STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1949-012

Enige stellingen van Lubelski uit de groepentheorie

"Actualiteiten"

C. Schogt

1949

Enige stellingen van Lubelski uit de groepentheorie.

(Voordracht door C. Schogt in de serie Actualiteiten, 26 Nov.'49).

Onder een groep verstaat men een verzameling, die aan de volgende axioma's voldoet:

ax. 1. Aan een geordend paar elementen A, B van de groep is eenduidig toegevoegd een element C. De operatie, waardoor het element C aan de elementen A, B wordt toegevoegd, zullen we in het volgende steeds vermenigvuldiging noemen. We schrijven dan C = AB en noemen C product van A en B.

ax. 2. De vermenigvuldiging is associatief:

$$(AB)C = A(BC).$$

ax. 3. De groep bevat een element E, zodat EA = A voor alle elementen A uit de groep.

ax. 4. Met elk element A bevat de groep een element A_i, zodat $A_iA = E$.

Stelling 1. $AA_i = E$.

Bewijs. $E = (A_i)_iA_i = (A_i)_iEA_i = (A_i)_i\, A_iAA_i = EAA_i = AA_i$.

Stelling 2. $AE = A$.

Bewijs. $AE = AA_iA = EA = A$.

Stelling 3. Deling is mogelijk:
Bij de elementen A en B behoort een element X met AX = B en een element Y met YA = B.

Bewijs. $A(A_iB) = B$ en $(BA_i)A = B$.

Stelling 4. Deling is ondubbelzinnig:
Uit AX = AX' volgt X = X'
" YA = Y'A " Y = Y' .

Bewijs. Uit AX = AX' volgt $A_iAX = A_iAX'$, dus X = X'.
Uit YA = Y'A volgt $YAA_i = Y'AA_i$, dus Y = Y'.

Stelling 4 heeft als gevolg, dat er geen ander element dan E zelf is met de eigenschappen van E uit ax. 3 en stelling 2 en dat er bij A geen ander element dan A_i zelf is met de eigenschappen van A_i uit ax. 4 en stelling 1.

Men noemt E het eenelement van de groep en A_i het inverse van A.

Stelling 5. $(AB)_i = B_iA_i$.

Bewijs. $B_iA_iAB = B_iEB = B_iB = E.$

Dan moet dus : $(AB)_i = B_iA_i$.

Onder een ondergroep van een groep $\mathcal{G}$ verstaat men een deelverzameling, die met betrekking tot de vermenigvuldiging in $\mathcal{G}$ weer een groep is.

Stelling 6. Een niet lege deelverzameling $\mathcal{G}_1$, van een groep $\mathcal{G}$ is dan en slechts dan ondergroep, als
1. met A en B ook AB tot $\mathcal{G}_1$ behoort.
2. met A ook A_i tot $\mathcal{G}_1$ behoort.

Bewijs. Het is duidelijk, dat de voorwaarden noodzakelijk zijn. Is aan de voorwaarden voldaan, dan voldoet, daar E als product van A en A_i ook tot $\mathcal{G}_1$ behoort, $\mathcal{G}_1$ aan de vier axioma's. $\mathcal{G}_1$ is dan dus ondergroep.

Is $\mathcal{H}$ ondergroep van een groep $\mathcal{G}$ en is A een element van $\mathcal{G}$, dan verstaat men onder de linker nevenklasse A$\mathcal{H}$ van $\mathcal{H}$ in $\mathcal{G}$ de deelverzameling van $\mathcal{G}$, bestaande uit die elementen, die men krijgt, als de elementen van $\mathcal{H}$ links vermenigvuldigd worden met A. Aan ieder element van $\mathcal{H}$ wordt zo een element van A$\mathcal{H}$ toegevoegd. Uit st. 4 volgt, dat deze correspondentie een 1-1 correspondentie is. A behoort tot A$\mathcal{H}$, want A = AE en E behoort tot $\mathcal{H}$.

Stelling 7 l. Is $\mathcal{H}$ ondergroep van een groep $\mathcal{G}$ en behoort het element B van $\mathcal{G}$ tot de nevenklasse A$\mathcal{H}$, dan is B$\mathcal{H}$ = A$\mathcal{H}$.
Het bewijs kan aan de lezer overgelaten worden.

Stelling 8 l. Twee verschillende linker nevenklassen van een ondergroep $\mathcal{H}$ van een groep $\mathcal{G}$ zijn disjunct.
Dit volgt direct uit de vorige stelling.

Op dezelfde wijze kunnen we invoeren rechter nevenklassen. Hiervoor gelden de overeenkomstige stellingen 7r en 8r.

Opm. De nevenklassen van een ondergroep $\mathcal{H}$ van een groep $\mathcal{G}$ zijn, behalve $\mathcal{H}$ zelf, geen groepen met betrekking tot de vermenigvuldiging in $\mathcal{G}$, want ze bevatten geen eenelement.

Onder de orde van een groep verstaat men het aantal elementen.

Stelling 9. (Lagrange)
Is $\mathcal{H}$ ondergroep van een eindige groep $\mathcal{G}$, dan is de orde van $\mathcal{H}$ een deler van die van $\mathcal{G}$.

Bewijs: Laat n de orde van $\mathcal{G}$ zijn, m die van $\mathcal{H}$. Beschouw nu de linker nevenklassen van $\mathcal{H}$. Die bevatten elk m elementen

en zijn disjunct. Dan moet, daar elk element van $\mathfrak{O}$ in zo'n nevenklasse ligt, n een veelvoud van m zijn.

Stelling 10. Is $\mathfrak{h}$ ondergroep van $\mathfrak{O}$, dan is het aantal linker nevenklassen van $\mathfrak{h}$ in $\mathfrak{O}$ gelijk aan het aantal rechter nevenklassen. Dit aantal noemt men de index van $\mathfrak{h}$ in $\mathfrak{O}$.

Bewijs: De inversen der elementen van een linker nevenklasse $A\mathfrak{h}$ vormen een rechter nevenklasse, n.l. $\mathfrak{h}A_i$.
Is AH n.l. een element van $A\mathfrak{h}$, dan is, daar $(AH)_i = H_iA_i$, $(AH)_i$ een element van $\mathfrak{h}A_i$. Omgekeerd is ieder element van $\mathfrak{h}A_i$ het inverse van een element van $A\mathfrak{h}$.
We krijgen zo een 1-1 correspondentie tussen de linker en rechter nevenklassen: $A\mathfrak{h} \longleftrightarrow \mathfrak{h}A_i$.
Hiermee is de stelling bewezen.

We definiëren nu machten van een element van een groep:

$$A^1 = A$$
$$A^{n+1} = A^nA, \text{ als n een natuurlijk getal is.}$$
$$A^0 = E$$
$$A^{-n} = A_i^n, \text{ als n een natuurlijk getal is.}$$

Volgens deze def. is $A^{-1} = A_i$. We zullen in het vervolg het inverse van een element A door A^{-1} aanduiden.

Voor de machten gelden nu, zoals gemakkelijk te bewijzen is, de regels:

$$A^r A^s = A^{r+s}$$
$$(A^r)^s = A^{rs},$$

waarin r en s willekeurige gehele rationale getallen zijn.

Verder is $(AB)^r = A^rB^r$, als $AB = BA$.

Onder een cyclische groep verstaat men een groep, die een element bezit, waarvan alle elementen van de groep machten zijn.

Beschouw een cyclische groep $\mathfrak{L}$. Er is dan een element A, zodat alle elementen van $\mathfrak{L}$ de gedaante A^r hebben.

Zijn alle machten van A met verschillende exponenten verschillend, dan is de orde van $\mathfrak{L}$ aftelbaar oneindig.

Is echter $A^s = A^t$, waarbij $s > t$, dan is er een natuurlijk getal j, zodat $A^j = E$, n.l. het getal $s - t$. Is nu n het kleinste nat. getal, zodat $A^n = E$ dan is n de orde van de groep $\mathfrak{L}$. Deze bestaat dan uit de elementen $E, A, A^2, \ldots, A^{n-1}$.

Is s een geheel rationaal getal, dan zijn er n.l. twee gehele rationale getallen q en k, zodat $s = qn + k$ en $0 \leqq k < n$.

Dan is $A^s = A^k$.

De elementen E, A,..., A^{n-1} zijn alle verschillend, anders zou er een natuurlijk getal m zijn, kleiner dan n, waarvoor $A^m = E$. Dit is onmogelijk, want n is de kleinste natuurlijke exponent, waarbij E als macht van A optreedt.

We merken op, dat een macht van A dan en slechts dan E is, als de exponent door n deelbaar is.

De machten van een element A van een groep $\mathcal{G}$ vormen een cyclische ondergroep $\mathcal{L}$ van $\mathcal{G}$. Men zegt, dat het element A de ondergroep $\mathcal{L}$ voortbrengt.

Onder de orde van een element van een groep verstaat men nu de orde van de door dat element voortgebrachte ondergroep.

Stelling 11. De orde van een element van een eindige groep is deler van de orde van de groep. Dit volgt direct uit st. 9.

Stelling 12. (Groepentheoretische formulering van de stelling van Fermat).
Voor elk element A van een eindige groep van de orde n geldt: $A^n = E$.
Dit volgt direct uit de vorige stelling.

Stelling 13. Heeft het element A van de groep $\mathcal{G}$ de eindige orde n, dan heeft A^t dan en slechts dan de orde n, als n en t relatief priem zijn.

Bewijs: Is m de orde van A^t, dan is m een deler van n, want $(A^t)^n = E$.
Zij d de g.g.d. van n en t.
Uit $A^{tm} = E$ volgt, dat tm een veelvoud van n is.
Is d = 1, dan is m dus een veelvoud van n.
Daar m een deler van n is, is dan m = n.
Is d > 1, dan is:

$$(A^t)^{\frac{n}{d}} = (A^n)^{\frac{t}{d}} = E .$$

Dan is m ten hoogste $\frac{n}{d}$, dus m < n.
A^t heeft dus dan en slechts dan de orde n, als d = 1, d.w.z. als n en t relatief priem zijn.

Een verzameling elementen van een groep $\mathcal{G}$ noemt men een complex van $\mathcal{G}$.

Zijn $\mathcal{A}$ en $\mathcal{B}$ complexen van de groep $\mathcal{G}$, dan verstaat men onder het product $\mathcal{A}\mathcal{B}$ het complex, dat bestaat uit de producten AB, waarbij A element van $\mathcal{A}$ is, B element van $\mathcal{B}$.

Onder de orde van een complex verstaat men het aantal elementen, waaruit het bestaat.

Stelling 14. De vermenigvuldiging van complexen is associatief: Zijn $\mathfrak{A}$, $\mathfrak{B}$ en $\mathfrak{C}$ complexen van een groep, dan geldt $(\mathfrak{A}\mathfrak{B})\mathfrak{C} = \mathfrak{A}(\mathfrak{B}\mathfrak{C})$.

Het bewijs kan aan de lezer overgelaten worden.

Stelling 15. Is het complex $\mathfrak{A}$ van een groep $\mathfrak{G}$ ondergroep van $\mathfrak{G}$, dan is $\mathfrak{A}\mathfrak{A} = \mathfrak{A}$.

Het bewijs kan weer aan de lezer overgelaten worden.

In een product van complexen wordt een uit één element bestaand complex door dat element voorgesteld. Een voorbeeld hiervan hebben we reeds gehad bij de voorstelling van de nevenklassen van een ondergroep.

Is $\mathfrak{A}$ een complex van de groep $\mathfrak{G}$, dan verstaat men onder een met $\mathfrak{A}$ geconjugeerd complex een complex $A\,\mathfrak{A}\,A^{-1}$, waarin A een element van $\mathfrak{G}$ is.

Een complex is met zichzelf geconjugeerd, want

$$\mathfrak{A} = E\,\mathfrak{A}\,E^{-1}.$$

De relatie "geconjugeerd met" is omkeerbaar:

Is $\mathfrak{B} = A\,\mathfrak{A}\,A^{-1}$, dan is $\mathfrak{A} = A^{-1}\mathfrak{B}\,(A^{-1})^{-1}$.

Verder ook transitief:

Is $\mathfrak{B} = A\,\mathfrak{A}\,A^{-1}$ en $\mathfrak{C} = B\,\mathfrak{B}\,B^{-1}$, dan is

$$\mathfrak{C} = BA\,\mathfrak{A}\,A^{-1}B^{-1} = (BA)\,\mathfrak{A}\,(BA)^{-1}.$$

We kunnen de complexen uit $\mathfrak{G}$ dus in klassen geconjugeerde indelen.

Men noemt een complex $\mathfrak{A}$ normaal, als het met geen ander dan met zichzelf geconjugeerd is, m.a.w. als $A\,\mathfrak{A}\,A^{-1} = \mathfrak{A}$ voor alle elementen A van $\mathfrak{G}$.

Men zegt, dat twee groepen $\mathfrak{G}$ en $\mathfrak{H}$ isomorf zijn, als er een 1-1 correspondentie tussen hun elementen bestaat, zodat, als A met A' en B met B' correspondeert, AB met A'B' correspondeert.

Zo'n correspondentie noemt men een isomorfisme. Men schrijft $\mathfrak{G} \cong \mathfrak{H}$.

Stelling 16. Is $\mathfrak{G}_1$ een ondergroep van een groep $\mathfrak{G}$, dan is een met $\mathfrak{G}_1$ geconjugeerd complex weer een ondergroep van $\mathfrak{G}$ en wel een met $\mathfrak{G}_1$ isomorfe ondergroep.

Bewijs: Beschouw twee elementen van het complex $A\,\mathfrak{G}_1\,A^{-1}$, n.l. AGA^{-1} en AHA^{-1}, waarin G en H elementen van $\mathfrak{G}_1$ zijn. Hun product is $(AGA^{-1})(AHA^{-1}) = A(GH)A^{-1}$.

Daar $\mathfrak{G}_1$ ondergroep is, is GH weer element van $\mathfrak{G}_1$; dan behoort $A(GH)A^{-1}$ tot $A\,\mathfrak{G}\,A^{-1}$,

Verder is: $(AGA^{-1})^{-1} = A\,G^{-1}\,A^{-1}$.

Daar $\mathcal{G}_1$ ondergroep is, behoort G^{-1} weer tot $\mathcal{G}_1$, dus $A\,G^{-1}\,A^{-1}$ tot $A\,\mathcal{G}_1\,A^{-1}$.

Volgens st. 6 is $A\,\mathcal{G}_1\,A^{-1}$ dan ondergroep van $\mathcal{G}$.

De correspondentie van het el. G van $\mathcal{G}_1$ met het element AGA^{-1} van $A\,\mathcal{G}_1\,A^{-1}$ is een isomorfisme.

Stelling 17. Een ondergroep $\mathcal{G}_1$ van een groep $\mathcal{G}$ is dan en slechts dan normaal, als linker en rechter nevenklassen identiek zijn.

Bewijs: Is $\mathcal{G}_1$ normaal, dan is $A\,\mathcal{G}_1\,A^{-1} = \mathcal{G}_1$ voor alle elementen A uit $\mathcal{G}$. Dan is $A\,\mathcal{G}_1 = \mathcal{G}_1\,A$, dus linker en rechter nevenklassen zijn identiek.

Zijn linker en rechter nevenklassen identiek, dan geldt voor elk element A uit $\mathcal{G}$ de formule $A\,\mathcal{G}_1 = \mathcal{G}_1 A$, dus ook $A\,\mathcal{G}_1 A^{-1} = \mathcal{G}_1$. Dan is $\mathcal{G}_1$ dus normaal.

Stelling 18. De nevenklassen van een normale ondergroep van een groep vormen met betrekking tot de vermenigvuldiging een groep.

Bewijs: Laat $\mathcal{G}_1$ een normale ondergroep van de groep $\mathcal{G}$ zijn. Beschouw de nevenklassen $\mathcal{G}_1 A$ en $\mathcal{G}_1 B$. Dan is:

$$(\mathcal{G}_1 A)(\mathcal{G}_1 B) = \mathcal{G}_1(A\,\mathcal{G}_1)B = \mathcal{G}_1(\mathcal{G}_1 A)B = (\mathcal{G}_1\mathcal{G}_1)(AB) =$$
$$= \mathcal{G}_1(AB) .$$

Het product van twee nevenklassen van $\mathcal{G}_1$ is dus weer een nevenklasse van $\mathcal{G}_1$.

De vermenigvuldiging van nevenklassen van $\mathcal{G}_1$ is natuurlijk associatief.

$\mathcal{G}_1$ heeft de eigenschap van het eenelement. Als inverse van $\mathcal{G}_1 A$ treedt $\mathcal{G}_1 A^{-1}$ op.

De nevenklassen van $\mathcal{G}_1$ vormen dus een groep.

De groep van de nevenklassen van de normale ondergroep $\mathcal{G}_1$ in de groep $\mathcal{G}$ duidt men aan door $\mathcal{G}/\mathcal{G}_1$ en noemt men factorgroep.

In verband hiermee wordt een normale ondergroep ook wel normaaldeler genoemd.

De orde van $\mathcal{G}/\mathcal{G}_1$ is de index van $\mathcal{G}_1$ in $\mathcal{G}$.

Onder de normalisator $\mathcal{N}$ van een complex $\mathcal{A}$ in een groep $\mathcal{G}$ verstaat men de verzameling van de elementen van $\mathcal{G}$, die met $\mathcal{A}$ verwisselbaar zijn (d.w.z. de elementen A, waarvoor $A\,\mathcal{A} = \mathcal{A}\,A$).

Is $\mathcal{A}$ normaal in $\mathcal{G}$, dan geldt voor ieder element A uit $\mathcal{G}$:

$$A\,\mathcal{A}\,A^{-1} = \mathcal{A} .$$

Dus: $A\,\mathcal{A} = \mathcal{A}A$.

Dan is $\mathcal{G}$ dus de normalisator van $\mathcal{A}$.

Stelling 19. De normalisator $\mathcal{N}$ van een complex $\mathcal{A}$ in een groep $\mathcal{G}$ is ondergroep van $\mathcal{G}$.

Bewijs: $\mathcal{N}$ is niet leeg, want E behoort tot $\mathcal{N}$.
Beschouw twee elementen A en B van $\mathcal{N}$.
Dan is:

$$A\,\mathcal{A} = \mathcal{A}\,A$$
$$B\,\mathcal{A} = \mathcal{A}\,B .$$

Dus $AB\,\mathcal{A} = A\,\mathcal{A}\,B = \mathcal{A}\,AB$.
AB behoort dus ook tot $\mathcal{N}$.
Met A behoort verder A^{-1} tot $\mathcal{N}$.
Uit $A\,\mathcal{A} = \mathcal{A}\,A$ volgt immers: $A^{-1}A\,\mathcal{A}\,A^{-1} = A^{-1}\mathcal{A}\,AA^{-1}$

$$\mathcal{A}\,A^{-1} = A^{-1}\mathcal{A} .$$

Volgens st. 6 is $\mathcal{N}$ dus ondergroep van $\mathcal{G}$.

Stelling 20. Is $\mathcal{N}$ de normalisator van een ondergroep $\mathcal{H}$ van $\mathcal{G}$, dan is $\mathcal{H}$ normaaldeler van $\mathcal{N}$.

Bewijs: Is A een element van $\mathcal{H}$, dan is, daar $\mathcal{H}$ ondergroep is, $A\,\mathcal{H} = \mathcal{H}\,A = \mathcal{H}$.
A behoort dus tot $\mathcal{N}$.
Dit geldt voor ieder element van $\mathcal{H}$, dus $\mathcal{H} \subset \mathcal{N}$. $\mathcal{H}$ is nu ondergroep van $\mathcal{N}$.
Is B een element van $\mathcal{N}$, dan is $B\,\mathcal{H} = \mathcal{H}\,B$.
$\mathcal{H}$ is dus normaaldeler van $\mathcal{N}$.

Zoals reeds opgemerkt, kan men de complexen van een groep $\mathcal{G}$ in klassen geconjugeerde complexen indelen. De klasse van een complex $\mathcal{A}$ in $\mathcal{G}$ is de verzameling van de complexen uit $\mathcal{G}$, die met $\mathcal{A}$ geconjugeerd zijn. Onder de orde van de klasse verstaat men het aantal complexen, waaruit deze bestaat.

Stelling 21. Is $\mathcal{A}$ een complex van een groep $\mathcal{G}$, $\mathcal{N}$ de normalisator van $\mathcal{A}$ in $\mathcal{G}$ en $\mathcal{K}$ de klasse van $\mathcal{A}$ in $\mathcal{G}$, dan is de index van $\mathcal{N}$ in $\mathcal{G}$ gelijk aan de orde van $\mathcal{K}$.

Bewijs: Zij $\mathcal{B}$ een complex uit $\mathcal{K}$. Dan is $\mathcal{B} = B\,\mathcal{A}\,B^{-1}$. Is nu $C\,\mathcal{A}\,C^{-1} = \mathcal{B}$, dan is $B^{-1}\,C\,\mathcal{A}\,C^{-1}\,B = B^{-1}\mathcal{B}\,B = \mathcal{A}$, dus $B^{-1}C\,\mathcal{A} = \mathcal{A}\,B^{-1}C$. Dan behoort $B^{-1}C$ dus tot $\mathcal{N}$, C dus tot $B\,\mathcal{N}$.
Behoort D tot $B\,\mathcal{N}$, dan is $D = BA$. waarin A tot $\mathcal{N}$ behoort. Dan is:

$$D\,\mathcal{A}\,D^{-1} = BA\,\mathcal{A}\,A^{-1}B^{-1} = B\,\mathcal{A}\,A\,A^{-1}B^{-1} = B\,\mathcal{A}\,B^{-1} = \mathcal{B} .$$

Dus $C\,\mathcal{A}\,C^{-1} = \mathcal{B}$ dan en slechts dan, als C tot $B\,\mathcal{N}$ behoort.
Er is zo een 1-1 correspondentie tussen de complexen van $\mathcal{K}$ en de linker nevenklassen van $\mathcal{N}$, waarbij een complex $C\,\mathcal{A}\,C^{-1}$ met de nevenklasse $C\,\mathcal{N}$ correspondeert. De index van $\mathcal{N}$ in $\mathcal{G}$ is dus gelijk aan de orde van $\mathcal{K}$.

Nu komen de stellingen van Lubelski.

Bij de volgende stelling maken we gebruik van $\varphi(n)$, de functie van Euler, waarin n een natuurlijk getal voorstelt. $\varphi(n)$ is het aantal natuurlijke getallen $\leq n$, die met n relatief priem zijn.

De getallentheorie leert ons, dat als $n > 1$

$$\varphi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i} ,$$

waarin $p_1, \ldots, p_k$ de verschillende priemfactoren van n zijn.

$$\varphi(1) = 1 .$$

Stelling 22. (Lubelski).

Onderstelde: Het natuurlijke getal M is deler van de orde h van een eindige groep $\mathcal{G}$. Het getal p is 1 of een priemfactor van M. $\mathcal{K}$ is het complex van $\mathcal{G}$, bestaande uit die elementen, waarvan de orde deler van M en veelvoud van iedere op M deelbare macht van p is.

Gestelde: De orde K van $\mathcal{K}$ is deelbaar door $\frac{M}{p}$.

Bewijs: We bewijzen de stelling door volledige inductie. Heeft $\mathcal{G}$ de orde 1, dan is $M = 1$ en $p = 1$, dus $\frac{M}{p} = 1$. Dan is K dus deelbaar door $\frac{M}{p}$.

We nemen nu aan, dat de stelling geldt, als de orde van de groep kleiner dan h is, en bewijzen de stelling dan voor de orde h.

1) We beschouwen eerst het geval $p > 1$.

Is a de exponent van de hoogste macht van p, die deler van M is, dan bestaat $\mathcal{K}$ uit die elementen van $\mathcal{G}$, waarvan de orde deler van M en veelvoud van p^a is.

Is $\mathcal{K}$ leeg, dan is $K = 0$ en het gestelde juist. We nemen nu aan, dat $\mathcal{K}$ niet leeg is.

We verdelen het complex $\mathcal{K}$ in complexen $\mathcal{K}_u^{(j)}$ waarbij een $\mathcal{K}_u^{(j)}$ bestaat uit de elementen van de orde u, die tot eenzelfde cyclische ondergroep van de orde u behoren.

Uit st. 13 volgt, dat een cyclische groep van de orde u juist $\varphi(u)$ elementen van de orde u bevat. De orde van een $\mathcal{K}_u^{(j)}$ is dus $\varphi(u)$.

Een element van $\mathcal{K}$ van de orde u behoort tot slechts één $\mathcal{K}_u^{(j)}$ want het behoort tot één cyclische ondergroep van de orde u, n.l. die, welke het voortbrengt.

De mogelijke waarden van u zijn door p^a deelbaar. Is u deelbaar door p^a, dan is $\varphi(u)$ deelbaar door p^{a-1}.

$\mathcal{K}$ is dus verdeeld in disjuncte complexen, waarvan de orde deelbaar is door p^{a-1}. De orde K van $\mathcal{K}$ is dan ook deelbaar door p^{a-1}.

We zullen nu aantonen, dat K deelbaar is door $\frac{M}{p^a}$. Zij A een element van $\mathfrak{K}$. Zij $m = \frac{M}{p^a}$. De orde van A is deler van M, dus $A^M = E$. Dan is $(A^m)^{p^a} = E$. De orde van A^m is dus deler van p^a. Daar de orde van A een veelvoud van p^a is, is

$$A^{mp^{a-1}} \neq E.$$

De orde van A^m is dus p^a.

Daar p^a en m relatief priem zijn, zijn er volgens de getallentheorie twee gehele rat. getallen x en y, zodat

$$p^a x + m y = 1.$$

We voeren nu in $U = A^{my}$ en $V = A^{p^a x}$.

Dan is $A = UV = VU$.

Daar y en p^a relatief priem zijn en A^m de orde p^a heeft, heeft volgens st. 13 ook A^{my} de orde p^a. De orde van U is dus p^a.

$$V^m = (A^{p^a x})^m = (A^{mp^a})^x = (A^M)^x = E.$$

De orde van V is dus een deler van m.

Zo is ieder element uit $\mathfrak{K}$ commutatief product van een element van de orde p^a en een element, waarvan de orde deler van m is.

Is gegeven $A = UV = VU$, waarbij U de orde p^a heeft en de orde van V een deler van m is, dan is:

$$U = U^{my} = U^{my}V^{my} = (UV)^{my} = A^{my}.$$

Laat U nu een willekeurig element van de orde p^a zijn. U brengt de cyclische groep $\mathfrak{P}$ voort, die uit p^a elementen bestaat. Zij $\mathfrak{N}$ de normalisator van U in $\mathfrak{G}$. Daar de machten van U met U verwisselbaar zijn, is $\mathfrak{P}$ ondergroep van $\mathfrak{N}$. De elementen van $\mathfrak{N}$ zijn met U verwisselbaar, dus ook met iedere macht van U. Ze zijn dus met $\mathfrak{P}$ verwisselbaar; $\mathfrak{P}$ is dus normaaldeler van $\mathfrak{N}$. De orde van $\mathfrak{N}$ is deelbaar door die van $\mathfrak{P}$, dus door p^a. Laat $p^a\tau$ de orde van $\mathfrak{N}$ zijn. Dan is τ de orde van $\mathfrak{N}/\mathfrak{P}$. Daar $p^a\tau \leq h$ is, is $\tau < h$.

We kunnen onze stelling dus op $\mathfrak{N}/\mathfrak{P}$ toepassen. Dit doen we nu met de g.g.d. s van m en τ voor M en 1 voor p. Dan krijgen we: Het aantal elementen van $\mathfrak{N}/\mathfrak{P}$, waarvan de orde een deler van s is, is door s deelbaar.

Laat $\mathfrak{P}R$ zo'n element zijn met orde e. Dan is $(\mathfrak{P}R)^e = \mathfrak{P} \cdot (UR)^e$ behoort dus tot $\mathfrak{P}$, is dus een macht van U. Daar R tot $\mathfrak{N}$ behoort, is $UR = RU$, dus $(UR)^e = U^eR^e$. Dus R^e is ook een macht van U. Zij $R^e = U^g$. e is deler van s, dus van m; p^a en e zijn dus relatief priem, waaruit volgt, dat er twee gehele rat. getallen k en t zijn, zodat $kp^a - te = g$. Dan is $R^e = U^{kp^a} U^{-te} = U^{-te}$.

Nu is, daar $U^tR = RU^t$, $(U^tR)^e = U^{te}R^e = E$.
We schrijven nu: $U^tR = R_1$.

Zij Q een willekeurig element van $\mathfrak{P}$ R. De orde v van Q is dan veelvoud van e. Uit $Q^v = E$ volgt n.l. $(\mathfrak{P} R)^v = \mathfrak{P}$; daar $\mathfrak{P}$ R in $\mathfrak{N}/\mathfrak{P}$ de orde e heeft, is v dus veelvoud van e. v is deler van $p^a e$. Daar $(\mathfrak{P} R)^e = \mathfrak{P}$ is, behoort Q^e tot $\mathfrak{P}$, waaruit volgt, dat $Q^{p^a e} = (Q^e)^{p^a} = E$ is.

Daar R_1 tot $\mathfrak{P}$ R behoort en $R_1^e = E$ is, heeft R_1 dus de orde e.

De orde n van UR_1 is, daar UR_1 tot $\mathfrak{P}$ R behoort, veelvoud van e. Daar $UR_1 = R_1U$ is, is $E=(UR_1)^n = U^n R_1^n = U^n$. Hieruit volgt, dat n veelvoud van p^a is. n is deler van $p^a e$, dus a fortiori van $p^a m = M$. UR_1 behoort dus tot $\mathfrak{L}$.

R_1 is het enige element van $\mathfrak{P}$ R, waarvan de orde een deler van m is.

Neem een ander element. Hiervoor kan men schrijven U^jR_1, waarin $0<j<p^a$. Dan is:

$$(U^jR_1)^m = U^{jm} R_1^m = U^{jm} .$$

Dit is niet E, daar jm niet deelbaar is door p^a. Iedere nevenklasse van $\mathfrak{P}$ in $\mathfrak{N}$, waarvan de orde in $\mathfrak{N}/\mathfrak{P}$ een deler is van s, bevat dus juist één element, waarvan de orde een deler is van m.

Is R' een element van $\mathfrak{N}$, waarvan de orde een deler van m is, dan is $(\mathfrak{P} R')^m = \mathfrak{P}$. De orde van $\mathfrak{P}$ R' in $\mathfrak{N}/\mathfrak{P}$ is dus ook deler van m en, daar $\mathfrak{N}/\mathfrak{P}$ de orde τ heeft, ook deler van τ, dus deler van s.

Ieder element van $\mathfrak{N}$, waarvan de orde een deler van m is, behoort dus tot een nevenklasse van $\mathfrak{P}$, waarvan de orde in $\mathfrak{N}/\mathfrak{P}$ een deler van s is.

Het aantal elementen van $\mathfrak{N}$, waarvan de orde een deler van m is, is dus gelijk aan het aantal elementen van $\mathfrak{N}/\mathfrak{P}$, waarvan de orde een deler van s is. Dit aantal is deelbaar door s; noem het sb. In iedere nevenklasse van $\mathfrak{P}$ in $\mathfrak{N}$, waarvan de orde in $\mathfrak{N}/\mathfrak{P}$ een deler van s is, heeft het element, waarvan de orde deler van m is, de eigenschap, dat zijn product met U tot $\mathfrak{K}$ behoort. Deze eigenschap heeft dus ieder element van $\mathfrak{N}$, waarvan de orde een deler van m is.

Dan is sb het aantal elementen van $\mathfrak{K}$, die als commutatief product van U met een element, waarvan de orde deler van m is, optreden.

Beschouw een element B. Brengt B de cyclische groep $\mathfrak{B}$ voort, dan brengt het met B geconjugeerde element CBC^{-1}, daar $(CBC^{-1})^j = CB^jC^{-1}$, de met $\mathfrak{B}$ geconjugeerde groep $C\mathfrak{B}C^{-1}$ voort. $\mathfrak{B}$ en $C\mathfrak{B}C^{-1}$ zijn isomorf, hebben dus dezelfde orde. De elementen B en CBC^{-1} hebben dus dezelfde orde.

Zij A een element uit $\mathfrak{A}$, dat als commutatief product van U met een element V, waarvan de orde deler van m is, optreedt.

Beschouw nu het met U geconjugeerde element CUC^{-1}. CUC^{-1} heeft, evenals U, de orde p^a.

Dan volgt uit A = UV = VU, dat $CAC^{-1}=(CUC^{-1})(CVC^{-1})= (CVC^{-1})(CUC^{-1})$. CAC^{-1} heeft dezelfde orde als A, behoort dus ook tot $\mathfrak{K}$. CVC^{-1} heeft dezelfde orde als V. CAC^{-1} is dus een element uit $\mathfrak{L}$, dat commutatief product van CUC^{-1} is met een element, waarvan de orde deler van m is.

Is A' een element uit $\mathfrak{K}$, dat commutatief product van CUC^{-1} is met een element, waarvan de orde deler van m is, dan is $C^{-1}A'C$ een element uit $\mathfrak{L}$, dat commutatief product van U is met een element, waarvan de orde deler van m is.

Er is zo een 1-1 correspondentie tussen de elementen uit $\mathfrak{L}$, die als commutatief product van U met een element waarvan de orde deler van m is, optreden, en de elementen uit $\mathfrak{K}$, die als commutatief product van CUC^{-1} met een element, waarvan de orde deler van m is, optreden.

Zo bepaalt ieder met U geconjugeerd element dus sb elementen van $\mathfrak{L}$, die als commutatief product van dit element met een element, waarvan de orde deler van m is, te schrijven zijn.

We hebben gezien, dat een element uit $\mathfrak{K}$ steeds als zo'n product van slechts één element van de orde p^a optreedt; dat is n.l. zijn my^e macht.

Elementen van $\mathfrak{L}$, die aan verschillende met U geconjugeerde elementen zijn toegevoegd, zijn dus verschillend.

De orde van de klasse van U, d.w.z. het aantal met U geconjugeerde elementen, is volgens st. 21 gelijk aan de index van $\mathfrak{N}$, dus $\frac{h}{p^a\tau}$.

Het aantal elementen van $\mathfrak{L}$, dat commutatief product is van één met U geconjugeerd element en een element, waarvan de orde een deler van m is, bedraagt dus $\frac{h}{p^a\tau}$. sb. We zullen bewijzen, dat dit door m deelbaar is.

h is deelbaar door $p^a m$, stel $h = p^a mq$.
s is g.g.d. van m en τ. Zij $m = m's$, $\tau = \tau's$.

Dan is: $$\frac{h}{p^a\tau} = \frac{p^a mq}{p^a\tau} = \frac{mq}{\tau} = \frac{m'sq}{\tau's} = \frac{m'q}{\tau'} = m'\frac{q}{\tau'}$$

Daar m' en τ' relatief priem zijn en m'q door τ' deelbaar is, is q door τ' deelbaar, dus $\frac{q}{\tau'}$ geheel.

$$\frac{h}{p^a\tau}\, sb = m'\frac{q}{\tau'}\, sb = m\frac{q}{\tau'}\, b$$

Men kan nu $\mathfrak{L}$ in disjuncte complexen verdelen, waarbij ieder complex bestaat uit elementen, waarvan de my^e machten geconjugeerd zijn. Het aantal elementen in elk van deze complexen is door m deelbaar. Dan is ook K, het aantal elementen van $\mathfrak{L}$, door m deelbaar.

K is deelbaar door p^{a-1} en door m; daar p^{a-1} en m relatief priem zijn, is K dus deelbaar door $m\,p^{a-1} = \frac{M}{p}$. Hiermee is het bewijs voor $p>1$ voltooid.

2). We beschouwen nu het geval $p = 1$.

Dan moet bewezen worden, dat het aantal elementen van $\mathcal{G}$, waarvan de orde een deler van M is, door M deelbaar is. Noem dit aantal N_M.

Is $M = h$, dan is de orde van alle elementen van $\mathcal{G}$ een deler van M en is dus $N_M = M$. Dan is het gestelde juist.

Laat het gestelde juist zijn, als het aantal priemfactoren van $\frac{h}{M}$ kleiner is dan r. We tonen aan, dat het juist is, als dit aantal r is:

Zij π een van de priemfactoren van $\frac{h}{M}$. Dan is r-1 het aantal priemfactoren van $\frac{h}{M\pi}$. Dan is $N_{M\pi}$ deelbaar door $M\pi$. Laat π^c de hoogste macht van π in $M\pi$ zijn. De delers van $M\pi$, die geen delers van M zijn, zijn de veelvouden van π^c onder de delers van $M\pi$.
$N_{M\pi} - N_M$ is dus het aantal elementen van $\mathcal{G}$, waarvan de orde deler van $M\pi$ en veelvoud van π^c is. Volgens het onder 1) bewezene is dit aantal door M deelbaar. Daar $N_{M\pi}$ ook door M deelbaar is, is dus N_M door M deelbaar. Hiermee is de stelling bewezen.

Stelling 23. (Lubelski)

Ondersteld: Het nat. getal $M = \prod p_j^{a_j}$, waarin de p's verschillende priemgetallen zijn, is een deler van de orde h van de eindige groep $\mathcal{G}$. Het getal $P = \prod_{i=1}^{s} p_i^{\alpha_i}$, $\alpha_i > 0$, is deler van M. $\mathcal{K}$ is het complex, dat uit die elementen van $\mathcal{G}$ bestaat, waarvan de orde deler van M en veelvoud van P is.

Gestelde: De orde K van het complex $\mathcal{K}$ is deelbaar door

$$\frac{M}{p_1^{a_1-\alpha_1+1} \cdot \ldots \cdot p_s^{a_s-\alpha_s+1}}$$

Bewijs: 1) Zij n_t het aantal elementen van $\mathcal{G}$, waarvan de orde deler van t is, $\overline{n}_t$ het aantal elementen, waarvan de orde veelvoud van t en deler van M is.

Zij p priemdeler van M, p^a de hoogste macht van p, die deelbaar is op M. Zij r een natuurlijk getal $\leq a$.

De delers van M, die geen veelvoud van p^r zijn, zijn de delers van $\frac{M}{p^{a-r+1}}$.

Dus:

$$n_M = \overline{n}_{p^r} + n_{\frac{M}{p^{a-r+1}}}$$

Volgens st. 22 is $n_{\frac{M}{p^{a-r+1}}}$ door $\frac{M}{p^{a-r+1}}$ deelbaar, N_M door M, dus ook door $\frac{M}{p^{a-r+1}}$.

Dan is ook $\overline{n}_{p^{\alpha}}$ deelbaar door $\frac{M}{p^{a-r+1}}$.

Onze stelling is hiermee bewezen voor $g = 1$.

2) We nemen nu aan, dat de stelling voor $g \leqslant m$ geldt, en bewijzen de stelling voor $g = m + 1$.

Dan is de stelling door volledige inductie bewezen. Nu is:

$$P = p_1^{\alpha_1} \ldots\ldots p_{m+1}^{\alpha_{m+1}}$$

Zij: $$\frac{M}{p_1^{a_1-\alpha_1+1} \ldots\ldots p_{m+1}^{a_{m+1}-\alpha_{m+1}+1}} = M_1 .$$

De delers van M_1 zijn de delers van M, die door geen van de getallen $p_i^{\alpha_i}$, $i = 1,\ldots,m+1$, deelbaar zijn.
Hieruit volgt:

$$n_{M_1} = n_M - \sum \overline{n}_{p_i^{\alpha_i}} + \sum \overline{n}_{p_i^{\alpha_i} p_j^{\alpha_j}} \ldots\ldots + (-1)^{m+1} \overline{n}_{p_1^{\alpha_1} \ldots p_{m+1}^{\alpha_{m+1}}}$$

Een element, waarvan de orde een deler van M, die door k getallen $p_i^{\alpha_i}$ deelbaar is $(k > 0)$, komt in het rechterlid n.l. $1 - \binom{k}{1} + \binom{k}{2} \ldots + (-1)^k \binom{k}{k} = (1-1)^k = 0$ maal voor.

Zo blijven juist die elementen over, waarvan de orde een deler van M is, die door geen van de getallen $p_i^{\alpha_i}$ deelbaar is.

Nu is n_M deelbaar door M_1, n_M door M, dus ook door M_1. Uit de onderstelling, dat de stelling geldt voor $g \leqslant m$, volgt, dat verder alle termen van het rechterlid, behalve de laatste, deelbaar zijn door M_1. Dan moet ook de laatste term deelbaar zijn door M_1.

Dus $\overline{n}_{p_1^{\alpha_1} \ldots p_{m+1}^{\alpha_{m+1}}}$ is deelbaar door M_1. Dit moest bewezen worden.

Opmerking: Stelling 22 is een uitbreiding van de stelling van Frobenius, die alleen het geval $p = 1$ behandelt.