STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 17.

Colloquim structuurtheorie der ringen.incompl.

W.Peremans.

1951

MATHEMATISCH CENTRUM
2de Boerhaavestr. 49
A M S T E R D A M O.

1950/51

Colloquium Structuurtheorie der ringen.

Inleiding

door

Dr W. Peremans

We gaan uit van een commutatieve groep G, waarvan de groepoperatie als optelling geschreven wordt. Een homomorfe afbeelding A van G in zich zelf heet een endomorfie. Daarvoor geldt dus

$$A(x+y) = Ax+Ay.$$

We definiëren nu som en product van twee endomorfieën door

$$(A+B)x = Ax+Bx$$
$$(AB)x = A(Bx).$$

Het is makkelijk na te gaan dat het resultaat weer een endomorfie is en dat de endomorfieën van G t.o.v. deze operaties een ring vormen.

Laat nu G de additieve groep van een ring R zijn. Dan kunnen we aan een element a toevoegen de afbeelding A=F(a) van de ring in zich zelf, die gedefinieerd wordt door Ax = ax. Uit de ringaxioma's volgt dan

$$F(a)\,(b+c) = a(b+c) = ab + ac = F(a)b + F(a)c.$$
$$F(a+b)c = (a+b)c = ac + bc = F(a)c + F(b)c = (F(a) + F(b))c$$
$$F(ab)c = (ab)c = a(bc) = a(F(b)c) = F(a)(F(b)c) = (F(a)F(b))c.$$

Hieruit blijkt dat F(a) een endomorfie is dat de afbeelding $a \to F(a)$ een ringhomomorfie is van R in de ring van endomorfieën van zijn additieve groep. Als R een één heeft (een element e waarvoor geldt ea = ae = a), dan is de homomorfie zelfs eeneenduidig (dus een isomorfie), want uit $a \neq b$ volgt $F(a)e = ae = a \neq b = be = F(b)e$. In het algemeen behoeft de afbeelding niet eeneenduidig te zijn; men bedenke dat men uitgaande van een willekeurige commutatieve groep een ring kan krijgen door te definiëren ab = 0 voor alle a en b. In zo'n ring is F(a) voor alle a de nulendormofie 0x = 0.

De doorsnede $H \cap K$ van twee ondergroepen van een commutatieve groep G is een ondergroep. De groep voortgebracht door een willekeurige deelverzameling V van G is de kleinste ondergroep van G die V omvat, dat is de verzameling van de eindige sommen $\sum \pm a_i (a_i \in V)$. De groep voortgebracht door de vereniging van twee ondergroepen H en K is de som van H en K: (H,K) bestaande uit de elementen $a + b$ ($a \in H$, $b \in K$). Als uit $a_1 + b_1 = a_2 + b_2$ ($a_i \in H$, $b_i \in K$) volgt $a_1 = a_2$, $b_1 = b_2$ dan heet de som een directe som van H en K: H + K. De structuur van de directe

som van H en K is door H en K alleen (dus onafhankelijk van G) bepaald. Deze is n.l. isomorf met de z.g. abstracte directe som van H en K die als volgt verkregen wordt: vorm de verzameling van de paren (a,b) met $a \in H$ en $b \in K$ en definieer $(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$. Deze is een groep die isomorf is met de directe som van $\bar{H}$ bestaande uit (a,0) isomorf met H en $\bar{K} = (0,b)$ isomorf met K.

Een deelverzameling S van een ring R heet een rechtsideaal (r-ideaal) resp. linksideaal (l-ideaal), als zij een additieve groep is en als uit $s \in S$, $r \in R$ volgt $ar \in S$ (resp. $ra \in S$). Een verzameling die zowel r-ideaal als l-ideaal is heet een ideaal (tweezijdig ideaal). Bij een ringhomomorfe afbeelding van R op een ring R' is de verzameling der elementen die in 0 van R' worden afgebeeld een ideaal S en R' is ringisomorf met de restklassenring R(mod S).

De doorsnede van twee r-idealen (resp. l-idealen) van een ring R is een r-ideaal (resp. l-ideaal). Het r-ideaal voortgebracht door een deelverzameling V van R is het kleinste r-ideaal dat V omvat. Het bestaat uit de elementen $\sum(a_i r_i + n_i a_i)$ met $a_i \in V$, $r_i \in R$, n_i gehele getallen. Analoog voor l-idealen: $\sum(r_i a_i + n_i a_i)$ en idealen $\sum(a_i r_i + s_i a_i + t_i a_i u_i + n_i a_i)$ met $a_i \in V$; $r_i, s_i, t_i, u_i \in R$ en n_i gehele getallen. Als R een één heeft kunnen de termen met gehele coëfficiënten weggelaten worden. Als V uit eindig veel elementen $a_1, \ldots, a_n$ bestaat wordt het ideaal voortgebracht door V geschreven $(a_1, \ldots, a_n)$. Een ideaal (a) heet een hoofdideaal. De som (V,W) van twee deelverzamelingen V en W is de verzameling der $a+b (a \in V, b \in W)$. Als V en W beide r-idealen, l-idealen of idealen zijn is hun som hetzelfde. Het product VW van twee deelverzamelingen V en W is de verzameling der $\sum a_i b_i (a_i \in V, b_i \in W)$. Als V uit slechts één element a bestaat schrijven we ook wel aW. Analoog Vb. Het is een r-ideaal, als W een r-ideaal is, een l-ideaal als V een l-ideaal is. Als een ring directe som is van twee idealen A+B, dan is AB de nulring (we schrijven dit ook AB = 0) want als $a \in A, b \in B$,

dan is $ab \in A$ en $ab \in B$ en dus $ab = 0$. Dan is voor $a_i \in A$, $b_i \in B$ $(a_1 + b_1)(a_2 + b_2) = a_1 a_2 + b_1 b_2$. De structuur van de ring is dan volledig bepaald door die van A en B.

Een ideaal P heet een priemideaal als voor twee idealen A en B met $AB \subset P$, geldt $A \subset P$ of $B \subset P$. Deze definitie wijkt af van de in de commutatieve ideaaltheorie gebruikelijke, n.l. P heet een priemideaal als uit $ab \in P$ volgt $a \in P$ of $b \in P$ (d.w.z. de restklassenring naar P bevat geen nuldelers). We tonen aan dat deze twee definities voor commutatieve ringen op hetzelfde neerkomen. In een commutatieve ring geldt n.l. (ab) = (a)(b), immers $(r a + na)(s b + mb) = (rs + mr + ns) ab + mn ab$. Laat P priemideaal volgens de eerste definitie zijn en $ab \in P$, $a \notin P$, dan is $(a)(b) = (ab) \subset P$ en $(a) \not\subset P$, dus $(b) \subset P$, dus $b \in P$. Laat omgekeerd P priemideaal zijn volgens de tweede definitie en A en B twee idealen met $AB \subset P$, $A \not\subset P$. Dan is er een $a \in A$ met $a \notin P$. Neem een willekeurige $b \in B$,

dan is $ab \in AB$, dus $ab \in P$, $a \notin P$, dus $b \in P$. Dus $D \subset P$.

We merken nog op dat een ring met één e een deelring $\neq 0$ met één e' kan bezitten, zodat $e \neq e'$. We nemen b.v. de ring met de vier elementen 0,a,b,e en de optellings- en vermenigvuldigingstabel:

+	0	a	b	e
0	0	a	b	e
a	a	0	e	b
b	b	e	0	a
e	e	b	a	0

·	0	a	b	e
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
e	0	a	b	e

De verzameling $\{0,a\}$ is een lichaam met a als één.

We beschouwen nu een groep G en een verzameling Ω van endomorfieën van G; deze worden ook wel operatoren genoemd. Een ondergroep H heet een Ω-ondergroep (toegelaten ondergroep), als voor een $A \in \Omega$ en een $h \in H$ geldt $Ah \in H$ (kort geschreven $\Omega H \subset H$). Men bedenke dat twee operatoren die op G verschillend zijn, op H gelijk kunnen zijn. Als H een normale Ω-ondergroep van G is, kan men de operatoren ook definiëren voor de factorgroep door $A(H + x) = H + Ax$. Dit is inderdaad een endomorfie, want $A(H+(x+y)) = H+A(x+y) = H+(Ax+Ay)$ en $A(H+x)+A(H+y)=(H+Ax)+(H+Ay)=H+(Ax+Ay)$. Alle dergelijke groepen heten Ω-groepen. Een homomorfie B van een Ω-groep G op een Ω-groep G' heet een Ω-homomorfie als het een homomorfie is en $BA = AB$ voor alle $A \in \Omega$. Evenzo Ω-isomorfie, Ω-endomorfie. De Ω-endomorfieën van G zijn dus die elementen van de endomorfieëring die met Ω verwisselbaar zijn. Als G tevens additieve groep van een ring is, spreken we ook van Ω-idealen enz.

We beschouwen nu n-rijige vierkante matrices (a_{ij}) met elementen uit een ring R. We schrijven ze $\Sigma' e_{ij}\, a_{ij}$ en definiëren $(\Sigma' e_{ij}a_{ij}) + (\Sigma' e_{ij}b_{ij}) = \Sigma' e_{ij}(a_{ij}+b_{ij})$; $(\Sigma' e_{ij}a_{ij})(\Sigma' e_{ij}b_{ij}) = \Sigma' e_{ij}(\sum_{k=1}^{n} a_{ik}b_{kj})$.

De matrices vormen dan een ring, de <u>volle matrixring R_n</u>. Deze bevat een deelring isomorf met R, n.l. bestaande uit de elementen $\Sigma' e_{ij}(a\delta_{ij})$, waarin δ_{ij} het Kronecker-symbool is:

$\delta_{ij} = 0$ als $i \neq j$ en $\delta_{ij} = 1$ als $i = j$. Als R geen één heeft is δ_{ij} geen element van de ring en moeten we het dus zo opvatten, dat $a\,\delta_{ij} = 0$ als $i \neq j$, en $a\,\delta_{jj} = a$ als $i = j$. We identificeren deze deelring met R dan is $R \subset R_n$. Als R een één heeft definiëren we $E_{pq} = \Sigma' e_{ij}\,(\delta_{ip}\,\delta_{jq})$ dat is de matrix met op het snijpunt van de p^e rij en de q^e kolom een 1 en elders nullen en dan is $\Sigma' e_{ij}a_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n} E_{ij}a_{ij}$, want $\sum_{k=1}^{n}\sum_{l=1}^{n} E_{kl}a_{kl} =$

$$= \sum_{k=1}^{n}\sum_{l=1}^{n}\Big(\Big(\sum{}' e_{ij}(\delta_{ik}\delta_{jl})\Big)\Big(\sum{}' e_{ij}(a_{kl}\delta_{ij})\Big) =$$

$$= \sum_{k=1}^{n}\sum_{l=1}^{n}\sum{}' e_{ij}\Big(\sum_{m=1}^{n}\delta_{ik}\delta_{ml}\delta_{mj}a_{kl}\Big) = \sum{}' e_{ij}\Big(\sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n}\delta_{ik}\delta_{ml}\delta_{mj}a_{kl}\Big) =$$

$= \sum{}' e_{ij}a_{ij}$. Verder geldt $E_{ij}E_{kl} = \delta_{jk}E_{il}$, $\sum_{i=1}^{n} E_{ii} = 1$ en voor $a \in R$: $aE_{ij} = E_{ij}a$. Als omgekeerd S een ring met één 1 is en elementen $F_{ij}(i,j = 1,\ldots,n)$ bevat, die voldoen aan $F_{ij}F_{kl} = \delta_{jk}F_{il}$ en $\sum_{i=1}^{n} F_{ii} = 1$ en S bevat een deelring R zodat $1 \in R$, $aF_{ij} = F_{ij}a$ voor alle $a \in R$ en ieder element van S is op één en slechts één wijze te schrijven in de gedaante $\sum_{i=1}^{n}\sum_{j=1}^{n} F_{ij}a_{ij}$, dan is S isomorf met R_n.

We bewijzen nu twee stellingen over matrixringen K_n, als K een scheef lichaam (niet-commutatief lichaam) is. We noemen een ring enkelvoudig als zij geen idealen bezit behalve het nulideaal en de ring zelf. We noemen een l-ideaal van een ring irreducibel als de ring geen l-idealen bevat die in het gegeven l-ideaal bevat zijn, behalve het nulideaal en het l-ideaal zelf (analoog voor r-ideaalen en idealen).

De ring K_n is enkelvoudig, als K een scheef lichaam is.

Bewijs: Neem een ideaal $A \neq 0$ in K_n en hierin een element $a = \sum E_{ij}a_{ij} \neq 0$.

Nu is $\sum_{k=1}^{n} E_{kp}\, a\, E_{qk} = a_{pq}$ dus $a_{pq} \in A$ voor alle p en q, maar deze zijn niet alle = 0, dus er is een $b \neq K$ met $b \in A$, maar dan is ook $b\,b^{-1} = 1 \in A$, dus $A = K_n$.

Als K een scheef lichaam is, is de ring K_n een directe som van n irreducibele l-idealen, die onderling isomorf zijn.

Bewijs: Voor een vaste k is K_nE_{kk} een l-ideaal. Het bestaat blijkbaar uit de elementen van de vorm $\sum_i E_{ik}a_{ik}$ (matrices waarin overal buiten de k^e kolom nullen staan). Laat A een l-ideaal $\neq 0$ zijn, bevat in K_nE_{kk} en hierin een element $a = \sum_i E_{ik}a_{ik} \neq 0$ en wel met $a_{pk} \neq 0$, dan is $E_{kk} = E_{kp}a_{pq}^{-1}a \in A$ dus $K_nE_{kk} \subset A$, dus $K_nE_{kk} = A$. Dus K_nE_{kk} is irreducibel. Klaarblijkelijk zijn alle K_nE_{kk} isomorf en is $K_n = K_nE_{11}+\ldots+K_nE_{nn}$ een directe som.

Een commutatieve groep G met een operatorenverzameling ϕ die een scheef lichaam is, dat de identieke endomorfie bevat, heet een vectorruimte. De identieke endomorfie is dan natuurlijk de één van ϕ. Daar in ϕ ieder element $\neq 0$ een inverse (links- en tevens rechtsinverse) bezit, zijn alle endomorfieën van ϕ eeneenduidige endomorfieën van G op zichzelf; in ϕ zijn alle elementen $\neq 0$ automorfieën van G (isomorfe afbeeldingen van G op zich zelf). Een ϕ-ondergroep van G heet een deelruimte.

De elementen van Φ heten scalaren; we schrijven ze met kleine Griekse letters. Dan geldt dus $\alpha(a+b) = \alpha a + \alpha b, (\alpha + \beta)a = \alpha a + \beta a, (\alpha\beta)a = \alpha(\beta a)$, $1a = a$; dat zijn juist de eisen die men gewoonlijk aan een vectorruimte stelt naast de eis dat ze een groep is en de scalaren een lichaam (in ons geval een scheef lichaam) vormen. Er moet verder nog gelden dat uit $\alpha x = \beta x$ voor alle x volgt dat $\alpha = \beta$, hetgeen zo is mits G niet de nulgroep is. We stellen nu nog de eis dat de ruimte eindig dimensionaal is, d.w.z. er zijn elementen $a_1, \ldots, a_n$ zodat ieder element te schrijven is als $\alpha_1 a_1 + \ldots + \alpha_n a_n$. We laten nu van de a_i zoveel weg tot ze een minimaal stelsel (basis) vormen, d.w.z. tot verdere weglating leidt tot verlies van de eigenschap dat ieder element van G als lineaire combinatie is te schrijven. Onder de systemen a_i zijn de bases gekarakteriseerd door de eigenschap, dat de schrijfwijze $\sum \alpha_i a_i$ eenduidig bepaald is (of dat uit $\sum \alpha_i a_i = 0$ volgt $\alpha_i = 0$ voor alle i). Immers, als $\sum \alpha_i a_i = 0$ en b.v. $\alpha_1 \neq 0$ dan is $a_1 = \sum_{i=2}^{n} (-\alpha_1^{-1}\alpha_i)a_i$, dus a_1 kan weggelaten worden. Omgekeerd als a_1 weggelaten kan worden is $a_1 = \sum_{i=2}^{n} \alpha_i a_i$ en $a_1 + \sum_{i=2}^{n} (-\alpha_i)a_i = 0$. We bewijzen nu dat het aantal elementen van een basis van G constant is. Stel twee bases $a_1, \ldots, a_n$ en $b_1, \ldots b_m$ en $m < n$. Dan is $b_1 = \sum_{i=1}^{n} \beta_{1i} a_i$ en niet alle $\beta_{1i} = 0$, b.v. $\beta_{11} \neq 0$. Dan is $a_1 = \beta_{11}^{-1} b_1 + \sum_{i=2}^{n} (-\beta_{11}^{-1}\beta_{1i})a_i$, dus $b_1, a_2, \ldots, a_n$ is een stelsel waarin alle elementen van G uit te drukken zijn. Het is echter zelfs een basis; stel n.l. $0 = \xi_1 b_1 + \sum_{i=2}^{n} \xi_i a_i = \xi_1 \beta_{11} a_1 + \sum_{i=2}^{n} (\xi_1 \beta_{1i} + \xi_i)a_i$ dus $\xi_1 \beta_{11} = 0$, $\xi_1 = 0$, maar uit $\sum_{i=2}^{n} \xi_i a_i = 0$ volgt $\xi_i = 0$. Stel nu k elementen a_i door b_i vervangen: $b_1, \ldots, b_k, a_{k+1}, \ldots, a_n$ zodat dit systeem een basis is. Dan is $b_{k+1} = \sum_{i=1}^{k} \beta_{k+1,i} b_i + \sum_{i=k+1}^{n} \gamma_{k+1,i} a_i$. Niet alle $\gamma_{k+1,i}$ zijn nul, omdat $b_1, \ldots, b_m$ een basis is, b.v. $\gamma_{k+1,k+1} \neq 0$. Dan is weer als boven a_{k+1} uit te drukken in $b_1, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots a_n$. Dit systeem is nu een basis van G want uit $0 = \sum_{i=1}^{k+1} \xi_i b_i + \sum_{i=k+2}^{n} \xi_i a_i = \sum_{i=1}^{k} (\xi_{k+1}\beta_{k+1,i} + \xi_i)b_i + \xi_{k+1}\gamma_{k+1,k+1} a_{k+1} + \sum_{i=k+2}^{n} (\xi_{k+1}\gamma_{k+1,i} + \xi_i)a_i$ volgt $\xi_{k+1}\gamma_{k+1,k+1} = 0$, $\xi_{k+1} = 0$, maar uit $\sum_{i=1}^{k} \xi_i b_i + \sum_{i=k+1}^{n} \xi_i a_i = 0$ volgt $\xi_i = 0$ voor alle i. We kunnen hiermee doorgaan tot we vinden dat $b_1, \ldots, b_m, a_{m+1}, \ldots a_n$ een basis is, maar dat is niet zo want $a_{m+1}, \ldots a_n$ zijn eruit weg te laten. Evenzo weerlegt men $m > n$; dus $m = n$.

Een Φ- endomorfie A van G heet een <u>lineaire transformatie</u> van G over Φ. Nu vormen in iedere ring de elementen, die verwisselbaar zijn met de elementen van een vaste deelverzameling van de ring, zelf een ring.

Dus is de verzameling lineaire transformaties een deelring L van de endomorfieënring van G. Als A een lineaire transformatie is en $a_1,\ldots,a_n$ is een basis van G over ϕ, dan is A volledig bepaald door de beelden Aa_i; want als $x = \sum \xi_i a_i$, dan is $Ax = A\sum \xi_i a_i = \sum A\xi_i a_i = \sum \xi_i (Aa_i)$. Omgekeerd als we n willekeurige elementen $y_1,\ldots,y_n$ uit G kiezen is de afbeelding $\sum \xi_i a_i \rightarrow \sum \xi_i y_i$ een lineaire transformatie A, waarvoor $Aa_i = y_i$. In het byzonder is er bij iedere $\alpha \in \phi$ één en slechts één lineaire transformatie α' zodat $\alpha' a_i = \alpha a_i$. Men bedenke dat α' behalve van α ook van de keuze van de basis afhangt. Volgens deze toevoeging is $(\alpha' + \beta')a_i = \alpha' a_i + \beta' a_i = \alpha a_i + \beta a_i = (\alpha+\beta)a_i = (\alpha+\beta)' a_i$ en $(\alpha'\beta')a_i = \alpha'(\beta' a_i) = \alpha'(\beta a_i) = (\alpha'\beta')a_i = (\beta\alpha')a_i = \beta(\alpha' a_i) = \beta(\alpha a_i) = (\beta\alpha)a_i = (\beta\alpha)' a_i$. De toevoeging is verder natuurlijk eeneenduidig. De α' vormen dus een scheef lichaam ϕ' dat <u>invers-isomorf</u> (of <u>anti-isomorf</u>) is met ϕ (daarmee is bedoeld een eeneenduidige toevoeging $\alpha \rightarrow \alpha'$ zodat uit $\alpha \rightarrow \alpha'$ en $\beta \rightarrow \beta'$ volgt $\alpha+\beta \rightarrow \alpha'+\beta'$ en $\alpha\beta \rightarrow \beta'\alpha'$). Nu is G ook een vectorruimte over ϕ'. Dan is ieder element blijkbaar te schrijven in de vorm $\sum \xi_i' a_i$, dus $a_1,\ldots,a_n$ vormen dan ook een basis en G is n-dimensionaal over ϕ'. De endomorfieën $\alpha \in \phi$ zijn verwisselbaar met de elementen van ϕ' en vormen dus lineaire transformaties van G over ϕ'; ze zijn blijkbaar op dezelfde wijze aan α' toegevoegd als eerst α' aan α; dus $(\alpha')' = \alpha$.

Noem E_{ij} de lineaire transformatie van G over ϕ gedefinieerd door $E_{ij}a_r = \delta_{jr}a_i$. Dan is $(E_{ij}\alpha')a_r = \alpha\delta_{jr}a_i = (\alpha' E_{ij})a_r$, dus E_{ij} is ook een lineaire transformatie van G over ϕ'. Als A een willekeurige lineaire transformatie is met $Aa_r = \sum_i \alpha_{ir}a_i$ dan is ook $(\sum_{ij} E_{ij}\alpha'_{ij})a_r = \sum_i \alpha_{ir}a_i$, dus $A = \sum_{ij} E_{ij}\alpha'_{ij}$. Omgekeerd is iedere $\sum_{ij} E_{ij}\alpha'_{ij}$ een lineaire transformatie A, waarvoor geldt $Aa_r = \sum_i \alpha_{ir}a_i$. Iedere lineaire transformatie is dus op één en slechts één wijze te schrijven in de vorm $\sum_{ij} E_{ij}\alpha'_{ij}$, met $\alpha'_{ij} \in \phi'$. Tenslotte geldt $E_{ij}E_{kl} = \delta_{jk}E_{il}$ en $\sum_i E_{ii} = 1$. Dus L isomorf met ϕ'_n:

De ring van de lineaire transformaties van een n-dimensionale vectorruimte over een scheef lichaam ϕ is isomorf met de matrixring ϕ'_n, waarin ϕ' een scheef lichaam is, invers-isomorf met ϕ.

We willen nu het centrum C van L karakteriseren. Onder het centrum van een ring verstaat men de verzameling der elementen a waarvoor geldt $ax = xa$ voor alle elementen der ring (dus de elementen die met alle elementen der ring verwisselbaar zijn). Zoals we al eerder zagen geldt voor de elementen van een matrixring ϕ'_n: $\alpha'_{pq} = \sum_k E_{kp}(\sum_{ij} E_{ij}\alpha'_{ij})E_{qk}$. Als $A = \sum_{ij} E_{ij}\alpha'_{ij} \in C$ dan is A verwisselbaar met alle E_{kl} en daaruit volgt $\delta_{pq}A = \alpha'_{pq}$, dus $\alpha'_{pq} = 0$ als $p \neq q$ en $\alpha'_{pp} = A$ voor alle p, dus $A = \alpha' \in \phi'$, dus C is het centrum van ϕ'. Om het centrum van ϕ te bepalen, bedenken we, dat dit blijkbaar gelijk is aan $\phi \cap \phi'_n$

is bevat in het centrum van ϕ'_n en dus in ϕ'. Dus is het centrum van ϕ gelijk aan $\phi \cap \phi'$. Om redenen van symmetrie is dan ook het centrum van ϕ' gelijk aan $\phi \cap \phi'$ en dus is $C = \phi \cap \phi'$. Als ϕ commutatief is, is $\alpha' = \alpha$ en dus onafhankelijk van de keuze van de basis. ϕ is dan het centrum van L.

We merken op, dat naast de op pg.1 voor een ring R gedefinieerde ring der linksvermenigvuldigingen, ook een ring der rechtsvermenigvuldigingen $G(a)x = xa$ bestaat die anti-homomorf is met R.

We gaan nu uit van een n-dimensionale vectorruimte G over een (commutatief)lichaam ϕ en nemen aan dat G nu additieve groep is van een ring R en wel zo dat in de endomorfieënring zowel de elementen van de ring der linksvermenigvuldigingen als die van de ring der rechtsvermenigvuldigingen verwisselbaar zijn met ϕ. Dan heet R een <u>hypercomplex systeem</u> of een (associatieve) <u>algebra</u> over ϕ. Dat betekent dat aan de eisen van een vectorruimte wordt toegevoegd, dat ϕ commutatief is, dat er in R een vermenigvuldiging gedefiniëerd is zodat R een ring is, en dat voor $\alpha \in \phi$, $a \in R$, $b \in R$ geldt $(\alpha a)b = a(\alpha b) = \alpha(ab)$. Als R een één e heeft vormen de α e een deelsysteem van R isomorf met ϕ en kunnen we R opvatten als een uitbreiding van ϕ. Dan is tevens ieder ideaal een ϕ-ideaal.

In een algebra geldt $(\alpha a)(\beta b) = (\alpha\beta)(ab)$. Daaruit volgt dat door de vermenigvuldiging van de basiselementen, die van de elementen van de hele algebra bepaald is, want als $a_i a_j = \sum_k \gamma_{ijk} a_k$, dan is $(\sum_i \xi_i a_i)(\sum_j \eta_j a_j) = \sum_{ij} (\xi_i \eta_j)(a_i a_j) = \sum_{ijk} (\xi_i \eta_j \gamma_{ijk}) a_k$. Om van een vectorruimte een algebra te maken is het voldoende de vermenigvuldiging van de basiselementen zo te definiëren, dat deze associatief is. Dit geeft voor de <u>structuurconstanten</u> γ_{ijk} de voorwaarde

$$\sum_l \gamma_{ijl}\gamma_{lkm} = \sum_l \gamma_{jkl}\gamma_{ilm}.$$

We kunnen het begrip algebra generaliseren door voor ϕ een willekeurige deelverzameling van de endomorfieënring van de additieve groep van een ring R te nemen. We spreken dan van een ϕ-ring, als de elementen van ϕ verwisselbaar zijn met de rechts-en linksvermenigvuldigingen. Door ϕ leeg te nemen krijgt men dan een gewone ring.

We beschouwen nu een willekeurige verzameling R en een klasse ψ van deelverzamelingen van R. We noemen $A \in \psi$ een <u>minimaal</u> element van ψ als uit $X \in \psi$, $X \subset A$ volgt $X = A$. Natuurlijk kan ψ meer dan één minimaal element bevatten. We noemen $A \in \psi$ het <u>kleinste</u> element van ψ als $A \subset X$ voor alle $X \in \psi$. Natuurlijk bevat ψ hoogstens één kleinste element. Als ψ een kleinste element bezit, is dit tevens het enige minimale element.

We zeggen dat ψ aan de <u>minimumvoorwaarde</u> voldoet als iedere niet-lege deelklasse $\Omega \subset \psi$ een minimaal element bevat.

We zeggen dat ψ aan de <u>dalende-kettingvoorwaarde</u> voldoet als bij

iedere rij $W_n \in \Psi$, waarvoor geldt $W_n \supset W_{n+1}$ een natuurlijk getal k te vinden is, zodat $W_n = W_k$ voor $n > k$ (de ketting "breekt af").

Deze twee voorwaarden zijn aequivalent. Immers als de minimumvoorwaarde niet geldt is in een deelklasse van ϕ zonder minimaal element makkelijk een niet afbrekende dalende ketting te vinden; als de minimumvoorwaarde wel geldt, breekt bij de index van het minimale element uit de klasse der W_n de ketting af.

Geheel analoge beschouwingen kunnen worden gehouden over maximaal, grootste, maximumvoorwaarde en stijgende-kettingvoorwaarde.

We tonen nu eerst aan dat voor vectorruimten zowel de minimumvoorwaarde als de maximumvoorwaarde voor deelruimten aequivalent is met de eindig-dimensionaliteit (deze voorwaarden zijn dus in dit geval altijd beide wel of beide niet vervuld). Daartoe bewijzen we eerst, dat een echte deelruimte H van een n-dimensionale vectorruimte G eindigdimensionaal is met dimensie $m < n$. Als in een vectorruimte $b_1,\ldots,b_k$ onafhankelijk zijn (d.w.z. uit $\sum_{i=1}^{k} \alpha_i b_i = 0$ volgt, dat alle $\alpha_i = 0$) en b_{k+1} is onafhankelijk van $b_1,\ldots b_k$ (d.w.z. er geldt niet $b_{k+1} = \sum_{i=1}^{k} \beta_i b_i$), dan zijn $b_1,\ldots,b_k b_{k+1}$ onafhankelijk. Immers uit $\sum_{i=1}^{k+1} \alpha_i b_i = 0$ volgt, dat alle $\beta_i = 0$ zijn, of $\beta_{k+1} \neq 0$; in het laatste geval is b_{k+1} afhankelijk van $b_1,\ldots,b_k$. Als H de nulruimte is, is H 0-dimensionaal. Kies anders in H een $b_1 \neq 0$ en vorm $\beta_1 b_1$ (β_1 doorloopt ϕ). Als H daarmee niet uitgeput is gaan we door met een b_2 en vormen $\beta_1 b_1 + \beta_2 b_2$ enz. Steeds zijn daarbij $b_1,\ldots,b_k$ onafhankelijk. Als na m stappen ($m < n$) H uitgeput is, is H m-dimensionaal en zijn we klaar. Als dat niet zo is zijn er $b_1,\ldots,b_n$ te vinden, alle in H, die onafhankelijk zijn. De elementen $\sum_{i=1}^{m} \beta_i b_i$ (β_i doorlopen ϕ) vormen een deelruimte K van G, en wel, omdat $K \subset H$, een echte deelruimte. Als $a_1,\ldots,a_n$ een basis van G is, is er minstens één a_i, waarvoor $a_i \notin K$. Nu gaan we aan $b_1,\ldots,b_n$ als boven achtereenvolgens $a_1 a_2$ enz. toevoegen en krijgen zo tenslotte een basis van G die uit meer dan n elementen bestaat, hetgeen een tegenspraak oplevert.

Uit het bovenstaande volgen voor n-dimensionale ruimten nu direct beide kettingvoorwaarden, daar een ketting niet meer dan n+1 verschillende deelruimten kan bevatten.

Als omgekeerd de maximumvoorwaarde voor deelruimten geldt, is volgens het bovenstaande procédé een stijgende ketting deelruimten te construeren, die afbreekt en zo de eindigdimensionaliteit levert. Laat nu de minimumvoorwaarde voor deelruimten vervuld zijn. Stel dat de ruimte G niet eindigdimensionaal is, dan is volgens bovenstaand procédé een oneindige rij elementen $b_1, b_2, \ldots$ te construeren, zodat iedere eindige deelverzameling eruit een onafhankelijk stelsel vormt. Vorm nu de deelruimte H voortgebracht door $b_i (i \geq 2)$; deze bestaat blijkbaar uit $\Sigma \beta_i b_i$

met slechts eindig veel $\beta_i \neq 0$. Nu is $b_1 \notin H$, want als $b_1 \in H$ was, was b_1 afhankelijk van een eindig stelsel der b_i. H is dus een echte deelverzameling van G en bovendien niet eindig dimensionaal (zij bevat deelruimten van willekeurig hoge dimensie). Op H kunnen we hetzelfde proces weer toepassen enz. en zo een niet afbrekende dalende ketting verkrijgen, hetgeen een tegenspraak oplevert.

Het is triviaal, dat als ψ aan de minimum-resp. maximumvoorwaarde voldoet, hetzelfde geldt voor een deelklasse $\mathfrak{A} \subset \psi$. Dus gelden in een hypercomplex systeem de maximum- en de minimumvoorwaarde voor ϕ-l-idealen, ϕ -r-idealen en ϕ- idealen.

De klassieke structuurtheorie van Wedderburn voor hypercomplexe systemen werd door Artin gegeneraliseerd voor ϕ -ringen, waarin de ϕ-l-idealen aan de maximum- en minimumvoorwaarde voldoen. Dit is inderdaad een uitbreiding, want hieraan voldoen uiteraard alle eindige ringen en de restklassenring mod m in de ring der gehele getallen is, als m geen priemgetal is, geen hypercomplex systeem.

Later is het gelukt uit de voorwaarden van Artin de maximumvoorwaarde nog weg te laten. Ook dit is een uitbreiding; neem het systeem bestaande uit oneindige rijen nullen en enen, waarin evenwel slechts eindig veel enen mogen voorkomen en definieer optelling door op te tellen alsof het duaal geschreven natuurlijke getallen waren, dus met tweetallenoverbrenging, maar laat hetgeen er aan de voorkant eventueel uitgeworpen wordt weg. B.v.

$$\begin{array}{r} 1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,\ldots \\ +\ 1\,1\,0\,0\,1\,1\,1\,0\,0\,0\,\ldots \\ \hline 0\,1\,1\,0\,1\,0\,1\,1\,0\,1\,\ldots \end{array}$$

Het is duidelijk, dat dit systeem een commutatieve groep vormt. We bewijzen dat alle echte ondergroepen eindig zijn en de ondergroepen dus aan de minimumvoorwaarde voldoen. Stel een oneindige ondergroep H dan bevat deze voor ieder natuurlijk getal n een element met een 1 rechts van de n^e plaats. Stel een element $a \in H$ met zijn meest rechtse 1 op de m^e plaats, dan is $2^{m-1}a = (1,0,0,\ldots)$, dus $(1,0\ 0,\ldots) \in H$, $2^{m-2}a = (*,1,0,0,\ldots)$, dus ook $(0,1,0,0,\ldots) \in H$ enz; dus H bevat alle elementen met nullen voorbij de m^e plaats. Daar dit voor iedere m geldt, is H de hele groep. De groep voldoet echter niet aan de maximumvoorwaarde voor ondergroepen, want voor iedere n is de verzameling van elementen die voorbij de n^e plaats nullen hebben een ondergroep, en deze ondergroepen vormen een niet- afbrekende stijgende keten. Maken we nu van de groep een ring door de definitie $ab = 0$ voor alle a en b, dan zijn alle ondergroepen tevens l-idealen; de verkregen ring voldoet dus wel aan de minimum- maar niet aan de maximumvoorwaarde voor l-idealen.

Een matrixring ϕ_n over een lichaam ϕ is blijkbaar een hypercomplex systeem van rang n^2 met basiselementen E_{ij}. Neem nu omgekeerd een hypercomplexsysteem G met één over ϕ. Dan is dit isomorf met de ring der linksvermenigvuldigingen en daar deze laatste verwisselbaar zijn met de elementen van ϕ, zijn het lineaire transformaties van de vectorruimte G over ϕ, welke laatste een ring vormen, isomorf met ϕ_n (ϕ is nu commutatief verondersteld). Dus G is isomorf (en wel ϕ- isomorf) met een deelring van ϕ_n. Als G geen één heeft kunnen we het inbedden in een hypercomplex systeem met één door een basiselement a_o toe te voegen en te definiëren $a_o\, a_i = a_i\, a_o = a_i$. Het zo verkregen systeem is isomorf meteen deelring van een matrixring en dus G a fortiori. Dus:

Een algebra over een lichaam ϕ is isomorf met een deelring van een matrixring over ϕ.

Een element a van een ring heet <u>nilpotent</u> als er een natuurlijk getal n bestaat waarvoor $a^n = o$. Een deelverzameling van een ring heet een <u>nilverzameling</u> als alle elementen van de verzameling nilpotent zijn. Een deelverzameling V van een ring heet nilpotent als er een natuurlijk getal n bestaat, zodat het product van n factoren V(ook geschreven V^n) alleen uit het nulelement bestaat; d.w.z. als ieder product van n factoren $a_1\, a_2 \ldots\ldots a_n$ uit V nul is. Uiteraard is een nilpotente verzameling een nilverzameling; het omgekeerde hoeft niet te gelden. De betekenis van begrippen als nilring, l - nilideaal, nilpotent r - ideaal enz. is nu wel duidelijk.

Een element $e \neq o$ van een ring heet <u>idempotent</u> als $e^2 = e$. Een idempotent element (kortweg een idempotent) e heet <u>primitief</u> als het onmogelijk is twee idempotenten e_1 en e_2 te vinden, zodat $e = e_1 + e_2$ en $e_1\, e_2 = e_2\, e_1 = o$. De betekenis van het laatste begrip blijkt uit het volgende.

Laat een commutatieve Ω-groep directe som zijn van Ω-ondergroepen : $G = G_1 + \ldots + G_n$. Dan is iedere $x \in G$ op één en slechts een wijze te schrijven als $x = x_1 + \ldots + x_n$ $(x_i \in G_i)$. De afbeelding $E_i\, x = x_i$ is dan een Ω endomorfie. Hiervoor geldt: $E_i^2 = E_i$, $E_i\, E_j = o$ als $i \neq j$ en $E_1 + \ldots E_n = 1$ (de identieke afbeelding). Als er omgekeerd n Ω-endomorfieën F_i bestaan, zodat $F_i^2 = F_i$, $F_i\, F_j = o$ als $i \neq j$ en $F_1 + \ldots + F_n = 1$ en we definiëren G_i als het beeld van G bij F_i $(G_i = F_i\, G)$ dan zijn G_i Ω-ondergroepen en $G = G_1 + \ldots + G_n$ en de bij deze ontbinding horende E_i zijn gelijk aan de F_i. Verder is als E een idempotente Ω-endomorfie is en Z_E is de verzameling van de elementen z van G

waarvoor $Ez = o$ (dit is blijkbaar een Ω-ondergroep van G), $G = E\,G + Z_E$, want $E(x - Ex) = o$, en als $E\,x + z = o$ en $E\,z = o$, dan is $o = E(E\,x + z) = E\,x$ en $z = o$. Als $Z_E = o$, dan is bij iedere x een y_x te vinden zodat $x = Ey_x$, dus $E\,x = E^2 y_x = E y_x = x$, dus $E = 1$. Als $Z_E \neq o$, dan is er een idempotente Ω-endomorfie E' zodat $E + E' = 1$, $E\,E' = E'\,E = o$, dus 1 is niet primitief. In een Ω-endomorfieënring is dus 1 dan en slechts dan primitief als het de enige idempotent is. We noemen een idempotente Ω-endomorfie een projectie. We noemen een Ω-groep G onontbindbaar als de enige manieren waarop G als directe som van twee Ω-ondergroepen te schrijven is, zijn $G = G + o$ en $G = o + G$. Een Ω-groep G is dan en slechts dan onontbindbaar als de identieke endomorfie een primitieve projectie is.

Als G een commutatieve Ω-groep is en A een Ω-endomorfie, dan noemen we Z_A de verzameling der elementen z, waarvan $A\,z = o$; dit is weer een Ω-ondergroep. Blijkbaar is $Z_A \subset Z_{A2} \subset Z_{A3} < \ldots\ldots$ Als $Z_{Ak} = Z_{Ak+1}$, dan is ook $Z_{Ak+1} = Z_{Ak+2} = \ldots$ Stel n.l. $z \in Z_{Ak+2}$, dus $A^{k+2}z = o$, dus $A^{k+1}(A\,z) = o$, dus $A\,z \in Z_{Ak+1}$, dus $A\,z \in Z_{Ak}$, dus $o = A^k(A\,z) = A^{k+1}z$, dus $z \in Z_{Ak+1}$. Stel nu $A\,G = G$ en $Z_A \neq o$, dan is er een $z \neq o$ met $A\,z = o$; bij z is er een x zodat $z = A\,x$ (dus $x \notin Z_A$) en $o = A\,z = A^2x$ (dus $x \in Z_{A2}$). Dus bevat Z_{A2} in dat geval meer dan Z_A; we schrijven dit $Z_{A2} > Z_A$ (dus $Z_{A2} \supset Z_A$ en $Z_{A2} \neq Z_A$). Op deze wijze verdergaande vinden we $Z_A < Z_{A2} < Z_{A3} < \ldots$. Hieruit vinden we:

Als de Ω-ondergroepen van G aan de maximumvoorwaarde voldoen en A is een Ω-endomorfe afbeelding van G op zichzelf ($A\,G = G$) dan is A isomorf ($Z_A = o$), dus een Ω-automorfie.

Beschouw nu de ketting $G \supset A\,G \supset A^2G \supset \ldots$ Als $A^kG = A^{k+1}G$, dan is $A^{k+1}G = A^{k+2}G = \ldots$ Stel nu $Z_A = o$ en $A^kG = A^{k+1}G$ dan is er bij iedere x een y_x te vinden zodat $A^{k+1}x = A^k y_x$, dus $o = A(A^kx - A^{k-1}y)$, dus $A^kx = A^{k-1}y$, dus $A^{k-1}G = A^kG$ enz. $A\,G = G$. Hieruit vinden we:

Als de Ω-ondergroepen van G aan de minimumvoorwaarde voldoen en A is een Ω-isomorfe afbeelding van G in zichzelf ($Z_A = o$), dan is A een afbeelding op ($A\,G = G$), dus een Ω-automorfie.

Door combinatie vinden we:

Als de Ω-ondergroepen van G aan de minimum- en aan de maximumvoorwaarde voldoen en A is een Ω-endomorfie, dan is A een automorfie of $A\,G < G$ en $Z_A \neq o$.

Als de maximumvoorwaarde geldt is er een kleinste k waarvoor $Z_{Ak} = Z_{Ak+1}$.

Daarvoor geldt $Z_{Ak} \cap A^kG = o$. Stel n.l. $w = A^kx$ en $A^kw = o$. Dan is $A^{2k}x = o$ en, daar $Z_{A2k} = Z_{Ak}$, $o = A^kx = w$.

Als de minimumvoorwaarde geldt is er een kleinste m waarvoor $A^mG = A^{m+1}G$. Daarvoor geldt $G=(A^mG, Z_{A^m})$, want bij iedere x is er een y te vinden zodat $A^mx = A^{2m}y$ en dus is $A^m(x-A^my)=0$ en $x=(x-A^my)+A^my\in(Z_{A^m},A^mG)$.

Als de maximum- en minimumvoorwaarden beide gelden is k=m. Uit $Z_{A^{k+1}}=Z_{A^k}$ volgt namelijk dat voor de door A in de Ω-ondergroep A^kG geïnduceerde endomorfie B geldt $Z_B=0$. Daar ook in A^kG de minimumvoorwaarde geldt volgt daaruit $B(A^kG)=A^kG$, dus $A^{k+1}G=A^kG$, dus $m \leqslant k$. Uit $A^mG=A^{m+1}G=A(A^mG)$ volgt, daar in A^mG de maximumvoorwaarde geldt, voor de in A^mG door A geïnduceerde endomorfie C, dat $Z_C=0$, dus $A^mG \cap Z_A=0$, dus $Z_{A^{m+1}} = Z_{A^m}$, dus $k \leqslant m$. Dus k = m, en in A^kG is A een automorfie. Verder is in Z_{A^k} natuurlijk A nilpotent. Dus

Stelling van Fitting: Als in een commutatieve Ω-groep G de Ω-ondergroepen aan de maximum- en de minimumvoorwaarde voldoen is bij iedere Ω-endomorfie A een natuurlijk getal k te vinden, zodat $G=A^kG+Z_{A^k}$ (directe som), waarbij A nilpotent is in Z_{A^k} en een automorfie in A^kG.

Een direct gevolg hiervan is:

Als in een commutatieve Ω-groep G de Ω-ondergroepen aan de maximum- en de minimumvoorwaarde voldoen en G is onontbindbaar, dan is iedere Ω-endomorfie van G nilpotent of een automorfie.

Een commutatieve Ω-groep G heet volledig reducibel als bij iedere Ω-ondergroep H van G een Ω-ondergroep H_1 van G bestaat, zodat $G=H+H_1$.

Een Ω-ondergroep H van een volledig reducibele Ω-groep G is volledig reducibel.

Neem een Ω-ondergroep K van H. Dan is er een K_1, zodat $G=K+K_1$, dus $H=(K, K_1 \cap H)$; verder is $K \cap K_1=0$, dus $K \cap K_1 \cap H = 0$, dus $H=K+(K_1 \cap H)$.

In een volledig reducibele Ω-groep volgt de minimumvoorwaarde voor Ω-ondergroepen uit de maximumvoorwaarde voor Ω-ondergroepen en omgekeerd.

Bewijs: Neem een niet-afbrekende dalende ketting $G=G_1 > G_2 > G_3 > \ldots$. Er zijn dan $G'_i \neq 0$ voor $i \geqslant 2$, zodat $G_{i-1}=G_i+G'_i$. Dan is $G_1=G'_2+G_2= G'_2+G'_3+G_3=\ldots$ en $G'_2 < G'_2+G'_3 < G'_2+G'_3+G'_4 < \ldots$ is een niet-afbrekende stijgende ketting. Dus uit de maximumvoorwaarde volgt de minimumvoorwaarde. Neem nu een niet-afbrekende stijgende ketting $0 < G_1 < G_2 < \ldots$. Bepaal G'_1 zodat $G=G_1+G'_1$ en G'_i voor $i>1$ zodat $G'_{i-1}=(G'_{i-1} \cap G_i)+ + G'_i$. Nu is $(G_i, G'_i) \supset G_{i-1}$ en $(G_i, G'_i) \supset G_{i-1}$ (omdat $G_i \supset G_{i-1}$) d

$(G_i, G'_i) \supset (G_{i-1}, G'_{i-1})$ en met inductie: $(G_i, G'_i)=G$. Nu is $G'_{i-1} \cap G_i \cap G'_i = 0$, maar $G'_i \cap G_i \cap G'_{i-1}$ (omdat $G'_i \subset G'_{i-1}$), dus $G_i \cap G'_i = 0$, dus $G = G_i + G'_i$. Hieruit volgt $G'_i < G'_{i-1}$; dus $G'_1 > G'_2 > \ldots$ is een niet-afbrekende dalende ketting. Dus uit de minimumvoorwaarde volgt de maximumvoorwaarde.

Als G volledig reducibel is en aan de maximum- of minimumvoorwaarde voor Ω-ondergroepen (en dus aan beide) voldoet, dan is $G = G_1 + \ldots + G_n$, waarin G_i enkelvoudige (of irreducibele) Ω-ondergroepen zijn. Als omgekeerd $G = (G_1, \ldots, G_n)$ en G_i zijn irreducibele Ω-ondergroepen, dan is G volledig reducibel en voldoet aan maximum- en minimumvoorwaarde.

Bewijs: Eerst concluderen we uitsluitend uit de maximumvoorwaarde, dat G te schrijven is $G = G_1 + \ldots + G_n$, waarin G_i onontbindbaar zijn. Stel namelijk dat het niet kon, dan was $G = G_1 + G'_1$ met $G_1 \neq 0$, $G'_1 \neq 0$ en minstens één van beide (b.v. G'_1) ook niet zo te schrijven. G'_1 splitsen we weer op dezelfde wijze verder enz. en krijgen zo voor iedere n : $G = G_1 + \ldots + G_n + G'_n$. Dan vormt $G_1 < G_1 + G_2 < \ldots$ een niet-afbrekende stijgende ketting. Stel nu in het geval, dat G volledig reducibel is, zo 'n schrijfwijze gegeven en laat G_i niet enkelvoudig zijn. Dus is er een G'_i met $0 < G'_i < G_i$. Daar G_i volledig reducibel is is er een G''_i zodat $G_i = G'_i + G''_i$. Maar nu is ook $0 < G''_i < G_i$ en dit is in strijd met de onontbindbaarheid van G_i. Dus zijn alle G_i irreducibel. Laat nu $G = (G_1, \ldots, G_n)$ met irreducibele G_i zijn. Neem een Ω-ondergroep H van G. Dan is $H \cap G_i = 0$ of $H \cap G_i = G_i$. Als de laatste betrekking van alle i geldt is $H = G$. Anders is er een i_1 zodat $H \cap G_{i_1} = 0$ en dus $H_1 = H + G_{i_1}$. Met H_1 herhalen we hetzelfde proces en vinden $H_1 = G$ of er is een $i_2 \neq i_1$ zodat $H_1 \cap G_{i_2} = 0$ en dus $H_2 = H + G_{i_1} + G_{i_2}$. Tenslotte vinden we $G = H + G_{i_1} + \ldots + G_{i_k} = H + K$ waarmee de volledige reducibiliteit van G is aangetoond. Om de maximumvoorwaarde aan te tonen, merken we op, dat we volgens het bovenstaande, als complement van H in de directe som steeds een som van G_i's kunnen nemen en wel zo dat als we H vergroten, de som door een deelsom wordt vervangen. Nemen we nu een ketting $H_1 \subset H_2 \subset \ldots$ en vormen we de complementen op de beschreven wijze, dan kunnen er slechts op eindig veel plaatsen $<$ in de ketting staan, want telkens waar dat gebeurt verdwijnt minstens één term uit het complement. De ketting breekt dus af.

Als R een ring met één 1 is, beschouwen we zijn additieve groep als een Ω - groep, waarin Ω bestaat uit de linksvermenigvuldigingen van R. Nu zijn de Ω - endomorfieën van de Ω - groep juist de rechtsvermenigvuldigingen. Laat n.l. $F(a)x = ax$ een linksvermenigvuldiging en $G(b)x = xb$ een rechtsvermenigvuldiging zijn, dan is $F(a)G(b)x = F(a)xb = axb = G(b)ax = G(b)F(a)x$, dus $G(b)$ is een Ω - endomorfie. Als A een Ω - endomorfie is, en $A1 = a$, dan is $Ax = A(x.1) = AF(x)1 = F(x)A1 = F(x)a = xa = G(a)x$, dus A een rechtsvermenigvuldiging. Daar bovendien R invers-isomorf is met de ring der rechtsvermenigvuldigingen, is het om de structuur van ringen met één na te gaan voldoende de structuur te bepalen van de Ω - endomorfieënring van een additieve groep met een operatorenverzameling Ω.

Als een ring R met één elementen $e_{ij}(i,j = 1,\ldots,n)$ bevat die voldoen aan $\sum_i e_{ii} = 1$ en $e_{ij}e_{kl} = \delta_{jk}e_{il}$, dan is R isomorf met B_n waarin B uit de elementen van R bestaat, die verwisselbaar zijn met alle e_{ij}. Bovendien is B isomorf met $e_{ii}Re_{ii}$.

Bewijs: Als $a \in R$, dan is $a_{ij} = \sum_k e_{ki}a\,e_{jk} \in B$ (want $\sum_k e_{ki}a\,e_{jk}e_{pq} = e_{pi}a\,e_{jq} = e_{pq}\sum_k e_{ki}a\,e_{jk}$) en verder is $a = \sum e_{ij}a_{ij}$ (want $\sum_{ij} e_{ij}\sum_k e_{ki}\,a\,e_{jk} = \sum_{ij} e_{ii}\,a\,e_{jj} = a$) en deze schrijfwijze is eenduidig, want uit $a_{ij} \in B$ en $\sum_{ij} e_{ij}\,a_{ij} = 0$ volgt $a_{ij} = \sum_k e_{ki}(\sum_{ij} e_{ij}\,a_{ij})e_{jk} = 0$. Hieruit volgt dat R isomorf is met B_n. Daar $e_{kk}(\sum_{ij} e_{ij}\,a_{ij})e_{kk} = e_{kk}\,a_{kk}$ geldt $e_{kk}\,R\,e_{kk} = e_{kk}B$ en de afbeelding $a \to e_{kk}a$ voor $a \in B$ is een isomorfie.

Als G, G_1, G_2 Ω- groepen zijn en $G = G_1 + G_2$ en $1 = E_1 + E_2$ zijn de bijbehorende projecties, dan is, als R de Ω- endomorfieënring van G is, de Ω-endomorfieënring R_1 van G_1 isomorf met E_1RE_1.

Bewijs: Voor $A \in R$ beeldt E_1AE_1 G_2 in 0 en G_1 in zichzelf af en induceert dus een $B \in R_1$ die dan en slechts dan nul is als $E_1AE_1 = 0$. Als omgekeerd $B \in R_1$ dan is $E_1BE_1 \in R$ en $E_1BE_1 = E_1(E_1BE_1)E_1 \in E_1RE_1$. In R_1 is E_1 echter de identieke transformatie dus daar is $E_1BE_1 = B$.

Als $G = G_1 + \ldots + G_n$ (alle Ω - groepen), waarin de G_i onderling Ω - isomorf zijn dan is de Ω - endomorfieënring R van G isomorf met S_n waarin S de Ω- endomorfieënring van een der G_i is.

Bewijs: Laat $1 = E_1 + \ldots + E_n$ de projecties zijn die bij de directe som behoren. Kies verder Ω- isomorfieën B_{i1} tussen G_1 en G_i $(i \neq 1)$. Noem $E_{ii} = E_i, E_{i1} = E_{ii}\,B_{i1}\,E_{11}$, $E_{1i} = E_{11}\,B_{i1}^{-1}\,E_{ii}$ en $E_{ij} = E_{i1}\,E_{1j}$ voor $i \neq j$, $i \neq 1$, $j \neq 1$. Dan is $E_{ij}E_{kl} = \delta_{jk}E_{il}$ voor alle i,j,k,l. De rest

volgt uit het bovenstaande.

Uit de stelling van Fitting volgt direct:

Stelling van Schur: Als een Ω- groep irreducibel is, is zijn Ω-endomorfieënring een scheef lichaam.

Stel nu een volledig reducibele Ω - groep G, die aan de minimum - of maximumvoorwaarde (en dus aan beide) voldoet en laat $G = G_1 + \ldots + G_n$ een splitsing in irreducibele Ω - ondergroepen zijn. Stel verder hierin $G_1, \ldots, G_{k_1}$ onderling Ω - isomorf, $G_{k_1+1}, \ldots, G_{k_1+k_2}$ onderling Ω - isomorf maar niet Ω - isomorf met G_1 enz. Laat nu H_1 en H_2 irreducibele Ω - ondergroepen van G zijn en B een Ω- homomorfie van H_1 in H_2, dan is B = 0 of een Ω - isomorfie van H_1 op H_2. Als $1 = E_1 + \ldots + E_n$ correspondeert met bovenstaande splitsing en A is een Ω - endomorfie van G dan induceert E_jAE_i een Ω - homomorfie van G_i in G_j. Als i een van de getallen $k_1 + \ldots + k_{p-1}+1, \ldots, k_1 + \ldots + k_p$ is en j een der getallen $k_1 + \ldots + k_{q-1}+1, \ldots, k_1 + \ldots + k_q$ met $q \neq p$, dan wordt G_i door E_jAE_i in 0 afgebeeld en G_k voor $k \neq i$ ook, dus dan is $E_jAE_i=0$. Als we nu stellen $E^{(1)} = E_1 + \ldots + E_{k_1}, \ldots, E^{(t)} = E_{k_1+\ldots+k_{t-1}+1} + \ldots + E_{k_1+\ldots+k_t}$, waarin $k_1 + \ldots + k_t = n$, dan is $A = \sum_{ij} E_iAE_j = E^{(1)}AE^{(1)} + \ldots + E^{(t)}AE^{(t)}$. Daar $(E^{(p)}AE^{(p)})(E^{(q)}BE^{(q)}) = 0$ als $p \neq q$, is $E^{(p)}RE^{(p)}$ een ideaal in R en R is directe som van deze idealen. Verder is $E^{(p)}RE^{(p)}$ isomorf met de ring der Ω- endomorfieën van $E^{(p)}G = G_{k_1+\ldots+k_{p-1}+1}+\ldots+G_{k_1+\ldots+k_p}$, dus is $E^{(p)}RE^{(p)}$ isomorf met een matrixring $\phi_{k_p}^{(p)}$ over een scheef lichaam $\phi^{(p)}$, dat isomorf is met de Ω - endomorfieënring van $G_{k_1+\ldots+k_{p-1}+1}$. Dit geeft de volgende structuurstelling:

De endomorfieënring van een volledig reducibele Ω - groep, die aan de minimum - (of maximum -) voorwaarde voor Ω - ondergroepen voldoet, is een directe som van idealen, die matrixringen over scheve lichamen zijn.

We herinneren ons, dat als een ring directe som van idealen is, de idealen elkaar annuleren en verder dat een matrixring over een lichaam enkelvoudig is. Als omgekeerd een ring R directe som is van elkaar annulerende ringen $R = R_1+ \ldots + R_n$ met $R_iR_j = 0$ voor $i \neq j$, dan zijn de R_i idealen, want uit $x_i \in R_i$ en $y = y_1 + \ldots + y_n \in R$ volgt $x_iy = x_iy_1+ \ldots + x_iy_n = x_iy_i \in R_i$ en $yx_i = y_ix_i \in R_i$. Verder zijn de R_i in dat geval, als ze enkelvoudig zijn als idealen in R ook enkelvoudig als ringen. Is namelijk S een linksideaal in R_i en $s \in S$ en $x = x_1+\ldots+x_n \in R$ dan is $xs = x_1s+\ldots+x_ns = x_is \in S$. Evenzo voor een rechtsideaal. Als ten slotte een ring met één directe som is van niet verder in een directe som van idealen te ontbinden idealen $R = R_1+\ldots+R_n$ dan zijn de idealen eenduidig bepaald. Laat n.l. volgens deze ontbinding $1 = e_1+\ldots e_n$

zijn, en verder een tweede dergelijke ontbinding $R = S_1+\ldots+S_m$ gegeven zijn.)

(Voor $s_1 \in S_1$ geldt dan $s_1 = 1s_1 = e_1s_1+\ldots+e_ns_1$, maar $e_is_1 \in R_i$ dus dit geeft een directe som, dus alle zijn nul behalve één en $S_1 \subset R_i$; evenzo bewijst men $R_i \subset S_k$, dus $k = 1$, dus $S_1 = R_i$ en evenzo voor de andere S_j.

Een ring S met één heet <u>volladig primair</u> als hij een nilideaal R bevat zodat S(mod R) een scheef lichaam is. Stel $b \in S$, $b \notin R$, dan is er een c zodat $cb \equiv bc \equiv 1 (\mathrm{mod} R)$, dus $bc = 1+z$ met $z \in R$. Als $z^m = 0$, dan is $(1+z)(1-z+z^2-\ldots+(-1)^{m-1}z^{m-1}) = 1$ en dus heeft b een rechtsinverse $c(1-z+\ldots+(-1)^{m-1}z^{m-1})$. Evenzo heeft b een linksinverse. R is dus juist het verzamelingstheoretische complement van de verzameling der z.g. <u>eenheden</u> van de ring S en is dus eenduidig bepaald (een eenheid van een ring met één is een element dat zowel een links- als een rechtsinverse bezit).

Als G een onontbindbare Ω-groep is die aan de minimum- en maximumvoorwaarde voor Ω-ondergroepen voldoet, dan is de endomerfieënring S van G volledig primair.

<u>Bewijs</u>: Volgens Fitting is een $A \in S$ een automorfie of nilpotent. In het laatste geval is zowel $AG = G$ als $Z_A = 0$. Noem de verzameling der Ω-endomerfieën, die geen automorfieën zijn R. Dan is als $B \in R$ en $A \in S$, $AB \in R$ en $BA \in R$. Laat verder voor $B_i \in R$, $B_1+B_2 = A$ een automorfie zijn, dan is, als $C_i = B_iA^{-1}$, $C_1+C_2 = 1$. Daar $C_2 \in R$, is C_2 nilpotent, dus $C_2^r = 0$ en dus $C_1(1+C_2+\ldots+C_2^{r-1}) = (1-C_2)(1+C_2+\ldots+C_2^{r-1}) = 1 = (1+C_2+\ldots C_2^{r-1})(1-C_2) = (1+C_2+\ldots+C_2^{r-1})C_1$, dus C_1 is een automorfie, dus $C_1 \notin R$ hetgeen een tegenspraak geeft. Dus R is een ideaal. Tenslotte geldt voor een nevenklasse $A+R \notin R$, dat A een automorfie is, dus $(A+R)(A^{-1}+R) = 1+R$, dus S(mod R) is een scheef lichaam.

Als een collectie ψ van l-idealen van een ring S zo is dat ze met twee l-idealen ook hun som bevat, dan is de verzamelingstheoretische vereniging V van de elementen van de l-idealen van ψ ook een l-ideaal.

<u>Bewijs</u>: Als $v_1 \in V$, $v_2 \in V$ dan zijn er $A_1 \in \psi$, $A_2 \in \psi$, zodat $v_1 \in A_1$, $v_2 \in A_2$, dus $v_1 \pm v_2 \in (A_1, A_2) \in \psi$, dus $v_1 \pm v_2 \in V$. Als $x \in S$, dan is $xv_1 \in A_1 \in \psi$, dus $xv_1 \in V$.

Als A_1 en A_2 nilpotente ϕ-l-idealen van een ϕ-ring zijn, is (A_1, A_2) ook een nilpotent ϕ-l-ideaal.

<u>Bewijs</u>: Stel $A_1^r = A_2^s = 0$. Vorm $(A_1, A_2)^{r+s-1}$. Deze bestaat uit elementen van de gedaante

$$\sum_i \prod_{k=1}^{r+s-1} (a_{ik}+b_{ik}) \text{ met } a_{ik} \in A_1, b_{ik} \in A_2.$$

Dit bestaat uit een som van termen van de gedaante $c_1 \ldots c_{r+s-1}$ met $c_i \in A_1$ of $c_i \in A_2$. In een dergelijk product komen of minstens r factoren uit A_1 of minstens s factoren uit A_2 voor. Neem het eerste geval (het andere gaat analoog). Daar A_1 een l-ideaal is kunnen telkens factoren

uit A_2 die links van een element van A_1 staan met dat element samengenomen worden tot een nieuw element van A_1. Zo komt er $d_1 d_2 \ldots d_r \ldots$ met $d_1, \ldots, d_r \in A_1$. Maar dit is nul. Dus is $(A_1, A_2)^{r+s-1} = 0$.

Een analoge stelling geldt voor r -idealen, en dus ook voor idealen. Daaruit volgt dat de vereniging R van alle nilpotente ϕ-idealen. een ϕ-ideaal is en wel natuurlijk een ϕ-nilideaal. R behoeft evenwel niet nilpotent te zijn. Wel omvat R alle nilpotente ϕ-1-idealen op grond van de volgende stelling:

Een nilpotent ϕ-1-ideaal A van een ϕ-ring S is bevat in een nilpotent ϕ-ideaal.

Bewijs: (A,AS) voldoet aan de vereisten, want het is een ϕ-ideaal omdat (A,AS) $S \subset AS \subset (A,AS)$ en $S(A,AS) \subset (A,AS)$ en het is nilpotent, want AS is nilpotent omdat $(AS)^{n+1} = A(SA)^n S$ en SA is nilpotent omdat $SA \subset A$, en AS is een 1-ideaal, dus de som van A en AS is nilpotent.

Dat R niet nilpotent hoeft te zijn, zien we aan het volgende voorbeeld. Neem over het lichaam der rationale getallen een hypercomplex systeem S(n) met n-1 basiselementen $e_1, \ldots, e_{n-1}$ en de vermenigvuldigingsdefinitie $e_i e_j = e_{i+j}$ als $i+j < n$ en $e_i e_j = 0$ als $i+j \geq n$. Dat deze vermenigvuldiging associatief is, volgt uit het feit dat zowel $e_i(e_j e_k)$ als $(e_i e_j)e_k$ gelijk is aan e_{i+j+k} als $i+j+k < n$ en gelijk is aan nul als $i+j+k \geq n$. Een product van n elementen van S(n) is blijkbaar steeds nul, maar $e_1^{n-1} = e_{n-1} \neq 0$. Dus $(S(n))^n = 0$, $(S(n))^{n-1} \neq 0$. We vormen nu oneindige rijen van de gedaante $(a_1, a_2, \ldots)$ met $a_i \in S(i)$, maar zo dat slechts eindig veel der $a_i \neq 0$ zijn. Optelling, aftrekking en vermenigvuldiging geschiedt componentsgewijze, dus $(a_1, a_2, \ldots) \pm (b_1, b_2, \ldots) = (a_1 \pm b_1, a_2 \pm b_2, \ldots)$ en $(a_1, a_2, \ldots)(b_1, b_2, \ldots) = (a_1 b_1, a_2 b_2, \ldots)$. Deze verzameling R is blijkbaar een ring. Nu is in R de verzameling der elementen $(a_1, a_2, \ldots)$ waarvoor alle $a_i = 0$ voor $i > n$ bij een vaste n blijkbaar een nilpotent ideaal en daar ieder element in zo 'n nilpotent ideaal ligt is de vereniging van alle nilpotente idealen R zelf. Maar R is niet nilpotent, want als we in S(n+1) een element b kiezen waarvan $b^n \neq 0$ dan is van het element $(a_1, a_2, \ldots)$ van R waarvoor geldt $a_i = 0$ voor $i \neq n+1$ en $a_{n+1} = b$ de n^{de} macht ook $\neq 0$.

Voor de structuurtheorie is het gewenst dat R wel nilpotent is. Artin verkreeg dit door de maximumvoorwaarde voor ϕ-1-idealen aan te nemen op zeer eenvoudige wijze: Neem een maximaal nilpotent ϕ-1-ideaal A, dan is $A \subset R$. Als er een $x \in R$, $x \notin A$ bestond, dan was $x \in B$, B een nilpotent ϕ-1-ideaal met $B \not\subset A$. Maar nu is (A,B) ook een nilpotent ϕ-1-ideaal en $A < (A,B)$ in strijd met de maximaliteit van A. Dus A=R en A is nilpotent.

Het is echter ook mogelijk hetzelfde uit de minimumvoorwaarde voor ϕ-1-idealen te halen met behulp van de volgende stelling:

Als de ϕ-1-idealen van een ϕ-ring aan de minimumvoorwaarde voldoen, dan is ieder ϕ-1-nilideaal nilpotent.

Bewijs: Laat A een ϕ - 1 - nilideaal zijn dan is $A \supset A^2 \supset A^3 \ldots$ een dalende ketting ϕ - 1 - idealen, die dus afbreekt $A^k=A^{k+1}=A^{k+2}\ldots$ We willen bewijzen dat $A^k=0$. Stel daarom $B=A^k \neq 0$, dan is $B = B^2$. Er bestaan dus ϕ - 1 - idealen $P \subset B$ waarvoor geldt $BP \neq 0$. Neem een minimaal ϕ-1- ideaal $P \subset B$ waarvoor $BP \neq 0$. Dan is er een $b \in P$ waarvoor $Bb \neq 0$. Maar Bb is een ϕ - 1 - ideaal, $Bb \subset P$ en $B(Bb) = B^2b = Bb \neq 0$, dus uit de minimaliteit van P volgt $Bb = P$. Er is dus een $a \in B$ zodat $ab = b$, maar hieruit volgt $b = ab = ab^2 = \ldots = 0$ omdat b nilpotent is. Dit geeft een tegenspraak met $Bb \neq 0$, dus $B = 0$.

In een ϕ - ring S, waarvan de ϕ - 1 - idealen aan de minimumvoorwaarde voldoen, heet de vereniging van alle nilpotente ϕ-idealen (die dus tevens alle ϕ - nilidealen omvat) het <u>radicaal</u> R van S. Het radicaal is dus nilpotent.

Men zou kunnen denken, dat een analoge beschouwing als hierboven voor nilpotente idealen gegeven is, ook voor nilidealen te geven is. Nu is de som van twee nilidealen wel weer een nilideaal, hetgeen volgt uit de volgende stelling.

Als A een nilideaal is van een ring S, $a \in A$, $b \in S$, b nilpotent, dan is a+b nilpotent.

Bewijs: $(a+b)^r = c+b^r$ met $c \in A$; als r zo groot is dat $b^r = 0$ is, is dus $(a+b)^r \in A$, maar de elementen van A zijn nilpotent, dus a+b is nilpotent.

Hieruit volgt dat de vereniging van alle ϕ - nilidealen weer een ϕ - nilideaal is, m.a.w. dat er een grootste ϕ-nilideaal bestaat. Het is echter onbekend of dit ook de ϕ - 1 - nilidealen omvat. Dit is een belangrijk open probleem van de ringtheorie. Dit hangt samen met het volgende open probleem (dat overigens met het bovenstaande aequivalent is):

Is de som van twee ϕ-1-nilidealen een ϕ - 1 - nilideaal?

We tonen nu nog even aan dat de twee problemen inderdaad aequivalent zijn. In de ene richting is dat heel makkelijk:

Als de vereniging U van alle ϕ - nilidealen ook alle ϕ - 1 - nilidealen omvat, is de som van twee ϕ - 1 - nilidealen een ϕ - 1 - nilideaal.

Immers alles is bevat in U.

Om het omgekeerde te bewijzen hebben we de volgende hulpstelling nodig:

Het ϕ - r - ideaal voortgebracht door een element a van een ϕ-1 - nilideaal is een ϕ - r - nilideaal (en duaal met vervanging van r door 1 en van 1 door r).

Bewijs: De elementen x van het ϕ - r - ideaal voortgebracht door a zijn $x=na+ar+\sum \pm \alpha_{i1}\alpha_{i2}\ldots\alpha_{ik}a$ met n geheel, r willekeurig in de ring en $\alpha_{ij} \in \phi$. Som en verschil van dergelijke elementen zijn

weer dergelijke elementen. Een dergelijk element van rechts vermenigvuldigd met s in de ring geeft (bedenk dat de elementen van ϕ verwisselbaar zijn met de rechts - en linksvermenigvuldigingen): $a(ns+rs+\sum_i \pm \alpha_{i1}\alpha_{i2}\cdots\alpha_{ik_i}s)$, dus weer zo'n element. Ten slotte geeft $\beta \in \phi$ toegepast op zo'n element: $a(\beta r)+\sum_{i=1}^{|m|}\frac{n}{|n|}\beta a+\sum_i \pm \beta\alpha_{i1}\alpha_{i2}\cdots\alpha_{ik_i}a$, dus weer zo'n element. Vorm nu het kwadraat van zo'n element, dan geeft dit: $a(nx+rx+\sum_i \pm \alpha_{i1}\alpha_{i2}\cdots\alpha_{ik_i}x) = ay$ met y in de ring. Omdat a in een 1 - nilideaal ligt is ya nilpotent: $(ya)^m = 0$, maar dan ook $(ay)^{m+1} = a(ya)^m y = 0$, dus x is nilpotent.

Als in een ϕ- ring steeds de som van twee ϕ- 1 - nilidealen een ϕ- 1 - nilideaal is, bevat de vereniging U van alle ϕ- nilidealen ook alle ϕ-1-nilidealen.

Bewijs: Vorm de vereniging L van alle ϕ- 1 - nilidealen. Op grond van het gegeven en een vroegere stelling is L een ϕ-1-nilideaal. We bewijzen nu dat L ook een r-ideaal, dus een ideaal is. Neem daartoe een $a \in L$ en een r uit de ring. Omdat a in het ϕ-1-nilideaal L ligt is het ϕ- r - ideaal voortgebracht door a een ϕ- r - nilideaal. Dit bevat ar; daar ar in een ϕ - r - nilideaal ligt, is het ϕ- 1 - ideaal voortgebracht door ar een ϕ- 1 - nilideaal. Dit is bevat in L, dus $ar \in L$. Nu is L als ϕ- nilideaal bevat in U, dus U bevat alle ϕ- 1 - nilidealen. (Natuurlijk is L = U, want een ideaal is a fortiori een 1 - ideaal).

Als de ϕ - 1 - idealen van een ϕ- ring aan de minimum- en maximumvoorwaarden voldoen, dan geldt voor ieder ϕ- 1 - ideaal, dat het nilpotent is of dat het een idempotent bevat.

Bewijs: Neem als operatorenverzameling Ω de vereniging van ϕ met de verzameling der linksvermenigvuldigingen, dan zijn de Ω- ondergroepen juist de ϕ - 1 - idealen. Als het ϕ - 1 - ideaal A niet nilpotent is en $A = A_1 + A_2$ (A_i ϕ - 1 - idealen) dan is minstens een van beide ook niet nilpotent. We mogen daarom A onontbindbaar veronderstellen. A is ook geen nilideaal (wegens de minimumvoorwaarde). Nu is een rechtsvermenigvuldiging G(b) met $b \in A$ toegepast op A een Ω- endomorfie, dus volgens Fitting is G(b) nilpotent of een automorfie. Als $\{G(b)\}^k = 0$ is $\{G(b)\}^k b = b^{k+1} = 0$, dus b nilpotent. Daar A geen nilring is, is er een $b \in A$ waarvoor G(b) een automorfie is. Er is dan een $e \in A$ waarvoor $b = G(b)e = eb$. Dan is $G(b)(e^2-e) = (e^2-e)b = 0$, dus $e^2-e = 0$, $e^2 = e$ en $e \neq 0$ wegens $A \neq 0$. Dus e is de gezochte idempotent.

Als A een irreducibel ϕ - 1 - ideaal van een ϕ- ring S is, is $A^2 = 0$ of $A = Se$, waarin e een idempotent is.

Bewijs: Dit loopt geheel analoog als het bewijs van de vorige stelling, nu met de stelling van Schur in plaats van die van Fitting. Nu is G(b) of de nulendomorfie of een automorfie. Als G(b) de nulendomorfie is voor alle b dan is $xb = 0$ voor alle $x \in A$, $b \in A$, dus $A^2 = 0$.

Anders is er een $b \in A$, waarvoor $G(b)$ een automorfie is. Evenals boven concludeert men hieruit dat A een idempotent e bevat. Nu bevat Se het element $e^2 = e \neq 0$, dus $Se \neq 0$ en $Se \subset A$. Uit de irreducibiliteit van A volgt dan $Se = A$.

Een ϕ - ring heet <u>halfenkelvoudig</u>, als de ϕ - 1 - idealen aan de minimumvoorwaarde voldoen en het radicaal nul is (d.w.z. de ring geen nilpotente ϕ1-idealen bevat)

Als S een ϕ- ring is, waarvan de ϕ- 1 - idealen aan de minimumvoorwaarde voldoen en R is het radicaal van S, dan is de restklassenring $\bar{S} = S \pmod R$ halfenkelvoudig.

<u>Bewijs</u>: Als $\bar{A}$ een ϕ - 1 - ideaal van $\bar{S}$ is en A is de verzameling der elementen der restklassen die $\bar{A}$ vormen (dus $\bar{A} = A \pmod R$) dan is A een ϕ - 1 - ideaal van S. Daaruit volgt onmiddellijk dat de ϕ - 1 - idealen van $\bar{S}$ ook aan de minimumvoorwaarde voldoen (Hiervoor hoeft R niet het radicaal te zijn; het geldt voor ieder ϕ - ideaal). Laat nu $\bar{A}$ een nilpotent ϕ - 1 - ideaal van $\bar{S}$ zijn, $\bar{A}^k = 0$, dan is blijkbaar $A^k \subset R$. Maar R is nilpotent, $R^m = 0$, dus $A^{km} \subset R^m = 0$. Dus A is nilpotent, dus $A \subset R$, dus $\bar{A} = 0$.

<u>Eerste hoofdstelling van de structuurtheorie</u>: Een halfenkelvoudige ϕ - ring S heeft een één en is directe som van irreducibele ϕ - 1 - idealen (d.w.z. als Ω bestaat uit ϕ en de linksvermenigvuldigingen is de Ω - groep volledig reducibel). Omgekeerd is een ϕ- ring met één, die een som is van irreducibele ϕ - 1 - idealen, halfenkelvoudig.

<u>Bewijs</u>: Stel S is halfenkelvoudig. We bewijzen eerst dat S directe som is van irreducibele ϕ - 1 - idealen. Als S de nulring is , is er niets te bewijzen. Anders bevat S een minimaal ϕ - 1 - ideaal $A_1 \neq 0$. Dan is ook $A_1^2 \neq 0$, dus $A = Se_1$ met een idempotente e_1. Als $S = A_1$ zijn we klaar. Stel nu $A_1 < S$. Noem A' de verzameling der $z \in S$ waarvoor $ze_1 = 0$. Dan is A' een ϕ - 1 - ideaal. Verder is $A \cap A' = 0$ (uit $x = ye_1$ en $xe_1 = 0$ volgt $0 = xe_1 = ye_1^2 = ye_1 = x$) en omdat voor $a \in S$ geldt $a = ae_1 + (a-ae_1)$ en $(a-ae_1)e_1 = 0$, is $S = A_1 + A'$. Verder is $0 < A' < S$. Als A' irreducibel is zijn we klaar; noem dan $A' = A_2$, dan is $S = A_1 + A_2$ en $A_2 = Se_2$ met een idempotente e_2. Anders gaan we met A_2 verder als boven met S en vinden $A' = A_2 + A''$ enz. Uit de minimumvoorwaarde volgt dat dit proces moet afbreken (anders was $S > A' > A'' > \ldots$). Dus $S = A_1 + \ldots + A_n$ met A_i irreducibele ϕ-1- idealen en $A_i = Se_i$ met idempotente e_i. Uit de constructie volgt verder nog $e_ie_j = 0$ voor $i > j$. Nu bewijzen we het bestaan van een één. Noem $v = \sum_i e_i - \sum_{i<j} e_ie_j + \sum_{i<j<k} e_ie_je_k \ldots + (-1)^{n-1} e_1e_2\ldots e_n$. We berekenen nu e_kv (als onder $\sum$ een index tussen haakjes staat betekent dat, dat over die index niet gesommeerd wordt):
$e_kv = \sum_{(i<k)} e_ke_i - \sum_{(i<j<k)} e_ke_ie_j + \ldots = e_k + \sum_{(k<i)} e_ke_i - \sum_{(k<j)} e_ke_j + \sum_{(k<j<i)} e_ke_ie_j + \ldots = e_k$. Daar iedere $a \in S$ te schrijven is als $a = \sum_k a_ke_k$, is ook

$av = a$ voor iedere $a \in S$. In het byzonder is $v^2 = v$. Vorm de verzameling B der $z \in S$ waarvoor $vz = 0$, dan is B een ϕ-r- ideaal. Als $z_i \in B$, is $z_1 z_2 = (z_1 v) z_2 = z_1 (v z_2) = 0$, dus $B^2 = 0$, dus $B = 0$. Voor iedere $a \in S$ geldt $v(a-va) = 0$, dus $a - va = 0$, dus $a = va$. Dus is v de gezochte één. Daarmee is de eerste helft van de hoofdstelling bewezen. Ga nu uit van een ϕ-ring met één die som is van irreducibele ϕ- 1 - idealen. Dan is de Ω-groep volledig reducibel en voldoen de Ω- ondergroepen aan de minimumvoor-aarde. Dus de ϕ- 1 - idealen voldoen aan de minimumvoorwaarde. Neem nu een ϕ - 1 - ideaal $A \neq 0$. Uit de volledige reducibiliteit volgt dat $S = A + A'$ met A' een ϕ - 1 - ideaal. Laat volgens deze splitsing $1 = e + e'$ zijn. Dan is voor een $a \in A$ ook $a = a1 = ae + ae'$ met $ae \in A$ en $ae' \in A'$, maar ook $a = a + 0$, dus $a = ae$, dus $e \neq 0$. Verder is $e = e^2$, dus A kan niet nilpotent zijn. Dus het radicaal van S is nul.

Uit de zoëven gegeven splitsing volgt nog $e + 0 = e = e^2 + ee'$, dus $ee' = 0$ en $0 + e' = e'e + e'^2$, dus $e'^2 = e'$ en $e'e=0$. Dit geeft nog de volgende stellingen.

Een halfenkelvoudige ϕ- ring S is directe som van irreducibele ϕ - 1 - idealen Se_i : $S = Se_1 + \ldots + Se_n$, waarin $e_i^2 = e_i$ en $e_i e_j = 0$ voor $i \neq j$. Speciaal is $1 = e_1 + \ldots + e_n$.

In een halfenkelvoudige ϕ - ring S wordt ieder ϕ- 1 - ideaal $\neq 0$ voortgebracht door een idempotent.

In een halfenkelvoudige ϕ- ring voldoen de ϕ- 1 - idealen ook aan de maximumvoorwaarde.

We hebben dus gevonden, dat de Ω - groep van een halfenkelvoudige ϕ- ring volledig reducibel is en de Ω - ondergroepen aan de minimum - en dus aan de maximumvoorwaarde voldoen. Aan de ene kant hebben we voor een dergelijke Ω - groep de structuur van de Ω- endomorfieën-ring bepaald. Aan de andere kant is echter, omdat de ring een één heeft, de ring invers-isomorf met de ring van de rechtsvermenigvuldigingen en wel zelfs ϕ - invers isomorf, omdat $\alpha x = (\alpha 1)x = x(\alpha 1)$ en dus $\alpha = G(\alpha 1) = F(\alpha 1)$ en met αx correspondeert $G(\alpha 1)\, G(x) = \alpha\, G(x)$. Hierbij wordt de ring der rechtsvermenigvuldigingen als ϕ - ring opgevat door de elementen van ϕ als links- (of ook als rechts -) vermenigvuldigingen te laten werken. Maar de rechtsvermenigvuldigingen zijn juist de Ω - endomorfieën. Verder is als S_n een matrixring en S' invers - isomorf met S, ook S'_n invers - isomorf met S_n; als n.l. $a \to a'$ de afbeelding van S op S' is, dan levert $\sum e_{ij} a_{ij} \to \sum e_{ij} a'_{ji}$ de gezochte invers - isomorfie, want $\sum e_{ij} \left(\sum_k a_{ik} b_{kj} \right) \to \sum e_{ij} \left(\sum_k b'_{ki} a'_{jk} \right)$ en $\left(\sum e_{ij} b'_{ji} \right) \left(\sum e_{ij} a'_{ji} \right) = \sum e_{ij} \left(\sum_k b'_{ki} a'_{jk} \right)$ Ten slotte zijn de scheve lichamen ook scheve ϕ - lichamen, want als K zo'n scheef lichaam is en K_n de bijbehorende matrixring, $a \in K$ en $\alpha \in \phi$ dan is $\alpha\, a \in K_n$ omdat K_n in de Ω- endomorfieënring een ideaal is en α een Ω- endo-

Ten gevolge van de op het colloquium gevoerde discussie met Dr Kemperman is mij gebleken, dat een passage in de syllabus nog wat vereenvoudigd kan worden.

Het hier volgende komt in de plaats van het gedeelte van de syllabus lopende van blz. 21, regel 19 v.o. tot en met blz. 22, regel 11 v.o.

We merken nu op, dat we bij halfenkelvoudige ringen achteraf het begrip ϕ-ring kunnen missen. A priori is de eis dat een ring een halfenkelvoudige ϕ-ring is zwakker dan de eis dat hij een halfenkelvoudige ring is. Laat n.l. een ring gegeven zijn als ϕ-ring en als ψ-ring met $\phi \subset \psi$. Dan is een ψ-l-ideaal tevens ϕ-l-ideaal, het ψ-radicaal is bevat in het ϕ-radicaal en als de minimumvoorwaarde voor ϕ-l-idealen geldt, is dat ook het geval voor ψ-l-idealen. Als de ϕ-ring halfenkelvoudig is, is de ψ-ring het ook. Achteraf geldt echter ook het omgekeerde. Dit volgt uit het feit dat een halfenkelvoudige ϕ-ring een één heeft, wat ϕ ook is. In een ϕ-ring S met één geldt voor $\alpha \in \phi$, $x \in S$, dat $\alpha x = \alpha(1x) = (\alpha 1)x$ en $\alpha x = \alpha(x1) = x(\alpha 1)$, dus $\alpha = F(\alpha 1) = G(\alpha 1)$. Dus een l-ideaal, resp. r-ideaal, ideaal is een ϕ-l-ideaal, resp. ϕ-r-ideaal, ϕ-ideaal, dus een halfenkelvoudige ϕ-ring is een halfenkelvoudige ring. We merken nog op, dat een deelring geen ϕ-deelring behoeft te zijn.

Aan de andere kant kunnen we ook proberen in een ring S met één ϕ zo groot mogelijk te maken. We zagen al dat $\alpha \in \phi$ hetzelfde is als links- of rechtsvermenigvuldiging met $\alpha 1$. Het element $\alpha 1$ is verwisselbaar met alle elementen van S en ligt dus in het centrum van S. Als omgekeerd $a \in S$ in het centrum van S ligt, voldoet de linksvermenigvuldiging (= rechtsvermenigvuldiging) met a blijkbaar aan de eisen die aan een element van ϕ gesteld zijn. De grootste ϕ die dus gekozen kan worden in een ring met één is de verzameling linksvermenigvuldigingen met centrumelementen.

We hebben in de eerste hoofdstelling gevonden dat de Ω-groep (Ω bestaat uit de linksvermenigvuldigingen) van een halfenkelvoudige ring volledig reducibel is en de Ω-ondergroepen aan de minimum- en dus aan de maximumvoorwaarde voldoen. Aan de ene kant hebben we van een dergelijke Ω-groep de structuur van de Ω-endomorfieënring bepaald. Aan de andere kant is echter, omdat de ring een één heeft, de ring invers-isomorf met de ring van de rechtsvermenigvuldigingen, dat zijn juist de Ω-endomorfieën. Als K_n een matrixring is en K' invers-isomorf met K, dan is ook K'_n invers-isomorf met K_n; als n.l. $a \to a'$ de afbeelding van K op K' is, levert $\sum e_{ij}a_{ij} \to \sum e_{ij}a'_{ji}$ de gezochte invers-isomorfie, want $\sum e_{ij}(\sum_\kappa a_{ik}b_{kj}) \to \sum e_{ij}(\sum_\kappa b'_{ki}a'_{jk})$ en $(\sum e_{ij}b'_{ji})\cdot(\sum e_{ij}a'_{ji}) = \sum e_{ij}(\sum_\kappa b'_{ki}a'_{jk})$. Ten slotte is, als K een der scheve lichamen is en a een element van het centrum van S (dus F(a) =

= G(a)), F(a)K $\subset$ K. Laat b $\in$ K zijn, dan is F(a)b een element van de matrixring K_n, want K_n is een ideaal in de Ω -endomorfieënring en G(a) is een Ω -endomorfie, maar F(a)b is ook verwisselbaar met alle e_{ij} uit K_n, want b is het omdat b $\in$ K en F(a) is, omdat F(a) $\in \Omega$, verwisselbaar met alle Ω -endomorfieën. Dus F(a)b $\in$ K. Hiermee is de eerste helft verkregen van de:

Tweede hoofdstelling van de structuurtheorie: Een halfenkelvoudige ring is een directe som van idealen, die isomorf zijn met matrixringen over scheve lichamen; deze scheve lichamen worden bij vermenigvuldiging met een element van het centrum van de ring in zichzelf getransformeerd (d.w.z. als de ring als ϕ -ring beschouwd wordt, zijn het scheve ϕ -lichamen). Omgekeerd is een directe som van elkaar annulerende matrixringen over scheve lichamen halfenkelvoudig.

De omkering bewijst men als volgt: Laat S = $A_1+\ldots+A_n$ een splitsing zijn in elkaar annulerende matrixringen over scheve lichamen. Laat e_i de één van A_i zijn en noem v = $e_1+\ldots+e_n$. Neem een willekeurige a $\in$ S en laat a = $a_1+\ldots+a_n$ zijn met $a_i \in A_i$. Dan is va = $e_1a_1+\ldots+e_na_n$ = $= a_1+\ldots+a_n$ = a en evenzo av = a, dus S bezit een één. Verder is A_i som van irreducibele l-idealen in A_i, die echter ook irreducibele l-idealen in S zijn. Dus S is som van irreducibele l-idealen. Volgens de eerste hoofdstelling is dus S halfenkelvoudig.

morfie en $\alpha a \in K$ omdat α a verwisselbaar is met alle matrixelementen e_{ij} (immers a is dat, en α is verwisselbaar met alle $\mathfrak{S}$-endomorfieën). Hiermee is de eerste helft verkregen van de:

Tweede hoofdstelling van de structuurtheorie: Een halfenkelvoudige ϕ-ring is een directe som van idealen, die matrixringen over scheve ϕ-lichamen zijn. Omgekeerd is een directe som van elkaar annulerende matrixringen over scheve lichamen halfenkelvoudig.

De omkering bewijst men als volgt: Laat $R = A_1+\ldots+A_n$ een splitsing zijn in elkaar annulerende ringen die elk isomorf zijn met een matrixring over een scheef lichaam. Laat e_i de één van A_i zijn en noem $v = e_1+\ldots+e_n$. Neem een willekeurige $a \in R$ en laat $a = a_1+\ldots+a_n$ zijn met $a_i \in A_i$. Dan is $va = e_1a_1+\ldots+e_na_n = a_1+\ldots+a_n = a$ en evenzo $av = a$, dus R bezit een één. Verder is A_i som van irreducibele 1-idealen in A_i die echter ook irreducibele 1-idealen in R zijn. Dus R is som van irreducibele 1-idealen. Volgens de eerste hoofdstelling is dus R halfenkelvoudig.

We merken nog op dat we bij halfenkelvoudige ringen achteraf het begrip ϕ-ring kunnen missen. A priori is de eis dat een ring een halfenkelvoudige ϕ-ring is zwakker dan de eis dat hij een halfenkelvoudige ring is. Als we n.l. ϕ uitbreiden dan krimpt de verzameling der ϕ-1-idealen in (of blijft dezelfde), dus het radicaal wordt kleiner (of blijft hetzelfde) en als de minimumvoorwaarde voor ϕ-1-idealen geldt, dan blijft dat zo, dus als de ϕ-ring halfenkelvoudig is blijft dat zo. Achteraf blijkt echter dat omgekeerd ook een halfenkelvoudige ϕ-ring een halfenkelvoudige ring is; dit volgt direct uit de tweede hoofdstelling, immers een halfenkelvoudige ϕ-ring is een directe som van elkaar annulerende ringen die matrixringen over scheve lichamen zijn, en die is een halfenkelvoudige ring. Dit is overigens ook nog op andere wijze in te zien: een halfenkelvoudige ϕ-ring heeft een één, maar daaruit volgt dat $\alpha \in \phi$ rechts- en tevens linksvermenigvuldiging is met $\alpha 1$, dus ϕ-1-idealen zijn 1-idealen.

Aan de andere kant kunnen we ook proberen ϕ zo groot mogelijk te maken. We zagen al dat $\alpha \in \phi$ hetzelfde is als de links- of rechtsvermenigvuldiging met $\alpha 1$. Het element $\alpha 1$ is verwisselbaar met alle elementen van S. Als omgekeerd $a \in S$ verwisselbaar is met alle elementen van S, (d.w.z. a ligt in het centrum van S), dan voldoet de linksvermenigvuldiging (= de rechtsvermenigvuldiging) met a blijkbaar aan de eisen die aan een element van ϕ gesteld zijn. De grootste ϕ die gekozen kan worden in een halfenkelvoudige ring S is dus het centrum van S.

De structuur van het centrum C van S bepalen we als volgt. Ontbind S volgens de tweede hoofdstelling in elkaar annulerende enkelvoudige ringen $S = A_1+\ldots+A_n$. Laat voor $a \in S$ de ontbinding $a = a_1+\ldots+a_n$ zijn en voor $c \in C$ de ontbinding $c = c_1+\ldots+c_n$ dan is voor ac de ontbinding $ac = a_1c_1+\ldots+a_nc_n$ en evenzo $ca = c_1a_1+\ldots+c_na_n$, maar nu is $ac = ca$, dus $a_ic_i = c_ia_i$. Omgekeerd als voor $d_i \in A_i$ geldt $d_ia_i = a_id_i$ voor alle $a_i \in A_i$ dan is ook $d_ia = ad_i$ voor alle $a \in S$. Dus C is de directe som van de centra C_i der afzonderlijke A_i: $C = C_1+\ldots+C_n$. Verder is blijkbaar $C_i = C \cap A_i$. We zagen vroeger al dat het centrum van een matrixring K_n over een scheef lichaam K het centrum van K is.

Dus de volgende stelling geldt:

Het centrum van een directe som van elkaar annulerende matrixringen over scheve lichamen (d.w.z. het isomorfe beeld van een willekeurige halfenkelvoudige ring) is de directe som van de centra dier scheve lichamen, dat is een directe som van (commutatieve) lichamen.

Passen we dit toe op een commutatieve ring S dan is C = S en we vinden:

Stelling van Dedekind: Een commutatieve halfenkelvoudige ring is een directe som van elkaar annulerende lichamen.

We leggen nu een verband tussen de eerste en de tweede hoofdstelling. Volgens de eerste hoofdstelling wordt S geschreven als $S = L_1+\ldots+L_k$, waarin de L_i irreducibele 1-idealen zijn; volgens de tweede als $S = A_1+\ldots+A_n$, waarin de A_j enkelvoudige idealen zijn. Neem nu een willekeurig irreducibel 1-ideaal $B \neq 0$ in S, dan is volgens de tweede ontbinding een $b \in B$ als $b = b_1+\ldots+b_n$ te schrijven met $b_j \in A_j$. Als nu e_j de één van A_j is is $e_j b = b_j \in B$. Dus is $B = B_1+\ldots+B_n$ met $B_j \subset A_j$ en B_j eveneens 1-idealen in S. Uit de irreducibiliteit van B volgt, dat alle $B_j = 0$ zijn op één na. Dus $B \subset A_j$ voor een of andere j. Passen we dit op de L_i uit de eerste ontbinding toe, dan volgt daaruit dat we deze in groepen bij elkaar kunnen nemen van 1-idealen die in een zelfde A_j liggen. Door een andere rangschikking der L_i kunnen we dus verkrijgen $S = (L_1+\ldots+L_{i_1})+(L_{i_1+1}+\ldots+L_{i_1+i_2})+\ldots+(L_{i_1+\ldots+i_{n-1}+1}+\ldots+L_{i_1+\ldots+i_n}) = M_1+\ldots+M_n$ met $M_j \in A_j$. Uit de directheid der som volgt dan, dat $M_j = A_j$.

Beschouwen we nu één der A_j, b.v. A_1 nog wat nader. $A_1 = L_1+\ldots+L_{i_1}$, maar aan de andere kant weten we dat A_1 isomorf is met een matrixring K_m over een scheef lichaam K deze is directe som van m irreducibele 1-idealen die onderling isomorf zijn: $K_m = K_m e_{11}+\ldots+K_m e_{mm} = H_1+\ldots+H_m$.

Nu geldt de volgende stelling over Ω-groepen:

Als G een Ω-groep is en $G = H_1+H_2 = H_1+H'_2$ met H_1, H_2, H'_2 Ω-groepen dan is H_2 Ω-isomorf met H'_2.

Bewijs: Beschouw de projectie van G op H'_2 en pas deze toe op H_2 dan geeft dit een Ω-endomorfie van H_2 in H'_2. De elementen van G die bij de projectie in 0 worden afgebeeld zijn de elementen van H_1; maar $H_1 \cap H_2 = 0$ dus de afbeelding van H_2 in H'_2 is isomorf. Het is echter ook een afbeelding op want als $a \in H'_2$ dan is a te schrijven $a = b + c$ met $b \in H_1$, $c \in H_2$ en $c = -b + a$, dus a is het beeld van c bij de afbeelding. Dus zijn H_2 en H'_2 Ω-isomorf.

Beschouw nu A_1 als Ω-groep met de linksvermenigvuldigingen als Ω. Dan is de Ω-groep volledig reducibel en volgens de stelling op pg 13

is bij iedere Ω-ondergroep H een som van H_j te vinden zodat H + $+ H_{j_1} + \ldots + H_{j_p} = G$. Dit geldt dan ook voor $L_i (1 \leq i \leq i_1)$, dus $G = L_i + H_{j_1} + \ldots + H_{j_p} = H_1 + \ldots + H_m$ dus L_i Ω-isomorf met $H_{k_1} + \ldots + H_{k_{m-p}}$ $(j_i, \ldots, j_p, k_1, \ldots, k_{m-p}$ is een permutatie van $1, \ldots, m)$, maar uit de irreducibiliteit van L_i volgt dat m-p=1 en L_i Ω-isomorf met een H_k. Dus alle L_i zijn onderling Ω-isomorf en hun aantal is m. Nemen we nu echter twee L_i uit verschillende A_j dan zijn deze zeker niet Ω-isomorf. Linksvermenigvuldiging met de één van een der twee A_j voert de elementen van de ene L_i in zichzelf en van de andere in nul over. Hiermee is bewezen:

In een halfenkelvoudige ring wordt de ontbinding in tweezijdige idealen volgens de tweede hoofdstelling verkregen door in de ontbinding in l-idealen volgens de eerste hoofdstelling die l-idealen in groepen samen te nemen, waarvan de additieve groepen Ω-isomorf zijn, waarin Ω uit de linksvermenigvuldigingen bestaat. Het aantal l-idealen in zo'n groep is gelijk aan de graad van de matrixring waarmee het tweezijdige ideaal isomorf is.

Neem een l-ideaal in een halfenkelvoudige ring S. Dan is dit te schrijven als Se en $S = Se + Se_1$ met $e^2 = e$, $e_1^2 = e_1$, $ee_1 = e_1e = 0$, $1 = e + e_1$. Nu is de verzameling der $x \in S$ waarvoor $(Se)x = 0$, juist e_1S, want $(Se)(e_1S) = 0$ en $x = 1x = ex + e_1x$, dus als $(Se)x=0$, is $0 = e^2x = ex$, dus $x = e_1x$, dus $x \in e_1S$. Nu is e_1S blijkbaar een r-ideaal, en de verzameling der $x \in S$ waarvoor $x(e_1S) = 0$ is weer Se (bewijs evenals boven). Als A een willekeurig r-ideaal in S is, dan is de verzameling der x waarvoor $xA = 0$ een l-ideaal $Se_2 (1 = e_2 + e_3)$. Voor $a \in A$ geldt $a = e_2a + e_3a$, en $0 = e_2^2a = e_2a$, dus $a = e_3a$, dus $A = e_3S$ en is juist de verzameling der $x \in S$ waarvoor $(Se_2)x = 0$. Hiermee is een eenduidige correspondentie tot stand gebracht tussen de verzameling der l-idealen en die der r-idealen. Bij deze afbeelding wordt blijkbaar de verzamelingstheoretische inclusie ($\subset$) omgekeerd. Hiermee is de volgende stelling bewezen:

In een halfenkelvoudige ring S voldoen de r-idealen aan de maximum- en minimumvoorwaarde. Als $S = Se_1 + \ldots + Se_n$ met $e_i^2 = e_i$, $e_ie_j \neq 0$ en $1 = e_1 + \ldots + e_n$ een ontbinding in irreducibele l-idealen is, is $S = e_1S + \ldots + e_nS$ een ontbinding in irreducibele r-idealen.

Een enkelvoudige ring behoeft niet halfenkelvoudig te zijn. Wel is de vereniging van alle nilpotente ϕ-idealen van een enkelvoudige ϕ-ring S makkelijk vast te stellen, daar S maar twee ϕ-idealen bezit n.l. 0 en S. De ene mogelijkheid is dat S niet nilpotent is; dan is deze vereniging nul en als S halfenkelvoudig is is S isomorf met een matrixring over een scheef lichaam. De andere mogelijkheid is dat S

nilpotent is, maar dan is $S^2 = 0$, want als $S^2 = S$, dan is $S^n = S$, dus $S = 0$ of S niet nilpotent en als $S^2 < S$, is $S^2 = 0$. Alle producten in S zijn dan nul en de ϕ-idealen zijn ϕ-ondergroepen van de additieve groep van S. De nilpotente enkelvoudige ϕ-ringen zijn dus juist de enkelvoudige additieve Ω-groepen (t.o.v. een willekeurige operatorenverzameling Ω), waarin de vermenigvuldiging gedefinieerd wordt door $xy = 0$ voor alle x en y.

Als S een hypercomplex systeem over een lichaam ϕ is, dan voldoen de ϕ-1-idealen zeker aan de minimumvoorwaarde, want zelfs de deelruimten van de vectorruimte voldoen aan deze voorwaarde. De vraag of S halfenkelvoudig is wordt dan dus alleen bepaald door de vraag of het radicaal nul is. Als S halfenkelvoudig is valt S volgens de tweede hoofdstelling uiteen in ϕ-idealen, die weer als hypercomplexe systemen over ϕ op te vatten zijn. S zelf en ook zo'n ϕ-ideaal bevatten een één en men kan dus bij beide ϕ als deelverzameling van het systeem opvatten; daar deze enen echter verschillend zijn, zijn dit niet dezelfde deelverzamelingen. Het zo verkregen enkelvoudige systeem is een matrixring over een scheef ϕ-lichaam; dit scheve lichaam is dus weer een hypercomplex systeem over ϕ.

Een byzonder geval van een hypercomplex systeem is een z.g. <u>groepenring</u>. Ga hiertoe uit van een eidige, eventueel niet-commutatieve groep G, die multiplicatief geschreven wordt. Noem de elementen $a_1, \ldots a_h$. Vorm nu een h-dimensionale vectorruimte over een lichaam ϕ en noem een basis daarvan ook $a_1, \ldots, a_h$ en maak hiervan een hypercomplex systeem door als vermenigvuldiging der basiselementen gewoon de groepvermenigvuldiging te nemen. De associativiteit der groepvermenigvuldiging waarborgt, dat zo inderdaad een hypercomplex systeem ontstaat. Deze beschouwingswijze is van voordeel voorde z.g. <u>representatietheorie</u> van groepen. Onder een representatie van een groep verstaat men een homomorfe afbeelding van de groep op een multiplicatieve groep van n-rijige vierkante matrices met elementen uit een lichaam ϕ. Deze n-rijige matrices kunnen geïnterpreteerd worden als lineaire transformaties van een n-dimensionale vectorruimte over ϕ. Vormen we nu van een eindige groep de groepenring S over hetzelfde lichaam ϕ, dan is deze homomorfe afbeelding direct uit te breiden tot een homomorfe afbeelding van S op een ring van lineaire transformaties. Als n.l. $a_i \to A_i$ dan definiëren we $\sum_{i=1}^{h} \alpha_i a_i \to \sum_{i=1}^{h} \alpha_i A_i$ en dit is een lineaire transformatie (ϕ is commutatief) en het is direct te zien dat met som en product ook som en product overeenstemmen. Omgekeerd bepaalt een homomorfe afbeelding van S in de ring der lineaire transformaties natuurlijk ook een representatie van de groep. We generaliseren het begrip representatie op een natuurlijke wijze als volgt: Een homomorfe afbeelding van een ring S in

de endomorfieënring van een additieve groep heet een representatie van de ring. Een voorbeeld hiervan is de vroeger behandelde afbeelding van de ring op de ring van zijn linksvermenigvuldigingen; dit is dus een representatie van de ring in zijn eigen additieve groep; deze representatie heet de reguliere representatie. We komen op deze representaties nog terug. Eerst bewijzen we nog een belangrijke stelling over groepenringen:

Een groepenring over een lichaam Φ is dan en slechts dan halfenkelvoudig, als de karakteristiek van Φ niet deelbaar is op de orde van de groep.

Bewijs: De groepenring heeft een één, n.l. de één van de groep. Laat de karakteristiek van Φ niet deelbaar zijn op de orde van de groep. Het is dan voldoende aan te tonen, dat de Ω -groep (Ω bestaande uit Φ en de linksvermeigvuldigingen) volledig reducibel is. We beschouwen de additieve groep nu behalve als Ω -groep ook als Φ -groep; de Φ -ondergroepen zijn de lineaire deelruimten en de Φ -endomorfieën lineaire transformaties van de vectorruimte over Φ . De Φ -groep is als eindigdimensionale vectorruimte volledig reducibel (S is som van de h verzamelingen αa_i (α doorloopt Φ), die kennelijk irreducibele Φ -groepen zijn). Neem een willekeurige Ω -ondergroep (d.w.z. Φ -l-ideaal)B, dan is B a fortiori een Φ -ondergroep dus kunnen we schrijven $S = B + B_1$, waarin B_1 een Φ -ondergroep is. Een linksvermenigvuldiging is een lineaire transformatie. Pas nu op B_1 achtereenvolgens linksvermenigvuldiging met a_i en daarna projectie op B_1 toe dan is dat een lineaire transformatie van B_1 in zichzelf, die we A_i noemen. Als $y \in B_1$, dan is dus $a_i y = c + A_i y$ met $c \in B$. Hierdoor is aan iedere a_i een A_i toegevoegd, maar aan een product wordt hierbij ook een product toegevoegd wordt $a_j a_i y = a_j c + a_j A_i y = a_j c + d + A_j A_i y$ met $d \in B$ maar dan is ook $a_j c + d \in B$, omdat B een l-ideaal is, dus aan $a_j a_i$ is inderdaad $A_j A_i$ toegevoegd. Verder is aan de één de identieke transformatie toegevoegd en dus aan een inverse ook de inverse transformatie. De transformaties zijn dus ook transformaties van B_1 op zichzelf. Noem nu $y' = Qy = \frac{1}{h} \sum_i a_i^{-1} A_i y$ dan is dit weer een lineaire transformatie van B_1 op een Φ -groep B'. Daar verder $A_i y = a_i y + c_i (c_i \in B)$ is, is $y' = \frac{1}{h} \sum_i a_i^{-1} (a_i y + c_i) = y + b$ met $b \in B$. Dus is $S = (B,B')$ maar als $y' \in B' \cap B$ en $y' = Qy$ dan is $y \in B$ en $y \in B_1$ dus $y = 0$, dus $y' = 0$, dus $S = B + B'$. We bewijzen nu tenslotte dat B' een Ω -ondergroep van S is. Neem daartoe een a_k en een $y' \in B'$, $y' = Qy$, dan is $a_k y' = \frac{1}{h} \sum_i a_k a_i^{-1} A_i y = \frac{1}{h} \sum_i (a_i a_k^{-1})^{-1} (A_i A_k^{-1}) A_k y =$ $= \frac{1}{h} \sum_i a_i^{-1} A_i A_k y = Q A_k y \in B'$. Voor een willekeurige $x \in S$ en $y' \in B'$ geldt dan ook $xy' \in B'$. Hiermee is de eerste helft van het bewijs voltooid. Stel nu de karakteristiek van Φ wel deelbaar op de orde h van de groep. We kunnen dan direct een nilpotent Φ -ideaal $\neq 0$ in de groepenring aangeven. Noem $s = \sum_{i=1}^{h} a_i$, dan is $a_k s = s a_k = s$ voor alle k; het

ϕ -ideaal voortgebracht door s bestaat uit de elementen αs (α doorloopt ϕ). Nu is $s^2=hs=0$ omdat h deelbaar is door de karakteristiek, / dus het kwadraat van het ϕ -ideaal is nul. De groepenring is dus niet halfenkelvoudig. Daarmee is de tweede helft van het bewijs geleverd.

We beschouwen nu een representatie van een ring S in een groep G. Dan is aan iedere $a \in S$ een endomorfie A van G toegevoegd. Men schrijft nu voor een $x \in G$ in plaats van Ax ook ax een product van een element van de ring en van de groep. Dit product voldoet dus aan $a(x+y)=ax+ay$, $(a+b)x=ax+bx$, $(ab)x=a(bx)$. Men noemt dan G een S-modulus. Iedere representatie van S bepaalt een S-modulus en omgekeerd. Een ondergroep van G, die toegelaten is t.o.v. de operatoren uit S heet een S-deelmodulus van G. Als S een één heeft behoeft daarmee niet de identieke transformatie van G te corresponderen. Bepaal in G de verzamelingen H en K waarvoor resp. $1x = x$ en $1x = 0$, dan zijn H en K blijkbaar ondergroepen, maar zelfs ook deelmoduli, want als $1x = x$, is $1(ax)=(1a)x=ax$ en als $1x = 0$, is $1(ax) = (1a)x = ax = (a1)x = a(1x) = a0 = 0$. Verder is $G = H+K$, want als $x \in G$, is $x = 1x + (x-1x)$ en $1(1x) = 1x$, $1(x-1x) = 1x-1x = 0$ en H en K hebben alleen 0 gemeen want uit $1x = x$ en $1x = 0$ volgt $x = 0$. G valt dus uiteen in een directe som van een deelmodulus waarin 1 wel de identieke transformatie induceert en een deelmodulus die door 1 en dus door alle elementen uit S geannuleerd wordt (immers uit $1x = 0$ volgt $ax = a(1x) = 0$). We zullen dikwijls eisen dat 1 de identieke transformatie induceert. Bij de reguliere representatie is dat het geval.

Beschouw nu een l-ideaal A in S en een element x in de S-modulus G en beschouw Ax bestaande uit alle producten ax (a loopt A), dan is Ax blijkbaar een S-deelmodulus. Verder is $a \rightarrow ax$ een S-homomorfie van A op Ax. Als A irreducibel is, is dan Ax of S-isomorf met A of nul. Als G als S-modulus irreducibel is, is $Ax = 0$ of $= G$ voor iedere x en ieder l-ideaal A. Onderstel nu S halfenkelvoudig, dan is $S = A_1+\ldots+A_k$ waarin A_i irreducibele l-idealen zijn. Als nu G irreducibel is en $SG \neq 0$, dan is er een $x \in G$ zodat $Sx \neq 0$ en een A_i zodat $A_ix \neq 0$. Daaruit volgt, dat $G = A_ix$ S-isomorf is met A_i. [Stel nu S halfenkelvoudig en $1x = x$ voor alle x uit de S-modulus G. Voor iedere x is dan $x = 1x \in Sx = (A_1x,\ldots,A_kx)$. Daar alle A_ix irreducibel of nul zijn wordt G voortgebracht door al zijn irreducibele S-deelmoduli. Als nu de S-deelmoduli van G aan de maximumvoorwaarde voldoen, wordt G voortgebracht door een eindig aantal van zijn irreducibele S-deelmoduli: $G = (G_1,G_2,\ldots,G_m)$, G_i irreducibel. We hebben vroeger al aangetoond, dat G dan volledig reducibel is en de S-deelmoduli ook aan de minimumvoorwaarde voldoen. Laat nu de S-deelmoduli van G aan de minimumvoorwaarde voldoen. Laat $H_1 < H_2 < \ldots$ een niet afbrekende stijgende ketting van S-deelmoduli zijn. Stel $x_i \in H_{i+1}, x_i \notin H_i$, dan is $Sx_i \subset H_i$.

Daar $x_i \in Sx_i = (A_1x_i,\ldots,A_kx_i)$ is er minstens een A_j zodat $A_jx_i \notin H_i$. Noem zo'n $A_jx_i = K_i$. Noem L_j de S-deelmodulus voortgebracht door de K_i voor $i \geqslant j$. Dan vormen de L_j een dalende ketting S-deelmoduli. We bewijzen nu $L_j > L_{j+1}$ voor alle j. Als namelijk $L_j = L_{j+1}$ was, was een $y_j \in K_j$ te schrijven als $y_j = y_{j+1}+\ldots+y_m$, met $y_i \in K_i$, waarbij we $y_m \neq 0$ kunnen veronderstellen. Dus $y_m = y_j-y_{j+1}\ldots-y_{m-1}$, en dus volgt uit $K_i \subset H_{i+1}$, dat $y_m \in H_m$. Dus $Sy_m \subset H_m$, maar daar Sy_m een S-modulus $\neq 0$ in K_m is en K_m een irreducibele S-modulus is, is $Sy_m = K_m$ hetgeen een tegenspraak geeft. Hiermee is een niet afbrekende dalende ketting geconstrueerd in strijd met de minimumvoorwaarde. De S-deelmoduli voldoen dus ook aan de maximumvoorwaarde. Hiermee is de volgende stelling verkregen.

Laat S een halfenkelvoudige ring zijn en G een S-modulus, zodat $1x = x$ voor alle $x \in G$. Als de S-deelmoduli van G aan een van beide van de maximumvoorwaarde en minimumvoorwaarde voldoen, voldoen ze aan de andere en G is als S-modulus volledig reducibel. Als G irreducibel is, is G S-isomorf met een irreducibel l-ideaal in S. Het aantal niet-isomorfe irreducibele S-moduli is gelijk aan het aantal idealen in de ontbinding van S volgens de tweede hoofdstelling.

Om dit toe te passen op groeprepresentaties moeten we voor S een groepenring over ϕ nemen en voor G een eindig-dimensionale vectorruimte over ϕ en eisen dat voor $\alpha \in \phi$, $a \in S$, $x \in G$ geldt $(\alpha a)x = \alpha(ax)$. Als verder de karakteristiek van ϕ niet deelbaar is op de orde van de gerepresenteerde groep, is S halfenkelvoudig. Als $1x = x$, dan is $(\alpha 1)x = \alpha x$, dus een S-deelmodulus van G is een lineaire deelruimte, dus de S-deelmoduli van G voldoen aan maximum- en minimumvoorwaarde, dus bovenstaande stelling kan toegepast worden en leert ons dat G als S-modulus volledig reducibel is. Als $G = G_1+\ldots+G_m$, G_i irreducibele S-moduli, dan kiezen we een basis $\{d_1,\ldots d_n\}$ van G door samenstelling van bases van G_i. Laat G_i de dimensie m_i hebben. Als voor $x \in G$ geldt $x = x_1+\ldots+x_m$ met $x_i \in G_i$, dan is voor $a \in S$, $ax = ax_1+\ldots+ax_m$ met $ax_i \in G_i$. De aan a toegevoegde matrix α_{ij} op het basisstelsel $\{d_1,\ldots,d_n\}$ wordt bepaald door $ad_j = \sum_i \alpha_{ij}d_i$ en daaruit volgt dat $\alpha_{ij} = 0$ als d_i en d_j in verschillende G_r liggen. De matrices zijn dus opgebouwd uit "kastjes" bestaande uit matrices van de graad m_i die langs de hoofddiagonaal geregen zijn en waarbuiten overal nullen staan. Bij een andere keuze van de basis van de vectorruimte is dat natuurlijk niet het geval. Nu heeft een basistransformatie met matrix T op een matrix A van een lineaire transformatie het effect, dat deze overgaat in TAT^{-1}. We noemen twee representaties $a \to A$ en $a \to A'$ van een groep aequivalent als er een vaste matrix T bestaat zodat steeds $A' = TAT^{-1}$ is. Onder de hierboven genoemde veronderstellingen is een representatie

aequivalent met een in "kastjes" geschreven representatie. We moeten nog nagaan, wat het voor de matrices betekent, dat de bij één zo 'n kastje behorende S-modulus irreducibel is. Als een S-modulus G reducibel is, d.w.z. als er een S-modulus H bestaat met $0<H<G$, dan is H ook een vectorruimte van dimensie $m>0$ kleiner dan de dimensie n van G. Kies dan een basis $\{d_1,\ldots,d_n\}$ van G zodat $d_1,\ldots,d_m$ in H liggen. Dan ligt voor $i\leqslant m$ ook ad_i in H, dus voor de matrices geldt $\chi_{ij}=0$ voor $j\leqslant m$ en $i>m$, d.w.z. een linkerbenedenhoek van m rijen en n-m kolommen bestaat steeds uit nullen. Omgekeerd is, als dat het geval is de deelruimte voortgebracht door de eerste m basiselementen een S-modulus. Een representatie heet irreducibel als hij niet aequivalent is met een representatie van dat type. Het aantal inaequivalente irreducibele representaties van een groep door matrices over een lichaam ϕ is gelijk aan het aantal componenten waarin de groepenring volgens de tweede hoofdstelling uiteen valt. Men kan door een nader onderzoek van de groepenring aantonen, dat als ϕ algebraisch afgesloten is, dit aantal gelijk is aan het aantal klassen geconjugeerde elementen in de groep en dat de dimensies van de irreducibele S-moduli (de "graden" van de irreducibele representaties) gelijk zijn aan de aantallen groepelementen in een klasse geconjugeerden en dus deelbaar zijn op de orde van de groep. We gaan daar nu niet verder op in. Wel kunnen we nog opmerken, dat blijkbaar iedere irreducibele representatie aequivalent is met een irreducibel bestanddeel van de reguliere representatie.

We keren nu weer terug tot algemene ringen. Stel een ring S en een S-modulus G. Laat A een ideaal in S zijn, dat G annuleert, d.w.z. $bx=0$ voor alle $b\in A$ en $x\in G$. Als we de restklasse van a mod A aangeven met $\bar{a}$, dan is blijkbaar de productdefinitie $\bar{a}x = ax$ onafhankelijk van de keuze van de representant in de restklasse en deze definitie maakt G tot een $\bar{S}$-modulus, waarin $\bar{S}= S(\text{mod } A)$. Blijkbaar zijn S-deelmoduli van G ook $\bar{S}$-deelmoduli en omgekeerd. Laat nu S een ϕ-ring zijn, waarvan de ϕ-l-idealen aan de minimumvoorwaarde voldoen en R het radicaal van S. Als $G\neq 0$ een irreducibele S-modulus is, is Rx een S-deelmodulus voor iedere x, dus of $Rx=0$ of $Rx=G$. Als voor een of andere x geldt $Rx=G$, dan is $G=Rx=R^2x=\ldots.=0$, maar G was $\neq 0$ verondersteld, dus R annuleert G en G is een $\bar{S}$-modulus, waarin $\bar{S}= S(\text{mod } R)$ halfenkelvoudig is. Als $\bar{S}=\bar{A}_1+\ldots+\bar{A}_n$, dan is of $\bar{S}G=0$, dus $SG=0$, of G is isomorf met een l-ideaal, bevat in een der $\bar{A}_i$. Dan is G een $\bar{A}_i$-modulus. Evenzo ziet men dat als G voortgebracht wordt door irreducibele S-deelmoduli , $RG=0$ en G een $\bar{S}$-modulus is. Daarmee is het volgende verkregen:

Laat S een ϕ-ring zijn, waarvan de ϕ-l-idealen aan de minimumvoorwaarde voldoen, R het radicaal van S en G een S-modulus, zodat $SG\neq 0$ Als G irreducibel is, is G een $\bar{A}_i$-modulus, waarin $\bar{A}_i$ een van de enkelvoudige idealen is waarin $\bar{S}= S(\text{mod } R)$ volgens de tweede hoofdstelling

uiteenvalt. Als G voortgebracht wordt door irreducibele S-deelmoduli, is G een $\bar{S}$-modulus.

Neem nu voor S een deelring $\neq 0$ van de endomorfieënring van een additieve groep G, zodat de l-idealen van S aan de minimumvoorwaarde voldoen. G is dan een S-modulus en de representatie van S is een isomorfie. Uit $aG = 0$ volgt dus $a = 0$. Bovenstaande stelling geeft dan het volgende:

Laat S een ring $\neq 0$ van endomorfieën van een additieve groep G zijn, waarvan de l-idealen aan de minimumvoorwaarde voldoen. Als G als S-groep irreducibel is, dan is S enkelvoudig halfenkelvoudig en als G voortgebracht wordt door irreducibele S-groepen, is S halfenkelvoudig.

Stel nu dat S een ring van endomorfieën van een additieve groep G is, die de identieke transformatie omvat. Stel verder $S = A_1+\ldots+A_n$, waarin A_i idealen in S zijn. Noem A_iG de kleinste S-deelmodulus van G die alle a_ix ($a_i \in A_i$, $x \in G$) bevat. Dan is blijkbaar $G=(A_1G,\ldots,A_nG)$. Als $1 = e_1+\ldots+e_n$ met $e_i \in A_i$, dan is e_i de één van A_i, dus als $x_i \in A_iG$ is $e_ix_i = x_i$ en daar $e_ie_j = 0$ voor $i \neq j$ is $e_jx_i = 0$ voor $i \neq j$. Als nu $x_1+\ldots+x_n = 0$ met $x_i \in A_iG$, dan is $0 = e_i(x_1+\ldots+x_n) = x_i$. Dus de som is direct: $G = A_1G+\ldots+A_nG$. Stel nu bovendien dat S halfenkelvoudig is en de S-deelmoduli van G aan maximum- of minimumvoorwaarde (dus aan beide) voldoen. Dan is G als S-groep volledig reducibel. Aan de ene kant is S als halfenkelvoudige ring te schrijven als directe som van elkaar annulerende matrixringen over scheve lichamen; aan de andere kant is ook de ring van de S-endomorfieën in een dergelijke gedaante te schrijven. We willen het verband tussen beide opsporen. We merken op dat A_iG vereniging is van irreducibele S-deelmoduli die isomorf zijn met de irreducibele l-idealen in A_i. Nu heeft de ring der S-endomorfieën van G de vorm $T = B_1+\ldots+B_n$ waarin B_i ontstaat uit de S-endomorfieën van A_iG door ze in de andere A_jG nul te verklaren. Nu is de endomorfieënring geïnduceerd door S in A_iG een matrixring over een scheef lichaam. We hebben nu eerst nog enkele resultaten over vectorruimten nodig.

Stel een additieve groep G met een stelsel ϕ_r van endomorfieën, waarin ϕ_r een matrixring is over een scheef lichaam ϕ, dat de identieke transformatie bevat. Noem de matrixbasis G_{ij}. Verder voldoen de ϕ_r-ondergroepen aan de maximumvoorwaarde. Uiteraard is G een vectorruimte over ϕ, maar we weten nog niet of het een eindigdimensionale vectorruimte is. Dit zullen we nu eerst bewijzen. Neem een $x \neq 0$ in G. Daar $\sum_i G_{ii} = 1$, is er een G_{pp} zodat $G_{pp}x \neq 0$. Noem $x_i = G_{ip}x$. Deze zijn lineair onafhankelijk : stel $\sum_i \rho_i x_i = 0$ dan is ook $0 = G_{pq}\sum_i \rho_i x_i = \sum_i \rho_i G_{pq}G_{ip}x = \rho_q G_{pp}x$, dus $\rho_q = 0$. Noem G_1 de verzameling der elementen $\sum \rho_i x_i$ dan is G_1 een ϕ_r-ondergroep: $G_{jk}\sum_i \rho_i x_i = \sum_i \rho_i G_{jk}G_{ip}x = \rho_k x_j$. Als $G_1 < G$, nemen we een y in G buiten G_1. Als boven is er dan een G_{qq} zodat $G_{qq}y$ niet in G_1 ligt. Stelt men $x_{r+i} = G_{iq}y$, dan vormen de elementen $\sum_i \rho_i x_{r+i}$ een ϕ_r-onder

groep G_2 waarvoor geldt $G_1 \cap G_2 = 0$. Als $G_1 + G_2 < G$ kunnen we dit proces herhalen. Wegens de maximumvoorwaarde komt hier een eind aan en is $G = G_1+\ldots+G_s$ en G heeft dimensie $n = rs$ over ϕ. Nu beschouwen we de ring van de lineaire transformaties ϕ'_m van G over ϕ. Op de bovengevormde basis $x_1,\ldots x_n$ is dan de matrixbasis $E_{\alpha\beta}$ bepaald door $E_{\alpha\beta}\, x_\gamma = \delta_{\beta\gamma}\, x_\alpha$. Nu is blijkbaar $G_{ij} = \sum_{m=0}^{s-1} E_{nr+i,nr+j}$. Het zijn n.l. beide lineaire transformaties en ze hebben op alle x_γ hetzelfde effect. Immers als $\gamma = kr+l$ $(1 \leqslant l \leqslant r)$, dan is $G_{ij}x_\gamma = \delta_{jl}x_{kr+i}$ en $\sum_{m=0}^{s-1} E_{nr+i,nr+j}x_\gamma = \sum_{m=0}^{s-1} \delta_{nr+j,\gamma}\, x_{nr+i} = \delta_{jl}x_{kr+i}$. Vorm nu $H_{\lambda\nu} = \sum_{k=1}^{r} E_{(\lambda-1)r+k,(\nu-1)r+k}$ voor $1 \leqslant \lambda \leqslant s$, $1 \leqslant \nu \leqslant s$. Dan is direct na te rekenen dat $H_{\lambda\nu}\, H_{\rho\sigma} = \delta_{\nu\rho}H_{\lambda\sigma}$, $H_{11}+\ldots+H_{ss} = 1$ en $G_{ij}H_{\lambda\nu} = E_{(\lambda-1)r+i,(\nu-1)r+j} = H_{\lambda\nu}\, G_{ij}$. Ieder element van ϕ'_m is te schrijven in de gedaante $\sum G_{ij}B_{ij}$ waarin B_{ij} een som $\sum H_{\lambda\nu}\,\beta'_{\lambda\nu}$ is met $\beta'_{\lambda\nu} \in \phi'$ en als $\sum G_{ij}B_{ij} = 0$, is $B_{ij} = 0$. Dus is $(\phi'_s)_r$ isomorf met ϕ'_{sr}. Evenzo is ieder element op een en slechts een manier te schrijven in de vorm $\sum H_{\lambda\nu}\, C_{\lambda\nu}$, waarin $C_{\lambda\nu}$ een som $\sum G_{ij}\gamma'_{ij}$ is met $\gamma'_{ij} \in \phi'$. Als $A = \sum_{ij} G_{ij}B_{ij}$, dan is $B_{ij} = \sum_{\kappa} G_{\kappa i}AG_{jk}$. Dus is de voorwaarde dat A met alle G_{ij} verwisselbaar is, $A = B_{ii} = \sum H_{\lambda\nu}\,\beta'_{\lambda\nu}$. Evenzo opdat A met alle $H_{\lambda\nu}$ verwisslbaar is, moet $A = \sum G_{ij}\,\gamma'_{ij}$ zijn. Daaruit volgt dat de ring van de ϕ_r-endomorfieën van G een matrixring ϕ'_s is, waarin ϕ' invers-isomorf is met ϕ; omgekeerd is ϕ_r de verzameling van de ϕ'_s-endomorfieën van G.

Uit de verkregen resultaten volgt nu, dat als A_i een matrixring $P^{(i)}_{k_i}$ is, dan B_i een matrixring $\bar{P}^{(i)}_{m_i}$ is, waarin $\bar{P}^{(i)}$ invers-isomorf is met $P^{(i)}$. Verder is S ook de T-endomorfieënring van G, want $A_iG = B_iG$. Hiermee is de volgende stelling verkregen:

Laat S een halfenkelvoudige ring van endomorfieën van G zijn, die de identieke transformatie bevat, en de S-ondergroepen van G aan een van beide van de maximum- en minimumvoorwaarden voldoen. Als $S = P^{(1)}_{k_1}+\ldots+P^{(n)}_{k_n}$, waarin $P^{(i)}_{k_i}$ een ideaal is en een matrixring van de graad k_i over het scheve lichaam $P^{(i)}$, dan heeft de ring T van de S-endomorfieën van G de vorm $T = \bar{P}^{(1)}_{m_1}+\ldots+\bar{P}^{(n)}_{m_n}$, waarin $\bar{P}^{(i)}_{m_i}$ een ideaal is en een matrixring van de graad m_i over het scheve lichaam $\bar{P}^{(i)}$, invers-isomorf met $P^{(i)}$. Omgekeerd is S de ring van de T-endomorfieën van G.

De boven behandelde hulpstelling kunnen we ook nog gebruiken om een eenduidigheidsstelling voor matrixringen te bewijzen. Stel een ring is op te vatten als een matrixring ϕ'_m en als een matrixring ψ'_n, waarin ϕ' en ψ' scheve lichamen zijn. We kunnen ϕ'_m opvatten als de ring van de lineaire transformaties van een n-dimensionale vectorruimte G over

ϕ, waarin ϕ invers-isomorf met ϕ' is. Stel G_{ij} de matrixbasis van ψ'_r. Dan vormen de endomorfieën $\sum \varrho_{ij} G_{ij}$ met ϱ_{ij} in ϕ een ring ϕ_r, maar dan volgt uit het hierboven bewezene dat de dimensie van G over ϕ gelijk is aan rs, maar deze is ook n, dus $r \leqslant n$. Analoog bewijst men $n \leqslant r$, dus $n = r$. Laat nu $y \neq 0$ een element van G zijn dan is er een G_{pp} zodat $G_{pp} y \neq 0$. Als boven bewijst men dan dat $y_i = G_{ip} y$ een basis van G vormen, waarvoor geldt $G_{ij} y_k = \delta_{jk} y_i$. Evenzo vindt men bij de matrixbasis E_{ij} van ϕ'_n een basis x_i van G zodat $E_{ij} x_k = \delta_{jk} x_i$. Laat S de lineaire transformatie zijn waarvoor $Sy_i = x_i$, dan is $S^{-1} x_i = y_i$. Dan geldt $G_{ij} = S^{-1} E_{ij} S$, want beide hebben hetzelfde effect op de y_k. De elementen van ψ' (resp. ϕ') zijn gekarakteriseerd als de lineaire transformaties, die verwisselbaar zijn met de G_{ij} (resp. E_{ij}). Daaruit volgt $\psi' = S^{-1} \phi' S$. Want als $\varphi' \in \phi'$, is $S^{-1} \varphi' S G_{ij} = S^{-1} \varphi' S S^{-1} E_{ij} S = S^{-1} E_{ij} \varphi' S = G_{ij} S^{-1} \varphi' S$, dus $S^{-1} \varphi' S \in \psi'$. Evenzo als $\varphi' \in \psi'$, dan is $S \varphi' S^{-1} \in \phi'$, dus $\varphi' \in S^{-1} \phi' S$. Dit geeft de volgende stelling:

Als $\phi_n = \psi_r$, waarin ϕ en ψ scheve lichamen zijn, dan is $n = r$, ϕ en ψ zijn isomorf en er is een S in ϕ_n, zodat $\psi = S^{-1} \phi S$ en $G_{ij} = S^{-1} E_{ij} S$ voor de matrixbases.

We behandelen nu nog enkele stellingen uit de groepentheorie. Deze stellingen gelden ook voor niet-commutatieve groepen. We zullen de groepen desondanks additief schrijven.

Eerste isomorfiestelling: Als G een Ω-groep is, H een Ω-ondergroep van G en N een normale Ω-ondergroep van G dan is $(N,H) = (H,N)$, $N \cap H$ normaal in H en $(N,H) \pmod N$ is Ω-isomorf met $H \pmod{N \cap H}$.

Bewijs: Uit de normaliteit van N volgt direct dat (N,H) een Ω-groep is en dat $(N,H) = (H,N)$ en dat N normaal is in (N,H). De elementen van $(N,H) \pmod N$ zijn restklassen $N+x$ $(x \in H)$. Dit geeft een Ω-homomorfe afbeelding van H op $(N,H) \pmod N$ waarbij blijkbaar $H \cap N$ in nul wordt afgebeeld. Dus $(N,H) \pmod N$ is Ω-isomorf met $H \pmod{N \cap H}$.

Tweede isomorfiestelling: Als de Ω-groep G Ω-homomorf is met de Ω-groep $\bar{G}$ (kern van de homomorfie is N), en $\bar{H}$ is een normale Ω-ondergroep van $\bar{G}$ en H de verzameling der elementen van G die in $\bar{H}$ worden afgebeeld, dan zijn $G \pmod H$ en $\bar{G} \pmod{\bar{H}}$ Ω-isomorf (m.a.w. $\{G \pmod N\} \{\mod H \pmod N\}$ is Ω-isomorf met $G \pmod H$).

Bewijs: Pas achter elkaar de Ω-homomorfieën van G op $\bar{G}$ en van $\bar{G}$ op $\bar{G} \pmod{\bar{H}}$ toe, dan 's de kern van de samengestelde Ω-homomorfie blijkbaar H en dus $G \pmod H$ Ω-isomorf met $\bar{G} \pmod{\bar{H}}$.

In een Ω-groep G heet een keten Ω-ondergroepen $G = G_1 \supset G_2 \supset \ldots \supset G_{s+1} = 0$ een normaalrij van lengte s als iedere G_i normaal is in G_{i-1}. De restklassengroepen heten de factoren van de rij. Een tweede normaalrij heet een verfijning van de eerste als zij alle

G_i bevat. Twee normaalrijen heten aequivalent (of ook isomorf) als er een eeneenduidige betrekking tussen de factoren van de rijen bestaat zodat overeenkomstige factoren Ω-isomorf zijn.

Stelling van Jordan-Hölder-Schreier-Zassenhaus: Twee normaalrijen van een Ω-groep G hebben aequivalente verfijningen en wel, als de normaalrijen als volgt geschreven zijn: $G = G_1 \supset G_2 \supset \ldots \supset G_{s+1} = 0$ en $G = H_1 \supset H_2 \supset \ldots \supset H_{t+1} = 0$, dan zijn de verfijningen resp. $G = G_{11} \supset G_{12} \supset \ldots \supset G_{1t} \supset G_{21} \supset \ldots \supset G_{2t} \supset \ldots \supset G_{st} = 0$ en $G = H_{11} \supset H_{12} \supset \ldots \supset H_{1s} \supset H_{21} \supset \ldots \supset H_{2s} \supset \ldots \supset H_{ts} = 0$, waarin $G_{ij} = (G_{i+1}, G_i \cap H_j)$ voor $j = 1,\ldots,t+1$ en $i = 1,\ldots,s$ en $H_{ij} = (H_{j+1}, H_j \cap G_i)$ voor $i = 1,\ldots,s+1$ en $j = 1,\ldots,t$.

Bewijs: $G_{i,t+1} = G_{i+1,1} = G_{i+1}$. Nu is direct duidelijk, dat de G_{ij} gerangschikt als boven inderdaad een dalende keten vormen, die een verfijning van de keten der G_i is. Verder is een tweetal opeenvolgende termen uit de keten steeds te schrijven als G_{ij} en $G_{i,j+1}$. Analoge beweringen gelden voor H_{ji}. We zijn klaar als we bewezen hebben, dat $G_{i,j+1}$ normaal in G_{ij} en $H_{j,i+1}$ normaal in H_{ji} is en $G_{ij}(\mathrm{mod}\ G_{i,j+1})$ Ω-isomorf is met $H_{ji}(\mathrm{mod}\ H_{j,i+1})$. Nu is volgens de eerste isomorfiestelling $H_j \cap G_{i+1} = H_j \cap G_i \cap G_{i+1}$ normaal in $G_i \cap H_j$ en $(G_i \cap H_j)$ $(\mathrm{mod}\ G_{i+1} \cap H_j)$ is Ω-isomorf met $(G_{i+1}, G_i \cap H_j)(\mathrm{mod}\ G_{i+1})$. Evenzo is $G_i \cap H_{j+1}$ normaal in $G_i \cap H_j$ en dus $(G_{i+1} \cap H_j, G_i \cap H_{j+1})$ normaal in $G_i \cap H_j$. In de homomorfie tussen $G_i \cap H_j$ en $(G_{i+1}, G_i \cap H_j)(\mathrm{mod}\ G_{i+1})$ wordt $(G_{i+1} \cap H_j, G_i \cap H_{j+1})$ afgebeeld in $(G_{i+1} \cap H_j, G_i \cap H_{j+1}, G_{i+1})$ $(\mathrm{mod}\ G_{i+1}) = (G_i \cap H_{j+1}, G_{i+1})(\mathrm{mod}\ G_{i+1})$. Dus is, volgens de tweede isomorfiestelling, $G_{i,j+1} = (G_{i+1}, G_i \cap H_{j+1})$ normaal in $G_{i,j} = (G_{i+1}, G_i \cap H_j)$ en $G_{ij}(\mathrm{mod}\ G_{i,j+1})$ Ω-isomorf met $(G_i \cap H_j)(\mathrm{mod}\ (G_i \cap H_{j+1}, G_{i+1} \cap H_j))$. Om redenen van symmetrie is dan ook $(G_i \cap H_j)(\mathrm{mod}\ (G_i \cap H_{j+1}, G_{i+1} \cap H_j))$ Ω-isomorf met $(H_{j+1}, G_i \cap H_j)(\mathrm{mod}\ (H_{j+1}, H_j \cap G_{i+1})) = H_{ji}\ (\mathrm{mod}\ H_{j,i+1})$, waarmee de stelling bewezen is.

In een normaalrij kunnen herhalingen ($G_i = G_{i+1}$) optreden. Een normaalrij zonder herhalingen, die zichzelf als enige verfijning zonder herhalingen heeft, heet een compositierij. Op grond van de tweede isomorfiestelling is een normaalrij dan en slechts dan een compositierij als zijn factoren irreducibele Ω-ondergroepen $\neq 0$ zijn. Uit het bovenstaande volgt nu:

Twee compositierijen van een zelfde Ω-groep zijn aequivalent. Als een Ω-groep een compositierij bezit, is iedere normaalrij te verfijnen tot een compositierij.

Stel nu dat de normale Ω-ondergroepen van een Ω-groep G aan de maximum- en minimumvoorwaarde voldoen. Volgens de maximumvoorwaarde is er een maximale normale Ω-ondergroep $G_2 \neq G$ en als $G_2 \neq 0$ een maximale

normale Ω-ondergroep $G_3 < G_2$ enz. Volgens de minimumvoorwaarde moet dit proces na eindig veel stappen afbreken. Het resultaat $G = G_1 > G_2 > \ldots > G_{s+1} = 0$ is blijkbaar een compositierij. (Het is een normaalrij van een byzonder soort, n.l. een waarin alle G_i niet alleen normaal in G_{i-1} maar zelfs in G zijn). Laat nu omgekeerd G een compositierij $G = G_1 > G_2 > \ldots > G_{s+1} = 0$ bezitten. Stel een oneindige stijgende ketting normale Ω-ondergroepen $H_1 < H_2 < \ldots$, dan is $0 \leqslant H_1 < H_2 < \ldots < H_{s+2} \leqslant G$ een normaalrij. Deze is te verfijnen tot een compositierij, die aequivalent is met de gegeven compositierij. Dit is echter onmogelijk, want de verfijning van de normaalrij heeft minstens s+1 factoren en de gegeven compositierij heeft er maar s. De normale Ω-ondergroepen voldoen dus aan de maximumvoorwaarde. Evenzo bewijst men dat ze aan de minimumvoorwaarde voldoen. Hiermee is gevonden

Een Ω-groep heeft dan en slechts dan een compositierij, als zijn normale Ω-ondergroepen aan de maximum- en minimumvoorwaarde voldoen.

Uit het bewijs volgt verder nog, dat als de normale Ω-ondergroepen aan de maximum- en minimumvoorwaarde voldoen, de lengte van de stijgende en dalende kettingen niet alleen eindig, maar zelfs <u>begrensd</u> is, d.w.z. er is een natuurlijk getal, dat alleen van de Ω-groep afhangt, waar de lengte van alle stijgende en dalende kettingen onder blijft.

We willen nu nog een belangrijke stelling over directe sommen bewijzen. Ook deze stelling geldt eveneens voor niet-commutatieve groepen. Daar we tot nu toe alle begrippen samenhangende met directe sommen alleen voor commutatieve groepen hebben afgeleid, zullen we ons ook nu tot commutatieve groepen beperken. Het bewijs gaat voor niet-commutatieve groepen vrijwel onveranderd door; alleen moet voor sommen van endomorfieën, die erin gebruikt worden, dan telkens bewezen worden, dat die weer endomorfieën zijn, wat bij commutatieve groepen automatisch het geval is.

We beschouwen een commutatieve Ω-groep $G \neq 0$, waarvan de Ω-ondergroepen aan de maximum- en minimumvoorwaarde voldoen. Dan is G te schrijven als directe som van onontbindbare Ω-ondergroepen $\neq 0$. We willen nu twee van dergelijke splitsingen ($G = G_1+\ldots+G_h = H_1+\ldots+H_k$) met elkaar vergelijken. Laat de bijbehorende projecties $1 = E_1+\ldots+E_h = F_1+\ldots+F_k$ zijn. Past men E_1F_j toe op G_1, dan is dit een Ω-endomorfie van G_1 in zichzelf; verder is $E_1 = E_1F_1+\ldots+E_1F_k$ in G_1 de identieke transformatie. We willen eerst bewijzen dat minstens één der E_1F_j een Ω-automorfie van G_1 is. Daartoe bewijzen we eerst de volgende hulpstelling.

Als een Ω-groep K, waarvan de Ω-ondergroepen aan de maximum- en minimumvoorwaarde voldoen, onontbindbaar is, A en B Ω-endomorfieën van K zijn en $1 = A+B$, dan is A of B een automorfie.

Bewijs: $A = A^2 + AB = A^2 + BA$, dus $AB = BA$. Als A en B geen van beide een automorfie zijn, zijn ze beide nilpotent (Schur). Nu is $1 = (A+B)^m$ een som van termen A^rB^s met $r+s=m$. Voor m voldoende groot is $A^r = 0$ of $B^s = 0$, hetgeen de tegenspraak $1 = 0$ oplevert.

Past men dit toe op $E_1F_1 = A_1$ en $E_1F_2+\ldots+E_1F_k = B_1$ in G_1. Als A_1 geen automorfie is, dan is B_1 een automorfie, dus B_1^{-1} bestaat. Dus $1 = B_1^{-1}E_1F_2+\ldots+B_1^{-1}E_1F_k$. Als $B_1^{-1}E_1F_2$ geen automorfie is, is $B_1^{-1}E_1F_3+\ldots+B_1^{-1}E_1F_k$ een automorfie enz. Zo vinden we dat er een natuurlijk getal j ($1 \leq j \leq k$) bestaat, zodat $B_{j-1}^{-1}\ldots B_2^{-1}B_1^{-1}E_1F_j$, $B_1^{-1},\ldots,B_{j-1}^{-1}$ automorfieën in G_1 zijn en dus ook E_1F_j een automorfie in G_1. Nummer de H's en de F's nu anders, zodat j=1.

Beschouw nu de Ω-homomorfie F_1 tussen G_1 en $F_1G_1 \subset H_1$. Daar E_1F_1 een automorfie in G_1 is, is F_1 een isomorfie. Nu is F_1G_1 een Ω-ondergroep van H_1 en evenzo $\bar{H}_1$, de verzameling der elementen z van H_1, waarvoor $E_1z = 0$. Bij een $y \in H_1$ is een $w \in G_1$ te vinden, zodat $E_1y = E_1F_1w$. Als we nu schrijven $y = (y - F_1w) + F_1w$, dan is $E_1(y-F_1w)=E_1y-E_1F_1w = 0$, dus $y - F_1w \in \bar{H}_1$; verder is $F_1w \in F_1G_1$. Verder is $\bar{H}_1 \cap F_1G_1 = 0$, want uit $E_1z = 0$, $z = F_1x, x \in G_1$ volgt $E_1F_1x = 0$, dus $x=0$, dus $z = 0$. Dus is $H_1 = \bar{H}_1 + F_1G_1$. Uit de onontbindbaarheid van H_1 volgt, dat $\bar{H}_1 = 0$ of $F_1G_1 = 0$, maar $F_1G_1 = 0$ kan niet, omdat F_1 een isomorfe afbeelding van G_1 is. Dus $\bar{H}_1 = 0$ en $H_1 = F_1G_1$. Dus is F_1 een isomorfie tussen G_1 en H_1 en, omdat E_1F_1 een automorfie van G_1 is, is E_1 een isomorfie tussen H_1 en G_1. Verder is $H_1 \cap (G_2+\ldots+G_h) = 0$, want als $z \in H_1, z \in G_2+\ldots+G_h$, dan is $E_1z = 0$ en daar E_1 een isomorfe afbeelding van H_1 is, $z = 0$. Dus $G' = H_1+G_2+\ldots+G_h$ is een directe som. Beschouw nu $D_1 = F_1E_1 + E_2+\ldots+E_h$, dan beeldt D_1 blijkbaar G op G' af. De directheid van de som in G' geeft nu, dat uit $D_1z = 0$ volgt $F_1E_1z = E_2z = \ldots = E_hz = 0$, maar omdat F_1 een isomorfe afbeelding van G_1 is, is dan ook $E_1z = 0$, dus $z = 0$. Volgens Fitting is dan D_1 een automorfie on $G = G'$. Dus $G = G_1+G_2+\ldots+G_h = H_1+G_2+\ldots+G_h$.

Stel nu dat een paring verkregen is tussen H_i en G_i voor $i = 1, \ldots, r < k$, zodat E_i een Ω-isomorfie tussen H_i en G_i en F_i een Ω-isomorfie tussen G_i en H_i is, $G = H_1+\ldots+H_r+G_{r+1}+\ldots+G_h$ en $D_r = F_1E_1+\ldots+F_rE_r + E_{r+1}+\ldots+E_h$ een Ω-automorfie. Vorm nu restklassengroepen naar $H_1+\ldots+H_r$. Blijkbaar is dan $\bar{G} = \bar{G}_{r+1}+\ldots+\bar{G}_h = \bar{H}_{r+1}+\ldots+\bar{H}_k$, waarin $\bar{G} = G(\text{mod } H_1+\ldots+H_r) \neq 0$, $\bar{G}_1 = (H_1+\ldots+H_r+G_1)$ $(\text{mod } H_1+\ldots+H_r)$. Dan is $\bar{G}_1$ Ω-isomorf met G_1 en $\bar{H}_j$ Ω-isomorf met H_j. Volgens het bovenstaande kunnen we nu, eventueel na permutatie der $H_{r+1},\ldots,H_k$, $\bar{G}_{r+1}$ paren met $\bar{H}_{r+1}$, zodat de overeenkomstige projecties $\bar{E}_{r+1}$ en $\bar{F}_{r+1}$ Ω-isomorfieën zijn tussen $\bar{H}_{r+1}$ en $\bar{G}_{r+1}$ (resp. $\bar{G}_{r+1}$ en $\bar{H}_{r+1}$). Verder is $\bar{G} = \bar{H}_{r+1} + \bar{G}_{r+2}+\ldots+\bar{G}_h$. Als nu $x \in (H_1+\ldots+H_{r+1}) \cap \bar{H}_j = (H_1+\ldots+H_r+H_j)(\text{mod } H_1+\ldots+H_r)$.

$\cap (G_{r+2}+\ldots+G_h)$, dan is de restklasse $\bar{x} \in \bar{H}_{r+1} \cap (\bar{G}_{r+2}+\ldots+\bar{G}_h)$, dus $\bar{x} = 0$, dus $x \in H_1+\ldots+H_r$, maar $(H_1+\ldots+H_r) \cap (G_{r+1}+\ldots+G_h) = 0$, dus $x = 0$, dus $H_1+\ldots+H_{r+1}+G_{r+2}+\ldots+G_h$ is een directe som. Uit $x \in G_{r+1}$, $F_{r+1}x = 0$ volgt $\bar{F}_{r+1}\bar{x} = 0$, dus $\bar{x} = 0$, dus $x \in H_1+\ldots+H_r$, dus $x=0$. Beschouw nu $D_{r+1} = F_1E_1+\ldots+F_{r+1}E_{r+1}+E_{r+2}+\ldots+E_h$ dan beeldt deze G af op $H_1+\ldots+H_{r+1}+G_{r+2}+\ldots+G_h$. Uit $D_{r+1}z = 0$ volgt dan $F_1E_1z = \ldots = F_{r+1}E_{r+1}z = E_{r+2}z = \ldots = E_hz = 0$, Maar dan is ook $E_1z = \ldots = E_{r+1}z = 0$, dus $z = 0$, dus D_{r+1} is een automorfie en $G = H_1+\ldots+H_{r+1}+G_{r+2}+\ldots+G_h$. Verder zijn F_{r+1} en E_{r+1} Ω-isomorfieën tussen G_{r+1} en H_{r+1} (resp. H_{r+1} en G_{r+1}). Hiermee is de volgende stelling verkregen:

Stelling van Remak-Krull-Schmidt: Als G een commutatieve Ω-groep is, waarvan de Ω-ondergroepen aan de maximum- en minimumvoorwaarde voldoen en $G = G_1+\ldots+G_h = H_1+\ldots+H_k$, waarin G_i en H_j onontbindbare Ω-groepen $\neq 0$ zijn dan is $h = k$ en er is een Ω-automorfie D en een ordening der H_j, zodat $DG_i = H_i$ en $G = H_1+\ldots+H_r+G_{r+1}+\ldots+G_h$.

Men kan deze stelling ook voor projecties formuleren als volgt:

Als G een commutatieve Ω-groep is, waarvan de Ω-ondergroepen aan de maximum- en minimumvoorwaarde voldoen en E_i en F_j zijn primitieve projecties $\neq 0$, zodat $E_1+\ldots+E_h = 1$, $F_1+\ldots+F_k = 1$, $E_iE_{i'} = 0$ als $i \neq i'$, $F_jF_{j'} = 0$ als $j \neq j'$, dan is $h = k$ en er is een Ω-automorfie D en een ordening der F_j zodat $F_i = DE_iD^{-1}$ en zodat $D_r = F_1E_1+\ldots+F_rE_r+E_{r+1}+\ldots+E_h$ een Ω-automorfie is.

In beide stellingen kiezen we $D = F_1E_1+\ldots+F_hE_h$, dan is $DE_i = F_iE_i = F_iD_1$, dus $F_i = DE_iD^{-1}$.

Als $G = G' + G''$ een willekeurige directe ontbinding in Ω-groepen is, is er een verfijning van deze tot een ontbinding in onontbindbare Ω-groepen. Als de H_j geschikt geordend worden, is er een automorfie D zodat $DG' = H_1+\ldots+H_t$ en $DG'' = H_{t+1}+\ldots+H_k$.

Laat nu G een commutatieve Ω-groep zijn waarvan de Ω-ondergroepen aan de maximum- en minimumvoorwaarde voldoen en V een verzameling van nilpotente Ω-endomorfieën, die gesloten is t.o.v. vermenigvuldiging. Als s de lengte is van een compositierij van G, dan is $V^s = 0$.

Bewijs: Neem een willekeurig stel $B_1,\ldots,B_s \in V$ en een Ω-ondergroep H van G, zodat $B_iH \subset H$ en stel $B_1\ldots B_sH \neq 0$. Nu is $H \supset B_iH \supset B_iB_jH \supset \ldots$ en iedere $B_i\ldots B_1H$ is een Ω-groep. Dus $H \supset \sum_{i_1} B_{i_1}H \supset \sum_{i_1,i_2} B_{i_1}B_{i_2}H \supset \ldots$ is een dalende ketting Ω-ondergroepen van G. Als ergens een gelijkteken staat, staan verder in de ketting ook gelijktekens. Daar de lengte van een compositierij van H $\leq s$ is, is er een $r < s$ zodat $\sum B_{i_1}\ldots B_{i_r}H = \sum B_{i_1}\ldots B_{i_{r+1}}H$. Noem $H' = \sum B_{i_1}\ldots B_{i_r}H$. Daar $B_1\ldots B_sH \neq 0$, is $H' \neq 0$. Verder is $H' = \sum B_iH = \ldots$, Er bestaat een oneindige rij $B_{i_1}, B_{i_2}, \ldots$ zodat $B_{i_1}\ldots B_{i_p}H' \neq 0$. Stel n.l. p

termen $B_{i_1},\ldots,B_{i_p}$ gevonden zodat $B_{i_1}\ldots B_{i_p}H' \neq 0$. Dan is $B_{i_1}\ldots B_{i_p}H' = -\sum_{j\neq i_1,\ldots,i_p} B_{i_1}\ldots B_{i_p}B_jH$, en dus is er een i_{p+1} zodat $B_{i_1}\ldots B_{i_{p+1}}H' \neq 0$. Laat k een der indices zijn, die oneindig vaak in de rij $B_{i_1},B_{i_2},\ldots$ voorkomen.

Daar we aan de voorkant een eindig aantal termen weg kunnen laten zonder de eigenschap, dat $B_{i_1}\ldots B_{i_p}H' \neq 0$ is te verstoren, mogen we $i_1 = k$ stellen. Dus bestaan er s endomorfieën $C_1,\ldots,C_s$ in V, waarin $C_i = B_kB'_i$ en B'_i een product van B_j's, zodat $C_1\ldots C_sH' \neq 0$. Daar B_k nilpotent is , is $B_kH' < H'$ en daar $\sum C_iH' \subset B_kH'$, is $\sum C_iH' < H'$. Met behulp van de redenering aan het begin van dit bewijs vinden we een Ω -ondergroep $\bar{H} \neq 0$, $< H'$ en dus $< H_1$ zodat $\bar{H} = \sum C_i\bar{H}$. Door de redenering te herhalen vinden we een $\bar{\bar{H}} \neq 0$, $< \bar{H}$ en endomorfieën D_i in V, zodat $\bar{\bar{H}} = \sum D_i\bar{\bar{H}}$. Dit leidt tot een niet-afbrekende dalende ketting Ω -ondergroepen van G. De onderstelling $B_1\ldots B_sH \neq 0$ is dus tegenstrijdig gebleken. Door dit op $H = G$ toe te passen, vinden we $B_1\ldots B_s = 0$.

Veronderstel voor dat de Ω -ondergroepen van G aan de maximum- en minimumvoorwaarde voldoen. Laat $G = G_1+\ldots+G_s$ een directe ontbinding zijn in onontbindbare Ω -groepen. $G_i \neq 0$; laat $1 = E_1+\ldots+E_s$ de bijbehorende projecties zijn. Noem de ring der Ω -endomorfieën S. Voor een $A \in S$ geldt dat A op een en slechts een manier te schrijven is als $A = \sum A_{ij}$, waarin $A_{ij} \in E_iSE_j$. Immers $A = \sum E_iAE_j$ is zo'n schrijfwijze en als $\sum E_iB_{ij}E_j = \sum E_iC_{ij}E_j$ met $B_{ij} \in S$, $C_{ij} \in S$, dan is $E_pB_{pq}E_q = E_p(\sum E_iB_{ij}E_j)E_q = E_p(\sum E_iC_{ij}E_j)E_q = E_pC_{pq}E_q$. Een $A_{ij} \in E_iSE_j$ beeldt G_k voor $k \neq j$ in 0 af en induceert een Ω -homomorfie tussen G_j en een Ω -ondergroep van G_i. We beweren nu dat het radicaal van S juist bestaat uit die Ω -endomorfieën B, waarvan de B_{ij} in de schrijfwijze $B = \sum B_{ij}, B_{ij} \in E_iSE_j$ geen van alle een Ω -isomorfie tussen G_j en G_i induceren. We moeten dus bewijzen, dat de verzameling R van deze B een nilpotent ideaal in S is en dat alle nilpotente idealen van S in R bevat zijn. Laat $B \in R$, $B = \sum B_{ij}$, $C \in R, C = \sum C_{ij}$ zijn en noem $A_{ij} = B_{ij} + C_{ij}$. Als A_{ij} een Ω -isomorfie $\bar{A}_{ij}$ tussen G_j en G_i induceert, stellen we $D_{ji} = E_j\bar{A}_{ij}^{-1}E_i$ dan is $D_{ji} \in E_jSE_i$. Nu volgt uit $P_{li} \in E_lSE_i$, $B_{ij} \in R$, $B_{ij} \in E_iSE_j$ dat $P_{li}B_{ij} \in R$. Daar $B_{ij} \in R$ geldt dat er een $z \neq 0$ in G_j is waarvoor $B_{ij}z = 0$ of dat $G'_i = B_{ij}G_j < G_i$. Als $B_{ij}z = 0$, dan ook $P_{li}B_{ij}z = 0$. Laat $G_i' < G_i$ zijn en stel dat $P_{li}B_{ij}$ een Ω -isomorfie tussen G_j en G_l induceert. Dan induceert P_{li} een Ω -isomorfie tussen G_i' en G_l. Dan bewijst men op dezelfde wijze als in het bewijs van de stelling van Remak-Krull-Schmidt dat $G_i = G_i' + G_i''$, waarin G_i'' de verzameling van die $z \in G_i$ is, waarvoor $P_{li}z = 0$.

(Bij $y \in G_i$ is een $w \in G_j$, zodat $P_{li}y=P_{li}B_{ij}w$; dan is $y=B_{ij}w+(y-B_{ij}w) \in$ $\in (G_i', G_i'')$; verder volgt uit $y=B_{ij}x$, $x \in G_j$, $P_{li}y=0$, dat $P_{li}B_{ij}x=0$, dus $x=0$, dus $y=0$). Uit de onontbindbaarheid van G_i volgt dat $G_i'=0$ of $G_i''=0$, maar $G_i''=0$ is onmogelijk wegens $G_i' < G_i$ en $G_i'=0$ is onmogelijk omdat $G_i=G_i''$ in strijd is met het feit dat P_{li} de hele G_l als beeld heeft. Dus $P_{li}B_{ij}$ induceert geen Ω-isomorfie tussen G_j en G_l, dus $P_{li}B_{ij} \in R$. Hieruit volgt dat noch $D_{ji}B_{ij}$ noch $D_{ji}C_{ij}$ een automorfie in G_j induceert, maar daar $E_j=\overline{A}_{ij}^{-1}A_{ij}=D_{ji}A_{ij}=D_{ji}B_{ij}+D_{ij}C_{ij}$ en E_j de identieke transformatie in G_j induceert komen we in strijd met een vroeger bewezen hulpstelling. Dus $B+C \in R$. Nu bewijzen we dat als $B \in R$, $B=\sum B_{ij}$, $A \in S$, $A=\sum A_{ij}$, dan $AB \in R$ en $BA \in R$ is. Het is voldoende te bewijzen dat $B_{ij}A_{kl} \in R$ en $A_{kl}B_{ij} \in R$. Voor $l \neq i$ is $A_{kl}B_{ij}=0 \in R$; voor $A_{ki}B_{ij}$ is het hierboven al bewezen. Als $j \neq k$ is $B_{ij}A_{kl}=0 \in R$; als A_{jl} geen Ω-isomorfie tussen G_i en G_j induceert, geldt $A_{jl} \in R$ en dus is $B_{ij}A_{jl} \in R$ al bewezen; als A_{jl} wel een Ω-isomorfie tussen G_j en G_j induceert, dan induceert $B_{ij}A_{jl}$ geen Ω-isomorfie tussen G_l en G_i omdat B_{ij} geen Ω-isomorfie tussen G_j en G_i induceert, dus $B_{ij}A_{jl} \in R$. Hiermee is bewezen dat R een ideaal is.

Om te bewijzen dat R nilpotent is nemen we een $B \in R$, $B=\sum B_{ij}$ en ontbinden G zo in $G=G'+G''$ dat B in G' nilpotent en in G'' een automorfie is (Fitting).

(Volgens de stelling van Remak-Krull-Schmidt is er een Ω-automorfie U en een ordening der G_i zodat $UG'=H_1=G_1+\ldots+G_t$ en $UG''=H_2=G_{t+1}+\ldots+G_s$. Dan is $C=UBU^{-1} \in R$ en C induceert een automorfie $\overline{C}$ in H_2. Stel $G'' > 0$, dus $t < s$. Noem $E^{(2)}=E_{t+1}+\ldots+E_s$, dan is $E^{(2)}=C\overline{C}^{-1}E^{(2)} \in R$, en dan ook $E_s=E^{(2)}E_s \in R$, maar $E_s \in E_sSE_s$ en is de identieke transformatie, dus een automorfie in G_s, dus $E_s \notin R$. Dit geeft een tegenspraak, dus $t=s$, $G''=0$, dus B is nilpotent. Uit de vorige stelling volgt dat R nilpotent is. Als T een nilpotent ideaal in S is en $N \in T$, $N=\sum N_{ij}$, dan is $N_{ij}=E_iNE_j$ dus $N_{ij} \in T$. Daar N_{ij} nilpotent is, kan N_{ij} geen isomorfie tussen G_j en G_i induceren, dus $N \in R$, dus $T \subset R$. Daarmee is alles bewezen en de volgende stelling verkregen:

Als $G=G_1+\ldots+G_s$ een ontbinding in onontbindbare Ω-groepen $\neq 0$ is van de Ω-groep G, waarvan de Ω-ondergroepen aan de maximum- en minimumvoorwaarden voldoen, $1=E_1+\ldots+E_s$ de bijbehorende projecties en S de ring der Ω-endomorfieën van G zijn, dan vormen de Ω-endomorfieën $\sum B_{ij}$, waarin $B_{ij} \in E_iSE_j$ en B_{ij} geen van alle Ω-isomorfieën tussen G_j en G_i induceren, een nilpotent ideaal R in S, dat alle nilpotente idealen in S omvat. R is dus het radicaal van S.

Rangschik nu G_i zo dat $G_1,\ldots,G_{k_1}$ onderling Ω-isomorf zijn, $G_{k_1+1},\ldots,G_{k_1+k_2}$ onderling Ω-isomorf, maar niet Ω-isomorf met $G_1,\ldots,G_{k_1}$ enz. tot $G_{k_1+\ldots+k_{t-1}+1},\ldots,G_{k_1+\ldots+k_t}$. Noem $G^{(1)}=G_1+\ldots+G_{k_1}$, $G^{(2)}=G_{k_1+1}+\ldots+G_{k_1+k_2},\ldots,G^{(t)}=G_{k_1+\ldots+k_{t-1}+1}+\ldots+G_{k_1+\ldots+k_t}$ en

$E^{(1)}=E_1+\ldots+E_{k_1},\ldots,E^{(t)}=E_{k_1+\ldots+k_{t-1}+1}+\ldots+E_{k_1+\ldots+k_t}$. Als i en j in verschillende gebieden $k_1+\ldots+k_{p-1}+1,\ldots,k_1+\ldots+k_p$ en $k_1+\ldots+k_{q-1}+1,\ldots,k_1+\ldots+k_q$ liggen, dan is $E_iSE_j \subset R$. Dus is $E^{(p)}SE^{(q)} \subset R$ als $p \neq q$ en daar $S=\sum_{p,q} E^{(p)}SE^{(q)}=(E^{(1)}SE^{(1)},\ldots,E^{(t)}SE^{(t)},R)$ en $E^{(p)}SE^{(p)}E^{(q)}SE^{(q)}=0$ voor $p \neq q$ is $(E^{(p)}SE^{(p)},R)$ een ideaal in S en $\bar{S}=S(\text{mod } R)=\bar{S}_1+\ldots+\bar{S}_t$, waarin $\bar{S}_p=(E^{(p)}SE^{(p)},R)(\text{mod } R)$. Daar $E^{(p)} \in E^{(p)}SE^{(p)}$ en $E^{(p)} \notin R$ is $\bar{S}_p \neq 0$. Nu is, zoals we vroeger gezien hebben het verband tussen $A_\rho \in E^{(p)}SE^{(p)}$ en zijn effect geïnduceerd in $G^{(p)}$ een isomorfie tussen $E^{(p)}SE^{(p)}$ en de ring van de Ω-endomorfieën van $G^{(p)}$. Daaruit volgt dat het radicaal van $E^{(p)}SE^{(p)}$ bestaat uit de elementen $\sum B_{ij}$ waarin i en j beide behoren tot $k_1+\ldots+k_{p-1}+1,\ldots,k_1+\ldots+k_p$ en B_{ij} geen van alle isomorfieën tussen G_j en G_i zijn. Het radicaal van $E^{(p)}SE^{(p)}$ is dus $E^{(p)}SE^{(p)} \cap R=E^{(p)}RE^{(p)}$ en hieruit volgt door toepassing van de eerste isomorfiestelling dat $\bar{S}_p$ isomorf is met $E^{(p)}SE^{(p)} \pmod{E^{(p)}RE^{(p)}}$.

Stel nu dat G <u>homogeen</u> is in die zin dat al zijn onontbindbare componenten G_i Ω-isomorf zijn (dus t=1). Dan hebben we vroeger bewezen dat S een matrixring T_s is, waarin T isomorf is met de ring van de Ω-endomorfieën van G_i, maar omdat G_i onontbindbaar is, is T volledig primair.

Stel nu dat S een matrixring T_s is over een volledig primaire ring T, dan is $T(\text{mod } R')$ een scheef lichaam als R' het radicaal van T is. Dan is $R \cap T$ een nilpotent ideaal in T, dus $R \cap T \subset R'$. Aan de andere kant, als E_{ij} de matrixbasis van S vormen en $A_{ij} \in R'$ dan vormen de elementen $\sum E_{ij}A_{ij}$ een nilpotent ideaal in S dat dus bevat is in R. Speciaal is voor $A \in R'$ ook $A=\sum E_{ii}A \in R$ dus $R' \subset R$. Dus $R \cap T=R'$. Als $B=\sum E_{ij}B_{ij}$ een element van R is, is $B_{ij}=\sum_k E_{ki}BE_{jk}$ een element van $R \cap T=R'$. Dus is $R=R'_s$ en de restklassering $\bar{S}=S \pmod R$ is isomorf met $(T(\text{mod}R'))_s$, een matrixring over een scheef lichaam, dus een enkelvoudige ring.

Stel nu dat $\bar{S}=S(\text{mod } R)$ enkelvoudig is. Verder is in het algemeen $\bar{S}=\bar{S}_1+\ldots+\bar{S}_t$ met $\bar{S}_i \neq 0$, dus in dit geval moet t=1, dus G homogeen zijn. Daarmee is de kring van implicaties gesloten en de volgende stelling verkregen:

Voor een Ω-groep G, waarvan de Ω-ondergroepen aan de maximum- en minimumvoorwaarden voldoen en waarvan S de ring van Ω-endomorfieën en R het radicaal van S is, zijn de volgende voorwaarden aequivalent:

1° G is homogeen ,

2° $S=T_s$ matrixring van graad s over een volledig primaire ring T,

3° $S(\text{mod } R)$ is enkelvoudig.

Als in een ring S met één de l-idealen aan de minimumvoorwaarde voldoen, dan voldoen ze ook aan de maximumvoorwaarde.

Bewijs: Als het radicaal R van S nul is en S dus halfenkelvoudig is hebben we het al vroeger bewezen. We mogen dus aannemen dat er een natuurlijk getal s is, zodat $R^s \neq 0$, $R^{s+1} = 0$. We beschouwen de reguliere representatie van S, d.w.z. we vatten de additieve groep van S op als S-modulus met als vermenigvuldiging de gewone ringvermenigvuldiging. Deelmoduli zijn dan juist l-idealen. De deelmoduli voldoen dus aan de minimumvoorwaarde. Nu is $S > R > \ldots > R^s > 0$ een dalende keten S-moduli. De restklassenmoduli S(mod R), R(mod R^2),... worden alle geannuleerd door R en zijn dus op te vatten als S(mod R)-moduli. Verder voldoen de restklassenmoduli S(mod R), R(mod R^2),... ook aan de minimumvoorwaarde. Daar $\bar{S}$=S(mod R) halfenkelvoudig is en zijn één de identieke transformatie in S(mod R), R(mod R^2),... induceert (immers S had zelf een één), volgt uit een stelling uit de representatietheorie, dat de $\bar{S}$-deelmoduli van deze $\bar{S}$-moduli ook aan de maximumvoorwaarde voldoen en dat deze $\bar{S}$-moduli dus compositierijen bezitten. Laat b.v. S(mod R)= $\bar{L}_1 > \bar{L}_2 > \ldots > \bar{L}_m = 0$ zijn, waarin $\bar{L}_j$(mod $\bar{L}_{j+1}$) irreducibele $\bar{S}$-moduli en dus irreducibele S-moduli zijn. Dus $S=L_1 > L_2 > \ldots > L_m=R$, waarin L_j het l-ideaal is dat op $\bar{L}_j$ wordt afgebeeld in de homomorfie tussen S en S(mod R). Volgens de tweede isomorfiestelling is L_j(mod L_{j+1}) S-isomorf met $\bar{L}_j$(mod $\bar{L}_{j+1}$) en dus een irreducibele S-modulus. Evenzo $R=L_m > \ldots > L_{m+p} = R^2$, waarin L_k weer l-idealen zijn en L_k(mod L_{k+1}) irreducibele S-moduli enz. Zo is $S=L_1 > \ldots > 0$ een compositierij van S-moduli en de S-moduli (dat zijn de l-idealen van S) voldoen dus ook aan de maximumvoorwaarde.

Op grond van deze stelling kunnen we de stellingen over endomorfieënringen nu toepassen. Laat S een ring met één zijn, waarvan de l-idealen aan de minimumvoorwaarde en dus aan de maximumvoorwaarde voldoen. Omdat S een één heeft, is S invers-isomorf met de ring van de rechtsvermenigvuldigingen van de additieve groep G van S. Vatten we G op als Ω-groep, waarin Ω bestaat uit de linksvermenigvuldigingen, dan zijn de Ω-ondergroepen van G de l-idealen van S en de Ω-endomorfieën van G zijn de rechtsvermenigvuldigingen. Hieruit volgt nu onmiddellijk:

Als S een ring met één is, waarvan de l-idealen aan de minimumvoorwaarde voldoen, dan is iedere nildeelring van S nilpotent.

Als S een ring met één is, waarvan de l-idealen aan de minimumvoorwaarde voldoen, dan zijn de volgende voorwaarden aequivalent:

1° S is een directe som van l-idealen, die als Ω-groepen (Ω bestaande uit de linksvermenigvuldigingen van de additieve groep van S) onontbindbaar en onderling Ω-isomorf zijn,

2° S(mod R) is enkelvoudig, waarin R het radicaal van S is.

3° $S=T_s$ een matrixring van graad s over een volledig primaire ring T.

Als een van deze voorwaarden vervuld is, heet S een primaire ring.

We zullen een l-ideaal A van S, dat als Ω-groep opgevat onontbindbaar is ook een onontbindbaar l-ideaal van S noemen, d.w.z. als A=B+C en B en C zijn l-idealen van S en dan is B=0 of C=0.

We nemen nog steeds aan dat S een één heeft en de l-idealen van S aan de minimumvoorwaarde voldoen. Als $S=L_1+\ldots+L_k$, L_i l-idealen en $1=e_1+\ldots+e_k$ de bijbehorende ontbinding van 1, dan is $e_i=e_ie_1+\ldots+e_ie_k$ en daar $e_ie_j \in L_j$, geldt $e_ie_j=0$ als $i\neq j$ en $e_i^2=e_i$. Verder is evenzo voor $a_i \in L_i$ $a_i=a_ie_1+\ldots+a_ie_k$, dus $a_ie_j=0$, voor $i\neq j$ en $a_ie_i=a_i$, dus $L_i=Se_i$. Laat omgekeerd $1=e_1+\ldots+e_l$ zijn met $e_ie_j=0$, voor $i\neq j$ en $e_i^2=e_i$, dan is $S=Se_1+\ldots+Se_l$, want als $x_1e_1+\ldots+x_le_l=0$ dan is $0=x_1e_1e_i+\ldots+x_le_le_i=x_ie_i$.

In een ring S met één, waarvan de l-idealen aan de minimumvoorwaarde voldoen is een minimaal niet-nilpotent l-ideaal hetzelfde als een onontbindbaar bestanddeel $\neq 0$ in een directe ontbinding van S in l-idealen.

Bewijs: 1° Laat A een minimaal niet-nilpotent l-ideaal van S zijn. A bevat een idempotent e (zie blz. 19). Nu is $Se \subset A$ en Se is een l-ideaal en niet-nilpotent want $e=e^2 \in Se$. Uit de minimaliteit van A volgt dat $Se=A$. Nu is $(1-e)^2=1-e$ en $e(1-e)=(1-e)e=0$, dus $S=Se+S(1-e)$. Verder is A onontbindbaar, want als $A=B+C$ was met $0<B<A$, $0<C<A$, B en C l-idealen in S, dan volgde uit de minimaliteit van A, dat B en C nilpotent zouden zijn, maar dan was A ook nilpotent.

2° Laat A een onontbindbaar bestanddeel $\neq 0$ zijn in een directe ontbinding van S in l-idealen, dus $S=A+B$, A en B l-idealen. Laat hierbij $1=e_1+e_2$ zijn, dan is $A=Se_1$. Omdat $A\neq 0$, is $e_1\neq 0$, dus e_1 een idempotent, verder $e_1 \in A$, dus A niet nilpotent. Als A niet minimaal is als niet-nilpotent l-ideaal, is er een minimaal niet-nilpotent l-ideaal $L<A$. Dan is $L=Se_3$, e_3 idempotent. Dan is $e_3e_1=e_3$ (e_1 is rechtséén in A); verder is voor alle $a \in A$, $ae_2=0$. Schrijven we nu $1=e_1e_3+(e_1-e_1e_3)+e_2$; dan is $(e_1e_3)^2=e_1e_3$, $(e_1-e_1e_3)^2=e_1-e_1e_3$, $e_2^2=e_2$, $e_1e_3(e_1-e_1e_3)=(e_1-e_1e_3)e_1e_3=e_1e_3e_2=e_2e_1e_3=(e_1-e_1e_3)e_2=e_2(e_1-e_1e_3)=0$, dus $S=Se_1e_3+S(e_1-e_1e_3)+Se_2$ en $A=Se_1e_3+S(e_1-e_1e_3)$. Maar $e_3=e_3e_1e_3 \in Se_1e_3$, dus $Se_1e_3=Se_3$, dus $A=L+S(e_1-e_1e_3)$ en $0<L<A$. Dit is in strijd met de onontbindbaarheid van A. Dus A is een minimaal niet-nilpotent l-ideaal.

Laat S een ring met één zijn, waarvan de l-idealen aan de minimumvoorwaarde voldoen. Als $S=L_1+\ldots+L_s$, L_i l-idealen $\neq 0$ $1=e_1+\ldots+e_s$, R het radicaal van S, $\bar{e}_i$ de restklasse (mod R) waar e_i in ligt en $\bar{1}$ die waar 1 in ligt, dan is blijkbaar $\bar{1}=\bar{e}_1+\ldots+\bar{e}_s$, $\bar{e}_i\bar{e}_j=0$ als $i\neq j$, $\bar{e}_i^2=\bar{e}_i\neq 0$ en $\bar{S}=S(\text{mod } R)=S\bar{e}_1+\ldots+S\bar{e}_s$. We willen nu bewijzen, dat iedere ontbinding van $\bar{S}$ in l-idealen nu ook op deze wijze te krijgen is. Het is blijkbaar voldoende, hiertoe de volgende hulpstelling te bewijzen:

Als $\bar{a}_1,\ldots,\bar{a}_k$ idempotente elementen in $\bar{S}$ zijn, zodat $\bar{a}_i\bar{a}_j=0$ voor $i\neq j$, dan is het mogelijk idempotente elementen $e_1,\ldots,e_k$ in S te kiezen, zodat e_i in de restklasse $\bar{a}_i$ ligt en $e_ie_j=0$ voor $i\neq j$; verder volt uit $\bar{a}_1+\ldots+\bar{a}_k=\bar{1}$, dat $e_1+\ldots+e_k=1$.

Bewijs: Laat $e_1,\ldots,e_m$ al bepaald zijn, zodat $e_i \in \bar{a}_i$, $e_i e_j = 0$ voor $i \neq j$, $e_i^2 = e_i$. Kies een $u \in \bar{a}_{m+1}$ en stel $v=u-eu-ue+eue$ met $e=\sum_{i=1}^{m} e_i$, dan is $v \equiv u \pmod R$ want $\overline{eu} = \sum_{i=1}^{m} \bar{a}_i \bar{a}_{m+1} = 0$ enz. Verder is $e_i v = v e_i = 0$ voor $i=1,\ldots,m$. Dus is $v^2 = v+z$ met z nilpotent; laat $z^s=0$. Nu is $zv=v^3-v^2=vz$. We proberen nu een element $w=f(z)v+g(z)$ te bepalen, zodat $w^2=w$ en $f(z)$ en $g(z)$ polynomen in z zijn met gehele coëfficiënten en wel $f(z)$ met constante term 1 en $g(z)$ met constante term 0. Dit leidt tot de vergelijkingen $f^2+2fg-f=0$ en $zf^2+g^2-g=0$. We lossen deze vergelijkingen eerst op in machtreeksen in een onbepaalde t. Door eliminatie vinden we $f(t)=(1+4t)^{-\frac{1}{2}}$ en $g(t)=\frac{1}{2}(1-f(t))$. Nu is $(1+4t)^{-\frac{1}{2}} = \sum_{n=0}^{\infty} \binom{-\frac{1}{2}}{n} 2^{2n} t^n = 1+\sum_{n=1}^{\infty} (-1)^n \binom{2n-1}{n} 2t^n$; de coëfficiënten zijn alle geheel. Hetzelfde geldt ook voor $g(t)$. De machtreeksen voldoen formeel aan de gevraagde betrekkingen. Vullen we z in voor t dan worden alle machten met exponent $\geq s$ nul; er komen dan veeltermen in z. Nu is $w \equiv v \pmod R$ en w idempotent. Verder is $e_i z = e_i(v^2-v)=0$ dus $e_i w = e_i f(z) v + e_i g(z) = 0$ en evenzo $we_i=0$. Dus kan w gebruikt worden als het element e_{m+1}. Als $\sum \bar{a}_i = \bar{1}$, dan is $\sum e_i = 1+y$, $y \in R$. Daar $\sum e_i$ idempotent is, is $(1+y)^2=1+y$, dus $y^2+y=0$, dus $y=-y^2=y^3=\ldots=0$, dus $\sum e_i = 1$.

Met een directe ontbinding $\bar{S}=\bar{S}\bar{a}_1+\ldots+\bar{S}\bar{a}_k$ met $\bar{1}=\bar{a}_1+\ldots+\bar{a}_k$ correspondeert $S=Se_1+\ldots+Se_k$ met $1=e_1+\ldots+e_k$. Blijkbaar is $\bar{S}\bar{a}_i$ onontbindbaar dan en slechts dan als Se_i onontbindbaar is. Omdat $\bar{S}$ halfenkelvoudig is, is $\overline{Sa_i}$ onontbindbaar dan en slechts dan als hij irreducibel is.

Beschouw nu $T=Se_i+Se_j=Se$, $e=e_i+e_j$, e_i en e_j primitief. Daar $S=T+S(1-e)$ zijn de projecties E en E' behorende bij deze ontbinding de rechtsvermenigvuldigingen $G(e)$ en $G(1-e)$. Noem weer Ω de ring der linksvermenigvuldigingen van S, dan is de ring ϕ der Ω-endomerfieën juist de ring der rechtsvermenigvuldigingen. De ring der Ω-endomorfieën van T is dan isomorf met $E \phi E$, dus invers-isomorf met eSe. Dus zijn Se_i en Se_j dan en slechts dan Ω-isomorf als eSe primair is. Nu is eSe (mod $R \cap eSe$) isomorf met $(eSe,R)(\mathrm{mod}\ R)=\overline{eSe}$ en $\overline{eSe}$ is invers-isomorf met de ring der Ω-endomorfieën van $\bar{T}=\bar{S}e$. Daar $\bar{T}$ volledig reducibel is, is $\overline{eSe}$ halfenkelvoudig. Hieruit volgt dat $R \cap eSe = eRe$, dat blijkbaar bevat is in het radicaal van eSe, met dit radicaal samenvalt. Dus is eSe primair dan en slechts dan als $\overline{eSe}$ enkelvoudig is en hieruit volgt:

Als $S=Se_1+\ldots+Se_k$, e_i primitief, dan zijn Se_i en Se_j dan en slechts dan Ω-isomorf als $\overline{Se_i}$ en $\overline{Se_j}$ Ω-isomorf zijn (alles onder dezelfde veronderstellingen en notaties als boven).

Als L een onontbindbaar l-ideaal van S is dat in een directe ontbinding van S in l-idealen optreedt, dan is er een grootste l-ideaal van S dat $\prec$ L is. Als L en L' onontbindbare l-idealen van S zijn, die in (eventueel verschillende) directe ontbindingen van S in l-idealen optreden dan zijn L en L' dan en slechts dan Ω-isomorf, als hun eerste composi-

tiefactoren Ω -isomorf zijn.

Bewijs: L is minimaal niet-nilpotent l-ideaal van S, dus is ieder l-ideaal van S, dat $< L$ is, nilpotent. Blijkbaar is $R \cap L$ het grootste dergelijke l-ideaal. De eerste compositiefactor van L is $L(\text{mod } R \cap L)$ en deze is isomorf met $(L,R)(\text{mod } R)=\bar{L}$. Volgens Remak-Krull-Schmidt is L Ω -isomorf met een van de l-idealen L_1 die voorkomen in de ontbinding van S die L' bevat. Dus zijn L en L' Ω -isomorf dan en slechts dan als hun eerste compositiefactoren het zijn.

We willen nu een verband leggen tussen de ontbinding van S in onontbindbare l-idealen en die in onontbindbare idealen. Hiertoe dient de volgende hulpstelling.

Laat G en G' S-moduli zijn met compositierijen, laat verder G een grootste deelmodulus $H < G$ hebben en G S-homomorf zijn met een S-deelmodulus $K \neq 0$ van G'. Dan bevat iedere compositierij van G' een factor die S-isomorf is met $G(\text{mod } H)$.

Bewijs: Laat Z de kern zijn van de homomorfie tussen G en K, dan is K S-isomorf met $G(\text{mod } Z)$. Daar $K \neq 0$, is $Z < G$, dus $Z \subset H$. Dus $G(\text{mod } Z) > H(\text{mod } Z)$, dus $G(\text{mod } Z)$ heeft de compositiefactor $G(\text{mod } Z)(\text{mod } H(\text{mod } Z))$, die S-isomorf is met $G(\text{mod } H)$. Hetzelfde geldt dus voor K, dus voor G'.

We beschouwen weer de onontbindbare l-idealen die in directe ontbindingen voorkomen, dat zijn de l-idealen Se waarin e een primitieve idempotent is. We zeggen dat twee dergelijke l-idealen Se en Se' tot hetzelfde blok behoren als er een eindige rij onontbindbare l-idealen $Se=Se_1, Se_2, \ldots, Se_k=Se'$ bestaat zodat iedere Se_i een compositiefactor bevat, S-isomorf met een van de compositiefactoren van Se_{i+1}. Deze relatie is blijkbaar een aequivalentierelatie en leidt dus tot een indeling van deze idealen in blokken. We noemen de rij Se_i een rij die Se en Se' verbindt. De volgende stelling legt een verband tussen een ontbinding in eenzijdige en in tweezijdige idealen.

Laat S een ring met één zijn waarvan de l-idealen aan de minimumvoorwaarde voldoen, laat verder $S=A_1+\ldots+A_n$ de ontbinding zijn van S in onontbindbare (tweezijdige) idealen. Dan behoren twee onontbindbare l-idealen Se en Se' dan en slechts dan tot hetzelfde blok als ze bevat zijn in dezelfde A_i. Dus is A_i de som van een stel onontbindbare l-idealen Se die tot hetzelfde blok behoren.

Bewijs: Een onontbindbaar l-ideaal L is altijd bevat in een der A_i, want $L_i=A_iL \subset L \cap A_i$ is een l-ideaal $\subset A_i$ en $L=SL=L_1+\ldots+L_n$.
Uit de onontbindbaarheid van L volgt dat alle $L_i=0$ zijn op één na. Stel nu eerst dat Se en Se' tot hetzelfde blok behoren en dat Se en Se' in verschillende A_i liggen, b.v. $Se \subset A_1$, $Se' \subset A_2$. Laat $1=d_1+\ldots+d_n$ met $d_i \in A_i$ zijn, dan is d_i de één van A_i. Dus is $d_1(Se)=Se$ en $d_1(Se')=0$ en dus is geen compositiefactor van Se S-isomorf met een van Se'. Als Se_j een rij is die Se en Se' verbindt dan volgt hieruit dat Se_j en Se_{j+1} in dezelfde A_i moeten liggen en dus dat Se en Se' in dezelfde A_i moeten

liggen. Stel nu dat Se en Se' tot verschillende blokken behoren, dan is Se'Se=0. Als n.l. Se'Se$\neq$ 0 was, was er een element b=e'ae$\neq$ 0 en de rechtsvermenigvuldiging G(b) induceerde een S-homomorfie tussen Se' en een S-deelmodulus $\neq$ 0 van Se. Uit de hulpstelling volgt dat Se en Se' isomorfe compositiefactoren zouden bezitten. Dus Se'Se=0. Laat nu $S=Se_1+\ldots+Se_k$ een ontbinding van S in onontbindbare l-idealen $\neq$ 0 zijn. Laat $Se_1,\ldots,Se_{k_1}$ tot hetzelfde blok behoren, $Se_{k_1+1},\ldots,Se_{k_1+k_2}$ tot hetzelfde blok behoren, maar tot een ander blok dan Se_1 enz. Noem $T_1=$ $= Se_1+\ldots+Se_{k_1}$, $T_2=Se_{k_1+1}+\ldots+Se_{k_1+k_2}$ enz. Dan is $Se_iSe_j=0$ als $i\leqslant k_1$; $j>k_1$. Dus is $(Se_i)S\subset(Se_i)T_1\subset T_1$ en dus is T_1 een ideaal en daar T_1 een som is van l-idealen uit hetzelfde blok is T_1 bevat in een der A_j. Hetzelfde geldt voor de andere T_j; dus kunnen we stellen $T_1=A_1,\ldots,T_n=A_n$. Neem nu weer aan dat Se en Se' tot verschillende blokken behoren. We mogen onderstellen dat $Se=Se_1\subset A_1$. Dan is $Se'Se_i=0$ voor $i\leqslant k_1$. Daar Se'S$\neq$ 0, is er een $j>k_1$ zodat $Se'Se_j\neq 0$ dus Se' en Se_j behoren tot hetzelfde blok en dus geldt $Se'\subset A_i$ met $i>1$, dus Se en Se' liggen in verschillende A_i.

De volgende stelling geeft een verband tussen ontbindingen in l-idealen en in r-idealen.

Als $S=Se_1+\ldots+Se_n$, dan is $S=e_1S+\ldots+e_nS$. Het r-ideaal e_iS is dan en slechts dan onontbindbaar als Se_i het is. Als Se_i en Se_j onontbindbaar zijn, zijn ze dan en slechts dan S-isomorf als e_iS en e_jS S-isomorf zijn.

Bewijs: Onontbindbaarheid betekent in beide gevallen, dat e_i primitief is. Voor het laatste deel van de stelling nemen we eerst aan dat S halfenkelvoudig is. Dan is de voorwaarde dat Se_i en Se_j S-isomorf zijn, dat ze in hetzelfde enkelvoudige ideaal A van S liggen. Daar $Se_i\subset A$ dan en slechts dan als $e_iS\subset A$ geeft dit de bewering voor dat geval. In het algemene geval volgt het door overgang op de restklassenring modulo het radicaal.

Hiermee hebben we voor de ringen met één, waarvan de l-idealen aan de minimumvoorwaarde voldoen structuurstellingen opgesteld die een zekere analogie vertonen met de structuurstellingen voor halfenkelvoudige ringen. In plaats van de eerste hoofdstelling komt nu een ontbinding in minimale niet-nilpotente l-idealen. Verder voldoen de l-idealen ook aan de maximumvoorwaarde. In de plaats van de tweede hoofdstelling komt nu een ontbinding in onontbindbare idealen; de in zo'n component bevatte minimale niet-nilpotente l-idealen behoren tot hetzelfde blok. Als de minimale niet-nilpotente l-idealen S-isomorf zijn is de ring primair. S is dus wel een directe som van primaire ringen, die elkaar evenwel niet behoeven te annuleren. Een primaire ring is een matrixring over een volledig primaire ring; de restklassenring van een volledig primaire ring naar zijn radicaal is een scheef lichaam.

We gaan nu over tot een nadere beschouwing van hypercomplexe systemen. Laat S_1 en S_2 hypercomplexe systemen zijn over hetzelfde grondlichaam Φ. We definiëren dan een direct product $S_1 \times S_2$ als volgt:

Kies een basis $y_1,\ldots,y_{n_1}$ in S_1 en een basis $z_1,\ldots,z_{n_2}$ in S_2. Laat $y_i y_j = \sum_p \gamma^{(1)}_{ijp} y_p$ en $z_k z_l = \sum_q \gamma^{(2)}_{klq} z_q$ zijn. Nu is $S_1 \times S_2$ een algebra over Φ met basis x_{ik} $(i=1,\ldots,n_1,\ k=1,\ldots,n_2)$ en vermenigvuldigingstabel $x_{ik}x_{jl} = \sum_p \sum_q \gamma^{(1)}_{ijp}\gamma^{(2)}_{klq} x_{pq}$. De associativiteit van deze vermenigvuldiging volgt direct uit de associativiteit van de vermenigvuldiging der y_i resp. z_k. Dus is $S_1 \times S_2$ een hypercomplex systeem van rang $n_1 n_2$ over Φ; de definitie hangt echter behalve van S_1 en S_2 ook nog van de basiskeuze in beide algebra's af. Kiest men echter b.v. in S_1 een andere basis $\bar{y}_1,\ldots,\bar{y}_{n_1}$ $(\bar{y}_i = \sum_p \alpha_{ip} y_p, y_s = \sum_j \beta_{sj}\bar{y}_j)$ dan is $\bar{y}_i\bar{y}_j = \sum_{t,r} \alpha_{it}\alpha_{jr} y_t y_r = \sum_{t,r,s,u} \alpha_{it}\alpha_{jr}\gamma^{(1)}_{trs}\beta_{su}\bar{y}_u$. Vormt men nu $\overline{S_1 \times S_2}$ met de nieuwe basis van S_1 dan geldt voor de nieuwe basiselementen $\bar{x}_{ik}$, dat $\bar{x}_{ik}\bar{x}_{jl} = \overline{\sum_{p,q,t,r,s} \alpha_{it}\alpha_{jr}\gamma^{(1)}_{trs}\beta_{sp}\gamma^{(2)}_{klq}x_{pq}}$. De toevoeging $\bar{x}_{ik} \to \sum_t \alpha_{it}x_{tk}$, $x_{ik} \to \sum_t \beta_{is}\bar{x}_{sk}$ induceert echter een isomorfie tussen beide systemen, immers $\bar{x}_{ik}\bar{x}_{jl} \to \overline{\sum_{p,q,t,r,s,u} \alpha_{it}\alpha_{jr}\gamma^{(1)}_{trs}\beta_{sp}\gamma^{(2)}_{klq}\alpha_{pu}x_{uq}} =$

$= \overline{\sum_{q,t,r,s} \alpha_{it}\alpha_{jr}\gamma^{(1)}_{trs}\gamma^{(2)}_{klq}x_{sq}} = \sum_{t,r} \alpha_{it}\alpha_{jr}x_{tk}x_{rl} =$

$= (\sum_t \alpha_{it}x_{tk})(\sum_r \alpha_{jr}x_{rl})$.

We kunnen dus zeggen, dat, op isomorfie na, $S_1 \times S_2$ niet van de keuze van de basis in S_1 (en evenzo natuurlijk in S_2) afhangt. Laat nu S_2 een één bezitten en kies deze als eerste basiselement, dus $z_1 = 1$; dan is $\gamma^{(2)}_{k1q} = \gamma^{(2)}_{1kq} = \delta_{kq}$. De elementen x_{i1} brengen dan een deelalgebra voort isomorf met S_1, immers $x_{i1}x_{j1} = \sum_p \gamma^{(1)}_{ijp}x_{p1}$. Dan is dus $S_1 \times S_2$, als we deze deelalgebra met S_1 identificeren, een uitbreiding van S_1. Evenzo is als S_1 een één heeft $S_1 \times S_2$ een uitbreiding van S_2. Als beide een één hebben en $y_1 = 1$, $z_1 = 1$ is, is $x_{ij} = x_{i1}x_{1j}$, dus na identificatie is $x_{ij} = y_i z_j$; evenzo is $x_{ij} = z_j y_i$. Een willekeurig element van $S_1 \times S_2$ is te schrijven in de vorm $\sum_{ij} \alpha_{ij}x_{ij} = \sum_i y_i(\sum_j \alpha_{ij}z_j)$ dus $S_1 \times S_2 = S_1 S_2$ en evenzo $S_1 \times S_2 = S_2 S_1$. Dus voldoet $S = S_1 \times S_2$ in dat geval aan de volgende voorwaarden:

1o de elementen van S_1 zijn verwisselbaar met die van S_2,

2o $S = S_1 S_2 = S_2 S_1$,

3o $(S:\Phi) = (S_1:\Phi)(S_2:\Phi)$, waarin het symbool $(A:\Phi)$ de rang van A over Φ voorstelt.

Door deze drie voorwaarden is omgekeerd een direct product ook bepaa

Stel nl. een algebra S over Φ met twee deelalgebra's S_1 en S_2 die aan 1o, 2o, en 3o voldoen en laat $y_1,\ldots,y_{n_1}$ en $z_1,\ldots,z_{n_2}$ bases resp. van S_1 en S_2 zijn. Dan is volgens 2o iedere $a\in S$ te schrijven in de gedaante $a=\sum_\kappa a_k^{(1)}a_k^{(2)}$ met $a_k^{(i)}\in S_i$. Door deze in de basiselementen uit te drukken vinden we $a=\sum_{ij}\alpha_{ij}y_iz_j$. De n_1n_2 elementen y_iz_j vormen volgens 3o een basis van S en zijn dus lineair onafhankelijk over Φ. Als de structuurconstanten van S_1 en S_2 als boven $\gamma_{ijp}^{(1)}$ en $\gamma_{klq}^{(2)}$ zijn, volgt voor de basiselementen $x_{ik}=y_iz_k$ van S met behulp van 1c dat $x_{ik}x_{jl}=y_iz_ky_jz_l=$ $=y_iy_jz_kz_l=\sum_{p,q}\gamma_{ijp}^{(1)}\gamma_{klq}^{(2)}y_pz_q=\sum_{p,q}\gamma_{ijp}^{(1)}\gamma_{klq}^{(2)}x_{pq}$, dus S is isomorf met $S_1\times S_2$. We merken nog op, dat uit 3o blijkt, dat het begrip direct product essentieel afhangt van Φ. Vervangen we b.v. Φ door een deellichaam Σ met $(\Phi:\Sigma)=m$ dan is $(S:\Sigma)=m(S:\Phi)$, maar $(S_1:\Sigma)(S_2:\Sigma)=$ $=m^2(S_1:\Phi)(S_2:\Phi)$. Als S_1 en S_2 enen hebben (resp. 1_1 en 1_2) dan is $1=1_11_2$ de één van S. Dan is $1_1=1_1(1_11_2)=1_11_2=1$ en evenzo $1_2=1$. Verder is $S_1\cap S_2$ ten hoogste eendimensionaal, want stel a en b lineair onafhankelijke elementen in $S_1\cap S_2$, dan zijn ze beide zowel in een basis van S_1 als in een basis van S_2 op te nemen. Uit het bovenstaande volgt dan dat a^2, ab, ba, b^2 lineair onafhankelijk zijn, maar dat kan niet want ab=ba. Als S_1 en S_2 dus enen hebben, bestaat $S_1\cap S_2$ uit de veelvouden $\alpha 1$.

Als S_2 een één heeft kunnen we de elementen van $S_1\times S_2$ schrijven in de gedaante $\sum y_ib_i$ met $b_i\in S_2$. Dit laat zich nu eenvoudig generaliseren tot het geval dat S_2 geen algebra over Φ meer is, maar een willekeurige ring, die Φ als deelring bevat (b.v. een eindig of oneindig uitbreidingslichaam van Φ). Ga dus uit van een algebra A over Φ met basis $x_1,\ldots,x_n$ en een ring S, zodat Φ bevat is in het centrum van S. Vorm de uitdrukkingen $\sum b_ix_i$ met $b_i\in S$ en definieer $(\sum b_ix_i)+(\sum b'_ix_i)=\sum(b_i+b'_i)x_i$ en $(\sum b_ix_i)(\sum b'_jx_j)=\sum_\kappa(\sum_{ij}\gamma_{ijk}b_ib'_j)x_k$ als $x_ix_j=\sum_k\gamma_{ijk}x_k$. Dat dit systeem een ring vormt, is eenvoudig te bewijzen en eveneens dat bij een andere basiskeuze in A een ring ontstaat die isomorf is met de eerstgevormde. We noemen deze ring A_S. Er is geen verwarring mogelijk door het feit dat $\Phi\subset S$ en dus $\sum\alpha_ix_i$ met $\alpha_i\in\Phi$ zowel in A als in A_S voorkomt, want de rekenregels zijn dezelfde; we mogen dus A als deelverzameling van A_S interpreteren. We definiëren nu $b(\sum b_ix_i)=$ $=\sum(bb_i)x_i$ voor $b\in S$; dan is A_S een S-modulus. Uit deze definitie volgt $1u=u$, $b(uv)=(bu)v$, $x(bu)=b(xu)$ voor $u\in A_S$, $v\in A_S$, $x\in A$, $b\in S$. Dus is de modulusoperatie verwisselbaar met de rechtsvermenigvuldigingen van A_S en met de linksvermenigvuldigingen met elementen van A.

Daar A_S een S-modulus is en $\Phi \subset S$ is A_S een Φ-modulus. Verder is voor $\alpha \in \Phi$ en $u,v \in A_S$: $\alpha(uv)=(\alpha u)v=u(\alpha v)$. Als A_S een eindig lineaire rang over Φ heeft, hetgeen zo is als S een eindig lineaire rang over Φ heeft, is A_S een algebra over Φ. Als $y_1,\ldots,y_m$ een basis van S over Φ zijn, vormen de mn elementen $y_i x_j$ een basis van A_S over Φ.

Als A een één e heeft is $e(\sum b_i x_i)=\sum e(b_i x_i)=\sum b_i(ex_i)=\sum b_i x_i$ en evenzo $(\sum b_i x_i)e=\sum b_i x_i$, dus e is de één van A_S. De elementen be $(b \in S)$ van A_S vormen een deelring $\bar{S}$ van A_S isomorf met S. We merken op dat $(be)u=bu$ en $x(be)=bx$ voor $u \in A_S$, $x \in A$. De elementen van A en $\bar{S}$ zijn dus verwisselbaar en het is duidelijk dat als S een algebra over Φ is, aan de eisen 1o, 2o en 3o voor direct product voldaan is zodat we in dit geval $A_S=A \times S$ mogen stellen.

Als A_1 een deelalgebra van A is, mogen we veronderstellen dat $x_1,\ldots,x_r$ een basis van A_1 is die tot $x_1,\ldots,x_n$ als basis van A aan te vullen is. De elementen $\sum_{i=1}^{r} b_i x_i$ vormen dan kennelijk een deelsysteem van A_S dat isomorf is met A_{1S}. Verder is het duidelijk, dat als A_1 een l-ideaal, nilpotent l-ideaal enz. in A is, dan ook A_{1S} een l-ideaal, nilpotent l-ideaal enz. in A_S is. Dus als A_S halfenkelvoudig of enkelvoudig is, is A halfenkelvoudig, resp. enkelvoudig.

Neem nu aan dat S een lichaam P is, dan is $\varrho(uv)=(\varrho u)v=u(\varrho v)$. Dus is A_P op te vatten als een algebra over P; blijkbaar is $(A_P:P)=(A:\Phi)$. Verder is $(A_1+A_2)_P=A_{1P}+A_{2P}$, $(A_1 \times A_2)_P=A_{1P} \times A_{2P}$ en als $P \subset \Sigma$ is $(A_P)_\Sigma=A_\Sigma$. Verder is als $A=\Phi_m$ een matrixring is, $A_S=S_m$. We kunnen dus zeggen:

Een enkelvoudige halfenkelvoudige algebra over Φ is te schrijven in de vorm $\Phi_m \times D$, waarin D een scheef lichaam is, dat Φ in zijn centrum bevat; omgekeerd is een dergelijk algebra enkelvoudig halfenkelvoudig.

Laat nu de algebra A over Φ een (commutatief) lichaam zijn, dat separabel over Φ is (d.w.z. ieder element van A voldoet aan een irreducibele algebraische vergelijking met coëfficiënten in Φ zonder meervoudige wortels). Laat P een willekeurig uitbreidingslichaam van Φ zijn. We willen de structuur van A_P bepalen. Onderstel eerst dat P het kleinste normale lichaam over Φ bevat dat A als deellichaam bevat. (Een algebraische uitbreiding van een lichaam Φ heet normaal als hij met ieder element a ook alle andere wortels van de algebraische vergelijking met coëfficiënten in Φ waaraan a voldoet bevat). Als dan $(A:\Phi)=n$, dan zijn er precies n isomorfieën $a \to a^{(i)}$, $i=1,\ldots,n$ tussen A en deellichamen van P. Dit zijn representaties van A door eenrijige matrices over P. Deze representaties zijn echter direct tot representaties van A_P uit te breiden. Als n.l. $x_k \to x_k^{(i)}$ dan stellen we $\sum \varrho_k x_k \to \sum \varrho_k x_k^{(i)}$ voor $\varrho_k \in P$. Dit geeft blijkbaar weer representatie van A_P. Deze n representaties zijn, omdat ze eenrijige zijn, zeker irreducibel en niet-aequivalent. Uit de representatietheorie volgt nu, dat, als R het radicaal van A_P voorstelt, $A_P(\mathrm{mod}\ R)$ een directe som is van ten minste n idealen.

Daar de rang van deze idealen over P ten minste 1 is en $(A_P : P) = n$, moet $R = 0$ zijn, dus A_P is halfenkelvoudig. Als P willekeurig is, nemen we een lichaam $\Sigma \supset P$, dat het kleinste normale lichaam bevat, dat A bevat. Dan is A_Σ volgens het bovenstaande halfenkelvoudig, maar $A_\Sigma = (A_P)_\Sigma$, dus A_P is halfenkelvoudig. Hiermee is de volgende stelling verkregen :

Als A een eindig, separabel lichaam over Φ is en $(A : \Phi) = n$ en P een willekeurig lichaam over Φ, dan is A_P halfenkelvoudig. Als P het kleinste normale lichaam over Φ bevat, dat A bevat, dan is A_P directe som van idealen, die alle isomorf zijn met P.

Als voorbeeld kunnen we voor Φ het lichaam der reële getallen en voor P het lichaam der complexe getallen nemen en voor A weer het lichaam der complexe getallen (basis 1,j ; $j^2 = -1$). A_P bestaat dan uit $\alpha + \beta j$, α en β complex. Door hierin over te gaan op de basiselementen $e_1 = \frac{1}{2} + \frac{1}{2}ij$, $e_2 = \frac{1}{2} + \frac{1}{2}ij$, zien we dat A_P directe som is van twee lichamen die elk isomorf zijn met het lichaam der complexe getallen, immers $e_1^2 = e_1$, $e_1e_2 = e_2e_1 = 0$, $e_2^2 = e_2$.

De separabiliteitsvoorwaarde is in bovenstaande stelling noodzakelijk in die zin, dat als A inseparabel is er een P te vinden is zodat A_P niet halfenkelvoudig is. Kies n.l. P algebraisch afgesloten en stel dat A_P halfenkelvoudig is. Dan is A_P een directe som van lichamen, die omdat P algebraisch afgesloten is alle isomorf met P en dus n in getal moeten zijn. De reguliere representatie van A_P is dus volledig reducibel en valt uiteen in n irreducibele representaties van de eerste graad over P deze induceren ook n verschillende niet-aequivalente representaties van A (door de representatie van de basiselementen is de hele representatie bepaald). Daar A een lichaam is, is de representatie een isomorfie; daar A inseparabel is, zijn er echter geen n verschillende isomorfieën van A in P mogelijk, hetgeen een tegenspraak geeft. Dus kan A_P niet halfenkelvoudig zijn.

Als voorbeeld kunnen we voor Φ het lichaam $R_2(t)$ nemen, ontstaande uit het lichaam R_2 van twee elementen door adjunctie van een onbepaalde t, dat is dus het lichaam der gebroken rationale functies van de veranderlijke t met gehele coëfficiënten, waarmee gerekend wordt modulo 2. Het polynoom $x^2 + t$ is irreducibel en inseparabel ; de adjunctie van de wortel $\sqrt{t}$ van de vergelijking $x^2 + t = 0$ geeft $P = \Phi(\sqrt{t})$. Voor A nemen we hetzelfde lichaam (basis 1,a ; $a^2 = t$). Dan bezit A_P het nilpotente element $\sqrt{t} + a$ (want $(\sqrt{t} + a)^2 = 0$) dat, omdat de ring commutatief is, een nilpotent ideaal voortbrengt. Dus A_P is niet halfenkelvoudig.

Een enkelvoudig halfenkelvoudig hypercomplex systeem A over Φ heet centraal (of ook normaal) als het centrum van A bestaat uit de

elementen $\alpha 1 (\alpha \in \Phi)$, m.a.w. , als we zoals we gewoonlijk doen de elementen $\alpha 1$ met α identificeren , als Φ het centrum van A is . Verder maken we de afspraak dat als we over een enkelvoudig hypercomplex systeem spreken , we daar een enkelvoudig halfenkelvoudig systeem $\neq 0$ mee bedoelen. Een enkelvoudige algebra A is een matrixring D_m over een scheef lichaam D . Daar het centrum van D_m het centrum van D is , kunnen we ook zeggen dat A centraal is als Φ het centrum van D is . Een enkelvoudige algebra is altijd als een centrale enkelvoudige algebra op te vatten door hem te beschouwen als een algebra over zijn centrum .

We veronderstellen nu dat A een willekeurige algebra met één is en B een centrale enkelvoudige algebra , beide over Φ. We zullen aantonen , dat de idealen van $A \times B$ eeneenduidig betrokken kunnen worden op de idealen van A . Laat L_0 een ideaal van A zijn dan is $L = L_0 B = L_{0B}$ een ideaal van A_B . Stel dat $x_1 , \ldots , x_n$ een dusdanige basis van A over Φ is, dat $x_1 , \ldots , x_r$ een basis van L_0 over Φ is . Dan is $\sum b_i x_i$ in A als $b_i = \beta_i$ in Φ is en $\sum b_i x_i$ in L als $b_{r+1} = \ldots = b_n = 0$. Dus bestaat $A \cap L$ uit de elementen $\sum_1^r \beta_i x_i$ en $A \cap L = L_0$. Dus is $L_{0B} = M_{0B}$ dan en slechts dan als $L_0 = M_0$. Laat nu L een willekeurig ideaal in $A \times B$ zijn en $L_0 = A \cap L$ en kies een basis $x_1 , \ldots , x_n$ voor A zo dat $x_1 , \ldots , x_r$ een basis van L_0 is . Het is duidelijk dat L_0 een ideaal in A is en dat $L_{0B} \subset L$. Stel nu $L_{0B} < L$ en stel dat $\sum_1^n b_i x_i$ een element van L is dat niet in L_{0B} ligt, dan heeft $\sum_{r+1}^n b_i x_i$ deze eigenschap ook en ten minste een der b_j ($j = r+1 , \ldots , n$) is $\neq 0$. Stel nu dat $b_{i_1} x_{i_1} + \ldots + b_{i_s} x_{i_s}$, $b_{i_j} \neq 0$, $i_j = r+1 , \ldots , n$ een element van L is waarvoor s de kleinste positieve waarde heeft (de b's hoeven niet dezelfde te zijn als de voorgaande) . De elementen $b (b_{i_1} x_{i_1} + \ldots + b_{i_s} x_{i_s})$ en $(b_{i_1} x_{i_1} + \ldots + b_{i_s} x_{i_s}) b$ behoren tot L voor een willekeurige $b \in B$. Hieruit volgt dat de coëfficiënten van x_{i_1} in de elementen van deze soort samen met 0 in D een ideaal $\neq 0$ vormen; dus is , omdat B enkelvoudig is , b_{i_1} willekeurig. Dus bevat L een element $x_{i_1} + b_2' x_{i_2} + \ldots + b_s' x_{i_s}$ en dus ook $b(x_{i_1} + b_2' x_{i_2} + \ldots + b_s' x_{i_s}) - (x_{i_1} + b_2' x_{i_2} + \ldots + b_s' x_{i_s}) b = \sum_{j=2}^{s} (b b_j' - b_j' b) x_{i_j}$. Daar s minimaal is is $b b_j' = b_j' b$ en dus omdat B centraal is , is $b_j' = \beta_j \in \Phi$. Dus bevat L het element $x_{i_1} + \beta_2 x_{i_2} + \ldots + \beta_s x_{i_s}$ dat tot A behoort . Dit is in strijd met het feit, dat $x_1 , \ldots , x_r$ een basis van L_0 is en dat $L_0 = L \cap A$. Daarmee is bewezen:

Als A een algebra met één is en B een centrale enkelvoudige algebra dan is de afbeelding $L_0 \to L_{0B}$ een eeneenduidige afbeelding tussen de idealen van A en die van $A \times B$.

Hieruit volgt direct:

Als A enkelvoudig is en B centraal enkelvoudig dan is $A \times B$ enkelvoudig.

Als in het algemene geval R het radicaal van $A \times B$ is, is $R_0 = A \cap R$ een nilpotent ideaal in A en dus bevat in het radicaal R'_0 van A. Aan de andere kant is R'_{0B} een nilpotent ideaal in $A \times B$, dus $R'_{0B} \subset R$. Dus is $R'_0 = R_0$. Hieruit volgt:

Als A halfenkelvoudig is en B centraal enkelvoudig, dan is $A \times B$ halfenkelvoudig.

Als $c = \sum b_i x_i$ een element van $A \times B$ is dat verwisselbaar is met alle $b \in B$ dan is $\sum (bb_i - b_i b)x_i = 0$ dus $bb_i = b_i b$ dus $b_i \in \Phi$ en $c \in A$. Dus is het centrum van $A \times B$ het centrum van A. Dus:

Als A een algebra met één is en B centraal enkelvoudig dan zijn de elementen van A de enige van $A \times B$ die met de elementen van B verwisselbaar zijn. Als A centraal enkelvoudig is, dan is ook $A \times B$ centraal enkelvoudig.

Een eindig algebraisch uitbreidingslichaam P van Φ is op te vatten als een enkelvoudige algebra over Φ. Als A een centrale enkelvoudige algebra over Φ is, volgt uit het bovenstaande, dat A_P enkelvoudig is. Uit het bovenstaande volgt verder dat het centrum van A_P het centrum van P, dat is P zelf is. Dus:

Als A een centrale enkelvoudige algebra over Φ is en P een eindige algebraische uitbreiding van Φ, dan is A_P ook enkelvoudig en mits opgevat als algebra over P ook centraal.

Als A een algebra met één over Φ is en $(A : \Phi) = n$, dan zijn voor een $a \in A$ de $(n+1)$ elementen $1, a, a^2, \ldots, a^n$ lineair afhankelijk over Φ, dus a voldoet aan een algebraische vergelijking $f(x) = 0$ met coëfficiënten in Φ. Er is dus blijkbaar ook een eenduidig bepaald polynoom $g(x)$ met coëfficiënten in Φ en coëfficiënt 1 bij de hoogste graad en van laagst mogelijke graad, zodat $g(a) = 0$. Dit polynoom heet het minimale polynoom van a. Als P een uitbreidingslichaam van Φ is en $a \in A$ dan is het minimale polynoom van a als element van de algebra A_P over P hetzelfde als dat van a als element van de algebra A over Φ. Dit volgt direct uit het feit dat een stel lineair onafhankelijke elementen van A t.o.v. Φ ook lineair onafhankelijke elementen van A_P t.o.v. P zijn (neem ze in een basis op). Als A een scheef lichaam is, is het minimale polynoom van een element a irreducibel; immers uit $g(x) = h(x)k(x)$ volgt $0 = g(a) = h(a)k(a)$ en omdat A geen nuldelers heeft is $h(a) = 0$ of $k(a) = 0$. Als $a \notin \Phi$, is de graad van $g(x) > 1$. Neem nu een uitbreidingslichaam P van Φ, waarin $g(x)$ reducibel wordt (b.v. een lichaam waarin $g(x) = 0$ een wortel heeft), dus $g(x) = h(x)k(x)$. In A_P geldt dan $0 = g(a) = h(a)k(a)$ en omdat $g(x)$ het minimale polynoom van a is, geldt $h(a) \neq 0$ en $k(a) \neq 0$, dus A_P heeft nuldelers.

Neem nu een centrale enkelvoudige algebra over Φ, dan is A een matrixring K_m, waarin K een scheef lichaam is met Φ als centrum. Dus $(A : \Phi) = m^2(K : \Phi)$. Volgens het bovenstaande is, als $K > \Phi$, Φ zo uit te breiden tot een lichaam P, dat K_P geen scheef lichaam is. Omdat K centraal enkelvoudig over Φ is, is K_P centraal enkelvoudig over P dus een matrixring K'_{m_1} met $m_1 > 1$ en K' een scheef lichaam met P als centrum. Verder is $(K:\Phi) = (K_P:P) = m_1^2(K':P)$. Dit proces is voort te zetten tot het scheve lichaam met zijn centrum samenvalt. Hieruit volgt, dat $(A : \Phi)$ een kwadraat is. Dit geeft de volgende stellingen:

Een scheef lichaam van eindige rang over zijn centrum Φ (en dus ook iedere centrale enkelvoudige algebra over Φ) heeft een rang over Φ, die een kwadraat is.

Bij iedere centrale enkelvoudige algebra A over Φ is een eindig uitbreidingslichaam P van Φ te vinden, zodat $A_P = P_m$ een matrixring over P is.

We noemen een uitbreidingslichaam P van Φ, zodat $A_P = P_m$ een splitsingslichaam (splitting field; Zerfällungskörper) van A.

We beschouwen nu een z.g. representatie door matrices van een algebra A over Φ in een scheef lichaam K. Dat is een homomorfe afbeelding van A op een deelring van de matrixring K_m. Hierbij wordt verder verondersteld dat K ook een algebra over Φ is en dat de homomorfie een Φ-homomorfie is. De matrixring K_m is op te vatten als de ring van de lineaire transformaties van een m-dimensionale vectorruimte R over het scheve lichaam K', dat invers-isomorf met K is. Zo opgevat valt deze representatie onder het vroegere algemene representatiebegrip: homomorfe afbeelding van een ring in de endomorfieënring van een additieve groep. Op grond van de representatie is R dus een A-modulus. We nemen aan dat A een één bezit en dat deze in de representatie met de identieke transformatie (de eenheidsmatrix) overeenkomt. We kunnen nu R ook opvatten als $A \times K'$-modulus door voor een element $\sum b_i a_i$ (a_i een basis van A en $b_i \in K'$) te definiëren $(\sum b_i a_i)x = \sum b_i(a_i x)$ voor $x \in R$. Dat dit inderdaad aan de modulusvoorwaarden voldoet is makkelijk in te zien (bedenk dat in $A \times K'$ de elementen van A en van K' verwisselbaar zijn). Omgekeerd is iedere $A \times K'$-modulus tevens A-modulus; als deze $A \times K'$-modulus een vectorruimte over K' is, is wegens de verwisselbaarheid van de elementen van A en K' de aan een element van A toegevoegde homomorfie een lineaire transformatie van deze vectorruimte. Nemen we nu aan dat A enkelvoudig is en dat van A en K' (of K) minstens een van beide normaal over Φ is, dan is $A \times K'$ ook enkelvoudig. Uit de representatietheorie volgt dan dat alle irreducibele $A \times K'$-moduli $A \times K'$-isomorf zijn en wel alle met een irreducibel 1-ideaal van $A \times K'$ en dat een $A \times K'$-modulus volledig reducibel is. Hieruit volgt dat twee irreducibele representaties van A door matrices van de graad n in K

aequivalent moeten zijn en dan hetzelfde ook voor reducibele representaties door splitsing van deze in irreducibele. Omdat A enkelvoudig is is de representatie een isomorfie. Twee isomorfe enkelvoudige deelringen van K_m zijn uiteraard op te vatten als representaties van een zelfde enkelvoudige algebra A. Verder heeft iedere centrale enkelvoudige algebra over Φ de vorm K_m. Hiermee is de volgende stelling verkregen:

Als A_1 en A_2 isomorfe enkelvoudige deelalgebra's, die 1 bevatten, van de centrale enkelvoudige algebra B zijn, dan is iedere isomorfie tussen A_1 en A_2 uit te breiden tot een inwendige automorfie van B.

Het is n.l. de inwendige automorfie met het element van B dat de aequivalentie tussen de twee representaties tot stand brengt.

Door speciaal $A_1 = A_2 = B$ te nemen vinden we:

Iedere automorfie van een centrale enkelvoudige algebra over Φ, die de elementen van Φ invariant laat, is een inwendige automorfie.

Keren we nu terug tot de representatie van A door matrices in K en nemen we weer aan dat A enkelvoudig is en A of K centraal. Dan is $A \times K'$ enkelvoudig dus $A \times K' = D_s$ een matrixring over een scheef lichaam D. Een willekeurige representatie is volledig reducibel en een irreducibele representatie geeft aanleiding tot een irreducibele $A \times K'$-modulus die isomorf is met een irreducibel 1-ideaal van $A \times K'$. Deze zijn ook K'-moduli en dus isomorf met een directe som van irreducibele K'-moduli; noem het aantal daarvan h. Omdat K' een scheef lichaam is, is een irreducibele K'-modulus eendimensionaal. Een irreducibele $A \times K'$-modulus is dus h-dimensionaal over K' en een representatie van A door matrices van graad N in K bestaat dan en slechts dan als $h \mid N$. Verder is $A \times K'$ zelf ook een $A \times K'$-modulus (reguliere representatie) en deze is directe som van s irreducibele $A \times K'$-moduli. Dus $A \times K'$ heeft dimensie sh over K'. Aan de andere kant is, als $(A : \Phi) = n$, ook $(A \times K' : K') = n$, dus $n = hs$, dus h is te vinden als $\frac{n}{s}$.

Neem nu een centrale enkelvoudige algebra K_m over Φ en een enkelvoudige deelalgebra A van K_m, die 1 bevat, dan is $a \to a$ voor $a \in A$ een representatie van A door matrices van de graad m in K. Als weer $(A : \Phi) = n$ en $A \times K' = D_s$, dan is volgens het voorgaande $n = hs$ en $h \mid m$. Noemen we $m = hl$, dan is $nl = hls = ms$, dus $n \mid ms$.

Het is eenvoudig in te zien, dat $(P \times Q)' = P' \times Q'$ (steeds geeft een accent de vorming van de inverse ring aan). Dus is ook $A' \times K = D'_s$ een matrixring over een scheef lichaam D'.

We kunnen dit ook toepassen voor $A = K_m$. Dan is $A \times A' = A \times K'_m = D_{sm}$ en $n \mid sm$. Aan de andere kant is $(A \times A' : \Phi) = n^2$, dus $s^2m^2 \mid n^2$, dus $sm \mid n$. Hieruit volgt $sm = n$ en $D = \Phi$.

Het directe product van een centrale enkelvoudige algebra A over Φ met zijn invers-isomorfe algebra is een matrixring over Φ $(A \times A' = \Phi_n)$.

Neemt men speciaal een enkelvoudige deelalgebra A, die 1 bevat, van een centraal scheef lichaam K (dus m = 1 in het bovenstaande), dan is $s|n$ en $n|s$ dus $n = s$ en $A \times K' = D_n$.

Als B een deelalgebra van een algebra A is noemen we de deelalgebra van A bestaande uit die elementen van A die met alle elementen van B verwisselbaar zijn de <u>centralisator</u> A(B) van B in A. We nemen aan dat A een één heeft. We beschouwen de endomorfieënring van de additieve groep van A. Daartoe behoren de linksvermenigvuldigingen a_l en de rechtsvermenigvuldigingen a_r met elementen van A. Noem A_l de ring van de links- en A_r de ring van de rechtsvermenigvuldigingen van A. Neem voor een deelring P van A $\bar{P}_l$ resp. $\bar{P}_r$ de ring van de links- resp. rechtsvermenigvuldigingen met elementen van P. Dan is $\bar{P}_l$ isomorf met P en $\bar{P}_r$ invers-isomorf met P omdat A een één heeft. Verder is A_r de ring van de A_l-endomorfieën en A_l de ring der A_r-endomorfieën. Als P een algebra over Φ is, zijn $\bar{P}_l$ en $\bar{P}_r$ ook als algebra's over Φ op te vatten. Nu is de ring van de endomorfieën verwisselbaar met die van A_r en $\bar{B}_l$ juist $\overline{A(B)}_l$. Want aan de ene kant is een endomorfie uit $\overline{A(B)}_l$ verwisselbaar met de endomorfieen uit A_r en $\bar{B}_l$. Neem een endomorfie C verwisselbaar met de endomorfieen uit A_r en $\bar{B}_l$, dan is $C = c_l$ en wegens de isomorfie van A_l en A is $c \in A(B)$. Als P nu 1 bevat, bevat de endomorfieënring $A_r\bar{B}_l = \bar{B}_l A_r$ A_r en $\bar{r}_l$. Dus dan is $\overline{A(B)}_l$ de ring van de $A_r\bar{B}_l$-endomorfieën. Neem nu aan, dat A centraal enkelvoudig is en B enkelvoudig is en 1 bevat. Dan is $A_r\bar{B}_l$ homomorf beeld van $A' \times B$, maar $A' \times B$ is enkelvoudig, dus de homomorfie is een isomorfie. Laat $A' \times B = E_s$ zijn, dan is $A_r\bar{B}_l = A_r \times \bar{B}_l = \bar{E}_s$ waarin $\bar{E}$ isomorf met E is. Nu is A een $\bar{E}_s$-modulus en wel een van eindige lineaire rang over $\bar{E}_s$ omdat $A_r 1 = A$. Dus is de ring van de $\bar{E}_s$-endomorfieën te schrijven als $\bar{E}'_t$, waarin $\bar{E}'$ invers-isomorf met $\bar{E}$ (dus met E) is en verder is st de dimensie van A over $\bar{E}$ en $\bar{E}_s$ de ring van de $\bar{E}'_t$-endomorfieën (zie blz. 30 en 31). Dus $\overline{A(B)}_l = \bar{E}'_t$ en $A(B) = E'_t$ waarin E' invers-isomorf met E is. Nu bepalen we $A(A(B))$. Evident is dat $B \subset A(A(B))$. Als $c \in A(A(B))$, dan is c_l een $\bar{E}'_t$-endomorfie, dus $c_l \in \bar{E}_s = A_r \times \bar{B}_l$. Omdat c_l verwisselbaar is met alle elemanten van A_r, geldt $c_l \in \bar{B}_l$ (zie blz 50), dus $c \in B$, dus $A(A(B)) = B$. Noem $(A : \Phi) = n$, $(E : \Phi) = e$. Dan is $n = (A : \bar{E})(\bar{E} : \Phi) = ste$. Omdat $A(B) = E'_t$, is $(A(B) : \Phi) = et^2$. Omdat $(A' \times B) = E_s$, is $((A' \times B) : \Phi) = n(B : \Phi) = es^2$. Dus $n(B : \Phi)(A(B) : \Phi) = e^2 s^2 t^2 = n^2 = n(A : \Phi)$, dus

$(B : \Phi)(A(B) : \Phi) = (A : \Phi)$. Hiermede is de volgende stelling verkregen:

Als A een centrale enkelvoudige algebra over Φ is en B een enkelvoudige deelalgebra van A die 1 bevat, als $A(B)$ de centralisator van B in A voorstelt en A' een algebra invers-isomorf met A, dan geldem de volgende beweringen:

1° $A(B)$ is enkelvoudig en bevat 1,

2° $A(A(B)) = B$,

3° Als $B \times A' = E_s$, waarin E een scheef lichaam is, dan is $A(B) = E'_t$, waarin E' invers-isomorf met E is,

4°, $(A : \Phi) = (B : \Phi)(A(B) : \Phi)$.

Neemt men in bovenstaande stelling aan dat B commutatief is, dan is $A(B) \supset B$ en $(A : \Phi) = (B : \Phi)(A(B) : \Phi) \geq (B : \Phi)^2$. Neem nu voor A een scheef lichaam en voor B een commutatief lichaam.

Als dan $A(B) > B$, dan kiezen we een $a \in A(B), a \notin B$, dan vormen de rationale functies van a met coëfficiënten in B een lichaam $B(a) > B$. Dit procédé kunnen we voortzetten tot we een lichaam K gevonden hebben, waarvoor $A(K) = K$. Als omgekeerd bij een lichaam $B \subset A$ nog een lichaam $C \subset A$ te vinden is zodat $C > B$, dan is $A(B) \supset C$, dus $A(B) > B$. De betrekking $A(B) = B$ karakteriseert dus onder de lichamen van A de maximale deellichamen. Voor een dergelijk maximaal deellichaam geldt dus $(A : \Phi) = (B : \Phi)^2$. Dit bewijst nogmaals dat de rang van een scheef lichaam over zijn centrum een kwadraat is, benevens de volgende stelling:

Als de rang van een scheef lichaam over zijn centrum δ^2 is, dan is δ de rang van een willekeurig maximaal (commutatief) deellichaam.

Men noemt δ de graad of de index van het scheve lichaam. Bij scheve lichamen is, anders dan bij commutatieve lichamen, de graad dus niet hetzelfde als de rang. Van een matrixring over een scheef lichaam noemt me de index de index van het scheve lichaam.

Als A een centrale enkelvoudige algebra over Φ is, dus $A = D_m$, δ de index van D, dan is $(A : \Phi) = (\delta m)^2$. Stel nu dat K een deellichaam van A is, dat Φ bevat en zodat $(K : \Phi) = \delta m$ (of A zo. deellichaam bevat laten we voorlopig in het midden). Uit $A(K) \supset K$ en $(\delta m)^2 = (A : \Phi) = (K : \Phi)(A(K) : \Phi) \geq (\delta m)^2$ volgt $A(K) = K$, dus K is een maximaal deellichaam van A. Nu is (zie blz. 52 onderaan) $K \times D = K' \times D = E_s$ en $s \mid \delta m, \delta m \mid ms$, dus $\delta \mid s$. Omdat D centraal enkelvoudig is, is het centrum van $K \times D$ het centrum van K, dat is K zelf. Aan de andere kant is het centrum van E_s bevat in E, dus $K \subset E$. Verder is $K \times A = E_{sm}$, dus $((K \times A) : \Phi) = (K : \Phi)(\delta m)^2 = (E : \Phi) = (sm)^2$. Omdat $(K : \Phi) \leq (E : \Phi)$ en $\delta \nmid s$, moet dus $K = E$ en $s = \delta$ zijn. Dus is $A_K = A \times K = K_{\delta m}$, d.w.z. K is een splitsingslichaam van A.

We merken op dat dezelfde lichamen splitsingslichamen van A en van D zijn. Als n.l. K splitsingslichaam van D is, dan natuurlijk ook van A. Omgekeerd

als K splitsingslichaam van A is, dus $A_K = K_n$, dan is $D_K = L_n$, omdat D centraal is, dus $A_K = L_{mn}$. Hieruit volgt $L = K$(zie blz. 32; in ieder geval is hier $L > K$), dus K is splitsingslichaam van D. Hiermee is de helft bewezen (n.l. het "voldoende")van de volgende stelling:

Nodig en voldoende opdat een eindig uitbreidingslichaam K van Φ een splitsingslichaam is van een centraal scheef lichaam D over Φ van index δ is dat de rang f van K over Φ een veelvoud $m\delta$ van δ is en dat K isomorf is met een deelalgebra die 1 bevat van D_m.

We tonen nu aan dat de voorwaarden nodig zijn. Laat K dus een splitsingslichaam van D zijn, dus $D \times K = D_K = K_\delta$. Dan is (zie blz. 52) $\delta \mid (K : \Phi) = f$, dus $f = \delta m$. Verder bestaat er een representatie van K in D'_m, die omdat K een lichaam is een isomorfie is en bij de inverse isomorfie tussen D'_m en D_m ook isomorf afgebeeld wordt.

Speciaal zijn de maximale deellichamen van D dus splitsingslichamen van D en natuurlijk ook hun eventuele eindige algebraische uitbreidingen. Neemt men een maximaal deellichaam L dat Φ bevat van een matrixring D_N, dan is omdat D centraal is $L \times D$ enkelvoudig dus $L \times D_N = E_n$ een matrixring; dus $L \times D'_N = E'_n$ en $D_N(L) = E_s$. Omdat L het centrum van $D_N(L)$ is, is $L \subset E$. Als $L < E$, zou er een deellichaam van D_N zijn $> L$ dus $L = E$ en $L \times D_N = L_n$, dus L is splitsingslichaam van D. Omgekeerd volgt uit bovenstaande stelling dat een splitsingslichaam van eindige rang over Φ ook maximaal deellichaam van een D_N is. Dus

Nodig en voldoende opdat een eindig uitbreidingslichaam K van Φ een splitsingslichaam van een centraal scheef lichaam D over Φ is, is dat K isomorf is met een maximaal commutatief deellichaam, dat Φ bevat, van een matrixring D_m.

We kunnen nu een vroegere stelling (zie blz. 50) nog wat uitbreiden:

Als A een centrale enkelvoudige algebra over Φ is en P een willekeurig uitbreidingslichaam van Φ, dan is A_P enkelvoudig en mits opgevat als algebra over P, ook centraal.

Bewijs:Neem een splitsingslichaam K van eindige rang over Φ en een lichaam Σ dat zowel P als K bevat. Dan is $A_\Sigma = (A_K)_\Sigma = (K_n)_\Sigma = \Sigma_n$, dus A_Σ is enkelvoudig, maar $A_\Sigma = (A_P)_\Sigma$, dus A_P is enkelvoudig. Verder is Σ het centrum van A_Σ, dus P het centrum van A_P.

We passen de verkregen resultaten nu toe om twee klassieke stellingen te bewijzen. Allereerst nemen we Φ algebraisch afgesloten en een hypercomplex systeem K over Φ dat een scheef lichaam is. Als $K > \Phi$, dan bevat K zeker een deellichaam $> \Phi$, immers als K centraal is van index δ, dan bevat het een lichaam van rang δ over Φ en als K niet centraal is dan is zijn centrum een lichaam $> \Phi$. Omdat Φ algebraisch afgesloten is heeft Φ geen echte algebraische uitbreidingen dus $K > \Phi$ is onmogelijk. Het enige hypercomplexe systeem over een algebraisch afgesloten lichaam Φ, dat een scheef lichaam is, is dus Φ zelf. Neem nu voor Φ het lichaam van de reële getallen of algemener een reëel afgesloten lichaam in de zin van

Artin en Schreier (Abh.Math.Sem.Hamburg 5 (1926), 83-115 of B.L.van der Waerden, Moderne Algebra I, 2.Aufl. § 70). Dan zijn de enige algebraische uitbreidingen van Φ Φ zelf en het lichaam der complexe getallen $\Phi(i)$. Neem nu een hypercomplex systeem K over Φ dat een scheef lichaam is. Als K niet centraal is, is het centrum van K een lichaam $> \Phi$, dat dus alleen $\Phi(i)$ kan zijn. Omdat $\Phi(i)$ algebraisch afgesloten is, en K als algebra over $\Phi(i)$ op te vatten is, is volgens het bovenstaande $K=\Phi(i)$. Onderstel nu K centraal over Φ van index δ. Dan bevat K een deellichaam van rang δ over Φ. De enige mogelijkheden daarvoor zijn Φ zelf, dus $\delta=1$, en $\Phi(i)$, dus $\delta=2$. In het eerste geval is $K=\Phi$. Het tweede geval beschouwen we nu nader. Er geldt dan $\Phi < \Phi(i) < K$. De afbeelding die aan een complex getal zijn geconjugeerd complexe toevoegt ($1\to 1$, $i\to -i$) is een automorfie van $\Phi(i)$, die tot een inwendige automorfie van K is uit te breiden (zie blz. 52). Er is dus een $u\in K$, zodat $uiu^{-1}=-i$ of $ui=-iu$. Omdat $\Phi(i)$ commutatief is, geldt $u\notin\Phi(i)$. Nu vormen de vier elementen $1,i,u,iu$ een basis van K. Stel n.l. $\alpha_1+\alpha_2 i+\alpha_3 u+\alpha_4 iu=0$, dan is $(\alpha_1+\alpha_2 i)+(\alpha_3+\alpha_4 i)u=0$. Als $\alpha_3+\alpha_4 i\neq 0$, dan is $u=-(\alpha_3+\alpha_4 i)^{-1}(\alpha_1+\alpha_2 i)\in\Phi(i)$, hetgeen niet zo is. Dus $\alpha_3+\alpha_4 i=0$, dus $\alpha_3=\alpha_4=0$ en dan ook $\alpha_1+\alpha_2 i=0$, dus $\alpha_1=\alpha_2=0$. Dus zijn $1,i,u,iu$ lineair onafhankelijk t.o.v. Φ en daar K rang 4 over Φ heeft vormen ze een basis. Nu is $u^2 i=-uiu=iu^2$ en daaruit volgt dat u^2 met de vier basiselementen em dus met alle elementen van K verwisselbaar is en dus $u^2=\alpha\in\Phi$, omdat K centraal is. Dus voldoet u aan de vergelijking $x^2-\alpha=0$ en omdat $u\notin\Phi$ is $x^2-\alpha$ het minimale polynoom van u. Omdat K een scheef lichaam is, is dit polynoom irreducibel, dus $\alpha<0$. Vervangt men nu u door $j=(-\alpha)^{-\frac{1}{2}}u$, dan is $j^2=-1$ en de tot nu toe afgeleide eigenschappen van u zijn ook geldig voor j (met $\alpha=-1$). Dan vormen $1,i,j,ij=k$ een basis van K en $i^2=j^2=-1$, $ij=-ji$. Met behulp hiervan is de vermenigvuldigingstabel makkelijk aan te vullen tot die van het quaternionensysteem. Hiermee is de volgende stelling verkregen:

Stelling van Frobenius: De enige hypercomplexe systemen over het lichaam der reële getallen ,die scheve lichamen zijn, zijn de systemen der reële getallen, der complexe getallen en der quaternionen.

Deze stelling is nog iets te generaliseren door de eis dat de systemen scheve lichamen zijn te vervangen door de schijnbaar zwakkere eis dat ze geen nuldelers hebben. Deze generalisering is niet essentieel, want ieder hypercomplex systeem zonder nuldelers is een scheef lichaam. Het systeem moet n.l. in de eerste plaats halfenkelvoudig zijn,want een nilpotent element $\neq 0$ geeft aanleiding tot nuldelers. Als halfenkelvoudig systeem is het een directe som van elkaar annulerende enkelvoudige ringen, maar als er meer dan één component $\neq 0$ in de directe som is geeft dit weer aanleiding tot nuldelers, dus het systeem is enkelvoudig. Als enkelvoudig systeem is het een matrixring over een scheef lichaam, maar een matrixring van graad > 1 geeft weer aanleiding tot nuldelers (b.v. $e_{11}e_{22}=0$), dus het systeem is een scheef lichaam.

Nu willen we bewijzen dat alle scheve lichamen met eindig veel elementen commutatief zijn. Daartoe behandelen we eerst een hulpstelling uit de groepentheorie. Laat G een eindige, multiplicatief geschreven, niet noodzakelijk commutatieve groep zijn en H een ondergroep van G. Noem g de orde van G, h de orde van H en s de index van H, dan is g=hs. Voor iedere $a \in G$ heeft de met H geconjugeerde ondergroep aHa^{-1} dezelfde orde als H. Als a en b in dezelfde linker nevenklasse van H liggen, is $aHa^{-1}=bHb^{-1}$. Het aantal verschillende geconjugeerde groepen van H is dus $\leq s$. Stel nu dat ieder element van G in minstens een der geconjugeerde groepen van H ligt, dan volgt uit g=sh, dat er s verschillende geconjugeerde ondergroepen moeten zijn, die bovendien nog alle verzamelingstheoretisch disjunct moeten zijn. Twee ondergroepen van G zijn echter nooit disjunct want ze hebben de 1 gemeen, dus moet s=1 en H=G zijn. Dit geeft de volgende stelling:

Als G een eindige groep is, H een ondergroep van G en ieder element van G in minstens een der met H geconjugeerde ondergroepen van G ligt (d.w.z. bij ieder element a van G een element b van G en een element c van H te vinden is, zodat $a=bcb^{-1}$), dan is H=G.

Neem nu een eindig scheef lichaam K. Het centrum Φ van K is een lichaam en K is op te vatten als een centrale algebra over Φ. Laat $(K:\Phi)=\delta^2$ zijn, dan is de rang over Φ van de maximale deellichamen van K, die Φ bevatten, gelijk aan δ. Ze hebben dus alle evenveel elementen en zijn dus volgens een bekende stelling over eindige lichamen isomorf. Verder gaan bij deze isomorfie de elementen van Φ in zichzelf over. Deze isomorfie is dus uit te breiden tot een inwendige automorfie van K. Dit is ook zo uit te drukken, dat, als we multiplicatieve groepen beschouwen die ontstaan door uit K en zijn deellichamen het nulelement weg te laten, de ondergroepen die behoren bij de maximale deellichamen van K alle geconjugeerd zijn. Verder ligt ieder element van K in een maximaal deellichaam van K, want als $a \in K$ dan vormen de rationale functies van a met coëfficiënten in Φ een deellichaam van K, dat Φ bevat, en dit is weer uit te breiden tot een maximaal deellichaam van K dat Φ bevat. Nu vinden we uit bovenstaande hulpstelling, als G de multiplicatieve groep behorende bij K is en H de ondergroep van G behorende bij een of ander maximaal deellichaam L van K, dat Φ bevat, dat H=G, dus L=K is, omdat ieder element van G in een geconjugeerde ondergroep van H ligt. Uit L=K volgt echter dat K commutatief en $\delta=1$ is, waarmee de volgende stelling bewezen is:

<u>Stelling van Wedderburn</u>: Alle eindige scheve lichamen zijn commutatief.