Doktori értekezés

KÉT ELEMMEL GENERÁLHATÓ SPECIÁLIS VÉGTELEN FÉLCSOPORTOK VIZSGÁLATA

Írta: Battha László

Sopron

1988

TARTALOM:

Bevezetés 1

1. Kongruenciarelációk, homomorfizmusok 2

2. Szabad félcsoportok. Generáló relációk. A biciklikus félcsoport. 4

3. Növelőelemek 9

4. Ideálok 13

5. A C, D és P_o félcsoportok 17

6. CSPI-félcsoportok 27

7. A két elemmel generálható CSPI-félcsoportok 40

8. Speciális félcsoportok 52

IRODALOM 60

BEVEZETÉS

A félcsoportok elmélete a matematikának egyik legújabb ága. Az első, kizárólag ezt a témakört tárgyaló kézikönyv [3] 1961-ben jelent meg. A funkcionálanalízis és a topológia egyes területein már korábban is szükségesnek mutatkozott bizonyos speciális félcsoportok tárgyalása. Az elmélet gyors fejlődésnek indult, megtörtént az algebrai alapok lerakása.

Az egyik legfontosabb terület a félcsoportok kongruenciáinak vizsgálata. Míg csoportok esetében egy kongruenciát egyértelműen meghatároz az az osztály (normálosztó), amely az egységelemet tartalmazza, addig félcsoportok esetében a helyzet bonyolultabb. Mivel minden félcsoport homomorf képe valamely szabad félcsoportnak (és minden homomorfizmus egy kongruencia-relációt határoz meg), kitüntetett szerepe van a szabad félcsoportok kongruencia-relációinak. A jelen munka arra ad eljárásokat, hogy - bizonyos esetekben - a generáló relációk ismeretében hogyan lehet a vizsgált félcsoportot a szabad félcsoport bizonyos kitüntetett elemeivel reprezentálni. Megvizsgálja a tárgyalt félcsoportok ideál-struktúráját, meghatározza a növelő elemeket és egyes esetekben nem-triviális automorfizmusok létezését.

Köszönetet mondok Dr.Megyesi László egyetemi docensnek, amiért rendszeres konzultációkon megismertetett ezzel a területtel, és a jelen munka megírására ösztönzött. Munkahelyem (MTA GGKI) lehetővé tette a disszertáció elkészítését, amit most megköszönök.

Sopron, 1988. január

1. Kongruenciarelációk, homomorfizmusok

Tegyük fel, hogy az S halmaz elemei között a * művelet van értelmezve, azaz S egyműveletes struktúra. Definiáljuk az S^1 struktúrát a következőképpen. Ha S tartalmaz (kétoldali) egységelemet, akkor legyen $S^1=S$, egyébként pedig legyen $S^1=S\cup\{1\}$, továbbá $x*1=1*x=x$ $(x\in S^1)$.

Ha K tetszőleges nemüres részhalmaza S-nek, akkor a legszűkebb, K-t tartalmazó részfélcsoportot $\langle K\rangle$-val jelöljük. Ez nyilván az összes, K-t tartalmazó részfélcsoport metszete. Ha $\langle K\rangle=S$, akkor azt mondjuk, hogy K generálja S-et.

Tegyük fel, hogy S_1 és S_2 egyműveletes struktúrák. Az $x,y\in S_1$ elemek szorzatát jelölje xy, az $x,y\in S_2$ elemek szorzatát pedig $x*y$. Ha a μ: $S_1\text{-->}S_2$ leképezésre teljesül, hogy

$(xy)\mu = x\mu*y\mu$ $(x,y\in S_1)$,

akkor μ-t homomorfizmusnak nevezzük. S_1 elemei között bevezetjük a következő ρ relációt: $x\rho y$ ha $x\mu=y\mu$.

1.1 Tétel ρ kongruenciareláció. (Nevezzük ρ-t a μ-höz tartozó kongruenciának.) A ρ szerinti kongruenciaosztályok halmazát jelölje S_1/ρ. Az $a\in S_1$ elemet tartalmazó osztályt jelölje $a\rho$. Vezessük be S_1/ρ-ban az alábbi műveletet:

(1) $a\rho\ b\rho =(ab)\rho$.

Az (1) művelettel S_1/ρ olyan egyműveletes struktúra, amely izomorf S_2-vel. Ha K tetszőleges ρ-osztály és $x\in K$, akkor legyen $K\eta = x\mu$. Ekkor η izomorfizmus S_1/ρ-ról S_2-re. Ha S_1 félcsoport, akkor S_2 (és így S_1/ρ is) szintén félcsoport. ∎

Ha ρ kongruenciareláció az S egyműveletes struktúrán, akkor legyen $\rho^{\#}$:$S\text{-->}S/\rho$ az a leképezés, amely minden S-beli x elemhez az x-et tartalmazó ρ-osztályt rendeli hozzá. Ekkor $\rho^{\#}$ homomorfizmus: a ρ-hoz tartozó természetes homomorfizmus.

Legyen ρ_o tetszőleges reláció az S egyműveletes struktúrán, és legyen ρ az összes olyan kongruencia metszete, amely tartalmazza ρ_o-t. ρ-t a ρ_o által generált kongruenciarelációnak nevezzük.

Ha ρ tetszőleges reláció, akkor ρ^{-1} jelentse ρ ellentettjét: $x\,\rho^{-1}\,y$ ha $y\rho x$. Jelölje e az egyenlőségrelációt: xey ha x=y.

Legyen ρ_o tetszőleges reláció az S félcsoportban, $\rho_1=\rho_o \cup \rho_o^{-1} \cup e$, és a ρ_o által generált kongruenciareláció legyen ρ. Definiáljuk a ρ_2 relációt a következőképpen: a ρ_2 b ha van olyan $c,d\in S$ és $x,y\in S^1$, hogy

$$a=xcy,\ b=xdy \text{ és } c\ \rho_1\ d.$$

Azt mondjuk, hogy a-t b-ből (vagy fordítva) elemi ρ_o-átmenettel állítottuk elő. ρ_2 nyilván reflexiv, szimmetrikus és kompatibilis; továbbá $\rho_o\subseteq\rho_1\subseteq\rho_2\subseteq\rho$. ρ_2 tranzitiv lezárása ρ_2^t: a ρ_2^t b ha van $c_1, c_2,\ldots,c_n\in S$, hogy a ρ_2 c_1, c_1 ρ_2 c_2, ..., c_n ρ_2 b. Kapjuk, hogy $\rho_2^t=\rho$. Ebből következik, hogy aρb akkor és csak akkor, ha b előállítható a-ból véges sok elemi ρ_o-átmenettel.

2. Szabad félcsoportok. Generáló relációk. A biciklikus félcsoport.

Legyen X tetszőleges nemüres halmaz. Nevezzük X elemeit betűknek. X-beli betűknek egy véges sorozatát szónak nevezzük. Legyen F_X az X-beli szavak halmaza. F_X elemei között az alábbi műveletet értelmezzük: Ha $x=(x_1,\ldots,x_m)$ és $y=(y_1,\ldots,y_n)$, akkor szorzatukat egyszerűen egymásmelléírással képezzük:

$$xy=(x_1,\ldots,x_m)(y_1,\ldots,y_n)=(x_1,\ldots,x_m,y_1,\ldots,y_n).$$

Ezzel a művelettel F_X félcsoport: az X által generált szabad félcsoport. Ha $u\in X$ és az egy betűből álló (u) szót u-val jelöljük, akkor $(x_1,x_2,\ldots,x_m)=x_1x_2\ldots x_m$. Az x_i-ket az x elemi tényezőinek nevezzük. x hossza elemi tényezőinek száma: $|x|=m$. F_X^1 egységeleme 1, $|1|=0$. Ekkor teljesül, hogy $|xy|=|x|+|y|$. Ha $x=x_1x_2\ldots x_n$ és $1\le i\le j\le n$, akkor beszélhetünk az i,j indexekhez tartozó $(i,j)_x$ részszóról, melynek értéke $x_ix_{i+1}\ldots x_j$. Az $(i,i)_x$ részszót röviden $(i)_x$-el jelöljük. Ha u és v részszavai x-nek, akkor $u\equiv v$ jelentse azt, hogy indexeik megegyeznek; $u=v$ pedig jelentse azt, hogy értékük ugyanaz. ($u\equiv v$ -ből következik, hogy $u=v$, de a fordított állítás nem igaz.) x összes részszavainak halmazát jelölje S_x. Legyen $u=(i,j)_x$ és $v=(k,l)_x$. $u\subseteq v$ jelentse azt, hogy v tartalmazza u-t, azaz $k\le i$ és $j\le l$. Bevezetjük az $u\cap v\equiv(\max(i,k),\min(j,l))_x$ jelölést is. u és v diszjunktak, ha $u\cap v=\emptyset$.

2.1 Lemma Legyen S tetszőleges félcsoport és φ_o tetszőleges leképezése X-nek S-be. Ekkor φ_o pontosan egyféleképpen terjeszthető ki F_X-re olymódon, hogy a kapott $\varphi:F_X\to S$ leképezés homomorfizmus legyen. ∎

Bizonyítás Ha egy φ homomorfizmus X-en megegyezik φ_o-al, akkor $x_i\in X$ esetén

(1) $(x_1x_2\ldots x_m)\varphi=(x_1\varphi_o)(x_2\varphi_o)\ldots(x_m\varphi_o)$.

Tehát legfeljebb egy ilyen φ homomorfizmus lehet. Másrészt (1) φ definíciójának is tekinthető, és az így definiált φ nyilván homomorfizmus.

2.2 Tétel Legyen ρ_o tetszőleges reláció F_X-en, és a ρ_o által generált reláció legyen ρ. Legyen S tetszőleges félcsoport, és φ olyan homomorfizmus F_X-ről S-be, hogy $u\varphi=v\varphi$ teljesül minden ρ_o-beli (u,v)-re. Jelöljük a φ-hez tartozó kongruenciát μ-vel. A φ-re tett feltételből következik, hogy $\rho\subseteq\mu$. Ha K tetszőleges μ-osztály és $x\in K$, akkor legyen $K\eta=x\varphi$. Ekkor η izomorfizmus F_X/μ-ről S-be. Definiáljuk az $\alpha : F_X/\rho \to F_X/\mu$ leképezést a következőképpen. Ha K tetszőleges ρ-osztály, akkor $K\alpha$ legyen az a μ-osztály, amely tartalmazza K-t. Ekkor α homomorfizmus, és $\rho^{\#}\alpha\eta=\varphi$. ∎

2.3 Definíció Legyen $X=\{a,b\}$, $s(a)=1$ és $s(b)=-1$. A 2.1 Lemma szerint s egyértelműen kiterjeszthető F_X-nek Z-be (az egészek additív csoportjába) történő homomorfizmusává. Legyen $s(1)=0$. Ekkor s homomorfizmus F_X^1-ről Z-re. Tehát ha $x=x_1\ldots x_n$ $(x_i\in X)$, akkor

$$s(x)=s(x_1)+\ldots+s(x_n).$$

Definiáljuk az $I\subseteq F_X$ halmazt a következőképpen. Legyen $x=x_1\ldots x_n$ $(x_i\in X)$. $x\in I$ akkor és csak akkor, ha

(2) $s(x)=0$ és $s(x_1\ldots x_i)<0$ $(i=1,2,\ldots,n-1)$

A fentivel ekvivalens állítás:

(2') $s(x)=0$ és $s(x_i x_{i+1}\ldots x_n)>0$ $(i=2,3,\ldots,n)$.

2.4 Lemma Legyen $x=x_1\ldots x_n$ $(x_i\in X)$.

(i) Ha $x\in I$, akkor vagy $x=ba$, vagy x egyértelműen a $bz_1z_2\ldots z_ka$ alakba írható, ahol $z_i\in I$ $(i=1,\ldots k)$. Van olyan i, hogy $x_i=b$ és $x_{i+1}=a$. Az $(i,i+1)_x=ba$ részszót alappárnak nevezzük.

(ii) Ha $u\in I$ és $xuy\in I$, akkor vagy $x=y=1$, vagy $x\neq1$ és $y\neq1$.

(iii) Legyen $u\in I$, $x\neq 1$ és $y\neq 1$. $xuy\in I$ akkor és csak akkor, ha $xy\in I$.

(iv) Ha $u\equiv(i,j)_x\in I$ és $v\equiv(k,l)_x\in I$, akkor vagy $u\subseteq v$, vagy $u\supseteq v$, vagy pedig $u\cap v=\emptyset$. Tehát u és v vagy diszjunktak, vagy valamelyik tartalmazza a másikat. Ezért beszélhetünk az x szó I-maximális részszavairól, amelyek diszjunktak.

(v) Legyen $x=x_1\dots x_n\in F_X$, $c\equiv(i,i+1)_x=ba$ és $y=x_1\dots x_{i-1}x_{i+2}\dots x_n$. Legyen

$$j\nu=\begin{matrix} j & \text{ha } j<i, \\ j-2 & \text{ha } j>i+1. \end{matrix}$$

Tehát ν 1-1 és monoton leképezése $\{1,\dots,i-1,i+2,\dots,n\}$-nek $\{1,\dots,n-2\}$-re, továbbá $y_{j\nu}=x_j$. Legyen $A=S_x\cap I\setminus\{c\}$ és $B=S_y\cap I$. Ha $(k,l)_x\in A$, akkor legyen $(k,l)_x\varphi=(k\nu,l\nu)_y$. Ekkor φ 1-1 leképezés A-ról B-re, továbbá az A-ban szereplő I-maximális részszavak a B-beli I-maximális részszavakra képződnek le. Következésképp $(j)_x$-t $(j\in\{1,\dots,i-1,i+2,\dots,n\})$ akkor és csak akkor tartalmazza valamilyen A-beli u, ha $(j\nu)_y$-t tartalmazza valamilyen B-beli v.

∎

2.5 Definíció Legyen $P\subseteq F_X$ azon szavak halmaza, melyeknek nincs I-beli részszava. Nyilván

$$P=\{a^ib^j:\ i\geq 0,\ j\geq 0,\ i+j>0\}$$

Definiáljuk a μ: $F_X\text{-->}P$ leképezést. $\mu(x)$ legyen az a szó, melyet x-ből az I-maximális részszavak elhagyásával kapunk. A 2.4 Lemmából következik, hogy ez a definíció egyértelmű. P elemei között bevezetjük az alábbi műveletet:

$$x*y=\mu(xy)\quad (x,y\in P).$$

2.6 Tétel μ homomorfizmus F_X-ről P-re:

(3) $\mu(xy)=\mu(x)*\mu(y)\quad (x,y\in F_X)$.

Ezért P a $*$ művelettel félcsoport. Neve: biciklikus félcsoport. A μ-höz tartozó ρ_P kongruenciarelációt $\rho_0=\{(ba,1)\}$ generálja. Ha a^ib^j helyett (i,j)-t írunk, akkor

(4) $(i,j)*(k,l)=(i+[k-j]^+,l+[j-k]^+)$,
ahol $[x]^+=x$ ha $x\geq 0$, és $[x]^+=0$ ha $x<0$. ∎

Bizonyítás A 2.4 Lemma (v) állításából következik, hogy
(5) $\mu(ubav)=\mu(uv)$ $(u,v\in F_X^1)$.
Legyen $x,y\in F_X$. Ha $\mu(x)\neq x$, akkor a 2.4 Lemma (i) állítása szerint x felírható $x=x_1=ubav$ alakban. Legyen $x_2=uv$. Hasonlóan képezzük x_2-ből x_3-at, stb. Mivel $|x_i|>|x_{i+1}|\geq 0$, kapunk egy véges $x_1,x_2,\ldots,x_k$ sorozatot, melyre (5) miatt
(6) $\mu(x)=\mu(x_1)=\mu(x_2)=\ldots=\mu(x_k)=x_k$.
Hasonló módon kapjuk, hogy

$$\mu(xy)=\mu(x_1y)=\mu(x_2y)=\ldots=\mu(x_ky)=\mu(\mu(x)y).$$

Megismételve a fenti eljárást x helyett y-al, kapjuk (3)-at. (6)-ból következik, hogy $\mu(x)$-t megkaphatjuk x-ből véges sok ρ_0-átmenettel. Ezért ρ_p-t a ρ_0 reláció generálja. (4)-et egyszerű számítással igazolhatjuk.

2.7 Tétel Ha az $S=\langle u,v\rangle$ egységelemes félcsoportban $vu=1$ de $uv\neq 1$, akkor S izomorf P-vel, a biciklikus félcsoporttal. ∎

Bizonyítás A 2.5 Definíció és 2.6 Tétel jelöléseit használjuk. A 2.1 Lemma szerint van olyan (egyértelműen meghatározott) φ homomorfizmus F_X-ről S-re, hogy $a\varphi=u$ és $b\varphi=v$. Legyen a φ-hez tartozó kongruenciareláció ν. Megmutatjuk, hogy $\nu=\rho_p$. Mivel $(ba)\varphi=vu=1$, kapjuk, hogy $\rho_p\subseteq\nu$. Most belátjuk, hogy egy ν-osztály nem tartalmazhat két különböző ρ_p-osztályt. Tegyük fel e célból, hogy $a^ib^j\nu a^kb^l$, azaz
(3) $u^iv^j=u^kv^l$.
A $vu=1$ és $uv\neq 1$ feltételekből következik, hogy
(4) az $ux=1$ és $yv=1$ egyenleteknek nincs megoldása S-ben.
(Pl. $ux=1$ -ből $x=1x=vux=v1=v$ és ezért $uv=1$ következne.) Tegyük fel, hogy $i>k$. (3) mindkét oldalát balról v^k-val, jobbról u^l-

el szorozva $u^{i-k}v^{j}u^{l}=1$, ellentmondásban (4)-el. Ezért $i=k$. Hasonlóan kapjuk, hogy $j=l$.

3. Növelőelemek

Az S félcsoport a elemét jobbnövelőnek nevezzük, ha S-nek van olyan T valódi részhalmaza ($T\subset S$), hogy $Ta=S$. A balnövelő elem definíciója az előbbinek a duálisa. A bal- és jobbnövelő elemek halmazát jelölje $S^{(l)}$ ill. $S^{(r)}$. A definícióból következik, hogy sem véges félcsoportnak sem csoportnak nem lehet növelő eleme.

3.1 Tétel $S^{(l)}\cap S^{(r)}=\emptyset$.

Bizonyítás Tegyük fel, hogy $a\in S^{(l)}\cap S^{(r)}$. Mivel $a\in S^{(r)}$, van $e\in S$, hogy $ea=a$. Legyen $x\in S$ tetszőleges. Mivel $a\in S^{(l)}$, van $y\in S$, hogy $x=ay$, így $ex=eay=ay=x$, azaz e baloldali egységeleme S-nek. Mivel $a\in S^{(r)}$, van $a'\in S$, hogy $a'a=e$. Így $ax=ay$ -ból következik, hogy $x=ex=a'ax=a'ay=ey=y$, ezért a nem lehet balnövelő, ellentmondásban feltevésünkkel.

3.2 Következmény Kommutativ félcsoportnak nincs növelő eleme.

3.3 Tétel Az $S^{(l)}$ és $S\backslash S^{(l)}$ halmazok (amennyiben nem üresek) részfélcsoportjai S-nek. ∎

Bizonyítás Legyen $b\in S^{(l)}$, $T\subset S$ és $bT=S$. Legyen továbbá $aS=S$ (ez teljesül, ha $a\in S^{(l)}$). Ekkor $(ab)T=a(bT)=aS=S$. Ezért $S^{(l)}$ részfélcsoport.

Tegyük fel, hogy a és b egyike sem balnövelő, de ab balnövelő: $T\subset S$ és $abT=S$. Mivel a nem balnövelő, de $a(bT)=S$, ezért $bT=S$, ellentmondásban azzal, hogy b nem balnövelő.

3.4 Következmény (i) Ha $S^{(n)}=S\backslash(S^{(l)}\cup S^{(r)})$ nem üres, akkor $S^{(n)}$ részfélcsoportja S-nek. (ii) Ha $S=\langle A\rangle$ és S-nek van bal-

[jobb]növelő eleme, akkor A is tartalmaz bal-[jobb]növelő elemet. ∎

Bizonyítás $S^{(n)}=(S\setminus S^{(l)})\cap(S\setminus S^{(r)})$.

3.5 Tétel Az $S^{(r)}$ félcsoportnak nincs balnövelő eleme.

Bizonyítás Tegyük fel, hogy b balnövelő eleme $S^{(r)}$-nek. Ekkor van $e\in S^{(r)}$, hogy $be=b$. Legyen $x\in S$ tetszőleges. Mivel $b\in S^{(r)}$, van $y\in S$, hogy $yb=x$, ezért $x=yb=ybe=xe$, tehát e jobboldali egységeleme S-nek, ellentmondásban az $e\in S^{(r)}$ feltevéssel.

3.6 Tétel Ha S egységelemes félcsoport, akkor az $S^{(n)}$ félcsoportnak nincs növelő eleme. ∎

Bizonyítás Tegyük fel, hogy u jobbnövelő eleme $S^{(n)}$-nek. Mivel $1\in S^{(n)}$, van $v\in S^{(n)}$, hogy $vu=1$, így $v(uS)=(vu)S=1S=S$. Mivel v nem balnövelő, $uS=S$. Így van w, hogy $uw=1$. Ha x,y tetszőleges elemei S-nek, és $xu=yu$, akkor $x=x1=xuw=yuw=y1=y$. Ezért u nem lehet jobbnövelő eleme $S^{(n)}$-nek.

3.7 Definíció Az S félcsoport a elemét jobbról invertálhatónak nevezzük, ha $aS=S$, azaz ha az $ax=b$ egyenlet tetszőleges b esetén megoldható. Az a elemet invertálhatónak nevezzük, ha jobbról is, és balról is invertálható.

3.8 Lemma Ha az S félcsoportnak van invertálható eleme, akkor van egységeleme is. ∎

Bizonyítás Tegyük fel, hogy $aS=Sa=S$. Ekkor van $e\in S$, hogy $ae=a$. Legyen $x\in S$ tetszőleges. Mivel $x\in S=Sa$, van $y\in S$, hogy $ya=x$. Ezért $xe=yae=ya=x$, tehát e jobboldali egységelem. A duális gondolatmenetet is elvégezve kapjuk, hogy e kétoldali egységelem, azaz

$e=1$.

3.9 Tétel Ha u jobbnövelő eleme az S félcsoportnak, akkor u balról invertálható, és nem invertálható jobbról. Ha S-nek van egységeleme, akkor a fordított állítás is igaz: Ha u balról invertálható, és nem invertálható jobbról, akkor u jobbnövelő. ∎

Bizonyítás Legyen u jobbnövelő eleme S-nek. Ekkor u nyilván balról invertálható. Tegyük fel, hogy - a tétel állításának ellentmondva - u jobbról is invertálható. Ekkor a 3.8 Lemma szerint S-nek van egységeleme, és u-nak van u' inverze. Ha $xu=yu$, akkor $x=x1=xuu'=yuu'=y1=y$, tehát u nem lehet jobbnövelő.

A fordított irányu állítás bizonyításához tegyük fel, hogy $1\in S$, u balról invertálható de jobbról nem, azaz $Su=S$ és $uS\neq S$. Mivel $Su=S$, van v, hogy $vu=1$. $uS\neq S$ miatt $uv\neq 1$, ezért $u^2v\neq u$, hiszen $u^2v=u$ -ból $uv=1uv=vu^2v=vu=1$ adódna. Mivel $(u^2v)u=u^2(vu)$ $=(u)u$, kapjuk, hogy u jobbnövelő eleme S-nek.

3.10 Tétel Az S félcsoport akkor és csak akkor egységelemes, ha tartalmaz legalább egy jobbról invertálható elemet, amely nem balnövelő, és legalább egy balról invertálható elemet, amely nem jobbnövelő. ∎

Bizonyítás A feltétel nyilván szükséges.

Fordítva, tegyük fel, hogy $uS=S$ és u nem balnövelő, továbbá hogy $Sv=S$ és v nem jobbnövelő. Adódik, hogy $ux=uy$ vagy $xv=yv$ esetén $x=y$ következik. Mivel $uS=S$, van $e\in S$, hogy $ue=u$. Innen tetszőleges $x\in S$-re $uex=ux$, és így $ex=x$, tehát e baloldali egységelem. A v-re tett feltételekből hasonló módon adódik egy f jobboldali egységelem létezése. Kapjuk, hogy $e=f=1$.

3.11 Lemma Legyen $P=\langle a,b\rangle$ a biciklikus félcsoport ($ba=1$, $ab\neq 1$).
(i) P balnövelő elemei b hatványai. P jobbnövelő elemei a hatványai.
(ii) P-nek nincs más automorfizmusa, mint az identikus automorfizmus. ∎

Bizonyítás (i) azonnal következik a P-beli szorzási szabályból (2.6 Tétel).

Tegyük fel, hogy φ automorfizmusa P-nek. Mivel $a\varphi$ jobbnövelő eleme P-nek, $a\varphi=a^k$ valamilyen $k\geq 1$ -re. Hasonlóan, $b\varphi=b^l$, $l\geq 1$. Következik, hogy

(1) $(a^ib^j)\varphi=a^{ik}b^{jl}$ $(i\geq 0, j\geq 0)$.

Mivel φ automorfizmus, van i és j, hogy $a^{ik}b^{jl}=ab$, azaz $ik=1$ és $jl=1$. Innen következik, hogy $k=1$ és $l=1$; és így (1) szerint φ az identikus leképezés.

3.12 Tétel Legyen S egységelemes félcsoport és $u\in S$. A következő három állítás ekvivalens:
(i) u jobbnövelő eleme S-nek.
(ii) Van $v\in S$, hogy $vu=1$ de $uv\neq 1$.
(iii) Van olyan izomorfizmus P-ről S-be, hogy $1\varphi=1$ és $a\varphi=u$.

Bizonyítás (i) és (ii) ekvivalenciáját bebizonyítottuk a 3.9 Tétellel, a (ii)-->(iii) implikációt pedig a 2.7 Tétellel.

Tegyük fel, hogy (iii) teljesül. Legyen $v=b\varphi$. Mivel $vu=(b\varphi)(a\varphi)=(ba)\varphi=1\varphi=1$, a (iii)-->(ii) implikáció bizonyításához már csak azt kell belátni, hogy $uv\neq 1$. De $uv=1$ -ből $(ab)\varphi=uv=1=1\varphi$, és mivel φ izomorfizmus, $ab=1$ következne.

3.13 Következmény Ha egy egységelemes félcsoportnak van balnövelő eleme, akkor van jobbnövelő is, és viszont.

4. Ideálok

Egy egyműveletes S struktúra nemüres A részhalmazát bal-[jobb]-ideálnak nevezzük, ha $SA\subseteq A$ [$AS\subseteq A$]. A-t kétoldali ideálnak nevezzük, ha A bal- és jobbideál. S-et egyszerűnek nevezzük, ha nem tartalmaz S-től különböző (kétoldali) ideált.

4.1 Lemma Az S félcsoport akkor és csak akkor egyszerű, ha $SxS=S$ teljesül minden $x\in S$-re.

Bizonyítás Elegendő annyit megjegyezni, hogy SxS tetszőleges x esetén kétoldali ideálja S-nek.

Ideálok tetszőleges rendszerének metszete (ha nem üres) szintén ideál. Ezért beszélhetünk S egy tetszőleges nemüres részhalmaza által generált ideálról. Pl. az $x\in S$ elem által generált jobbideál $xS \cup \{x\}=xS^1$. Az egy elem által generált ideált főideálnak nevezzük. Az x által generált fő-jobbideált jelölje $R(a)$ $(=xS^1)$, az x által generált fő-balideált pedig $L(a)$ $(=S^1x)$. Ha S összes bal- és összes jobbideálja főideál, akkor S-et főideál-félcsoportnak nevezzük.

4.2 Tétel (Lyapin) Legyen S tetszőleges félcsoport. A következő két állítás ekvivalens:

(i) S minden balideálja fő-balideál;

(ii) S balideáljainak halmazában a $\subset$ reláció duálisan jólrendezés. (Tehát ha L_1 és L_2 balideálok, akkor $L_1\supset L_2$ vagy $L_1\subset L_2$; továbbá ha Ω balideáloknak egy tetszőleges rendszere, akkor Ω-nak van maximális eleme.)

Megjegyzés A bizonyításból kiderül, hogy a tétel érvényes marad, ha balideálok helyett jobbideálokra vagy kétoldali ideálokra mondjuk ki.

Bizonyítás (i)-->(ii) Tegyük fel, hogy S minden balideálja bal-főideál. Legyenek L_1 és L_2 tetszőleges balideálok, és $L=L_1 \cup L_2$. Mivel L balideál, ezért $L=L(a)$ valamilyen a-ra. Mivel $a \in L=L_1 \cup L_2$, ezért $a \in L_1$ vagy $a \in L_2$. Legyen pl. $a \in L_1$. Ekkor $L_1 \subseteq L_1 \cup L_2=L(a) \subseteq L_1$, ezért $L_1=L_1 \cup L_2$, ezért $L_2 \subseteq L_1$. Következésképp, S balideáljai között a $\subset$ reláció teljes rendezést valósít meg.

Legyen most Ω balideáloknak egy tetszőleges rendszere. Tegyük fel, hogy Ω-nak nincs maximális eleme. Legyen $L_1 \in \Omega$. Mivel L_1 nem maximális, van $L_2 \in \Omega$, hogy $L_1 \subset L_2$. Ezt az eljárást folytatva ideáloknak egy $L_1 \subset L_2 \subset \dots$ sorozatához jutunk. Legyen $L=\cup_{i=1}^{\infty} L_i$. Mivel L balideál, $L=L(a)$ valamilyen a-ra. Mivel $a \in L$, van $i>0$, hogy $a \in L_i$. Kapjuk, hogy $L_i \subseteq L=L(a) \subseteq L_i$, tehát $L=L_i$, azaz L_i maximális eleme Ω-nak.

(ii)-->(i) Tegyük fel, hogy S balideáljai a $\subset$ relációval duálisan jólrendezettek. Legyen L tetszőleges balideálja S-nek. Tegyük fel, hogy L nem bal-főideál, és válasszunk tetszőleges $x_1 \in L$ elemet. Feltevésünk szerint $L_1=L(x_1) \subset L$. Válasszunk tetszőleges $x_2 \in L \setminus L_1$ elemet. Ekkor $L_1 \subset L_2=L(x_2) \subset L$. Hasonlóan választjuk az $x_3 \in L \setminus L_2$ elemet, stb. Ezen a módon balideáloknak egy $L_1 \subset L_2 \subset \dots \subset L$ szigorúan monoton növekvő sorozatát kapjuk. Az $\{L_i\}_{i=1}^{\infty}$ rendszernek nincs maximális eleme, ellentmondásban feltevésünkkel.

Ha S tetszőleges félcsoport, bevezetjük S-ben a következő ekvivalenciarelációt: $a \mathcal{L} b$ ha a és b ugyanazt a bal-főideált generálják, azaz ha $S^1a=S^1b$. Adódik, hogy $\mathcal{L}$ jobbkompatibilis ekvivalenciareláció. Jelölje L_a azt az $\mathcal{L}$-ekvivalenciaosztályt, amely tartalmazza a-t. Duális módon definiáljuk az $\mathcal{R}$ ekvivalenciarelációt és az R_a halmazt.

4.3 Lemma Tegyük fel, hogy $L(a)$ maximális fő-balideálja az S egyszerű félcsoportnak, L_b pedig tetszőleges $\mathcal{L}$-osztálya S-nek. Ekkor van $y\in S^1$, hogy $L_b y\subseteq L_a$.

■

Bizonyítás Mivel S egyszerű, a 4.1 Lemma szerint $SbS=S$, ezért van $x,y\in S$, hogy $xby=a$. Mivel $L(by)\supseteq L(xby)=L(a)$, és $L(a)$ maximális, ezért $L(by)=L(a)$. Ha $u\in L(b)$, akkor $L(uy)=L(u)y=L(b)y=L(by)=L(a)$, ezért $uy\in L_a$. Kapjuk, hogy $L_b y\subseteq L_a$.

4.4 Lemma (Green) Legyenek a és b $\mathcal{R}$-ekvivalens elemei az S félcsoportnak. Ekkor van $s,s'\in S^1$, hogy $as=b$ és $bs'=a$. Legyen $\sigma:x\longrightarrow xs$ $(x\in L(a))$ és $\sigma':y\longrightarrow ys'$ $(y\in L(b))$. Ekkor σ és σ' kölcsönösen inverz, 1-1 leképezései $L(a)$-nak $L(b)$-re ill. $L(b)$-nek $L(a)$-ra, továbbá $x\sigma\ \mathcal{R}\ x$ $(x\in L(a))$ és $y\sigma'\ \mathcal{R}\ y$ $(y\in L(b))$, azaz σ és σ' $\mathcal{R}$-osztály megtartók. Ha σ és σ' helyett ezek megszorításait vesszük L_a ill. L_b-re, akkor az is igaz, hogy σ és σ' kölcsönösen inverz, $\mathcal{R}$-osztály megtartó, 1-1 leképezései L_a-nak L_b-re ill. L_b-nek L_a-ra. ■

Bizonyítás Legyen $x\in L(a)$. Ekkor $x\sigma=xs\in L(as)=L(b)$. Tehát σ $L(a)$-t $L(b)$-be képezi le. Hasonlóan, $\sigma'\in L(b)\longrightarrow L(a)$.

Legyen $x\in L(a)$. Ekkor van $t\in S^1$, hogy $x=ta$, és így

$$x\sigma\sigma'=xss'=tass'=tbs'=ta=x.$$

Tehát $\sigma\sigma'$ az identikus leképezése az $L(a)$ halmaznak. Hasonlóan, $\sigma'\sigma$ az identikus leképezése $L(b)$-nek. Kapjuk, hogy σ és σ' kölcsönösen inverz, 1-1 leképezései $L(a)$-nak $L(b)$-re ill. $L(b)$-nek $L(a)$-ra.

Ha $x\in L(a)$, akkor $x\sigma=xs$ és $x=x\sigma\sigma'=x\sigma s'$, ahonnan $x\ \mathcal{R}\ x\sigma$. Hasonlóan, $y\ \mathcal{R}\ y\sigma'$, ha $y\in L(b)$.

Vegyük most σ és σ' helyett ezek megszorítását L_a-ra ill. L_b-re. Mivel az $\mathcal{L}$ reláció jobb kompatibilis, $\sigma\in L_a\longrightarrow L_b$ és $\sigma'\in L_b\longrightarrow L_a$. A bizonyítás első részét megismételve úgy, hogy

$L(a)$ és $L(b)$ helyett L_a-t ill. L_b-t írunk, kapjuk az utolsó állítást.

Legyen $\mathfrak{H}=\mathfrak{L}\cap\mathfrak{R}$. $\mathfrak{H}$ nyilván ekvivalenciareláció. Az $a\in S$ elemet tartalmazó ekvivalenciaosztály $H_a=R_a\cap L_a$. Ha $H_x=\{x\}$ $(x\in S)$, akkor S-et kombinatorikusnak nevezzük.

5. A C, D és P_o félcsoportok

Legyen $X=\{a,b\}$, és használjuk a 2.3 Definíció jelöléseit. Legyen $x\in F_X$, és y részszava x-nek. y C-elhagyható, ha $y\in I$ és van $u,v,z\in F_X^1$, hogy $s(z)<0$ és $x=uzyv$. A 2.4 Lemmából következik, hogy ha u és v C-elhagyhatók, akkor vagy diszjunktak, vagy valamelyik tartalmazza a másikat. Ezért beszélhetünk x-nek C-maximális részszavairól. Ezek diszjunktak.

5.1 Lemma (i) Legyen $x=uvwz$, ahol $v,w\in I$. v akkor és csak akkor C-elhagyható, ha w C-elhagyható.
(ii) Ha $x=x_1x_2...x_n$ $(x_i\in X)$ tartalmaz C-elhagyható részszót, akkor van i, hogy $x_ix_{i+1}x_{i+2}=bba$, tehát x tartalmaz C-elhagyható alappárt.
(iii) Legyen y C-maximális részszava x-nek, és az y-t tartalmazó I-maximális részszó legyen $u=bz_1...z_ka$, ahol $z_i\in I$. $(i=1,...,k)$. Ekkor vagy $y\equiv u$ vagy $y\equiv z_i$ valamilyen i-re. ∎

Bizonyítás (i) a 2.3 Definícióból következik.
(ii) Legyen $y=x_k...x_l$ a legelső (legkisebb indexü) C-maximális részszava x-nek. Könnyen belátható, hogy $x_{k-1}=b$. Legyen j az a k-nál nagyobb legelső index, melyre $x_j=a$. Ha $i=j-2$, akkor $x_ix_{i+1}x_{i+2}=bba$.

5.2 Definíció Legyen $C\subseteq F_X$ azon szavak halmaza, melyeknek nincs C-elhagyható részszava. Definiáljuk a $\mu:F_X\text{-->}C$ leképezést a következőképpen. $\mu(x)$ legyen az a szó, melyet x-ből a C-maximális részszavak elhagyásával kapunk. C-ben bevezetjük az alábbi műveletet:

$$x*y=\mu(xy) \quad (x,y\in C).$$

5.3 Tétel μ homomorfizmus F_X-ről C-re:

(1) $\mu(xy)=\mu(x)*\mu(y) \quad (x,y\in F_X)$.

Ezért C a * művelettel félcsoport. A μ-höz tartozó ρ_c kongruenciát $\rho_o=\{(b^2a,b)\}$ generálja. ∎

Bizonyítás μ definíciójából és a 2.4 Lemmából következik, hogy

(2) $\mu(ubbav)=\mu(ubv) \quad (u,v\in F_X^1)$.

Legyen $x\in F_X$. Ha $\mu(x)\neq x$, akkor az 5.1 Lemma (ii) állítása szerint $x=x_1=ubbav$. Legyen $x_2=ubv$. Hasonlóan képezzük x_2-ből x_3-at, stb. Kapunk egy véges $x=x_1,x_2,\dots,x_k$ sorozatot, melyre (2) szerint

(3) $\mu(x)=\mu(x_1)=\mu(x_2)=\dots\mu(x_k)=x_k$.

Ha $y\in F_X$, akkor (3)-ból (2) felhasználásával kapjuk, hogy

(4) $\mu(xy)=\mu(x_1y)=\mu(x_2y)=\dots=\mu(x_ky)=\mu(\mu(x)y)$.

Megismételve a fenti eljárást $\mu(x)y$-ra, kapjuk, hogy

(5) $\mu(\mu(x)y)=\mu(\mu(x)\mu(y))=\mu(x)*\mu(y)$.

(4) és (5) egybevetéséből kapjuk (1)-et.

(3)-ból következik, hogy $\mu(x)=\mu(y)$ akkor és csak akkor, ha y előállítható x-ből véges sok ρ_o-átmenettel. Ezért ρ_o generálja ρ_c-t.

5.4 Lemma (i) Ha $x\in F_X$, $y\in F_X$ és $xy\in C$, akkor $x\in C$, $y\in C$ és $x*y=xy$.

(ii) $\mu(ax)=a\mu(x) \quad (x\in F_X)$,

(iii) $\mu(xb)=\mu(x)b \quad (x\in F_X)$.

(iv) Ha $\mu(x)=1$, akkor $x=1$.

(v) Ha $x*y=1$, akkor $x=y=1$.

(vi) Ha $xa\in C$, akkor $s(xa)=k\geq 0$ és $b^{k+1}*xa=b$.

(vii) Ha $ua\in C$ és $v\in C$, akkor $ua*v=uav$.

(viii) Ha xab, $y\in C$, akkor $xab*y=xabz$ valamilyen z-re.

(ix) Ha $xab\in C$ és $|xab*y|=|xab|$, akkor $y=z_1z_2\dots z_k$ alaku, ahol $z_i\in I$, vagy pedig $y=1$. Ezért $xab*y=xab$. ∎

5.5 Lemma Ha $x,y\in C^1$ és $x*u=y*u$, ahol u=a vagy b (tehát $|u|=1$), akkor $x=y$.

Bizonyítás Ha $u=b$, akkor az 5.4 Lemma (iii) állításából következik, hogy $x=y$. Legyen $u=a$. Ha $\mu(xa)\neq xa$, akkor $x=x'bb$ alakú, és $\mu(xa)=x'b$. Következik, hogy $\mu(ya)\neq ya$, $y=y'bb$ és $\mu(ya)=y'b$. Kapjuk, hogy $x'b=y'b$, ahonnan $x=y$.

5.6 Tétel (i) C^1-ben érvényes a jobboldali egyszerűsítés szabálya: Ha $x*z=y*z$, akkor $x=y$.
(ii) C-nek nincs idempotens eleme: $x^2\neq x$ $(x\in C)$.

■

Bizonyítás (i) $|z|=1$ esetén ez az 5.5 Lemma állítása. Tegyük fel, hogy $n>1$, az állítás teljesül $|z|<n$ esetén, és legyen $z=z'u$ $(=z'*u)$, ahol $|z|=n$ és $|u|=1$. Ekkor

$$(x*z')*u=x*(z'*u)=x*z=y*z=(y*z')*u,$$

így az 5.5 Lemma és az indukciós feltevés alapján $x=y$.
(ii) $x*x=x$ -ből (i) miatt $x=1$ következne.

5.7 Tétel a irreducibilis C-ben. Ezért C nem írható $C*x$ vagy $y*C$ alakban; speciálisan C-nek nincs növelő eleme.

■

Bizonyítás Könnyen belátható, hogy ρ_0-átmenettel a nem kapható meg egyetlen a-tól különböző F_X-beli elemből sem. ■

5.8 Tétel (i) C minden $\mathcal{R}$-osztálya egyetlen elemből áll. Ha $x=x'a\in C$, akkor $\{x\}$ egyelemű $\mathcal{R}$-osztály. C bármely más $\mathcal{R}$-osztálya $\{xb,xb^2,\ldots\}$ alaku, ahol $x=1$ vagy $x=x'a$.
(ii) Reprezentáljon minden $\mathcal{R}$-osztályt a legrövidebb eleme, tehát az $\{xb,xb^2,\ldots\}$ $\mathcal{R}$-osztályt reprezentálja xb. Legyenek x és y különböző $\mathcal{R}$-osztályok reprezentánsai. $R(x)\supset R(y)$ akkor és csak akkor, ha $y=xu$. Következésképp a $\supset$ reláció nem teljes rendezés C jobbideáljai között.

(iii) Vezessük be C elemei között az alábbi rendezést. Legyen $x=x_m x_{m-1}\dots x_1$, $y=y_n y_{n-1}\dots y_1$ ($|x_i|=|y_j|=1$). Legyen $x<y$, ha az alábbi feltételek valamelyike teljesül:

(1) $m<n$ és $x_i=y_i$ $(i=1,2,\dots,m)$

(2) Van olyan k, hogy $1\le k\le \min\{m,n\}$, $x_i=y_i$ $(1\le i<k)$, $x_k=a$, és $y_k=b$.

A fenti rendezéssel $x<y$ akkor és csak akkor, ha $L(x)\supset L(y)$. A $<$ reláció teljes rendezés, de nem jólrendezés, és duálisan sem az. ∎

Bizonyítás (i) Tegyük fel, hogy $x\mathcal{L}y$. Ekkor $x=u*y$ és $y=v*x$, ezért $y=(v*u)*y$. Az 5.6 Tétel miatt $v*u=1$, és az 5.4 Tétel (v) állítása szerint $u=v=1$, tehát $x=y$.

Tegyük fel, hogy $ua\mathcal{R}y$. Ekkor van v, hogy $ua*v=y$, és van w, hogy $y*w=ua$. Ezért az 5.4 Lemma (vii) állítása miatt $ua=y*w= ua*(v*w)=ua(v*w)$, ahonnan $v*w=1$, és ezért $v=w=1$. Tehát $ua=y$.

Mivel $xb^{n+1}a=xb^n$, kapjuk, hogy $xb,xb^2,\dots$ $\mathcal{R}$-ekvivalens elemek. Most belátjuk, hogy ha $xb\mathcal{R}yb$, ahol $x,y\in Ca\cup\{1\}$, akkor $x=y$. Először megmutatjuk, hogy ha $xab\in C$, akkor $xab\mathcal{R}b$ nem lehetséges. Ellenkező esetben ugyanis lenne u, hogy $b=xab*u$. De az 5.4 Lemma (viii) állítása miatt $|xab*u|\ge 2$, ami ellentmondás.

Tegyük most fel, hogy xab, $yab\in C$ és $xab\mathcal{R}yab$. Ekkor van u és v, hogy $xab*u=yab$ és $xab=yab*v$. Az 5.4 Lemma (viii) állításából következik, hogy $|xab|=|yab|$, és így az 5.4 Lemma (ix) állítása szerint $xab=yab$.

(ii) Tegyük fel, hogy $R(x)\supset R(y)$. Ekkor $y=x*u$. Ha $x=x'a$, akkor az 5.4 Lemma (vii) állítása szerint $y=xu$. Ha $x=b$, akkor nyilván $y=xv$ alaku.

(iii) Ha $x\ne y$, akkor nyilván teljesül vagy (1) vagy (2) (esetleg x-et y-al felcserélve), ezért $x<y$ vagy $x>y$. Ha $x<y$, akkor az 5.4 Lemma (vi) állítása alapján kapjuk, hogy $L(x)\supset L(y)$. Ha-

sonlóan, $x>y$ esetén $L(x)\subset L(y)$.

Ha $x_1=b$, $x_2=ba,\ldots$, $x_n=ba^{n-1}$, akkor $x_1>x_2>\ldots$, így $<$ nem jólrendezés. Ha $c=ba$ és $x_1=c$, $x_2=c^2,\ldots,x_n=c^n,\ldots$, akkor $x_1<x_2<\ldots$, ezért a $<$ reláció duálisan sem jólrendezés.

5.9 Tétel (i) Ha $C=\langle u,v\rangle$ és $v^2*u=v$, akkor $u=a$ és $v=b$.
(ii) C-nek egyetlen automorfizmusa van: az identikus leképezés. ∎

Bizonyítás (i) Mivel $a\in\langle u,v\rangle$ és a irreducibilis, következik, hogy $u=a$. v nem lehet $v=ax$ alaku, hiszen ekkor 5.4(ii) miatt $\langle a,v\rangle$ minden eleme ax alaku lenne. Ezért $v=bw$. Mivel $b\in\langle a,v\rangle$, van x, hogy $b=vx$. Kapjuk, hogy $b\mathcal{R}v$, ezért az 5.8 Tétel szerint $v=b^k$ valamilyen $k\geq 1$ -re. Mivel $-k=s(v)=s(v^2*a)=2s(v)+1=-2k+1$, kapjuk, hogy $k=1$, azaz $v=b$.
(ii) Ha φ tetszőleges automorfizmusa C-nek, $a\varphi=u$ és $b\varphi=v$, akkor u és v eleget tesznek az (i) állítás feltételének, ezért $u=a$ és $v=b$. Ezért φ az identikus leképezés.

5.10 Tétel A C és P félcsoportok közül egyik sem tartalmazza a másikat. ∎

Bizonyítás Az 5.4 Lemma (v) állításából következik, hogy C nem tartalmazhatja P-t.

Tegyük fel, hogy P tartalmazza C-t. Legyen $P=\langle a,b\rangle$ és $ba=1$, továbbá $u=a^ib^j=(i,j)$, $v=a^kb^l=(k,l)$, $v^2*u=v$ és $C=\langle u,v\rangle$. A P-beli szorzási szabály (2.6 Tétel) szerint

$v*u=(k+[i-l]^+,j+[l-i]^+)=(m,n)$ és így

$(k,l)=v*(v*u)=(k,l)(m,n)=(k+[m-l]^+,n+[l-m]^+)$, ahonnan $[m-l]^+=0$, ezért $l=n+[l-m]^+=n+l-m$ és $m=n$. De ekkor $(v*u)^2=(m,n)^2=(m,n)=v*u$, és az 5.6 Tétel miatt $v*u=1$, ezért $u=v=1$, ami ellentmond $C=\langle u,v\rangle$ -nek.

5.11 Definíció Definiáljuk a D félcsoportot, mint a C félcsoport duálisát. Legyen $X=\{a,b\}$ és használjuk a 2.3 Definíció jelöléseit. Legyen $x\in F_X$ és y részszava x-nek. y D-elhagyható, ha $y\in I$, és van $u,v,z\in F_X^1$, hogy $s(z)>0$ és $x=uyzv$. Mint C esetében, most is adódik, hogy x D-maximális részszavai egyértelműen meghatározottak. A C-re vonatkozó összes eredményünk duálisa természetesen érvényes D-re.

Most egy olyan félcsoportot definiálunk, amely homomorf képe C-nek is és D-nek is. Legyen $x\in F_X$, és y részszava x-nek. y-t elhagyhatónak nevezzük, ha C-elhagyható vagy D-elhagyható. A maximális elhagyható részszavakat P_o-maximálisaknak nevezzük. Hasonló állítások érvényesek, mint C esetében.

5.12 Lemma (i) Legyen $x=uvwz$, ahol $v,w\in I$. v akkor és csak akkor elhagyható, ha w elhagyható.
(ii) Ha $x=x_1x_2\ldots x_n$ $(x_i\in X)$ tartalmaz elhagyható részszót, akkor van i, hogy $x_ix_{i+1}x_{i+2}=bba$ vagy baa, tehát x tartalmaz elhagyható alappárt.
(iii) Legyen y P_o-maximális részszava x-nek, és az y-t tartalmazó I-maximális részszó legyen $u=bz_1z_2\ldots z_ka$, ahol $z_i\in I$ $(i=1,\ldots,k)$. Ekkor vagy $y\equiv u$ vagy $y\equiv z_i$ valamilyen i-re.

5.13 Definíció Legyen $P_o\subseteq F_X$ azon szavak halmaza, melyeknek nincs elhagyható részszava. Definiáljuk a $\mu:F_X\to P_o$ leképezést a következőképpen. Ha $x\in F_X$, akkor $\mu(x)$ legyen az a szó, melyet x-ből a P_o-maximális részszavak elhagyásával kapunk. P_o-ban bevezetjük az alábbi műveletet:

$$x*y=\mu(xy) \quad (x,y\in P_o).$$

5.14 Tétel μ homomorfizmus F_X-ről P_o-ra:

(6) $\mu(xy)=\mu(x)*\mu(y) \quad (x,y\in F_X)$.

Ezért P_o a $*$ művelettel félcsoport. A μ-höz tartozó ρ kongruenciát $\rho_o=\{(b^2a,b),(ba^2,a)\}$ generálja.

∎

Bizonyítás μ definíciójából és a 2.4 Lemmából következik, hogy

$$(7) \quad \begin{aligned} &\mu(ubbav)=\mu(ubv) \quad (u,v\in F_X^1), \\ &\mu(ubaav)=\mu(uav) \quad (u,v\in F_X^1). \end{aligned}$$

Legyen $x\in F_X$. Ha $\mu(x)\neq x$, akkor az 5.12 Lemma (ii) állítása szerint $x=x_1=ubbav$ vagy $x=x_1=ubaav$. Az első esetben legyen $x_2=ubv$, a másodikban $x_2=uav$. Hasonlóan képezzük x_2-ből x_3-at, stb. Kapunk egy véges $x=x_1$, x_2, ..., x_k sorozatot, melyre (7) szerint

$$\mu(x)=\mu(x_1)=...=\mu(x_k).$$

Az 5.3 Tétel bizonyításának második részét megismételve kapjuk a tétel állításait.

5.15 Tétel (i) $P_o=\{a^kc^lb^m\colon k+l+m>0\}$, ahol $c=ba$. A P_o-beli szorzási szabály:

$$a^kc^lb^m*a^{k'}c^{l'}b^{m'}=\begin{cases} a^{k+k'-m}c^{l'}b^{m'} & \text{ha } k'>m \\ a^kc^{l+l'+1}b^{m'} & \text{ha } k'=m>0 \\ a^kc^{l+l'}b^{m'} & \text{ha } k'=m=0 \\ a^kc^lb^{m-k'+m'} & \text{ha } k'<m. \end{cases}$$

(ii) P_o-nak nincs idempotens eleme;

(iii) Legyen $u=a^kc^lb^m$ és $u'=a^{k'}c^{l'}b^{m'}$. Az $u'\in R(u)$ reláció akkor és csak akkor igaz, ha az alábbi feltételek valamelyike teljesül:

(a) $k<k'$

(b) $k=k'$ és $l<l'$

(c) $k=k'$, $l=l'$ és $m=0$

(d) $k=k'$, $l=l'$, $m>0$ és $m'>0$.

Következésképp az $u \in R(u')$ és $u' \in R(u)$ relációk közül legalább egy teljesül, továbbá $u' \in R(u)$ esetén $k \le k'$.

A fenti állítások duálisa: $u' \in L(u)$ akkor és csak akkor, ha az alábbi feltételek valamelyike teljesül

(a') $m<m'$

(b') $m=m'$ és $l<l'$

(c') $m=m'$, $l=l'$ és $k=0$

(d') $m=m'$, $l=l'$, $k>0$ és $k'>0$.

Az $u \in L(u')$ és $u' \in L(u)$ relációk közül legalább egy teljesül. $u' \in L(u)$ esetén $m \le m'$.

(iv) Ha $u \neq u'$ és $u \mathcal{R} u'$, akkor $k=k'$, $l=l'$, $m>0$ és $m'>0$. Következésképp P_o $\mathcal{R}$-osztályai:

$\mathcal{R}_{k,l,o}=\{a^k c^l\}$ $(k+l>0)$,

$\mathcal{R}_{k,l,1}=\{a^k c^l b,\ a^k c^l b^2, \dots\}$ $(k+l \ge 0)$.

Hasonlóan kapjuk, hogy P_o $\mathcal{L}$-osztályai:

$\mathcal{L}_{o,l,m}=\{c^l b^m\}$ $(l+m>0)$

$\mathcal{L}_{1,l,m}=\{ac^l b^m,\ a^2 c^l b^m, \dots\}$ $(l+m \ge 0)$.

∎

Bizonyítás A P_o-beli szorzási szabályból mindegyik állítás egyszerű számolással adódik.

5.16 P_o $\mathcal{R}$-osztályai között vezessük be az alábbi rendezést: $\mathcal{R}_{k,l,m} < \mathcal{R}_{k',l',m'}$ ha $k<k'$ vagy $k=k', l<l'$ vagy $k=k', l=l', m<m'$. (Itt m és m' csak 0 vagy 1 lehet. Ezért $m<m'$ -ből $m=0$ és $m'=1$ következik.) A fenti rendezés nyilván jólrendezés, továbbá ha $u \in \mathcal{R}_{k,l,m}$ és $u' \in \mathcal{R}_{k',l',m'}$, akkor az $\mathcal{R}_{k,l,m} < \mathcal{R}_{k',l',m'}$ reláció akkor és csak akkor teljesül, ha $R(u) \supset R(u')$. Ezért P_o fő-jobbideáljai a $<$ relációra nézve duálisan jólrendezettek.

Legyen most R tetszőleges jobbideálja P_o-nak. R nyilván bizonyos $\mathcal{R}$-osztályok egyesítése. Ha ezen $\mathcal{R}$-osztályok legkisebbikének egy eleme u, akkor azonnal adódik, hogy $R=R(u)$. Kapjuk, hogy P_o főideálfélcsoport.

Mivel $b^{k+1}*a^k c^l b^m*a^m=b$ és $b^k*a^k c^l b^m*a^{m+1}=a$, kapjuk, hogy P_o egyszerű. Az 5.15 Tételből azonnal adódik, hogy P_o kombinatorikus.

Egy S félcsoportot CSPI-(Combinatorial Simple Principal Ideal)félcsoportnak nevezünk, ha S kombinatorikus, egyszerű és főideál-félcsoport, továbbá tartalmaz legalább két elemet.

Beláttuk tehát:

5.17 Tétel P_o CSPI-félcsoport.

$\blacksquare$

5.18 Tétel Ha $P_o=\langle u,v\rangle$, $v^2*u=v$ és $v*u^2=u$, akkor $u=a$ és $v=b$.

$\blacksquare$

Bizonyítás A feltételekből adódik, hogy $v*P_o=P_o$ és $P_o*u=P_o$. Kapjuk, hogy $v\mathcal{R}b$ és $u\mathcal{L}a$. Az 5.15 Tétel (iii) állításából következik, hogy $v=b^t$ és $u=a^k$. Mivel $b^t=v=v^2*u=b^{2t}*a^k=b^{2t-k}$, kapjuk, hogy $t=k$. Az s függvény definíciójából (2.3) adódik, hogy tetszőleges $x\in P_o$-ra $k|s(x)$. Mivel $s(a)=1$, kapjuk, hogy $k|1$, azaz $k=1$.

5.19 Következmény P_o-nak nincs más automorfizmusa, mint az identikus leképezés.

$\blacksquare$

5.20 Tétel A P_o és C félcsoportok közül egyik sem tartalmazza a másikat.

$\blacksquare$

Bizonyítás Tegyük fel, hogy C tartalmazza a $P_o=\langle u,v\rangle$ részfélcsoportot, ahol $v^2*u=v$ és $v*u^2=u$. A második egyenlőségből az 5.6 Tétel szerint következik, hogy $v*u=1$, ahonnan 5.4(v) szerint $u=v=1$, ami lehetetlen.

Tegyük most fel, hogy P_o tartalmazza C-t. Legyen $C=\langle u,v\rangle$, és $v^2*u=v$. (Az 5.9 Tétel szerint u és v egyértelműen meghatározottak.) Legyen $u=a^k c^l b^m$ és $v=a^{k'} c^{l'} b^{m'}$. Mivel 5.6 szerint $v^2 \neq v$, és mivel $v^2 * u=v$ miatt $v^2 \mathcal{R} v$, 5.15(iv)-ből következik, hogy $m'>0$ és $v^2=a^{k'} c^{l'} b^{m''}$, ahol $m''>0$. $k'>m'$ nem lehetséges, hiszen akkor $v^2=a^{k'+k'-m'} c^{l'} b^{m'}$ lenne. $k'=m'>0$ sem lehet, mert akkor $v^2=a^{k'} c^{2l'+1} b^{m'}$ lenne. $k'=m'=0$ szintén nem lehet, mert akkor $l'>0$ és $v^2=c^{2l'}$ következne. Ezért

(1) $\quad k'<m',\ 2m'-k'>0$

és

(2) $\quad v^2=a^{k'} c^{l'} b^{2m'-k'}$.

$v^2 * u=v$ -ből (1) és (2) miatt következik, hogy

(3) $\quad 2m'-k'>k$

és

(4) $\quad a^{k'} c^{l'} b^{m'}=v=v^2 * u=a^{k'} c^{l'} b^{2m'-k'} * a^k c^l b^m=a^{k'} c^{l'} b^{m+(2m'-k')-k}$,

ahonnan $m'=m+(2m'-k')-k$, vagyis

(5) $\quad m'-k'=-(m-k)$.

(1) és (5) egybevetéséből

(6) $\quad k>m$.

Elég nagy n-re (5) és (6)-ból kapjuk, hogy

$v * u^n=a^{k'} c^{l'} b^{m'} * a^{k+(n-1)(k-m)} c^l b^m=a^{k+(n-2)(k-m)} c^l b^m=u^{n-1}$,

ellentmondásban a C-beli szorzási szabállyal.

6. CSPI-félcsoportok

Az 5.17 Tétel szerint P_o CSPI-félcsoport. A következőkben belátjuk, hogy minden olyan CSPI-félcsoport, amely két elemmel generálható, homomorf képe P_o-nak; továbbá megadjuk az összes ilyen félcsoport generáló relációit és szorzási szabályát.

6.1 Lemma Ha S egyszerű főideálfélcsoport, és L_o az S maximális $\mathcal{L}$-osztálya (tehát $x\in L_o$, ha $S^1x=S$), akkor L_o részfélcsoportja S-nek. ∎

Bizonyítás Először belátjuk, hogy ha $x\in L_o$, akkor $Sx=S$. Tegyük fel e célból, hogy $Sx\subset S$. Ekkor $L_o=\{x\}$. Mivel S egyszerű, $SxS=S$, és így van u és v, amelyekre $uxv=x$. Ezért $xv\in L_o$, és így $xv=x$. Kapjuk, hogy $x=ux\in Sx$, tehát $Sx=S^1x=S$.

Ha $x,y\in L_o$, akkor a fenti eredmény alapján $Sxy=(Sx)y=Sy=S$, ezért $xy\in L_o$.

6.2 Definíció Legyen a természetes számok $N=\{0,1,2,...\}$ halmazának rendszáma ω. Egy tetszőleges λ rendszámot felbonthatatlannak nevezünk, ha $\lambda=\alpha+\beta$ -ból $\lambda=\beta$ következik. Az első két felbonthatatlan rendszám 1 és ω.

Legyen $O_\lambda=\{\alpha \mid \alpha<\lambda\}$. Belátjuk, hogy ha λ felbonthatatlan, akkor O_λ a rendszámok összeadására nézve zárt, azaz félcsoport.

Legyen $\alpha,\beta \in O_\lambda$. $\alpha+\beta=\lambda$ -ból λ felbonthatatlansága miatt $\beta=\lambda$ következne, ami ellentmondás. Tegyük fel, hogy $\alpha+\beta>\lambda$. Ekkor van $\beta'<\beta$, hogy $\alpha+\beta'=\lambda$, és így $\beta'=\lambda$, ahonnan $\beta>\lambda$, ami ellentmondás. Mivel bármely két rendszám összehasonlítható, a fenti két eset kizárásából következik, hogy $\alpha+\beta<\lambda$.

6.3 Lemma Ha e idempotens eleme az S főideálfélcsoportnak (tehát $e^2=e$), akkor az e-t tartalmazó $\mathcal{L}$-osztálynak e az egyetlen idempotens eleme.

■

Bizonyítás Tegyük fel, hogy $e^2=e$, $f^2=f$ és $e\mathcal{L}f$. Mivel S főideál-félcsoport, ezért $e\in R(f)$ vagy $f\in R(e)$. Legyen pl. $f\in R(e)$. Mivel $e\in L(f)=S^1f$, ezért

(1) $\quad ef=e$.

Mivel e baloldali egységeleme R(e)-nek, ezért $ef=f$. Figyelembe véve (1)-et, kapjuk, hogy $e=f$.

6.4 Lemma Ha R_1 és R_2 jobbideáljai az S félcsoportnak, $R_1\subset R_2$ és $u\in S$, akkor uR_1 és uR_2 jobbideálok, továbbá $uR_1\subseteq uR_2$. Ha R' jobbideál, $uR_1\subset R'\subset uR_2$ és $R=\{x \mid x\in R_2,\ ux\in R'\}$, akkor R jobbideál, $R_1\subset R\subset R_2$ és $uR=R'$. ■

Bizonyítás Az első állítás nem szorul bizonyításra.

Tegyük fel, hogy $x\in R$ és $y\in S$. Mivel $ux\in R'$ és R' jobbideál, $uxy\in R'$. Mivel R_2 jobbideál és $x\in R_2$, $xy\in R_2$. Adódik, hogy $xy\in R$. Kapjuk, hogy R jobbideál. R definíciójából következik, hogy $uR\subseteq R'$. Legyen y tetszőleges eleme R'-nek. Mivel $R'\subset uR_2$, van $x\in R_2$, hogy $ux=y$. Mivel nyilvánvalóan $x\in R$, ezért $y\in uR$. Tehát $R'\subseteq uR$. Kapjuk, hogy $uR=R'$. Az $R_1\subset R\subset R_2$ reláció azonnal adódik.

6.5 Lemma Ha S CSPI-félcsoport és L_o az S maximális $\mathcal{L}$-osztálya, akkor van olyan felbonthatatlan λ, hogy L_o izomorf vagy O_λ-val, vagy $O_\lambda\setminus\{0\}$ -val.

Bizonyítás Ha L_o tartalmaz idempotens elemet, akkor ez nyilván jobboldali egységeleme S-nek. A 6.3 Lemma szerint L_o legfeljebb egy idempotens elemet tartalmazhat. Most belátjuk, hogy L_o kell tartalmazzon legalább egy nem-idempotens elemet. Tegyük fel ugyanis, hogy $e^2=e$ és $L_o=\{e\}$. Tegyük fel, hogy $xy=e$.

Ekkor $e \in L(y)$, ezért $y \in L_o$, tehát $y=e$. Mivel e jobboldali egységeleme $L(e)=S$ -nek, ezért $x=xe=xy=e$. Tehát $xy=e$ csak az $x=y=e$ esetben teljesül. Ebből következik, hogy $S \setminus \{e\}$ kétoldali ideálja S-nek, ellentmondásban azzal, hogy S egyszerű. Ha L_o^* jelöli L_o nem-idempotens elemeinek halmazát, akkor a fenti eredmény szerint $L_o^* \neq \emptyset$. Megmutatjuk, hogy L_o^* részfélcsoportja S-nek. Ha L_o-nak nincs idempotens eleme, akkor $L_o^*=L_o$, és állításunk a 6.1 Lemma. Ha e idempotens eleme L_o-nak, akkor $L_o^*=L_o \setminus \{e\}$. Tegyük fel, hogy $x,y \in L_o^*$, de $xy \in S \setminus L_o^*$, azaz $xy=e$. Mivel e jobboldali egységeleme S-nek, $x^2y=x(xy)=xe=x$, ahonnan $x^2 \mathcal{R} x$; és mivel S kombinatorikus, $x^2=x$, ahonnan $x=e$, ami ellentmond feltevésünknek. Ha $x \in L_o^*$, akkor a fenti eredményből az is következik, hogy $e \in R(x)$ nem lehetséges, ezért $x \in R(e)$, ahonnan

$$ex=x \quad (x \in L_o).$$

Tehát e kétoldali egységeleme L_o-nak.

Mivel S kombinatorikus, L_o-nak bármely $\mathcal{R}$-osztállyal vett metszete legfeljebb egy elemet tartalmaz. Ezért bevezethetjük L_o elemei között a következő rendezést:

(1) $\quad x<y$ ha $R(x) \supset R(y)$.

Mivel S főideálfélcsoport, ezért az (1) relációval L_o jólrendezett. Legyen L_o^* legkisebb eleme a. Mivel $xS^1 \supseteq xaS^1$, ezért

$$x \leq xa \quad (x \in L_o).$$

Belátjuk, hogy itt nem állhat egyenlőség. Tegyük fel, hogy $x \in L_o$ és $x=xa$. Mivel $x \in L_o$, van $t \in S^1$, hogy $a=tx$, és így $a^2=txa=tx=a$, ellentmondásban az a-ra tett feltevésünkkel. Tehát

(2) $\quad x<xa \quad (x \in L_o)$.

Most belátjuk, hogy x és xa között nincs eleme L_o-nak, azaz

(3) $\quad xa=\min\{y \mid x<y\} \quad (x \in L_o)$.

Tegyük fel e célból, hogy van olyan $x \in L_o$, melyre nem teljesül (3), azaz

(4) $\quad y \in L_o$ és $x<y<xa$.

Ekkor $y=xt$ valamilyen $t\in L_o$-ra. t nem lehet idempotens, hiszen akkor $xt=x$ következne. (4) miatt $t=a$ sem lehet. Kapjuk, hogy $a<t$, ezért $t=as$ valamilyen $s\in L_o$-ra; és így

$$y=xt=xas\geq xa,$$

ellentmondásban (2)-vel.

Mivel L_o^* jólrendezett, és legkisebb eleme a, van olyan egyértelműen meghatározott λ rendszám, hogy az $O_\lambda\backslash\{O\}$ jólrendezett halmaz rendszáma megegyezik L_o^* rendszámával. Így létezik (egyértelműen meghatározott) $\varphi:L_o^*\dashrightarrow O_\lambda\backslash\{O\}$ monoton 1-1 leképezés. (Mivel (2) miatt L_o^* nem véges halmaz, $O_\lambda\backslash\{O\}$ és O_λ rendszáma megegyezik, tehát definiálhattuk volna λ-t mint L_o rendszámát.) (3)-ból kapjuk, hogy

(5) $\quad \varphi(a)=1$ és $\varphi(xa)=\varphi(x)+1 \quad (x\in L_o^*)$.

Következésképp $y=a$ -ra teljesül, hogy

(6) $\quad \varphi(xy)=\varphi(x)+\varphi(y)$.

Megmutatjuk, hogy ha $z\in L_o$ és (6) teljesül minden $y<z$ esetén, akkor teljesül $y=z$ -re is. Feltehetjük, hogy $a<z$. Mivel $\varphi(x)+\varphi(z)$ a legkisebb olyan rendszám, amely tetszőleges $y<z$ esetén nagyobb mint $\varphi(x)+\varphi(y)=\varphi(xy)$, ezért elegendő azt belátnunk, hogy

(7) $\quad xz>xy \quad (y<z)$;

és

(8) $\quad$ ha $u>xy \quad (y<z)$, akkor $u\geq xz$.

Ha $y<z$, akkor (3) szerint $ya\leq z$, ahonnan $xy<xya\leq xz$. Ezzel beláttuk (7)-et. Tegyük fel, hogy (8) nem teljesül valamilyen u-ra, azaz

(9) $\quad u>xy \quad (y<z)$, de $xz>u$.

Mivel $a<z$, (9) szerint $xa<u$, ahonnan $u=xat$ valamilyen $t\in L_o$-ra. Tehát $u=xat<xz$, ahonnan a 6.4 Lemma szerint $at<z$. $y=at$-ra alkalmazva (9)-et, kapjuk, hogy $u>xat=u$, ami ellentmondás. Ezzel igazoltuk (8)-at. Beláttuk:

(10) $\quad \varphi(xy)=\varphi(x)+\varphi(y) \quad (x,y\in L_o^*)$,

tehát φ izomorfizmus L_o^*-ról $O_\lambda \setminus \{0\}$ -ra. (10)-ből az is következik, hogy O_λ zárt a rendszámok összeadására nézve, ezért λ felbonthatatlan.

Ha L_o-nak van e idempotens eleme, akkor e kétoldali egységeleme L_o-nak, ezért e=min L_o, és a $\varphi(e)=o$ definícióval φ izomorfizmus L_o-ról O_λ-ra.

6.6 Definíció Ha $\sigma<\lambda$, akkor legyen definíció szerint $a^\sigma=\varphi^{-1}(\sigma)$. (10)-ből következik, hogy $a^\rho a^\sigma=a^{\rho+\sigma}$. (5)-ből következik, hogy véges n esetén a^n-nek a fenti definíciója megegyezik a szokásos (n-edik hatvány) definícióval. Ezért a^σ-t az a elem "transzfinit hatványának" nevezhetjük.

A 6.5 Lemmának tekinthetjük a duális változatát is. Legyen R_o^* legkisebb eleme b. Ekkor R_o elemei egyértelműen a b^ν alakban írhatók, és

$$b^{\sigma+\rho}=b^\rho b^\sigma .$$

CSPI-félcsoportok esetében a és b továbbra is jelentsék L_o ill. R_o minimális nem-idempotens elemét.

6.7 Definíció Legyen λ felbonthatatlan rendszám. Az O_λ-t önmagába képező transzformációk félcsoportját jelölje T_λ. Ha ρ, $\sigma \in O_\lambda$, akkor az a_ρ és b_σ T_λ-beli transzformációkat a következőképpen definiáljuk:

$$\nu a_\rho=[\nu-\rho]=\begin{matrix}\delta & \text{ha } \rho\leq\nu=\rho+\delta, \\ o & \text{ha } \nu<\rho;\end{matrix}$$

$$\nu b_\sigma=\sigma+\nu .$$

6.8 Lemma Ha $a_\rho b_\sigma=a_\mu b_\eta$, akkor $\rho=\mu$ és $\sigma=\eta$.

Bizonyítás Mivel $\sigma=\rho a_\rho b_\sigma=\rho a_\mu b_\eta=\eta+[\rho-\mu]$, ezért $\eta\leq\sigma$. Hasonlóan, $\sigma\leq\eta$; és így $\sigma=\eta$. Mivel

$$\sigma+[\mu-\rho]=\mu a_\rho b_\sigma=\mu a_\mu b_\sigma=\sigma ,$$

ezért $[\mu-\rho]=o$, azaz $\mu\leq\rho$. Hasonlóan, $\rho\leq\mu$. Kapjuk, hogy $\rho=\mu$.

6.9 Definíció Legyen B_λ az $a_\rho b_\sigma$ alaku, T_λ-beli transzformációk halmaza. A 6.8 Lemma szerint az $a_\rho b_\sigma$ transzformáció helyett írhatunk egyszerűen (ρ,σ)-t.

6.10 Tétel (i) B_λ részfélcsoportja T_λ-nak. Neve: λ-biciklikus félcsoport. B_λ szorzási szabálya:

$$(\rho,\sigma)(\mu,\eta)=(\rho+[\mu-\sigma],\eta+[\sigma-\mu]);$$

(ii) B_λ CSPI-félcsoport;

(iii) $B_\omega=P$ a biciklikus félcsoport (2.5 Definíció).

Bizonyítás (i) Az alábbi azonosságok könnyen ellenőrizhetők:

$$b_\sigma a_\mu=a_{[\mu-\sigma]}b_{[\sigma-\mu]},$$
$$a_\rho a_\mu=a_{\rho+\mu},$$
$$b_\sigma b_\eta=b_{\eta+\sigma}.$$

A fenti azonosságok felhasználásával

$$a_\rho b_\sigma a_\mu b_\eta=a_\rho a_{[\mu-\sigma]}b_{[\sigma-\mu]}b_\eta=a_{\rho+[\mu-\sigma]}b_{\eta+[\sigma-\mu]}.$$

(ii) Közvetlen számolással ellenőrizhető, hogy

$$(o,\rho)(\rho,\sigma)(\sigma,o)=(o,o)=1,$$

ezért B_λ egyszerű. Továbbá B_λ $\mathcal{R}$- és $\mathcal{L}$-osztályai:

$$R_{(\rho,\sigma)}=\{(\rho,\nu)\mid \nu<\lambda\},\quad R(\rho,\sigma)=\{(\mu,\eta)\mid \mu\geq\rho\},$$
$$L_{(\rho,\sigma)}=\{(\nu,\sigma)\mid \nu<\lambda\},\quad L(\rho,\sigma)=\{(\mu,\eta)\mid \eta\geq\sigma\};$$

ahonnan $R_{(\rho,\sigma)}\cap L_{(\mu,\eta)}=(\rho,\eta)$, ezért B_λ kombinatorikus.

Ha R tetszőleges jobbideálja B_λ-nak, akkor ρ legyen az a legkisebb rendszám, melyre $R_{(\rho,o)}\cap R\neq\emptyset$. Azonnal adódik, hogy $R=R(\rho,o)$, ezért B_λ főideálfélcsoport.

(iii) P szorzási szabályából (2.6 Tétel) következik, hogy $P=B_\omega$.

6.11 Definíció B_λ maximális jobbideálját jelölje $B_\lambda^*=R(1,o)$. Nyilvánvaló, hogy $B_\lambda^*=\{(\rho,\sigma)\mid \rho\geq1\}$.

6.12 Tétel Legyen S CSPI-félcsoport, és $L_o \cong O_\lambda$. Ha S-nek van e_r jobboldali egységeleme, akkor B_λ homomorf képe S-nek. Ha S-nek nincs jobboldali egységeleme, akkor B_λ^* homomorf képe S-nek.

Bizonyítás Ha S-nek van e_r jobboldali egységeleme, akkor a 6.5 Lemma szerint $e_r=a^o$, tehát

(1) $xa^o=x$ $(x\in S)$.

Ha S-nek nincs jobboldali egységeleme, akkor a^o-t tekintsük egy S-hez "hozzávett" jobboldali egységelemnek. (De ebben az esetben a^o-t nem tekintjük S-beli elemnek.) Így (1) mindkét esetben érvényes.

Legyen x tetszőleges eleme S-nek. A 4.3 Lemma szerint van $\sigma<\lambda$, hogy $xa^\sigma\in L_o$. Ezért definiálhatjuk a $\psi:S\text{-->}B_\lambda$ leképezést a következőképpen:

$\psi(x)=(\rho,\sigma)$ ha $xa^\sigma=a^\rho$ és $xa^\tau\notin L_o$ ha $\tau<\sigma$.

Speciális esetként kapjuk, hogy $\psi(a^\rho)=(\rho,o)$.

Először belátjuk, hogy ψ homomorfizmus. Legyen $\psi(x)=(\rho,\sigma)$ és $\psi(y)=(\rho',\sigma')$. Két eset lehet.

Az első esetben $\sigma\geq\rho'$, azaz van ξ, hogy $\sigma=\rho'+\xi$, és

$$xya^{\sigma'+\xi}=xa^{\rho'+\xi}=xa^\sigma=a^\rho.$$

Ha $\tau<\sigma'+\xi$, akkor $xya^\tau\notin L_o$. Ha ugyanis $\tau<\sigma'$, akkor $ya^\tau\notin L_o$, és ezért $xya^\tau\notin L_o$; ha pedig $\tau\geq\sigma'$, akkor van ξ', hogy $\tau=\sigma'+\xi'$, ahol $\xi'<\xi$, és így $xya^\tau=xa^{\rho'+\xi'}\notin L_o$, mivel $\rho'+\xi'<\rho'+\xi=\sigma$.

A második esetben $\sigma<\rho'$, azaz van $\eta>o$, hogy $\rho'=\sigma+\eta$. Ekkor

$$xya^{\sigma'}=xa^{\sigma+\eta}=a^{\rho+\eta},$$

és $xya^\tau\notin L_o$ ha $\tau<\sigma'$, hiszen ekkor még $ya^\tau\in L_o$ sem teljesül.

Mindkét esetben igaz tehát, hogy

$$\psi(xy)=(\rho+[\rho'-\sigma],\sigma'+[\sigma-\rho'])=\psi(x)\psi(y),$$

tehát ψ homomorfizmus.

Most már csak azt kell megmutatnunk, hogy B_λ ill. B_λ^* tetszőleges (ρ,σ) eleméhez van $x\in S$, hogy $\psi(x)=(\rho,\sigma)$.

Legyen a^δ a minimális eleme L_o-nak. (Tehát δ=o vagy 1.)

Legyen σ tetszőleges ($<\lambda$). Ekkor van $x\in S$, hogy

(2) $xa^{\sigma}=a^{\delta}$.

Ha $\sigma=o$, akkor $x=a^{\delta}$, és így

(3) $\psi(x)=(\delta,\sigma)$.

Ha $\sigma>o$, akkor szintén teljesül (3). Tegyük fel ugyanis, hogy $\tau<\sigma=\tau+\xi$, és $xa^{\tau}\in L_o$ azaz $xa^{\tau}=a^{\rho}$ valamilyen ρ-ra. Ekkor (2) miatt

$$a^{\delta}=xa^{\tau+\xi}=a^{\rho+\xi},$$

ami lehetetlen, hiszen $\rho+\xi>\rho\geq\delta$.

Tehát (3) tetszőleges σ esetén következik (2)-ből, ezért tetszőleges σ-hoz van x, hogy (3) teljesül.

Tetszőleges σ-ra definiáljuk az

$$S_{\sigma}=\{y \mid \psi(y)=(\rho,\tau),\ \tau\geq\sigma\}$$

halmazt. Mivel ψ homomorfizmus, S_{σ} balideál, és így $S_{\sigma}a^{\sigma}$ is balideál. Mivel a (3)-ban szereplő x eleme S_{σ}-nak, ezért $a^{\delta}=xa^{\sigma}\in S_{\sigma}a^{\sigma}$, és mivel $a^{\delta}\in L_o$, kapjuk, hogy $S_{\sigma}a^{\sigma}=S$. Így tetszőleges ρ esetén, ha $\delta\leq\rho<\lambda$, található $t_{\rho}\in S_{\sigma}$, hogy $t_{\rho}a^{\sigma}=a^{\rho}$. S_{σ} definíciójából következik, hogy $\psi(t_{\rho})=(\rho,\sigma)$.

Arra jutottunk, hogy ha $\delta\leq\rho<\lambda$ és $\sigma<\lambda$, akkor $\psi^{-1}(\rho,\sigma)$ nemüres, tehát $\psi(S)=B_{\lambda}$ vagy B_{λ}^{*}, annak megfelelően, hogy $\delta=o$ vagy 1.

6.13 LEMMA Legyen S CSPI-félcsoport, továbbá λ és ψ értelmezése ugyanaz, mint a 6.12 Tételben. Ha $o<\tau<\lambda$, τ felbonthatatlan és C generátorrendszere S-nek (tehát $S=\langle C\rangle$), akkor C tartalmaz olyan x-et és y-t, melyekre $\psi(x)=(\xi+\tau,\xi')$ és $\psi(y)=(\eta,\eta'+\tau)$ teljesül valamilyen ξ, ξ', η és η' mellett.

Bizonyítás Nevezzük a ν rendszámot az α rendszám komponensének, ha $\alpha=\rho+\nu$ valamilyen ρ-ra. Ha ν felbonthatatlan, akkor könnyen ellenőrizhető, hogy ν akkor és csak akkor komponense $\alpha+[\beta-\gamma]$ -nak, ha $\beta\leq\gamma$ és ν komponense α-nak, vagy $\beta>\gamma$ és ν komponense β-nak.

Tegyük fel, hogy $\psi(C)$ nem tartalmaz pl. $(\xi+\tau,\xi')$ alaku elemet. Mivel $\langle\psi(C)\rangle=\psi(S)$, a fenti megállapítás és B_λ szorzási szabálya alapján kapjuk, hogy $\psi(S)$ sem tartalmazhat $(\xi+\tau,\xi')$ alaku elemet, de ugyanakkor pl. $(\tau,o)\in\psi(S)$, ami ellentmondás.

6.14 Lemma Legyen S CSPI-félcsoport és $b^\sigma\in R_o$. Ekkor van olyan (egyértelműen meghatározott) $\chi(\sigma)$ rendszám, hogy az $a^\rho \to b^\sigma a^\rho$ leképezés az $\{a^\rho \mid \lambda>\rho\geq\chi(\sigma)\}$ halmazt monoton és 1-1 módon L_o-ra képezi le.

∎

Bizonyítás A 6.1 Lemma bizonyítása során beláttuk, hogy $xS=S$ ha $x\in R_o$. Ezért $b^\sigma S=S$, és így van $x\in S$, hogy $b^\sigma x=a^\delta$, ahol a^δ a legkisebb eleme L_o-nak. Legyen $x=a^{\chi(\sigma)}$. A bizonyítandó állítás most már a 6.5 Lemmából adódik.

6.15 Lemma A $\chi(\sigma)$ függvény monoton.

Bizonyítás Mivel

$$b^{\sigma+\rho}a^{\chi(\sigma)}=b^\rho b^\sigma a^{\chi(\sigma)}=b^\rho a^\delta,$$

ezért

$$b^{\sigma+\rho}a^{\chi(\sigma)+[\chi(\rho)-\delta]}=b^\rho a^{\delta+[\chi(\rho)-\delta]}=b^\rho a^{\chi(\rho)}=a^\delta;$$

és így

$$\chi(\sigma+\rho)=\chi(\sigma)+[\chi(\rho)-\delta]\geq\chi(\sigma).$$

6.16 Lemma Ha az S CSPI-félcsoportnak van kétoldali e egységeleme, akkor $L_o\cap R_o=\{e\}$, egyébként $L_o\cap R_o=\emptyset$.

Bizonyítás Tegyük fel, hogy $u=a^\rho=b^\eta\in L_o\cap R_o$. Ekkor van $x\in L_o$, hogy $a^\rho x=a$. Legyen $x=a^\sigma$. Ekkor a 6.5 Lemma szerint $\rho+\sigma=1$. Ha $\rho=1$, akkor a^ρ nem lehet eleme R_o-nak, hiszen $a^o<a^\rho$ és $a^o\in R_o$. Tehát $\rho=1$ nem lehet, és így $\rho=0$. Hasonlóan kapjuk, hogy $\eta=0$.

Ezért u jobb- és baloldali egységeleme S-nek.

■

6.17 Lemma Legyen S CSPI-félcsoport.

A/ Az alábbi három (egymást kizáró) eset lehetséges:

(a) $b^2a=b$, $ba^2=a$

(b) $b^\sigma a=b$ (σ végtelen), $ba=a$

(c) $ba=b$, $ba^\rho=a$ (ρ végtelen).

B/ Ha S-nek van jobboldali e_r egységeleme, de nincs baloldali egységeleme, akkor az alábbi két (egymást kizáró) eset lehetséges:

(d) $ba=e_r$ $(\dashrightarrow b^2a=b)$

(e) $ba=b$, $ba^\rho=e_r$ (ρ végtelen).

C/ Ha S-nek van baloldali e_l egységeleme, de nincs jobboldali egységeleme, akkor a B/-nek megfelelő duális állítás érvényes.

D/ Ha e kétoldali egységeleme S-nek, akkor

$$ba=e.$$

■

Bizonyítás A 6.14 Lemma szerint van egyértelműen meghatározott ρ rendszám, hogy

(1) $\quad ba^\rho=a,$

és van egyértelműen meghatározott σ rendszám, hogy

(2) $\quad b^\sigma a=b.$

A1/ Tegyük fel, hogy $\rho=m$ és $\sigma=n$ véges számok. Tehát (1) és (2) most az alábbi alakban írhatók:

$$ba^m=a, \quad b^na=b.$$

A 6.16 Lemmából adódik, hogy $m>0$ és $n>0$, hiszen pl. $m=0$ -ból $a=ba^0=be_r=b$ következne.

Belátjuk, hogy $m>1$ és $n>1$. Tegyük fel, hogy pl. $n=1$. Ekkor $ba=b$, és így $a=ba^m=baa^{m-1}=ba^{m-1}=\ldots=ba=b$, ami ellentmondás.

Mivel

(3) $\quad a=ba^m=b^na^{m+1}=b^{n-1}(ba^m)a=b^{n-1}a^2,$

ezért $a\in L(ba^2)$, és így $ba^2\in L_0$, azaz $ba^2=a^\mu$ valamilyen μ-re.

$\mu=0$ nem lehet, hiszen akkor (3) szerint n=2 esetén $a^1=a^0$ következne; n>2 esetén pedig $a=b^{n-2}ba^2=b^{n-2}e_r=b^{n-2}$. $\mu>1$ sem lehet, hiszen ekkor a 6.14 Lemma szerint m=1 lenne. Kapjuk, hogy $\mu=1$, és így $ba^2=a$. Hasonlóan, $b^2a=b$.

A2/ Tegyük most fel, hogy σ végtelen. Belátjuk, hogy $\rho>1$ nem lehetséges. Legyen ugyanis $1<\rho=1+\rho'$. Ekkor

(4) $b=b^\sigma a=b^\sigma ba^\rho=b^{1+\sigma}a^{1+\rho'}=b^\sigma aa^{\rho'}=ba^{\rho'}$.

ρ nem lehet végtelen, hiszen akkor $\rho'=\rho$, és (4)-ből $b=ba^\rho=a$ következne. Tehát $\rho=m$ véges, és feltevésünk szerint m>1. (4) most a következő alakot ölti:

(4') $b=ba^{m-1}$.

Innen m-1>0 miatt következik, hogy $ba\in R_0$. Legyen $ba=b^\eta$. (4')-ből következik, hogy

$$b^\eta=ba=ba^m=a,$$

ami ellentmondás. Mivel a $\rho>1$ feltevés ellentmondáshoz vezetett, kapjuk, hogy $\rho=1$, ami a (b) esetnek felel meg.

A3/ Ha ρ végtelen, akkor a duális gondolatmenettel adódik (c).

B/ Tegyük fel, hogy e_r jobboldali egységeleme S-nek. A 6.5 Lemma alapján $e_r=a^0$.

Ha az (a) eset áll fenn ($b^2a=b$ és $ba^2=a$), akkor a 6.14 Lemma miatt $ba=e_r$. Tehát (d) teljesül.

Ha a (c) eset áll fenn ($ba=b$ és $ba^\rho=a$, ahol ρ végtelen), akkor ugyancsak a 6.5 Lemma alapján létezik ρ', melyre $\rho=\rho'+1$ és $ba^{\rho'}=e_r$. Így most az (e) esetet kapjuk.

A (b) eset nem foroghat fenn, hiszen ba=a -ból a 6.5 Lemma szerint $b=be_r=ba^0=a^0=e_r$ következne.

C/ Ez a duálisa B/-nek.

D/ Legyen e (kétoldali) egységeleme S-nek. Mivel e jobboldali egységelem, a (c) eset nem állhat fenn. Kapjuk, hogy az (a) esetnek kell igaznak lennie, ahonnan a 6.14 Lemma miatt ba=e.

6.18 Tétel Legyen e egységeleme az S CSPI-félcsoportnak. A 6.5

Lemma szerint L_o izomorf O_λ-val, R_o pedig O_χ-vel, valamilyen felbonthatatlan λ és χ rendszámokra. A következő állítások teljesülnek:

(i) $\lambda=\chi$

(ii) $S_1=\langle a,b\rangle$ minden eleme egyértelműen az $a^\alpha b^\beta$ alakban írható, ahol $\alpha<\lambda$ és $\beta<\lambda$. Ha $\psi(a^\alpha b^\beta)=(\alpha,\beta)$, akkor ψ izomorfizmus S_1-ről B_λ-ra. (Az itt szereplő ψ a 6.12 Tételbeli ψ megszorítása S_1-re.)

Bizonyítás Legyen $\lambda\leq\chi$. Először belátjuk, hogy

(1) $\quad b^\nu a^\nu=e \quad (\nu<\lambda)$.

$\nu=1$ -re ez a 6.17 Lemma D/ állítása. Tegyük fel, hogy (1) nem teljesül valamilyen ν-re; legyen ez a ν minimális $(0<\nu<\lambda)$. Mivel $b^\nu\in R_o$, ezért van x, hogy $b^\nu x=e$. Mivel $x\in L_o$, $x=a^\rho$ valamilyen $\rho<\lambda$ -ra. $\rho<\nu$ nem lehet, hiszen $\rho<\nu=\rho+\delta$ esetén $b^\delta=b^\delta e$ $=b^\delta b^\rho a^\rho=b^{\rho+\delta}a^\rho=b^\nu x=e$ következne. Tehát

(2) $\quad b^\nu a^\rho=e, \quad \nu\leq\rho=\nu+\rho'$.

Hasonlóan,

(3) $\quad b^\tau a^\nu=e, \quad \nu\leq\tau=\nu+\tau'$.

(2) és (3)-ból kapjuk, hogy

$$a^{\rho'}=ea^{\rho'}=(b^\tau a^\nu)a^{\rho'}=b^{\nu+\tau'}(a^\nu a^{\rho'})=b^{\tau'}b^\nu a^\rho=b^{\tau'}e=b^{\tau'},$$

ahonnan a 6.16 Lemma alapján $\rho'=\tau'=0$, és így $b^\nu a^\nu=e$, ellentmondásban feltevésünkkel.

Tegyük fel, hogy $\lambda<\chi$. Mivel $b^\lambda\in R_o$, van $x\in L_o$, hogy $b^\lambda x=e$. Legyen $x=a^\nu$, ahol $\nu<\lambda=\nu+\lambda'$. Ekkor $b^{\lambda'}=b^{\lambda'}e=b^{\lambda'}b^\nu a^\nu=b^\lambda x=e$, ami ellentmondás. Hasonlóan, $\lambda>\chi$ sem lehetséges.

(ii) (1)-ből adódik, hogy

(4) $\quad b^\beta a^\alpha=a^{[\alpha-\beta]}b^{[\beta-\alpha]}$,

így S_1 minden eleme $a^\alpha b^\beta$ alaku. Tegyük fel, hogy $a^\alpha b^\beta=a^{\alpha'}b^{\beta'}$. Legyen pl. $\alpha\leq\alpha'=\alpha+\delta$. Ekkor

$$b^{\beta'}=(b^{\alpha'}a^{\alpha'})b^{\beta'}=b^{\alpha'}a^\alpha b^\beta=b^{\beta+\delta},$$

ahonnan $\beta'=\beta+\delta$, így

$$e=b^{\alpha}(a^{\alpha}b^{\beta})a^{\beta}=b^{\alpha}a^{\alpha'}b^{\beta'}a^{\beta}=a^{\delta}b^{\delta},$$

ahonnan $a^{\delta}\in R_o$ és $b^{\delta}\in L_o$, ezért $\delta=0$, vagyis $\alpha=\alpha'$ és $\beta=\beta'$.

(4)-ből azonnal adódik, hogy ψ izomorfizmus.

7. A két elemmel generálható CSPI-félcsoportok

7.1 Lemma Ha az S CSPI-félcsoportot két eleme generálja, és λ ugyanaz, mint a 6.5 Lemmában, akkor

(i) $\lambda=\omega$

(ii) $S=\langle a,b\rangle$ (a és b a 6.6 Definíció szerinti)

(iii) $b^2a=b$ és $ba^2=a$.

∎

Bizonyítás (i) Legyen ψ a 6.5 Tétel bizonyítása során definiált leképezés, továbbá legyen $S=\langle x,y\rangle$.

Nyilvánvaló, hogy L_0-nak tartalmaznia kell x és y közül legalább az egyiket. Legyen pl. $x\in L_0$. Ekkor $\psi(x)=(\xi,0)$ valamilyen ξ-re. A 6.13 Lemmából a $\tau=1$ esetben következik, hogy $\psi(y)=(\eta,\eta'+1)$ valamilyen η és η' mellett. Ezért az idézett Lemmából a $\tau=\omega$ esetben az is következik, hogy $(1,\omega)\notin B_\lambda$, azaz $\lambda\leq\omega$, ahonnan $\lambda=\omega$.

(ii) A fentiek szerint $x=a^k$ és $y=b^m$ valamilyen pozitiv és véges k és m -re. Így $S=\langle a,b\rangle$ is teljesül.

(iii) A 6.17 Lemma (b) és (c) esetei $\lambda=\omega$ miatt nem lehetségesek, tehát (a)-nak kell teljesülnie.

7.2 Következmény Bármely, két elemmel generálható CSPI-félcsoport homomorf képe P_0-nak.

∎

7.3 Lemma (i) Főideálfélcsoport homomorf képe főideálfélcsoport.

(ii) Egyszerű félcsoport homomorf képe egyszerű félcsoport.

∎

Megjegyzés Az viszont már nem igaz, hogy kombinatorikus félcsoport homomorf képe kombinatorikus. Pl. ha $P=\langle a,b\rangle$ a 2.5 Definíció szerinti biciklikus félcsoport, és $s(a^ib^j)=i-j$, akkor s homomorfizmus és $s(P)=Z$ az egészek additiv csoportja, amely nem kombinatorikus.

7.4 Lemma Legyen π homomorfizmus P_o-ról $P_o\pi$ -re, $P_o\pi$ kombinatorikus, a π-hez tartozó kongruenciareláció (1.1 Tétel) pedig legyen ϖ. Tegyük fel, hogy $x,y\in P_o$, $x\varpi y$ és $L(x)\supseteq L(y)$, $R(x)\supseteq R(y)$. Ha $L(x)\supseteq L(z)\supseteq L(y)$ és $R(x)\supseteq R(z)\supseteq R(y)$, akkor $x\varpi z$ (és $y\varpi z$).

■

Bizonyítás Mivel $L(x)\pi=(P_o^1x)\pi=(P_o^1\pi)(x\pi)=(P_o^1\pi)(y\pi)=L(y)\pi$, kapjuk, hogy $L(x)\pi=L(z)\pi=L(y)\pi$, vagyis $x\pi\ \mathcal{L}\ z\pi\ \mathcal{L}\ y\pi$. Hasonlóan kapjuk, hogy $x\pi\ \mathcal{R}\ z\pi\ \mathcal{R}\ y\pi$. Adódik, hogy $x\pi\ \mathcal{H}\ z\pi\ \mathcal{H}\ y\pi$, ahonnan a feltevés szerint $x\pi=z\pi$.

■

7.5 Lemma Tegyük fel, hogy a 7.4-ben szereplő π homomorfizmus nem triviális. Ha $a^kc^lb^m\in P_o$, $a^{k'}c^{l'}b^{m'}\in P_o$ és

(1) $\qquad a^kc^lb^m\ \varpi\ a^{k'}c^{l'}b^{m'}$,

akkor $k=k'$ és $m=m'$.

■

Bizonyítás Tegyük fel, hogy $k\leq k'$. (1) mindkét oldalát balról $b^{k+k'+1}$-el szorozva:

(2) $\qquad b^{m+k'+1}\varpi\ b^{m'+k+1}$.

Két eset lehetséges.

(a) $m+k'\neq m'+k$. A 7.4 Lemmából következik, hogy található $s>0$, melyre

$$b^s\ \varpi\ b^{s+1}.$$

A fenti kongruenciát jobbról a megfelelő hatványaival szorozva:

(3) $\qquad b\ \varpi\ b^2,\quad c\varpi\ b,\quad a\ \varpi\ c.$

Legyen $u=b\varpi$. (3)-ból következik, hogy $u^2=u$, és tetszőleges k, l, m esetén

$$a^kc^lb^m\pi\ =\ u^ku^lu^m=u,$$

tehát π triviális homomorfizmus.

(b) $m+k'=m'+k$, vagy más alakban $m'-m=k'-k=v$. Tegyük fel, hogy

- állításunkkal ellentétben - $v \neq 0$, pl. $v > 0$. Szorozzuk meg (1)-et balról $b^{k'}$-vel, jobbról pedig $a^{m'}$-vel:

$$c \,\pi\, c^{l'+2},$$

ahonnan a 7.4 Lemma szerint

$$c \,\pi\, c^{2}.$$

Ebből következik, hogy

(4) $\qquad c \,\pi\, c^{i} \quad (i=1,2,\ldots).$

Ha (1)-et megszorozzuk balról b^{k}-val, jobbról pedig a^{m}-el, akkor (4)-et is felhasználva kapjuk, hogy

$$c \,\pi\, a^{v}b^{v} \quad \text{vagy} \quad c \,\pi\, a^{v}cb^{v},$$

annak megfelelően, hogy $l'=0$ vagy $l'>0$. Mivel

$$L(c) \supset L(ab) \supseteq L(a^{v}b^{v}) \supset L(a^{v}cb^{v})$$

és

$$R(c) \supset R(ab) \supseteq R(a^{v}b^{v}) \supset R(a^{v}cb^{v}),$$

a 7.4 Lemma miatt

(5) $\qquad c \,\pi\, ab.$

Legyen $\alpha = a\pi$, $\beta = b\pi$. (5)-ből következik, hogy

(6) $\qquad \alpha\beta = \beta\alpha = \tau.$

Mivel $\alpha\tau = \tau\alpha = \alpha$ és $\beta\tau = \tau\beta = \beta$, τ kétoldali egységeleme $P_{o}\pi$-nek. (6)-ból következik, hogy $P_{o}\pi$ (véges vagy végtelen) ciklikus csoport, amely nem kombinatorikus, kivéve az $\alpha = \beta$ esetet, ez azonban π trivialitását jelentené, amit kizártunk.

∎

7.6 Lemma Legyen az S CSPI-félcsoport nem-triviális homomorf képe P_{o}-nak. Ekkor az alábbi egyenlőségek közül legalább egy teljesül (itt a és b a P_{o}-beli a ill. b homomorf képe):

(α_n) $\qquad c^{n} = c^{n+1}$

(β_n) $\qquad ac^{n} = ac^{n+1}$

(γ_n) $\qquad c^{n}b = c^{n+1}b$

(δ_n) $\qquad ac^{n}b = ac^{n+1}b.$

∎

Bizonyítás Legyen az állításban szereplő homomorfizmushoz tartozó kongruencia π. A 7.5 Lemma szerint

(1) $\quad a^k c^l b^m \,\pi\, a^k c^{l'} b^m \quad (l<l')$

valamilyen nemnegativ k,l,l',m mellett.

(a) k=m=0. Ekkor l>0. A 7.4 Lemma szerint $c^l \pi\, c^{l+1}$. Ez az (α_1) eset.

(b) k>0, m=0. (1)-et balról szorozva b^{k-1}-el: $ac^l \pi\, ac^{l'}$. A 7.4 Lemmát alkalmazva: $ac^l \pi\, ac^{l+1}$, ez (β_1).

(c) k=0, m>0. Ez (b)-nek a duálisa.

(d) k>0, m>0. (1)-et balról b^{k-1}-el, jobbról a^{m-1}-el szorozva: $ac^l b \,\pi\, ac^{l'} b$, ahonnan a 7.4 Lemmával $ac^l b \,\pi\, ac^{l+1} b$, ami a ($\delta_1$) eset.

7.7 Definíció A 7.6 Lemmában szereplő félcsoportot n-ed rendűnek nevezzük, ha n az a minimális kitevő, melyre a következő esetek közül valamelyik teljesül:

(ρ_1^n) $\quad ac^n = ac^{n+1}, \quad c^n b = c^{n+1} b$

(ρ_2^n) $\quad ac^n = ac^{n+1}$

(ρ_3^n) $\quad c^n b = c^{n+1} b$

(ρ_4^n) $\quad c^{n+1} = c^{n+2}, \quad ac^n b = ac^{n+1} b$

(ρ_5^n) $\quad c^{n+1} = c^{n+2}$

(ρ_6^n) $\quad ac^n b = ac^{n+1} b$

Az n-ed rendű (n≥0) félcsoportot n/i típusúnak (i=1,...,6) nevezzük, ha (ρ_i^n) teljesül, de (ρ_1^n),...,(ρ_{i-1}^n) nem.

7.8 Tétel (i) Legyen az S CSPI-félcsoport nem-triviális homomorf képe P_o-nak. Ekkor pontosan egy olyan (n,i) pár van, hogy S típusa n/i.

(ii) Tetszőleges (n,i) esetén pontosan egy n/i típusú félcsoport van. Jelölje ezt a félcsoportot S_i^n. Ennek generáló relációit (a $b^2a=b$ és $ba^2=a$ egyenlőségeken kivül) (ρ_i^n) tartalmazza.

(iii) Jelentse S-->T azt, hogy a T félcsoport homomorf képe

S-nek. Ekkor azok a CSPI-félcsoportok, melyek homomorf képei P_o-nak, az alábbi homomorf láncba rendezhetők:

$$\begin{tikzcd}
 & & & S_5^n \arrow[dr] & & S_2^n \arrow[dr] & & & \\
P_o \arrow[r, dashed] & \dots \arrow[r] & S_1^{n+1} \arrow[ur] \arrow[dr] & & S_4^n \arrow[ur] \arrow[dr] & & S_1^n & \dots \arrow[r] & S_1^o. \\
 & & & S_6^n \arrow[ur] & & S_3^n \arrow[ur] & & &
\end{tikzcd}$$

A lánc utolsó tagja $S_1^o=P$, a biciklikus félcsoport.

∎

Bizonyítás (i) azonnal következik a 7.6 Lemmából.

(ii) Az 5.13 Definíciónak megfelelően, P_o-at $F_{\{a,b\}}$ részhalmazának tekintjük. Legyen (n,i) rögzített. Ha $a^kc^lb^m \in P_o$, akkor legyen $\mu(a^kc^lb^m)=a^kc^{l'}b^m$, ahol l' az a maximális kitevő, melyre

1/ $l' \leq l$,

2/ a (ρ_i^n)-ben szereplő azonosságok felhasználásával l' helyébe nem írható kisebb kitevő.

Pl. ha $n=2$ és $i=1$, akkor $\mu(ac^5b^2)=ac^2b^2$ és $\mu(c^5)=\mu(bac^4)=bac^2=c^3$.

$\mu(P_o)$ elemei között vezessük be az alábbi műveletet:

(1) $\quad x*y = \mu(x.y) \quad (x,y \in \mu(P_o))$,

ahol $x.y$ az x és y elemek P_o-beli szorzatát jelöli. A P_o-beli szorzási szabályt (5.15 Tétel) megvizsgálva egyszerűen belátható, hogy μ homomorfizmus. Azonnal következik, hogy $\mu(P_o)$ az (1) művelettel a $b^2a=b$, $ba^2=a$ és a (ρ_i^n) alatti egyenlőségek által generált félcsoport.

Most belátjuk, hogy $\mu(P_o)$ kombinatorikus. Tegyük fel, hogy $u=a^kc^lb^m$, $v=a^{k'}c^{l'}b^{m'}$, továbbá $u,v \in \mu(P_o)$ és $u \mathcal{H} v$. Ekkor van $w=a^{k''}c^{l''}b^{m''} \in \mu(P_o)$, hogy

(2) $\quad w*u=v$, azaz $\mu(w.u)=v$.

μ definíciója miatt (2)-ből következik, hogy $w.u=a^{k'}c^jb^{m'}$ valamilyen j-re. Az 5.15 Tétel (iii) állításából következik, hogy $m' \geq m$. Hasonlóan, u és v szerepét felcserélve kapjuk, hogy $m \geq m'$; tehát $m=m'$. A duális gondolatmenettel kapjuk, hogy $k=k'$.

(2)-ből következik, hogy $m''\leq k$. Ha $m''<k$, akkor $l=l'$. Ha $m''=k$, akkor $\mu(a^k c^{l''+l+j} b^m)=a^k c^{l'} b^m$, ahol $j=0$ vagy 1. Azonnal adódik, hogy $l'\geq l$. u és v szerepét felcserélve $l\geq l'$; tehát $l=l'$. Azt kaptuk, hogy $u=v$.

Ha egy S félcsoport n/i típusú, akkor a 7.5 Lemma segítségével belátható, hogy $S\cong\mu(P_0)$.

(iii) Példaként megmutatjuk, hogy $S_2^n \dashrightarrow S_1^n$. (ii) szerint $S_1^n = P_0/\pi_1^n$, ahol π_1^n az a legszűkebb kongruencia-reláció, amely tartalmazza ρ_1^n-t. Ha egy kongruencia-reláció tartalmazza ρ_1^n-et, akkor tartalmazza ρ_2^n-t is, ezért $S_2^n \dashrightarrow S_1^n$. Hasonlóan látható be a többi homomorf kapcsolat is.

7.9 Lemma Ha $u=a^k c^l b^m$, $v=a^{k'} c^{l'} b^{m'}$; $u,v\in S_1^n$ és $u\mathcal{R}v$ (S_1^n-ben), akkor $k=k'$.

Bizonyítás Van $w=a^{k''} c^{l''} b^{m''} \in S_1^n$, hogy $u*w=v$, azaz

$$\mu(a^k c^l b^m . a^{k''} c^{l''} b^{m''})=a^{k'} c^{l'} b^{m''}.$$

A P_0-beli szorzási szabályból és μ definíciójából következik, hogy $k\leq k'$.

u és v szerepét felcserélve kapjuk, hogy $k\geq k'$, ezért $k=k'$.

7.10 Lemma Legyen $u,v \in S_1^n$, $u=a^k c^l b^m$, $v=a^k c^{l'} b^{m'}$; továbbá $l\leq l'$ és ha $l=l'$, akkor $m'<m$. $u\mathcal{R}v$ akkor és csak akkor, ha az alábbi három eset valamelyike teljesül:

(i) $l=l'$, $m'>0$

(ii) $l=l'$, $m'=0$ és $\mu(a^k c^{l+1})=a^k c^l$

(iii) $l+1=l'$, $m>0$, $m'=0$ és $\mu(a^k c^{l+1} b)=a^k c^l b$.

Következmény: $u\mathcal{R}v$ és $u\neq v$ esetén $m\neq m'$.

∎

Bizonyítás Könnyen belátható, hogy az (i)-(iii) feltételek bármelyikéből következik $u\mathcal{R}v$.

Tegyük most fel, hogy uRv.

I. $l=l'$ és $m'=0$. Választható $w=a^{k''}c^{l''}b^{m''}\in S_i^n$, hogy

(1) $u*w=v$ azaz $\mu(a^kc^lb^m.a^{k''}c^{l''}b^{m''})=a^kc^l$.

Azonnal adódik, hogy $m=k''$ és $m''=0$, és így (1) szerint:

$$\mu(a^kc^{l+l''+1})=a^kc^l,$$

ahonnan $\mu(a^kc^{l+1})=a^kc^l$, tehát teljesül (ii).

II. Ha $l=l'$ és $m'>0$, akkor (i) teljesül.

III. Ha $l<l'$, akkor van $w=a^{k''}c^{l''}b^{m''}\in S_i^n$, hogy

(2) $v*w=u$ azaz $\mu(a^kc^{l'}b^{m'}.a^{k''}c^{l''}b^{m''})=a^kc^lb^m$.

Nyilván $m'\geq k''$.

A/ $m'>k''$. (2)-ből kapjuk, hogy

(3) $\mu(a^kc^{l'}b^{m''+(m'-k'')})=a^kc^lb^m$,

ahonnan $m=m''+(m'-k'')>0$. Mivel $m'>0$ és $a^k c^{l'}b^{m'}\in S_i^n$, kapjuk, hogy $\mu(a^kc^{l'}b^m)=a^kc^{l'}b^m$, és így (3) miatt $l=l'$, ellentmondásban feltevésünkkel.

B/ $m'=k''>0$. Ekkor (2):

(4) $\mu(a^kc^{l'+l''+1}b^{m''})=a^kc^lb^m$.

Mivel $m'>0$ és $a^kc^{l'}b^{m'}\in S_i^n$, kapjuk, hogy $a^kc^{l'}b^m\in S_i^n$, ezért (4) miatt $l'\leq l$, , megintcsak ellentmondásban feltevésünkkel.

C/ $m'=k''=0$. Ekkor (2)

$$\mu(a^kc^{l'+l''}b^{m''})=a^kc^lb^m,$$

ahonnan $m''=m>0$ és így az $l<l'$ feltétel miatt

(5) $\mu(a^kc^{l+1}b)=a^kc^lb$.

Mivel $a^kc^{l'}\in S_i^n$, és mivel (5) miatt $\mu(a^kc^{l+2})=\mu(a^kc^{l+1}ba)=a^kc^{l+1}$, kapjuk, hogy $l'=l+1$; tehát teljesül (iii).

7.11 Lemma Ha S_i^n-ben érvényes az $ac=a$ azonosság (tehát S_1^o és S_2^o esetében), akkor $L_o=\{c,a,a^2,\ldots\}$, egyébként $L_o=\{a,a^2,\ldots\}$. Ha S_i^n-ben érvényes a $cb=b$ azonosság, (S_1^o és S_3^o esetében), akkor $R_o=\{c,b,b^2,\ldots\}$, egyébként $R_o=\{b,b^2,\ldots\}$.

∎

Bizonyítás Legyen a 7.10 Lemmában $u=b$, azaz $k=l=0$. A (ii) eset nem teljesülhet. A (iii) eset akkor és csak akkor teljesül, ha $v=c$ és $\mu(cb)=b$. Az L_o-ra vonatkozó állítás az előbbinek a duálisa.

7.12 Tétel (i) Ha $S_i^n=\langle u,v\rangle$, $v^2*u=v$ $v*u^2=u$, akkor $u=a$ és $v=b$.
(ii) S_i^n-nek nincs más automorfizmusa, mint az identikus leképezés.
(iii) S_i^n balnövelő elemei $b,b^2,\dots$; jobbnövelő elemei pedig $a,a^2,\dots$.

Bizonyítás (i) A 7.11 Lemma birtokában megismételhető az 5.18 Tételre adott bizonyítás.
(ii) következik (i)-ből.
(iii) c nem lehet balnövelő, hiszen ha $c\in R_o$, akkor a 7.11 Tétel szerint c baloldali egységeleme S_i^n-nek.

Ha $cb\neq b$, akkor $b(cb)=(bc)b=bb$, ezért b balnövelő. Ha $cb=b$, akkor $b(ab)=cb=b=bc$, és mivel $ab\neq c$, b balnövelő.

7.13 Tétel (i) S_i^n nem tartalmazza C-t.
(ii) Ha az S CSPI-félcsoportot két eleme generálja, akkor S nem tartalmazza C-t, és C sem tartalmazza S-et.

Bizonyítás (i) Tegyük fel, hogy $u,v\in S_i^n$, $v^2*u=v$ és $\langle u,v\rangle\cong C$. Mivel $v\in C$, $v^2\neq v$. $v^2*u=v$ miatt $v\mathcal{R}v^2$.

Legyen $v=a^kc^lb^m$. A 7.9 Lemma szerint $v\mathcal{R}v^2$-ből következik, hogy $m\geq k$. $m=k$ esetén

$$v^j=\begin{cases}\mu(c^{jl}) & \text{ha } k=0\\ \mu(a^kc^{l+(j-1)(l+1)}b^k & \text{ha } k>0,\end{cases}$$

és így van $\varepsilon>0$, hogy $j\geq\varepsilon$ esetén $v^j=v^\varepsilon$, ellentmondásban $v\in C$-vel. Következésképp $m\neq k$, azaz

(1) $\quad m>k$

és

(2) $\quad v^2=a^kc^lb^{2m-k}$.

Legyen $u=a^{k'}c^{l'}b^{m'}$. $2m-k=k'$ esetén

$$v=v^2*u=\mu(a^kc^{l+l'+1}b^{m'}),$$

ahonnan $m=m'$ és

$$v*u=a^kc^lb^m*a^{2m-k}c^{l'}b^m=a^mc^{l'}b^m\in C,$$

de fentebb már beláttuk, hogy C-nek ilyen alaku eleme nem lehet. Tehát $2m-k\neq k'$, és így $v^2*u=v$ miatt (2)-ből következik, hogy $2m-k>k'$, és így

$$a^kc^lb^m=v^2*u=a^kc^lb^{2m-k}*a^{k'}c^{l'}b^{m'}=a^kc^lb^{m'+(2m-k)-k'},$$

ahonnan $m=m'+(2m-k)-k'$, vagyis

$$m-k=-(m'-k'),$$

ahonnan (1) miatt $m'<k'$, és így elég nagy j-re

$$v*u^j=a^kc^lb^m*a^{k'+(j-1)(k'-m')}c^{l'}b^{m'}=a^{k'+(j-2)(k'-m')}c^{l'}b^{m'}=u^{j-1},$$

ellentmondásban a C-beli szorzási szabállyal.

(ii) Az állítás következik (i)-ből, továbbá a 7.8 és az 5.20 Tételekből.

A következőkben feltesszük, hogy az $S=\langle a,b\rangle$ CSPI-félcsoport homomorf képe P_o-nak. Olyan transzformáció-félcsoportot adunk meg, amely izomorf S-el.

7.14 Lemma Ha $u,v\in S$, $u\mathcal{R}v$, de $u\neq v$, akkor van $i>0$, hogy b^iu és b^iv már nem $\mathcal{R}$-ekvivalensek.

Bizonyítás Legyen $u=a^kc^lb^m$ és $v=a^{k'}c^{l'}b^{m'}$. A 7.9 Lemma szerint $m=m'$, a 7.10 Lemma szerint pedig $k\neq k'$. Legyen pl. $k<k'$. Ekkor $b^{k'+1}u=b^{m+k'-k+1}$ és $b^{k'+1}v=b^{m+1}$ nyilván nem $\mathcal{R}$-ekvivalensek, ezért $i=k'+1$ megfelelő.

7.15 Tétel Legyen $\Pi=\{S^1x:\ x\in S^1\}$, és legyen T a Π-t Π-be vivő transzformációk félcsoportja. Definiáljuk az $\varphi\in$ S-->T leképezést a következőképpen. Ha $u \in S$, akkor legyen

$$(S^1x)(u\eta) \overset{d}{=} S^1xu \quad (x \in S^1).$$

Ekkor η izomorfizmus S-ről T-be.

Bizonyítás A definícióból következik, hogy η homomorfizmus. A 7.14 Lemma szerint η 1-1 leképezés S-ről T-be.

Az $a\eta$ és $b\eta$ transzformációkat S_1^o és S_2^o esetében az alábbi diagramok szemléltetik:

$$\begin{array}{llll}
 & a\eta & & b\eta \\
S_1^o: & S^1 \leftarrow S^1b \leftarrow S^1b^2 \leftarrow \dots & & S^1 \rightarrow S^1b \rightarrow S^1b^2 \rightarrow \dots \\
 & S^1c \leftarrow S^1cb \leftarrow S^1cb^2 \leftarrow \dots & & S^1c \rightarrow S^1cb \rightarrow S^1cb^2 \rightarrow \dots \\
S_2^o: & \uparrow \nwarrow & & \\
 & S^1 \qquad S^1b \leftarrow S^1b^2 \leftarrow \dots & & S^1 \rightarrow S^1b \rightarrow S^1b^2 \rightarrow \dots
\end{array}$$

$S=P_o$ esetében erősebb állítás is igaz: a 7.17 Tétel. A következőkben P_o helyett S-et írunk.

7.16 Lemma Legyen $u=a^kc^lb^m \in S$ és $v=a^{k'}c^{l'}b^{m'} \in S$. $Su=Sv$ akkor és csak akkor, ha $l=l'$ és $m=m'$.

Bizonyítás $Su=Sv$ -vel ekvivalens, hogy $S^1au=S^1av$, azaz $au\mathcal{L}^1av$. Az 5.15 Tételből következik, hogy ez akkor és csak akkor teljesül, ha $m=m'$ és $l=l'$.

7.17 Tétel Legyen $\Pi=\{Sx: x \in S\}$, és legyen T a Π-t Π-be vivő transzformációk félcsoportja. Definiáljuk az $\eta \in S \rightarrow T$ leképezést a következőképpen. Ha $u \in S$, akkor legyen

$$(Sx)(u\eta) \overset{d}{=} Sxu \quad (x \in S).$$

Ekkor η izomorfizmus S-ről T-be.

Bizonyítás Tegyük fel, hogy $u,v \in S$ és $u\eta = v\eta$. Belátjuk, hogy $u=v$. Tegyük fel e célból, hogy $u \neq v$. A 7.16 Lemma szerint $u=a^k c^l b^m$ és $v=a^{k'} c^l b^m$, ahol $k \neq k'$, pl. $k<k'$. Legyen $i=1$ ha $k'=k+1$, és $i=0$ ha $k'>k+1$. Ekkor

$$Sa^{k'-k-1}c^{l+i}b^m = Sb^{k+1}v = Sb^{k+1}u = Sb^{m+1},$$

ellentmondásban a 7.16 Lemmával. Tehát $k=k'$, azaz $u=v$. Ezért η izomorfizmus.

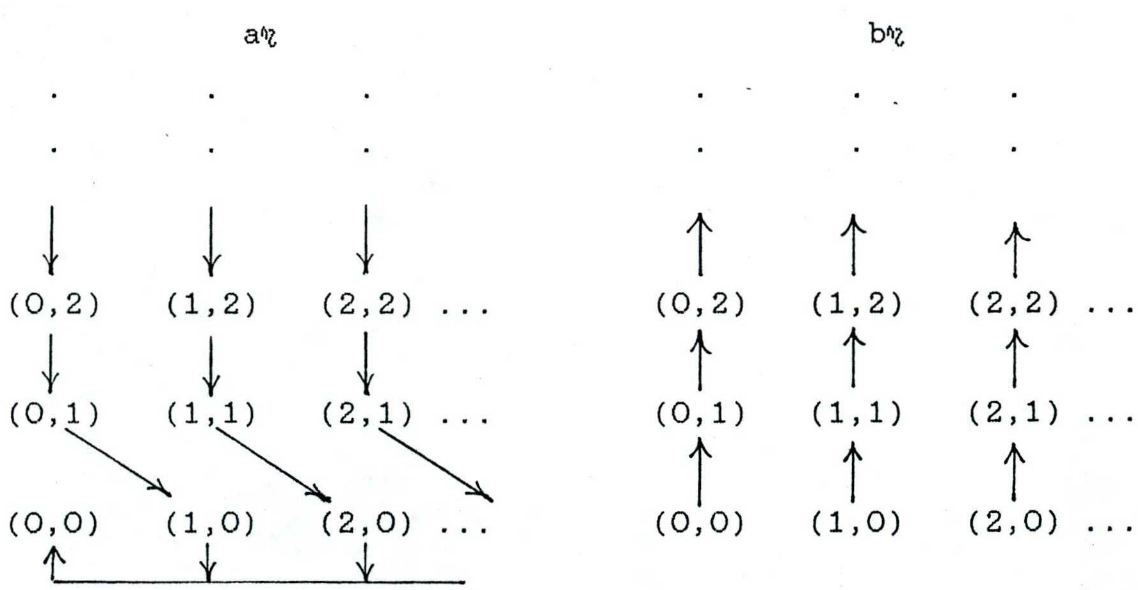
Megjegyzés S_2^o-ben a 7.17 Tétel már nem igaz. Pl.

$$S_2^o xbab = S_2^o xb \qquad (x \in S_2^o),$$

de $bab \neq b$.

Az $a\eta$ és $b\eta$ transzformációk szemléltetése céljából feleltessük meg Π elemeit a sík (l,m) koordinátáju rácspontjainak, ahol $l \geq 0$ és $m \geq 0$. $Sa^k c^l b^m = Sc^l b^m$-nak feleljen meg az (l,m) rácspont. Ekkor

$$(l,m)(a\eta) = \begin{cases} (l,m-1) & \text{ha } m>1 \\ (l+1,0) & \text{ha } m=1 \\ (0,0) & \text{ha } m=0. \end{cases} \qquad (l,m)(b\eta) = (l,m+1)$$



7.18 Tétel Ha az S félcsoportnak nincs (kétoldali) egységeleme, de van c jobboldali egységeleme, továbbá $bS=S$, akkor
(i) Ha S kombinatorikus, akkor tartalmazza S_2°-t.
(ii) b balnövelő eleme S-nek.
(iii) S-nek van jobbnövelő eleme is.

Bizonyítás Válasszunk olyan a'-t, melyre $ba'=c$, és legyen $a=ca'$. Ekkor

(1) $\qquad ca=c(ca')=a,$

és

(2) $\qquad c=ba'=(bc)a'=ba.$

$cb=b$ -ből $bS=S$ miatt következne, hogy c baloldali egységelem is, ezért

(3) $\qquad cb\neq b,$ de $b(cb)=(bc)b=bb.$

(1) és (2)-ből, továbbá az $ac=a$ és $bc=b$ azonosságokból következik, hogy $\langle a,b\rangle$ homomorf képe S_2°-nek. Mivel (3) szerint $\langle a,b\rangle$-nek nincs (kétoldali) egységeleme, $\langle a,b\rangle$ nem lehet homomorf képe S_1°-nek. Mivel $\langle a,b\rangle$ kombinatorikus, a 7.8 Tételből következik, hogy $\langle a,b\rangle=S_2^{\circ}$.

(3)-ból következik (ii).

Mivel $S\supseteq Sa\supseteq Sba=Sc=S$, ezért $Sa=S$. Mivel $(cb)a=c(ba)=cc=c=ba$, (3)-ból kapjuk, hogy a jobbnövelő eleme S-nek.

8. Speciális félcsoportok

Ha b balnövelő eleme az S félcsoportnak, akkor b^2 is az, ezért van $a\in S$, hogy $b^2a=b$. Ezért S tartalmazza C-t vagy annak homomorf képét. A megforditás akkor sem igaz, ha S C-t is, és D-t is tartalmazza. Példa erre a most ismertetendő félcsoport.

Legyen $C=\langle a,b\rangle$ és $D=\langle u,v\rangle$, ahol C és D generáló relációi $b^2a=b$ ill. $vu^2=u$. Legyen E azon véges sorozatok halmaza, amelyeknek minden tagja eleme C-nek vagy D-nek, továbbá két szomszédos tag közül az egyik C-nek, a másik D-nek eleme. Pl. $ba^5bav^2auv=[\alpha_1,\alpha_2,\alpha_3,\alpha_4]\in E$, ahol $\alpha_1=ba^5ba$, $\alpha_2=v^2$, stb. Az $\alpha=[\alpha_1,\ldots,\alpha_k]$ sorozat hossza definíció szerint $|\alpha|=k$.

Ha $\alpha=[\alpha_1,\ldots,\alpha_k]$ és $\beta=[\beta_1,\ldots,\beta_l]$ E-beli sorozatok, akkor szorzatukat a következőképpen definiáljuk. Ha α_k és β_1 különböző típusúak (tehát az egyik C-nek, a másik D-nek eleme), akkor

(1-a) $\alpha*\beta=[\alpha_1,\ldots,\alpha_k,\beta_1,\ldots,\beta_l]$,

egyébként

(1-b) $\alpha*\beta=[\alpha_1,\ldots,\alpha_k*\beta_1,\ldots,\beta_l]$.

Az (1-a) esetben $|\alpha*\beta|=|\alpha|+|\beta|$, az (1-b) esetben pedig $|\alpha*\beta|=|\alpha|+|\beta|-1$, ezért

(2) $|\alpha|+|\beta|-1\leq|\alpha*\beta|\leq|\alpha|+|\beta|$.

Legyen $X=\{a,b,u,v\}$, és definiáljuk az η: $F_X\dashrightarrow E$ leképezést a következőképpen. Ha $\alpha\in F_X$, akkor α egyértelműen $\alpha_1\alpha_2\ldots\alpha_k$ alakba írható, ahol $\alpha_i\in F_{\{a,b\}}$ vagy $\alpha_i\in F_{\{u,v\}}$ $(i=1,\ldots,k)$, és ha $i<k$, akkor α_i és α_{i+1} közül az egyik $F_{\{a,b\}}$-nek, a másik $F_{\{u,v\}}$-nek eleme. Legyen

$$\eta(\alpha)=[\mu(\alpha_1),\mu(\alpha_2),\ldots,\mu(\alpha_k)],$$

ahol μ az 5.2 Definíció szerinti. Könnyen belátható, hogy ha E-ben az (1) alatti műveletet tekintjük, akkor η homomorfizmus. Ezért E félcsoport, melyet a $b^2a=b$ és $vu^2=u$ relációk generálnak.

8.1 Tétel (i) E tartalmazza C-t is és D-t is.
(ii) E-nek nincs növelő eleme.
(iii) E nem tartalmazza P_o-t, sem annak homomorf képét.

Bizonyítás (i) és (ii) egyszerűen ellenőrizhető.
(iii) Tegyük fel, hogy $\alpha=[\alpha_1,\dots,\alpha_k]$ és $\beta=[\beta_1,\dots,\beta_l]$ E-beli sorozatok, és

(3) $\quad \beta^2*\alpha=\beta,\quad \beta*\alpha^2=\alpha.$

Két eset lehetséges.

a/ α_k és β_1 különböző típusúak. Ekkor (2) szerint

$$|\beta|=|\beta^2*\alpha|=|\beta^2|+|\alpha|\geq 2|\beta|-1+|\alpha|>|\beta|,$$

ami ellentmondás.

b/ α_k és β_1 azonos típusúak. Ekkor

$$|\beta|=|\beta^2*\alpha|=|\beta^2|+|\alpha|-1\geq 2|\beta|+|\alpha|-2,$$

ahonnan $|\alpha|+|\beta|\leq 2$, és így $|\alpha|=|\beta|=1$. Ezért α és β vagy mindketten C-ben, vagy mindketten D-ben vannak. Ha pl. mindketten C-ben vannak, akkor (3)-ból az 5.6 Tétel (i) állítása szerint $\beta*\alpha=1$, ellentmondásban az 5.4 Tétel (v) állításával.

A következőkben $F_{\{a,b\}}$-nek azt a homomorf képét vizsgáljuk, melyet (a c=ba jelölés mellett) a

$$bc = b \quad \text{és} \quad c^n a = a$$

relációk generálnak. Jelöljük ezt a félcsoportot C_n-el. Adódik, hogy $C_1=P_o$ és mindegyik C_n homomorf képe C-nek.

Legyen $C'=\langle a,c\rangle$, tehát C' részfélcsoportja C-nek. Könnyen látható, hogy $C'=F_{\{a,c\}}$, ezért C' tetszőleges x' elemére

(1) $\quad x'=x_1\dots x_r$ ahol $x_t=a^i$ vagy $x_t=c^j$ $(t=1,\dots,r)$.

Feltehetjük, hogy (1)-ben az a^i és c^j alakú tényezők váltakozva követik egymást, azaz ha $t<r$, akkor x_t és x_{t+1} egyike a-hatvány, a másika c-hatvány. Pl. $a^2c^5a\in C'$. Ezzel a feltevéssel az (1) alatti előállítás egyértelmű. Jelölje a továbbiak-

ban $x.y$ az $x,y \in C$ elemek C-beli szorzatát. Ekkor

(2) $\quad x'.y' = x'y' \quad (x',y' \in C')$.

C tetszőleges x eleme egyértelműen felírható a

(3) $\quad x= x'b^k \quad (x'\in C'\cup\{1\},\ k\geq 0)$

alakban. Ha $x=x'b^k$ és $y=y'b^l$, akkor

(4) $\quad x.y = x'(b^k.y')b^l$.

Ezért ha $x\in C'$ $(k=0)$, vagy ha $y=b^l$ $(y'=1)$, akkor $x.y=xy$.

Legyen $x=x'b^k$ tetszőleges eleme C-nek, ahol x' az (1) szerinti. Definiáljuk a $H\subseteq C$ halmazt: $x\in H$ ha $t<r$ és $x_t=c^j$ esetén (ekkor tehát $x_{t+1}=a^i$ valamilyen $i>0$ -ra) teljesül, hogy $j<n$.
Definiáljuk a μ: $C\dashrightarrow H$ leképezést:

(5) $\quad \mu(x)=x_1'x_2'\ldots x_r'$ ahol $t<r$ és $x_t=c^i$ esetén $x_t'=c^{i'}$, ahol $i'<n$ és $i'\equiv i \pmod n$; egyébként $x_t'=x_t$.

Pl. $n=3$ esetén $\mu(a^2c^5ac^3a^2b)=a^2c^2a^3b$.

Ha $x.y=xy$, akkor adódik, hogy

(6) $\quad \mu(xy)=\mu(\mu(x)y)=\mu(x\mu(y))=\mu(\mu(x)\mu(y))$.

Definiáljuk H elemei között a következő műveletet

(7) $\quad x*y=\mu(x.y) \quad (x,y\in H)$.

8.2 Tétel (i) μ homomorfizmus C-ről H-ra, és $H=C_n$.
(ii) C_n balnövelő elemei $b,b^2,\ldots$.
(iii) C_n jobbnövelő elemei az $x=x'a$ alakúak, ahol $x'\in C'$.
(iv) Legyen $x=x'ac^ib^k$ és $y=y'ac^jb^l$ (i,k,j,l nemnegativ egészek). $x\mathcal{L}y$ akkor és csak akkor, ha $i=j$ és $k=l$. Ha $x=c^ib^k$, akkor $L_x=\{x\}$.
(v) Legyen $x'\in C'$ és $y'\in C'$. $x'b\mathcal{R}y'b$ akkor és csak akkor, ha $x'=y'$. Ha $x'\in C'$, akkor $R_{x'}=\{x'\}$.
(vi) C_n kombinatorikus és egyszerű.
(vii) Ha $n>1$, akkor C_n balideáljainak a halmaza (a tartalmazásra nézve) teljesen rendezett, de nem jólrendezett, és duálisan sem az. Ezért C_n nem főideálfélcsoport.
(viii) Ha $u=ac^{n-1}$ és $v=b$, akkor $\langle u,v\rangle=P_0$.

Bizonyítás (i) Azt kell megmutatnunk, hogy

(8) $\mu(x.y)=\mu(\mu(x).\mu(y))$ $(x,y\in C)$.

Először belátjuk (8)-at az $x=b$ esetre. Feltehetjük, hogy $\mu(y)\neq y$ és így $y=c^j a^i z$, ahol $j\geq 0, i>0$. Mivel $\mu(y)=\mu(c^j a^i)\mu(z)$, (6)-ot felhasználva

$$\mu(b.y)=\mu(ca^{i-1}z)=\mu(ca^{i-1}\mu(z))=\mu(b.\mu(y)).$$

Tegyük most fel, hogy (8) teljesül $x=b^k$-ra $(k=1,\dots,m)$. Ekkor

$$\mu(b^{m+1}.y)=\mu(b.\mu(b^m.y))=\mu(b.(b^m.\mu(y)))=\mu(b^{m+1}.\mu(y)).$$

Következésképp (8) tetszőleges k esetén teljesül, ha $x=b^k$.

Végül, ha $x=x'b^k$ és $y=y'b^l$, akkor

$$\mu(\mu(x).\mu(y))=\mu(\mu(x')(b^k.\mu(y'))b^l)=\mu(x'(b^k.y')b^l)=\mu(x.y).$$

(ii) Mivel $cb\neq b$, de $b(cb)=(bc)b=bb$, ezért b balnövelő. Ha $x=x'b^k$ balnövelő, akkor van y, hogy $x*y=b$, ahonnan (4) szerint $x'=1$, azaz $x=b^k$.

(iii) Ha $x'\in C'$ és $x=x'a\in C_n$, akkor van i és j, hogy $c^{i+ns}b^j*x=a$ tetszőleges $s\geq 0$ -ra. Ha x jobbnövelő, akkor nyilván nem írható sem $x'c$, sem $x'b$ alakba.

(iv) és (v) közvetlen számolással igazolható, C_n kombinatorikus volta pedig ezekből következik.

Tetszőleges $x\in C_n$-hez van k, hogy $b^k*x=b^l$ valamilyen l-re. Mivel b^l balnövelő, kapjuk, hogy $C_n x C_n=C_n$. Ezért C_n egyszerű.

(vii) A balideálokra vonatkozó állítás az 5.8 Tételhez hasonlóan bizonyítható. Mivel pl. $ca\notin R(ac)$ és $ac\notin R(ca)$, ezért a jobbideálok halmaza nem teljesen rendezett.

(viii) $v^2*u=b^2*ac^{n-1}=b$, $v*u^2=b*ac^{n-1}ac^{n-1}=c^n*ac^{n-1}=ac^{n-1}=u$.

Mivel $v*u=vu=c^n$ és $u*u=uu$, ezért $u^k(vu)^l v^m\in C_n$.

A következőkben a

$$b(ba)^n\sim b \text{ és } (ba)^n a\sim a$$

relációk által generált H_n félcsoport tulajdonságait tárgyaljuk. Ezek hasonlóak a C_n-re bizonyítottakhoz: H_n-nek is van bal- és jobb-növelő eleme, továbbá tartalmazza P_o-t.

8.3 Definíció A $p=u_i,u_j$ és $q=u_k,u_l$ párokról azt mondjuk, hogy p tartalmazza q-t, ha $i<k$ és $l<j$. A p párt maximálisnak nevezzük, ha nincs olyan q pár, hogy $p\subset q$.

8.4 Lemma Ha a $p=u_iu_j$ pár nem elemi (azaz $i+1<j$), akkor p tartalmaz egy olyan egyértelműen meghatározott párláncot, melyben az első pár kezdőbetűje $u_{i+1}=b$, és az utolsó pár záróbetűje $u_{j-1}=a$. Ezt a láncot p belső láncának nevezzük.

8.5 Lemma Ha p nem elemi pár, akkor van olyan $q\subseteq p$, hogy q nem elemi pár, de q belső láncának minden szeme elemi.

8.6 Definíció Definiáljuk a Π_o, Π_1,... halmazokat, melyeknek elemei u-beli ($u\in F_{\{a,b\}}$) párok. Π_o legyen az összes u-beli elemi pár halmaza. Ha már definiáltuk Π_i-t, akkor Π_{i+1} legyen azon párok halmaza, melyek Π_i-ben vannak, vagy amelyek belső láncának minden szeme Π_i-ben van, továbbá ezen belső lánc szemeinek száma$\equiv 0$ (mod n). Legyen $r=r(u)$ az a (nyilvánvalóan létező) minimális index, melyre $\Pi_r=\Pi_{r+1}$.

Egy p párt Π_r-maximálisnak nevezünk, ha $p\in\Pi_r$, és nincs olyan $q\in\Pi_r$, hogy $p\subset q$.

Egy láncot Π_r-maximálisnak nevezünk, ha minden szeme Π_r-maximális, továbbá egyik irányban sem folytatható további Π_r-maximális pár hozzávételével. Q-láncnak nevezünk egy Π_r-maximális láncot, ha baltámasza (vagyis az őt megelőző betű) b, vagy jobbtámasza a.

Definiáljuk a $H_n\subset F_{\{a,b\}}$ halmazt a következőképpen: $u\in H_n$ akkor és csak akkor, ha minden u-beli Q-lánc $(ba)^i$ alakú, ahol $i<n$. (Tehát u-nak nincs $b(ba)^n$ vagy $(ba)^n a$ alakú részszava.

Definiáljuk a γ: $F_{\{a,b\}} \to H_n$ függvényt a következőképpen. Legyen $u \in F_{\{a,b\}}$. Ha L tetszőleges, u-beli Q-lánc, melynek k szeme van, akkor L zónáját helyettesítsük $y=(ba)^l$-el, ahol $0 \leq l < n$ és $k \equiv l \pmod n$. Legyen L zónája z. Ha $|z|>|y|$, akkor Q-t redukálhatónak nevezzük. Az összes Q-láncra elvégezve a fenti helyettesítést, kapjuk $\gamma(u)$-t. u-t redukálhatónak nevezzük, ha $u \in F_{\{a,b\}} \setminus H_n$, tehát ha u tartalmaz legalább egy redukálható Q-láncot.

$L=(ba)^n$-t elhagyható alapláncnak nevezzük, ha baltámasza b vagy jobbtámasza a.

8.7 Lemma Ha u' u-ból egy elhagyható L alaplánc elhagyásával kapható, akkor $\gamma(u')=\gamma(u)$.

Bizonyítás Ha L egy Q-lánc része (annak eleje vagy vége), akkor az állítás γ definíciójából következik. Ha nem, akkor van olyan $p \in \Pi_r$ pár, hogy L része p belső láncának. Nyilvánvaló, hogy L elhagyása után is $p \in \Pi_r$, ezért $\gamma(u')=\gamma(u)$.

8.8 Lemma Minden redukálható Q-lánc tartalmaz elhagyható alapláncot.

Bizonyítás Ha az L redukálható Q-láncnak van olyan szeme, amely nem elemi pár, akkor a 8.5 Lemma és Π_r definíciója szerint ez a szem tartalmaz elhagyható alapláncot. Ha L-nek minden szeme elemi, akkor L első vagy utolsó n szeme elhagyható alapláncot határoz meg.

8.9 Definíció A H_n halmazon értelmezzük a következő műveletet

$$x*y = \gamma(xy) \qquad (x,y \in H_n).$$

8.10 Tétel (i) A fenti művelettel H_n félcsoport, γ homomorfizmus $F_{\{a,b\}}$-ről H_n-re, a γ-hoz tartozó kongruenciát pedig a

(1) $b(ba)^n \sim b$, $(ba)^n a \sim a$

relációk generálják.

(ii) H_n balnövelő elemei azok a $v=bv'$ alakú szavak, melyekben az első pozicióban levő b pártalan, továbbá v minden párja elemi.

(iii) Ha $u=a(ba)^{n-1}$ és $v=b$, akkor $\langle u,v\rangle=P_o$.

(iv) H_n-ben (a tartalmazásra nézve) sem a balideálok, sem a jobbideálok nem teljesen rendezettek.

Bizonyítás (i) Legyen $x_1=x$, x_{i+1} pedig adódjon x_i-ből egy elhagyható alaplánc elhagyásával. A 8.7 és 8.8 Lemmák alapján $\gamma(x)=x_k$ valamilyen k-ra, továbbá $\gamma(xy)=\gamma(x_1y)=\ldots=\gamma(x_ky)$. Megismételve ezt az eljárást y-ra, kapjuk, hogy $\gamma(xy)=\gamma(x)*\gamma(y)$, tehát γ homomorfizmus. Az x_i-k képzési szabályából adódik, hogy a γ-hoz tartozó kongruenciát az (1) relációk generálják.

(ii) közvetlen számolással adódik.

Mivel $v*u=(ba)^n$, ezért $v^2*u=v*(v*u)=b*(ba)^n=b=v$ és $v*u^2=(v*u)*u=(ba)^n*a(ba)^{n-1}=u$. Ha $k+l+m>0$, akkor könnyen ellenőrizhető, hogy $u^k(vu)^l v^m \in H_n$, ahonnan $\langle u,v\rangle=P_o$.

(iv) Pl. $ac \notin R(ca)$ és $ca \notin R(ac)$.

A következőkben $F_{\{a,b\}}$-nek azt a homomorf képét vizsgáljuk, melynek generáló relációi

(1) $b^{n+1}a^n \sim b$, $b^n a^{n+1} \sim a$.

Jelölje ezt a félcsoportot K_n. Belátjuk, hogy K_n-nek van mindkét oldali növelő eleme, és tartalmazza P_o-t.

Legyen $u \in F_{\{a,b\}}$. Képezzük az alábbi halmazokat, melyeknek elemei u-beli párok. Ha $1 \leq i \leq n$, akkor legyen $\pi_o^i=\{$p: a p pár belseje $b^{i-1}a^{i-1}$, vagyis p zónája (a p által meghatározott I-beli részszó) $b^i a^i\}$. Ha már definiáltuk π_j^i-t, akkor legyen $\pi_{j+1}^i=\{$p: $p\in\pi_j^i$, vagy p belső L lánca eleget tesz az alábbi követelményeknek:

ha $i=1$, akkor L minden szeme $\in\Pi_j^n$;

ha $i>1$, akkor L tartalmaz pontosan egy Π_j^{i-1}-beli szemet, az összes többi szem $\in\Pi_j^n$.} Nyilván $\Pi_o^i\subseteq\Pi_1^i\subseteq\ldots$ és a $\Pi_j^1, \Pi_j^2,\ldots,\Pi_j^n$ halmazok diszjunktak. Van $r\geq 0$, hogy $\Pi_r^i=\Pi_{r+1}^i$ $(i=1,\ldots,n)$.

Egy p párt n-maximálisnak nevezünk, ha $p\in\Pi_r^n$, és nincs olyan $q\in\Pi_r^n$, hogy $p\subset q$. Egy L láncot n-maximálisnak nevezünk, ha L minden szeme n-maximális, és L egyik irányban sem folytatható. Végül, $\gamma(u)$ legyen az a szó, melyet úgy kapunk u-ból, hogy elhagyunk minden olyan n-maximális láncot, melynek baltámasza b vagy jobbtámasza a. A H_n-re adott bizonyítást megismételve kapjuk, hogy γ homomorfizmus $F_{\{a,b\}}$-ről K_n-re, melyhez az (1) alatti relációk által generált kongruencia tartozik, azaz $F_{\{a,b\}}/\gamma\equiv K_n$.

8.11 Tétel (i) K_n balnövelő elemei a $bu_1u_2\ldots u_m$ alaku szavak, ahol $m\geq 0$ tetszőleges, és az u_t tényezőkre teljesül, hogy

$$u_t=b^ib^ja^j,\ i+j\geq n.$$

(ii) Ha $u=a^n$ és $v=b^n$, akkor $\langle u,v\rangle=P_o$.

(iii) K_n-ben sem a bal-, sem a jobb-ideálok nem teljesen rendezettek (a tartalmazásra nézve).

Bizonyítás Közvetlen számolással adódik, a H_n-re adott bizonyításhoz hasonlóan.

IRODALOMJEGYZÉK:

[1] Megyesi,L. and Pollák,G., Über die Struktur der Hauptideal-halbgruppen, I, Acta Sci. Math. (Szeged) 29 (1968), 261-270. MR 38 # 3370.

[2] Megyesi, L. and Pollák, G., On Simple Principal Ideal Semi-groups, Studia Sci. Math. (Budapest) 16 (1981), 437-448.

[3] Clifford, A. H. and Preston, G. B., The Algebraic Theory of Semigroups, Vol. I(Providence, 1961).

[4] Lajos, S., A félcsoportok növelő elemeiről, A Magyar Tudományos Akadémia III. Osztályának Közleményei XV./3. (1965), 273-287.

[5] Lyapin,E.C.:Félcsoportok, Moszkva, 1960.

[6] Jones, P. R., Analogs of the Bicyclic Semigroup in Simple Semigroups Without Idempotents, (megjelenés alatt).