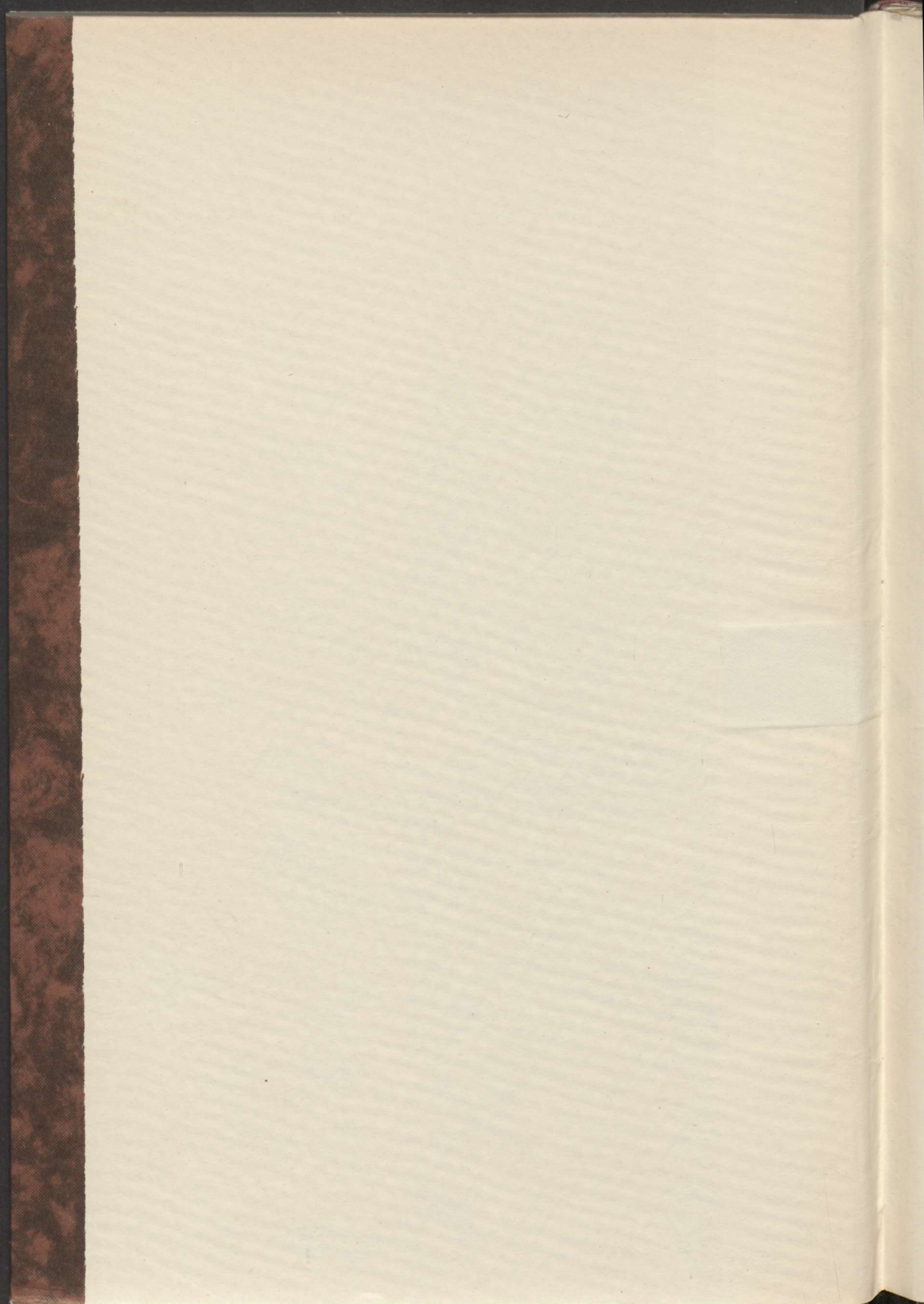
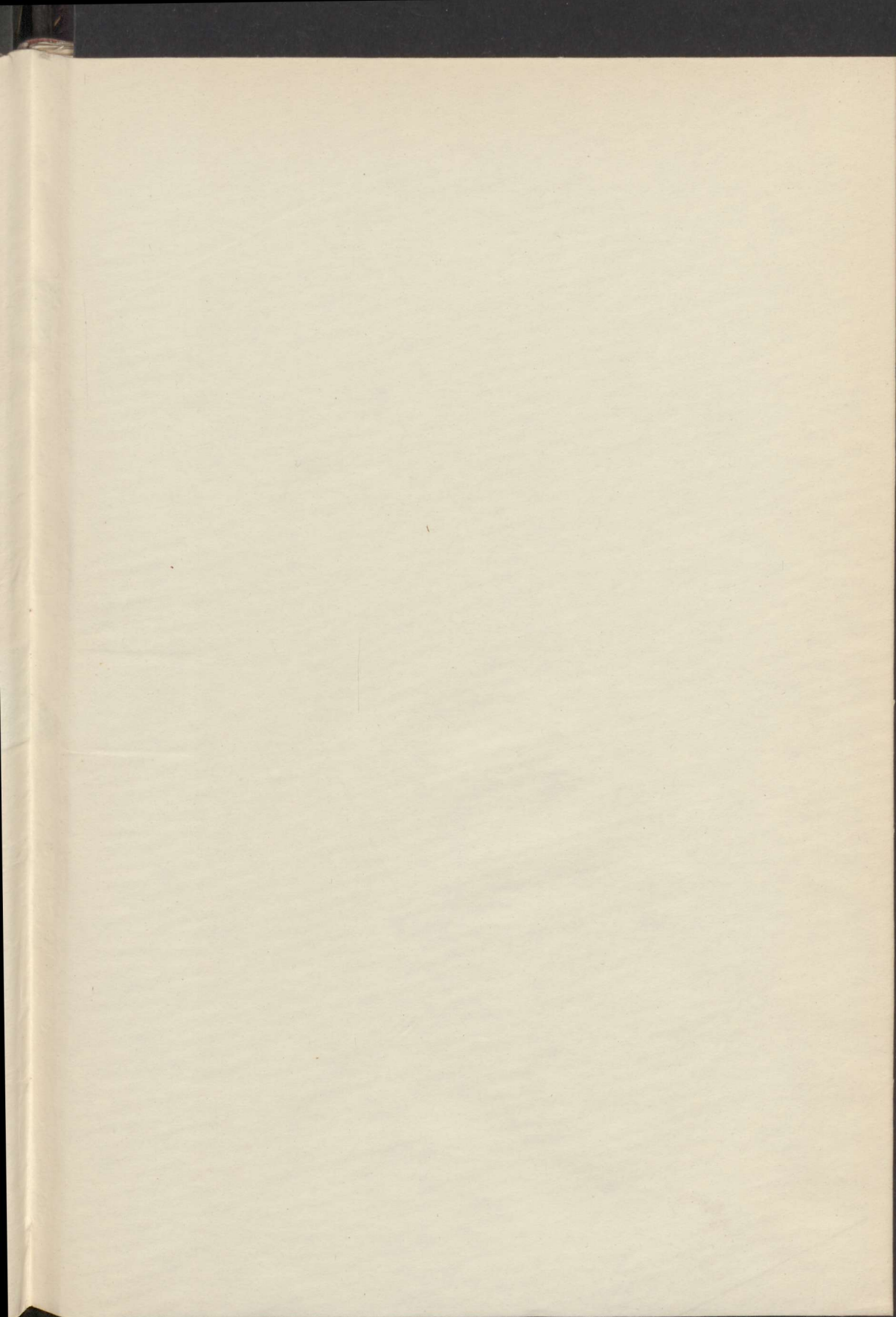
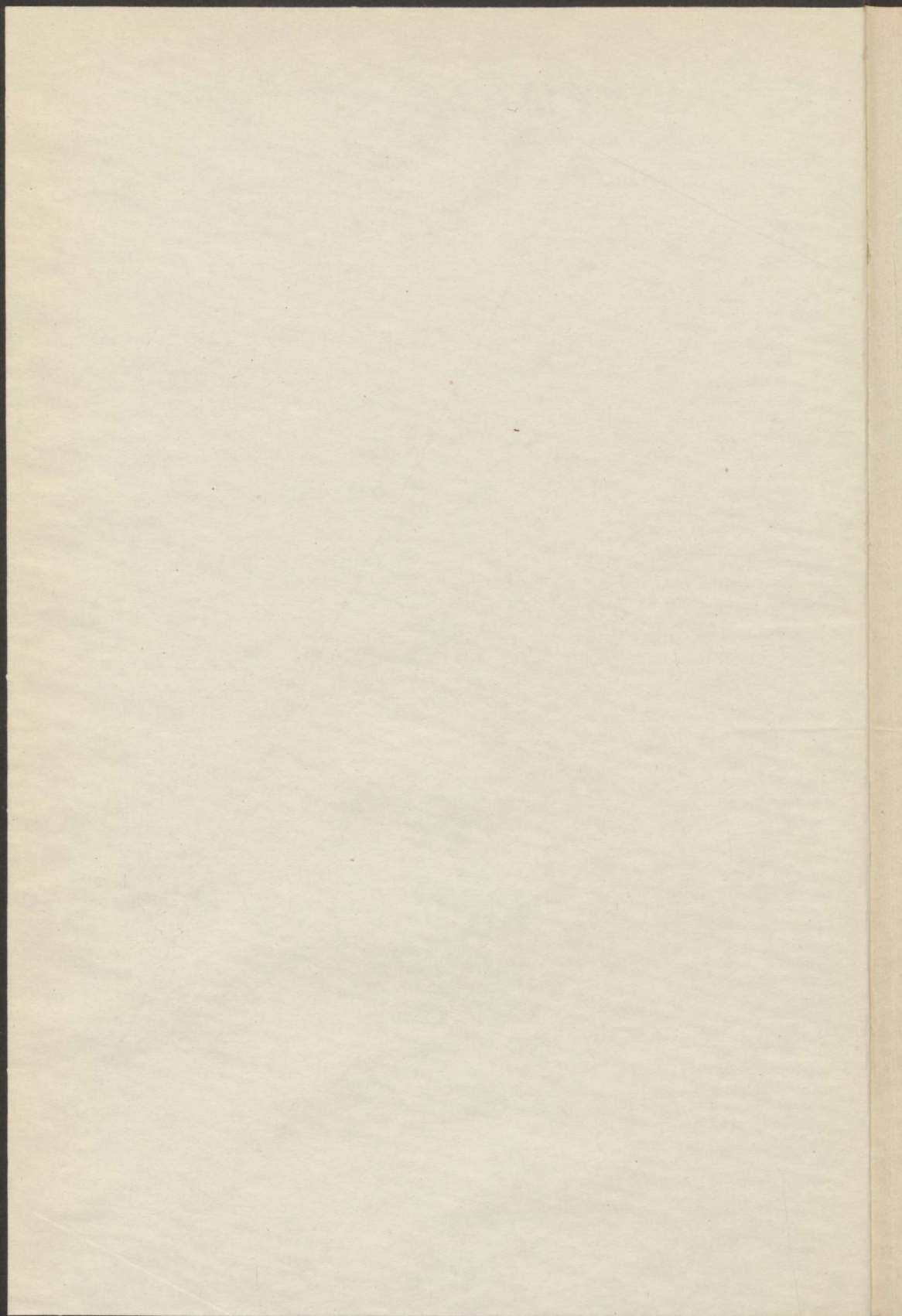


619.475







619.475

M. N. MŰZEM KÖNYVTÁRA
Nyamt. Nővödőknapi.

13 818

Acad.
750 a.

A LINEÁRIS CSOPORTOK ELMÉLETÉHEZ.

A matematikai kutatásokban a lineáris csoportoknak jutott fontos szerep teljesen indokolja azt az érdeklődést, melyet JORDAN-tól¹ kezdve DICKSON-ig² a matematikusok a lineáris csoportok elmélete iránt tanúsítottak. Habár ez az érdeklődés sok szép fejtegetésnek lett a kútforrásává, azért — úgy hiszem — azoknak gazdagítása a következő sorokkal épen nem válik fölöslegessé, a mennyiben az elmélet alapjainak megszilárdítása egy új módszerrel — az *elemi osztók* segítségével — csak javára válhatik azoknak a kutatásoknak, melyek ezen a téren folyamatban vannak.

1. Definíciók.

Az $X_{x_1 \dots x_n}$ határozatlanok száma, ha az *indexek* egymás től függetlenül egy (mod. m) teljes maradék-rendszer minden értékét fölveszik: m^n .

Az x_1, \dots, x_n minden szubsztitúciójának megfelel az $X_{x_1 \dots x_n}$ elemeknek egy, de csakis egy szubsztitúciója.

Ha az (x_1, \dots, x_n) halmaz m^n értékrendszerét (mod. m) a $[\varphi_1(x_1, \dots, x_n), \dots, \varphi_n(x_1, \dots, x_n)]$ halmaz is bizonyos sorrendben fölveszi, akkor az

$$s = \begin{pmatrix} x_1 & \dots & x_n \\ \varphi_1(x_1, \dots, x_n) & \dots & \varphi_n(x_1, \dots, x_n) \end{pmatrix} \pmod{m} \quad (1)$$

¹ JORDAN, Traité de substitutions et des équations algébriques, 1870.

² DICKSON, Linear groups with an exposition of the Galois field theory. 1901.

szubsztituczióval teljesen jellemeztük az $X_{x_1} \dots x_n$ elemek megfelelő szubsztituczióit.

Az s szubsztitucziót még így is szokás jelölni:

$$s = [x_1, \dots, x_n; \varphi_1(x_1, \dots, x_n), \dots, \varphi_n(x_1, \dots, x_n)] \pmod{m}. \quad (2)$$

Ha pedig kétértelműség nem forog fenn, akkor vagy az

$$s = \begin{pmatrix} x_i \\ \varphi_i(x_1, \dots, x_n) \end{pmatrix} \pmod{m}, \quad (1')$$

vagy pedig az

$$s = x'_i \equiv \varphi_i(x_1, \dots, x_n) \pmod{m} \quad (i=1, \dots, n) \quad (2')$$

szimbolumot használjuk.

Pl. Az

$$s(a) = x'_i \equiv x_i + a_i \pmod{m} \quad (i=1, \dots, n)$$

szubsztitucziók, ha az a -k egymástól függetlenül \pmod{m} minden értéket felvesznek egy m^n fokú, m^n rendű tranzitív ÁBEL-féle csoportot alkotnak.

Ha

$$s_i = \left. \begin{array}{l} x'_i \equiv x_i + 1 \\ x'_k \equiv x_k \\ i \neq k \end{array} \right\} \pmod{m},$$

akkor

$$s(a) = s_1^{\alpha_1} \dots s_n^{\alpha_n}$$

következőleg az $s(a)$ -k alkotta ÁBEL-féle csoport n -ed rangú; ezt a csoportot *aritmetikai csoportnak* nevezzük.

2. A lineáris csoport fogalma.

Határozzuk meg azt a legáltalánosabb csoportot, mely az aritmetikai csoportot invariánsul hagyja.

Legyen ennek a csoportnak egyik szubsztitucziója az előbbi fejezet (1) alatt levő szubsztitucziója s . Mivel $s^{-1}s_1s$ föltevésünk értelmében meg van az aritmetikai csoportban, azért

$$s^{-1} s_1 s = \begin{pmatrix} \varphi_i(x_1, x_2, \dots, x_n) \\ \varphi_i(x_1, +1, x_2, \dots, x_n) \end{pmatrix} = \\ = \begin{pmatrix} \varphi_i(x_1, \dots, x_n) \\ \varphi_i(x_1, \dots, x_n) + a_{i1} \end{pmatrix} \pmod{m},$$

következően

$$\varphi_i(x_1 + 1, x_2, \dots, x_n) = \varphi_i(x_1, \dots, x_n) + a_{i1},$$

épen így

$$\begin{aligned} \varphi_i(x_1, x_2 + 1, \dots, x_n) &= \varphi_i(x_1, \dots, x_n) + a_{i2}, \\ &\vdots \\ \varphi_i(x_1, x_2, \dots, x_n + 1) &= \varphi_i(x_1, \dots, x_n) + a_{in}. \end{aligned}$$

Ezekből a redukziós képletekből, ha a $\varphi_i(0, \dots, 0)$ konstanst a_i -vel jelöljük, $\varphi_i(x_1, \dots, x_n)$ számára a következő analitikai alakot nyerjük:

$$\varphi_i(x_1, \dots, x_n) = a_i + a_{i1}x_1 + \dots + a_{in}x_n.$$

Ennélfogva az aritmetikai csoportot az összes

$$s = x'_i \equiv a_i + a_{i1}x_1 + \dots + a_{in}x_n \pmod{m} \\ (i = 1, \dots, n)$$

szubsztitucziók invariánsul hagyják. Miként könnyű belátni, ezek a szubsztitucziók egy m^n fokú csoportot alkotnak, melyet *lineáris csoportnak* nevezünk.

Az

$$s s^{-1}(a) = x'_i = a_{i1}x_1 + \dots + a_{in}x_n \pmod{m} \\ (i = 1, \dots, n)$$

szubsztitucziók a lineáris csoport egyik alcsoportját képezik, melyet *homogén lineáris csoportnak* nevezünk. Ennélfogva:

Az a *maximális csoport*, mely az aritmetikai csoportot invariánsul hagyja, a *lineáris csoport*; az a *maximális*, az aritmetikai csoporton kívül álló csoport pedig, mely az aritmetikai csoportot invariánsul hagyja, a *homogén lineáris csoport*.

3. A homogén lineáris csoport elemi szubsztituciói.

Az

$$\left. \begin{aligned} s(i, 1) &= x'_i \equiv x_i + x_1, & x'_k &\equiv x_k \\ s(1, i) &= x'_1 \equiv x_1 + x_i, & x'_k &\equiv x_k \end{aligned} \right\} \pmod{m} \quad (i \neq 1)$$

szubsztituciókat a homogén lineáris csoport elemi szubsztitucióinak nevezzük.

Könnyű belátni, hogy

$$\left. \begin{aligned} s^{-1}(i, 1) &= x'_i \equiv x_i - x_1, & x'_k &\equiv x_k \\ s^{-1}(1, i) &= x'_1 \equiv x_1 - x_i, & x'_k &\equiv x_k \end{aligned} \right\} \pmod{m} \quad (i \neq 1)$$

$$s^{-1}(i, 1), s(1, k) s(i, 1) s^{-1}(1, k) = s(i, k) = \left. \begin{aligned} x'_i &\equiv x_i + x_k, & x'_l &\equiv x_l \end{aligned} \right\} \pmod{m} \quad (i \neq k)$$

$$s^a(i, k) = x'_i \equiv x_i + ax_k, \quad x'_l \equiv x_l \pmod{m} \quad (i \neq k)$$

bármily pozitív, vagy negatív egész szám legyen is a .

4. Az elemi szubsztituciókkal való szorzás szabályai.

Ha s_a -nak, illetőleg s_b -nek nevezzük azokat a szubsztituciókat, melyeknek matrixai rendre:

$$\begin{aligned} a &= \| a_{i1} \cdots a_{in} \|, \\ b &= \| b_{i1} \cdots b_{in} \|, \\ &\quad (i=1, \dots, n) \end{aligned}$$

akkor a szubsztituciók szorzási szabálya szerint:

$$s_a s_b = s_c,$$

ha

$$c = \| c_{i1} \cdots c_{in} \|, \quad (i=1, \dots, n)$$

$$c_{ik} = b_{i1}a_{1k} + b_{in}a_{nk}.$$

1. Pl. Az

$$s_a s(1, i) = s_c$$

szubsztitució matrixa

$$\begin{vmatrix} c_{1k} \\ c_{2k} \\ \vdots \\ c_{nk} \end{vmatrix} = \begin{vmatrix} a_{1k} + a_{ik} \\ a_{2k} \\ \vdots \\ a_{nk} \end{vmatrix}$$

2. Pl. Az

$$s(1, i) s_a = s_c$$

szubsztitució matrixa

$$\begin{aligned} & \begin{vmatrix} c_{k1} \dots c_{ki-1} c_{ki} c_{ki+1} \dots c_{kn} \end{vmatrix} = \\ & = \begin{vmatrix} a_{k1} \dots a_{ki-1} a_{ki} + a_{i1} a_{ki+1} \dots a_{kn} \end{vmatrix}. \end{aligned}$$

Általában az $s_a s(i, k)$ matrixát az a -ból úgy nyerjük, ha az i -edik sorhoz hozzáadjuk a k -adikat: az $s(i, k) s_a$ matrixát pedig az a -ból úgy kapjuk, ha a k -adik oszlopához hozzáadjuk az i -ediket.

Ha tehát az a matrix egyik sorának illetőleg oszlopának ε -szorosát hozzáadjuk egy másik sor-, illetőleg oszlophoz, akkor nem teszünk mást, mint s_a -t szorozzuk jobbról-, illetőleg balról egy elemi szubsztitució ε -adik hatványával.

5. A homogen lineáris csoport szubsztitucióinak redukciója.

Az előbbi fejezet fejtegetései szerint elemi szubsztituciókkal szorzunk, midőn az a matrixszal a következő műveleteket végezzük:

1. Ha a_{ik} az a matrix abszolút értékére nézve legkisebb — mindig zérustól különbözőt értve — eleme, akkor az i -edik sor megfelelő többszörösének a többi sorhoz való hozzáadásával elérhetjük, hogy az így transzformált matrix k -adik oszlopában a_{ik} -nál abszolút értékre nézve csak kisebb elemek forduljanak elő.

2. Megfelelő művelettel elérhetjük, hogy a matrix i -edik sorának elemei is abszolút értékre nézve kisebbek legyenek a_{ik} -nál.

3. Az így transzformált matrixra alkalmazzuk újból az imént

leírt műveletet s ezt folytassuk addig, míg egy oly matrixhoz nem jutunk, melynek abszolút értékre nézve legkisebb elemének sorában és oszlopában minden más elem zérus.

4. Ha valamelyik sorban van olyan elem, melyben a legkisebb elem nem foglaltatik maradék nélkül, akkor ezt a sort adjuk a legkisebb elem sorához s azután kezdjük ismét előről leírtuk a műveletet.

5. Ha végre eljutunk egy oly matrixhoz, melynek abszolút értékre nézve legkisebb elemének sorában és oszlopában minden más elem zérus és ez a legkisebb elem a matrix minden más elemében maradék nélkül foglaltatik, akkor a legkisebb elem sorát adjuk a matrix legelső sorához s aztán oszlopának annyiszorosát adjuk az első oszlophoz; hogy ezáltal az első elem pozitív legyen s egyenlő legyen az abszolút értékre nézve legkisebb elem abszolút értékével.

6. Miután az 1. és 2. pontban leírt eljárással az első sor- és oszlopnak is minden elemét, a legelsőt leszámítva, zérussá tettük, matrixunk így alakú lesz:

$$\begin{vmatrix} e_1 & 0 & \dots & 0 \\ 0 & a'_{22} & \dots & a'_{1n} \\ \vdots & \vdots & \dots & \vdots \\ 0 & a'_{n2} & \dots & a'_{nn} \end{vmatrix}$$

Ha már most a leírtuk műveletet alkalmazzuk az

$$\| a'_{i2} \dots a'_{in} \| \quad (i=2, \dots, n)$$

matrixra, akkor világos, hogy műveletsorozatuk végén matrixunk ilyen alakúvá lesz:

$$e = \begin{vmatrix} e_1 & 0 & \dots & 0 \\ 0 & e_2 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & e_n \end{vmatrix}$$

Ennélfogva az elemi szubsztitucziókból elő tudunk állítani oly szorzatokat σ_1 -t és σ_2 -t, melyekre nézve

$$\sigma_1 s_a \sigma_2 = s_e = x_i \equiv e_i x_i \pmod{m}.$$

(i=1, \dots, n)

De $e_i x_i \pmod{m}$ minden értéket csak úgy vehet fel, ha

$$(e_i, m) = 1.$$

Ennélfogva s_a csak úgy lehet valóságos szubsztitució, ha a elemi osztói m -hez viszonylagos törzsszámok, azaz ha

$$(e_1 \dots e_n, m) = 1.$$

Ha a matrix determinánsát röviden $|a|$ -val jelöljük, akkor világos, hogy

$$|a||b| = |c|.$$

Következőleg

$$|a| = |e|.$$

Főntebbi tételünket tehát így is fogalmazhatjuk:

s_a csak úgy lehet valóságos szubsztitució, ha determinansa $|a|$ és m viszonylagos törzsszámok.

6. Az s_e szubsztitucziók transzformálása.

Legyenek $y_1, y_2, y_3, y_4 \pmod{m}$ még egyelőre határozatlan számok. Könnyű meggyőződni, hogy az

$$s_e s^{y_1} (1, 2) s^{y_2} (2, 1) s^{y_3} (1, 2) s^{y_4} (2, 1)$$

szubsztituczió megegyezik a következővel:

$$x'_1 \equiv e_1 (1 + y_2 y_3) x_1 + e_2 [y_1 (1 + y_2 y_3) + y_3] x_2$$

$$x'_2 \equiv e_1 [y_4 (1 + y_2 y_3) + y_2] x_1 + e_2 \{y_4 [y_1 (1 + y_2 y_3) + y_3] + 1 + y_1 y_2\} x_2$$

$$x'_i \equiv e_i x_i$$

Ha már most azt az

$$s^{y_1} (1, 2) s^{y_2} (2, 1) s^{y_3} (1, 2) s^{y_4} (2, 1)$$

szubsztitucziót, melyet az

$$y_2 y_3 \equiv e_2 - 1$$

$$y_3 \equiv -e_2 y_1 \pmod{m}$$

$$y_2 \equiv -e_2 y_4$$

feltételeknek megfelelően konstruálunk $s(1, 2; e_2)$ -nek nevezzük, akkor

$$s_e s(1, 2; e_2) = x'_1 \equiv e_1 e_2 x_1$$

$$x'_2 \equiv x_2$$

$$x'_i \equiv e_i x_i,$$

tehát

$$s_e s(1, 2; e_2) s(1, 3; e_3) \dots s(1, n; e_n) = x'_1 \equiv e_1 \dots e_n x_1$$

$$x'_i \equiv x_i.$$

Ha tehát az s_a szubsztitució determinansát d -nek nevezzük, akkor:

Mindig elő tudunk állítani az elemi szubsztituciókból oly σ' és σ'' szorzatokat, melyekre nézve:

$$\sigma' s_a \sigma'' = x'_1 \equiv dx_1, x'_i \equiv x_i \pmod{m}.$$

Ha

$$d \equiv 1 \pmod{m},$$

akkor

$$s_a = \sigma'^{-1} \sigma''^{-2} = \sigma,$$

azaz: minden \pmod{m} egységdeterminansú szubsztitució előállítható, mint az elemi szubsztituciók szorzata.

Ha s_a egy tetszőleges oly szubsztitució, melynek determinansa d és

$$s = x'_1 = dx_1, x'_i = x_i \pmod{m},$$

akkor ss_a^{-1} determinansa 1, tehát

$$ss_a^{-1} = \sigma$$

$$s = \sigma s_a$$

tehát minden s_a szubsztitucióhoz meghatározható oly elemi szubsztituciókból előállított szorzat σ , melyre nézve

$$\sigma s_a = x'_1 \equiv dx_1, x'_i \equiv x_i,$$

vagy

$$s_a \sigma = x''_1 \equiv dx_1, x'_i \equiv x_i.$$

7. A homogen lineáris csoport konstrukciója.

Ha az

$$x^{q(m)} \equiv 1 \pmod{m}$$

kongruenciának egyik primitív gyöke d , és

$$s = x'_1 \equiv dx_1, x'_i \equiv x_i,$$

akkor minden s_a substituációhoz meghatározhatunk oly α számot, melyre nézve

$$s_a s^{-\alpha} = \sigma,$$

hol σ -nak az előbbi fejezetben megállapított jelentése van, következőleg:

$$s_a = \sigma s^\alpha.$$

Ha tehát a homogen lineáris csoportot G -vel jelöljük, akkor

$$G = \{s(1, i), s(i, 1); s\}.$$

Mivel $s^{-1}s(i, k)s \pmod{m}$ egységdeterminansú substituáció, azért a

$$\Gamma = \{s(1, i), s(i, 1)\}$$

csoport G -nek invariants alcsoportja, tehát

$$\begin{aligned} G &= \Gamma, \Gamma s, \dots, \Gamma s^{q(m)-1} \\ &= \Gamma, s\Gamma, \dots, s^{q(m)-1}\Gamma. \end{aligned}$$

8. A homogen lineáris csoport rendszáma.

Ha G -nek azt az alcsoportját, mely x_1 -et invariantsul hagyja, G_1 -nek nevezzük, akkor

$$G = G_1, G_1 g_2, \dots, G_1 g_r.$$

A g -k x_1 különbözőképpen transzformálják, mert ha g_i és g_k egyformán transzformálná, akkor $g_i g_k^{-1}$ invariantsul hagyná; de ekkor $g_i g_k^{-1}$ tagja lenne G_1 -nek, tehát g_i a $G_1 g_k$ halmazban is előfordulna, a mi nem lehetséges.

Ha a_{11}, \dots, a_{1n} relativ törzsszám m -hez, azaz

$$(a_{11}, \dots, a_{1n}, m) = 1,$$

akkor van oly szubsztituczió, mely az x_1 -et $a_{11}x_1 + \dots + a_{1n}x_n$ -be transzformálja.

Már most ha $\varphi(m, n)$ -nel jelöljük azt a számot, mely megmondja, hogy az $0, 1, \dots, m-1$ számok közül hányféleképen választhatunk ki oly (a_{11}, \dots, a_{1n}) halmazokat, melyekre nézve

$$(a_{11}, \dots, a_{1n}, m) = 1,$$

akkor

$$\nu = \varphi(m, n).$$

Legyen

$$m = p_1^{a_1} \dots p_r^{a_r}$$

mivel a $0, 1, 1, \dots, m-1$ számokból kiválasztható m^n különböző (a_{11}, \dots, a_{1n}) halmaz között

$$\left(\frac{m}{p_1 \dots p_r}\right)^n$$

olyan fordul elő, melyek mindegyikének tagjai oszthatók $p_1 \dots p_r$ -rel, melyeket röviden $p_1 \dots p_r$ -rel osztható halmaznak mondunk

s mivel a $\sum \left(\frac{m}{p_1}\right)^n$ halmaz között a $p_1 \dots p_r$ -rel oszthatók mindegyike $\binom{r}{1}$ -szer fordul elő, a $\sum \left(\frac{m}{p_1 p_2}\right)^n$ halmazsokaságban minden $p_1 \dots p_r$ -rel osztható halmaz $\binom{r}{2}$ -ször fordul elő stb., azért az

$$\binom{r}{1} - \binom{r}{2} + \dots + (-1)^{r-1} \binom{r}{r} = 1$$

képlet figyelembe vételével könnyű belátni, hogy

$$\varphi(m, n) = m^n - \sum \left(\frac{m}{p_1}\right)^n + \sum \left(\frac{m}{p_1 p_2}\right)^n \dots = m^n \prod_{i=1}^r \left(1 - \frac{1}{p_i^n}\right).$$

Mivel G rendszáma, melyet $R(m, n)$ -nel jelölünk, ν -nek és

G_1 rendszámának a szorzata, azért még ez utóbbit kell meghatároznunk.

G_1 bármely szubsztitucziója ily alakú:

$$x'_1 \equiv x_1, x'_i \equiv a_{i1}x_1 + \dots + a_{in}x_n \pmod{m}, \quad (i=2, \dots, n)$$

hol a $(\text{mod. } m)$ tetszőleges (a_{21}, \dots, a_{n1}) halmazok száma m^{n-1} , az

$$(|a_{ik}|, m) = 1 \quad (i, k=2, \dots, n)$$

föltételt kielégítő

$$\|a_{i2}, \dots, a_{in}\| \quad (i=2, \dots, n)$$

matrixok száma pedig $R(m, n-1)$; következésképp G_1 rendszáma $m^{n-1}R(m, n-1)$, ennél fogva:

a homogen lineáris csoportunk rendszáma

$$R(m, n) = m^{n-1} \varphi(m, n) R(m, n-1),$$

hol

$$R(m, 1) = \varphi(m, 1) = \varphi(m).$$

Ezt a tételt ily általánosságban először JORDAN¹ mutatta ki.

Az $m=p$ -re vonatkozó s GALOIS által fölfedezett

$$R(p, n) = p^{\frac{n(n-1)}{2}} \prod_{r=1}^n (p^r - 1)$$

tételt először BETTI igazolja.

Mivel m és n a csoportra nézve jellemző számok, azért ezután a homogen lineáris csoportot rendszáma után $R(m, n)$ csoportnak fogjuk nevezni.

9. A kompozíció sor képzési módja.

Ha p_1, \dots, p_r törzsszámok és

$$m_1 = p_1^{a_1}, m_2 = p_2^{a_2} \dots p_r^{a_r}.$$

$$m = m_1 m_2,$$

¹ JORDAN, Traité p. 95.

akkor, ha az $R(m, n)$ csoport minden szubsztitucziójához

$$s = x'_1 \equiv a_{i1}x_1 + \dots + a_{in}x_n \pmod{m}$$

mellé rendelünk egy

$$\sigma = x'_1 \equiv a_{i1}x_1 + \dots + a_{in}x_n \pmod{m_1}$$

szubsztitucziót, akkor világos, hogy a σ -k oly $R(m_1, n)$ csoportot alkotnak, mely $R(m, n)$ -nel izomorfizmusban van, $R(m_1, n)$ csoport egységének $R(m, n)$ -ben megfelelnek az

$$s_1 = x'_i \equiv x_i + m_1(a_{i1}x_1 + \dots + a_{in}x_n) \pmod{m}$$

szubsztitucziók, melyek $R(m, n)$ -nek egyik invariants alcsoportját alkotják.

Mivel az

$$1 = \nu m_1 + \mu m_2$$

relációnál fogva

$$s_1 = x'_i = \mu m_2 x_i + m_1(a_{i1}x_1 + \dots + (a_{ii} + \nu)x_i + \dots + a_{in}x_n) \pmod{m},$$

azért s_1 determinansa akkor s csakis akkor relativ törzsszám m -hez, ha

$$\left(\begin{vmatrix} a_{11} + \nu \dots a_{1n} \\ \vdots \\ a_{n1} & \dots & a_{nn} + \nu \end{vmatrix}, m_2 \right) = 1.$$

Ennélfogva az s_1 szubsztitucziók csoportja egyszerű izomorfizmusban van egy oly $R(m_2, n)$ csoporttal, melynek szubsztitucziói

$$s_2 = x'_1 \equiv a_{i1}x_1 + \dots + (a_{ii} + \nu)x_i + \dots + a_{in}x_n \pmod{m_2}$$

Ha már most a fönntebbi $R(m_1, n)$ csoport kompozíció sora

$$\Gamma, \Gamma_1, \dots, \Gamma_i,$$

kompozíció-tényezői pedig $\gamma_1, \dots, \gamma_i$, akkor ezeknek a Γ -áknak $R(m, n)$ -ban megfelel a

$$G, G_1, \dots, G_i$$

sor, mely nem más, mint az $R(m, n)$ kompozíció-sorának G_i -ig terjedő része, a melynek kompozíció-tényezői szintén $\gamma_1, \dots, \gamma_i$ és a melyben G_i egyszerű izomorfizmusban van az imént fölirt $R(m_2, n)$ csoporttal, melynek fölbontására ugyanazt a szabályt kell alkalmaznunk, mint a melyet most alkalmaztunk, az $R(m, n)$ csoport felbontására.

Az $R(m, n)$ csoport felbontása tehát visszavezethető $R(p^\alpha, n)$ felbontására.

10. Az $\mathcal{R}(p^\alpha, n)$ csoport fölbontása.

Az előbbi fejezet fejtegetéseivel hasonlóan az $R(p^\alpha, n)$ csoport minden szubsztitúciójához

$$s = x'_i \equiv a_{i1}x_1 + \dots + a_{in} \pmod{p^\alpha}$$

rendeljünk egy

$$\sigma = x'_i \equiv a_{i1}x_1 + \dots + a_{in}x_n \pmod{p}$$

szubsztitúciót ezek egy oly $R(p, n)$ csoportot alkotnak, mely az adottal

$$\frac{R(p^\alpha, n)}{R(p, n)} = p^{(\alpha-1)n^2}$$

rendű izomorfizmusban van.

Ha az $R(p, n)$ csoport kompozíció-sorának $R(p^\alpha, n)$ -ben megfelel a

$$G, G_1, \dots, G_k$$

sorozat, akkor G_k rendszáma: $p^{(\alpha-1)n^2}$; ennél fogva G_k már feloldható csoport.

Az $R(p^\alpha, n)$ csoport felbontása tehát visszavezethető az $R(p, n)$ csoport felbontására.

11. Az $\mathcal{R}(p, n)$ csoport fölbontása.

Ha csoportunkat röviden G -nek —, a $(\text{mod. } p)$ egységdeterminansú szubsztitúcióiból alkotott invariants alcsoportját Γ -nak nevezzük, akkor a 7. fejezet fejtegetései értelmében

$$G = \Gamma, \Gamma s, \dots, \Gamma s^{p-2},$$

hol

$$s = x'_1 \equiv dx_1, \quad x'_i \equiv x_i \pmod{p},$$

d pedig az

$$x^{p-1} \equiv 1 \pmod{p}$$

kongruenciának egyik primitív gyöke.

Γ -ra vonatkozólag kimutatjuk a következő tételeket:

1. Ha γ Γ -nak oly szubsztituciója, melyet Γ invariantsul hagy, akkor γ ily alakú:

$$\gamma = x'_i \equiv g_{ii} x_i \pmod{p}.$$

Legyen ugyanis

$$\gamma = x'_i \equiv g_{i1} x_1 + \dots + g_{in} x_n,$$

a Γ egy tetszőleges szubsztituciója pedig

$$s = x'_i = a_{i1} x_1 + \dots + a_{in} x_n.$$

Föltevésünk értelmében

$$s\gamma = \gamma s,$$

azaz

$$g_{ii} a_{1k} + \dots + g_{in} a_{nk} = a_{i1} g_{1k} + \dots + a_{in} g_{nk}.$$

Így ha

$$s = s(i, k),$$

akkor

$$g_{ii} = g_{kk}, \quad g_{ri} = 0, \quad g_{ks} = 0, \quad r \neq i, k \neq s$$

a mi már tételünket igazolja.

Határozzuk meg most g értékét. Minthogy γ determinansa $(\text{mod. } p)$ egy, azért

$$g^n \equiv 1 \pmod{p}.$$

Ha tehát az

$$x^{p-1} \equiv 1 \pmod{p}$$

kongruencia egyik primitív gyöke a és

$$g = a^x,$$

akkor

$$a^{nx} \equiv 1 \pmod{p},$$

tehát

$$nx \equiv 0 \pmod{p-1},$$

honnan, ha n és $p-1$ legnagyobb közös osztóját d -vel jelöljük,

$$x = \frac{p-1}{d} \nu, \quad (\nu=0, 1, \dots, d-1)$$

ennélfogva:

2. Γ -nak azon szubsztitucziói, melyeket Γ invariánsul hagy egy d -ed rendű

$$\Gamma_1 = (1, \gamma, \dots, \gamma^{d-1})$$

invariáns csoportot alkotnak, hol

$$d = (n, p-1)$$

$$\gamma = x'_i \equiv a^{\frac{p-1}{d}} x_i \pmod{p}$$

és a az

$$x^{p-1} \equiv 1 \pmod{p}$$

egyik primitív gyöke.

3. Ha Γ valamelyik invariáns alcsoportja az elemi szubsztitucziók egyikét tartalmazza, akkor az összeesik Γ -val.

Az általánosság rovása nélkül feltételezhetjük, hogy egy ily invariáns alcsoport H tartalmazza az $s(1, 2)$ elemi szubsztitucziót. Mivel

$$s_1 = x'_1 \equiv -x_i, \quad x'_i \equiv x_1, \quad x'_r \equiv x_r,$$

$$s_2 = x'_2 \equiv -x_k, \quad x'_k \equiv x_2, \quad x'_r \equiv x_r$$

egységssubsztitucziók, azért H tartalmazza az

$$s_1^{-1} s(1, 2) s_1 = s(i, 2),$$

$$s_2^{-1} s(i, 2) s_2 = s(i, k)$$

szubsztitucziókat is, a mivel tételünket igazoltuk.

4. Γ minden oly invariáns alcsoportja, mely a Γ_1 csoporton kívül levő szubsztitucziókat is tartalmaz, összeesik Γ -val, ha $n > 2$, vagy ha $n = 2$, de $p > 3$.

Legyen ugyanis H egy oly invariáns alcsoport, melyben van oly

$$s = x'_i \equiv a_{i1}x_1 + \dots + a_{in}x_n$$

szubsztituczió, mely Γ_1 -ben nem fordul elő, akkor világos, hogy van oly elemi szubsztituczió — mondjuk $s(1, 2)$, mely s -et nem hagyja invariánsul, következésképpen az

$$s^{-1}s^{-1}(1, 2)ss(1, 2) = s_1 = x'_1 \equiv a'_{11}x_1 + \dots + a'_{1n}x_n, \quad x'_i \equiv x_i - a_{i1}x_2,$$

hol X_2 avval a lineáris függvénynyel helyettesítendő, a melybe $s^{-1}x_2$ -t transzformálja, oly szubsztituczió, mely az identitástól föltétlenül különbözik. Ha tehát.

$$a'_{i1} \equiv 0, \quad (i=2, \dots, n)$$

akkor $a'_{11} \equiv 1$; és az általánosság rovása nélkül föltételezhetjük, hogy $a'_{12} \not\equiv 0$; ennél fogva ha λ oly szám, melyre nézve

$$\frac{a'_{12}}{\lambda} \equiv 1 \pmod{p},$$

akkor a

$$\sigma = x'_1 \equiv x_1, \quad x'_2 \equiv \frac{a'_{12}}{\lambda}x_2 + \dots + \frac{a'_{1n}}{\lambda}x_n, \quad x'_i \equiv x_i$$

szubsztituczióval

$$\sigma^{-1}s_1\sigma = s^2(1, 2)$$

szubsztituczióhoz jutunk, melyből, ha

$$\lambda v \equiv 1 \pmod{p}$$

az

$$s^{2v}(1, 2) = s(1, 2),$$

következésképpen H összeesik Γ -val.

Ha pedig az a_{i1} -ek nem mindegyike null, pl. a_{21} nem zérus, akkor a

$$\sigma_1 = x'_1 \equiv x_1, \quad x'_2 \equiv x_2, \quad x'_i \equiv x_i - \frac{a_{i1}}{a_{21}}x_2$$

szubsztituczió alkalmazásával

$$\begin{aligned} s_2 = \sigma_1^{-1}s\sigma_1 &= x'_1 \equiv b_{11}x_1 + \dots + b_{1n}x_n, \\ x'_2 &\equiv b_{21}x_1 + \dots + b_{2n}x_n, \\ x'_i &\equiv x_i, \end{aligned}$$

ebből pedig

$$\begin{aligned} s_2^{-1}s^{-1}(1, 3) s_2 s(1, 3) &= x'_1 \equiv x_1 - (b_{11} - 1) x_3 \\ &\quad x'_1 \equiv x_2 - b_{21} x_3 \\ &\quad x'_i \equiv x_i. \\ s_2^{-1}s^{-1}(2, 3) s_2 s(2, 3) &= x'_1 \equiv x_1 - b_{12} x_3 \\ &\quad x'_2 \equiv x_2 - (b_{22} - 1) x_3 \\ &\quad x'_i \equiv x_i. \end{aligned}$$

Ezen szubsztitucziók mindegyike ily alakú:

$$s_3 = x'_1 \equiv x_1 + \lambda_1 x_3, \quad x'_2 \equiv x_2 + \lambda_2 x_3, \quad x'_i \equiv x_i.$$

Ha λ_1 és λ_2 nem mindegyike, pl. λ_1 nem null, akkor a

$$\sigma_2 = x'_1 \equiv x_1, \quad x'_2 \equiv -\frac{\lambda_2}{\lambda_1} x_1 + x_2, \quad x'_i \equiv x_i$$

szubsztituczióval való transzformációval nyerjük, hogy

$$\sigma_2^{-1} s_3 \sigma_2 = s^{\lambda_1}(1, 3),$$

tehát H összeesik Γ -val.

Ha pedig $\lambda_1 = \lambda_2 = 0$, akkor

$$b_{11} = b_{22} = 1, \quad b_{12} = b_{21} = 0.$$

Mivel s_2 nem lehet identitás, azért a b -k között kell zérustól különbözőnek lenni. Ha b_{13} és b_{23} nem mindegyike zérus, de

$$\begin{aligned} b_{1i} &= 0, \\ b_{2i} &= 0, \end{aligned}$$

akkor s_2 , már s_3 alakú. Ha pedig a b_{13} és b_{23} -on kívül még más zérustól különböző b is van, pl. b_{14} , akkor

$$\begin{aligned} s_2^{-1}s^{-1}(4, 3) s_2 s^{-1}(4, 3) &= x'_1 \equiv x_1 - b_{14} x_3, \\ &\quad x'_2 \equiv x_2 - b_{24} x_3, \\ &\quad x'_i \equiv x_i, \end{aligned}$$

mely már szintén s_3 alakú. Mivel több eset nem lehetséges, azért $n > 2$ esetre tételünk igazolást nyert.

A közöltük levezetés csekély változtatással megegyezik DICKSON levezetésével.¹ JORDAN² levezetése hiányos.

Az $n = 2$ esetben legyen

$$\begin{aligned} s &= x'_1 \equiv a_1 x_1 + b_1 x_2, \\ x'_2 &\equiv a_2 x_1 + b_2 x_2 \end{aligned}$$

H -nak oly szubsztitucziója, mely nincs meg Γ_1 -ben.

a) Ha $a_2 \equiv 0$, akkor $b_2 \equiv a_1^{-1}$.

a) az $a_1^2 \equiv 1$ esetben az

$$e = x'_1 \equiv -x_1, \quad x'_2 \equiv -x_2$$

jelölést számon tartva s , vagy se ily alakú:

$$\begin{aligned} s^\mu(1, 2) &= x'_1 \equiv x_1 + \mu x_2, \\ x'_2 &\equiv x_2, \end{aligned}$$

tehát H tartalmazza az $s^\mu(1, 2)$ -t, vagy az $s^{2\mu}(1, 2)$ -t.

$\beta)^3$ Az $a_1^2 \not\equiv 1$ esetben pedig

$$s^{-1}(1, 2) s s(1, 2) s^{-1} = s^{\frac{1-a_1^2}{a_1^2}}(1, 2).$$

b) Ha $a_2 \not\equiv 0$, akkor, ha $a_2 \lambda \equiv 1$, a

$$\begin{aligned} \sigma &= x'_1 \equiv a_2 x_1 + b_2 x_2 \\ x'_2 &\equiv \lambda x_2 \end{aligned}$$

szubsztituczióval való tranzformáció után

$$s_1 = \sigma^{-1} s \sigma = x'_1 \equiv a x_1 - \lambda^{-1} x_2, \quad x'_2 \equiv \lambda x_1,$$

ebből pedig, ha

$$\begin{aligned} \sigma_1 &= x'_1 \equiv -(\lambda k)^{-1} x_2, \quad x'_2 \equiv \lambda k x_1, \\ s_2 &= \sigma_1^{-1} s_1 \sigma_1 s_1 = x'_1 \equiv -k^2 x_1 - a \frac{k^{-2} + 1}{\lambda} x_2, \\ x'_2 &\equiv -k^{-2} x_2. \end{aligned}$$

¹ DICKSON, Linear groups. p. 83.

² JORDAN, Traité p. 108.

³ Innen kezdve az $n=2$ -re vonatkozó bizonyítás DICKSON-énál egyszerűbb.

$p > 5$ esetben k mindig megválasztható a

$$k^4 \not\equiv 1 \pmod{p}$$

föltételnek megfelelően és ekkor a β) esettel állunk szemben és

$$s^{-1}(1, 2) s_2 s(1, 2) s_2^{-1} = s^{\frac{1-k^4}{k^4}}(1, 2).$$

Ha $p = 5$, akkor $k^4 \equiv 1 \pmod{p}$, ha tehát $a \not\equiv 0$, akkor az a) alatt tárgyalt esettel állunk szemben. Ha pedig $a \equiv 0$, akkor

$$s_1 = x'_1 \equiv -\lambda^{-1}x_2, \quad x'_2 \equiv \lambda x_1,$$

ebből pedig

$$\begin{aligned} s_3 &\equiv s^{-1}(1, 2) s_1 s(1, 2) s_1 = x'_1 \equiv -x_1 + x_2, \\ x'_2 &\equiv \lambda^2 x_1 - (\lambda^2 + 1)x_2. \end{aligned}$$

Ez pedig a

$$\sigma_1 = x'_1 \equiv x_1, \quad x'_2 \equiv (\lambda^2 + 1)x_1 + x_2$$

szubsztitúcióval való transzformációval a következővé lesz:

$$s_4 = \sigma_1^{-1} s_3 \sigma_1 = x'_1 \equiv -(\lambda^2 + 2)x_1 + x_2, \quad x'_2 \equiv -x_1.$$

Mivel bármily λ -ra nézve teljesül a

$$\lambda^3 + 2 \not\equiv 0 \pmod{5}$$

föltétel, azért s_4 olyan s_1 alakú szubsztitúció, melyre nézve $a \not\equiv 0$; ezt az esetet pedig már tárgyaltuk. Ezzel aztán tételünket az $n = 2$, $p > 3$ esetre nézve is igazoltuk.

Ezek után már könnyen megkonstruálhatjuk G kompozíció sorát. Ugyanis $\frac{G}{\Gamma}$ egyszeres izomorfizmusban van az $(1, s, \dots, s^{p-2})$ csoporttal. Ha tehát

$$\begin{aligned} p-1 &= p_1 \dots p_r, \\ d &= q_1 \dots q_s, \end{aligned}$$

akkor $\frac{G}{\Gamma}$ és Γ_1 kompozíció sorai rendre:

$$\frac{G}{\Gamma}, \frac{G_{p-1}}{p_1}, \frac{G_{p-1}}{p_1 p_2}, \dots, 1$$

$$\Gamma_1, \frac{\Gamma_d}{q_1}, \frac{\Gamma_d}{q_1 q_2}, \dots, 1.$$

Ennélfogva G kompozíció sora ily alakú

$$G, \frac{G_{p-1}}{p_1} \Gamma, \frac{G_{p-1}}{p_1 p_2} \Gamma, \dots, \Gamma, \Gamma_1, \frac{\Gamma_d}{q_1}, \frac{\Gamma_d}{q_1 q_2}, \dots, 1.$$

Következően G kompozíció tényezői:

$$p_1, \dots, p_r, \frac{R(p, n)}{d(p-1)}, q_1, \dots, q_s.$$

Pl. Ha $n = 1$, akkor

$$R(p, 1) = p-1, d = 1;$$

$$\Gamma = \Gamma_1 = 1.$$

Tehát az $R(p, 1)$ kompozíció sora

$$G, \frac{G_{p-1}}{p_1}, \frac{G_{p-1}}{p_1 p_2}, \dots, 1,$$

kompozíció tényezői pedig

$$p_1, \dots, p_r,$$

ennélfogva az $R(p, 1)$ csoport föloldható csoport.

12. Alkalmazások.

1. Az aritmetikai csoportot $A(m, n)$ -el jelölve

$$A(p, 1) = (1, s, \dots, s^{p-1}),$$

hol

$$s = x' \equiv x+1 \pmod{p},$$

tehát $A(p, 1)$ ciklikus csoport tranzitív.

Azt a maximális csoportot, mely $A(p, 1)$ -et tartalmazza s egyúttal invariánsul hagyja, metaciklikus csoportnak nevezzük.

A metacziklikus csoport tehát az $R(p, 1)$ csoportnak és az $A(p, 1)$ -nek a szorzata, ennél fogva a rendszáma $p(p-1)$; a kompozíció sora:

$$A(p, 1) G, A(p, 1) G_{\frac{p-1}{p_1}}, \dots, A(p, 1), 1$$

a kompozíció tényezői pedig:

$$p_1, \dots, p_r, p,$$

tehát a metacziklikus csoport föloldható.

Megfordítva minden tranzitív föloldható p -ed fokú csoport maga a metacziklikus csoport, vagy pedig annak egyik alcsoportja.

Ugyanis a tranzitív föloldható p -ed fokú csoport kompozíciósorának az egység előtti csoportja éppen $A(p, 1)$, mely az adott csoportban is invariáns,¹ ebből pedig éppen kimondott tételünk következik.

Ha már most általánosan az összes

$$A(p, 1) G_{\frac{p-1}{p_1 \dots p_i}}$$

csoportokat metacziklikus csoportoknak nevezzük, akkor kimondhatjuk a tételt, hogy a

p -ed fokú irreduktibilis egyenletek közül csak a metacziklikus egyenletek oldhatók meg algebrailag.

2. Minden p^n -ed fokú primitív föloldható G csoport fősorának az egység előtti csoportja oly

$$s_1^{\alpha_1} \dots s_n^{\alpha_n} \quad (\alpha = 0, \dots, p-1)$$

szubsztitúciókból áll, melyekben az s -ek egymással fölcserélhetők s egymástól független p -ed rendű szubsztitúciók,² tehát az 1. fejezetben mondottak értelmében ez a csoport nem más, mint az $A(p, n)$ csoport; de mivel ez a csoport invariáns G -ben,

¹ BIANCHI, Lezioni sulla teoria dei gruppi di sostituzioni. 1900. p. 79.

² Netto, Gruppen u. Substitutionen theorie. 1908. p. 174.

azért G az $A(p, n)$ és $R(p, n)$ csoportok szorzata, vagy ennek egy alcsoportja. Ennélfogva:

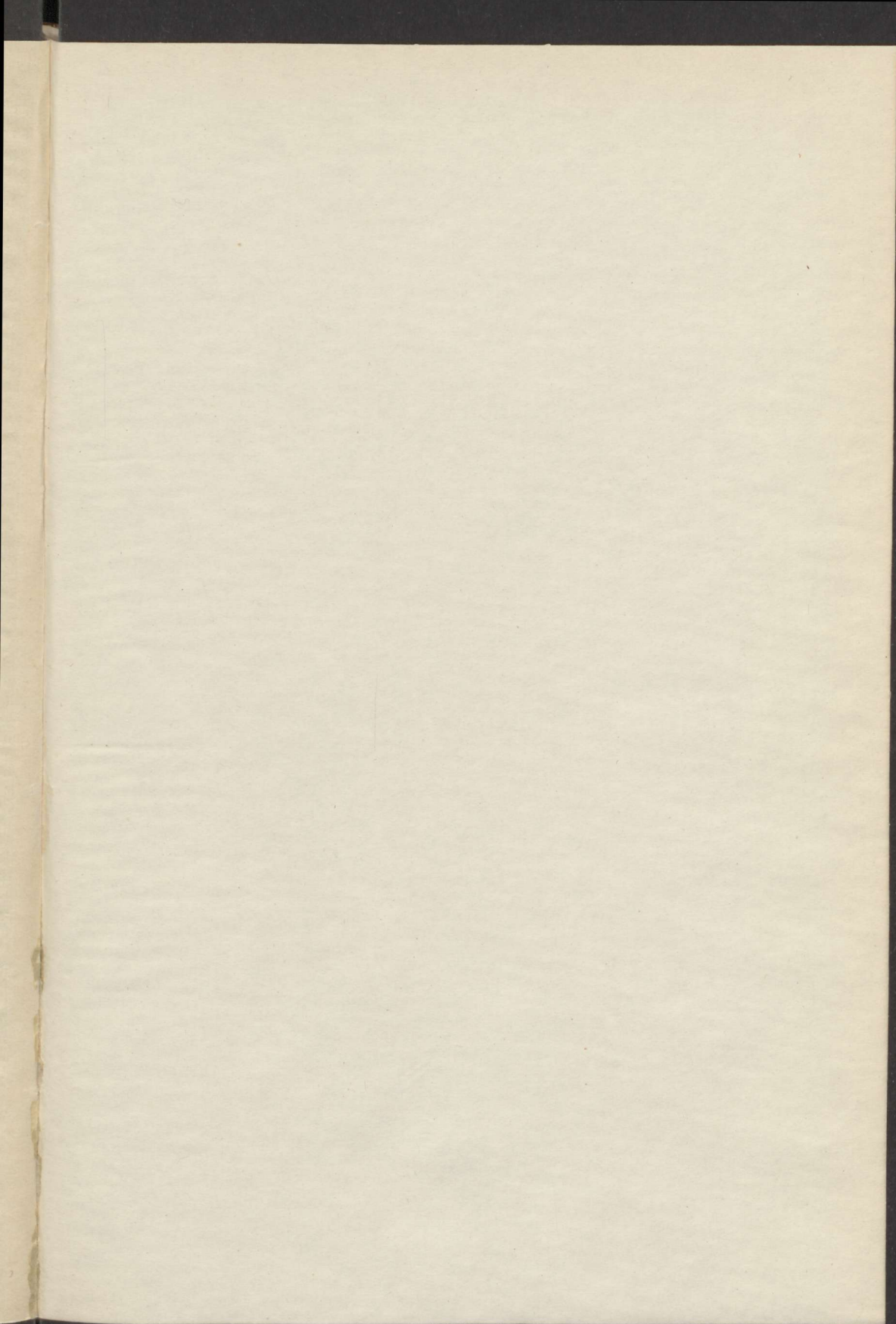
Minden p^n -ed fokú primitív föloldható csoport az $A(p, n)$ -és $R(p, n)$ csoportok szorzata, vagy pedig ennek a szorzatnak egyik alcsoportja.

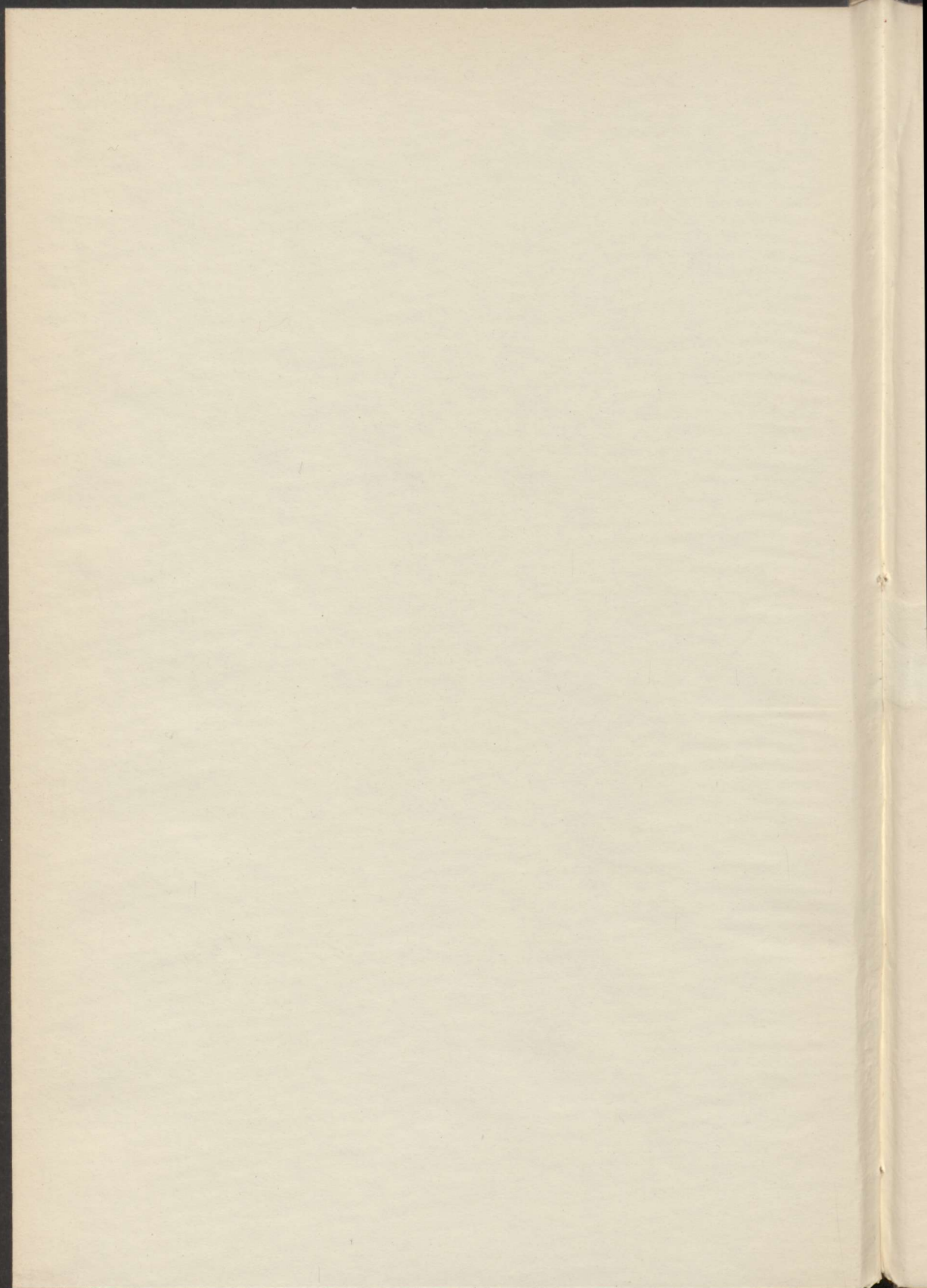
Tételünknek az algebrai egyenletek elméletében a következő felel meg:

Egy primitív p^n -ed fokú egyenlet csak akkor lehet algebrailag megoldható, ha csoportja az $A(p, n) \cdot R(p, n)$ csoportnak alcsoportja.

Suták József.







1972 MAY 16

