Eötvös Loránd Tudományegyetem
Természettudományi Kar

Bodor Bertalan
Matematikus MSc

Homogén struktúrák reduktjai

Az $\mathbb{F}_p^\omega$ vektortér reduktjai páratlan prímek esetén

Szakdolgozat

Témavezető: Szabó Csaba egyetemi tanár
Algebra és Számelmélet Tanszék

Tartalomjegyzék

Tartalomjegyzék **3**

1. Bevezető **4**

2. Reduktok **4**

3. A vektortér 0-t fixáló reduktjai **6**

3.1. Azon zárt csoportok leírása, amik a teljes szimmetrikus csoportként hatnak a $\sim_G$-ekvivalenciaosztályok halmazán 17

4. A vektortér 0-t nem fixáló reduktjai **25**

Kivonat

Ebben a dolgozatban leírjuk az $\mathbb{F}_p$ feletti megszámlálhatóan végtelen dimenziós vektortér elsőrendben definiálható reduktjait, ahol $p \geq 3$ tetszőleges prím.

1. Bevezető

Legyen K egy tetszőleges véges test. Jelölje K^ω a K test feletti megszámlálhatóan végtelen dimenziós vektorteret. A lineáris leképezésekre vonatkozó kiterjesztési tulajdonság miatt igaz az, hogy K^ω bármely két véges altere közti izomorfizmus kiterjeszthető a teljes vektortér egy automorfizmusává. Ez a tulajdonság a homogenitás. Emellett ez a struktúra univerzális is abban az értelemben, hogy bármely véges vagy megszámlálhatóan végtelen K feletti vektortér beágyazható K^ω-ba. Szintén fontos tulajdonsága ennek a vektortérnek az ω-kategoricitás: egy struktúrát ω-kategorikusnak nevezünk, ha az elsőrendű elméletének pontosan egy megszámlálható modellje van izomoria erejéig.

A megszámlálható, homogén, ω-kategorikus struktúrákat azért szokták vizsgálni, mert bizonyos értelemben a végtelen struktúrák közül ezek állnak legközelebb a véges struktúrákhoz. Ezek közé tartoznak például a véletlen gráf, a racionális számok halmaza a szokásos rendezési relációval ellátva, és a megszámlálható atommentes Boole-algebra. Egy struktúra megértésénél fontos kérdés lehet, hogy a struktúrának mik az elsőrendben kifejezhető reduktjai, azaz milyen, esetleg gyengébb struktúrák adhatók meg a struktúra alaphalmazán elsőrendű definícióval. Egy megszámlálható ω-kategorikus struktúrával azért kényelmes dolgozni, mert ezen struktúráknál a struktúra reduktjai egyértelmű módon jellemezhetőek az automorfizmuscsoportjaikkal.

Már számos homogén, megszámlálható, ω-kategorikus struktúrára ismert a reduktok teljes klasszifikációja. Ezek közé tartoznak például a véletlen gráf [15], a véletlen hipergráf [16] és a véletlen POSET [12]. Ezekben az eredményekben az a közös, hogy a vizsgált struktúrák véges relációs nyelven homogén struktúrák. A legtöbb klasszifikáció ad hoc számolásokat használ, újabban Bodirsky és Pinsker munkája nyomán Ramsey-elméleti módszereket alkalmaztak sikerrel [5].

Ebben a dolgozatban a K^ω vektortér reduktjait vizsgáljuk abban az esetben, amikor $K = \mathbb{F}_p$, ahol $p \geq 3$ prím. A K^ω vektortér az eddig vizsgált struktúrákkal szemben nem írható le véges relációs nyelven, úgy hogy homogén legyen, így ebben az esetben az eddig ismert módszerek nem működnek.

2. Reduktok

Egy $\mathfrak{A}$ struktúra reduktja egy olyan $\mathfrak{B}$ struktúra, aminek ugyanaz az alaphalmaza, mint $\mathfrak{A}$-nek, és a $\mathfrak{B}$ struktúra minden relációja és művelete kifejezhető az $\mathfrak{A}$ struktúra relációiból és műveleteiből valamilyen elsőrendű formula segítségével. Két reduktot ekvivalensnek tekintünk, ha egymásnak is reduktjai. Ha $\mathfrak{B}$ reduktja $\mathfrak{A}$-nak, akkor $\mathrm{Aut}(\mathfrak{A}) \subset \mathrm{Aut}(\mathfrak{B}) \subset \mathrm{Sym}(\mathfrak{A})$, továbbá könnyen ellenőrizhető az is, hogy $\mathrm{Aut}(\mathfrak{B})$ mindig zárt $\mathrm{Sym}(\mathfrak{A})$-ban. A zártságot a pontonkénti konvergencia topológiája szerint értjük. Ekkor egy $G \leq \mathrm{Sym}(\mathfrak{A})$ csoport zártsága azzal ekvivalens, hogy ha $g \in \in \mathrm{Sym}(\mathfrak{A})$, és az $\mathfrak{A}$ struktúra alaphalmazának tetszőleges véges F halmazához létezik olyan $h \in G$, amire $g|_F = h|_F$, akkor $g \in G$ is teljesül. Ha az $\mathfrak{A}$ struktúra ω-kategorikus, akkor ennek a megfordítása is igaz:

2.0.1. Tétel. *Legyen $\mathfrak{A}$ egy megszámlálható, ω-kategorikus struktúra. Ekkor az $\mathfrak{A}$ alaphalmazán ható,* $\mathrm{Aut}(\mathfrak{A})$*-t tartalmazó zárt permutációcsoportok éppen a $\mathfrak{A}$ struktúra reduktjainak automorfizmuscsoportjai, továbbá két redukt automorfizmuscsoportja pontosan akkor egyezik meg, ha ekvivalensek.*

Ez azt jelenti, hogy ha egy ω-kategorikus struktúra reduktjai megfeleltethetőek az automorfizmuscsoportját tartalmazó zárt permutációcsoportoknak. Egy megszámlálható struktúra ω-kategoricitása könnyen ellenőrizhető a struktúra automorfizmuscsoportja segítségével.

2.0.2. Tétel. *Egy megszámlálható $\mathfrak{A}$ struktúra pontosan akkor ω-kategorikus, ha az automorfizmuscsoportja* $\mathrm{Aut}(\mathfrak{A})$ oligomorf*, azaz minden $n \in \omega$ esetén véges sok n-orbitja van $\mathfrak{A}$-n.*

2.0.3. Következmény. *Egy megszámlálható ω-kategorikus struktúra reduktja is ω-kategorikus.*

Bizonyítás. Legyen $\mathfrak{A}$ egy megszámlálható struktúra, és $\mathfrak{B}$ ennek egy reduktja. Ekkor $\mathrm{Aut}(\mathfrak{B}) \supset \mathrm{Aut}(\mathfrak{A})$, így az $\mathrm{Aut}(\mathfrak{B})$ csoport minden n-orbitja az $\mathrm{Aut}(\mathfrak{A})$ csoport néhány n-orbitjának egyesítése. Ebből következik, hogy ha az $\mathfrak{A}$ struktúra automorfizmuscsoportja oligomorf, akkor ez minden reduktjára is igaz. A 2.0.2. Tételt használva ebből azonnal következik az állítás. $\square$

2.0.4. Állítás. *Legyen V egy megszámlálhatóan végtelen dimenziós vektortér egy véges test fölött. Ekkor V ω-kategorikus.*

Bizonyítás. A V struktúra megszámlálható, ezért alkalmazható a 2.0.2. Tétel. Legyen $n \in \omega$ tetszőleges, és legyen U egy n dimenziós altere V-nek. Legyenek most $v_1, \ldots, v_n$ tetszőleges elemek. Ekkor $\dim\langle v_1, \ldots, v_n\rangle \leq n$, így létezik olyan $g \in \mathrm{Aut}\, V$ lineáris leképezés, amire $v_1^g, \ldots, v_n^g \in U$. Ez azt jelenti, hogy az U elemeiből alkotott rendezett n-esek reprezentálnak minden n-orbitot. U azonban egy véges dimenziós tér egy véges test fölött, tehát véges. Így U^n is véges, tehát az n-orbitok száma is véges. $\square$

2. Bizonyítás. Ez az állítás közvetlenül a definícióból is bizonyítható. Jelöljük a V-hez tartozó alaptestet K-val. Tegyük fel most, hogy W egy megszámlálható modellje V elméletének. Ekkor mivel V vektortér, ezért V elmélete tartalmazza a vektortér axiómákat is. Ekkor azonban W elmélete is tartalmazza a vektortér axiómákat, így

W is egy vektortér K fölött. Azt kell még belátnunk, hogy $\dim W = \omega$. $\dim W$ nem lehet véges, mert ha $\dim W$ véges lenne, akkor mivel K véges, ezért W is véges lenne, ami nem lehet. Tehát $\dim W$ végtelen. Ekkor azonban mivel K véges, ezért $\omega = |W| = \dim W$, és ezt kellett bizonyítanunk. $\square$

Ebben a dolgozatban azzal az esettel foglalkozunk, amikor az alaptest $K = \mathbb{F}_p$, ahol p egy páratlan prím. A dolgozat felépítése a következő: A 3. fejezetben azon zárt szupercsoportokat vizsgáljuk, amik a 0-t fixálják. Itt definiáljuk a $\sim_k$ ekvivalencia-relációkat, amik $p-1/k$ darab k elemű részre osztanak minden 1 dimenziós alteret. Kiderül, hogy a K^ω vektortér automorfizmuscsoportjának bármely G 0-t fixáló zárt szupercsoportjához van olyan k, hogy G hat a $\sim_k$-ekvivalenciaosztályok halmazán, és ez a hatás vagy (1) a teljes szimmetrikus csoport, vagy (2) a projektív lineáris csoport (és ekkor $k = p-1$). A 3.1. alfejezetben megadjuk az (1) esethez tartozó szupercsoportok teljes klasszifikációját. Végül a 3. fejezet eredményeit használva a 4. fejezetben bebizonyítjuk, hogy a vektortérnek pontosan 2 olyan reduktja van, ami a 0-t nem fixálja: ezek a végtelen dimenziós affin tér és megszámlálhatóan végtelen halmaz (struktúra nélkül).

3. A vektortér 0-t fixáló reduktjai

Legyen $p \geq 3$ prím és jelölje V a megszámlálhatóan végtelen dimenziós vektorteret $\mathbb{F}_p$ fölött. Ebben a fejezetben V automorfizmuscsoportjának azon zárt $\mathrm{Aut}(V) \leq$ $\leq G \leq \mathrm{Sym}(V)$ szupercsoportjait vizsgáljuk, amelyek stabilizálják a 0-t. Ehhez először szükségünk lesz néhány definícióra. Tetszőleges $k|p-1$ esetén jelölje Γ_k az $\mathbb{F}_p$-beli k-adik egységgyökök által alkotott részcsoportot: $\Gamma_k = \{g \in \mathbb{F}_p \mid g^k = 1\}$. Nyilván, $\Gamma_k \leq \mathbb{F}_p^\times$ és $|\Gamma_k| = k$.

3.0.5. Definíció. *Legyen $k|p-1$, $a, b \in V \setminus 0$. Ekkor legyen $a \sim_k b$ ha $a = \lambda b$ valamely $\lambda \in \Gamma_k$ esetén.*

Mivel Γ_k csoport, $\sim_k$ ekvivalencia reláció. Valóban: $a \sim_k a$, mert $a = 1 \cdot a$. Ha $a \sim_k b$, akkor $a = \lambda b$ valamilyen $\lambda \in \Gamma_k$-ra, így $b = \lambda^{-1} a$, azaz $\sim_k$ szimmetrikus. Ha $a \sim_k b$ és $b \sim_k c$, akkor $a = \lambda b$ és $b = \mu c$ valamely $\lambda, \mu \in \Gamma_k$-ra. Mivel Γ_k csoport, ezért $\lambda\mu \in \Gamma_k$, így $a = \lambda\mu c$, tehát $a \sim_k c$ és így $\sim_k$ tranzitív is. A $\sim_k$ reláció az egydimenziós altereket $p-1/k$ darab k elemû osztályra osztja.

3.0.6. Definíció. *Legyen G egy tetszőleges csoport, ami hat $V \setminus 0$-n: $G \leq \mathrm{Sym}(V)$ és $a, b \in V \setminus 0$. Legyen $a \sim_G b$, ha $\langle a^g \rangle = \langle b^g \rangle$ minden $g \in G$ esetén.*

Ekkor $\sim_G$ ekvivalenciareláció $V \setminus 0$-n. Egy $a \in V \setminus \{0\}$ esetén jelölje $\sim_G(a)$ az a vektor $\sim_G$- osztályát.

3.0.7. Állítás. *Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ tetszőleges csoport. Ekkor $\sim_G = \sim_k$ valamilyen $k|p-1$ esetén.*

Bizonyítás. Ha $\mathrm{Aut}(V) \leq H \leq G \leq \mathrm{Sym}(V)_0$, akkor $\sim_G(a) \subseteq \sim_H(a)$, így $\sim_G(a) \subseteq \subseteq \sim_{\mathrm{Aut}(V)}(a) = \langle a \rangle \setminus \{0\}$ teljesül. Legyen most $H_a = \{\lambda \in \mathbb{F}_p^\times \mid a \sim_G \lambda a\}$. Azt állítjuk, hogy H_a nem függ a választásától, azaz $a, b \in V \setminus \{0\}$ esetén $H_a = H_b$. Tegyük fel ugyanis, hogy $a \sim_G \lambda a$, de $b \not\sim_G \lambda b$. Ekkor definíció szerint létezik olyan $h \in G$, hogy $\langle b^h \rangle \neq \langle \lambda b^h \rangle$. Legyen $g \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, amelyre $a^g = b$. Ekkor $a^{gh} = b^h$ és $(\lambda a)^{gh} = (\lambda b^h)$, azaz $\langle a^{gh} \rangle \neq \langle \lambda a^{gh} \rangle$, ami ellentmond annak, hogy $a \sim_G \lambda a$. Jelöljük ezt a közös H_a halmazt Γ-val. Azt állítjuk, hogy Γ részcsoport $\mathbb{F}_p^\times$-ben. Mivel $\sim_G$ reflexív, $1 \in \Gamma$. A szimmetria miatt ha $\lambda \in \Gamma$ akkor $\lambda a \sim_G \lambda^{-1}(\lambda a)$-bõl következik, hogy Γ zárt az inverzképzésre. Végül tegyük fel, hogy $\mu, \lambda \in \Gamma$, és $a \in V \setminus 0$ tetszőleges. Ekkor $a \sim_G \lambda a \sim_G \mu(\lambda a)$, így $a \sim_G \mu\lambda a$, így $\mu\lambda \in \Gamma$. Tehát Γ valóban részcsoportja $\mathbb{F}_p^\times$-nek, ami ciklikus, ezért ha $|\Gamma| = k$, akkor $k|p-1$ és $\Gamma = \Gamma_k$. Ebből pedig következi, hogy $u \sim_G v$ pontosan akkor teljesül, ha van olyan $\lambda \in \Gamma$, hogy $u = \lambda v$, azaz pontosan akkor, ha $u \sim_k v$, és ezt kellett bizonyítani. □

A továbbiakban egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ csoport esetén jelölje k_G azt a $k|p- -1$ értéket, amelyre $\sim_G = \sim_k$. A $\sim_G$ reláció definíciójából látható, hogy G megőrzi a $\sim_G$ relációt, így G hat a $\sim_G$-ekvivalenciaosztályok halmazán. Ha $k_G = p-1$, azaz a $\sim_G$-ekvivalenciaosztályok V egydimenziós alterei (a 0 nélkül), akkor a $\sim_G$-elvivalenciaosztályok egy megszámlálhatóan végtelen dimenziós $\mathbb{F}_p$ feletti projektív teret alkotnak az örökölt struktúrában. Most azt fogjuk belátni, hogy ha $\mathrm{Aut}(V) \leq \leq G \leq \mathrm{Sym}(V)_0$ egy zárt csoport, akkor G-re az alábbiak valamelyikre teljesül:

1. $k_G = p - 1$, és G a $P := (V \setminus 0)/\sim_G$ projektív téren a projektív lineáris transzformációk csoportjaként hat,

2. G a szimmetrikus csoportként hat a $\sim_G$-ekvivalenciaosztályok halmazán.

Ezen állítás bizonyításához először belátjuk n szerinti indukcióval, hogy ha egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ csoportra nem teljesül a fenti (1) feltétel, akkor n tetszőleges pont beleképezhető egy G-beli elemmel V egy „elég kicsi” alterébe. Az alábbi észrevételt számos alkalommal fogjuk használni.

3.0.8. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, és legyen* S *egy véges részhalmaza* V*-nek. Ekkor egy* $v \in V \setminus S$ *vektorra az alábbiak ekvivalensek:*

1. $G_S(v)$ *végtelen.*

2. $G_S(v)$ *tartalmaz olyan vektort, ami nincs benne az* $\langle S \rangle$ *altérben.*

3. $G_S(v) \supset V \setminus \langle S \rangle$.

Bizonyítás. Az (1) $\to$ (2) irány nyilvánvaló, hiszen $\langle S \rangle$ véges. A (3) $\to$ (1) irány szintén nyilvánvaló, hiszen $V \setminus \langle S \rangle$ végtelen. Tegyük fel most, hogy v-re teljesül (2). Ekkor van olyan $u \in G_S(v)$ vektor, amit nem tartalmaz az $\langle S \rangle$ altér. Ekkor használva, hogy G_S tranzitív $V \setminus \langle S \rangle$-en (3) adódik. □

3.0.9. Definíció. *A továbbiakban egy $G \leq \mathrm{Sym}(V)_0$ csoport és egy $S \subset V$ részhalmaz esetén jelölje $A_k^G(S)$ azon $v \in V$ vektorok halmazát, amelyre $S \cup \{v\}$ beleképezhető egy G-beli elemmel V egy k dimenziós alterébe.*

3.0.10. Lemma. *Legyen $G \leq \mathrm{Sym}(V)_0$ egy csoport, és legyen $S \subset V$, $|S| = b$ egy tetszőleges részhalmaz. Ekkor az alábbiak valamelyik teljesül:*

- $|A_k^G(S)| = 0$,
- $|A_k^G(S)| = p^k$, *és van olyan $g \in G$, amire $A_k^G(S)^g$ egy k dimenziós altere V-nek.*
- $A_k^G(S) = V$.

Bizonyítás. Ha az S halmaz nem képezhető bele egy k dimenziós altérbe egy G-beli elemmel, akkor definíció szerint $A_k^G(S) = \emptyset$. Tegyük fel most, hogy nem ez a helyzet, és legyen ekkor $g \in G$ egy olyan transzformáció, amire S^g-t tartalmazza V egy U k-dimenziós altere. A definícióból könnyen látható, hogy $A_k^G(S) = (A_k^g(S^g))^{g^{-1}}$, így elég belátni, hogy $|A_k^G(S^g)| = p^k$ vagy $A_k^G(S^g) = V$. Nyilván $U \subset A_k^G(S^g)$. Ha $U = A_k^G(S^g)$, akkor készen vagyunk, hiszen $|U| = p^k$, és U egy altér.

Ha nem, akkor $A_k^G(S^g)$ tartalmaz olyan v vektort, ami nincs benne U-ban, tehát $\langle S^g \rangle$-ben sincs benne. Ekkor a 3.0.8. Lemma szerint

$$G_{S^g}(v) \supset V \setminus \langle S \rangle \supset V \setminus U,$$

így $A_k^G(S^g) \supset V \setminus U$. Azonban láttuk, hogy $A_k^G(S^g) \supset U$ is teljesül, így $A_k^G(S^g) = V$.

□

3.0.11. Lemma. *Legyen $G \leq \mathrm{Sym}(V)_0$ egy csoport, és legyen $S \subset V$, $|S| = n$ egy tetszőleges részhalmaz. Tegyük fel továbbá, hogy egy $g \in G$ elemre teljesül, hogy $S^g \subset A_k^G(S)$. Ekkor $A_k^G(S) = A_k^G(S)^g$.*

Bizonyítás. Ha $A_k^G(S) = \emptyset$ vagy $A_k^G(S) = V$, akkor az állítás nyilvánvaló. Ha nem, akkor a 3.0.10. Lemma szerint $|A_k^G(S)| = p^k$, és $A_k^G(S)^h$ egy k dimenziós altere V-nek valamilyen $h \in G$-re. Ez azonban azt jelenti, hogy tetszőleges $v \in A_k^G(S)$ esetén

$$v \in A_k^G(A_k^G(S)) \subset A_k^G(S^g) = A_k^G(S)^g,$$

hiszen $S^g \subset A_k^G(S)$. Tehát $A_k^G(S) \subset A_k^G(S)^g$, de $|A_k^G(S)| = |A_k^G(S)^g| = p^k$, így $A_k^G(S) = A_k^G(S)^g$ □

A 3.0.11. lemmát általában abban az esetben fogjuk használni, amikor g egy lineáris transzformáció és S lineárisan független elemekből áll. Ebben az esetben az állítás az alábbi formában is igaz.

3.0.12. Következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, és legyen $S \subset V$. Tegyük fel továbbá, hogy $x_1, \dots, x_m \in A_k^G(S)$ és $y_1, \dots, y_m \in A_k^G(S)$ lineárisan független rendszerek. Ekkor tetszőleges $\lambda_1, \dots, \lambda_m \in \mathbb{F}_p$ esetén*

$$\sum_{i=1}^m \lambda_i x_i \in A_k^G(S) \quad \textit{pontosan akkor, ha} \quad \sum_{i=1}^m \lambda_i y_i \in A_k^G(S).$$

Bizonyítás. Legyen $S := \{a_1, \dots, a_n\}$. Az általánosság megszorítása nélkül feltehető, hogy $y_1 = a_1, \dots, y_m = a_m$. Mivel $x_1, \dots, x_m$ lineárisan függetlenek és $\dim\langle a_1, \dots, a_n, x_1, \dots, x_m\rangle \geq n$, ezért létezik olyan $\{i_{m+1}, \dots, i_n\} \subset \{1{,}2, \dots, n\}$, hogy $x_1, x_2, \dots, x_m, a_{i_{m+1}}, \dots, a_{i_n}$ lineárisan függetlenek. Ekkor létezik olyan $g \in$ $\in \mathrm{Aut}(V) \subset G$ lineáris transzformáció, amire $a_j^g = x_j$, ha $1 \leq j \leq m$ és $a_j^g =$ $= a_{i_j}$. Ekkor $S^g \subset A_k^G(S)$ a feltétel szerint, így a 3.0.11. Lemma szerint $A_k^G(S) =$ $= A_k^G(S)^g$. Mivel g lineáris, ezért ekkor $\sum_{i=1}^m \lambda_i a_i \in A_k^G(S)$ pontosan akkor teljesül, ha $\left(\sum_{i=1}^m \lambda_i a_i\right)^g \in A_k^G(S)$. Ismét a linearitást használva ez ekvivalens azzal, hogy $\sum_{i=1}^m \lambda_i a_i^g \in A_k^G(S)$, azaz $\sum_{i=1}^m \lambda_i x_i \in A_k^G(S)$ és ezt kellett bizonyítanunk. □

A továbbiakban többször fogjuk használni az alábbi affin geometriai tényt, ezért most külön is kimondjuk.

3.0.13. Lemma. *Legyen A egy véges dimenziós affin tér egy K test felett, ahol $\mathrm{char}\, K \neq 2$. Tegyük fel továbbá, hogy a $\emptyset \neq H \subset A$ halmazra teljesül a következő: ha $x, y \in H$, akkor $L(x, y) \subset H$, ahol $L(x, y)$ jelöli az x és y pontok által kifeszített egyenest. Ekkor H affin altere A-nak.*

Vegyük észre, hogy a 3.0.13. Lemmában tényleg szükséges a $\mathrm{char}\, K \neq 2$ feltétel. Tegyük fel ugyanis, hogy $K = \mathbb{F}_2$, és legyen A tetszőleges affin altér $\mathbb{F}_2$ felett. Ekkor A tetszőleges részhalmazára teljesül a feltétel, hiszen ekkor tetszőleges $x, y \in A$ különböző pontok esetén $L(x, y) = \{x, y\}$.

3.0.14. Lemma. *Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ egy csoport, és legyen $S \subset V$, $|S| = n$ lineárisan független vektorok halmaza. Ekkor ha $A_k^G(S)$ tartalmaz egy 0-n nem átmenő affin egyenest, akkor $|A_k^G(S)| \geq p^{n-1} + 1$. Speciálisan $k < n$ esetén $A_k^G(S) = V$.*

Bizonyítás. Legyen $S = \{a_1, \dots, a_n\}$, és legyen L egy affin egyenes, ami nem megy át a 0-n, és $L \subset A_k^G(S)$. Legyen u, v két tetszőleges (különböző) pont L-en, ekkor $L = L(u, v)$. Mivel az L egyenes nem megy át a 0-n, ezért az u és v vekorok lineárisan függetlenek. Legyen most A az $a_1, \dots, a_n$ pontok által kifeszített affin altér V-ben, és legyen $H := A \cap A_k^G(S)$. Azt állítjuk, hogy a H halmazra teljesülnek a 3.0.13. Lemma feltételei. Legyenek ugyanis $x, y \in H$ tetszőlegesek. Azt kell belátnunk, hogy $L(x, y) \subset A \cap A_k^G(S)$. Az $l(xy) \subset A$ tartalmazás triviális, mert A affin altér. Tehát már csak azt kell belátnunk, hogy az $L(x, y)$ egyenest tartalmazza $A_k^G(S)$.

Tegyük fel először, hogy az x és y vektorok lineárisan összefüggenek. Ekkor $y =$ $= \lambda x$ valamilyen $\lambda \in \mathbb{F}_p$-re, és így $0 \in L(x, y)$. Ekkor azonban $0 \in A$ is teljesül, mert A affin altér. Ez azonban lehetetlen, hiszen A minden eleme $\sum_{i=1}^n \lambda_i a_i$ alakú, ahol $\sum \lambda_i = 1$, ami nem lehet 0, mivel az $a_1, \dots, a_n$ vektorok lineárisan függetlenek.

Legyenek most x és y lineárisan függetlenek. Azt kell belátnunk, hogy minden $\lambda \in \mathbb{F}_p$-re $\lambda x + (1 - \lambda) y \in A_k^G(S)$. A 3.0.12. Következmény miatt ehhez elég belátni, hogy vannak olyan x' és y' lineárisan független elemek $A_k^G(S)$-ben, amire $\lambda x' + (1 -$ $- \lambda) y' \in A_k^G(S)$ teljesül. Mivel $L = L(u, v) \subset A_k^G(S)$, ezért az $x' = u$ és az $y' = v$ választás megfelel.

Ezzel beláttuk, hogy a H halmazra teljesülnek a 3.0.13. Lemma feltételei, így a 3.0.13. Lemma szerint H affin altér. Mivel H tartalmazza az $a_1, \ldots, a_n$ vektorokat, ezért csak $H = A$ lehetséges. Azt kaptuk tehát, hogy az $a_1, \ldots, a_n$ vektorok által kifeszített affin alteret tartalmazza $A_k^G(S)$. Mivel ezek a vektorok lineárisan függetlenek, ezért affin függetlenek is, így ezen altér számossága p^{n-1}. Amint már láttuk, ez az altér nem tartalmazza a 0-t. A 0-t azonban mindig tartalmazza $A_k^G(S)$, ha nem üres, így $|A_k^G(S)| \geq p^{n-1} + 1$. Végül ha $n \geq k+1$, akkor $|A_k^G(S)| > p^k$, és ekkor a 3.0.10. Lemma szerint csak $A_k^G(S) = V$ lehetséges. □

A következő állítás bizonyításához szükségünk lesz az alábbi technikai jellegű lemmára.

3.0.15. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, és legyen* $S \subset V$, $|S| = n$ *lineárisan független vektorok halmaza. Tegyük fel továbbá, hogy az* $A_k^G(S)$ *halmaz tartalmaz egy*

$$v = \sum_{i=1}^{n} \lambda_i a_i \in A_k^G(G)$$

alakú vektort valamilyen λ_i*-kre, ahol a* λ_i *együtthatók közül legalább 2 nem 0 és nem mindegyik -1.*

Ekkor léteznek olyan $b_1, \ldots, b_n, w \in A_k^G(S)$ *vektorok, amelyekre* $b_1, \ldots, b_n$ *lineárisan függetlenek,* $w \notin \langle b_1 + b_2 + \ldots + b_n \rangle$ *és* $w \notin \langle b_i, b_j \rangle$ *semmilyen* i, j*-re.*

Bizonyítás. Ha a $b_i = a_i$, $v = w$ választás jó, akkor készen vagyunk. Tegyük fel ezért, hogy nem ez a helyzet. Ekkor $v = \lambda(a_1 + a_2 + \ldots + a_n)$ valamilyen $\lambda \neq -1$-re vagy $v \in \langle a_i, a_j \rangle$ valamilyen $1 \leq i < j \leq n$ indexekre. Tegyük fel először, hogy $v = \lambda(a_1 + a_2 + \ldots + a_n)$ valamilyen $\lambda \neq -1$-re. Ebben az esetben $a_1 = \frac{1}{\lambda} v - a_2 - \ldots - a_n$, így mivel $n \geq 3$ és $\frac{1}{\lambda} \neq -1$, ezért ekkor a $b_1 = v, b_2 = a_2, \ldots, b_n = a_n, w = a_1$ választás megfelel a feltételeinknek.

Maradt az az eset, amikor $v \in \langle a_i, a_j \rangle$ teljesül valamilyen $1 \leq i < j \leq n$-re. Ebben az esetben $v = \lambda a_i + \mu a_j$ alakú, ahol $\lambda, \mu \neq 0$. Mivel $n \geq 3$, ezért létezik egy $l \neq i, j$ index. Legyen ekkor $w = \lambda a_i + \mu a_j$. A 3.0.12. Következmény szerint $w \in A_k^G(S)$. Legyen most $b_i = \lambda a_i + \mu a_j$, és legyen $b_m = a_m$, ha $m \neq i$. Ekkor $b_1, \ldots, b_n, w \in A_k^G(S)$ és mivel $\lambda \neq 0$, ezért a $b_1, \ldots, b_n$ vektorok lineárisan függetlenek, továbbá

$$w = \lambda a_i + \mu a_l = \lambda a_i + \mu a_j + \mu(a_l - a_j) = b_i + \mu b_l - \mu b_j.$$

Ezt azt jelenti, hogy a $b_1, \ldots, b_n, w$ vektorok ezen választása megfelel a feltételeinknek, hiszen $\mu \neq 0$, és $p \geq 3$ miatt $1 = \mu = -\mu$ nem lehetséges. □

Tegyük fel, hogy $G \leq \mathrm{Sym}(V)_0$ egy olyan csoport, amire teljesül, hogy tetszőleges $a_1, \ldots, a_n$ nem nulla elemek beleképezhetőek egy k dimenziós W altérbe egy G-beli transzformációval valamilyen k-ra. Azt állítjuk, hogy ekkor $n \leq \frac{p^k - 1}{k_G}$. Ekkor ugyanis, hogy az $a_1, \ldots, a_n$ vektorokkal együtt a $\sim_G(a_i)$ osztály minden eleme is beleképződik az altérbe. Mivel ezen osztályok diszjunktak, és $0 \in W$, a $\sim_G(a_i)$

osztályok elemszáma k_G, az $nk_G + 1 \leq |W| = p^k$ becslés adódik, azaz átrendezve $n \leq \frac{p^k-1}{k_G}$.

Azt kaptuk tehát, hogy $\frac{p^k-1}{k_G}$ egy olyan n lehetséges legnagyobb értéke, amire minden V-beli n-es beleképezhető V egy k dimenziós alterébe egy G-beli transzormációval. A továbbiakban majd belátjuk, hogy bizonyos feltételek mellett ez az érték „majdnem” el is érhető.

3.0.16. Állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, amire* $k_G < p-1$*; vagy* $k_G = p-1$ *és* G *hatása a* $P := (V \setminus 0)/\sim_G$ *projektív téren* nem *a projektív lineáris transzformációk csoportja. Tegyük fel továbbá, hogy az* $n \geq 3$*, és legyen* k *a legkisebb olyan egész szám, amire teljesül, hogy* $k \geq 2$ *és* $n \leq \frac{p^k-1}{k_G} - 1$*. Ekkor tetszőleges* $S \subset V, |S| = n$ *halmaz beleképezető* V *egy* k *dimenziós alterébe egy* G*-beli elemmel.*

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk. Tegyük fel először, hogy $n = 3$. Ekkor elég belátni, hogy 3 lineárisan független elem beleképezhető V egy 2 dimenziós alterébe egy G-beli elemmel.

1/a eset: $n = 3$ **és** $k_G = p-1$ ♦ Tegyük fel, hogy $k_G = p-1$. Tekintsük ekkor G hatását a $P := (V \setminus 0)/\sim_G$ projektív téren. A feltétel szerint ez nem a projektív lineáris csoport, legyen tehát $g \in G$ egy olyan elem, aminek a hatása a P projektív téren nem projektivitás. A projektív geometria alaptétele szerint egy $\mathrm{Sym}(P)$-beli permutáció pontosan akkor projektivitás, ha tartja az egyeneseket, így van olyan $L \subset P$ projektív egyenes, amire L^g nem projektív egyenes. Legyen U az L egyeneshez tartozó 2 dimenziós altér V-ben. Ekkor tehát $\dim\langle U^g\rangle \geq 3$, így vannak olyan $a, b, c \in U^g \subset V$ lineáris an független elem, amikre $a^{g^{-1}}, b^{g^{-1}}, c^{g^{-1}}$ vektorokat tartalmazza az U 2 dimenziós altér. Mivel $\mathrm{Aut}(V)$ (és így G is) tranzitívan hat a V-beli lineárisan független hármasok halmazán, így tetszőleges lineáris független hármas beleképezhető egy 2-dimenziós altérbe.

1/b eset: $n = 3$ **és** $k_G < p-1$ ♦ Ekkor léteznek olyan $0 \neq a, b \in V$ elemek, amikre $\langle a\rangle = \langle b\rangle$, de $a \not\sim_G b$. Ekkor tehát a^g, b^g lineárisan függetlenek valamilyen $g \in G$ esetén. Legyen c egy az a^g és b^g-től független vektor V-ben. Ekkor tehát az a^g, b^g, c lineárisan független vektorokat a $g^{-1} \in G$ transzformáció V egy 2-dimenziós alterébe képezi. Az $\mathrm{Aut}(V)$ csoport (és így G is) azonban tranzitívan hat a V-beli lineárisan független hármasok halmazán, így tetszőleges lineáris független hármas beleképezhető egy 2-dimenziós altérbe.

2. eset: $n > 3$ ♦ Tegyük fel most, hogy teljesül az állítás n-re. Belátjuk, hogy ekkor $n+1$-re is teljesül. Legyen k a legkisebb olyan egész, amire $k \geq 2$ és $n \leq \frac{p^k-1}{k_G} - 1$. Ha $n+1 > \frac{p^k-1}{k_G} - 1$, akkor készen vagyunk, hiszen ekkor a legkisebb olyan k' egész, amire $k' \geq 2$ és $n+1 \leq \frac{p^{k'}-1}{k_G} - 1$ is teljesül, az legalább $k+1$. Tegyük fel most, hogy $n+1 \leq \frac{p^k-1}{k_G} - 1$, azaz $n \leq \frac{p^k-1}{k_G} - 2$. Ekkor azt kell belátnunk, hogy tetszőleges $T \subset V, |T| = n+1$ esetén a T halmaz beleképezhető egy k dimenziós altérbe egy G-beli transzformációval.

Tegyük fel, hogy ez nem teljesül, és legyen ekkor T olyan ellenpélda, amire $\dim\langle T\rangle$ maximális.

2/a eset: $\dim\langle T\rangle \leq n$. ♦ Ha $\dim\langle T\rangle \leq n$, akkor van olyan $v \in T$, hogy $\langle T \setminus \setminus \{v\}\rangle = \langle T\rangle$. Az indukciós feltétel szerint van olyan $g \in G$, hogy $(T \setminus \{v\})^g$-t tartalmazza V egy k dimenziós altere. Ekkor azonban v nem lehet benne ebben az altérben, így $v^g \notin \langle (T \setminus \{v\})^g\rangle$, amiből a 3.0.8. Lemma szerint $|G_{(T\setminus\{v\})^g}(v^g)| = \infty$, és így $|G_{T\setminus\{v\}}(v)| = \infty$ is teljesül. Ebből következik szintén a 3.0.8. Lemma szerint, hogy van olyan $h \in G$, ami stabilizálja a $T \setminus \{v\}$ halmazt, de $v^h \notin \langle T \setminus \{v\}\rangle$. Ez azt jelenti, hogy $\dim\langle T^h\rangle = \dim\langle T, v^h\rangle > \dim\langle T\rangle$. Mivel $\dim\langle T\rangle$ maximális, ezért létezik olyan $h' \in G$ transzformáció, ami a T^h halmazt egy k dimenziós altérbe viszi. Ekkor azonban a $hh' \in G$ transzformáció egy legfeljebb k dimeziós altérbe viszi T-t, ami ellentmondás.

2/b eset: $\dim\langle T\rangle = n+1$ ♦ Legyen most $S := T \setminus \{v\}$ valamilyen $v \in T$-re. Ekkor $|S| = n$, és S lineárisan független rendszer. A feltétel szerint $v \notin A_k^G(S)$, így $A_k^G(S) \neq V$. A 3.0.10. Lemma szerint ekkor $A_k^G(S) \leq p^k$. Ha $u \in A_k^G(S)$, akkor az $A_k^G(S)$ halmaz definíciója szerint $G_S(u) \subset A_k^G(S)$, speciálisan $G_S(u)$ véges. Ekkor a 3.0.8. lemma szerint $u \in \langle S\rangle$. Tehát $A_k^G(S) \subset \langle S\rangle$. Három alesetet különböztetünk meg.

2/b/1 aleset: $\lambda a_i \in A_k^G(S)$ valamilyen $\lambda \notin \Gamma_{k_G} \cup \{0\}$ és $i = 1,2,\ldots,n$ esetén. Legyen

$$S_j := S \cup \{\lambda a_i\} \setminus \{a_j\}$$

minden $j \neq i$ esetén. Ekkor minden $j \neq i$-re $a_j \notin \langle S_j\rangle$, így a 3.0.8. Lemma szerint $|G_{S_j}(a_j)| = \infty$. Mivel $\lambda \notin \Gamma_{k_G} \cup \{0\}$, ezért $0 \neq \lambda a_i \not\sim a_i$, azaz létezik olyan $g \in \in G$ transzformáció, amire a_i^g és $(\lambda a_i)^g$ lineárisan függetlenek. Válasszuk meg ezt a g transzformációt úgy, hogy $\dim\langle (S \cup \{\lambda a_i\})^g\rangle$ maximális legyen. Azt állítjuk, hogy ekkor $\dim\langle (S \cup \{\lambda a_i\})^g\rangle = n+1$, azaz az $(S \cup \{\lambda a_i\})^g$ halmaz elemei lineárisan függetlenek. Tegyük fel ugyanis, hogy $\dim\langle (S \cup \{\lambda a_i\})^g\rangle \leq n$. Ekkor mivel a_i^g és $(\lambda a_i)^g$ lineárisan függetlenek, ezért létezik olyan $j \neq i$, hogy $\langle S_j^g\rangle = \langle S_j \cup \{a_j\}\rangle = = \langle (S \cup \{\lambda a_i\})^g\rangle$. Ebből következik, hogy $G_{S_j}(a_j) = \infty$, és így $|G_{S_j^g}(a_j^g)| = \infty$. Ezért a 3.0.8. Lemma szerint van olyan $h \in G$, hogy $(S_j^g)^h = S_j^g$, de $a_j^h \notin \langle S_j^g\rangle$. Ebből

$$\dim\langle (S \cup \{\lambda a_i\})^{gh}\rangle = \dim\langle (S \cup \{\lambda a_i\})^g\rangle + 1,$$

ami ellentmond $\dim\langle (S \cup \{\lambda a_i\})^g\rangle$ maximalitásának. Tehát $(S \cup \{\lambda a_i\})^g$ elemei lineárisan függetlenek. Megint a 3.0.8. Lemmát használva adódik, hogy $|G_{S^g}((\lambda a_i)^g)| = \infty$, így $|G_S(\lambda a_i))| = \infty$. Ez azonban lehetetlen, hiszen $\lambda a_i \in A_k^G(S)$, így $G_S(\lambda a_i) \subset \subset A_k^G(S)$, ami véges.

2/b/2 aleset: $v = \sum_{i=1}^n \lambda_i a_i \in A_k^G$ valamilyen λ_i-kre, ahol a λ_i együtthatók közül legalább 2 nem 0 és nem mindegyik -1. Ebben az esetben a 3.0.15. Lemma szerint léteznek olyan $b_1, \ldots, b_n, w \in A_k(S)$ elemek, amelyekre $b_1, \ldots, b_n$ lineárisan függetlenek, $w \notin \langle b_1+b_2+\ldots+b_n\rangle$ és $w \notin \langle b_i, b_j\rangle$ semmilyen i,j-re. A 3.0.12. Következményt az $a_1, a_2, \ldots, a_n$ és $b_1, b_2, \ldots, b_n$ lineáris független rendszerekre alkalmazva adódik, hogy létezik olyan $w \in A_k(S)$ is, amire $w \notin \langle b_1 + b_2 + \ldots + b_n\rangle$ és $w \notin \langle b_i, b_j\rangle$. Rögzítsünk most egy ilyen tulajdonságú w-t. Ekkor $w = \sum_{i=1}^n \lambda_i a_i$ alakú, ahol a λ_i együtthatók közül legalább 3 nem 0, és nem mindegyik egyforma. Legyen tehát $1 \le i < j \le n$ olyan indexek, amire $\lambda_i \neq \lambda_j$. Legyen $\lambda := \lambda_i - \lambda_j \neq 0$. Legyen továbbá $a'_j = a_i, a'_i = a_j$ és $a'_l = a_l$ minden $i,j \neq l$ index esetén. Ekkor a 3.0.12. Következményt az $a_1, a_2, \ldots, a_n$ és $a'_1, a'_2, \ldots, a'_n$ vektorrendszerekre alkalmazva azt kapjuk, hogy

$$A_k^G(S) \ni w' := \sum_{i=1}^n \lambda_i a'_i = \sum_{i=1}^n \lambda_i a_i + \lambda(a_j - a_i) = w + \lambda(a_j - a_i).$$

A feltevésünk szerint $w \notin \langle a_i, a_j\rangle$, így $w, a_i, a_j \in A_k^G(S)$ lineárisan függetlenek. Ekkor persze $w' = w + \lambda(a_j - a_i), a_i$ és a_j is lineárisan függetlenek. Alkalmazzuk most a 3.0.12. Következményt a w, a_i, a_j és w', a_i, a_j vektorrendszerekre. Mivel $w + \lambda a_i + + \lambda a_j = w' \in A_k^G(S)$, ezért ekkor

$$A_k^G(S) \ni w'' := w' + \lambda a_i + \lambda a_j = w + 2\lambda(a_i + a_j).$$

Ezt az eljárást folytatva adódik, hogy $w + s\lambda(a_j - a_i) \in A_k^G(S)$ minden $s \in \mathbb{F}_p$ esetén. Mivel $\lambda \neq 0$, ezért ezt azt jelenti, hogy

$$L := \{w + \mu(a_j - a_i) : \mu \in \mathbb{F}_p\} \subset A_k^G(S).$$

Mivel azonban w, a_1, a_2 lineárisan függetlenek, így L egy 0-n nem átmenő affin egyenes, így a 3.0.14. Lemma szerint $|A_k(S)| \ge p^{n-1} + 1$. Azonban már láttuk, hogy $|A_k(S)| \le p^k$, így $p^{n-1} < p^{n-1} + 1 \le p^k$, azaz $n - 1 < k$. A k szám a definíciója alapján a legkisebb olyan pozitív egész, amire $k \ge 2$ és $n \le \frac{p^k-1}{k_G} - 1$ teljesülnek. Ez azt jelenti, hogy a $k' = n - 1$ választás „túl kicsi", azaz ekkor a $k' \ge 2$ és az $n \le \frac{p^{k'}-1}{k_G} - - 1$ egyenlőtlenségek valamelyikre nem teljesül. Mivel $n \ge 3$, így a $k' = n - 1 \ge 2$ egyenlőtlenség teljesül. Tehát

$$n > \frac{p^{k'} - 1}{k_G} - 1 = \frac{p^{n-1} - 1}{k_G} - 1 \ge \frac{p^{n-1} - 1}{p - 1} - 1 = (1 + p + p^2 + \ldots + p^{n-2}) - 1 \ge$$
$$\ge p + p^2(1 + p + \ldots + p^{n-4}) \ge 3 + (n - 3) = n,$$

hiszen $p \ge 3$, ami ellentmondás.

2/b/3 aleset: Minden $A_k^G(S)$-beli elem vagy $v = \lambda a_i$ alakú valamilyen $\lambda \in \Gamma_{k_G}$ és $1 \le i \le n$-re, vagy $v' = \lambda(a_1 + a_2 + \ldots + a_n)$ alakú, ahol $\lambda \in \{0, -1\}$. Ez a feltétel pontosan azt jelenti, hogy az $A_k^G(S)$ halmazt tartalmazza a

$$H := \{\lambda a_i : 1 \le i \le n, \lambda \in \Gamma_{k_G}\} \cup \{0, -a_1 - a_2 - \ldots - a_n\}$$

halmaz. Mivel $|\Gamma_{k_G}| = k_G$, ezért a H halmaz számossága $nk_G + 2$. Ekkor az $n \le \le \frac{p^k-1}{k_G} + 2$ egyenlőtlenséget használva

$$|A_k^G(S)| \le |H| = nk_G + 2 \le p^k - 1 - 2k_G + 2 \le p^k - 1 < p^k$$

adódik, ami ellentmondás, hiszen feltettük, hogy $A_k^G(S) = p^k$.

Tehát minden esetben ellentmondáshoz vezetett a feltevésünk, így valóban tetszőleges $T \subset V, |T| = n+1$ halmaz beleképezhető egy k dimenziós altérbe egy G-beli transzformációval, és ezt kellett bizonyítanunk. □

3.0.17. Következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, amire* $k_G < p-1$*; vagy* $k_G = p-1$ *és* G *hatása a* $P := (V \setminus 0)/\sim_G$ *projektív téren* nem *a projektív lineáris transzformációk csoportja. Legyen továbbá* $k \geq 2$ *tetszőleges egész. Ekkor tetszőleges* $S \subset V, |S| = \frac{p^k-1}{k_G} - 1$ *halmaz beleképezető* V *egy* k *dimenziós alterébe egy* G*-beli elemmel.*

Bizonyítás. Alkalmazzuk a 3.0.16. Állítást $n := \frac{p^k-1}{k_G} - 1$ esetén. □

3.0.18. Állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, amire* $k_G < p-1$*; vagy* $k_G = p-1$ *és* G *hatása a* $P := (V \setminus 0)/\sim_G$ *projektív téren* nem *a projektív lineáris transzformációk csoportja. Ekkor tetszőleges* $k \geq 2$ *pozitív egészre a* G *csoport* $\frac{p^k-1}{k_G} - 1$*-szeresen tranzitívan hat a* $\sim_G$*-ekvivalenciaosztályok halmazán.*

Bizonyítás. Legyen $k \geq 2$ és $n := \frac{p^k-1}{k_G} - 1$. Mivel $\mathrm{Aut}(V)$ (és így G is) tranzitívan hat a lineárisan független n-esek halmazán, ezért az állításhoz elég belátni, hogy tetszőleges n (különböző) ekvivalenciaosztály átvihető n független vektorhoz tartozó ekvivalenciaosztályba egy G-beli transzformációval. Ehhez elég belátni, hogy tetszőleges $a_1, \ldots, a_n$ páronként inekvivalens elem elemek átvihetők n lineárisan független elembe egy G-beli transzformációval.

Legyenek tehát $a_1, \ldots, a_n \in V \setminus 0$ páronként inekvivalens elemek, és $b_1, \ldots, b_n \in V \setminus 0$ lineárisan független elemek. A 3.0.17. Következmény szerint ekkor léteznek olyan $g, h \in G$ transzformációk, amire az $\{a_1^g, \ldots, a_n^g\}$ és a $\{b_1^h, \ldots, b_n^h\}$ halmazt is tartalmazza V egy k dimenziós altere. Mivel $\mathrm{Aut}(V)$ (és így G is) tranzitívan hat V k dimenziós alterein, azért feltehető, hogy az előbbi két k dimenziós altér megegyezik. Jelöljük ezt az alteret U-val. Minden egydimenziós altér pontosan $\frac{p-1}{k_G}$ darab $\sim_G$-ekvivalenciaosztály és a $\{0\}$ uniója, így V minden k dimenziós altere $\frac{p^k-1}{p-1} \cdot \frac{p-1}{k_G} = \frac{p^k-1}{k_G}$ darab $\sim_G$-ekvivalenciaosztály és a $\{0\}$ uniója. A $\sim_G$ relációja definíciójából adódik, hogy az $\{a_1^g, \ldots, a_n^g\}$ és a $\{b_1^h, \ldots, b_n^h\}$ halmaz elemei páronként inekvivalensek. Ez azonban azt jelenti, hogy léteznek olyan $u, v \in U \setminus 0$ vektorok, hogy $\{a_1^g, \ldots, a_n^g, u\}$ és a $\{b_1^h, \ldots, b_n^h, v\}$ halmazok is az $U \setminus 0$ halmazbeli ekvivalenciaosztályok egy teljes reprezentációs rendszerét adják. Legyen most $\gamma \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, ami fixálja az U alteret, mint halmazt, és az $u^\gamma = v$. Ekkor azonban az $a_1^{g\gamma}, \ldots, a_n^{g\gamma}$ vektorokhoz tartozó ekvivalenciaosztályok halmaza megegyezik a $b_1^h, \ldots, b_n^h$ vektorokhoz tartozó ekvivalenciaosztályok halmazával. Ez azt jelenti, hogy létezik az $1, 2, \ldots, n$ indexeknek egy olyan $\pi \in S_n$ permutációja, amire $a_i^{g\gamma} \sim_G b_{\pi(i)}^h$ minden $1 \leq i \leq n$-re. Ekkor azonban $a_i^{g\gamma h^{-1}} \sim_G b_{\pi(i)}$. Speciálisan léteznek olyan $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_p^\times$ számok, hogy $a_i^{g\gamma h^{-1}} = \lambda_i b_{\pi(i)}$ minden $1 \leq i \leq n$-re. A jobb oldalon álló vektorok azonban lineárisan függetlenek, hiszen a feltétel szerint $b_1, \ldots, b_n$ lineárisan függetlenek. Tehát a $g\gamma h^{-1} \in G$ transzformáció bizonyítja az állítást. □

A fejezet főtételének bizonyításához szükségünk lesz még az alábbi lemmára.

3.0.19. Lemma. *Tegyük fel, hogy $G \subset \mathrm{Sym}(H)$ egy zárt csoport, ahol $|H| = \omega$, és legyen $\sim$ egy ekvivalenciareláció H-n, amire minden $\sim$-ekvivalenciaosztály véges. Tegyük fel továbbá, hogy G kompatibilis a $\sim$ ekvivalenciarelációval, azaz $x \sim y$ pontosan akkor teljesül, ha $x^g \sim y^g$. Ekkor G hatása a $\sim$-ekvivalenciaosztályok halmazán is zárt.*

Bizonyítás. Legyen $g \in \mathrm{Sym}(H/\sim)$ tetszőleges, amire teljesül, hogy tetszőleges $F \subset H/\sim$ véges halmaz esetén van olyan $\tilde{h} \in G$, amire $\tilde{h}$ és g hatása megegyezik F-en. Be kell látnunk, hogy ekkor létezik olyan a $\tilde{g} \in G$ transzformáció is, amire $\tilde{g}$ és g hatása megegyezik az összes $\sim$-ekvivalenciaosztályok halmazán.

Egy $F \subset H/\sim$ esetén jelölje $\tilde{F}$ az F-beli ekvivalenciaosztályok unióját. Ekkor ha F véges, akkor $\tilde{F}$ is. Legyen $X_1, X_2, \ldots$ a $\sim_G$ ekvivalenciaosztályok egy felsorolása. Legyen $F_i := \{X_1, X_2, \ldots, X_n\}$. Ekkor az F_i halmazok végesek, $\emptyset = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \ldots$,és $\bigcup_{i=0}^{\infty} F_i = H/\sim$. Mivel g bijekció, ezért $\bigcup_{i=0}^{\infty} F_i^g = H/\sim$ is teljesül. Ezekből következik az is, hogy

$$\bigcup_{i=1}^{\infty} X_i = \bigcup_{i=1}^{\infty} X_i^g = H.$$

Definiáljuk a T gyökeres fát a következőképpen. Jelölje T_n a T gyökeres fa n-edik szintjét. Ekkor minden n-re a T_n-en lévő csúcsok legyenek az olyan f függvények, amikre $D(f) = \tilde{F}_n$, és létezik olyan $\tilde{h} \in G$ függvény, amire $\tilde{h}|_{\tilde{F}_i} = h$, továbbá $\tilde{h}$ és g hatása megegyezik a $H/\sim$ halmazon. A T gráfban az $f_1 \in T_{n-1}$ és $f_2 \in T_n$ csúcsok között vezessen él, ha $f_2|_{\tilde{F}_n} = f_1$. Ekkor az egyetlen T_0-beli csúcs az üres függvény, jelöljük ezt most f_0-lal. Ez lesz a T gyökeres fa gyökere. A definícióból könnyen látható, hogy ebben a gráfban ha $f \in V(T_n)$, akkor f_0-ból pontosan egy út vezet f-be, nevezetesen

$$(f_0 = f|_{\tilde{F}_0}, f|_{\tilde{F}_1}, \ldots, f|_{\tilde{F}_{n-1}}, f).$$

A T gráf tehát valóban fa. Azt állítjuk, hogy létezik az f_0 csúcsból induló végtelen út T-ben. Ehhez a König-lemmát feltételeit fogjuk ellenőrizni.

(1) Létezik akármilyen hosszú f_0-ból induló út. Ehhez elég belátni, hogy T_n nem üres minden n-re. Legyen tehát n tetszőleges, és legyen ekkor $\tilde{h}$ egy olyan függvény, amire $\tilde{h}$ és g hatása megegyezik F_n-en. A feltételeink szerint létezik ilyen $\tilde{h}$. Legyen most $\tilde{h}|_{\tilde{F}_n} = f$. Ekkor T_n definíciója szerint $f \in V(T_n)$.

(2) Minden T-beli csúcs kifoka véges. Ennél többet fogunk bizonyítani, belátjuk ugyanis, hogy T_n véges minden n-re. Tegyük fel, hogy $f \in T_n$. Ekkor $D(f) = \tilde{F}_n = \bigcup_{i=1}^{n} X_i$, és a feltétel szerint

$$R(f) \subset \bigcup_{i=1}^{n} X_i^f = \bigcup_{i=1}^{n} X_i^g.$$

Az $\bigcup_{i=1}^n X_i \to \bigcup_{i=1}^n X_i^g$ függvények száma azonban véges, hiszen az $X_1, \dots, X_n, X_1^g, \dots, X_n^g$ ekvivalenciaosztályok végesek, és ekkor a $\bigcup_{i=1}^n X_i$ és $\bigcup_{i=1}^n X_i$ halmazok is végesek.

Tehát a T gyökeres fára (ahol f_0 a gyökér) valóban teljesülnek a König-lemma feltételei. Ekkor a König-lemma szerint létezik az f_0 csúcsból induló végtelen út T-ben. Legyen ez $(f_0, f_1, \dots)$. Ekkor $f_n \in T_n$, így $D(f_n) = \tilde{F}_n$, és $j > i$ esetén $f_j|_{\tilde{F}_i} = f_i$. Ebből következik, hogy $\bigcup_{i=0}^\infty f_i$ is függvény. Legyen ez f. Ekkor

$$D(f) = \bigcup_{i=0}^{\infty} D(f_i) = \bigcup_{i=0}^{\infty} D(f_i) = \bigcup_{i=0}^{\infty} X_i = H,$$
$$R(f) = \bigcup_{i=0}^{\infty} R(f_i) = \bigcup_{i=0}^{\infty} R(f_i) = \bigcup_{i=0}^{\infty} X_i^g = H.$$

Tegyük fel most, hogy $u \neq v \in H$. Ekkor van olyan n, hogy $u, v \in D(f_n) = \tilde{F}_n$. Legyen most $\tilde{h} \in G$ egy olyan függvény, amire $\tilde{h}|_{\tilde{F}_n} = f_n$. Ekkor mivel $\tilde{h}$ bijekció, ezért $u^{\tilde{h}} \neq v^{\tilde{h}}$, amiől $u^{f_n} \neq v^{f_n}$, és így $u^f \neq v^f$. Az f függvény tehát egy $H \to H$ bijekció.

Belátjuk most, hogy $f \in G$. Ehhez G zártsága miatt elég belátni, hogy H tetszőleges F véges részhalmazához létezik olyan $\tilde{h} \in G$ függvény, amire $\tilde{h}|_{\tilde{F}_n} = f_n = f|_{\tilde{F}_n}$. Legyen tehát F egy tetszőleges véges részhalmaza H-nak. Ekkor van olyan n, hogy $F \subset D(f_n) = \tilde{F}_n$, és ekkor az f_n függvény definíciója miatt létezik $\tilde{h} \in G$ függvény, amire $\tilde{h}|_{\tilde{F}_n} = f_n = f|_{\tilde{F}_n}$.

Azt állítjuk most, hogy a $\tilde{g} = f$ választás jó lesz, azaz f és g hatása megegyezik a $H/\sim$ halmazon. Legyen ugyanis $X_i \in H/\sim$ tetszőleges. Ekkor $j \geq i$ esetén az f_j függvények definíciója miatt $X_i^{f_j} = X_i^g$, és így $X_i^f = X_i^g$. □

3.0.20. Tétel. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport. Ekkor az alábbiak valamelyike teljesül:*

1. $k_G = p - 1$, *és* G *a* $P := (V \setminus 0)/\sim_G$ *projektív téren a projektív lineáris transzformációk csoportjaként hat,*

2. G *teljes szimmetrikus csoportként hat a* $\sim_G$*-ekvivalenciaosztályok halmazán.*

Bizonyítás. Tegyük fel, hogy a G csoportra nem teljesül az (1) feltétel. Be kell látni, hogy ekkor G szimmetrikus csoportként hat a $\sim_G$-ekvivalenciaosztályok halmazán.

Ha G-re nem teljesül az (1) feltétel, akkor a 3.0.11. Állítás szerint a G csoport $\frac{p^k-1}{k_G} - 1$-szeresen tranzitív a $\sim_G$-ekvivalenciaosztályok halmazán minden $k \geq 2$-re. Mivel $\frac{p^k-1}{k_G} - 1$ érték tetszőleges nagy lehet, ezért ebből következik az is, hogy G minden n-re n-tranzitívan hat a $\sim_G$-ekvivalenciaosztályok halmazán, tehát G hatása sűrű a $\sim_G$-ekvivalenciaosztályok halmazán.

Be kell még látnunk, hogy ez a hatás zárt is. Ez a 3.0.19. Lemma szerint teljesül, hiszen G kompatiblis a $\sim_G$ relációval, és minden $\sim_G$ ekvivalenciaosztály véges. □

A későbbiekben még szükségünk lesz a 3.0.20. Tétel állítására a $k_G = 1$ esetben, ezért ezt külön is kimondjuk.

3.0.21. Következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, amire* $k_G = 1$*. Ekkor* $G = \mathrm{Sym}_0(V)$*.*

Bizonyítás. Mivel $p \geq 3$, ezért $k_G = 1 \neq p - 1$, tehát ekkor a G csoportra 3.0.20. Tételbeli (2) feltétel teljesül. $k_G = 1$ esetén definíció szerint a $\sim_G$ ekvivalenciaosztályok egy eleműek, tehát ekkor G a szimmetrikusan csoportként hat $V \setminus 0$-n, azaz $G = \mathrm{Sym}_0(V)$. □

3.1. Azon zárt csoportok leírása, amik a teljes szimmetrikus csoportként hatnak a $\sim_G$-ekvivalenciaosztályok halmazán

Ebben a fejezetben klasszifikációját azon $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ zárt csoportokat, amikre a 3.0.20. Tétel (2) feltétele teljesül, azaz amikre G hatása a $\sim_G$-ekvivalenciaosztályok halmazán a teljes szimmetrikus csoport. Ezen csoportok leírásához szükségünk lesz a következő definíciókra.

3.1.1. Definíció. *Legyen* $k|p-1$ *tetszőleges. Ekkor egy* $f : V \setminus 0 \to \Gamma_k$ *függvényt* k-címkézés*nek hívunk, ha tetszőleges* $u \in V \setminus 0$ *és* $\lambda \in \Gamma_k$ *esetén* $f(\lambda u) = \lambda f(u)$*.*

A definícióból könnyen látható, hogy a $V \setminus 0$ halmaz k-címkézései természetes módon megfeleltethetőek a $\sim_k$-ekvivalenciaosztályok egy reprezentánsrendszerével. Ebből speciálisan az is következik, hogy minden $k|p-1$-re van címkézése $V \setminus 0$-nak. A megfeleltetés a következő: ha adott egy f címkézés, akkor az 1 elem f szerinti őszképe egy reprezentánsrendszer. Megfordítva: ha adott egy X reprezentánsrendszere a $\sim$ $\sim_k$-ekvivalenciaosztályoknak, akkor minden $v \in V \setminus 0$ esetén legyen $f(v)$ értéke az az egyetlen λ, amire $v = \lambda v'$ alakú valamilyen $v' \in X$ esetén. A továbbiakban a $\{v \in V \setminus 0 : f(v) = 1\}$ halmazt jelöljük V^f-fel.

3.1.2. Definíció. *Legyen* $k|p-1$ *tetszőleges, és* f *egy* k*-címkézés* $V \setminus 0$*-n. Ekkor egy* $g \in \mathrm{Sym}(V)_0$ *permutációról azt mondjuk, hogy az* f k*-címkézéssel* kompatibilis*, ha* g *megőrzi a* $\sim_k$ *relációt, és* $f(v^g) = f(v)$ *minden* $v \in V \setminus 0$*-ra.*

3.1.3. Definíció. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy csoport, legyen továbbá* f *egy tetszőleges* k_G*-címkézés* $V \setminus 0$*-n. Jelölje ekkor* G_f *azon* $g \in G$ *elemek részcsoportját, amik kompatibilisek* f*-fel.*

3.1.4. Definíció. *Legyen* $k|p-1$ *tetszőleges, és* f *egy* k*-címkézés* $V \setminus 0$*-n. Ekkor egy* $g \in \mathrm{Sym}((V \setminus 0)/\sim_k)$ *elem esetén jelölje* g^f *azt az egyértelmű* $\tilde{g} \in \mathrm{Sym}(V)_0$ *elemet, amire* $\tilde{g}$ *kompatibilis az* f k*-címkézéssel, és* g *és* $\tilde{g}$ *hatása megegyezik a* $\sim_k$*-ekvivalenciaosztályok halmazán.*

Egy $H \leq \mathrm{Sym}((V \setminus 0)/\sim_k)$ *részcsoport esetén legyen* $H^f = \{g^f : g \in H\}$*.*

A 3.1.5 - 3.1.9. Lemmákban a címkézések segítségével leírjuk azon $\mathrm{Aut}(V) \leq$ $\leq G \leq \mathrm{Sym}(V)_0$ zárt csoportok szerkezetét, amik a szimmetrikus csoportként hatnak a $\sim_{k_G}$-ekvivalenciaosztályok halmazán. Kiderül, hogy minden ilyen G előáll $G^* \cdot (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f)$ alakban, ahol a G^* csoport azon G-beli elemek csoportja, amik minden $\sim_G$-ekvivalenciaosztályt (halmazként) stabilizálnak.

Ezután a 3.1.10 - 3.1.17. Lemmákban leírjuk azon csoportokat, amik előállnak az előbbi G^* csoportként, és ezzel megkapjuk a teljes klasszifikációt is. Kiderül végül, hogy azon $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ zárt csoportok, amik a szimmetrikus csoportként hatnak a $\sim_k$-ekvivalenciaosztályok halmazán bijekcióban állnak a k fokú szimmetrikus csoport bizonyos tulajonságú (N, H) részcsoportpárjaival. Ez a bijekció nem fog függeni attól, hogy melyik címkézést használjuk, azonban a definíciójukban, és a későbbi bizonyításokban végig használni kell valamilyen k-címkézést.

Első lépésként bebizonyítjuk, hogy ha $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ egy zárt csoport, ami a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán, akkor $G_f = (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$.

3.1.5. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, és* f *egy* k_G *címkézés. Ekkor* G_f *is zárt.*

Bizonyítás. A definícióból látható, hogy $G_f = G \cap (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$ így elég belátni, hogy $(\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$ zárt. Tegyük fel tehát, hogy $g \in \mathrm{Sym}(V)$ és minden $F \subset V$ véges halmazra van olyan $h \in (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$, hogy $g|_F = h|_F$. Be kell látnunk, hogy ekkor g is kompatibilis f-fel. Tegyük fel tehát, hogy $u \in V \setminus 0$. Legyen ekkor $F = \{u\}$. Erre alkalmazva az előbbi észrevételt $f(u) = f(u^h) = f(u^g)$. Mivel ez minden $u \in V \setminus 0$-ra teljesül, ezért g kompatibilis f-fel. □

3.1.6. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim_{k_G}$*-ekvivalenciaosztályok halmazán, és* f *egy* k_G*-címkézés. Tegyük fel továbbá, hogy* G_f *tartalmaz egy olyan* g *elemet, amire a* $\{v \in V \setminus 0 :$ $: v \neq v^g\} \cap V^f$ *halmaz véges, nem üres, és elemei lineárisan függetlenek. Ekkor* $G_f = (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$.

Bizonyítás. Egy f k_G-címkézéssel kompatibilis permutáció hat a $V^f = \{v \in V \setminus 0 :$ $: f(v) = 1\}$ halmazon, továbbá egy f-fel kompatibilis g permutációt meghatároz a g permutációnak a $\sim_{k_G}$-ekvivalenciaoszályok halmazán való hatása, amit viszont meghatároz g hatása az V^f halmazon. Ez ezt jelenti, hogy a lemma állításához elég belátni, hogy $G_f|_{V^f} = \mathrm{Sym}(V^f)$. A 3.1.5. Lemma szerint G_f zárt, így $G_f|_{V^f}$ is zárt. Ez azt jelenti, hogy a lemma állításához elég belátni, hogy a lemma feltételei mellett G_f hatása sűrű a V^f halmazon. Ehhez azt fogjuk bizonyítani, hogy G_f hatása a V^f halmazon tartalmaz minden transzpozíciót.

Legyen X egy tetszőleges végtelen, lineáris független elemekből álló halmaz, ami tartalmazza a $\{v \in V \setminus 0 : v \neq v^g\} \cap V^f$ halmazt. Legyen $\mathrm{Sym}^F(X)$ azon $h \in$ $\in \mathrm{Sym}(X)$ elemek csoportja, amik véges sok kivétellel minden X-beli elemet fixen hagynak, legyen továbbá $\mathrm{Alt}^F(X)$ a páros permutációk csoportja $\mathrm{Sym}^F(X)$-ben. Legyen $H := \mathrm{Sym}^F(X) \cap ((G_f)_X)|_X$, azaz azon $h \in \mathrm{Sym}^F(X)$-ek halmaza, amiket identitásként kiterjesztve $V \setminus X$-re egy G_f-beli elemet kapunk. Azt állítjuk, hogy ekkor a H csoport normálosztó $\mathrm{Sym}^F(V^f)$-ben.

Legyen ugyanis $h \in H$, és $\gamma \in \mathrm{Sym}^F(X)$ tetszőleges. Ekkor γ kiterjed V egy automorfizmusává, jelöljük ezt a kiterjesztést is γ-val. Feltehető, hogy ez a kiterjesztés kompatibilis f-fel. Ekkor tehát $\gamma \in \mathrm{Aut}(V)_f \subset G_f$. Tekintsük ekkor a $\gamma h \gamma^{-1} \in \in \mathrm{Sym}(X)$ permutációt. Ekkor $\gamma h \gamma^{-1} \in ((G_f)_X)|_X$, és ekkor $\gamma h \gamma^{-1} \in ((G_f)_X)|_X \cap \cap \mathrm{Sym}^F(X) = H$. Tehát valóban $H \triangleleft \mathrm{Sym}^F(X)$. Ismert, hogy ekkor $H = 1$ vagy $H \supset \mathrm{Alt}^F(X)$. A lemma feltétele szerint a $\{v \in V \setminus 0 : v \neq v^g\} \cap V^f \subset X$ halmaz nem üres, így $\mathrm{id} \neq g|_X \in H$. Tehát H nem lehet a triviális csoport.

Azt kaptuk tehát, hogy H tartalmazza $\mathrm{Alt}^F(X)$-et. Ekkor persze $((G_f)_X)|_X$ is tartalmazza $\mathrm{Alt}^F(X)$-et. Az $\mathrm{Alt}^F(X)$ alternáló csoport azonban sűrű $\mathrm{Sym}(X)$-ben. Azt állítjuk, hogy $((G_f)_X)|_X$ zárt is. Ehhez elég belátni, hogy $(G_f)_X$ zárt. Ez teljesül, hiszen a $G_f|_{V^f}$ csoportról láttuk, hogy zárt, és $X \subset V^f$. Ebből következik, hogy $((G_f)_X)|_X = \mathrm{Sym}(X)$. Speciálisan $((G_f)_X)|_X$ tartalmaz minden transzpozíciót. Ez azt jelenti, hogy minden $u, v \in X$ elemre $G_f|_{V^f}$ tartalmazza az (uv) transzpozíciót. Ekkor persze $G_f|_{V^f}$ bármely $u, v \in V^f$ lineárisan független elemekre tartalmazza az $u, v \in V^f$ transzpozíciót. Be kell még látnunk, hogy ez akkor is teljesül, ha $u, v \in V^f$ nem lineárisan függetlenek. Ebben az esetben legyen $w \in V^f \setminus \langle u, v \rangle$ egy tetszőleges vektor. Ekkor $(uw), (vw) \in G_f|_{V^f}$, amiből $(uv) = (uw)(vw)(uw) \in \in G_f|_{V^f}$. A $G_f|_{V^f}$ csoport tehát valóban tartalmaz minden transzpozíciót, és ezt kellett bizonyítanunk. □

A következő állítás bizonyításához szükségünk lesz az alábbi jelölésre.

3.1.7. Definíció. *Legyen $k | p-1$ és legyen $g \in \mathrm{Sym}(V)_0$ egy tetszőleges elem, ami megőrzi a $\sim_k$-ekvivalenciarelációt. Legyen továbbá f egy tetszőleges k-címkézés $V \setminus \setminus 0$-n. Ekkor egy $v \in V \setminus 0$ esetén jelölje $\sigma_f(g, v)$ a*

$$\lambda \mapsto f((\lambda \tilde{v})^g) : \Gamma_{k_G} \to \Gamma_k$$

leképezést, ahol $\tilde{v}$ jelöli az $\sim_G(v)$ ekvivalenciaosztály egyetlen olyan elemét, amire $f(v) = 1$ (azaz $\tilde{v} = \frac{v}{f(v)}$). Amennyiben ez nem okoz félreértést a σ leképezésben az f címkézést nem írjuk ki.

A definícióból könnyen látható, hogy a $\sigma(g, v)$ leképezés mindig bijekció, és $v \sim \sim_G v'$ esetén $\sigma(g, v) = \sigma(g, v')$. Ha a $g, h \in \mathrm{Sym}(V)_0$ elem megőrzik a $\sim_k$ relációt, akkor tetszőleges $v \in V \setminus 0$ esetén $\sigma(gh, v) = \sigma(g, v)\sigma(h, v^g)$.

A következő állításban belátjuk, hogy a 3.1.6. Lemma feltételei valójában automatikusan teljesülnek minden megfelelő G csoportra.

3.1.8. Állítás. *Legyen $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ egy zárt csoport, ami a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán, és f egy k_G címkézés. Ekkor $G_f = (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$.*

Bizonyítás. Ezen állítás bizonyításához a 3.1.6. Lemmát fogjuk használni. Legyenek $a_1, a_2, \ldots, a_p \in V_f$ tetszőleges lineáris független elemek. A bizonyítás további részében az indexeket mod p értjük. Mivel G a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán, ezért van olyan $g \in G$, amire $(\sim_G(a_i))^g = \sim_G(a_{i+1})$ és $b^g = b$ minden $b \in (V \setminus 0)/\sim_{k_G} \setminus \{\sim_G(a_1), \sim_G(a_2), \dots, \sim_G(a_p)\}$-re. Legyen $\sigma_i := \sigma(g, a_i)$, és legyen γ_i egy olyan lineáris transzformáció, amire $a_j^{\gamma_i} = a_{j+i}$ minden $j = 1{,}2, \dots, p$-re. Legyen továbbá $g_i := \gamma_i^{-1} a_i \gamma_i$. Ekkor persze az így kapott g_i-kre is teljesül, hogy $(\sim_G(a_j))^{g_i} = \sim_G(a_{j+1})$ és $b^{g_i} = b$ minden $b \in (V \setminus 0)/\sim_{k_G} \setminus \{\sim_G(a_1), \sim_G(a_2), \dots, \sim_G(a_p)\}$, azaz g_i és g hatása megegyezik $(V \setminus 0)/\sim_G$-n. Azt állítjuk, hogy $\sigma(g_i, a_j) = \sigma_{j-i}$. Valóban mivel γ_i lineáris, ezért tetszőleges $j = 1{,}2, \dots, p$ és $\lambda \in \Gamma_{k_G}$ esetén

$$f((\lambda a_j)^{g_i}) = f(\lambda a_j^{g_i}) = f(\lambda a_{j+i}) = \lambda,$$

így $\sigma(\gamma_i, a_j) = \mathrm{id}\,\Gamma_k$, amiből

$$\begin{aligned}\sigma(g_i, a_j) = \sigma(\gamma_{-i} g \gamma_i, a_j) = \sigma(\gamma_{-i}, a_j)\sigma(g\gamma_i, a_j^{\gamma_{-i}}) = \sigma(g\gamma_i, a_j^{\gamma_{-i}}) = \\ = \sigma(g\gamma_i, a_{j-i}) = \sigma(g, a_{j-i})\sigma(\gamma_i, a_{j-i}^{\gamma_i}) = \sigma_{j-i}\sigma(\gamma_i, a_j) = \sigma_{j-i}.\end{aligned}$$

Legyen most $g' = g_0 g_1, \dots, g_{k_G!-1} \in G$. Az így kapott g' hatása a $\sim_{k_G}$ ekvivalenciaosztályok halmazán megegyezik $g^{k!}$ hatásával és tetszőleges $i = 1{,}2, \dots, p$-re

$$\begin{aligned}\sigma(g', a_i) = \sigma(g_0, a_i)\sigma(g_1, a_i^{g_0})\sigma(g_2, a_i^{g_0 g_1}) \dots \sigma(g_{k_G!-1}, a_i^{g_0 g_1, \dots, g_{k_G!-2}}) = \\ = \sigma(g_0, a_i)\sigma(g_1, a_{i+1}) \dots \sigma(g_{k_G!-1}, a_{i+k_G!-1}) = \sigma(g, a_i)^{k_G!} = \mathrm{id}\,\Gamma_{k_G},\end{aligned}$$

hiszen $|\operatorname{Sym}(\Gamma_{k_G})| = k_G!$

Legyen $g'' = g'^{k_G!-1} \in G$. Azt állítjuk, hogy $g'' \in G_f$, azaz minden $u \in \operatorname{Sym}((V \setminus 0)/\sim_{k_G}$ esetén $\sigma(g, u) = \mathrm{id}\,\Gamma_{k_G}$. Tegyük fel először, hogy $u = \sim_G(a_i)$ valamilyen i-re. Ekkor

$$\begin{aligned}\sigma(g'', a_i) = \sigma(g', a_i)\sigma(g', a_i^{g'}) \dots \sigma(g', a_i^{g'^{k_g!-1}}) = \\ = \sigma(g', a_i)\sigma(g', a_{i+k_G!}) \dots \sigma(g', a_{i+(k_G!-1)k_G!}) = \mathrm{id}\,\Gamma_{k_G}.\end{aligned}$$

Tegyük fel most, hogy u különbözik minden $\sim_G(a_i$-től. Ekkor

$$\sigma(g'', u) = \sigma(g', u)\sigma(g', u^{g'}) \dots \sigma(g', u^{g'^{k_g!-1}}) = \; = \sigma(g', u)^{k_G!} = \mathrm{id}\,\Gamma_{k_G},$$

hiszen $|\operatorname{Sym}(\Gamma_{k_G})| = k_G!$.

A $g'' \in G_f$ permutáció hatása a $\sim_G$-ekvivalenciaosztályok halmazán megegyezik $g'^{k_G!}$ hatásával, ami pedig megegyezik $g^{(k_G!)^2}$ hatásával. Ebből következik, hogy $a_i^{g''} \sim_G a_i^{g^{(k_G!)^2}} = a_{i+(k_G!)^2} \not\sim_G a_i$, hiszen az $a_1, \dots, a_p$ elemek páronként inekvivalensek, és $k_G < p$ miatt $((k_G!)^2, p) = 1$, amiből $i \not\equiv i + (k_G!)^2 \mod p$. Speciálisan $a_i^{g''} \neq a_i$. Ha egy $v \in V \setminus 0$ elem nincs benne a $\sim_G(a_i)$ ekvivalenciaosztályok egyikében sem, akkor $v^{g''} \sim_G v$. Ekkor azonban mivel $g'' \in G_f$, ezért $f(v^{g''}) = f(v)$ is teljesül, ami csak $v^{g''} = v$ esetén lehetséges. Tehát a $g'' \in G_f$ permutációra

$$\{v \in V \setminus 0 : v \neq v^g\} \cap V^f = \{a_1, \dots, a_p\}.$$

Ez a halmaz véges és nem üres, így a 3.1.6. Lemma szerint $G_f = (\operatorname{Sym}((V \setminus 0)/\sim_{k_G})^f$. $\square$

3.1.9. Következmény. *Legyen* $\mathrm{Aut}(V) \le G \le \mathrm{Sym}(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim_{k_G}$*-ekvivalenciaosztályok halmazán, és* f *egy* k_G*-címkézés. Ekkor* $G = G^* \cdot (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$ *alakú, ahol*

$$G^* = \{g \in G : g \textit{ identitásként hat } (V \setminus 0)/\sim_{k_G}\textit{-n}\}.$$

Bizonyítás. A „$\supset$" tartalmazás következik a 3.1.8. Állításból. Tegyük fel most, hogy $g \in G$. Ekkor a 3.1.8. Állítás szerint van olyan $g' \in G_f$, hogy g és g' hatása megegyezik a $\sim_G$-ekvivalenciaosztályok halmazán. Ekkor $g^* := gg'^{-1} \in G^*$, és $g = g^*g'$. $\square$

A 3.1.9. Következményből következik az is, hogy a G^* csoport már meghatározza G-t, így elég a lehetséges G^* csoportokat klasszifikálni. A bizonyításból az is könnyen látható, hogy a $G = G^* \cdot (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$ szorzat valójában egy $G = G^* * \rtimes (\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$ szemidirekt szorzat.

Egy $k|p-1$ szám esetén jelöljük $\mathrm{Sym}_0^{(k)}(V)$-vel azon permutációk csoportját, amik megőrzik a $\sim_k$ relációt. Ekkor persze $\mathrm{Aut}(V) \le \mathrm{Sym}_0^{(k)}(V)$ minden $k|p-1$-re, és egy $\mathrm{Aut}(V) \le G \le \mathrm{Sym}(V)$ csoportra pontosan akkor teljesül $k_G = k$, ha $G \le \mathrm{Sym}_0^{(k)}(V)$, de $G \not\le \mathrm{Sym}_0^{(k')}(V)$ minden $k' < k$-ra. Legyen

$$\mathcal{S}^{(k)} = (\mathrm{Sym}_0^{(k)}(V))^*,$$

azaz azon permutációk halmaza, amik minden $\sim_k$ ekvivalenciaosztályt önmagukra képeznek. Ekkor egy $\mathrm{Aut}(V) \le G \le \mathrm{Sym}(V)_0$ csoportra $G^* = G \cap \mathcal{S}^{(k_G)}$.

Ha a g, h elemek az $\mathcal{S}^{(k)}$ részcsoportban vannak, akkor tetszőleges $v \in V \setminus 0$-ra $\sigma(gh, v) = \sigma(g, v)\sigma(h, v)$. Ezt azt jelenti, hogy a

$$\mathcal{S}^{(k)} \to \mathrm{Sym}(\Gamma), g \mapsto \sigma(g, u)$$

leképezés egy homomorfizmus minden $u \in V \setminus 0$ esetén. Azt állítjuk, hogy egy $g \in \mathcal{S}^{(k)}$ csoportbeli elemet meghatároz a $\sigma(g, u)$ homomorfizmusnál vett képei. Valóban ha a $\sigma(\cdot, u)$ homomorfizmusok adottak, akkor egy $u \in V \setminus 0$ esetén $u^g = f(u)^{\sigma(g,u)} \frac{u}{f(u)}$. Ez azt jelenti, hogy az előbbi G^* csoport meghatározásához elég meghatározni, hogy egy G^*-beli elemnek mik lehetnek a képei a $\sigma(\cdot, u) : u \in V \setminus 0$ homomorfizmusoknál.

3.1.10. Definíció. *Legyen* $G \le \mathrm{Sym}_0^{(k)}(V)$ *egy csoport és* f *egy* k*-címkézés. Ekkor egy* $v \in V \setminus 0$ *elemre legyen*

$$H_v(G) := \{\sigma(g, v) : g \in G^*\}$$

és

$$N_v(G) := \{\sigma(g, v) : g \in G^*, \sigma(g, u) = \mathrm{id}\, \Gamma_k \textit{ minden } u \not\sim_k v\textit{-re}\}.$$

A definícióból látható, hogy $N_v(G)$ és $H_v(G)$ részcsoportjai $\mathrm{Sym}(\Gamma_k)$-nak, és $N_v(G) \subset H_v(G)$.

3.1.11. Lemma. *Legyen* $G \le \mathrm{Sym}_0^{(k)}(V)$ *egy csoport és* f *egy* k*-címkézés. Ekkor ha* G *tartalmazza* $\mathrm{Aut}(V)$*-t, akkor az* $N_v(G)$ *és* $H_v(G)$ *csoportok nem függnek a* v *vektor választásától.*

Bizonyítás. Tegyük fel, hogy $\mathrm{Aut}(V) \leq G$. Az állítást nyilván elég belátni V^f-beli vektorokra. Tegyük fel tehát, hogy $u, v \in V^f$, és legyen $\gamma \in \mathrm{Aut}(V) \leq G$ egy lineáris transzformáció, amire $u^\gamma = v$.

Tegyük fel most, hogy egy σ permutáció benne van $H_u(G)$-ben. Ekkor van olyan $g \in G^*$, hogy $\sigma(g, u) = \sigma$. Ezesetben a $\gamma^{-1} \in G^*$ permutációra $\sigma(\gamma^{-1} g \gamma, v) = \sigma$. Tehát $H_u(G) \subset H_v(\mathrm{g})$. Hasonlóan $H_v(G) \subset H_u(G)$ is teljesül, így $H_u(G) = H_v(G)$.

Tegyük fel, hogy $\sigma \in N_u(G)$. Ekkor van olyan $g \in G^*$, hogy $\sigma(g, u) = \sigma$ és $\sigma(g, u') = \mathrm{id}\,\Gamma$ minden $u' \not\sim {}_k u$ esetén. Ezesetben a $\gamma^{-1} \in G^*$ permutációra $\sigma(\gamma^{-1} g \gamma, v) = \sigma$ és $\sigma(\gamma^{-1} g \gamma, v') = \mathrm{id}\,\Gamma$ minden $v' \not\sim {}_k v$ esetén, így $N_u(G) \subset N_v(G)$. Hasonlóan $N_v(G) \subset N_u(G)$. Tehát $N_u(G) = N_v(G)$. □

A továbbiakban az $N_u(G)$ és $H_u(G)$ jelöléseknél néha el fogjuk hagyni az alsó indexeket, amennyiben $G \geq \mathrm{Aut}(V)$. Ezt a A 3.1.11. Lemma miatt megtehetjük.

3.1.12. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}_0^{(k)}(V)$ *egy csoport és* f *egy* k*-címkézés. Ekkor* $N(G) \triangleleft H(G)$.

Bizonyítás. Legyenek $\sigma \in N(G), \sigma' \in H(G)$ tetszőlegesek, legyen továbbá $u \in V \setminus 0$ tetszőleges. Be kell látnunk, hogy $\sigma'^{-1} \sigma \sigma' \in N(G)$. A felírt tartalmazások szerint vannak olyan $g, h \in G^*$, hogy $\sigma(h, u) = \sigma', \sigma(g, u) = \sigma$ és $\sigma(g, u') = \mathrm{id}(G)$ minden $u' \not\sim u$ esetén. Ekkor $h^{-1} g h \in G^*$ és $\sigma(h^{-1} g h, u) = \sigma'^{-1} \sigma \sigma'$. Ha $u' \not\sim u$, akkor $\sigma(h^{-1} g h, u) = \sigma'^{-1}\,\mathrm{id}\,\Gamma_k \sigma' = \sigma'^{-1} \sigma' = \mathrm{id}\,\Gamma_k$. Ez éppen azt jelenti, hogy $\sigma'^{-1} \sigma \sigma' \in$ $\in N(G)$. □

3.1.13. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim {}_{k_G}$*-ekvivalenciaosztályok halmazán. Ekkor az* $N(G)$ *és* $H(G)$ *részcsoportok a címkézéstől is függetlenek.*

Bizonyítás. Ebben a bizonyítás az $N(G)$ és $H(G)$ csoportoknál felső indexben jelezzük, hogy melyik k_G-címkézést használjuk a definíciójuknál. A $\mathcal{S}^{(k(G))}$ csoport nem függ a címkézéstől, így a $G^* = G \cap \mathcal{S}^{(k(G))}$ csoport sem. Egy rögzített f k_G-címkézésre, egy $g \in G^*$-beli elemre és egy $v \in V \setminus 0$ vektorra pontosan akkor teljesül $\sigma_f(g, u) = \mathrm{id}\,\Gamma_{k_G}$, ha g identitásként hat a $\sim {}_G(v)$ ekvivalenciaosztályon. Így ez a tény is független a címkézés megválasztásától. Ezeket használva a következő módon bizonyítható a lemma.

Legyenek f és f' két tetszőleges k_G-címkézés $V \setminus 0$-n. Legyen most f'' egy olyan címkézés, amelyik valamelyik k_G ekvivalenciaosztályon megegyezik f-fel és valamelyik ekvivalenciaosztályon megegyezik f'-vel. Legyen u tehát egy olyan elem, amire a $\sim {}_G(u)$ ekvivalenciaosztályon f és f'' megegyezik. Ekkor egy $g \in G^*$ elemre $\sigma_f(g, u) = \sigma_{f''}(g, u)$. Ebből következik, hogy $H^f(G) = H_u^f(G) = H_u^{f''}(G) = H^f(G)$. Tegyük fel most, hogy $\sigma \in N^f(G)$. Ekkor van olyan $g \in G^*$ transzformáció, amire $\sigma_f(g, u) = \sigma$ és $\sigma_f(g, u') = \mathrm{id}\,\Gamma_{k_G}$ minden $u' \not\sim u$-ra. Ebből következik $\sigma_{k_G, f''}(g, u) =$ $= \sigma_{f''}(g, u) = \sigma$ és $\sigma_{f''}(g, u') = \mathrm{id}\,\Gamma_{k_G}$ minden $u' \not\sim u$-ra, hiszen amint láttuk az, hogy $\sigma_f = \mathrm{id}\,\Gamma_{k_G}$ teljesül-e nem függ a címkézés megválasztásától. Tehát $\sigma \in N^{f''}(G)$. Azt kaptuk tehát, hogy $N^f(G) \subset N^{f''}(G)$. Hasonlóan adódik a másik irányú tartalmazás is, így valójában $N^f(G) = N^{f''}(G)$.

Tehát $H^f(G) = H^{f''}(G)$ és $N^f(G) = N^{f''}(G)$. Hasonlóan bizonyíthatóak a $H^{f'}(G) = H^{f''}(G)$ és $N^{f'}(G) = N^{f''}(G)$ egyenlőségek is, így $H^f(G) = H^{f'}(G)$ és $N^f(G) = N^{f'}(G)$. $\square$

A Γ_k csoport hat saján magán a balról (vagy jobbról) szorzással. Ez a hatás hű, így adódik egy természetes $\Gamma_k \hookrightarrow \mathrm{Sym}(\Gamma_k)$ beágyazás.

3.1.14. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)_0$ *egy zárt csoport, ami a szimmetrikus csoportként hat a* $\sim_{k_G}$*-ekvivalenciaosztályok halmazán, és* f *egy* k_G*-címkézés. Ekkor* $\Gamma_{k_G} \leq N(G)$.

Bizonyítás. Legyenek $u, v \in V^f, u \neq v$ tetszőlegesek. Legyen $\lambda \in \Gamma_{k_G}$ tetszőleges. Belátjuk, hogy $\lambda \in N(G)$.

Legyen f' az a címkézés, amire $f'(u') = f(u')$ minden $u' \not\sim_G u$ esetén, és $f'(u') = \lambda u'$ minden $u' \sim_G u$ esetén. Legyen továbbá $g \in \mathrm{Sym}((V \setminus 0)/\sim_{k_G})$ az a permutáció, ami kicseréli u és v ekvivalenciaosztályát. Ekkor $g^f g^{f'} \in G$ a 3.1.8. Állítás szerint. Nyilván $g^f g^{f'} \in \mathcal{S}^{(k(G))}$, így $g^f g^{f'} \in G^* = G \cap \mathcal{S}^{(k(G))}$ is teljesül. Azt állítjuk, hogy ekkor $\sigma(g^f g^{f'}, v) = \lambda$ és $\sigma(g^f g^{f'}, v') = \mathrm{id}\,\Gamma_{k_G}$ minden $v' \not\sim v$-re. Ezt elég bizonyítani, hiszen az $N(G)$ csoport definíciója szerint $\lambda \in N(G)$.

Tegyük fel, hogy $v' = \mu v$ valamilyen $\mu \in \Gamma_{k_G}$-re. Ekkor

$$v'^{g^f g^{f'}} = ((\mu v)^{g^f})^{g^{f'}} = (\mu u)^{g^{f'}} = \frac{f'(\mu u)}{f'(\mu v)} \mu v = \frac{\lambda \mu}{\mu} \mu v = \lambda \mu v.$$

Tegyük fel most, hogy $v' \not\sim v$. Ebből $v'^{g^f} \not\sim u$, és így $f(v'^{g^f g^{f'}}) = (f(v'^{g^f})^{g^{f'}} = (f(v'^{g^f})^{g^f} = f(v')$. Mivel $g^f g^{f'} \in G^*$, ezért $v'^{g^f g^{f'}} \sim_G v'$ is teljesül, így $v'^{g^f g^{f'}} = v'$, azaz $\sigma(g^f g^{f'}, v) = \mathrm{id}\,\Gamma_{k_G}$. $\square$

3.1.15. Definíció. *Legyen* f *egy tetszőleges* k*-címkézés valamilyen* $k|p-1$*-ra. Legyenek továbbá* $\Gamma_k \leq N \lhd H \leq \mathrm{Sym}(\Gamma_k)$ *tetszőleges csoportok.*

Ekkor legyen $G_f^*(N, H)$ *azon* $g \in \mathrm{Sym}_0(V)$ *elemek csoportja, stabilizál minden* $\sim_k$*-ekvivalenciaosztályt, a* $\sigma_f(g, v) : v \in V \setminus 0$ *elemek mind elemei* H*-nak, és a* H/N *faktorcsoportban megegyeznek.*

Legyen $G_f(N, H) := G_f^*(N, H)(\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$.

A 3.1.10 és 3.1.15 definíciókból könnyen látható, hogy ha $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}_0^{(k)}(V)$ egy csoport, és f egy k-címkézés, akkor $N(G_f(N, H)) = N$ és $H(G_f(N, H)) = H$. Ennek a megállapításnak egyszerű következménye, hogy a $G_f(N, H) \leq G_f(N', H')$ pontosan akkor teljesül, ha $N \leq N'$ és $H \leq H'$, továbbá hogy $G_f(N, H) = G_f(N', H')$ esetén $N = N'$ és $H = H'$ (azaz a $G_f(N, H)$ csoportok páronként különbözőek).

3.1.16. Lemma. *Legyen f egy tetszőleges k-címkézés valamilyen $k|p-1$-ra. Legyenek továbbá $\Gamma_k \le N \triangleleft H \le \mathrm{Sym}(\Gamma_k)$ tetszőleges csoportok. Ekkor $G_f(N,H)$ tartalmazza $\mathrm{Aut}(V)$-t, $k_{G(N,H)} = k$, és $G_f(N,H)$ a teljes szimmetrikus csoportként hat a $\sim_k$-ekvivalenciaosztályok halmazán.*

Bizonyítás. A lemmában felsorolt állításokból csak az nem triviális, hogy $\mathrm{Aut}(V) \le$ $\le G_f(N,H)$. Mivel $\Gamma_k \le N, H$, ezért $G_f(\Gamma_k,\Gamma_k) \le G_f(N,H)$, így elég belátni, hogy $\mathrm{Aut}(V) \le G_f(\Gamma_k,\Gamma_k)$. Legyen $\gamma \in \mathrm{Aut}(V)$ tetszőleges. Ekkor van olyan $g \in$ $\in \mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$, hogy $g' := \gamma g$ stabilizál minden $\sim_k$ ekvivalenciaoszályt. Mivel $\gamma \in \mathrm{Aut}(V)$, ezért $\sigma(g,u) \in \Gamma_k$ minden $u \setminus V \setminus 0$-ra. A g egy f-fel kompatibilis permutáció, így $\sigma(g,u) = \mathrm{id}\,\Gamma_k$. Ebből következik, hogy $\sigma(\gamma g,u) \in \Gamma_k$ minden $u \in$ $\in V \setminus 0$-ra. Ez definíció szerint éppen azt jelenti, hogy $g' = \gamma g \in G^*_f(\Gamma_k,\Gamma_k)$, amiből

$$\gamma = g'^{-1} g \in G^*_f(\Gamma_k,\Gamma_k)\,\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f = G_f(\Gamma_k,\Gamma_k).$$

Tehát valóban $\mathrm{Aut}(V) \le G_f(\Gamma_k,\Gamma_k)$. □

3.1.17. Tétel. *Legyen $\mathrm{Aut}(V) \le G \le \mathrm{Sym}(V)_0$ egy zárt csoport, ami a szimmetrikus csoportként hat a $\sim_{k_G}$-ekvivalenciaosztályok halmazán, és f egy k_G-címkézés. Ekkor vannak olyan $\Gamma_{k_G} \le N \triangleleft H \le \mathrm{Sym}(\Gamma_{k_G})$ csoportok, hogy $G = G_f(N,H)$.*

Bizonyítás. Azt állítjuk az $N := N(G)$ és $H := H(G)$ választás jó lesz. Ekkor a 3.1.12. és a 3.1.14. Lemmák szerint a $\Gamma_{k_G} \le N \triangleleft H \le \mathrm{Sym}(\Gamma_{k_G})$ tartalmazások teljesülnek. A 3.1.9. Következmény szerint $G = G^*(\mathrm{Sym}((V \setminus 0)/\sim_{k_G})^f$, így elég belátni, hogy $G^* = G^*_f(N,H)$.

Tegyük fel, hogy $g \in G^*$, és legyen v, w tetszőleges inekvivalens elemei $V \setminus 0$-nak. Ekkor $\sigma(g,v) \in H(G) = H$. Azt kell még belátni, hogy $\sigma(g,v)$ és $\sigma(g,w)$ képe megegyezik a H/N faktorcsoportban. Ehhez elég belátni, hogy $\sigma(g,v)\sigma(g,w)^{-1} \in$ $\in N$. Legyen most $t \in \mathrm{Sym}((V \setminus 0)/\sim_{k_G})$ az a transzpozíció, ami felcseréli v és w ekvivalenciaosztályát. Tekintsük ekkor a $h = gt^f g^{-1}(t^{-1})^f = gt^f g^{-1} t^f$ kommutátort. Ez minden $\sim_G$-ekvivalenciaosztály stabilizál, és

$$\sigma(h,v) = \sigma(g,v)\sigma(t^f,v)\sigma(g^{-1},w)\sigma(t^f,w) = \sigma(g,v)\sigma(g,w)^{-1},$$

továbbá minden $u \not\sim_G v, w$ esetén

$$\sigma(h,u) = \sigma(g,u)\sigma(t^f,u)\sigma(g^{-1},u)\sigma(t^f,u) = \mathrm{id}(\Gamma_{k_G}).$$

Legyen most v rögzített és $w_1, w_2, \ldots$ a $V \setminus 0$ halmaz elemeinek egy felsorolása.

Legyen ekkor minden i-re $t_i \in \mathrm{Sym}((V \setminus 0)/\sim_{k_G})$ az a transzpozíció, ami felcseréli w és w_i ekvivalenciaosztályát. Tekintsük ekkor a $h_i := t_i^f h (t_i^f)^{-1} = t_i^f h t_i^f$ permutációkat. Ekkor $h_i \in G^*$,

$$\sigma(h_i,v) = \sigma(t_i^f,v)\sigma(g,v)\sigma(g,w)^{-1}\sigma(t_i^f,v)^{-1} = \sigma(g,v)\sigma(g,w)^{-1},$$

és minden olyan u-ra, ami nem ekvivalens a v és w_i elemek egyikével sem

$$\sigma(h_i,u) = \sigma(t_i^f,u)\sigma(t_i^f,u^{t_i^f})\sigma(t_i^f,u^{t_i^f}) = \mathrm{id}(\Gamma_{k_G}).$$

Ekkor a $h_1, h_2, \dots$ sorozat konvergens, és ennek a h határértékére h stabilizál minden $\sim_G$-ekvivalenciaosztályt, $\sigma(h,v) = \sigma(g,v)\sigma(g,w)^{-1}$ és $\sigma(h,u) = \mathrm{id}(\Gamma_{k_G})$ minden $u \not\sim_G v$-re. Ebből következik, hogy $\sigma(g,v)\sigma(g,w)^{-1} \in N(H) := N$. Ezzel beláttuk, hogy $G^* \subset G^*_f(N,H)$.

Most belátjuk, hogy $G^*_f(N,H) \subset G^*$. Legyen U egy véges részhalmaza V-nek. Mivel G zárt, ezért az állításhoz elég belátni, hogy $G^*_f(N,H)|_U \subset G^*|_U$. A $G^*_f|_U$ hatást generálják a $g_{n,u} : n \in N, u \in U$ és a $g'(h) : h \in H$ elemek megszorításai U-ra, ahol a $g_{n,u}$ és $g'(h)$ elemek stabilizálnak minden $\sim_G$-ekvivalenciaosztályt, $\sigma(g'(h),v) = h$ minden $v \in U$-ra, $\sigma(g(n,v),v) = n$ és $\sigma(g(n,u),v) = \mathrm{id}(\Gamma_{k_G})$ minden $u \in U \setminus \sim_G(v)$-re. Az $N = N(G)$ csoport definíciójából következik, hogy a $g(n,u)|_U$ elemeket mind tartalmazza $G^*|_U$, így elég belátni, hogy tetszőleges $h \in$ $\in H$ esetén $g'(h)|_U \in G^*|_U$. A H csoport definíciója miatt van olyan $g_0 \in G^*$ elem, amire $\sigma(g_0,v) = h$ valamilyen $v \in V \setminus 0$-ra. Láttuk, hogy $G^* \subset G^*_f(N,H)$. Ebből következik, hogy minden $u \in V \setminus 0$ esetén $\sigma(g_0,u) = hn_u$ valamilyen $n_u \in N$-re. Legyen U' a V^f egy olyan véges halmaz, amire $\bigcup_{v \in V^f} \sim_G(v)$ lefedi U-t, és tekintsük a $g_1 = g_0 \prod_{u \in U'} g^{-1}(n_u,u)$ permutációt. A $g(n_u,u)$ transzformációk páronként felcserélhetőek, így az előbbi szorzatnál mindegy, hogy milyen sorrendben szorozzuk össze az elemeket. Ekkor tetszőleges $u \in U$ esetén

$$\sigma(g_1,u) = \sigma(g_0,u)\sigma(g^{-1}(n_u,u)) = hn_u n_u^{-1} = h = \sigma(g',u),$$

így $g_1|_U = g'(h)|_U$, és ezt kellett bizonyítanunk. □

3.1.18. Következmény. *Ha $\Gamma_k \leq N \lhd H \leq \mathrm{Sym}(\Gamma_k(G))$, akkor a $G_f(N,H)$ jelölés független az f címkézés megválasztásától.*

Bizonyítás. Legyen f és f' két tetszőleges k címkézés. Ekkor $H(G_f(N,H)) = H$ és $N(G_f(N,H)) = N$. Ekkor azonban a 3.1.17. Tételt alkalmazva a $G_f(N,H)$ csoportra és az f' címkézésre adódik, hogy $G_f(N,H) = G_{f'}(N,H)$. □

4. A vektortér 0-t nem fixáló reduktjai

Legyen V továbbra is egy megszámlálhatóan végtelen dimenziós vektortér $\mathbb{F}_p$ fölött, ahol $p \geq 3$ prím. Ebben a fejezetben belátjuk, hogy ha V automorfizmuscsoportjának egy zárt szupercsoportjának van olyan eleme, ami nem tartja a 0-t, akkor V vagy az affin transzformációk csoportja vagy a teljes szimmetrikus csoport. Ezen állítás bizonyításához használni fogjuk az előző fejezet eredményeit.

Jelölje $\mathrm{Aff}(V)$ az affin transzformációk csoportját V-ben. Egy $v \in V$ vektor esetén jelölje τ_v az $u \mapsto u + v$ eltolást V-n. Ekkor minden $g \in \mathrm{Aff}(V)$ egyértelműen felírható $g = g_0 \tau_u$ alakban, ahol $g_0 \in \mathrm{Aut}\, V$ és $u \in V$. Mivel $\mathrm{Aut}(\mathbb{F}_p)$ triviális, és $p \geq 3$, ezért az affin geometria alaptétele szerint egy $g \in \mathrm{Sym}(V)$ transzformáció pontosan akkor affin transzformáció, ha kollineáció, azaz g minden affin egyenest egyenesbe visz. Erre az észrevételre még szükségünk lesz a későbbiekben.

4.0.19. Lemma. *Ha* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *csoport, ami nem tartja a 0-t, akkor* G *tranzitívan hat* V*-n.*

Bizonyítás. $\mathrm{Aut}(V)$ tranzitívan hat $V \setminus 0$-n, ezért és G-nek van olyan eleme, ami a 0-t egy $V \setminus 0$-beli vektorba képezi. Ebből következik, hogy G tranzitív. □

A bizonyításhoz szükségünk lesz az alábbi jelölésre.

4.0.20. Definíció. *Legyen* G *egy csoport, ami hat* V*-n, és legyenek,* $a, b \in V$ *tetszőlegesek. Ekkor jelölje* $F_G(a, b)$ *az* $\{a, b\}$ *halmaz elemenkénti stabilizátorának véges orbitjainak unióját.*

Ez a jelölés a következő módon függ össze a 3. fejezetbeli „$\sim_G$” jelöléssel.

4.0.21. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy csoport. Ekkor* $b \in F_G(0, a)$ *pontosan akkor teljesül, ha* $b \sim_{G_0} a$ *vagy* $b = 0$*.*

Bizonyítás. $b = 0$ esetén az állítás triviális, tegyük fel most, hogy $b \neq 0$.

Tegyük fel először, hogy $b \sim_{G_0} a$. Ekkor definíció szerint minden $g \in G_0$ esetén $b^g \in \langle a^g \rangle$, így minden $b \in (G_0)_v$ esetén $b^g \in \langle a \rangle$. Ekkor mivel $\langle a \rangle$ véges, így b orbitja is véges. Tehát $b \in F_G(0, a)$.

Tegyük fel most, hogy $b \not\sim a$. Ekkor van olyan $g \in G_0$, hogy a^g, b^g lineárisan függetlenek. Legyen $h \in \mathrm{Aut}(V) \subset G_0$ egy olyan lineáris transzformáció, ami a^g-t a-be viszi. Ekkor $gh \in (G_0)_a$ és $b^{gh} \notin \langle a \rangle$. Ekkor a 3.0.8. Lemma szerint $(G_0)_a(b)$ végtelen, így $b \notin F_G(0, a)$. □

4.0.22. Következmény. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy csoport, ami nem tartja a 0-t. Ekkor tetszőleges* $u, v \in V$ *különböző vektorok esetén* $|F_G(u, v)| = k_{G_0} + 1$*.*

Bizonyítás. A 4.0.19. Lemma szerint G tranzitív, így az állítást elég belátni abban az esetben, amikor $u = 0$. A 4.0.21. Lemma szerint azonban ekkor $F(u, v) = F(0, v) = \{w \in V : w \neq 0, w \sim_{G_0} v\} \cup \{0\}$, speciálisan $F(0, v) = k_{G_0} + 1$. □

4.0.23. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy csoport, ami nem stabilizálja a 0-t. Ekkor tetszőleges* $a, b \in V, a \neq b$ *és* $u, v \in F_G(a, b), u \neq v$ *esetén* $F_G(u, v) = F_G(a, b)$*.*

Bizonyítás. A 4.0.19. Lemma szerint G tranzitív, így feltehető, hogy $a = 0$. A 4.0.21. Lemma szerint ekkor $c \in F(a, b)$ pontosan akkor teljesül, ha $c \sim_{G_0} b$. Tegyük fel most, hogy $u, v \in F_G(a, b), u \neq v$ és $w \notin F_G(a, b)$. Ekkor $u \sim_{G_0} b \sim_{G_0} v$ és $w \not\sim_{G_0} b \sim_{G_0} u$. Ebből következik, hogy létezik olyan $g \in G_0$, hogy w^g és u^g lineárisan függetlenek. A $\sim_{G_0}$ reláció definíciója miatt $v^g \in \langle u^g \rangle$, így $w^g \notin \langle u \rangle = \langle u^g, v^g \rangle$. Így a 3.0.8. Lemma szerint $(G_0)_{u^g, v^g}(w^g)$ végtelen. Ekkor $(G_0)_{u,v}(w)$ is végtelen, és így $G_{u,v}(w)$ is végtelen. Tehát $w \notin F_G(u, v)$. Beláttuk tehát, hogy $w \notin F_G(a, b)$ esetén $w \notin F_G(u, v)$. Ez azt jelenti, hogy $F_G(u, v) \subset F_G(a, b)$. A 4.0.22. Következmény szerint azonban $|F_G(a, b)| = |F_G(u, v)| = k_{G_0} + 1$, így $F_G(u, v) = F_G(a, b)$. □

4.0.24. Lemma. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy zárt csoport, ami nem fixálja a 0-t. Ekkor* $k_{G_0} = 1$ *vagy* $k_{G_0} = p - 1$.

Bizonyítás. Tegyük fel, hogy $1 < k_{G_0} < p - 1$. Ez azt jelenti, hogy létezik olyan $\lambda \in \mathbb{F}_p \setminus \{0,1\}$, hogy $\lambda v \not\sim_{G_0} v$. Ekkor a 4.0.21. Lemma szerint $\lambda v \notin F_G(0, v)$. Azt állítjuk, hogy ekkor $0 \notin F_G(v, \lambda v)$. Tegyük fel ugyanis, hogy $0 \in F_G(v, \lambda v)$. Ebből a 4.0.23. Lemma szerint $F(v, \lambda v) = F_G(0, v)$ következik, amiből $\lambda v \in F_G(0, v)$, ami nem lehet. Mivel $1 < k_{G_0}$, ezért a 4.0.22. Következmény szerint van olyan $u \in F_G(v, \lambda v)$, amire $u \neq v, \lambda v$. Az előbbiek szerint $u = 0$ nem lehetséges. Mivel $u \in F_G(v, \lambda v)$, ezért $G_{v,\lambda v}(u)$ véges, és így $(G_0)_{v,\lambda v}(u)$ is véges. Ekkor a 3.0.8. Lemma szerint $u \in \langle v, \lambda v\rangle = \langle v\rangle$. Azt kaptuk tehát, hogy létezik olyan $\mu \in \mathbb{F}_p \setminus \{0,1, \lambda\}$, hogy $\mu v = u \in F_G(v, \lambda v)$.

1. eset: $\mu v \not\sim_{G_0} v$ **és** $\mu v \not\sim_{G_0} \lambda v$**.** ♦ Ebben az esetben $v, \lambda v, \mu v$ páronként inekvivalens vektorok. A $G_0 = G \cap \mathrm{Sym}(V)_0$ csoport zárt, és tartalmazza $\mathrm{Aut}(V)$-t, így a 3.0.20. Tétel szerint G_0 3-tranzitían hat a $\sim_{G_0}$ ekvivalenciaosztályok halmazán. Speciálisan létezik olyan $g \in G_0$, amire a $v^g, (\lambda v)^g, (\mu v)^g$ vektorok lineárisan függetlenek. Ekkor a 3.0.8. Lemma szerint $(G_0)_{v^g,(\lambda v)^g}(\mu g)$ végtelen, és így $(G_0)_{v,\lambda v}(\mu v)$ is végtelen, ami ellentmond annak, hogy $\mu v \in F_G(v, \lambda v)$. Tehát $\mu v \sim_{G_0} v$ vagy $\mu v \sim_{G_0} \lambda v$.

2. eset: $\mu v \sim_{G_0} v$**.** ♦ Ekkor a 4.0.22. Következményt használva $\mu v \in F_G(v, \lambda v)$, amiből $\lambda v \in F_G(v, \mu v) = F_G(0, v)$, ami ellentmondás.

3. eset: $\mu v \sim_{G_0} \lambda v$**.** ♦ Ekkor megint a 4.0.22. Következményt használva $\mu v \in$ $\in F_G(v, \lambda v)$, amiből $v \in F_G(\lambda v, \mu v) = F_G(0, \lambda v)$ adódik, és így a 4.0.21. Lemma szerint $\lambda v \sim_{G_0} v$, ami ellentmondás.

Minden esetben ellentmondást kaptunk, tehát $k_{G_0} = 1$ vagy $k_{G_0} = p - 1$. □

A 4.0.22 és a 4.0.24. Lemmák szerint, ha egy $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ csoport nem fixálja a 0-t, akkor tetszőleges $u, v \in V, u \neq v$ elemek esetén $|F(u, v)| = 2$ vagy $|F(u, v)| = p + 1$. Az előbbi esetben nyilván $F(u, v) = \{u, v\}$. Belátjuk, hogy az utóbbi esetben $F(u, v) = L(u, v)$, az u, v vektorokat összekötő affin egyenes. Ehhez először szükségünk lesz az alábbi lemmára.

4.0.25. Lemma. *Legyen* U *egy 2 dimenziós vektortér* $\mathbb{F}_p$ *felett, és legyen* $H \subset$ $\subset U, |H| = p$ *egy olyan halmaz, amelynek elemei páronként lineárisan függetlenek, és kielégíti az alábbi feltételt:*

$$\textit{Tetszőleges } \lambda, \mu \in \mathbb{F}_p \textit{ és } u, v, u', v' \in H \textit{ esetén, ha } u \neq v, u' \neq v' \textit{ és } \lambda u + \mu v \in H, \textit{ akkor } \lambda u' + \mu v' \in H. \quad (4.0.1)$$

Ekkor H *egy affin egyenes* U*-ban.*

Bizonyítás. A bizonyításban jelöljük I-vel azon $(\lambda, \mu) \in \mathbb{F}_p^2$ párok halmazán, amire $\lambda u + \mu v \in H$ valamelyik (az összes) különböző elemekből álló $(u, v) \in H^2$ esetén. Könnyen látható, hogy ekkor $(\lambda, \mu) \in I$ pontosan akkor teljesül, ha $(\mu, \lambda) \in I$ teljesül.

1. állítás. Ha $(\lambda, \mu) \in I$**, ahol** $\lambda, \mu \neq 0$**, akkor** $(\mu + 1, -\mu) \in I$**.** ♦ Legyenek ugyanis $a, b \in H, a \neq b$ tetszőlegesek. Tekintsük most a következő összefüggést.

$$\frac{1}{\lambda}(\lambda a + \mu b) - \frac{\mu}{\lambda} b = a \in H.$$

Mivel $\mu \neq 0$, ezért $\lambda a + \mu b \neq b$, és így $(\frac{1}{\lambda}, -\frac{\mu}{\lambda}) \in I$. Hasonlóan $\frac{1}{\lambda}a - \frac{\mu}{\lambda}b \neq a$, hiszen $\mu \neq 0$. Ekkor mivel $(\lambda, \mu) \in H$, ezért

$$H \ni \lambda(\frac{1}{\lambda}a - \frac{\mu}{\lambda}b) + \mu a = (\mu + 1)a - \mu b.$$

Ebből következik, hogy $(\mu + 1, -\mu) \in I$.

Most belátjuk a lemma állítását. Legyenek megint $a, b \in H, a \neq b$ tetszőlegesek. Ha $p = 3$ és $-a - b \in H$, akkor készen vagyunk, hiszen ekkor csak $H = \{a, b, -a - b\} = L(a, b)$ lehetséges. Tegyük fel ezért, hogy $p > 3$, vagy $p = 3$ és $-a - b \notin H$. Mivel $|H| = p$, ezért mindkét esetben azt kapjuk, hogy van olyan $(\lambda, \mu) \in I$ pár, amire $\lambda \neq 0, \mu \neq 0$ és a λ, μ elemek valamelyike nem -1. Mivel $(\lambda, \mu) \in I$ pontosan akkor teljesül, ha $(\mu, \lambda) \in I$, ezért feltehető, hogy $\mu \neq -1$. Ekkor az előbbiek szerint $(\mu + 1, -\mu) \in I$.

Legyen most M azon ν-k halmaza, amire $(\nu + 1, -\nu) \in I$ teljesül. Ekkor $0, -1, \mu \in M$, és a feltételeink szerint $\mu \neq 0, -1$. Ha $(\nu + 1, -\nu b) \in I$ és $\nu \neq 0, -1$, akkor az 1. állítás szerint $(\nu + 2, -(\nu + 1)) \in I$. Ebből következik, hogy $\mu, \mu + 1, \ldots, p - 2 \in M$. Ha $(\nu + 1, -\nu) \in I$ és $\nu, \neq 0, -1$, akkor $(-\nu, 1 + \nu) \in I$, és ekkor az 1. állítás szerint $(-\nu + 1), \nu) \in I$ és így $(\nu, -(\nu - 1)) \in I$. Ebből következik, hogy $\mu, \mu - 1, \ldots, 2 \in M$. Ez azonban azt jelenti, hogy csak $M = \mathbb{F}_p$ lehetséges, és ekkor $I \supset \{(\nu + 1, -\nu) : \nu \in \mathbb{F}_p\}$, amiből

$$H \supset \{(\nu + 1)a - \nu b : \nu \in \mathbb{F}_p\} = L(a, b)$$

adódik. Az $L(a, b)$ egyenes számossága azonban p, így csak $H = L(a, b)$ lehetséges. □

4.0.26. Állítás. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy zárt csoport, ami nem fixálja a 0-t. Ekkor ha* $k_{G_0} = p - 1$*, akkor* $F_G(a, b) = L(a, b)$ *tetszőleges* $a, b \in V$ *különböző elemek esetén.*

Bizonyítás. Tegyük fel először, hogy $a, b \in V$ lineárisan összefüggenek. Ekkor ha $v \notin \langle a, b \rangle$, akkor a 3.0.8. Lemma szerint $(G_0)_{a,b}(v)$ végtelen, és így $G_{a,b}(v)$ is végtelen, amiből következik, hogy $v \notin F_G(a, b)$. Tehát $F_G(a, b) \subset \langle a, b \rangle$. Ha a, b lineárisan összefüggenek, akkor $|\langle a, b \rangle| = |L(a, b)| = p$. A 4.0.22. Következmény szerint a $F_G(a, b)$ halmaz is p elemű. Ez csak $F_G(a, b) = L(a, b)$ esetén lehetséges.

Tegyük fel most, hogy $a, b \in V$ lineárisan függetlenek. Legyen $U = \langle a, b\rangle$, ekkor $\dim U = 2$. Az előbbiekhez hasonlóan $v \notin \langle a, b\rangle$ esetén $v \notin F_G(a, b)$, így $F_G(a, b) \subset \subset U$. Belátjuk, hogy ekkor az U 2 dimenziós altérre, és a $H := F_G(a, b)$ halmazra teljesülnek a 4.0.25. Lemma feltételei. Ez elég, hiszen ekkor a 4.0.25. Lemma szerint $H = F_G(a, b)$ egyenes, és ekkor ez az egyenes csak $L(a, b)$ lehet, hiszen $a, b \in F_G(a, b)$.

A 4.0.22. Következmény szerint $|H| = |F_G(a, b)| = k_{G_0} + 1 = p$. Belátjuk most, hogy H nem tartalmaz két különböző lineárisan összefüggő vektort. Tegyük fel ugyanis, hogy $0 \neq u, \lambda u \in F(a, b)$, ahol $\lambda \neq 1$. Ekkor a 4.0.23. Lemma szerint $F(a, b) = F(u, \lambda u)$, ami lehetetlen, hiszen az állításnak a már bizonyított előző esete szerint $F(u, \lambda u) = \langle u\rangle$, és ekkor $F(u, \lambda u)$ nem tartalmazhatna két lineárisan független vektort. Be kell még látni a 4.0.25. Lemma (1) feltételét. Ehhez tegyük fel, hogy $u, v, u', v' \in H$ olyan vektorok, hogy $u \neq v$, $u' \neq v'$, és legyenek $\mu, \lambda \in \mathbb{F}_p$ olyan együtthatók, amelyekre $\lambda u + \mu v \in H$ teljesül. Be kell látnunk, hogy ekkor $\lambda u' + \mu v' \in H$. A 4.0.23. Lemma szerint $F(a, b) = F(u, v) = F(u', v')$, így ezen állításhoz elég belátni, hogy $G_{u',v'}(\lambda u' + \mu v')$ véges. Legyen most $g \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, amire $(u')^g = u$ és $(v')^g = v$. Ilyen létezik, hiszen az u, v és az u', v' is lineárisan független párok. Ekkor

$$|G_{u',v'}(\lambda u + \mu v)| = |G_{(u')^g,(v')^g}((\lambda u' + \mu v')^g)| = |G_{u,v}(\lambda u + \mu v)|,$$

ami véges, hiszen $\lambda u + \mu v \in H = F_G(a, b) = F_G(u, v)$. □

4.0.27. Tétel. *Legyen* $\mathrm{Aut}(V) \leq G \leq \mathrm{Sym}(V)$ *egy zárt csoport, ami nem fixálja a 0-t. Ekkor* $G = \mathrm{Aff}(V)$ *vagy* $G = \mathrm{Sym}(V)$.

Bizonyítás. A 4.0.24. Lemma szerint $k_{G_0} = 1$ vagy $k_{G_0} = p - 1$.

1. eset. $k_{G_0} = 1$ ♦ A $G_0 = G \cap \mathrm{Sym}_0(V)$ csoport zárt, így a 3.0.21 Következmény szerint $G_0 = \mathrm{Sym}_0(V)$. A 4.0.19. Lemma szerint azonban a G csoport tranzitívan hat V-n. Ez csak $G = \mathrm{Sym}(V)$ esetén lehetséges.

2. eset. $k_{G_0} = p - 1$ ♦ Ekkor először belátjuk, hogy $G \leq \mathrm{Aff}(V)$. Ehhez elég belátni, hogy G minden eleme kollineáció. Legyen tehát $g \in G$ és $L = L(a, b)$ egy tetszőleges affin egyenes V-ben. Ekkor a 4.0.26. Állítás szerint $L(a, b) = F_G(a, b)$. Az $F_G(a, b)$ halmaz definíciójából könnyen látható, hogy $(F_G(a, b))^g = F_G(a^g, b^g)$, így $(L(a, b))^g = F_G(a^g, b^g) = L(a^g, b^g)$. Tehát g valóban kollineáció. Tehát $G \leq \mathrm{Aff}(V)$.

Belátjuk most, hogy valójában $G = \mathrm{Aff}(V)$. Tegyük fel ugyanis, hogy $g \in G$ és g nem fixálja a 0-t. Ekkor $g = g_0 \tau_v$ alakú valamilyen $g_0 \in \mathrm{Aut}(V)$-re és $v \in \in V \setminus 0$-ra. Ekkor $g_0 \in \mathrm{Aut}(V) \subset G$ miatt $\tau_v \in G$ is teljesül. Belátjuk, hogy ekkor már G tartalmaz minden eltolást. Ez elég, hiszen az eltolások generálják $\mathrm{Aff}(V)$-t. Legyen tehát $w \in V \setminus 0$ tetszőleges. Legyen ekkor $h \in \mathrm{Aut}(V) \subset G$ egy olyan lineáris transzformáció, ami v-t w-be képezi. Ekkor tetszőleges $u \in V$ esetén

$$u^{h^{-1} \tau_v h} = (u^{h^{-1}} + v)^h = (u^{h^{-1}})^h + v^h = u + v^h = u + w = u^{\tau_w},$$

így $G \ni h^{-1} \tau_v h = \tau_w$. □

A 4.0.27. Tétel azonnali következménye a következő tétel.

4.0.28. Tétel. *Legyen $\mathfrak{A}$ a V struktúra egy reduktja, amiben a 0 nem definiálható. Ekkor $\mathfrak{A}$ vagy ekvivalens V-vel, mint egy megszámlálhatóan végtelen dimenziós affin térrel, vagy ekvivalens a megszámlálhatóan végtelen, struktúra nélküli halmazzal.*

Bizonyítás. Legyen $G := \mathrm{Aut}(\mathfrak{A})$. Legyen továbbá $\mathfrak{A}^0$ az a struktúra, amit $\mathfrak{A}$-ból kapunk úgy, hogy hozzávesszük a 0-t, mint konstanst. Mivel a 0 nem definiálható $\mathfrak{A}$-ban, ezért $\mathfrak{A}$ és $\mathfrak{A}^0$ nem ekvivalensek. Ekkor a 2.0.1. Tétel szerint

$$G = \mathrm{Aut}(\mathfrak{A}) \neq \mathrm{Aut}\,\mathfrak{A}^0 = G \cap \mathrm{Sym}(V)_0.$$

Speciálisan $G \nleq \mathrm{Sym}(V)_0$. A G csoport egy struktúra automorfizmuscsoportja, így zárt. Ekkor a 4.0.27. Tétel szerint $G = \mathrm{Aff}(V)$ vagy $G = \mathrm{Sym}(V)$, amiből szintén a 2.0.1. Tételt használva adódik a tétel állítása. $\square$

Hivatkozások

[1] Bhattachabya, P. (1981). On groups containing the projective special linear group. *Arch. Math.* 37:295-299.

[2] Bodirsky, M., Chen, H., Pinsker, M. (2010). The reducts of equality up to primitive positive interdefinability. *Journal of Symbolic Logic.* 75(4):1249-1292.

[3] Bodirsky, M., Pinsker, M. (2010). Minimal functions on the random graph. *Israel Journal of Mathematics.* to appear

[4] Bodirsky, M., Pinsker, M., Tsankov, T. Decidability of definability. *Journal of Symbolic Logic.* 78:1036-1054.

[5] Bodirsky, M., Pinsker, M. (2011). Reducts of Ramsey structures. *Model Theoretic Methods in Finite Combinatorics.* 558. Contemporary Mathematics. American Mathematical Society 489-519.

[6] Cameron, P. J. (1976). Transitivity of permutation groups on unordered sets. *Mathematische Zeitschrift.* 148:127-139.

[7] Hodges, W. (1993). *Model theory.* Cambridge University Press, Cambridge

[8] Junker, M., Ziegler, M. (2008). The 116 reducts of $(\mathbb{Q}; <; a)$. *Journal of Symbolic Logic.* 74(3):861-884.

[9] Kantor, W. M., McDonough, T. P., (1974). On the maximality of $\mathrm{PSL}(d + 1, q), d \geq 2$. *J. London Math. Soc. (2)* 8:426.

[10] Macpherson, D. (2011). A survey of homogeneous structures. *Discrete Mathematics.* 311(15):1599-1634.

[11] Pach, P. P., Pinsker, M., Pongrácz, A., Szabó, Cs. (2013). A new transformation of partially ordered sets. *J. Comb. Theory A.* 120(7):1450-1462.

[12] Pach, P. P., Pinsker, M., Pluhár, G., Pongrácz, A., Szabó, Cs. (2014). Reducts of the random partial order. *Advances in Mathematics* to appear

[13] Pogorelov, P. A. (1974). Maximal subgroups of symmetric groups that are defined on projective spaces over finite fields. (Russian) *Mat. Zametki.* 16:91-100.

[14] Pongrácz, A. (2013). Reducts of the Henson graphs with a constant. *Annals of Pure and Applied Logic.* to appear

[15] Thomas, S. (1991). Reducts of the random graph. *Journal of Symbolic Logic.* 56(1):176-181.

[16] Thomas, S. (1996). Reducts of random hypergraphs. *Annals of Pure and Applied Logic.* 80(2):165-193.