Vacantiecursus Groepontheorie 1949

Inleidende Voordracht II.   F. van der Blij

Abstracte beschouwingen.
Groepen van transformaties van het platte vlak.
Voorbeelden.

Abstracte beschouwingen.

Een verzameling elementen heet een groep wanneer:

i. aan ieder geordend tweetal elementen a,b een element c is toegevoegd. (a.b = c, product)

(a.b).c = a.(b.c) associatieve wet. de uitdrukking a.b.c. is [illegible]

iii. er een element e bestaat zodat voor alle elementen a geldt e.a = a.

iv. er bij ieder element a een element a^{-1} bestaat met $a^{-1}.a = e$.

Inplaats van iii en iv kunnen we ook nemen

v. er bij ieder tweetal elementen a en b twee elementen x en y bestaan met a.x = b en y.a = b.

We kunnen direct enkele stellingen bewijzen:

$a.a^{-1} = e$ voor alle elementen a, a^{-1} heet inverse van a.

a.e = a voor alle elementen a. e heet eenheidselement.

Het aantal elementen van een groep heet de orde.

Een deelverzameling H van een groep G heet een ondergroep indien:

i. uit $a \in H$ en $b \in H$ volgt $ab \in H$

ii. uit $a \in H$ volgt $a^{-1} \in H$.

Inplaats van i en ii mogen we ook nemen:

iii. uit $a \in H$ en $b \in H$ volgt $ab^{-1} \in H$.

Een ondergroep H roept een klasseindeling van de elementen van de groep te voorschijn, door alle elementen, die op een rechts (links) factor van H na, gelijk zijn in eenzelfde klasse op te nemen. Een eerste klasse is de ondergroep zelf. Indien er een element a bestaat dat niet tot H behoort, vormen alle elementen a.h, waarin $h \in H$ een tweede klasse, die we voorstellen door a.H. Indien er een element b bestaat dat noch tot H noch tot a.H behoort, bepalen we analoog een nieuwe klasse b.H, etc.

Hierdoor wordt inderdaad een indeling in klassen vastgelegd. De klassen noemen we nevenklassen. We beschouwen nu de verzameling van alle (linkszijdige) nevenklassen en trachten deze verzameling als een groep op te vatten.

Aan de klassen a.H en b.H moet een klasse toegevoegd worden. We kiezen hiervoor de verzameling van alle producten van een element uit a.H met een element uit b.H. Deze verzameling zou een nevenklasse K moeten zijn en omdat uit $e \in H$ volgt a.e.b.e.=.ab$\in$ K moet het de nevenklasse van a.b zijn. Alle elementen $a.h_1.b.h_2$ moeten in a.b.H liggen, d.w.z. bij iedere $h_1 \in H$ en $h_2 \in H$ moet een $h_3 \in H$ bestaan met $a.h_1.b.h_2 = a.b.h_3$.

Of bij ieder element $h_1 \in H$ moet een $h_4 \in H$ bestaan zodat $h_1 b = b.h_4$.
De linker en rechter nevenklassen b.H en H.b moeten identiek zijn. Indien dit voor ieder element b zo is heet de ondergroep H een normaaldeler. De groep van de nevenklassen H,a.H,b.H etc. heet de factorgroep G/H. De nevenklasse H is het eenheidselement van de factorgroep. Het aantal nevenklassen heet de index van de ondergroep. De orde van G is het product van de index en de orde van ondergroep H.

Opmerking. In een groep waarin steeds geldt a.b = b.a (commutatieve of Abelse groep) is iedere ondergroep een normaaldeler. In iedere groep zijn de groep zelf en het eenheidselement triviale voorbeelden van normaaldelers. Een groep die geen andere normaaldelers bezit heet enkelvoudig (einfach).

Twee groepen g en G met elementen a,b,... en A,B,... resp. heten isomorf (1-isomorf) wanneer de elementen a,b,... en A,B,... één-éénduidig aan elkaar toegevoegd kunnen worden zodat de product relaties bewaard blijven d.w.z. dat steeds uit toevoegingen $a \leftrightarrow A$ en $b \leftrightarrow B$ volgt $ab \leftrightarrow AB$. Twee groepen g en G heten homomorf indien de toevoeging van de elementen wel de productrelaties bewaart, maar niet één-éénduidig is.

Voorbeeld. Een groep G en zijn factorgroep G/H zijn homomorf. Aan ieder element $a \in G$ voegen we toe de nevenklasse a.H$\in$ G/H.

Een automorfie is een isomorfie, die een groep aan zichzelf toevoegt. Een eenvoudig voorbeeld wordt gegeven door aan ieder element x een element axa^{-1} toe te voegen, waarin a een willekeurig, vast gekozen element van de groep is. Deze automorfismen heten in het bizonder inwendige automorfismen. Indien een ondergroep onder alle inwendige automorfismen invariant is, heet deze ondergroep een invariante ondergroep. Het is eenvoudig in te zien dat een invariante ondergroep hetzelfde als een normaaldeler is.

Onder een maximale normaaldeler N van een groep G verstaan we een normaaldeler, die geen echte deelverzamling is van een andere normaaldeler van G. Een groep kan verscheidene maximale normaaldelers hebben. Zo heeft de groep $A, A^2, A^3, A^4, A^5, A^6 = E$ de maximale normaaldelers E, A^2, A^4 en E, A^3.

Laat N nu een maximale normaaldeler van G zijn en N_1 een maximale normaaldeler van N, N is dan niet noodzakelijk normaaldeler van G. We beschouwen de rij van factorgroepen G/N, N/N_1, N_1/N_2,... ... N_α/E, waarin steeds N_{i+1} een maximale normaaldeler van N_i zal zijn.

De rij $G, N, N_1, N_2, \ldots N_\alpha, E$ heet <u>compositierij</u> van G. Alle factorgroepen uit de rij factorgroepen zijn <u>enkelvoudig</u>.

<u>Opmerking</u>. Wanneer de orde van iedere factorgroep een priemgetal is, zijn de factorgroepen <u>cyclisch</u> d.w.z. alle elementen zijn voor te stellen als machten van een enkel element, en de groep G heet <u>oplosbaar</u>. Voor twee verschillende compositierijen van eenzelfde groep G geldt dat de factorgroepen afgezien van de volgorde isomorf zijn. (<u>Stelling van Jordan-Hölder</u>). Het bewijs van deze stelling kan met volledige inductie geleverd worden.

<u>Groepen van transformaties van het platte vlak</u>

We beschouwen verschillende ondergroepen van de groep van de projectieve transformaties (niet singulier):

$$\begin{pmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{pmatrix} \text{ d.w.z. } \bar{x} = \frac{a_1 x + b_1 y + d_1}{a_3 x + b_3 y + d_3} \quad , \; \bar{y} = \frac{a_2 x + b_2 y + d_2}{a_3 x + b_3 y + d_3} \; .$$

(bij de projectieve transformaties is de dubbelverhouding van 4 punten op een rechte invariant).

Eerst de ondergroep van de <u>affiene</u> transformaties:

$$\begin{pmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ 0 & 0 & 1 \end{pmatrix}$$

Onder deze transformaties blijven // lijnen evenwijdig, terwijl de verhouding van twee afstanden op evenwijdige lijnen invariant blijft.

Een ondergroep van de affiene groep is de groep van de <u>gelijkvormigheidstransformaties</u>:

$$A: \begin{pmatrix} c & s & d_1 \\ -s & c & d_2 \\ 0 & 0 & 1 \end{pmatrix} \text{ en } B: \begin{pmatrix} c & s & d_1 \\ s & -c & d_2 \\ 0 & 0 & 1 \end{pmatrix}$$

A is de groep van de <u>directe gelijkv. transf.</u>, B de verzameling van de <u>gespiegelden</u>. Invarianten zijn hier de hoek tussen twee lijnen en de verhouding van twee afstanden.

De ondergroep van de <u>congruenties</u> wordt gevormd door de transformaties A en B, waarvoor $c^2 + s^2 = 1$. Hierbij zijn hoek en afstand invariant. De groep van de congruenties heeft o.a. de drie volgende ondergroepen:

i. de translaties in X richting $\begin{pmatrix} 1 & 0 & d_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

samen translaties $\begin{pmatrix} 1 & 0 & d_1 \\ 0 & 1 & d_2 \\ 0 & 0 & 1 \end{pmatrix}$

ii. de translaties in Y richting $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & d_2 \\ 0 & 0 & 1 \end{pmatrix}$

iii. de <u>rotaties</u> $\begin{pmatrix} c & s & 0 \\ -s & c & 0 \\ 0 & 0 & 1 \end{pmatrix}$

We hadden verstandiger bij de affiene transformaties de translaties direct af kunnen splitsen. Iedere affiene transformatie is te schrijven als het product van een translatie en een affiene transformatie met O als dekpunt.

$$\begin{pmatrix} 1 & 0 & d_1 \\ 0 & 1 & d_2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a_1 & b_1 & 0 \\ a_2 & b_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ 0 & 0 & 1 \end{pmatrix}$$

We bestuderen nu de groep van de <u>affiene transformaties</u> met O als dekpunt. We kunnen ze kenmerken door:

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$$

Onder deze transformaties is voor ieder tweetal punten (x_1, y_1) en (x_2, y_2), die met O op een rechte lijn liggen de verhouding

$\dfrac{x_1}{x_2} = \dfrac{y_1}{y_2}$ invariant.

We hebben de ondergroep van de <u>gelijkvormigheidstransformaties</u> met O als dekpunt:

$\begin{pmatrix} c & s \\ -s & c \end{pmatrix}$ en $\begin{pmatrix} c & s \\ s & -c \end{pmatrix}$

De invarianten zijn o.a.

$$\frac{x_1^2 + y_1^2}{x_2^2 + y_2^2} \quad \text{en} \quad \frac{(x_1 x_2 + y_1 y_2)^2}{(x_1^2 + y_1^2)(x_2^2 + y_2^2)}$$

De ondergroep van de <u>congruenties</u> met O als dekpunt wordt gevormd door de rotaties en rotaties gevolgd door een spiegeling:

$\begin{pmatrix} c & s \\ -s & c \end{pmatrix}$ met $c^2 + s^2 = 1$; $\begin{pmatrix} c & s \\ s & -c \end{pmatrix}$ met $c^2 + s^2 = 1$.

De invarianten zijn nu $x^2 + y^2$ en $x_1 x_2 + y_1 y_2$.

<u>Opmerking</u>: Er zijn nog meer ondergroepen, we wijzen b.v. op de ondergroep van de affiene transformaties, die gevormd wordt door

alle transformaties

$$\begin{pmatrix} a_1 & b_1 & d_1 \\ 0 & b_2 & d_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Voorbeelden.

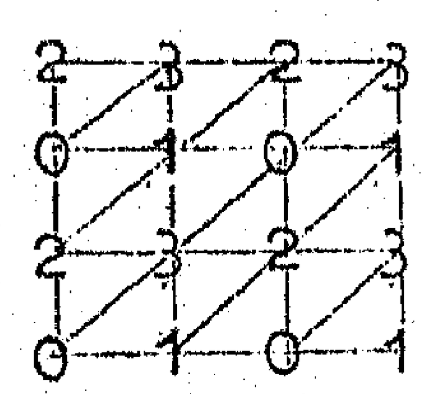
We beschouwen meetkunden waarin o.a. aan de volgende axioma's voldaan is:

i. door iedere 2 punten gaat één rechte.

ii. door ieder punt buiten een rechte ℓ gaat één rechte $/\!/ \ \ell$.

I Meetkunde met 4 punten.

We nummeren de punten 0,1,2,3 en de rechten 01,02,03,12,13,23. Hierbij geldt 01 // 23, 02 // 13, 03 // 12. Deze meetkunde is b.v. gerealiseerd in de figuur van de hoekpunten en ribben van een viervlak indien we overstaande ribben "evenwijdig" noemen. Een andere realisatie levert ons de analytische meetkunde van punten waarvan de coördinaten gehele getallen modulo 2 zijn.



gelijk genummerde punten zijn identiek.
rechten, die twee gelijkgenummerde punten gemeen hebben zijn identiek.
er zijn 4 punten, 2 horizontale, 2 verticale en 2 diagonale rechten.

We beschouwen nu de groep van de affiene transformaties $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$

Ligging van de punten na de transformaties:

23	31	12	13	32	21
01	02	03	02	01	03

Transformatormatrices:

$$E\begin{pmatrix}1&0\\0&1\end{pmatrix} \quad A\begin{pmatrix}1&1\\1&0\end{pmatrix} \quad B\begin{pmatrix}0&1\\1&1\end{pmatrix} \quad C\begin{pmatrix}0&1\\1&0\end{pmatrix} \quad D\begin{pmatrix}1&1\\0&1\end{pmatrix} \quad F\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

Groepentafel

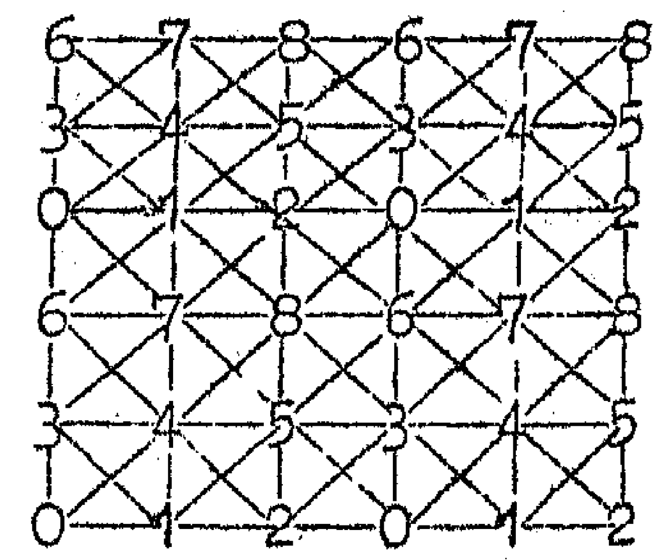
EABCDF
ABEDFC
BEAFCD
CFDEBA
DCFAEB
FDCBAE

Ondergroepen:
Gelijkvormige = congruente groep E,C geen normaaldeler.
de groepen E,D en E,F zijn geen normaaldeler.
de groep E,A,B is een normaaldeler.

II Meetkunde met 9 punten.

Analytische Meetkunde van punten met gehele coördinaten modulo 3. Er zijn 9 punten en 4 stel van 3 onderling evenwijdige rechten:

$\begin{cases}012\\345\\678\end{cases}$ $\begin{cases}036\\147\\258\end{cases}$ $\begin{cases}048\\156\\237\end{cases}$ $\begin{cases}057\\138\\246\end{cases}$



Door ieder punt gaan 4 rechten, op iedere rechte liggen 3 punten.

Er zijn 48 affiene transformaties met 0 als dekpunt.

De 8 congruenties (rotaties met of zonder spiegeling) zijn:

$\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix}$ en $\begin{pmatrix}0 & \pm1\\ \pm1 & 0\end{pmatrix}$.

De overige 8 gelijkvormigheidstransformaties zijn:

$\begin{pmatrix}\pm1 & \pm1\\ \pm1 & \pm1\end{pmatrix}$; tekens zo kiezen dat òf 1 plus en 3 min òf 1 min en 3 plus.

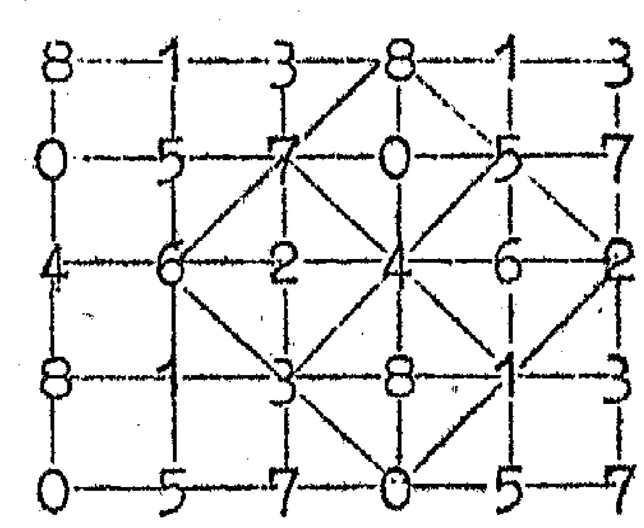
De overige 32 affiene transformaties zijn:

$\begin{pmatrix}0 & \pm1\\ \pm1 & \pm1\end{pmatrix}$, $\begin{pmatrix}\pm1 & 0\\ \pm1 & \pm1\end{pmatrix}$, $\begin{pmatrix}\pm1 & \pm1\\ 0 & \pm1\end{pmatrix}$ en $\begin{pmatrix}\pm1 & \pm1\\ \pm1 & 0\end{pmatrix}$.

Voorbeeld van een gelijkvormigheidstransformatie:

We kiezen $\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$

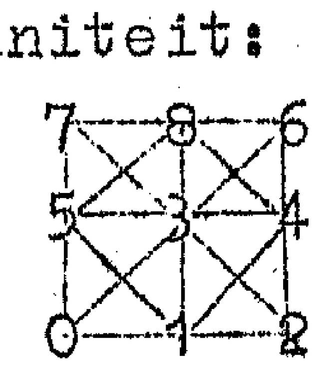
Op te bouwen uit een rotatie over 45 en een vermenigvuldiging uit 0 met $\sqrt{2}$



Voorbeeld van een niet-gelijkvormige affiniteit:

We kiezen $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$

In de oorspronkelijke figuur was $01 \perp 03$, dit is bij de transformatie verloren gegaan



VC 4

Syllabus
Vacantiecursus 1949

Prof. Dr C. Visser.

Inleiding

Het begrip groep is nauw verbonden met het begrip symmetrie. Wij spreken van symmetrie, wanneer een geheel is opgebouwd uit delen, die alle op dezelfde manier in het geheel zijn geplaatst.

Beschouwing van enige voorbeelden van symmetrie.

Wiskundige formulering van het begrip symmetrie door het begrip symmetrisch ensemble. Daaronder verstaan we een verzameling van objecten A, B,... met een gelijkheidsrelatie (A:B=C:D) voor geordende paren, die de volgende eigenschappen heeft:

1. De gelijkheid is transitief (als A:B=C:D en C:D=E:F, dan A:B=E:F), reflexief (A:B=A:B) en omkeerbaar (als A:B=C:D, dan C:D=A:B).

2. Als A:B=P:Q en B:C=Q:R, dan A:C=P:R.

3. A:A=B:B.

4. Als A:B=C:D, dan B:A=D:C.

5. Bij A, B, C, een ondubbelzinnig bepaalde D zodanig, dat A:B=C:D.

Twee symmetrische ensembles, die één-aan-één op elkaar kunnen worden afgebeeld op zodanige wijze, dat de gelijkheid van paren invariant is, heten isomorph.

Een groep is een verzameling van elementen a,b,... met de volgende byzonderheden:

1. Elk tweetal elementen a,b kan in die volgorde worden gecomponeerd tot een element ab.

2. ab.c=a.bc, associativiteit van de compositie.

3. Een der elementen - eenheidselement, e - heeft de eigenschap, dat ae=ea=a voor elke a.

4. Bij iedere a is er een element a^{-1}, inverse van a, zodanig dat $aa^{-1}=e$.

Onmiddellijke consequenties: Er is slechts één eenheidselement; a is inverse van a^{-1}; ieder element heeft slechts één inverse. Bij gegeven a en b is er één x zodanig, dat $ax=b$, nl. $x=a^{-1}b$, en één y zodanig, dat $ya=b$, nl. $y=ba^{-1}$. Uit $ab=ac$, en eveneens uit $ba=ca$, volgt $b=c$.

Onder de orde van een groep verstaat men het aantal der elementen; de orde kan eindig of oneindig zijn. Is voor elke a en b voldaan aan $ab=ba$, dan heet de groep commutatief of abels.

Twee groepen, die één-aan-één op elkaar kunnen worden afgebeeld op zodanige wijze, dat de compositie invariant is, heten isomorph.

Onder een automorphisme van een symmetrisch ensemble verstaan we een afbeelding $X \to X'$ van het ensemble op zichzelf met de eigenschap, dat $A':B'=A:B$. De automorphismen van een symmetrisch ensemble vormen een groep (de compositie ab van de automorphismen a en b is het automorphisme, dat we krijgen door de afbeelding a te laten volgen door de afbeelding b).

Omgekeerd kan men aan iedere groep een symmetrisch ensemble toevoegen, waarvan de automorphismengroep isomorph is met die groep. Deze toevoeging is op isomorphie (van groep en symmetrisch ensemble) na eenduidig. De theorie der symmetrische ensembles is dus equivalent met de theorie der groepen.

Voorbeelden van groepen.

Eerste beginselen van de theorie der groepen.

Is H een ondergroep van de groep G, dan zijn de "complexen" Ha en Hb identiek of geheel buiten elkaar gelegen. G valt dus uiteen in complexen Ha (rechtse nevenklassen van H). Ook kan men G splitsen in linkse nevenklassen aH. x en y behoren dan en dan alleen tot dezelfde rechtse (linkse) nevenklasse van H, als xy^{-1} $(x^{-1}y)$ in H ligt.

Stelling van Lagrange. Is G van eindige orde, dan is de orde van een ondergroep H een deler van de orde G. Het quotient heet de index van H in G.

Gevolgen: De orde (of periode) van elk element van G is een deler van de orde van G. Een groep, waarvan de orde een priemgetal is, is cyclisch.

Geconjugeerde elementen. a en b heten geconjugeerd, als $s^{-1}as=b$. Deze relatie is reflexief, omkeerbaar en transitief, zodat G uiteenvalt in klassen van geconjugeerde elementen. Het eenheidselement vormt een klasse op zichzelf.

Stelling. In een eindige groep is het aantal der elementen van een klasse een deler van de orde van de groep.

Bij de afbeelding $x \to s^{-1}xs$ van G op G is de compositie invariant. Het is dus een isomorphe afbeelding van G op G, een automorphisme van G; een automorphisme van deze soort heet een inwendig automorphisme. Een ondergroep H gaat daarbij over in een zgn. geconjugeerde ondergroep $s^{-1}Hs$.

Normaaldeler. Een ondergroep, die identiek is met de geconjugeerde ondergroepen, heet normaaldeler (met zichzelf geconjugeerde ondergroep, invariante ondergroep). Equivalente defitie: een normaaldeler is een ondergroep, waarbij linkse en rechtse nevenklassen identiek zijn.

Neemt men uit twee nevenklassen C_1 en C_2 van een normaal deler N representerende elementen a_1 en a_2, dan ligt $a_3 = a_1a_2$ in een nevenklasse C_3, die onafhankelijk is van de gekozen representanten, dus alleen afhangt van C_1 en C_2. De compositie $C_1C_2 = C_3$ maakt de verzameling der nevenklassen tot een groep. Deze heet de factorgroep $G|N$ van G naar N.

Een (groep-)homomorphisme is een afbeelding $x \longrightarrow x'$ van een groep G op een groep G' zodanig, dat, als ab=c, ook $a'b' = c'$. Is de afbeelding één-aan-één, dan spreekt men van een isomorphisme.

Beschouw nu een normaaldeler N en zijn factorgroep $G|N$. De afbeelding $x \longrightarrow$ de nevenklasse, waarin x ligt is een homomorphisme van G op $G|N$.

Omgekeerd: Is $G \longrightarrow G'$ een homomorphisme, dan vormen de elementen van G, die op het eenheidselement van G' worden afgebeeld, een normaaldeler N in G; de elementen, die op een willekeurig element van G' worden afgebeeld, vormen een nevenklasse van N en de toevoeging element van $G' \longrightarrow$ deze nevenklasse is een isomorphisme van G' met $G|N$.

Een groep G, die behalve e en G geen normaaldelers heeft, heet enkelvoudig. De alternerende permutatiegroep van 5 of meer variabelen is enkelvoudig. Daaruit vloeit in de theorie van Galois voort, dat de algemene n^{de} machtsvergelijking voor $n \geq 5$ onoplosbaar is met behulp van worteltekens.

Een keten $G = G_0 \supset G_1 \supset \ldots\ldots \supset G_r = e$, waarbij iedere G_i maximale normaaldeler is in G_{i-1}, heet een <u>compositiereeks</u> van G.

<u>Stelling van Jordan-Hölder.</u> Twee compositiereeksen van G zijn even lang en de factorgroepen $G_i \mid G_{i+1}$ van de ene reeks zijn, in een of andere volgorde, isomorph met die van de andere.
