $k+b$.

□

7.7. Következmény

Ha van olyan b és b' nem negatív egész, amelyek közül legalább az egyik pozitív, hogy $\left(\mathbf{s}^{(b)}\right)^{(b')} = \mathbf{s}$, akkor **s** tisztán periodikus a $b+b'$ periódussal. Fordítva, ha **s** tisztán periodikus a p minimális periódussal, akkor tetszőleges b pozitív egészhez van olyan, p-nél kisebb, b' nemnegatív egész, hogy **s** b-eltoltjának b'-eltoltja **s**.

Δ

Bizonyítás:

a) A tétel első felében megfogalmazott feltétel szerint $b+b'$ pozitív egész, továbbá tetszőleges nem negatív egész i-re $s_i = \left(\left(\mathbf{s}^{(b)}\right)^{(b')}\right)_i = s^{(b)}_{i+b'} = s_{i+(b+b')}$, így **s** tisztán periodikus a $b+b''$ periódussal.

b) Legyen $b' = p\left\lceil \frac{b}{p} \right\rceil - b$. Ekkor $\left(\left(\mathbf{s}^{(b)}\right)^{(b')}\right)_i = s_{i+(b+b')} = s_{i+\left\lceil \frac{b}{p} \right\rceil \cdot p} = s_i$ bármely nem negatív egész i-re teljesül, ami éppen a tisztán periodikusság feltétele.

□

7.8. Tétel

k-tól a p periódussal periodikus **s** sorozat d-decimáltja periodikus $\left\lceil \frac{k}{d} \right\rceil$-től a $\frac{p}{(d,p)}$ periódussal (k nem negatív egész és p, d pozitív egész).

Δ

Bizonyítás:

Bármely nem negatív egész i-re

$$
\begin{aligned}
{}^{(d)}s_{\left\lceil \frac{k}{d} \right\rceil + i + \frac{p}{(d,p)}} &= s_{d\cdot\left(\left\lceil \frac{k}{d} \right\rceil + i + \frac{p}{(d,p)}\right)} = s_{d\cdot\left\lceil \frac{k}{d} \right\rceil + d\cdot i + d\cdot\frac{p}{(d,p)}} = \\
= s_{d\cdot\left\lceil \frac{k}{d} \right\rceil + d\cdot i + \frac{d}{(d,p)}\cdot p} &= s_{d\cdot\left\lceil \frac{k}{d} \right\rceil + d\cdot i} = s_{d\cdot\left(\left\lceil \frac{k}{d} \right\rceil + i\right)} = {}^{(d)}s_{\left\lceil \frac{k}{d} \right\rceil + i},
\end{aligned}
$$

hiszen $d\cdot\left\lceil \frac{k}{d} \right\rceil \geq k$.

□

Megjegyezzük, hogy a d-decimált periodikusságából nem következik az eredeti sorozat periodikussága. Ha például **s**-ben s_i akkor és csak akkor 1, ha $i = 2j$ vagy $i = 2\left(\frac{(j+1)j}{2} + 1\right)$, ahol $j \in \mathbf{N}_0$, egyébként 0, akkor ebben a sorozatban a páros indexű tagok mindegyike 1, a sorozat 2-decimáltja konstans sorozat, és így periodikus is. Ugyanakkor az eredeti sorozat nem az, amit a követ-

kező módon láthatunk be. Ha $\sigma^{(j)}$ egy olyan, $2(j+1)$ hosszúságú sorozat, amelyben az 11-et j darab 10 követ, akkor **s** a $\sigma^{(j)}$-k egymás után írásával előálló sorozat. Tegyük fel, hogy **s** k-tól periodikus a p periódussal. Ha j mind k-nál, mind p-nél nagyobb, akkor **s** a $\sigma^{(j)}$-re eső szakaszon periodikus a p periódussal, és $\sigma^{(j)}$ hossza $2(j+1) \geq 2(p+2) = 2p+4 > p+3$, így $\sigma^{(j)}_{p+1} = \sigma^{(j)}_{1+p} = \sigma^{(j)}_1 = 1$ és $\sigma^{(j)}_{p+2} = \sigma^{(j)}_{2+p} = \sigma^{(j)}_2 = 1\ \sigma^{(j)}_{p+2}$, ami lehetetlen, mivel a három kezdő elemtől eltekintve $\sigma^{(j)}$ szomszédos elemei különbözőek. Ugyanígy a decimált sorozatnak mind a küszöbindexe lehet $\left\lceil \frac{k}{d} \right\rceil$-nél kisebb, mind a minimális periódusa $\frac{p}{(d,p)}$-nél kisebb: ha **s** az 10-t követő 1011-ek periodikus ismétlése, akkor **s** a 2 küszöbtől periodikus a 4 minimális periódussal, miközben a 2-decimáltja tisztán periodikus az 1 periódussal.

7.9. Definíció

A nem üres S halmaz feletti **s** végtelen sorozat *m*-**edrendű rekurzív sorozat**, ha $m \in \mathbf{N}_0$, és létezik olyan $\varphi : S^m \to S$ leképezés, hogy minden nem negatív egész i-re $s_{i+m} = \varphi(s_i, \ldots, s_{i+m-1})$. φ **a rekurziós összefüggés**, **rekurziós kapcsolat** vagy **rekurziós szabály**, és m **a rekurzió rendje**. Egy sorozat **rekurzív**, ha legalább egy m-re m-edrendű rekurzív sorozat; a rekurzió **minimális rendje** m, ha a sorozat m-edrendű rekurzív sorozat, de nem létezik olyan m-nél kisebb nem negatív egész m', amellyel a sorozat m'-rendű rekurzív sorozat.

Egy sorozat *k*-**tól** *s*-**sorozat**, ha a $k \in \mathbf{N}_0$ indextől kezdve valamennyi tagja s, és *k*-**tól konstans sorozat**, ha valamilyen s-re k-tól s-sorozat; ha az előbbi k minimális a mondott tulajdonságra, akkor k a **küszöb**, vagyis **s** a k küszöbtől s-sorozat illetve a k küszöbtől konstans sorozat. Amennyiben $k = 0$, akkor egyszerűen *s*-**sorozat**ot illetve **konstans sorozat**ot mondunk. Abban az esetben, ha S-ben van nullelem, és az s-sorozatban s a nullával azonos, akkor használjuk a **nullsorozat** elnevezést is.

Ha **s** m-edrendben rekurzív, úgy $s^{(i)} := (s_i, \ldots, s_{i+m-1})$ **a sorozat** *i*-**edik állapota**. $s^{(0)}$ a **kezdeti** vagy **kezdő állapot**.

Δ

7.10. Tétel

Rekurzív sorozat minimális rekurziós rendje létezik és egyértelmű, és ha a minimális rend m, akkor a sorozat minden $m \leq m' \in \mathbf{N}_0$-ra m'-rendű rekurzív. Rekurzív sorozatot egyértelműen meghatározza kezdő állapota.

Δ

Bizonyítás:

Ha a sorozat rekurzív, akkor a rekurziós rendek halmaza a nem negatív egész számok halmazának nem üres részhalmaza, így tartalmaz egyértelműen meghatározott legkisebb elemet, és ez maga is rekurziós rendje a sorozatnak. Legyen m az előbbiek szerint létező minimális rekurziós rend, φ a hozzá tartozó rekurziós összefüggés, m' az m-nél nem kisebb nem negatív egész, és $\varphi' : S^{m'} \to S$, ahol $\varphi'(u_0, \ldots, u_{m'-m-1}, u_{m'-m}, , u_{m'-1}) := \varphi(u_{m'-m}, , u_{m'-1})$, ha $(u_0, \ldots, u_{m'-m-1}, u_{m'-m}, , u_{m'-1}) \in S^{m'}$. Most tetszőleges $i \in \mathbf{N}_0$ esetén $s_{i+m} = \varphi(s_{i+m'-m}, \ldots, s_{i+m'-1}) = \varphi'(s_i, \ldots, s_{i+m'-m-1}, s_{i+m'-m}, \ldots, s_{i+m'-1})$, hiszen $m' \geq m$ következtében $m' - m \geq 0$, vagyis a sorozat m' renddel is rekurzív.

Ha **s** m-edrendű rekurzív sorozat, akkor $s_m = \varphi(s_0, \ldots, s_{m-1})$, ahol φ a rekurziós kapcsolat, va-

gyis $s^{(0)} = (s_0, \ldots, s_{m-1})$ meghatározza s_m-et, és így $s^{(1)} = (s_1, \ldots, s_m)$-et, azaz a kezdő állapotból megkaptuk $s^{(1)}$-et. Innen indukcióval kapjuk az állítást.

□

7.11. Következmény

Rekurzív sorozat *k*-adik állapota egyértelműen meghatározza a sorozat *k*-nál nem kisebb indexű tagját (*k* nemnegatív egész).

Δ

Bizonyítás:

m-edrendű rekurzív **s** sorozat *b*-eltoltjának *j*-edik állapota az eredeti sorozat $j + b$-edik állapota, hiszen $\left(s^{(b)}\right)^{(j)} = \left(s_j^{(b)}, ..., s_{j+m-1}^{(b)}\right) = \left(s_{j+b}, \ldots, s_{j+b+m-1}\right) = s^{(j+b)}$. Mivel minden sorozatot egyértelműen meghatározza a kezdő állapota, ezért ez igaz **s** *k*-eltoltjára is, $\mathbf{s}^{(k)}$ bármely s_i elemét, de akkor **s** bármely $s_{k+i} = s_{i+k}$ elemét egyértelműen meghatározza $\left(s^{(k)}\right)^{(0)} = s^{(0+k)} = s^{(k)}$.

□

7.12. Tétel

m-edrendű rekurzív sorozat *b*-eltoltja is *m*-edrendű rekurzív sorozat. Visszafelé, ha a *b*-eltolt *m*-edrendű rekurzív sorozat, akkor az eredeti sorozat $m + b$-edrendű rekurzív sorozat.

Δ

Bizonyítás:

a) $s_{i+m}^{(b)} = s_{i+m+b} = \varphi(s_{i+b}, ..., s_{i+m-1+b}) = \varphi\left(s_i^{(b)}, ..., s_{i+m-1}^{(b)}\right)$

b) $$\begin{aligned} s_{i+(m+b)} = s_{i+m+b} = s_{i+m}^{(b)} &= \varphi\left(s_i^{(b)}, ..., s_{i+m-1}^{(b)}\right) = \varphi(s_{i+b}, ..., s_{i+m-1+b}) = \varphi(s_{i+b}, ..., s_{i+m-1+b}) = \\ &= \varphi(s_{i+b}, ..., s_{i+b+m-1}) = \varphi'(s_i, ..., s_{i+b+m-1}) = \varphi'\left(s_i, ..., s_{i+(m+b)-1}\right) \end{aligned}.$$

□

7.13. Tétel

Ha az *S* feletti **s** sorozat periodikus a *k* küszöbindextől a *p* minimális periódussal, akkor **s** rekurzív sorozat, és a rekurzió minimális rendje legfeljebb $k + p$. Fordítva, ha *S* elemeinek száma *q*, és **s** rekurzív sorozat az *m* minimális renddel, akkor a sorozat periodikus, és $p \le p + k \le q^m$, ahol *p* a minimális periódus és *k* a küszöbindex.

Δ

Bizonyítás:

Először legyen $\varphi: S^{k+p} \to S$ olyan, hogy $(w_0, \ldots, w_k, \ldots, w_{k+p-1}) \overset{\varphi}{\mapsto} w_k$ tetszőleges *S* elemeiből álló rendezett $k + p$-esre. Ez valóban S^{k+p}-nek *S*-be való leképezése, hiszen S^{k+p} minden eleméhez *S* egy és csak egy elemét rendeli. Most $s_{i+k+p} = s_{k+i+p} = s_{k+i} = s_{i+k} = \varphi(s_i, \ldots, s_{i+k}, \ldots, s_{i+k+p-1})$ tetszőleges nem negatív egész *i*-re, ami azt jelenti, hogy a sorozat $k + p$ renddel rekurzív.

Másodszor legyen a sorozat *m*-edrendű rekurzív sorozat. Ha egy $0 \le i < j$ re $s^{(i)} = s^{(j)}$, azaz $(s_i, \ldots, s_{i+m-1}) = (s_j, \ldots, s_{j+m-1})$, akkor $s_{i+m} = \varphi(s_i, \ldots, s_{i+m-1}) = \varphi(s_j, \ldots, s_{j+m-1}) = s_{j+m}$, majd ebből az egyenlőségből $s^{(i+1)} = (s_{i+1}, \ldots, s_{i+m}) = (s_{j+1}, \ldots, s_{j+m}) = s^{(j+1)}$, és innen indukcióval tetszőleges *t* nem

negatív egészre $s^{(i+t)} = s^{(j+t)}$, és $s_{i+t+m} = s_{j+t+m}$, vagyis ha u nem negatív egész, akkor $s_{i+u} = s_{j+u}$. Amennyiben S elemeinek száma q, akkor a lehetséges állapotok száma nem lehet nagyobb q^m-nél, ezért biztosan van olyan $0 \le i < j \le q^m$ nem negatív egész, amellyel $s^{(i)} = s^{(j)}$. Ekkor az előzőek felhasználásával minden u nem negatív egészre $s_{i+u} = s_{j+u} = s_{i+(j-i)+u} = s_{i+u+(j-i)}$, ami a $j - i = p'$ jelöléssel azt jelenti, hogy $s_{i+u+p'} = s_{i+u}$, a sorozat legalábbis i-től biztosan periodikus a p' periódussal, tehát $k + p \le i + p' = i + j - i = j \le q^m$. Ez minden rekurziós rendre, tehát a minimális rendre is igaz, viszont a küszöbindex nem negatív, így nyilván teljesül a $p \le k + p$ egyenlőtlenség is.

□

7.14. Tétel

Véges halmaz felett rekurzív sorozat d-decimáltja is rekurzív.

Δ

Bizonyítás:
Véges halmaz felett rekurzív sorozat periodikus, így d-decimáltja periodikus, tehát rekurzív.

□

A decimált sorozat rekurzivitásából nem következik az eredeti sorozat rekurzivitása: korábban már beláttuk, hogy nem periodikus sorozat decimáltja lehet periodikus, tehát rekurzív, ugyanakkor az eredeti sorozat biztosan nem rekurzív, ha a tagjai egy véges halmaz elemei (a sorozat alaphalmaza lehet végtelen is), hiszen a feltétel szerint az eredeti sorozat nem periodikus.

7.15. Definíció

Ha $\mathsf{R} = (R;+,\cdot)$ gyűrű, $m \in \mathbf{N}_0$, és minden nem negatív egész i-re $s_{i+m} = \sum_{j=0}^{m-1} c_j s_{i+j}$ R-beli c_j elemekkel, akkor **s** (R **feletti**) **homogén lineáris rekurzív sorozat**.

Δ

7.16. Megjegyzés

Látható, hogy $m = 0$-val **s** nullsorozat, míg ha $m > 0$, és minden c_i nulla, akkor m-től nullsorozat. Ha viszont $m > 0$ mellett $c_{m-1} = e$, és $m - 1 > i \in \mathbf{N}_0$-ra $c_i = 0$, akkor **s** $m - 1$-től konstans sorozat, és $m = 1$ esetén konstans sorozat.

Δ

7.17. Tétel

Egységelemes gyűrű feletti periodikus sorozat homogén lineáris rekurzív sorozat.

Δ

Bizonyítás:
Legyen az **s** küszöbindexe k és minimális periódusa p, e az egységelem. Ekkor bármely $i \in \mathbf{N}_0$-ra $s_{i+k+p} = s_{k+i+p} = s_{k+i} = s_{i+k} = e \cdot s_{i+k} = \sum_{j=0}^{k+p-1} c_j s_{i+j}$, ahol minden c_t nulla, kivéve a k indexhez tartozót, amely e.

□

7.18. Definíció

Egységelemes gyűrű feletti **s** sorozat **generátorfüggvény**e $S=\sum_{i=0}^{\infty}s_i x^i$. Ha $f=\sum_{i=0}^{m}c_i x^i$ a gyűrű feletti főpolinom, akkor az $s_{i+m}=\sum_{j=0}^{m-1}\left(-c_j\right)s_{i+j}$ rekurzióval generálható sorozatok halmaza $\Omega(f)$, és ha **s** eleme az $\Omega(f)$ halmaznak, úgy *f* **az s sorozat karakterisztikus polinomja**.

Δ

Ha a gyűrű egységelemes, akkor az $s_{i+m}=\sum_{j=0}^{m-1}\left(-c_j\right)s_{i+j}$ rekurziós összefüggéssel megadott *m*-edrendű homogén lineáris rekurzív sorozat átírható a $\sum_{j=0}^{m}c_j s_{i+j}=0$ egyenlőségbe a $c_m=e$ választással. Innen visszafelé azt kapjuk, hogy ha az adott gyűrű feletti **s** homogén lineáris rekurzív sorozat karakterisztikus polinomja $\sum_{i=0}^{m}c_i x^i$, akkor bármely nem negatív egész *i*-re $\sum_{j=0}^{m}c_j s_{i+j}=0$.

7.19. Tétel

Ha R egységelemes gyűrű, $f\in R[x]$ *n*-edfokú főpolinom, és $T:=\left\{\tau\in R[x]\,\middle|\,\delta(\tau)<n\right\}$, akkor $\tau\mapsto\left(f^*\right)^{-1}\tau$ a T unitér jobb oldali R modulus $\Omega(f)$-re való izomorf leképezése.

Δ

Bizonyítás:

Legyen $f=\sum_{i=0}^{n}c_i x^i$, ahol $c_n=e$ R egységeleme, és tekintsünk egy *T*-beli τ polinomot. Mivel *f* főegyütthatója, és így f^* konstans tagja egységelem, tehát egyben egység R-ben, ezért f^* egység az R feletti formális hatványsorok gyűrűjében, ennél fogva van inverze. Legyen *S* az f^* inverzének és τ-nak a (mondott sorrendben vett) szorzata, ekkor $\tau=f^*S=\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}c_{n-j}s_{i-j}\right)x^i$. A feltétel szerint $\delta(\tau)<n$, ezért a jobb oldalon minden $n\le i\in\mathbf{N}_0$-ra a zárójelben álló kifejezés nulla, azaz $n\le i\in\mathbf{N}_0$ esetén $0=\sum_{j=0}^{i}c_{n-j}s_{i-j}=\sum_{j=n-i}^{n}c_j s_{i-n+j}$. Vegyük még figyelembe, hogy amennyiben *t* negatív, akkor $c_t=0$, ezért ha *i* legalább *n*, úgy $\sum_{j=0}^{n}c_j s_{i-n+j}=0$, vagy másként mondva minden nem negatív egész *i*-re $\sum_{j=0}^{n}c_j s_{i+j}=0$, ami $c_n=e$ következtében átrendezés után azt adja, hogy $i\in\mathbf{N}_0$-ra $s_{i+n}=\sum_{j=0}^{n-1}\left(-c_j\right)s_{i+j}$, **s** olyan homogén lineáris rekurzív sorozat, amelynek a karakterisztikus polinomja éppen *f*, azaz $S\in\Omega(f)$. Ez a leképezés injektív: ha $\left(f^*\right)^{-1}\tau_1=\left(f^*\right)^{-1}\tau_2$, akkor $\tau_1=\tau_2$, hiszen f^*, de akkor az inverze is egység, és így nem lehet nullosztó.

Nézzük a szürjektivitást. Ha $S=\sum_{i=0}^{\infty}s_i x^i$ tetszőleges elem $\Omega(f)$-ből, akkor

$$f^*S=\left(\sum_{i=0}^{n}c_{n-i}x^i\right)\left(\sum_{i=0}^{\infty}s_i x^i\right)=\sum_{i=0}^{\infty}\left(\sum_{j=0}^{i}c_{n-j}s_{i-j}\right)x^i=$$

$$=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{i}c_{n-j}s_{i-j}\right)x^i+\sum_{i=n}^{\infty}\left(\sum_{j=0}^{n}c_{n-j}s_{i-j}\right)x^i= \qquad ,$$

$$=\sum_{i=0}^{n-1}\left(\sum_{j=n-i}^{n}c_j s_{(i-n)+j}\right)x^i+\sum_{i=0}^{\infty}\left(\sum_{j=0}^{n}c_j s_{i+j}\right)x^{n+i}=\sum_{i=0}^{n-1}\left(\sum_{j=n-i}^{n}c_j s_{(i-n)+j}\right)x^i=\tau$$

mert ha $t<0$ vagy $t>n$, akkor $c_t=0$, és $\sum_{j=0}^{n} c_j s_{i+j}=0$. Láthatóan τ egy K feletti legfeljebb $n-1$-edfokú polinom, és $S=\left(f^*\right)^{-1}\tau$.

A fentiek szerint a megadott szabály egy $T\to\Omega(f)$ bijekció. Ha τ_1 és τ_2 K feletti legfeljebb $n-1$-edfokú polinom, és c_1, c_2 R eleme, $\left(f^*\right)^{-1}(\tau_1c_1+\tau_2c_2)=\left(\left(f^*\right)^{-1}\tau_1\right)c_1+\left(\left(f^*\right)^{-1}\tau_2\right)c_2$, ami mutatja a művelettartást, és a bijekcióval az izomorfizmust.

□

7.20. Következmény

Ha K test, és $f\in K[x]$ n-edfokú főpolinom, akkor $\Omega(f)$ n-dimenziós lineáris tér K felett. Amennyiben $|K|=q$, akkor $|\Omega(f)|=q^n$.

Δ

Bizonyítás:

A K test feletti legfeljebb $n-1$-edfokú polinomok n-dimenziós lineáris teret alkotnak a test felett, továbbá ha K test, akkor kommutatív, így $K[x]$ is kommutatív, ezért a legfeljebb $n-1$-edfokú polinomok jobb oldali modulusa egyben bal oldali is, de akkor a vele izomorf $\Omega(f)$ is hasonló tulajdonságú. Végül ha $|K|=q$, akkor a τ-polinomok száma q^n.

□

7.21. Tétel

Ha $S\in\Omega(f)$, ahol f m-edfokú, $\mathbf{F}_q$ fölött irreducibilis polinom, $\hat{f}(0)\neq 0$, és α az f gyöke, akkor $s_i=S_{\mathbf{F}_{q^m}|\mathbf{F}_q}\left(\tau\alpha^i\right)$ a q^m-elemű test alkalmas τ elemével. Amennyiben f primitív polinom, és **s** nem a nullsorozat, akkor $s_i=S_{\mathbf{F}_{q^m}|\mathbf{F}_q}\left(\alpha^{r+i}\right)$ valamilyen $0\le r<q^m-1$ egésszel.

Δ

Bizonyítás:

$\hat{f}(0)\neq 0$ biztosítja, hogy $\alpha\neq 0$, míg az irreducibilitás alapján a polinom foka, m, nagyobb nullánál. f irreducibilis m-edfokú polinom $\mathbf{F}_q$ fölött, így $\mathbf{F}_{q^m}=\mathbf{F}_q(\alpha)$, és α első m hatványa (a 0-dikkal kezdve) az $\mathbf{F}_{q^m}$, mint $\mathbf{F}_q$ fölötti m-dimenziós vektortér, bázisa. Van egy és csak egy olyan $T_\tau:\mathbf{F}_{q^m}\to\mathbf{F}_q$ lineáris leképezés, amely α^i-t s_i-be képezi valamennyi $m>i\in\mathbf{N}_0$ indexre, ehhez a leképezéshez viszont létezik az egyértelműen meghatározott $\tau\in\mathbf{F}_{q^m}$, amellyel $T_\tau\left(\alpha^i\right)=S_{\mathbf{F}_{q^m}|\mathbf{F}_q}\left(\tau\alpha^i\right)$. Az eddigiek alapján $m>i\in\mathbf{N}_0$-ra $s_i=S_{\mathbf{F}_{q^m}|\mathbf{F}_q}\left(\tau\alpha^i\right)$. Most legyen minden nem negatív egész i-re $u_i=S_{\mathbf{F}_{q^m}|\mathbf{F}_q}\left(\tau\alpha^i\right)$. Ez minden esetre egy $\mathbf{F}_q$ fölötti sorozat, amelynek első m eleme egybeesik **s** első m elemével. Legyen az eredeti sorozat karakterisztikus polinomja $f=x^m+\sum_{j=0}^{m-1}c_jx^j$, ekkor a rekurziós összefüggés $s_{t+m}=\sum_{j=0}^{m-1}\left(-c_j\right)s_{t+j}$, vagyis $\sum_{j=0}^{m}c_js_{t+j}=0$. Ugyanakkor az is igaz, hogy

$\sum_{j=0}^{m} c_j u_{t+j} = \sum_{j=0}^{m} c_j S_{\mathbf{F}_{q^m}\mid\mathbf{F}_q}\left(\tau\alpha^{t+j}\right) = S_{\mathbf{F}_{q^m}\mid\mathbf{F}_q}\left(\tau\alpha^t \sum_{j=0}^{m} c_j \alpha^j\right) = 0$, hiszen a legutolsó szumma értéke 0, mert α gyöke a polinomnak, és nullának a nyoma 0. Ez azt jelenti, hogy minden *i*-re u_i az $s_0,\ldots,s_{m-1}$ kezdőértékekkel az *f* polinom által generált *m*-edrendű rekurzív sorozat *i*-edik tagja. Mivel egy *m*-edrendű rekurzív sorozatot az első *m* eleme egyértelműen meghatározza, ezért $s_i = u_i = S_{\mathbf{F}_{q^m}\mid\mathbf{F}_q}\left(\tau\alpha^i\right)$.

Végül ha *f* primitív, akkor α primitív elem $\mathbf{F}_{q^m}$-ben, és $\mathbf{F}_{q^m}^*$ minden eleme, így τ is α valamely $q^m - 1 > r \in \mathbf{N}_0$-kitevős hatványa. Most $\tau \neq 0$, hiszen ha τ nulla, akkor **s** a nullsorozat a kikötéssel ellentétben.

□

7.22. Definíció

s minimálpolinomja *m*, ha $S \in \Omega(m)$, és $S \in \Omega(f)$ csak $\deg(m) \leq \deg(f)$ esetén lehet.

Δ

7.23. Tétel

Test fölötti **s** homogén lineáris rekurzív sorozatnak van egyértelműen meghatározott minimálpolinomja, és ha ez *m*, akkor *S* akkor és csak akkor eleme $\Omega(f)$-nek, ha $m \mid f$.

Δ

Bizonyítás:

Test fölötti homogén lineáris rekurzív sorozatnak van karakterisztikus polinomja, és ez főpolinom. Ha a sorozatnak van minimálpolinomja, és igaz az oszthatóságra vonatkozó állítás, akkor abból következik a minimálpolinom egyértelműsége is: ha $m^{(1)}$ és $m^{(2)}$ egyaránt minimálpolinom, akkor a kölcsönös oszthatóság miatt asszociáltak, és mivel minimálpolinom karakterisztikus polinom, vagyis főpolinom, ezért a két polinom meg is egyezik. Azt kell tehát megmutatni, hogy van minimálpolinom, és ez osztója a sorozat karakterisztikus polinomjainak, de csak az ilyen főpolinomoknak.

Legyen $f = x^{i_f} f_1$ K fölötti *n*-edfokú főpolinom, ahol $\hat{f}_1(0) \neq 0$, és $S \in \Omega(m)$. Ekkor $S = \frac{\tau_f}{f^*}$ alkalmas, legfeljebb $n-1$-edfokú $K[x]$-beli polinommal. Ha $d = (\tau_f, f^*)$, akkor *d* osztója f^*-nak, így $\hat{d}(0) \mid \hat{f}^*(0) = e$, tehát *d* konstans tagja nem nulla, és akkor $(d^*)^* = d$. Nem nulla legnagyobb közös osztó csupán asszociált, azaz egy nem nulla konstans szorzó erejéig egyértelmű, legyen ezért *d* konstans tagja *e*, ekkor d^* főpolinom. $d \mid f^*$-ból $d^* \mid (f^*)^* = f_1$. Jelöljük $\frac{f_1}{d^*}$-ot m_1-el, továbbá $\frac{\tau_f}{d}$-t τ_m-el. τ_f egyértelműen írható $\tau_f = uf^* + \tau$ alakban, ahol *u* és τ K feletti polinomok, és τ vagy nulla, vagy $\deg(\tau) < \deg(f^*) = \deg(f_1)$. Legyen $i_m = 0$, ha $u = 0$, egyébként $i_m = \deg(u)+1$, és $m = x^{i_m} m_1$. $m^* = m_1^* = \frac{f_1^*}{d} = \frac{f^*}{d}$, így $S = \frac{\tau_f}{f^*} = \frac{d\tau_m}{dm^*} = \frac{\tau_m}{m^*}$. Ekkor $\tau_m = \frac{\tau_f}{f^*} m^* = um^* + \tau'$, ahol $\tau' = \frac{\tau}{\frac{f^*}{m^*}} = \frac{\tau}{d}$, és ha $\tau \neq 0$, akkor $\deg(\tau') = \deg(\tau) - \deg(d) < \deg(f_1) - \deg(d) = \deg(f_1) - \deg(d^*) = \deg(m_1)$. Ha $\tau_m = 0$, akkor *m* a sorozat karakterisztikus polinomja. Nézzük azt az esetet, amikor $\tau_m \neq 0$. Ekkor *u* és τ' egyike különbözik a nullától. Ha $u = 0$, akkor $\tau' \neq 0$, és $\deg(\tau_m) = \deg(\tau') < i_m + \deg(m_1)$, mert most $i_m = 0$. Ha viszont $u \neq 0$, akkor $\deg(\tau') < \deg(m_1) = \deg(m^*) \leq \deg(u) + \deg(m^*) = \deg(um^*)$, így

$\deg(\tau_m)=\deg(um^*+\tau')=\deg(um^*)=\deg(u)+\deg(m^*)=i_m-1+\deg(m^*)<i_m+\deg(m^*)$, tehát ismét igaz, hogy $\deg(\tau_m)<i_m+\deg(m_1)$. De $i_m+\deg(m_1)=\deg(x^{i_m})+\deg(m_1)=\deg(x^{i_m}m_1)=\deg(m)$, vagyis ha $\tau_m\neq 0$, akkor $\deg(\tau_m)<\deg(m)$, és ez a $\frac{\tau_m}{m^*}=S$ egyenlőséggel igazolja, hogy $S\in\Omega(m)$, m karakterisztikus polinomja **s**-nek.

Ha $g=x^{i_g}g_1$ is karakterisztikus polinomja **s**-nek, ahol $\hat{g}_1(0)\neq 0$, akkor létezik olyan τ_g polinom, hogy $\frac{\tau_g}{g^*}=S=\frac{\tau_m}{m^*}$, azaz $\tau_g m^*=\tau_m g^*$. $(\tau_m,m^*)=\left(\frac{\tau_f}{d},\frac{f^*}{d}\right)$, így τ_m és m^* relatív prímek, hiszen *d* éppen τ_f és f^* legnagyobb közös osztója, ennél fogva m^* osztója g^*-nak, amiből következik, hogy m_1 is osztója g_1-nek. Ha $i_m=0$, akkor nyilván $i_g\geq i_m$, míg ha $i_m>0$, akkor *u*, és így $\tau_m=um^*+\tau'$ nem nulla, ennél fogva $\tau_g\neq 0$, és

$$i_g+\deg(g_1)=\deg(g)>\deg(\tau_g)=\deg(\tau_m)-\deg(m^*)+\deg(g^*)=$$
$$=\deg(u)+\deg(g_1)=i_m-1+\deg(g_1)$$

vagyis $i_g>i_m-1$, ami azonos az $i_g\geq i_m$ relációval, és ez egyben azt is jelenti, hogy *m* osztója *g*-nek. Mivel ez **s** bármely karakterisztikus polinomjára igaz, és osztó foka legfeljebb akkora, mint az osztandó foka, ezért egyben azt is kaptuk, hogy *m* a sorozat minimálpolinomja.

Az előbb már kiderült, hogy a minimálpolinom ugyanezen sorozat valamennyi karakterisztikus polinomjának osztója. Ha viszont $f=hm$ főpolinom, akkor $\frac{h^*\tau_m}{f^*}=\frac{h^*\tau_m}{h^*m^*}=\frac{\tau_m}{m^*}=S$, és

$$\deg(h^*\tau_m)=\deg(h^*)+\deg(\tau_m)<\deg(h)+\deg(m)=\deg(f)$$

feltéve, hogy $\tau_m\neq 0$, tehát $h^*\tau_m\neq 0$. Ez azt jelenti, hogy *f* karakterisztikus polinomja a sorozatnak, vagyis **s** minimálpolinomjának minden főpolinom többszöröse karakterisztikus polinomja **s**-nek.

□

7.24. Következmény

a) a nullsorozatnak és csak a nullsorozatnak *e* a minimálpolinomja

b) ha $\frac{\tau_f}{f^*}=S\in\Omega(f)$, úgy $f=x^{i_f}f_1$ pontosan akkor minimálpolinomja **s**-nek, ha τ_f és f^* relatív prímek, és $i_f=\max\{0,\delta\}$, ahol $\delta=0$, ha τ_f nulla, egyébként $\delta=\deg(\tau_f)-\deg(f^*)+1$

c) nem nulla sorozat irreducibilis karakterisztikus polinomja minimálpolinom

d) bármely *f* főpolinomhoz van olyan sorozat, amelynek *f* a minimálpolinomja.

Δ

Bizonyítás:

a) A nullsorozat homogén lineáris rekurzív sorozat, így van karakterisztikus polinomja. Ha *f* egy karakterisztikus polinom, akkor a sorozat generátorfüggvénye $\frac{0}{f^*}$, így $u=0$ és $d=f^*$, ahonnan $m=e$. Fordítva, ha **s** minimálpolinomja *e*, akkor $S=\frac{\tau}{e}$-ben τ csak 0 lehet, hiszen *e* foka 0, és ha τ nem nulla, akkor a foka kisebb lenne, mint 0, ami lehetetlen, így viszont **s** a nullsorozat.

b) A tétel bizonyítása során láttuk, hogy ha $\tau_f = uf^* + \tau$, és $\tau \neq 0$ esetén $\deg(\tau) < \deg(f^*)$, továbbá *d* a τ_f és f^* (alkalmasan választott) legnagyobb közös osztója, akkor az *m* minimálpolinom $m = x^{i_m} m_1$, ahol $i_m = 0$, ha $u = 0$, egyébként $i_m = \deg(u)+1$, és $m_1 = \frac{f_1}{d^*}$. Innen kapjuk, hogy *f* pontosan akkor esik egybe *m*-mel, vagyis *f* akkor és csak akkor minimálpolinomja a sorozatnak, ha d^*, de akkor egyben *d* konstans, vagyis τ_f és f^* relatív prím, másrészt ha $i_f = i_m$. $\delta > 0$ ekvivalens azzal, hogy $\deg(\tau_f) \geq \deg(f^*)$, ami viszont szükséges és elégséges ahhoz, hogy $u \neq 0$ teljesüljön, ekkor viszont $i_m = \deg(u)+1 = \deg(\tau_f) - \deg(f^*)+1 = \delta$.

c) Ha a sorozat karakterisztikus polinomja *f* és minimálpolinomja *m*, akkor a tétel alapján *m* osztója *f*-nek, ami *f* felbonthatatlanságával csak úgy lehetséges, ha *f* és *m* asszociáltak (mert *m* legalább elsőfokú), és mivel a főegyütthatójuk azonos, ezért meg kell, hogy egyezzenek.

d) Ha *f* a konstans *e* polinom, akkor *f* minimálpolinomja a nullsorozatnak. A többi esethez legyen $\deg(f) = n \geq 1$, $f = x^{i_f} f_1$, $\hat{f}_1(0) \neq 0$, és $\tau = x^{n-1}$, akkor $\deg(\tau) < \deg(f)$, és $\frac{\tau}{f^*} \in \Omega(f)$. τ, mint láttuk, $\tau = uf^* + \sigma$ alakban írható, ahol $\sigma = 0$, vagy $\deg(\sigma) < \deg(f^*)$. Mivel τ és f^* relatív prímek, ezért hasonló igaz σ-ra és f^*-ra, így már csak azt kell belátni, hogy amennyiben $i_f > 0$, akkor $u \neq 0$, és az *u* polinom foka éppen $i_f - 1$. De ha i_f pozitív, vagyis ha $i_f \geq 1$, hiszen i_f egész szám, akkor $\deg(f^*) = \deg(f_1) = \deg(f) - i_f \leq n-1 = \deg(\tau)$, tehát $\tau = uf^* + \sigma$-ban $u \neq 0$, ennek következtében *u*-nak van foka, és $\deg(u) = \deg(\tau) - \deg(f^*) = n - 1 - \deg(f^*) = \deg(f) - \deg(f^*) - 1 = i_f - 1$.

□

7.25. Tétel

Ha a K test feletti **s** sorozat *k*-tól periodikus a *p* periódussal, és $f = x^k(x^p - e)$ $K[x]$-beli polinom, akkor $S \in \Omega(f)$, míg ha $f = x^k f_1 \in K[x]$, és f_1 osztója $x^p - e$-nek, úgy bármely $\Omega(f)$-beli sorozat periodikus *k*-tól a *p* periódussal.

Δ

Bizonyítás:

a) Legyen a sorozat generátorfüggvénye *S*, továbbá $k' = kp$. Mivel $p \in \mathbf{N}$, ezért $kp \geq k$, **s** biztosan periodikus k'-től. Ha $\sigma = \sum_{i=0}^{p-1} s_{k'+i} x^i$, akkor σ legfeljebb $p-1$-edfokú, így $T = \frac{\sigma}{e - x^p}$-ben bármely nem negatív egész *i*-re $t_i = \sigma_{(i \bmod p)} = \sigma_i = s_{k'+i}$, $\mathbf{t} = \mathbf{s}^{(k')}$. Ebből, valamint abból, hogy az eredeti sorozat *k*-tól periodikus a *p* periódussal következik, hogy **t** tisztán periodikus a *p* periódussal, és *k*-tól **s** és **t** azonos, hiszen $t_{k+i} = s_{k+i+k'} = s_{k+i+kp} = s_{k+i}$. Legyen $u = S - T$, akkor az előbb mondottak alapján **u**-ban minden, a *k*-nál nem kisebb *i* indexre $u_i = s_i - t_i = 0$, ezért *u* legfeljebb $k-1$-edfokú polinom. De **s** küszöbindexe *k*, így ha $k > 0$, akkor $u_{k-1} = s_{k-1} - t_{k-1} \neq s_{k-1+p} - t_{k-1+p} = 0$, vagyis $\deg(u) = k-1$, míg ha $k = 0$, akkor **s** és **t** minden indexre megegyezik, és így $u = 0$. Ezek alapján $S = u + T = u + \frac{\sigma}{e - x^p} = \frac{u(e - x^p) + \sigma}{e - x^p} = \frac{\tau}{e - x^p} = \frac{\tau}{\left(x^k(e - x^p)\right)^*}$, ahol $\tau = u(e - x^p) + \sigma$, és ha $\tau \neq 0$, akkor $\deg(\tau) < k + p = \deg(f)$, mert ha $u = 0$, akkor $\tau = \sigma \neq 0$, és így $\deg(\sigma) < p \leq k + p$, míg ha $u \neq 0$, akkor $\deg(\tau) = \deg(u) + p = k - 1 + p < k + p$.

b) $f \mid x^k\left(x^p - e\right) = g$, így g karakterisztikus polinomja **s**-nek, ezért $S = \frac{\tau}{e - x^p} = u + \frac{\sigma}{e - x^p}$, ahol $\tau = ug^* + \sigma$, és $\sigma = 0$, vagy $\deg(\sigma) < p$. Ha $u = 0$, akkor $S = \frac{\sigma}{e - x^p}$, és ez a sorozat tisztán periodikus, tehát *k*-tól is periodikus a *p* periódussal. Amennyiben viszont *u* nem a nullpolinom, akkor $k + p = \deg(g) > \deg(\tau) = \deg(u) + \deg(g^*) = \deg(u) + p$, ezért $\deg(u) < k$, tehát *k*-tól *S* és $\frac{\sigma}{e - x^p}$ megegyezik, ami ismét azt jelenti, hogy *S k*-tól periodikus a *p* periódussal.

□

7.26. Következmény

a) Ha *S* a K test felett periodikus a *k* küszöbtől *p* minimális periódussal, és $\sigma = \sum_{i=0}^{p-1} s_{kp+i} x^i$, akkor a sorozat minimálpolinomja $x^k m_1$, ahol $m_1 = \frac{x^p - e}{\left(\sigma^*, x^p - e\right)}$

b) Ha a K test feletti *S* homogén lineáris rekurzív sorozat minimálpolinomja $x^k m_1$, m_1 osztója $x^p - e$-nek, ahol *p* pozitív egész, de $p > p' \in \mathbf{N}$ esetén nem osztója $x^{p'} - e$-nek, akkor a sorozat periodikus a *k* küszöbtől a *p* minimális periódussal

c) Véges test feletti homogén lineáris rekurzív sorozat minimális periódusa osztója a karakterisztikus polinom rendjének

d) Véges test feletti homogén lineáris rekurzív sorozat minimális periódusa megegyezik minimálpolinomjának rendjével

e) $\mathbf{F}_q$ fölötti *n*-edrendű homogén lineáris sorozat *k* küszöbindexére és *p* minimális periódusára $p \le k + p \le q^n - 1$, eltekintve attól az esettől, amikor $n = 0$, vagy $q = 2$ és $f = x$.

f) Ha $S \in \Omega(f)$, ahol $f \in \mathbf{F}_q[x]$, $\hat{f}(0) \neq 0$, $\deg(f) = n$, és f irreducibilis $\mathbf{F}_q$ fölött, akkor a sorozat tisztán periodikus, és minimális periódusa osztója $q^n - 1$-nek.

Δ

Bizonyítás:

a) Azt már beláttuk, hogy a minimálpolinom $x^{k'} m_1$, ahol $k' \le k$, így még azt kell igazolni, hogy az előbbi relációban egyenlőségnek kell teljesülnie. Ez viszont annak következménye, hogy ha $x^{k'} m_1$ karakterisztikus polinom, akkor a sorozat k'-től periódikus, ahonnan $k' \ge k$, hiszen *k* a küszöbinex.

b) *S k*-tól periodikus a *p* periódussal. Ha a sorozat k'-től periodikus a p' periódussal, akkor karakterisztikus polinomja $x^{k'}\left(x^{p'} - e\right)$, és a minimálpolinom ennek osztója, ami csak úgy lehet, ha $k' \ge k$ és m_1 osztója $x^{p'} - e$-nek, azaz ha $p' \ge p$.

c) Ha $f = x^i f_1$ a karakterisztikus polinom, ahol $\hat{f}_1(0) \neq 0$, és *f* rendje *p*, akkor f_1 osztója $x^p - e$-nek, tehát *p* periódusa a sorozatnak, ugyanakkor a minimális periódus osztója a sorozat bármely periódusának.

d) c) alapján a *p* minimális periódus osztója a rendnek, ha viszont a minimálpolinom $m = x^k m_1$, akkor a) szerint m_1 osztója $x^p - e$-nek, amiből következik, hogy a rend osztója *p*-nek.

e) $p \le k + p$ nyilván igaz. Legyen $f = x^u f_1$ az **s** sorozat karakterisztikus polinomja, ahol $\hat{f}_1(0) \neq 0$, és $n = \deg(f)$. **s** *u*-tól biztosan periódikus, így $k \le u$. $v \le q^v - 1$ bármely $v \in \mathbf{N}_0$ és $1 < q \in \mathbf{N}$ esetén érvényes, és egyenlőség csupán $v = 0$, illetve $v = 1$ és $q = 2$ esetén áll. Ha $u = n$,

akkor $p=1$, és ebből $n=0$, illetve $v=1$ és $q=2$ esetén $n+1>n=q^n-1$, vagyis ilyenkor nem feltétlenül teljesül a $k+p\le q^n-1$ reláció. Amennyiben viszont $n>1$, és vagy $f\neq x$, vagy $q>2$, akkor már $n<q^n-1$, tehát $k+p\le n+1\le q^n-1$.

Most legyen $u<n$, így $q^{n-u}-1\ge 1$, $\deg(f_1)=n-u$, $p\le o(f_1)\le \max\{1,q^{n-u}-1\}=q^{n-u}-1$. Ekkor $p\le k+p\le u+q^{n-u}-1\le q^u-1+q^{n-u}-1\le (q^u-1)q^{n-u}+q^{n-u}-1=q^n-1$, vagyis az egyenlőtlenséglánc lényeges részét kiírva $p\le k+p\le q^n-1$.

f) Mivel $\hat{f}(0)\neq 0$, ezért az $f=x^k f_1$, $\hat{f}_1(0)\neq 0$ alakú felírásban $k=0$, ami mutatja, hogy a sorozat 0-tól periodikus, és így tisztán periodikus. Ami a második állítást illeti, az abból következik, hogy $\mathbf{F}_q$ fölött irreducibilis *n*-edfokú polinom rendje osztója q^n-1-nek.

□

Azt már korábban bizonyítottuk, hogy *q*-elemű halmaz elemeinek *n*-edrendű rekurzív sorozata periodikus, és a *k* küszöbindexre és *p* minimális periódusra teljesül a $p\le k+p\le q^n$ reláció, most ezt élesítettük homogén lineáris rekurzív sorozatokra. Ha csak azt akarjuk belátni, hogy a legalább elsőrendű homogén lineáris sorozatok esetén $p\le q^n-1$, akkor ez lényegesen egyszerűbben is megtehető. Ha a sorozatban előfordul a nullállapot, akkor a homogén lineáris rekurzió következtében minden ez utáni állapot is a nullállapot, vagyis a sorozat minden további eleme 0, a periódus 1, és $n\ge 1$, $q\ge 2$ következtében $q^n-1\ge 2^1-1=1\ge 1$. Ha viszont a sorozatban nem szerepel a nullállapot, akkor az állapotok száma legfeljebb q^n-1, így az első q^n állapot között biztosan előfordul valamelyik legalább kétszer, és a kettő közötti távolság legfeljebb q^n-1.

Az előbb megmutattuk, hogy a *q*-elemű test fölött az *n*-edfokú polinom által generált homogén lineáris rekurzív sorozat minimális periódusa legfeljebb q^n-1. Kérdés, hogy van-e olyan sorozat, amelynek minimális periódusa eléri ezt a felső korlátot, és ha igen, akkor melyek ezek a sorozatok.

7.27. Definíció

A *q*-elemű K test fölötti **s** *n*-edrendű homogén lineáris rekurzív sorozat **maximális periódusú**, ha nem a nullsorozat és nem az 1 indextől nulla bináris sorozat, és minimális periódusa q^n-1.

Δ

7.28. Tétel

$\mathbf{F}_q$ fölötti *n*-edrendű homogén lineáris rekurzív sorozat pontosan akkor maximális periódusú, ha minimálpolinomja *n*-edfokú primitív polinom $\mathbf{F}_q$ fölött. Maximális periódusú sorozat tisztán periodikus.

Δ

Bizonyítás:

$\mathbf{F}_q$ feletti homogén lineáris rekurzív sorozat periodikus, minimális periódusa a minimálpolinom rendje, amely legfeljebb $\max\{1,q^n-1\}$, és pontosan akkor q^n-1, ha $q=2$ és $m=x$, vagy ha *m* primitív polinom. Ám az első eset azt a bináris sorozatot generálja, amelynek első elem *e*, az összes többi 0.

Maximális periódusú sorozatra $k+p\le q^n-1=p$, és $k\ge 0$, így *k* valóban nulla.

□

7.29. Tétel

Ha a K test feletti **s** homogén lineáris rekurzív sorozat karakterisztikus polinomja $f = x^u f_1$, ahol $\hat{f}_1(0) \neq 0$, b nem negatív egész, és $v = \max\{0, u-b\}$, akkor $\mathbf{t} = \mathbf{s}^{(b)}$ karakterisztikus polinomja $f = x^v f_1$. Fordítva, ha a b-eltolt karakterisztikus polinomja $x^v f_1$, akkor az eredeti sorozatnak $f = x^{v+b} f_1$ karakterisztikus polinomja.

Δ

Bizonyítás:

Legyen $\deg(f) = n$, $f = x^u f = x^u \sum_{i=0}^{n-u} c_i x^i = \sum_{i=u}^{n} c_{i-u} x^i$, $c_{n-u} = e$, és $r = \min\{u, b\}$. Ekkor $r \leq u \leq n$, így

$$t_{i+(n-r)} = s_{i+n-r+b} = s_{i-r+b+b} = \sum_{j=u}^{n-1} \left(-c_{j-u}\right) s_{i-r+b+j} =$$

$$= \sum_{j=u}^{n-1} \left(-c_{j-u}\right) s_{i-r+j+b} = \sum_{j=u}^{n-1} \left(-c_{j-u}\right) t_{i-r+j} = \sum_{j=u-r}^{n-r-1} \left(-c_{j-u+r}\right) t_{i+j}$$

tehát $\sum_{i=u-r}^{n-r} c_{i-u+r} x^i = x^{u-r} \sum_{i=0}^{n-u} c_i x^i = x^{u-r} f_1$ karakterisztikus polinomja **t**-nek. Mind u, mind b nem negatív, így r is az, és $-r = \max\{-u, -b\}$, innen $u - r = \max\{u-u, u-b\} = \max\{0, u-b\} = v$.

Most tegyük fel, hogy **t** karakterisztikus polinomja $f = \sum_{i=v}^{n} c_{i-v} x^i$ Ekkor

$$s_{i+(n+b)} = t_{i+n} = \sum_{j=v}^{n-1} \left(-c_{j-v}\right) t_{i+j} = \sum_{j=v+b}^{n+b-1} \left(-c_{j-v-b}\right) s_{i+j} = \sum_{j=v}^{n-1} \left(-c_{j-v}\right) s_{i+j+b},$$

ami mutatja, hogy **s**-nek karakterisztikus polinomja $\sum_{i=v+b}^{n+b} c_{i-(v+b)} x^i = x^b \sum_{i=v}^{n} c_{i-v} x^i = x^b f$.

□

7.30. Kiegészítés

a) Ha **s** minimálpolinomja $m = x^k m_1$, ahol $\hat{m}_1(0) \neq 0$, és $k' = \max\{0, k-b\}$, akkor $\mathbf{s}^{(b)}$ minimálpolinomja $m^{(b)} = x^{k'} m_1$, és $m^{(b)} \mid m$.

b) Ha **s** tisztán periodikus, akkor **s** és $\mathbf{s}^{(b)}$ minimálpolinomja megegyezik.

Δ

Bizonyítás:

a) $m^{(b)}$ karakterisztikus polinomja az eltoltnak, így az eltolt minimálpolinomja osztója $m^{(b)}$-nek. Ha a minimálpolinom $x^u m'$, akkor egyrészt $0 \leq u \leq k'$ és m' osztója m_1-nek, másrészt az eredeti sorozatnak karakterisztikus polinomja $x^{u+b} m'$, ahonnan $u + b \geq k$ és $m_1 \mid m'$. A két oszthatóságból $m' = m_1$ (mert mindkettő főpolinom), és $k' = \max\{0, k-b\} \leq u \leq k'$, tehát $u = k'$, $m^{(b)}$ az $\mathbf{s}^{(b)}$ minimálpolinomja.

b) Ha **s** tisztán periodikus, akkor $k = 0$, és akkor k' is 0, tehát $k' = k$.

□

7.31. Tétel

Ha az $\mathbf{F}_q$ fölötti *n*-edrendű maximális periódusú **s** sorozat minimálpolinomja *m*, és **0** a nullsorozat, akkor $\Omega(m)=\{\mathbf{0}\}\cup\left\{\mathbf{s}^{(b)}\,\middle|\, q^n-1>b\in\mathbf{N}_0\right\}$, és $\mathbf{s}^{(b)}$ minden *b*-re *n*-edrendű maximális periódusú.

Δ

Bizonyítás:

Maximális periódusú sorozat tisztán periodikus, így $\mathbf{s}^{(b)}\in\Omega(m)$, másrészt $s_{i+b}=s_{i+b'}$ akkor és csak akkor teljesül, ha $b\equiv b'\ (p)$, ahol *p* a sorozat minimális periódusa, azaz ha $b\equiv b'\ (q^n-1)$, ezért a $0\le b<q^n-1$ eltoláshoz tartozó $\mathbf{s}^{(b)}$ sorozatok páronként különbözőek, és minden eltolt sorozat ezek valamelyikével azonos. Az eltolt sorozatok száma q^n-1, és éppen ennyi $\Omega(m)$-ben a nullától különböző sorozatok száma, ezért a megadott két halmaz azonos.

Homogén lineáris rekurzív sorozat minimális periódusát a minimálpolinom egyértelműen meghatározza, így igaz a másik állítás is.

□

7.32. Tétel

Legyen **s** az $\mathbf{F}_q$ fölötti *n*-edrendű maximális periódusú sorozat, $r\in\mathbf{N}$, $c^{(r)}=(c_0,\ldots,c_{r-1})$ $\mathbf{F}_q$ fölötti tetszőleges *r*-es. Ekkor a sorozat egy periódusában $c^{(r)}$ előfordulási gyakorisága q^{n-r}, ha $r\le n$ és legalább egy indexre $c_i\neq 0$, $q^{n-r}-1$, ha $r\le n$ és valamennyi *i*-re $c_i=0$, míg $r>n$ esetén vagy nulla, vagy 1.

Δ

Bizonyítás:

Legyen először $r\le n$. Mivel egy maximális periódusú sorozatban a nullától különböző minden állapot pontosan egyszer fordul elő, ezért könnyen látható, hogy kölcsönösen egyértelmű megfeleltetés létesíthető az egy periódusban található $c^{(r)}$-sorozatok, valamint a sorozat azon állapotai között, amelyekben az első *r* elem éppen $c^{(r)}$, így annyi ilyen sorozat van egy periódusban, ahányféleképpen az állapot utolsó $n-r$ eleme választható. Az ilyen választások száma q^{n-r}, kivéve azt az esetet, amikor az állapot valamennyi eleme 0, azaz amikor mind $c^{(r)}$ minden eleme, mind a további elemek mindegyike nulla, ez indokolja ebben az esetben a -1-es korrekciót.

Mint korábban bizonyítottuk, *n*-edrendű rekurzív sorozatban bármely *n* egymás utáni elem meghatározza az összes utána következőt, így ha $r>n$, és $c^{(r)}$ első *n* eleme $c^{(r)}$-t generálja, akkor $c^{(r)}$ egyszer szerepel a sorozatban egy adott periódusba eső kezdőponttal, míg ha az utolsó $r-n$ elem nem felel meg az elől álló *n* elemnek, akkor egyszer sem, ide sorolva a csupa 0-ból álló $c^{(r)}$-t is, mert bár ez generálódna az első *n* elemből, de a sorozatban nem szerepel.

□

7.33. Tétel

Legyen **s** az $\mathbf{F}_q$ fölötti *n*-edrendű maximális periódusú sorozat, és $r\in\mathbf{N}_0$. Ekkor tetszőleges *t* nem negatív egészre $k(r):=\dfrac{1}{q^n-1}\sum_{i=0}^{q^n-2}\kappa(s_{t+i})\overline{\kappa}(s_{t+i+r})=-\dfrac{1}{q^n-1}$, ha *r* nem osztható a periódussal, egyébként 1 (κ a test kanonikus additív karaktere).

Δ

Bizonyítás:

$\kappa(s_{t+i})\overline{\kappa}(s_{t+i+r}) = \kappa(s_{t+i} - s_{t+i+r}) = \kappa(s_{t+i+b})$ valamilyen $q^n - 1$-nél kisebb nem negatív egészszel, ha *r* nem többszöröse a periódusnak, egyébként κ argumentuma minden indexre 0, hiszen a második kifejezésben két ugyanazon primitív polinommal generált sorozat lineáris kombinációja áll. Nézzük az első esetet. Ha most egy teljes periódusra összegzünk, és a sorozathoz hozzáadunk $\kappa(0)$-t, akkor ez egy olyan összeg, ahol κ argumentumaként a test valamennyi eleme ugyanannyiszor fordul elő, ezért az összeg 0 (mert kanonikus karakter nem főkarakter), így ismét levonva $\kappa(0) = 1$-et, kapjuk az első eredményt. A második abból adódik, hogy ekkor csupa 1-et adunk össze.

□

7.34. Megjegyzés

Az előbbi két tétel közül az első alapján véges test feletti *n*-edrendű maximális periódusú sorozatban minden nem nulla elem azonos gyakorisággal fordul elő, míg a nulla eggyel kevesebbszer, továbbá tetszőleges, *n*-nél rövidebb sorozat után bármely elem ugyanazon valószínűséggel következik, kivéve a csupa 0-t követő 0, és ez is csak eggyel kisebb gyakorisággal található a sorozatban. A másik tétel szerint a sorozat korreláltsága nem függ a távolságtól, ha ez a távolság nem a periódus többszöröse.

Δ

Ha megadjuk egy *n*-edrendű homogén lineáris rekurzív sorozat első *n* elemét és a rekurziós összefüggés *n* együtthatóját, akkor ebből a sorozat valamennyi eleme számolható, vagyis ez a $2n$ adat egyértelműen meghatározza a teljes sorozatot. Ebből arra gondolhatunk, hogy egy ilyen sorozat $2n$ egymás utáni elemének ismerete elegendő információt tartalmaz a teljes további sorozatról, így nem meglepő az alábbi

7.35. Tétel

Test fölötti *n*-edrendű homogén lineáris rekurzív sorozat $2n$ egymás utáni elemének ismeretében a sorozat tetszőleges további eleme egyértelműen meghatározható. Ha *n* a minimális rend, akkor ennél kevesebb elemmel az egyértelműség nem teljesül.

Δ

Bizonyítás:

Mivel a sorozat *n*-edrendű homogén lineáris rekurzív sorozat, ezért egy $s_{i+n} = \sum_{j=0}^{n-1} c_j s_{i+j}$ alakú rekurziós összefüggéssel generálható, ahol *i* tetszőleges nem negatív egész, és az *n* darab c_j együttható egyelőre ismeretlen. Tegyük fel, hogy az $r \in \mathbf{N}_0$ indextől kezdve ismerjük a sorozat $2n$ számú egymás után következő $s_r, \ldots, s_{r+2n-1}$ elemét. Most $n > t \in \mathbf{N}_0$-ra $\sum_{j=0}^{n-1} s_{r+t+j} x_j = s_{r+t+n}$ egy *n* egyenletből álló *n*-ismeretlenes lineáris egyenletrendszer, amely megoldható, hiszen egy megoldása például $c_0, \ldots, c_{n-1}$. Legyen valamelyik megoldás $b_0, \ldots, b_{n-1}$. Ekkor egyrészt $\sum_{j=0}^{n-1} b_j s_{r+t+j} = s_{r+t+n}$ minden $n > t \in \mathbf{N}_0$ esetén, hiszen éppen így határoztuk meg a b_i együtthatókat, másrészt

$$\sum_{j=0}^{n-1} b_j s_{r+n+j} = \sum_{j=0}^{n-1} \left(b_j \sum_{t=0}^{n-1} c_t s_{r+j+t} \right) = \sum_{t=0}^{n-1} \left(c_t \sum_{j=0}^{n-1} b_j s_{r+t+j} \right) = \sum_{t=0}^{n-1} c_t s_{r+n+t} = s_{r+2n},$$

ezért a $\sum_{j=0}^{n-1} b_j s_{r+t+j} = s_{r+t+n}$ rekurziós összefüggés $t = n$-re és innen indukcióval bármely $t \in \mathbf{N}_0$-ra is érvényes.

$2n$-nél kevesebb tagot ismerve $n > 0$, és *n*-nél kevesebb egyenlet írható fel, viszont ha a rekurzió minimális rendje *n*, úgy a minimálpolinomban *n* ismeretlen van, és minden, a sorozatot generáló karakterisztikus polinom megadásához legalább ennyi együttható meghatározása szükséges. Ekkor tehát a rekurziós összefüggésben legalább egy együtthatót szabadon választunk. Ha két azonos fokszámú főpolinom egyikében egyetlen együtthatót szabadon választunk, akkor van olyan választás is, ahol a két polinom nem azonos és így nem is asszociált (hiszen a főegyütthatók azonosak). Ebben az esetben viszont a két polinom különböző sorozatot generál, mert ellenkező esetben nem lenne egyértelmű a sorozat minimálpolinomja.

□

Bizonyos esetekben az előbbi tulajdonság nem kívánatos, például a rejtjelezésben inkább olyan sorozatra van szükségünk, amely rendelkezik az álvéletlen sorozatok tulajdonságaival, de az előrejelzés minél bonyolultabb. Ezen bonyolultság egy lehetséges mértéke az, hogy mekkora *n*-el tudjuk az adott sorozatot mint homogén lineáris rekurzív sorozatot generálni. Ez persze véges test és nem periodikus sorozat esetén nem lehetséges, de bármely *k* nemnegatív egészre az első *k* elemből álló szegmensre már igen (másrészt véges test feletti rekurzív sorozat biztosan periodikus). Ez indokolja az alábbi definíciót.

7.36. Definíció

A K test feletti **s** sorozat *k* hosszúságú kezdőszeletének **lineáris komplexitás**a $L_k(\mathbf{s})$, ha van olyan K feletti $L_k(\mathbf{s})$-rendű homogén lineáris rekurzív sorozat, amelynek első *k* eleme azonos **s** első *k* elemével, de $L_k(\mathbf{s})$-nél kisebb renddel nincs ilyen sorozat. **s** lineáris komplexitása az $\{L_k(\mathbf{s}) | k \in \mathbf{N}_0\}$ halmaz felső határa, feltéve, hogy a felső határ létezik, egyébként ∞.

Δ

Mivel az $L_k(\mathbf{s})$ értékek nem negatív egészek, ezért ha a megadott halmaz korlátos, akkor van benne maximális elem, tehát létezik a felső határ, míg ha nem korlátos, akkor nincs felső határa.

A sorozat elemeit 0-tól indexeljük, így az első *k* elem a $0 \le i \le k-1$ indexeket jelenti. A definícióból látszik, hogy $L_k(\mathbf{s})$ a megfelelő minimálpolinom foka.

Célunk a továbbiakban, hogy becslést adjunk a lineáris komplexitásra. Test feletti sorozatokat vizsgálunk, és a *k* hosszúságú kezdőszeletet generáló minimálpolinomot $m^{\langle k \rangle}$-val, az általa generált homogén lineáris rekurzív sorozatot $\mathbf{s}^{\langle k \rangle}$-val jelöljük. Amennyiben nyilvánvaló, hogy melyik sorozatról van szó, akkor $L_k(\mathbf{s})$ helyett egyszerűen L_k-t írunk.

7.37. Tétel

Egy sorozat lineáris komplexitása minden $k \in \mathbf{N}_0$-ra egyértelműen meghatározott. $0 \le L_k \le k$, minden $k \ge t \in \mathbf{N}_0$-hoz van olyan **s** sorozat, amelyre $L_k(\mathbf{s}) = t$, továbbá ha $0 \le u < v$, akkor $L_u \le L_v$, .

Δ

Bizonyítás:

Véges hosszúságú sorozatunkat a szakasz állandó ismétlésével periodikussá téve lehetséges a homogén lineáris rekurzió úgy, hogy a generált sorozat k hosszúságú kezdőszelete éppen a megadott sorozat, így a definícióban szereplő rendek halmaza a nem negatív egészek halmazának nem üres részhalmaza, amelyben van egyértelműen meghatározott legkisebb elem.

A nullsorozat 0-adrendű rekurzióval is generálható, így ha a sorozat első *k* eleme 0, akkor $L_k = 0$. Most nézzük azt a sorozatot, amelyben minden elem 0, kivéve a *t* indexhez tartozót. Mivel a nullák bármely lineáris kombinációja 0, ezért s_t nem állítható elő az előtte álló *t* darab s_i-ből lineáris rekurzióval, tehát $L_k > t$. Ugyanakkor az x^{t+1} polinom által meghatározott homogén lineáris rekurzív sorozat minden eleme 0 a $t+1$ indextől kezdve, tehát ettől a ponttól a generált sorozat megegyezik **s**-sel. Ha ebben a homogén lineáris rekurzív sorozatban a szabadon választható első $t+1$ elem 0, kivéve a $t+1$ indexhez tartozót, amely azonos **s** ugyanezen pozíciójában álló elemével, akkor a két sorozat teljesen megegyezik, tehát az első *k* elemük is azonos, így viszont $L_k \le t+1$, és akkor $L_k = t$.

Ha az első *v* elem generálható egy összefüggéssel, akkor az egyben az első *u* elemet is helyesen generálja, tehát valóban fennáll az egyenlőtlenség.

□

7.38. Tétel

Ha **s** és **t** test fölötti sorozatok, és *a*, *b* a test eleme, akkor $L_k(a\mathbf{s}+b\mathbf{t}) \le L_k(\mathbf{s}) + L_k(\mathbf{t})$.

Δ

Bizonyítás:

Ha az **s** sorozat kezdő *k* hosszúságú szeletének lineáris komplexitása $L_k(\mathbf{s})$, akkor van olyan $L_k(\mathbf{s})$-rendű $\mathbf{s}^{\langle k\rangle}$ homogén lineáris rekurzív sorozat, amelynek első *k* eleme megegyezik **s** első *k* elemével, és ugyanez igaz az **s** és **t** felcserélésével a másik sorozatra is. Az előbbi két sorozattal az is teljesül, hogy a $k > i \in \mathbf{N}_0$ indexekre $a\mathbf{s}+b\mathbf{t}$ és $a\mathbf{s}^{\langle k\rangle} + b\mathbf{t}^{\langle k\rangle}$ megegyezik, vagyis ha *f* karakterisztikus polinomja $a\mathbf{s}^{\langle k\rangle} + b\mathbf{t}^{\langle k\rangle}$-nak, akkor $L_k(a\mathbf{s}+b\mathbf{t}) \le \deg(f)$. Legyen a két homogén lineáris rekurzív sorozat minimálpolinomja $m_{\mathbf{s}}^{\langle k\rangle}$ és $m_{\mathbf{t}}^{\langle k\rangle}$. Ekkor $m_{\mathbf{s}}^{\langle k\rangle}$ foka $L_k(\mathbf{s})$, $m_{\mathbf{t}}^{\langle k\rangle}$ foka $L_k(\mathbf{t})$, és $m_{\mathbf{s}}^{\langle k\rangle} m_{\mathbf{t}}^{\langle k\rangle}$ foka $L_k(\mathbf{s}) + L_k(\mathbf{t})$. $m_{\mathbf{s}}^{\langle k\rangle} m_{\mathbf{t}}^{\langle k\rangle}$ karakterisztikus polinomja mind $\mathbf{s}^{\langle k\rangle}$-nak, mind $\mathbf{t}^{\langle k\rangle}$-nak, de akkor ezen két sorozat bármely lineáris kombinációjának, így $a\mathbf{s}^{\langle k\rangle} + b\mathbf{t}^{\langle k\rangle}$-nak is, amiből az előzőek alapján következik a tételben megadott egyenlőtlenség.

□

7.39. Tétel

Ha $m^{\langle k\rangle}$ helytelenül generálja **s** $k+1$-edik elemét, akkor $L_{k+1} = \max\{L_k, k+1-L_k\}$.

Δ

Bizonyítás:

Legyen $\delta_k = s_k - s_k^{\langle k\rangle}$. A feltétel szerint az $\mathbf{u} = \mathbf{s} - \mathbf{s}^{\langle k\rangle}$ sorozat első *k* eleme 0, míg a $k+1$-edik éppen $u_k = \delta_k \ne 0$. Ekkor

$$k+1 = L_{k+1}(\mathbf{u}) = L_{k+1}(\mathbf{s}-\mathbf{t}) \le L_{k+1}(\mathbf{s}) + L_{k+1}(\mathbf{t}) = L_{k+1} + L_k$$

hiszen $s_k^{\langle k\rangle}$-t is $m^{\langle k\rangle}$ generálja, vagyis $L_{k+1} \ge k+1-L_k$, és korábban már beláttuk, hogy $L_{k+1} \ge L_k$.

Most megmutatjuk az ellenkező irányú egyenlőtlenséget azáltal, hogy megadunk egy olyan $L = \max\{L_k, k+1-L_k\}$-fokú polinomot, amely helyesen generálja **s**-nek valamennyi elemét a *k* indexűig, beleértve még ezt a tagot is.

A bizonyítás indukcióval történik. A nulla hosszúságú kezdőszeletre nyilván vehető $L_0 = 0$ és $m^{\langle 0\rangle} = e$, ahol *e* a test egységeleme. Ez a polinom mindaddig helyesen generálja a sorozatot, amíg a

sorozat tagjai 0-k. Legyen a sorozatban az első nem nulla elem az u indexnél (ez tehát az $u+1$-edik elem!), akkor L_u még 0, $m^{\langle 0\rangle}=e$, míg $L_{u+1}=u+1=\max\{0,u+1\}=\max\{L_u,u+1-L_u\}$, továbbá $m^{\langle u+1\rangle}=x^{u+1}$ egy alkalmas minimálpolinom (de tetszőleges $u+1$-edfokú főpolinom megfelel, így látható, hogy míg a lineáris komplexitás egyértelmű, tehát a polinom foka is, addig maga a polinom nem). Tegyük fel, hogy az $u+1\le k$ esetekben $m^{\langle k\rangle}$ helyesen állítja elő az **s** sorozat első k elemét, de a $k+1$-ediket, azaz s_k-t egy $\delta_k\neq 0$ hibával. Mivel $L_0=0$, de a feltétel szerint $L_k\ge L_{u+1}>0=L_0$, ezért kell lennie olyan $u\le t<k$ indexnek, hogy $L_{t+1}=\max\{L_t,t+1-L_t\}\neq L_t$, vagyis $L_{t+1}=t+1-L_t$, és ha az ilyen indexek maximuma r, akkor tehát $L_k=L_{r+1}=r+1-L_r$. Ebből az is következik, hogy $m^{\langle r\rangle}$ az s_r-t a megelőző elemekből egy $\delta_r\neq 0$ eltéréssel generálta. Nézzük az

$$m=x^{L-L_k}m^{(k)}-\delta_k\delta_r^{-1}x^{L-(k+1-L_k)}m^{(r)}=\sum_{i=0}^{L_k}c_i^{(k)}x^{i+(L-L_k)}-\delta_k\delta_r^{-1}\sum_{i=0}^{L_r}c_i^{(r)}x^{i+(L-(k+1-L_k))}$$

polinomot. Az első rész egy L-edfokú polinom, míg a második $L-(k-r)<L$-edfokú, hiszen $\delta_k\delta_r^{-1}\neq 0$, és $L_k=L_{r+1}=r+1-L_r$-ből $L_r+(L-(k+1-L_k))=L-(k-r)$, ahol $r<k$. Ez azt jelenti, hogy m egy L-edrendű homogén lineáris rekurzív sorozat karakterisztikus polinomja, és pontosan akkor generálja **s** első $k+1$ elemét, ha bármely $k-L\ge i\in\mathbf{N}_0$-ra

$$\begin{aligned}&\sum_{j=0}^{L_k}c_j^{(k)}s_{i+j+(L-L_k)}-\delta_k\delta_r^{-1}\sum_{j=0}^{L_r}c_j^{(r)}s_{i+j+(L-(k+1-L_k))}=\\&=\sum_{j=0}^{L_k}c_j^{(k)}s_{i+j+(L-L_k)}-\delta_k\delta_r^{-1}\sum_{j=0}^{L_r}c_j^{(r)}s_{i+j+((L-L_r)-(k-r))}=0\end{aligned}.$$

Adott i-re **s** legnagyobb indexe az első összegben $u=i+L_k+L-L_k=i+L$, míg a másodikban hasonló számítással $v=i+L-k+r$. Ha $i<k-L$, akkor tehát $u<k$, $v<r$, így mindkét összeg nullát ad. Maradt az $i=k-L$ eset, vagyis amikor $u=k$ és $v=r$. Ekkor az első összeg az s_k-nak és az $m^{\langle k\rangle}$ által generált $\mathbf{s}^{\langle k\rangle}$ sorozat k indexű tagjának, $s_k^{\langle k\rangle}$-nak a különbsége, vagyis δ_k, míg a szumma előtt álló tényező nélkül a második összeg hasonló módon δ_r-et ad, így a teljes összeg értéke ismét 0. Ez azt bizonyítja, hogy m egy olyan karakterisztikus polinom, amely helyesen generálja az **s** sorozatot a $k\ge i\in\mathbf{N}_0$ indexekre. Ebből következik, hogy $L_{k+1}\le L$, és mivel korábban beláttuk az ellenkező irányú egyenlőtlenséget, ezért $L_{k+1}=L$.

□

Ismét hangsúlyozzuk, hogy míg a lineáris komplexitás értéke, tehát L_k egyértelműen meghatározott, addig egy alkalmas $m^{\langle k\rangle}$ polinomra ez általában nem igaz, hiszen nyilvánvalóan több olyan L_k-rendű homogén lineáris rekurzív sorozat létezik, amelynek az első k tagja azonos.

Függelék

Tétel

Legyen $\mathsf{G} = (G;\cdot)$ csoport, *g* a csoport *n*-edrendű eleme, és *e* a csoport egységeleme . Ekkor

a) tetszőleges $u \in \mathbf{Z}$-re $g^u = e$ akkor és csak akkor, ha $n \mid u$

b) bármely *u* és *v* egész számra $g^u = g^v$ akkor és csak akkor, ha $u \equiv v \quad (n)$

c) $n > k \in \mathbf{N}_0$-ra a g^k elemek páronként különbözőek, és minden *m* egész számhoz van olyan egyértelműen meghatározott $n > j \in \mathbf{N}_0$, hogy $g^m = g^j$

d) $\left| g^m \right| = \dfrac{n}{(m,n)}$

e) $\left| g^m \right| = |g| \Leftrightarrow (m,n) = 1$, és ekkor tetszőleges *k* egész számra $\left| \left(g^k\right)^m \right| = \left| g^k \right|$

f) ha G véges csoport, akkor $n \mid |G|$

g) tetszőleges *u* és *v* egész számra $\left| g^{uv} \right| \mid \left(\left| g^u \right|, \left| g^v \right| \right)$

Δ

Bizonyítás:

a) Ha $n \mid u$, akkor $u = r\,n$ egy *r* egész számmal, és ekkor $g^u = g^{r\,n} = \left(g^n\right)^r = e^r = e$. Fordítva, legyen $g^u = e$. Ha $u = rn + s$, ahol $n > s \in \mathbf{N}_0$, akkor $e = g^u = g^{r\,n+s} = \left(g^n\right)^r g^s = g^s$. Mivel *n* a legkisebb pozitív egész, amely kitevős hatványa *g*-nek az egységelem, ezért *s* nem lehet pozitív egész szám, így $s = 0$, de akkor $u = r\,n$, azaz $n \mid u$.

b) $g^u = g^v$-ből $g^{v-u} = g^0 = e$, és így a) alapján $n \mid v - u$, azaz $u \equiv v \quad (n)$.

c) Ha *i* és *j* olyan egész számok, hogy $0 \le i < j < n$, akkor $0 < j - i < n$, így, ha $n \mid j - i$, akkor $i = j$, amiből következik az állítás első fele, míg a második egyszerű következménye annak, hogy bármely *u* egész számra $0 \le (u \mod n) \equiv u \quad (n)$, és $(u \mod n)$ egyértelműen meghatározott.

d) $e = \left(g^m\right)^l = g^{m \cdot l}$ akkor és csak akkor igaz az *l* egész számra, ha $n \mid ml$, ami viszont pontosan akkor teljesül, ha $\dfrac{n}{(m,n)} \Big| l$. A legkisebb ilyen tulajdonságú pozitív egész $\dfrac{n}{(m,n)}$, tehát ez lesz g^m rendje.

e) Az előbbi pont alapján $\left| g^m \right| = \dfrac{n}{(m,n)}$, és ez pontosan akkor egyenlő *n*-nel, ha a nevező 1. Az állítás második fele pedig következik abból, hogy ha $(m,n) = 1$, akkor $(km,n) = (k,n)$.

f) Ez következik a Lagrange-tételből, amely szerint véges csoport részcsoportjának rendje és indexe osztója a csoport rendjének.

g) Legyen g^u, g^v és g^{uv} rendje az előbbi sorrendben *r*, *s* és *t*. Ekkor $\left(g^v\right)^s = e$, így $e = e^u = \left(\left(g^v\right)^s\right)^u = g^{suv} = \left(g^{uv}\right)^s$, tehát $t \mid s$. Hasonlóan kapjuk a $t \mid r$ oszthatóságot, amiből következik a $t \mid (r,s)$ oszthatóság is.

□