LINEAIRE ALGEBRA

§1. Lichamen

Definitie 1. Een (getallen) lichaam L is een niet-lege verzameling van complexe getallen met de volgende eigenschappen:

(1) Als $a \in L$ en $b \in L$, dan ook $a + b \in L$ en $ab \in L$.

(2) Als $a \in L$ en $a \neq 0$, dan ook $-a \in L$ en $a^{-1} \in L$.

(3) L bevat minstens één element $a \neq 0$.

Voorbeelden.

a) De rationale getallen, evenals de reële en de complexe getallen vormen een lichaam.

b) De verzameling van alle complexe getallen van de vorm $z = a + bi\sqrt{2}$ met rationale a en b is een lichaam.

c) De verzameling van alle reële getallen van de vorm $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ met rationale coëfficiënten a, b en c is een lichaam.

Definitie 2. Een lichaam L heet een deellichaam van het lichaam K en het lichaam K een uitbreiding van het lichaam L als $L \subset K$.

Ieder willekeurig lichaam is dus een deellichaam van het lichaam van de complexe getallen.

Stelling 1. Ieder willekeurig lichaam L is een uitbreiding van het lichaam der rationale getallen Q en bevat dus het getal 1.

Bewijs. Stel $a \neq 0$, $a \in L$. Uit de definitie van L volgt, dat ook $a^{-1} \in L$ en dus $a.a^{-1} = 1 \in L$.

Met inductie volgt dan dat ook ieder natuurlijk getal $m = (m-1) + 1 \in L \Rightarrow -m \in L$ en $\frac{1}{m} \in L \Rightarrow \frac{m}{n} \in L$ en $-\frac{m}{n} \in L$.

Opmerking.

In de moderne algebra wordt een lichaam meestal abstract gedefiniëerd als een niet-lege verzameling L met twee binaire algebraïsche operaties, een optelling en vermenigvuldiging, die aan bepaalde voorwaarden voldoen.

(zie colloquium "Groepentheorie en lineaire algebra" 1964/65 blz. 47). Deellichamen van het lichaam der complexe getallen worden getallen lichamen genoemd om ze te onderscheiden van dergelijke "abstracte" lichamen. Wij zullen ons in dit colloquium beperken tot getallen lichamen, hoewel een veralgemening van de theorie tot willekeurige lichamen mogelijk is.

§2. Lineaire ruimten

Definitie 1. Een lineaire ruimte of vectorruimte over het lichaam L is een verzameling V, tezamen met een afbeelding $\mathcal{F}$: V × V → V en een afbeelding $\mathcal{T}$: L × V → V met de volgende eigenschappen (in plaats van $\mathcal{F}(x,y)$ en $\mathcal{T}(\alpha,x)$ $(x,y \in V, \alpha \in L)$ schrijven wij respectievelijk x + y en αx :

(1) $x + y = y + x$ commutatieve wet.

(2) $(x + y) + z = x + (y + z)$ associatieve wet.

(3) Er bestaat een element $0 \in V$ zodanig dat voor elke $x \in V$ geldt $0 + x = x + 0 = x$. (0 heet het nulelement van V).

(4) Voor elke $x \in V$ bestaat er een element $-x \in V$ zodanig dat $x + (-x) = 0$. (-x heet het tegengestelde van x).

(5) $\alpha(x + y) = \alpha x + \alpha y$.

(6) $(\alpha + \beta)x = \alpha x + \beta x$.

(7) $(\alpha\beta)x = \alpha(\beta x)$.

(8) $1x = x$,

voor alle $\alpha, \beta \in L$ en voor alle $x, y, z \in V$.

Opmerking 1.

De elementen van V noemt men dikwijls vectoren; wij zullen ze in de regel aangeven met symbolen als x, y, z, ...

Het element $x + y \in V$ heet de som van x en y en de operatieve + heet de optelling van vectoren.

Uit de eigenschappen (1) t/m (4) volgt dat de verzameling V met de optelling een abelse groep is.

Zowel het nulelement van de groep V als het getal nul zullen wij met 0 aanduiden, hoewel we hier i.h.a. met twee verschillende objecten te doen hebben.

Opmerking 2.

De getallen uit het lichaam L zullen wij aangeven met de griekse letters $\alpha, \beta, \gamma, \ldots$. Men noemt ze in dit verband vaak scalairen.

Het element $\alpha x \in V$ heet produkt van α en x en de afbeelding heet de vermenigvuldiging van vectoren met getallen.

In het linkerlid van (6) geeft het teken + de optelling in L aan; in het rechterlid staat + echter voor de optelling binnen V. Evenzo moet men in (7) onderscheid maken tussen de vermenigvuldiging van getallen binnen het lichaam L en de vermenigvuldiging van een vector met een getal.

Stelling 1. Zij V een vectorruimte over L. Er geldt:

(a) V bezit precies één nulelement.

(b) Voor elke $x \in V$ bestaat er maar één tegengestelde -x.

(c) Voor ieder tweetal elementen x en y van V is de vergelijking $z + x = y$ éénduidig oplosbaar.

Bewijs.

(a) Stel zowel 0 als 0' nulelement van V. Voor willekeurige $x, y \in V$ geldt dan $0 + x = x$ en $y + 0' = y$.

Nemen wij i.h.b. $x = 0'$ en $y = 0$, dan vinden we

$$0 + 0' = 0' \text{ en } 0 + 0' = 0.$$

Dus $0' = 0$.

(b) Stel zowel -x als -x* tegengestelde van x.

Dan is $x + (-x) = 0$ en $(-x^*) + x = 0$.

$$-x^* = (-x^*) + 0 = (-x^*) + (x + (-x)) = ((-x^*) + x) + (-x) =$$
$$= 0 + 0 + (-x) = -x.$$

(c) $z = y + (-x)$ is een oplossing van de vergelijking.

Dit is ook de enige oplossing, daar uit $z + x = y$ volgt $z + x + (-x) =$
$= y + (-x) = z$.

Opmerking 3.

De vector $y + (-x)$ zullen wij kortweg aanduiden met $y - x$. $y - x$ heet het verschil van de vectoren y en x.

Ook het symbool - gebruiken wij dus in twee betekenissen.

Uit stelling 1)(c) volgt dat als $x + y = x + z$, dan is $y = z$. Als x dus een vector is van V en $x + x = x$, dan is $x = 0$.

Stelling 2. Zij V een vectorruimte over L. Voor willekeurige $\alpha, \beta \in L$ en $x, y \in V$ geldt:

(a) $\alpha.0 = 0$.

(b) $0.x = 0$.

(c) $\alpha x = 0 \Rightarrow \alpha = 0$ of $x = 0$.

(d) $(-\alpha)x = -(\alpha x) = \alpha(-x)$.

(e) $\alpha(x - y) = \alpha x - \alpha y$.

(f) $(\alpha - \beta)x = \alpha x - \beta x$.

Bewijs.

(a) $\alpha.0 = \alpha.(0 + 0) = \alpha 0 + \alpha 0 \Rightarrow \alpha 0 = 0$.

(b) $0x = (0 + 0)x = 0x + 0x \Rightarrow 0x = 0$.

(c) Stel $\alpha x = 0$ en $\alpha \neq 0$. Dan is $x = 1x = (\frac{1}{\alpha}.\alpha)x = \frac{1}{\alpha}(\alpha x) = \frac{1}{\alpha}.0 = 0$.

(d) $\alpha x + (-\alpha)x = (\alpha + (-\alpha))x = 0x = 0 \Rightarrow (-\alpha)x = -(\alpha x)$.

$\alpha x + \alpha(-x) = \alpha(x + (-x)) = \alpha 0 = 0 \Rightarrow \alpha(-x) = -(\alpha x)$.

(e) $\alpha(x - y) = \alpha(x + (-y)) = \alpha x + \alpha(-y) = \alpha x + -(\alpha y) = \alpha x - \alpha y$.

(f) $(\alpha - \beta)x = \alpha x + (-\beta)x = \alpha x - \beta x$.

Voorbeelden.

1) Zij R het lichaam der reële getallen en R^n de verzameling van alle geordende n-tallen reële getallen $x = (x_1, x_2, \ldots, x_n)$ met als optelling

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1+y_1, x_2+y_2, \ldots, x_n+y_n).$$

Voor $\alpha \in R$ en $x = (x_1, x_2, \ldots, x_n) \in R^n$ zij

$$\alpha x = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n).$$

Dan is R^n een vectorruimte over R.

Algemener: Zij L een willekeurig lichaam en L^n de verzameling van alle geordende n-tallen getallen uit L. Optelling in L^n en vermenigvuldiging van een $x \in L^n$ met een $\alpha \in L$ definiëren wij als boven. Dan is L^n een lineaire ruimte over L.

2) Zij G het getallenlichaam van Gauss, d.i. de verzameling van alle complexe getallen van de vorm a + bi met rationale a en b.
Dan is G een vectorruimte over Q als we voor het produkt van een rationaal getal α en een willekeurige a + bi steeds nemen hun produkt in het lichaam G.

Algemener: Zij L een willekeurig lichaam en K een deellichaam van L. Dan is L een vectorruimte over K. Zo is i.h.b. het lichaam van de complexe getallen C een vectorruimte over ieder willekeurig lichaam. Verder kan ieder willekeurig lichaam opgevat worden als een vectorruimte over het lichaam van de rationale getallen (zie §1 stelling 1).

3) Stel a, b zijn reële getallen met $a < b$; met $C[a,b]$ geven wij aan de verzameling van alle continue reëelwaardige functies gedefiniëerd op het interval $[a,b]$. Als $f,g \in C[a,b]$ en als $\alpha \in R$ dan definiëren we functies $f + g$ en $\alpha f \in C[a,b]$ door

$(f + g)(x) = f(x) + g(x)$

$(\alpha f)(x) = \alpha . f(x) \qquad x \in [a,b]$.

Dan is $C[a,b]$ een lineaire ruimte over R.

3') Zij D de verzameling van alle op $(-\infty,+\infty)$ differentiëerbare reële functies f met $f(0) = 0$.
Laat een optelling en een vermenigvuldiging met reële getallen in D gedefiniëerd zijn als boven. Dan is D een vectorruimte over R.

4) Zij L een willekeurig lichaam en $L[x]$ de verzameling van alle uitdrukkingen van de gedaante $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots = \sum_{n=1}^{\infty} \alpha_n x^n$, waarbij de coëfficiënten α_n getallen uit L zijn met $\alpha_n \neq 0$ voor slechts eindig veel n. $P = \sum_{n=1}^{\infty} \alpha_n x^n$ noemt men een veelterm of polynoom over L. Als n het grootste getal is met $\alpha_n \neq 0$, dan heet n de graad van P.
Voor $\alpha \in L$ en veeltermen $P_1 = \sum_{n=1}^{\infty} \beta_n x^n$, $P_2 = \sum_{n=1}^{\infty} \gamma_n x^n \in L[x]$ definiëren wij

$P_1 + P_2 = \sum_{n=1}^{\infty} (\beta_n + \gamma_n) x^n$ en $\alpha P_1 = \sum_{n=1}^{\infty} (\alpha \beta_n) x^n$.

Dan is $L[x]$ een vectorruimte over L.

Definitie 2. Zij V een lineaire ruimte over een lichaam L en B een deelverzameling van V.
B heet een (lineaire) deelruimte van V indien aan de volgende voorwaarde is voldaan:

$\alpha x + \beta y \in B$ voor alle $x,y \in B$ en alle $\alpha,\beta \in L$.

Opmerking 4.

Men kan gemakkelijk nagaan dat een deelruimte B van V zelf weer een vectorruimte over L is, als we de optelling in B en de vermenigvuldiging met getallen uit L op dezelfde wijze definiëren als in V.
Verder kan men eenvoudig bewijzen dat de doorsnede van een willekeurig aantal deelruimten van V weer een deelruimte is van V.
Zij nu gegeven een willekeurige deelverzameling A van V, dan bestaat er een kleinste lineaire deelruimte van V die A omvat, namelijk de doorsnede van alle deelruimten die A omvatten.
Deze deelruimte noemen wij het lineaire omhulsel van A of ook de deelruimte opgespannen door A.

Stelling 3. Zij V een vectorruimte over L en $A \subseteq V$.
Dan is er een kleinste lineaire deelruimte H(A) van V die A omvat.
H(A) bestaat uit alle lineaire combinaties van eindig veel elementen uit A.

Bewijs.

Als $x_1, x_2, \ldots, x_n \in A$ en $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, dan zal de vector $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ moeten behoren tot alle lineaire deelruimten die A omvatten; dus $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \in H(A)$.
Omgekeerd vormen al deze lineaire combinaties van elementen uit A kennelijk een lineaire deelruimte van V die A omvat.

Stelling 4. Zij V een vectorruimte over L en H(A) de deelruimte opgespannen door A. Dan geldt:

(1) Als $A \subseteq B \subseteq V$ dan $H(A) \subseteq H(B)$.
(2) Als $x \in H(A)$, dan is er een eindige deelverzameling A_0 van A waarvoor $x \in H(A_0)$.
(3) $A \subseteq H(A)$.
(4) $H(H(A)) = H(A)$.
(5) Als $x \in H(A \cup \{y\})$ en $x \notin H(A)$ dan $y \in H(A \cup \{x\})$.

Bewijs.

De eigenschappen (1) en (3) zijn evident. Eigenschap (2) volgt uit het feit dat ieder element van H(A) een lineaire combinatie is van eindig veel elementen uit A.

Daar H(A) een deelruimte is van V is H(A) zeker de kleinste deelruimte van V die H(A) omvat, dus H(H(A)) = H(A).

Stel tenslotte dat $x \in H(A \cup \{y\})$. Dan is x te schrijven als:

$$x = \alpha_0 y + \sum_{i=1}^{n} \alpha_i y_i \quad \text{met } \alpha_i \in L \quad i = 0, \ldots, n \quad \text{en}$$
$$y_i \in A \quad i = 1, \ldots, n.$$

Daar $x \notin H(A)$ is $\alpha_0 \neq 0$. Dus

$$y = \alpha_0^{-1} x - \sum_{i=1}^{n} \alpha_0^{-1} \alpha_i y_i \Rightarrow y \in H(A \cup \{x\}).$$

Voorbeelden.

5) De reële getallen en de zuiver imaginaire getallen vormen elk een lineaire deelruimte van C als vectorruimte over R (of over Q).

6) De vectorruimte D uit voorbeeld 3' is een lineaire deelruimte van $C[-\omega, \omega]$ uit voorbeeld 3.

7) De polynomen over L met graad $\leq n$ vormen een lineaire deelruimte van $L[x]$.

8) Zij L een lichaam en $A = \{1, x, x^2, \ldots, x^n\} \subset L[x]$.
Dan is H(A) de deelruimte van $L[x]$ bestaande uit alle polynomen met graad $\leq n$.

9) In C, beschouwd als lineaire ruimte over zichzelf spant $A = \{1\}$ heel C op: H(A) = C.
Beschouwen wij C daarentegen als lineaire ruimte over R, dan bestaat het lineair omhulsel van $\{1\}$ uit alle reële getallen: H(A) = R.
H(A) hangt dus mede af van het scalairen lichaam L.

Opgaven.

1. Zij $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{3}$ en Q het lichaam van de rationale getallen.
   Bewijs dat alle getallen $a + b\omega$ met $a,b \in Q$ een lichaam $Q(\omega)$ vormen.

2. Een niet-lege deelverzameling L van C is een lichaam als L met elk tweetal elementen a en b zowel $a - b$ als ab^{-1} voor $b \neq 0$ bevat.

3. Zij W de verzameling van alle convergente meetkundige reeksen. W_1 is de deelverzameling van W, gevormd door alle reeksen met beginterm gelijk aan 1. W_2 is de deelverzameling van W, gevormd door alle reeksen met dezelfde reden r.
   Vormt W onder de gebruikelijke optelling en vermenigvuldiging met een reëel getal een vectorruimte over R?
   Zijn W_1 en W_2 vectorruimten?

4. Gegeven is de verzameling V van vectoren
   $$(4,1,4) + \lambda(1,2,0) + \mu(a,-1,4) \quad \text{in } R^3.$$
   Bepaal a zodanig dat V een lineaire deelruimte is.

5. Zij V een vectorruimte over L en $a,b,c \in V$.
   Gegeven is dat $a \neq 0$, $a \in H(\{b,c\})$, $b \notin H(\{a,c\})$.
   Bewijs dat $c \in H(\{a\})$.

6. Stel V een vectorruimte over L. Als B_1 en B_2 deelruimten zijn van V, dan is ook $B_1 + B_2 := \{x + y \mid x \in B_1, y \in B_2\}$ een lineaire deelruimte van V.

7. Stel V een vectorruimte over L en $A \subset V$, $B \subset V$.
   Dan is $H(A \cup B) = H(A) + H(B)$.

8. Zij B een lineaire deelruimte van een vectorruimte V over L en $a \in V$.
   Geëf nodige en voldoende voorwaarde(n) opdat a + B een lineaire ruimte is.

§3. Lineaire afhankelijkheid en onafhankelijkheid. Basis

In deze paragraaf is L een gegeven lichaam, V een vectorruimte over L en A een niet-lege deelverzameling van V, $V \neq \{0\}$.

Definitie 1. Een deelverzameling A van V met de eigenschap dat $H(A) = V$ heet een stel voortbrengenden van V.

Definitie 2. Een deelverzameling A van V heet lineair onafhankelijk indien $x \notin H(A \setminus \{x\})$ voor iedere $x \in A$.
A heet lineair afhankelijk indien A niet lineair onafhankelijk is.

Opmerking 1.
Uit §2 stelling 3 volgt dat een stel voortbrengenden A van V een deelverzameling is van V met de eigenschap dat ieder element van V een lineaire combinatie is van eindig veel elementen uit A. Verder is A een stel voortbrengenden van de vectorruimte H(A).

Opmerking 2.
Zij ϕ de lege verzameling, dan is $H(\phi) = \{0\}$, de vectorruimte die alleen uit de nulvector bestaat.
De nulvector ligt dus in $H(A \setminus \{0\})$ voor iedere deelverzameling A van V. Dus als $0 \in A$, dan is A lineair afhankelijk. I.h.b. is de deelverzameling $A = \{0\}$ lineair afhankelijk en iedere deelverzameling $A = \{x\}$ met $x \neq 0$ lineair onafhankelijk.

Opmerking 3.
Zij $X = \{x_i\}_{i \in I}$ een willekeurige verzameling van elementen uit V; $x_i \in V$ voor alle $i \in I$.
X noemen wij dan lineair onafhankelijk als voor iedere $j \in I$ geldt $x_j \notin H(\{x_i\}_{i \neq j, i \in I})$.
Voor lineair onafhankelijke verzamelingen $X = \{x_i\}_{i \in I}$ geldt dus steeds dat $x_i \neq x_j$ als $i \neq j$, $ij \in I$.

Stelling 1. Een deelverzameling A van V is dan en slechts dan lineair onafhankelijk indien uit de betrekking

$$(*) \qquad \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0$$

volgt dat $\alpha_i = 0$, $i = 1, \ldots, n$. Hierbij zijn de $x_1, x_2, \ldots, x_n$ onderling verschillende vectoren uit A en $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$.

Bewijs.

a) Stel A lineair onafhankelijk en laat in (*) bijvoorbeeld $\alpha_1 \neq 0$ zijn. Dan is als $n = 1$, $\alpha_1 x_1 = 0 \Rightarrow x_1 \neq 0$, dus A lineair afhankelijk. Als $n \neq 1$, dan $x_1 = \sum_{i=2}^{n} \alpha_1^{-1} \alpha_2 x_i \in H(A \setminus \{x_1\})$, zodat A niet lineair onafhankelijk is.

b) Stel omgekeerd A lineair afhankelijk. Dan is er een $x_1 \in A$ met $x_1 \in H(A \setminus \{x_1\})$, d.w.z.

$$x_1 = \alpha_2 x_2 + \ldots + \alpha_n x_n \text{ met onderling verschillende } x_i \in A, \quad i = 1, \ldots, n$$

en $\alpha_i \in L$, $i = 2, \ldots, n$.
Maar dan geldt (*) met $\alpha_1 = -1 \neq 0$.
Als A maar uit één element bestaat, dan is $A = \{0\}$ en is aan (*) voldaan voor alle α: $\alpha . 0 = 0$.

Gevolg 1; A is dan en slechts dan lineair onafhankelijk indien alle eindige deelverzamelingen van A lineair onafhankelijk zijn.

Gevolg 2: Een eindige verzameling $A = \{x_1, x_2, \ldots, x_n\}$ is dan en slechts dan lineair afhankelijk als er getallen $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ bestaan, niet alle 0, waarvoor $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0$.

Stelling 2. Als A lineair onafhankelijk is en $x_0 \notin H(A)$, dan is ook $A \cup \{x_0\}$ lineair onafhankelijk.

Bewijs. Stel $A \cup \{x_0\} = A_0$ lineair afhankelijk. Dan is er een x_1 met $x_1 \in A_0$ en $x_1 \in H(A_0 \setminus \{x_1\})$. Daar $x_0 \notin H(A)$ is zeker $x_1 \neq x_0$ en dus $x_1 \in A$.

Er geldt dus als $A^1 = A \setminus \{x_1\}$ dat $x_1 \in H(A^1 \cup \{x_0\})$ en $x_1 \notin H(A^1)$.
Volgens §2 stelling 4 (5) is dan voldaan aan $x_0 \in H(A^1 \cup \{x_1\}) = H(A)$,
in tegenspraak met de gegevens.

Definitie 3. Een basis voor V is een lineair onafhankelijk stel voortbrengenden van V.

Stelling 3. Zij B een basis voor V. Iedere $x \in V$ is op één en slechts één wijze (op volgorde-wijzigingen na) te schrijven in de vorm

$x = \alpha_1 x_1 + \ldots + \alpha_n x_n$, met onderling verschillende $x_1, x_2, \ldots, x_n \in B$ en met coëfficiënten $\alpha_i \neq 0$, $\alpha_i \in L$, $i = 1, \ldots, n$.

Bewijs. Daar $H(B) = V$, is ieder element van V een lineaire combinatie van elementen uit B.
Stel nu dat $x = \alpha_1 x_1 + \ldots + \alpha_n x_n$
en $x = \beta_1 x_1 + \ldots + \beta_n x_n$.
Dan is $(\alpha_1 - \beta_1)x_1 + \ldots + (\alpha_n - \beta_n)x_n = 0$.
Uit de lineaire onafhankelijkheid van B volgt dan dat
$\alpha_1 - \beta_1 = 0$; $\alpha_2 - \beta_2 = 0$; $\ldots$; $\alpha_n - \beta_n = 0$, d.w.z.
$\alpha_1 = \beta_1$; $\alpha_2 = \beta_2$; $\ldots$; $\alpha_n = \beta_n$.
Hiermee is de ondubbelzinnigheid van de schrijfwijze aangetoond.

Stelling 4. Zij A een deelverzameling van V.
De volgende drie beweringen zijn equivalent:
(a) A is een minimaal stel voortbrengenden van V.
(b) A is een basis voor V.
(c) A is een maximale lineair onafhankelijke deelverzameling.

Bewijs.
(a) $\Rightarrow$ (b): Stel dat A niet lineair onafhankelijk is. Dan is er een $x \in A$ met $x \in H(A \setminus \{x\})$. Daar $A \setminus \{x\} \subset H(A \setminus \{x\})$ (§2 stelling 4 (3)) hebben wij $A \subset H(A \setminus \{x\})$.
Hieruit volgt dat $V = H(A) \subset H(H(A \setminus \{x\})) = H(A \setminus \{x\}) \Rightarrow V = H(A \setminus \{x\})$.
$A \setminus \{x\}$ is dus een stel voortbrengenden van V, in tegenspraak met de minimaliteit van A.

(b) $\Rightarrow$ (c). Stel $x \in V$, $x \notin A$. Dan is daar $H(A) = V$, $x \in H(A)$. De deelverzameling $A \cup \{x\}$ is dus niet lineair onafhankelijk.
A is dus inderdaad een maximale lineair onafhankelijke deelverzameling.
(c) $\Rightarrow$ (a). Stel $H(A) \neq V$. Dan is er een $y \in V$ met $y \notin H(A)$.
Uit §3 stelling 2 volgt dan dat ook $A \cup \{y\}$ lineair onafhankelijk is, in tegenspraak met de maximaliteit van A. A is dus een stel voortbrengenden van V.
Wij bewijzen nu dat A minimaal is. Stel voor zekere $x \in A$, $A \setminus \{x\}$ ook een stel voortbrengenden.
Dan geldt $x \in V = H(A \setminus \{x\})$ en dit is in strijd met de lineaire onafhankelijkheid van A.

Voorbeelden.

a) In R^n vormen de n vectoren $e_1 = (1, 0, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, 0, 0, \ldots, 1)$ een basis.
In R^3 zijn de vectoren $x_1 = (1, 2, 3)$, $x_2 = (1, 0, -1)$ en $x_3 = (0, 1, 2)$ lineair afhankelijk.

b) Voor iedere $\varepsilon \in (0,1]$ zij f_ε een continue reëelwaardige functie op $[0,1]$ met de eigenschap $f_\varepsilon(t) \neq 0$ voor $0 \leqslant t < \varepsilon$; $f_\varepsilon(t) = 0$ voor $\varepsilon \leqslant t \leqslant 1$.
Dan is $A = \{f_\varepsilon : 0 < \varepsilon \leqslant 1\}$ een oneindige lineair onafhankelijke deelverzameling van $C[0,1]$; A is geen basis.

c) Zij $L[x]$ de verzameling van alle polynomen over L.
Stel $A = \{1, x, x^2, x^3, \ldots\}$.
Dan is A een basis voor $L[x]$.

d) Zij $Q(i\sqrt{2})$ de verzameling van alle complexe getallen van de vorm $z = a + bi\sqrt{2}$ met rationale a en b.
Dan is $A = \{1, i\sqrt{2}\}$ een basis voor $Q(i\sqrt{2})$ beschouwd als vectorruimte over Q.

e) R beschouwd als vectorruimte over Q heeft geen eindige basis.

Definitie 4. Een vectorruimte V heet eindig-dimensionaal als V een eindig stel voortbrengenden heeft.

Stelling 5. Iedere eindig dimensionale vectorruimte V heeft een eindige basis.

Bewijs. Zij $A = \{x_1, \ldots, x_n\}$ een eindig stel voortbrengenden van V. Dan is er daar A slechts eindig veel deelverzamelingen heeft, een deelverzameling B van A zó dat B een minimaal stel voortbrengenden is. Uit stelling 4 volgt dan dat B een basis is voor V.

Opmerking 4.
Men kan in het algemeen bewijzen dat iedere lineaire ruimte V over een lichaam L een basis heeft. Als V niet eindig-dimensionaal is, gebruikt men voor het bewijs van deze stelling één of andere vorm van het keuze axioma (het Lemma van Zorn of de Welordeningsstelling van Zermelo).

Stelling 6. Als een vectorruimte V een eindige basis B heeft van n elementen, dan is iedere andere basis B^1 van V eindig en heeft precies n elementen.

Bewijs. Stel $B = \{x_1, x_2, \ldots, x_n\}$ en stel $B \notin B^1$, dan is er een x_i b.v. $x_1 \notin B^1$. Dan is daar B minimaal is $B \setminus \{x_1\}$ geen stel voortbrengenden van V, dus $H(B \setminus \{x_1\}) \neq V$.
Daar $H(B^1) = V$ volgt dat $B^1 \notin H(B \setminus \{x_1\})$.
Er is dus een $y_1 \in B^1$ met $y_1 \notin H(B \setminus \{x_1\})$. Daar $y_1 \in H(B) = V$ volgt dat $x_1 \in H(B \setminus \{x_1\}) \cup \{y_1\})$.
Daar $B \setminus \{x_1\} \subset H((B \setminus \{x_1\}) \cup \{y_1\})$ is $B \subset H((B \setminus \{x_1\}) \cup \{y_1\})$.
$(B \setminus \{x_1\}) \cup \{y_1\} = B_1$ is dus een stel voortbrengenden van V.
Tevens is B_1 lineair onafhankelijk (§3 stelling 2) en dus een basis voor V. B_1 heeft weer n elementen en het aantal elementen uit $B^1 \cap B_1$ is één groter dan het aantal elementen uit $B^1 \cap B$. $|B_1 \cap B^1| = |B \cap B^1| + 1$.
Geldt $B_1 \notin B^1$, dan is er een basis B_2 met n elementen zó dat
$|B_2 \cap B^1| = |B_1 \cap B^1| + 1 = |B \cap B^1| + 2$.
Na eindig veel stappen komt men zo tot een basis B_m met n elementen zó dat $|B_m \cap B^1| = n \Rightarrow B_m \subset B^1$. Uit §3 stelling 4 volgt dan dat $B_m = B^1$ en dus dat $|B^1| = n$.

Definitie 5. Een vectorruimte V over een lichaam L met een basis van n-elementen heet een n-dimensionale vectorruimte.
Notatie: $[V : L] = n$ of $\dim(V) = n$.
Als V geen eindige basis heeft noemen wij V oneindig dimensionaal, $\dim(V) = \infty$.

Opmerking 5.
De vectorruimte $V = \{0\}$ die alleen uit de nulvector bestaat, zullen wij 0-dimensionaal noemen.
De dimensie van een vectorruimte hangt mede af van het scalairen lichaam. Zo is $[C : C] = 1$, maar $[C : R] = 2$.

Stelling 7. Zij V een n-dimensionale vectorruimte en A een lineair onafhankelijke deelverzameling. Dan is $|A| \leq n$.

Bewijs. Stel $B = \{x_1, x_2, \ldots, x_n\}$ een basis voor V. Als A een basis is voor V dan $|A| = n$ volgens stelling 6.
Zij nu $H(A) \neq V$, dan $B \not\subset H(A)$. Stel $x_1 \notin H(A)$. Dan $A \cup \{x_1\} = A_1$, lineair onafhankelijk. Als $B \not\subset H(A \cup \{x_1\})$ dan is er een $x_2 \in B$ met $x_2 \notin H(A \cup \{x_1\})$ en $A \cup \{x_1\} \cup \{x_2\} = A_2$ lineair onafhankelijk. Daar B eindig is komt men na eindig veel stappen tot een lineair onafhankelijke verzameling $A_m = A \cup \{x_1\} \cup \ldots \cup \{x_m\}$ met $H(A_m) = V$.
A_m is dus een basis voor V en volgens stelling 6 is dan $|A_m| = n \Rightarrow |A| \leq n$.

Opgaven.

1. Voor welke waarden van λ is het stelsel $\{(\lambda,1,3), (4,\lambda,6), (3,0,3)\} \subset R^3$ afhankelijk?
2. Gegeven is dat $\{a,b,c\}$ een basis is voor een vectorruimte V over R. Is het stelsel $\{x,y,z\}$ met $x = a + b + c$, $y = 2a + b + 3c$, $z = a - b + 3c$ een basis?
3. Zij V een n-dimensionale vectorruimte en V^1 een lineaire deelruimte van V. Dan is $\dim V^1 = m \leq n$. Als $V^1 \neq V$ dan $\dim V^1 < \dim V$.
4. Zij V een n-dimensionale vectorruimte en A een lineair onafhankelijk stel vectoren uit V. Dan kan A aangevuld worden tot een basis van V.

5. Zijn A en B twee lineaire deelruimten van een eindig dimensionale vectorruimte V. Dan geldt voor de dimensies:
   $\dim (B + C) = \dim B + \dim C - \dim (B \cap C)$.

6. In R^3 zijn gegeven de vectoren $x_\lambda = (\lambda^2,2,1)$, $y_\lambda = (4,\lambda,1)$ en $z = (4,2,1)$.
   Bepaal voor iedere waarde van $\lambda \in R$ de dimensie van $H\{x_\lambda, y_\lambda, z\}$.

§4. Lineaire afbeeldingen

Definitie 1. Stel V en W twee lineaire ruimten over eenzelfde lichaam L. Een afbeelding $\varphi : V \to W$ heet een lineaire afbeelding of homomorfisme indien

1^o) $\varphi(x + y) = \varphi(x) + \varphi(y)$ voor alle $x,y \in V$

2^o) $\varphi(\alpha x) = \alpha \varphi(x)$ voor alle $x \in V$ en $\alpha \in L$.

Indien $V = W$ dan heet φ ook een endomorfisme.

Een 1-1 duidige lineaire afbeelding heet een isomorfisme.

Een automorfisme is een 1-1 duidige endomorfisme van V op V.

Uit definitie 1 volgt onmiddellijk:

Stelling 1. De afbeelding $\varphi : V \to W$ is lineair dan en slechts dan als $\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y)$ voor alle $\alpha,\beta \in L$ en $x,y \in V$.

Voorbeelden.

a) Zij V een vectorruimte over L en $\lambda \in L$. Dan is de afbeelding φ: $V \to V$ met $\varphi(x) = \lambda x$ voor alle $x \in V$ lineair.

b) Zij $L[x]$ de ruimte van alle polynomen in x met coëfficiënten uit L. Dan is de afbeelding $\varphi : L[x] \to L[x]$ met $\varphi(\sum_{i=1}^{n} \alpha_i x^i) = \sum_{i=1}^{n} \alpha_i x^{i+1}$ een lineaire afbeelding.

c) De afbeelding $f(x) \to \int_a^b f(x)dx$ is een lineaire afbeelding van $C[a,b]$ op R.

d) De afbeeldingen Re en Im die aan $x \in C$ respectievelijk het reële en het imaginaire deel toevoegen zijn lineaire afbeeldingen van C in R (beide beschouwd als vectorruimten over R).

e) Zij V een vectorruimte over L. Onder een <u>lineaire functie</u> φ op V verstaat men een lineaire afbeelding van V in het lichaam L opgevat als vectorruimte over L.

Zijn nu $\varphi_1, \ldots, \varphi_n$ n lineaire functies op V, dan is de afbeelding $x \to (\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x))$ een homomorfisme van V in L^n.

f) Zij $A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ & & & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$ een reële m×n matrix.

Met behulp van A kunnen wij een homomorfisme T van R^n in R^m definieren als volgt:

als $x = (x_1, \ldots, x_n) \in R^n$, dan zij Tx het element $y = (y_1, \ldots, y_m) \in R^m$ met $y_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n$ $(i = 1, 2, \ldots, m)$.

<u>Definitie 2</u>. Is φ: V → W een homomorfisme dan heet

$\varphi V = \{\varphi x \mid x \in V\}$ het <u>beeld</u> van φ en

$\varphi^{-1}(0) = \{x \mid x \in V, \varphi(x) = 0\}$ de <u>kern</u> van φ.

<u>Stelling 2</u>. De kern $\varphi^{-1}(0)$ en het beeld $\varphi(V)$ van een homomorfisme φ: V →W, zijn lineaire deelruimten van respectievelijk V en W.

<u>Bewijs</u>. Zijn x en y vectoren uit $\varphi^{-1}(0)$ en $\alpha, \beta \in L$ dan is

$\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y) = \alpha 0 + \beta 0 = 0$.

Dus $\alpha x + \beta y \in \varphi^{-1}(0) \Rightarrow \varphi^{-1}(0)$ een lineaire deelruimte van V.

Is $x^* = \varphi(x) \in \varphi V$ en $y^* = \varphi(y) \in \varphi(V)$ en $\alpha, \beta \in L$ dan is $\alpha x^* + \beta y^* =$

$= \alpha\varphi(x) + \beta\varphi(y) = \varphi(\alpha x + \beta y) \in \varphi(V)$.

Het beeld $\varphi(V)$ is dus een lineaire deelruimte van W.

<u>Stelling 3</u>. Zij φ een homomorfisme van een n-dimensionale vectorruimte V in een vectorruimte W. Dan is de som van de dimensies van kern en beeld gelijk aan de dimensie van V: $\dim \varphi^{-1}(0) + \dim \varphi(V) = \dim V$.

Bewijs. Daar $\varphi^{-1}(0)$ een lineaire deelruimte is van V is $\varphi^{-1}(0)$ eindig dimensionaal en dim $(\varphi^{-1}(0)) = m \leqslant n = \dim V$.
Kies een basis $x_1, \ldots, x_m$ van $\varphi^{-1}(0)$ en vul deze aan tot een basis $x_1, \ldots, x_m, x_{m+1}, \ldots, x_n$ van V (vgl. §3 opgave 3 en 4).
Dan is $\varphi(x_i) = 0$, $i = 1, \ldots, m$.
Stel $\varphi(x_i) = y_i$, $m < i \leqslant n$.
We zullen nu bewijzen dat de vectoren $\{y_i\}$, $i = m+1, m+2, \ldots, n$ een stel voortbrengenden van $\varphi(V)$ vormen.
Immers voor willekeurige $y = \varphi(x) \in \varphi(V)$ geldt:

$$\begin{aligned} y = \varphi(x) = \varphi(\alpha_1 x_1 + \ldots \alpha_n x_n) &= \alpha_1\varphi(x_1) + \ldots + \alpha_m\varphi(x_m) + \alpha_{m+1}\varphi(x_{m+1}) + \ldots \alpha_n\varphi(x_n) \\ &= \alpha_1 0 + \ldots + \alpha_m 0 + \alpha_{m+1} y_{m+1} + \ldots + \alpha_n y_n \\ &= \alpha_{m+1} y_{m+1} + \ldots + \alpha_n y_n. \end{aligned}$$

Het stelsel $\{y_i\}$ $m < i \leqslant n$ is zelfs lineair onafhankelijk en dus een basis, daar als $\alpha_{m+1} y_{m+1} + \ldots + \alpha_n y_n = 0$ dan is
$\alpha_{m+1}\varphi(x_{m+1}) + \ldots + \alpha_n\varphi(x_n) = \varphi(\alpha_{m+1} x_{m+1} + \ldots + \alpha_n x_n) = 0$.
Dus $\alpha_{m+1} x_{m+1} + \ldots + \alpha_n x_n \in \varphi^{-1}(0)$.
Omdat $x_1, \ldots, x_m$ een basis van $\varphi^{-1}(0)$ is, bestaan er getallen $\alpha_1, \ldots, \alpha_m$ zó dat $\alpha_{m+1} x_{m+1} + \ldots + \alpha_n x_n = \alpha_1 x_1 + \ldots + \alpha_m x_m$.
Uit de lineaire onafhankelijkheid van $x_1, \ldots, x_n$ volgt dan dat
$\alpha_{m+1} = \alpha_{m+2} = \ldots = \alpha_n = 0$.
De dimensie van $\varphi(V)$ is dus gelijk aan $n - m$, waarmee het gestelde is aangetoond.

Gevolg 1. Als φ een isomorfisme is van V in W dan is dim V = dim $\varphi(V)$.
Immers dan is $\varphi^{-1}(0) = \{0\}$ en dus 0-dimensionaal.

Uit het feit dat $\varphi^{-1}(0) = \{0\}$ dan en slechts dan als φ 1-1 duidig is, volgt onmiddellijk:

Gevolg 2. Zij V een eindig dimensionale vectorruimte en φ een endomorfisme van V. Een noodzakelijke en voldoende voorwaarde opdat φ een automorfisme is, is dat φ een afbeelding op is.

Definitie 3. Twee vectorruimten V en W over een lichaam L heten isomorf als er een isomorfisme φ van V op W bestaat.

Stelling 4. Een homomorfisme φ: V $\rightarrow$ W is volkomen bepaald door haar werking op de vectoren van een basis van V.
Vormen $v_1, \ldots, v_n$ een basis van V en zijn $w_1, \ldots, w_n$ elementen uit W, dan bestaat precies één homomorfisme σ met $\sigma(v_i) = w_i$, i = 1,...,n.

Bewijs.
1) Daar ieder element $x \in V$ te schrijven is als $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$ is dus $\varphi(x) = \alpha_1 \varphi(v_1) + \ldots + \alpha_n \varphi(v_n)$ en is φ volkomen bepaald door haar werking op de basis vectoren.
2) Stel nu $w_1, \ldots, w_n \in W$ en definiëer voor $x \in V$ met $x = \alpha_1 v_1 + \ldots + \alpha_n v_n$, $\sigma(x) = \alpha_1 \sigma(v_1) + \ldots + \alpha_n \sigma(v_n) = \alpha_1 w_1 + \ldots + \alpha_n w_n$.
Dan is als $y = \beta_1 v_1 + \ldots + \beta_n v_n$,
$\alpha x + \beta y = (\alpha\alpha_1 + \beta\beta_1) v_1 + \ldots + (\alpha\alpha_n + \beta\beta_n) v_n$ en
$\sigma(\alpha x + \beta y) = \alpha\sigma(x) + \beta\sigma(y)$. Volgens §4 stelling 1 is σ dan een homomorfisme.

Stelling 5. Zij V een n-dimensionale vectorruimte over L. Dan is V isomorf met L^n.

Bewijs. Stel $a_1, \ldots, a_n$ een basis voor V en $e_1 = (1, 0, \ldots 0), \ldots, e_n = (0, 0, \ldots, 1)$ een basis voor L^n, dan is volgens stelling 4 de afbeelding φ gedefiniëerd door $\varphi(a_i) = e_i$, i = 1, ..., n voort te zetten tot een homomorfisme van V in L^n.
Daar $e_i \in \varphi(V)$, i = 1, ..., n is $\varphi(V)$ een n-dimensionale deelruimte van L^n en dus gelijk aan L^n. Dus φ is een afbeelding op.
Verder is dan volgens stelling 3 dim $\varphi^{-1}(0) = 0$, dus $\varphi^{-1}(0) = \{0\} \Rightarrow$
$\Rightarrow \varphi$ 1-1 duidig.

Definitie 4. Is φ een homomorfisme van V in W, dan verstaat men onder de rang van φ de dimensie van $\varphi(V)$.

Opmerking 1.
Stel dat $v_1, \ldots, v_n$ een basis is voor V, dan wordt $\varphi(V)$ opgespannen door de vectoren $\varphi(v_1), \ldots, \varphi(v_n)$ en de rang van φ is dus gelijk aan

het maximale aantal lineair onafhankelijke vectoren uit $\varphi(v_1)$, ..., $\varphi(v_n)$.

Zijn $\varphi_1 : V \to W$ en $\varphi_2 : W \to Z$ homomorfismen, dan zullen wij de samengestelde afbeelding van V in Z, die aan $v \in V$ toevoegt $\varphi_2(\varphi_1(v)) \in Z$ aangeven met $\varphi_2 \circ \varphi_1$.
Deze afbeelding is zelf weer een homomorfisme van V in Z.
Indien $\varphi : V \to W$ zowel één-éénduidig is als op dan is φ ondubbelzinnig omkeerbaar, voor de omkeer afbeelding schrijven wij φ^{-1}.
Men gaat gemakkelijk na dat ook φ^{-1} weer een isomorfisme is. Verder geldt dat als $\varphi_1 : V \to W$ en $\varphi_2 : W \to Z$ isomorfismen op zijn, dan is $\varphi_2 \circ \varphi_1$ een isomorfisme van V op Z en $(\varphi_2 \circ \varphi_1)^{-1} = \varphi_1^{-1} \circ \varphi_2^{-1}$.

Stelling 6. Voor het product $\varphi_2 \circ \varphi_1$ van 2 homomorfismen $\varphi_1 : V \to W$, $\varphi_2 : W \to Z$ geldt steeds $\text{rang}\, \varphi_2 \circ \varphi_1 \leqslant \text{rang}\, \varphi_1$ en
$\text{rang}\, \varphi_2 \circ \varphi_1 \leqslant \text{rang}\, \varphi_2$.

Bewijs. Uit stelling 4 volgt dat voor iedere vectorruimte E_1 en homomorfisme φ van E_1 in E_2 geldt

$$\dim \varphi(E_1) \leqslant \dim E_1 .$$

Dus $\text{rang}\,(\varphi_2 \circ \varphi_1) = \dim \varphi_2(\varphi_1(V)) \leqslant \dim \varphi_1(V) = \text{rang}\, \varphi_1$.
Verder is daar $\varphi_2(\varphi_1(V)) \subset \varphi_2(W)$ ook
$\dim \varphi_2(\varphi_1(V)) \leqslant \dim \varphi_2(W) = \text{rang}\, \varphi_2$. q.e.d.

Zijn φ_1 en φ_2 twee homomorfismen van V en W en is $\lambda \in L$, dan kan men de volgende afbeeldingen van V in W beschouwen:
$\varphi_1 + \varphi_2$ is de afbeelding gedefiniëerd door
$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$, $x \in V$ en
$(\lambda\varphi_1)(x) = \lambda(\varphi_1(x))$ $x \in V$.
Men bewijst nu gemakkelijk:

Stelling 7. Met de bovengenoemde definities van optelling en vermenigvuldiging met getallen uit L vormen de homomorfismen van V in W een vectorruimte Hom(V,W) over L.

Opmerking 2.

De vectorruimte Hom(V,L) die bestaat uit alle lineaire functies van V in L zullen wij de duale ruimte V^+ van V noemen.

§5. Matrices

Wij zullen in deze paragraaf steeds homomorfismen van de vectorruimten L^n en L^m beschouwen. Dit is geen wezenlijke beperking, daar volgens §4 stelling 5 iedere n-dimensionale vectorruimte over L isomorf is met L^n.

Vectoren uit L^n zullen wij steeds aangeven als kolommen van n getallen

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} .$$

Als basis kiezen wij de vectoren

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} , \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} , \ldots , e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} .$$

Een homomorfisme $\varphi: L^n \to L^m$ is volgens §4 stelling 4 ondubbelzinnig bepaald door haar werking op de basis vectoren:

$$\varphi(e_1) = a_1 = \begin{pmatrix} \varphi_{11} \\ \vdots \\ \varphi_{m1} \end{pmatrix} , \varphi(e_2) = a_2 = \begin{pmatrix} \varphi_{12} \\ \vdots \\ \varphi_{m2} \end{pmatrix} , \ldots , \varphi(e_n) = a_n = \begin{pmatrix} \varphi_{1n} \\ \vdots \\ \varphi_{mn} \end{pmatrix} .$$

Het homomorfisme φ geeft men dan ook vaak aan door het volgende schema van de m n getallen φ_{ij}.

$$\varphi = \begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2n} \\ \vdots & \vdots & & \vdots \\ \varphi_{m1} & \varphi_{m2} & \cdots & \varphi_{mn} \end{pmatrix}$$

Een dergelijk schema van m rijen en n kolommen noemt men een m × n-matrix.

Stelling 1. De homomorfismen $\varphi: L^n \to L^m$ worden 1-1 duidig voorgesteld door de m × n-matrices.

Bewijs. Dit volgt onmiddellijk uit §4 stelling 4.

Het beeld van een willekeurige vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ onder het homomorfisme $\varphi = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix}$ wordt gegeven door

$$\begin{pmatrix} \varphi_{11} \cdots \varphi_{1n} \\ \vdots \\ \varphi_{m1} \cdots \varphi_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \varphi_{11}x_1+\varphi_{12}x_2+\ldots\varphi_{1n}x_n \\ \varphi_{21}x_1+\varphi_{22}x_2+\ldots\varphi_{2n}x_n \\ \vdots \\ \varphi_{m1}x_1+\varphi_{m2}x_2+\ldots\varphi_{mn}x_n \end{pmatrix} = x_1\varphi(e_1)+\ldots x_n\varphi(e_n).$$

Definitie 1. Het α-voud, de som en het product van matrices is de matrix-voorstelling van het α-voud, de som en het product van de homomorfismen die de matrices voorstellen.

Opmerking 1.
Daar de som van 2 homomorfismen φ_1 en φ_2 alleen gedefiniëerd is als $\varphi_1: L^n \to L^m$ en $\varphi_2: L^n \to L^m$, is ook de som van een m × n-matrix en een k × r-matrix alleen gedefiniëerd als k = m, n = r.
Evenzo is het product van een m × n-matrix en een k × r-matrix alleen gedefiniëerd als k = n.

Het α-voud van φ is het homomorfisme dat de vector e_i transformeert in $\alpha\varphi(e_i)$; $\alpha\varphi$ wordt dus voorgesteld door de matrix

$$\alpha \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} = \begin{pmatrix} \alpha\varphi_{11} & \cdots & \alpha\varphi_{1n} \\ \vdots & & \\ \alpha\varphi_{m1} & & \alpha\varphi_{mn} \end{pmatrix}.$$

$\varphi + \psi$ is het homomorfisme dat de vector e_i transformeert in $\varphi(e_i) + \psi(e_i)$, dus

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} + \begin{pmatrix} \psi_{11} & \cdots & \psi_{1n} \\ \vdots & & \\ \psi_{m1} & \cdots & \psi_{mn} \end{pmatrix} = \begin{pmatrix} \varphi_{11}+\psi_{11} & \cdots & \varphi_{1n}+\psi_{1n} \\ \vdots & & \\ \varphi_{m1}+\psi_{m1} & \cdots & \varphi_{mn}+\psi_{mn} \end{pmatrix}.$$

Als $\varphi\colon L^n \to L^m$ en $\psi\colon L^m \to L^k$, dan is $\psi \circ \varphi(e_i) = \psi\varphi(e_i) =$

$$= \begin{pmatrix} \psi_{11} & \cdots & \psi_{1m} \\ \vdots & & \\ \psi_{k1} & \cdots & \psi_{km} \end{pmatrix} \begin{pmatrix} \varphi_{1i} \\ \vdots \\ \varphi_{mi} \end{pmatrix} = \begin{pmatrix} \psi_{11}\varphi_{1i}+\cdots+\psi_{1m}\varphi_{mi} \\ \vdots \\ \psi_{k1}\varphi_{1i}+\cdots+\psi_{km}\varphi_{mi} \end{pmatrix}.$$

Dus $\psi \circ \varphi = \sigma$ met $\sigma_{rs} = \sum_{i=1}^{m} \psi_{ri}\varphi_{is}$, $r = 1,\ldots,k$, $s = 1,\ldots,n$.

Daar voor homomorfismen de associatieve wet van de vermenigvuldiging geldt, geldt deze ook voor matrices $\varphi(\psi\sigma) = (\varphi\psi)\sigma$.

Is $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ een willekeurige vector uit L^n, dan kunnen wij x opvatten als een $n \times 1$-matrix en dus als een homomorfisme van $L^1 = L$ in L^n.

De vergelijking $\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \varphi_{11}x_1+\cdots+\varphi_{1n}x_n \\ \vdots \\ \varphi_{m1}x_1+\cdots+\varphi_{mn}x_n \end{pmatrix}$ is

dan op te vatten als het product van de homomorfismen:

$$\varphi\colon L^n \to L^m \text{ en } x\colon L^1 \to L^n.$$

Definitie 2. Zij $\varphi = (\varphi_{ij})$, $i = 1,\ldots,m$, $j = 1,\ldots,n$ een willekeurige $m \times n$-matrix. Onder de getransponeerde of gespiegelde matrix φ^t verstaan wij de $n \times m$-matrix met elementen

$$(\varphi^t)_{ij} = \varphi_{ji}.$$

Stelling 2. Als φ een $m \times n$-matrix is en ψ een $n \times k$-matrix, dan geldt

$$(\varphi.\psi)^t = \psi^t \,.\, \varphi^t.$$

Bewijs. $\varphi\psi$ is een $m \times k$-matrix met als elementen $(\varphi\psi)_{rs} = \sum_{i=1}^{n} \varphi_{ri}\varphi_{is}$, $r = 1,\ldots,m$, $s = 1,\ldots,k$.

Dus $(\varphi\psi)^t$ heeft als elementen $(\varphi\psi^t)_{rs} = (\varphi\psi)_{sr} = \sum_{i=1}^{n} \varphi_{si}\psi_{ir} =$

$= \sum_{i=1}^{n} (\varphi^t)_{is}(\psi^t)_{ri} = \sum_{i=1}^{n} (\psi^t)_{ri}(\varphi^t)_{is}$, $r = 1,\ldots,k$, $s = 1,\ldots,m$.

Dus $(\varphi\psi)^t = \psi^t \cdot \varphi^t$.

Definitie 3. Onder de rang van een $m \times n$-matrix φ verstaan wij de rang van het homomorfisme φ voorgesteld door de matrix.

Stel $\varphi = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix}$, dan is φ een homomorfisme van L^n in L^m en $\varphi(L^n)$ wordt opgespannen door de kolom vectoren $\begin{pmatrix} \varphi_{11} \\ \vdots \\ \varphi_{m1} \end{pmatrix}$, ..., $\begin{pmatrix} \varphi_{1n} \\ \vdots \\ \varphi_{mn} \end{pmatrix}$.

De dimensie van φ en dan ook de rang van de matrix φ, is dus gelijk aan het maximum aantal lineair onafhankelijke kolom vectoren.

Stelling 3. De rang van een matrix is gelijk aan de rang van de getransponeerde matrix.
Anders gezegd: Een matrix heeft evenveel lineair onafhankelijke rijen als kolommen.

Bewijs. Stel dat de rang van φ: $L^n \to L^m$ gelijk is aan r en die van φ^t gelijk aan s.
Kies nu in L^n een basis b_1, ..., b_n zó dat $\varphi(b_i) = 0$, $i > r$ en stel $\varphi(b_i) = c_i$, $i = 1,\ldots,r$.
Daar $\varphi(L^n)$ r-dimensionaal is en opgespannen wordt door de vectoren c_1, ..., c_r zijn deze lineair onafhankelijk.
Wij kunnen het stelsel $\{c_i\}_{i=1}^{r}$ dus aanvullen tot een basis c_1, ..., c_m van L^m.
Laat nu ψ: $L^m \to L^m$ zo gedefiniëerd zijn dat $\psi(c_i) = e_i$, $i = 1,\ldots,m$ en stel σ: $L^n \to L^n$ zó dat $\sigma(e_i) = b_i$.

Dan is $\psi.\varphi.\sigma = \psi.\varphi \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & & b_{nn} \end{pmatrix} = \psi \begin{pmatrix} c_{11} & \cdots & c_{1r} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{m1} & & c_{mr} & 0 & & 0 \end{pmatrix} =$

$$\begin{matrix} & \overbrace{}^{r} & \\ r\Big\{ & \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & & \vdots & \vdots & & \\ 0 & 0 & \ldots & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & & \vdots & \vdots & & \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix} \end{matrix} .$$

Het aantal lineair onafhankelijke rijen van de matrix $\psi\varphi\sigma$ is dus gelijk aan het aantal lineair onafhankelijke kolommen.
Dus rang $\psi\varphi\sigma$ = rang $(\psi\varphi\sigma)^t$ = r.
Hieruit volgt met §4 stelling 6:
s = rang $\varphi^t \leq$ rang $\sigma^t\varphi^t\psi^t$ = rang $(\psi\varphi\sigma)^t$ = r.
Dus rang $\varphi^t \leq$ rang φ.
Evenzo geldt rang $(\varphi^t)^t$ = rang $\varphi \leq$ rang φ^t dus rang φ = rang φ^t.

Opmerking 3.
Als φ een endomorfisme is van L^n in L^n, dan wordt φ voorgesteld door een n × n-matrix, die wij een vierkante matrix noemen. Het endomorfisme φ is dan en slechts dan een automorfisme als $\varphi^{-1}(0) = \{0\}$, dus als de rang van φ gelijk is aan n.
Zij nu ε de identieke afbeelding van L^n in L^n.
Dan wordt ε voorgesteld door de matrix

$$\varepsilon = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \quad \text{, de eenheidsmatrix.}$$

Voor de omkeerafbeelding φ^{-1} van het automorfisme φ geldt dus $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = \varepsilon$.

Definitie 4. Een matrix φ heet inverteerbaar als er een matrix φ^{-1} bestaat met $\varphi.\varphi^{-1} = \varphi^{-1}.\varphi = \varepsilon . \varphi^{-1}$ heet de inverse van φ.

Men bewijst nu gemakkelijk de volgende stelling:

Stelling 4. Een m x n-matrix φ is dan en slechts dan inverteerbaar als de rang φ = n. Tevens is de matrix φ^{-1} eenduidig bepaald.

§6. Stelsels lineaire vergelijkingen

Zij L een willekeurig lichaam.

Het stelsel
$$\begin{cases} \alpha_{11}x_1 + \ldots + \alpha_{1m}x_m = 0 \\ \vdots \\ \alpha_{n1}x_1 + \ldots + \alpha_{nm}x_m = 0 \end{cases} \qquad (*)$$

met bekende getallen $\alpha_{ij} \in L$ en onbekenden $x_1, \ldots, x_m$ heet een stelsel van n homogene lineaire vergelijkingen in m onbekenden.
Een stelsel $x_1, \ldots, x_m$ van elementen uit L, dat aan de vergelijkingen (*) voldoet, heet een oplossing van het stelsel (*).
Als alle elementen $x_1, \ldots, x_m$ gelijk zijn aan 0, heet de oplossing triviaal, anders niet-triviaal.

Stelling 1. Een stelsel van n homogene lineaire vergelijkingen in m onbekenden heeft altijd een niet-triviale oplossing als n < m.

Bewijs. Stel φ: $L^m \to L^n$ het homomorfisme voorgesteld door de matrix

$$\varphi = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & & \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix} \qquad \text{en } x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} .$$

Het stelsel vergelijkingen (*) kunnen wij dan samenvatten in de ene vergelijking $\varphi(x) = 0$, met onbekende vector x.
Een stelsel $x_1, \ldots, x_m$ van elementen uit L is dus een oplossing van (*) als de vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ bevat is in $\varphi^{-1}(0)$, de kern van φ en omgekeerd.

Zij nu r de rang van φ, dan is $r \leq m$ en daar $\varphi(L^m) \subset L^n$ ook $r \leq n$. $\varphi^{-1}(0)$ bevat dan en slechts dan een vector $\neq 0$ als de dim $\varphi^{-1}(0) = m - r$ groter is dan 0.
Is $m > n$, dan ook $m > n \geq r$, dus $m - r > 0$ en $\varphi^{-1}(0) \neq \{0\}$.

Opmerking 1.
De oplossingen van het stelsel (*) vormen dus een m-r dimensionale deelruimte van L^m.
Is $r = m$, dan is er precies één oplossing, de triviale.

Zij nu gegeven het stelsel
$$\begin{cases} \alpha_{11}x_1 + \ldots \alpha_{1m}x_m = \beta_1 \\ \vdots \\ \alpha_{m1}x_1 + \ldots \alpha_{nm}x_m = \beta_n \end{cases} \qquad (**)$$
met bekende getallen $\alpha_{ij}, \beta_i \in L$, $i = 1,\ldots,n$, $j = 1,\ldots,m$ en onbekenden $x_1, \ldots, x_m$.
Een dergelijk stelsel noemt men een stelsel van n niet-homogene lineaire vergelijkingen in m onbekenden.
Evenals in het homogene geval kunnen wij (**) samenvatten in de ene vergelijking

$$\varphi(x) = b \text{ , waarbij } b = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} \in L^n$$

en $\varphi = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & & \alpha_{nm} \end{pmatrix}$.

Onder de aangevulde matrix φ' van (**) verstaan we de matrix

$$\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m}\beta_1 \\ \vdots & & \\ \alpha_{n1} & \cdots & \alpha_{nm}\beta_n \end{pmatrix} .$$

Stelling 2. Het stelsel (**) van n niet-homogene lineaire vergelijkingen heeft dan en slechts dan een oplossing als de rang van de matrix φ gelijk is aan de rang van de aangevulde matrix φ'.

Bewijs. Het is duidelijk dat (**) een oplossing heeft als de vector

$b = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$ bevat is in $\varphi(L^m)$.

Nu wordt $\varphi(L^m)$ opgespannen door de vectoren $a_1 = \begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{n1} \end{pmatrix}$, ...,

$a_m = \begin{pmatrix} \alpha_{1m} \\ \vdots \\ \alpha_{nm} \end{pmatrix}$.

Dus daar $b \in \varphi(L^m) = H(\{a_1,\ldots,a_n\})$ geldt $\varphi(L^m) = H(\{a_1,\ldots,a_n,b\})$.
Het aantal lineair onafhankelijke vectoren uit $\{a_1,\ldots,a_n\}$ is dus gelijk aan het aantal lineair onafhankelijke vectoren uit
$\{b,a_1,\ldots,a_n\} \Rightarrow$ rang φ = rang φ'.
Stel nu dat het stelsel (**) geen oplossing heeft, dan is b niet bevat in $\varphi(L^m)$, d.w.z.
$b \notin H\{a_1,\ldots,a_n\} \Rightarrow H\{a_1,\ldots,a_n,b\} \neq H\{a_1,\ldots,a_n\} = \varphi(L^m)$.
Daar $H(\{a_1,\ldots,a_n\})$ een echte deelruimte is van $H(\{a_1,\ldots,a_n,b\})$
is dus dim $H(\{a_1,\ldots,a_n\}) <$ dim $H(\{a_1,\ldots,a_n,b\}) \Rightarrow$ rang $\varphi <$ rang φ'.

Opmerking 2.

Is $x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ een oplossing van het stelsel (**), dus $\varphi(x) = b$ en y

een oplossing van het homogene stelsel, $\varphi(y) = 0$, dan is ook x+y een oplossing van (**).
Immers $\varphi(x + y) = \varphi(x) + \varphi(y) = b + 0 = b$.
Is omgekeerd x' een oplossing van (**), dan is x' - x een oplossing van het homogene stelsel.
De oplossingen van (**) worden dus gegeven door $x + \varphi^{-1}(0)$, waarbij x een willekeurige oplossing is.

Stelling 3. Een stelsel van n niet-homogene lineaire vergelijkingen in n onbekenden heeft dan en slechts dan precies één oplossing als de rang van de matrix φ gelijk is aan n.

Bewijs. Daar n = rang $\varphi \leq$ rang $\varphi' \leq$ n, geldt dat rang φ = rang φ' en volgens stelling 2 is er dus minstens één oplossing.
Uit opmerking 1 volgt tevens dat het homogene stelsel slechts de triviale oplossing heeft, dus $\varphi^{-1}(0) = 0$.
Het niet-homogene stelsel heeft dan ook maar 1 oplossing.
Heeft omgekeerd het niet-homogene stelsel slechts één oplossing dan heeft ook het homogene stelsel slechts één oplossing en is dus de rang φ = n.

GALOIS THEORIE

§6.0 Inleiding

Het doel van de Galois theorie is, de oplossingen (wortels) te bestuderen van hogeremachtsvergelijkingen

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

waarbij de coëfficiënten a_i tot een gegeven lichaam k behoren. Men wenst, indien mogelijk, de oplossingen met behulp van radicalen (wortelvormen) expliciet in de coëfficiënten uit te drukken. Dat dit in het algemeen niet mogelijk is zodra de graad $n \geqslant 5$ is, werd voor het eerst door Abel aangetoond.
In de Galois theorie wordt de klassieke, meer analytische werkwijze vervangen door zuiver algebraïsche methoden, zoals

1. Lineaire algebra (vector analyse),
2. Lichaamstheorie,
3. Groepentheorie (voor zover het eindige permutatiegroepen betreft).

§6.1 Lichaamstheorie

Alle te beschouwen lichamen zullen deellichamen zijn van C (= het lichaam der complexe getallen); van deze lichamen is Q het kleinste (ga dit na) en C het grootste. Naast Q en C bestaan er talloze andere lichamen, zoals (ga dit na): R (= het lichaam der reële getallen), $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a,b \in Q\}$, $Q(i) = \{a + bi \mid a,b \in Q\}$, $Q(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in Q\}$.

Definitie 1. Zij A een willekeurige deelverzameling van C en zij k een lichaam.
Onder k(A) verstaan we dan het kleinste lichaam dat zowel A als k omvat; dit lichaam bestaat en is gelijk aan de doorsnede van alle lichamen die zowel A als k omvatten (ga dit na).

Het lichaam k(A) kunnen we expliciet aangeven; men gaat gemakkelijk na dat

$$k(A) = \left\{ \frac{p(a_1,\ldots,a_m)}{q(b_1,\ldots,b_n)} \;\middle|\; a_i, b_j \in A \right\}$$

waarbij $p(x_1, \ldots, x_m)$ en $q(x_1, \ldots, x_n)$ polynomen zijn met coëfficiënten uit k, terwijl $q(b_1, \ldots, b_n) \neq 0$.

Meestal zullen wij slechts A's beschouwen met eindig veel elementen; heel vaak zal A zelfs uit slechts één element bestaan.
In het geval $A = \{\alpha\}$ kunnen we dan schrijven

$$k(A) = k(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} \right\}$$

waarbij p(x) en q(x) polynomen zijn met coëfficiënten uit k, terwijl $q(\alpha) \neq 0$.
We noemen $k(\alpha)$ een enkelvoudige lichaamsuitbreiding van k, met behulp van het element α; we zeggen ook wel dat $k(\alpha)$ uit k ontstaat door adjunctie van α.

Definitie 2. Zij k een gegeven lichaam; het complexe getal α heet algebraïsch over k als het nulpunt is van een polynoom $f(x) \in k[x]$ (= de verzameling van alle polynomen met coëfficiënten uit k), $f(x) \not\equiv 0$; is α niet algebraïsch over k, dan heet α transcendent over k.

Definitie 3. Is α algebraïsch (transcendent) over k, dan heet $k(\alpha)$ een enkelvoudige algebraïsche (transcendente) uitbreiding van k.

Zij k_1 een deellichaam van k_2; voornamelijk wegens

$$x, y \in k_2 \Rightarrow x - y \in k_2$$

en

$$\left.\begin{array}{l} a \in k_1 \\ x \in k_2 \end{array}\right\} \Rightarrow a.x \in k_2$$

kan k_2 worden opgevat als een lineaire ruimte over k_1 (ga dit na).

Er zijn nu twee mogelijkheden:

1. k_2 is eindig dimensionaal over k_1; in dit geval heet k_2 een eindige uitbreiding van k_1, en de dimensie van k_2 over k_1 wordt aangegeven met $[k_2 : k_1]$.

2. k_2 is niet eindig dimensionaal over k_1.

Stelling 1. Is k_2 een eindige uitbreiding van k_1, dan is elk element $\alpha \in k_2$ algebraïsch over k_1.

Bewijs: Zij m de dimensie van k_2 over k_1; dan zijn de elementen $1, \alpha, \alpha^2, \ldots, \alpha^m$ zeker lineair afhankelijk. Er bestaan dus in k_1 elementen $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_m$ (niet alle gelijk aan 0) zodanig dat

$$\lambda_0 + \lambda_1\alpha + \ldots + \lambda_m\alpha^m = 0,$$

waaruit volgt dat α algebraïsch is over k_1.

Zijn f(x) en g(x) polynomen uit $k[x]$, $g(x) \not\equiv 0$, dan kunnen we, zoals bekend, schrijven

$$f(x) = g(x) \cdot q_1(x) + r_1(x),$$

waarbij de polynomen $q_1(x)$, $r_1(x) \in k[x]$ eenduidig bepaald zijn door de eis dat òf $r_1(x) \equiv 0$ of $r_1(x)$ een lagere graad heeft dan g(x). Zetten we deze "deling met rest" als volgt voort

$$f(x) = g(x) \cdot q_1(x) + r_1(x)$$

$$g(x) = r_1(x)q_2(x) + r_2(x)$$

$$r_1(x) = r_2(x)q_3(x) + r_3(x)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-3}(x) = r_{n-2}(x)q_{n-1}(x) + r_{n-1}(x)$$

$$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x)$$

$$r_{n-1}(x) = r_n(x) \cdot q_{n+1}(x) + r_{n+1}(x) \quad (= r_n(x) \cdot q_{n+1}(x))$$

dan verkrijgen we een rij resten

$$r_1(x),\ r_2(x),\ \ldots\ (r_i(x) \in k[x])$$

met dalende graad, zodat na een eindig aantal stappen een rest $r_{n+1}(x)$ overblijft die gelijk is aan het nulpolynoom.

Stelling 2. $r_n(x)$ is een grootste gemene deler (g.g.d.) van $f(x)$ en $g(x)$; $r_n(x)$ is te schrijven als

$$r_n(x) = a(x)\ f(x) + b(x)\ g(x)$$

met $a(x), b(x) \in k[x]$.

Bewijs: $r_n(x)$ is een deler van $r_{n-1}(x)$, zodat wegens

$$r_{n-2}(x) = r_{n-1}(x)\ q_n(x) + r_n(x)$$

$r_n(x)$ een deler is van $r_{n-2}(x)$, enz., enz. $r_n(x)$ is dus een gemeenschappelijke deler van $f(x)$ en $g(x)$. Deze werkwijze leidt tevens tot het inzicht dat $r_n(x)$ te schrijven is als

$$r_n(x) = a(x)\ f(x) + b(x)\ g(x)\ \ (a(x), b(x) \in k[x])$$

waaruit dan bovendien volgt dat elke gemeenschappelijke deler van $f(x)$ en $g(x)$ een deler is van $r_n(x)$. Dus: $r_n(x)$ is <u>een</u> g.g.d. van $f(x)$ en $g(x)$. (Welk verband bestaat er tussen alle g.g.d.'s van $f(x)$ en $g(x)$?). De g.g.d. waarvan de z.g. kopcoëfficiënt gelijk is aan 1, heet <u>de</u> g.g.d. van $f(x)$ en $g(x)$.

Bij elke g.g.d. $d(x)$ van $f(x)$ en $g(x)$ zijn dus polynomen $a(x)$ en $b(x)$ uit $k[x]$ te vinden zodanig dat

$$d(x) = a(x)\ f(x) + b(x)\ g(x).$$

Stel α is algebraïsch over k; dan is er een polynoom $p(x) \in k[x]$ $(p(x) \not\equiv 0)$ zodanig dat $p(\alpha) = 0$, terwijl $p(x)$ van alle polynomen uit $k[x]$ met α als nulpunt de laagste graad heeft; $p(x)$ heet <u>een</u> minimaalpolynoom van α over k; is bovendien de kopcoëfficiënt van $p(x)$ gelijk aan 1 dan spreken we van <u>het</u> minimaalpolynoom van α over k.

Stelling 3. $p(x)$ is irreducibel, d.w.z. $p(x)$ is niet te schrijven als $p(x) = p_1(x)\ p_2(x)$, waarbij $p_1(x)$ en $p_2(x) \in k[x]$ polynomen zijn van lagere graad dan $p(x)$.

Het bewijs wordt aan de lezer overgelaten.

Stelling 4. Is α tevens nulpunt van het polynoom $f(x) \in k[x]$ dan is $f(x)$ deelbaar door $p(x)$.

Bewijs: $$f(x) = p(x)\ q(x) + r(x)$$

waarbij $r(x)$ een lagere graad heeft dan $p(x)$ (is $r(x) \equiv 0$ dan is reeds aan de stelling voldaan).
Substitutie van α levert $r(\alpha) = 0$, waaruit in verband met de definitie van $p(x)$ volgt $r(x) \equiv 0$.

Stelling 5. Zij α algebraïsch over k en zij $p(x)$ een minimaal polynoom van α; heeft $p(x)$ de graad m ($\geqslant 1$) dan is

$$1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$$

een basis van $k(\alpha)$ over k.

Bewijs: Uit de definitie van $p(x)$ volgt direct, dat deze elementen lineair onafhankelijk zijn. Rest ons nog aan te tonen dat elk element van $k(\alpha)$ te schrijven is als lineaire combinatie van

$$1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$$

(met coëfficiënten uit k).
Alle elementen van $k(\alpha)$ zijn te schrijven als $\frac{f(\alpha)}{g(\alpha)}$ waarbij $f(x)$ en $g(x)$ polynomen zijn uit $k[x]$ terwijl $g(\alpha) \neq 0$.
We tonen aan dat $\frac{1}{g(\alpha)}$ ook te schrijven is als $a(\alpha)$, waarbij $a(x) \in k[x]$.
$g(x)$ en $p(x)$ zijn onderling ondeelbare polynomen, zodat er volgens stelling 2 twee polynomen $a(x)$ en $b(x)$ te vinden zijn die voldoen aan

$$1 = a(x)\ g(x) + b(x)\ p(x)$$

Dus: $1 = a(\alpha)g(\alpha) + b(\alpha)p(\alpha) = a(\alpha)g(\alpha) \quad (p(\alpha) = 0)$,

met als gevolg $\frac{1}{g(\alpha)} = a(\alpha)$.

Dus: $\frac{f(\alpha)}{g(\alpha)} = a(\alpha)\ f(\alpha)$.

Nu is a(x)f(x) te schrijven als:

$$a(x)f(x) = q(x)p(x) + r(x)$$

waarbij de graad van r(x) hoogstens gelijk is aan m-1.
Dus $a(\alpha)f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$, waaruit volgt

$$\frac{f(\alpha)}{g(\alpha)} = r(\alpha) = r_0 + r_1\alpha + r_2\alpha^2 + \ldots + r_{m-1}\alpha^{m-1}$$

met $r_i \in k$.
Hieruit volgt dat $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ een basis is voor $k(\alpha)$.

Gevolg: Het lichaam $k(\alpha)$ is dan en slechts dan eindig dimensionaal over k als α algebraïsch is over k. De dimensie van $k(\alpha)$ over k is gelijk aan de graad van het minimaal polynoom van α.
Het lichaam $k(\alpha)$ is dus dan en slechts dan oneindig dimensionaal over k, als α transcendent is over k.

We kunnen ook zeggen dat de begrippen: Enkelvoudige eindige uitbreiding, en: Enkelvoudige algebraïsche uitbreiding, equivalent zijn.

In de verzamelingenleer wordt op eenvoudige wijze aangetoond dat er vele complexe getallen α bestaan, die niet algebraïsch zijn over Q en dus aanleiding geven tot een transcendente uitbreiding $Q(\alpha)$.
Voorbeelden hiervan zijn π en e.

Stelling 6. Is $k_1 \subset k_2 \subset k_3$ terwijl $[k_3 : k_1]$ eindig is, dan is
$$[k_3 : k_2] \cdot [k_2 : k_1] = [k_3 : k_1].$$

Bewijs: Zij $\alpha_1, \alpha_2, \ldots, \alpha_k$ een basis voor k_2 over k_1 en
$\beta_1, \beta_2, \ldots, \beta_h$ een basis voor k_3 over k_2.

We tonen aan dat de elementen $\alpha_i\beta_j \in k_3$ (i = 1, 2, ..., k; j = 1, 2, ..., h) een basis vormen voor k_3 over k_1.
Zij $x \in k_3$, dan is x te schrijven als:

$$x = \sum_{j=1}^{h} \lambda_j \beta_j \quad (\lambda_j \in k_2).$$

Alle coëfficiënten λ_j zijn op hun beurt te schrijven als

$$\lambda_j = \sum_{i=1}^{k} \mu_{ij} \alpha_i \quad (\mu_{ij} \in k_1).$$

Dus: $x = \sum_{j=1}^{h} \sum_{i=1}^{k} \mu_{ij}\alpha_i\beta_j$ zodat het stelsel $\{\alpha_i\beta_j\}$ een stelsel voortbrengenden is.
Nu moet nog bewezen worden dat $\{\alpha_i\beta_j\}$ lineair onafhankelijk is.
Stel $\sum_{i,j} V_{ij} \alpha_i \beta_j = 0. \quad (V_{ij} \in k_1).$

Hiervoor kunnen we schrijven:

$$\sum_{j=1}^{h} (\sum_{i=1}^{k} V_{ij} \alpha_i)\beta_j = 0.$$

Uit de onafhankelijkheid van het stelsel $\{\beta_j\}$ volgt nu

$$\sum_{i=1}^{k} V_{ij} \alpha_i = 0 \quad \text{voor } j = 1,2,\ldots,h$$

aaruit op grond van de onafhankelijkheid van het stelsel $\{\alpha_i\}$ volgt:

$$V_{ij} = 0.$$

Het stelsel $\{\alpha_i \beta_j\}$ is dus een lineair onafhankelijk stel voortbrengenden van k_3 en is dus een basis van k_3 over k_1. De dimensie van k_3 over k_1 is dus $k.h = [k_2 : k_1] \cdot [k_3 : k_2] = [k_3 : k_1]$, hetgeen te bewijzen was.

Vraagstukken

1. Bepaal de g.g.d. van de polynomen

$$f(x) = x^9 + 2x^8 + x^7 + 2x^6 + x^5 + 2x^4 + 5x^3 + 2$$

en $g(x) = x^6 + 2x^5 + 3x^4 + 6x^3 + x^2 + 3$

2. Bepaal de polynomen a(x) en b(x) zodanig dat

$$a(x).(x^2 + 1) + b(x).(x^3 + 1) = 1.$$

3. Bepaal de minimaal polynomen over Q van de volgende radicalen:

1. $\sqrt[5]{2 + \sqrt{7}}$
2. $i\sqrt{3} + \sqrt{5}$
3. $\sqrt{2} + \sqrt[3]{3}$
4. $\sqrt[3]{3} + \sqrt[3]{5}$

4. Bepaal de dimensie van de volgende lichamen over Q

1. $Q(7 - \sqrt{7} + i\sqrt[3]{7})$
2. $Q(1 + \sqrt{\frac{3}{2} + \sqrt{2}})$
3. $Q(\sqrt[3]{21 + 3\sqrt[3]{20} + 6\sqrt[3]{50}})$
4. $Q(A)$ waarbij $A = \{i, \sqrt{2}, \sqrt{3}\}$.

5. Bepaal de dimensie van k_2 over k_1, als

1. $k_2 = Q(i + \sqrt{2})$ en $k_1 = Q(\sqrt{2})$
2. $k_2 = Q(i + \sqrt{3} + \sqrt[3]{5})$ en $k_1 = Q(\sqrt{3})$
3. $k_2 = Q(\sqrt{6} + \sqrt{3}, \sqrt[3]{2} + \sqrt[3]{6}, \sqrt[6]{6})$ en
   $k_1 = Q(\sqrt{6} + \sqrt{3}, \sqrt[3]{2} + \sqrt[3]{6})$

6. Toon aan dat de volgende uitbreidingen van Q enkelvoudig algebraïsch zijn.

1. $Q(\sqrt{2}, \sqrt{3})$

2. $Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$

3. $Q(\sqrt{2}, \sqrt[3]{2})$

7. Groepen.

(Voor een nadere uitwerking van dit onderwerp verwijzen wij naar de syllabus "Groepentheorie en Lineaire Algebra", 1964-1965).

Definitie 1. Een niet lege verzameling G heet een groep als er in G een binaire operatie * is gedefiniëerd met de volgende eigenschappen:

1. $a,b \in G \Rightarrow a * b \in G$
2. $(a * b) * c = a * (b * c)$ (associatieve wet)
3. G bevat een element e (eenheidselement) met de eigenschap $a * e = e * a$ voor alle $a \in G$.
4. bij elke $a \in G$ bestaat een element $a^{-1} \in G$ zodanig dat $a * a^{-1} = a^{-1} * a = e$.

Definitie 2. Geldt in de groep (G,*) bovendien

$a * b = b * a$ (commutatieve wet)

voor alle $a,b \in G$, dan heet G een Abelse groep.

Definitie 3. De groep (G,*) heet cyclisch indien er in G een element a bestaat zodanig dat elk element $g \in G$ te schrijven is als

$g = a^n = a * a * \ldots * a$ $(n = 0,1,2,\ldots)$ $(a^0 = e)$

of als

$g = a^{-m} = (a^{-1})^m$ $(m = 1, 2, 3, \ldots)$.

Opgave: Ga na dat elke cyclische groep Abels is; laat aan de hand van een voorbeeld zien dat niet elke Abelse groep cyclisch is.

Definitie 4. De groep (G,*) heet eindig als G eindig veel elementen bevat. Onder de orde van G verstaan we het aantal elementen van G.

Voorbeelden:

1. De verzameling der gehele getallen Z met als operatie de gewone optelling, is een oneindige cyclische groep.
2. De verzameling $\{1, i, -1, -i\}$ met de bekende vermenigvuldiging als operatie, is een eindige cyclische groep van de orde 4.
3. De verzameling $\{e,a,b,c,d,f\}$ met als operatie *, gedefiniëerd in de volgende tabel, is een eindige niet-Abelse groep van de orde 6.

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

Definitie 5. Een niet lege deelverzameling H van de groep G heet een ondergroep van G als met $a,b \in H$ ook geldt $a * b^{-1} \in H$. (Verifiëer dat H weer een groep is.)

Voorbeeld 4. De groep der positieve rationale getallen (Q,.) is een ondergroep van de groep der positieve reële getallen (R,.).

Definitie 6. Een ondergroep H van de groep G heet een normaaldeler van G, als voor elk element $h \in H$ geldt

$$a * h * a^{-1} \in H \quad \text{voor alle } a \in G.$$

Opmerking. In een Abelse groep G is dus elke ondergroep H een normaaldeler van G.

Definitie 7. Zij H een ondergroep van de groep G; onder een linker-(resp. rechter) nevenklasse $a * H$ (resp. $H * a$) van H verstaan we de verzameling van alle elementen $a * h$ (resp. $h * a$), waarbij $a \in G$ vast gekozen is en h geheel H doorloopt.

Stelling 1. Is H een normaaldeler van de groep G dan is elke linker-nevenklasse tevens rechter-nevenklasse:

$$a * H = H * a.$$

Bewijs: $h_1 \in H \Rightarrow a * h_1 * a^{-1} = h_2 \in H \Rightarrow$

$a * h_1 = h_2 * a \in H * a \Rightarrow a * H \subset H * a.$

Evenzo: $H * a \subset a * H.$

Stelling 2. Is H een ondergroep van G dan zijn twee linker-(resp. rechter-) nevenklassen òf disjunct òf ze vallen samen.

Bewijs: Stel $c \in a * H$ en $c \in b * H \Rightarrow c = a * h_1 = b * h_2$

$b = a * h_1 * h_2^{-1} \Rightarrow b * H \subset a * H.$

Evenzo: $a * H \subset b * H.$

Dus: $a * H = b * H.$

Definitie 8. Zij H een normaaldeler van de groep G; de verzameling van alle verschillende nevenklassen van H kunnen we tot een groep maken, door te definiëren

$$(a * H) \circ (b * H) = (a * b) * H.$$

In deze groep is H het eenheidselement en de inverse van $a * H$ is $a^{-1} * H$. Deze groep wordt aangeduid met

$$G/H$$

en wordt de factorgroep van G over H genoemd.

Definitie 9. De afbeelding φ: $(G_1,*) \to (G_2,o)$ heet een homomorfisme indien voor alle $a,b \in G$ geldt

$$\varphi(a * b) = \varphi(a) \circ \varphi(b).$$

Is deze afbeelding bovendien 1-1 duidig, dan heet φ een isomorfisme.

Is daarbij ook nog $(G_1,*) = (G_2,o)$ dan heet φ een automorfisme.

Stelling 3. Is φ: $(G_1,*) \to (G_2,o)$ een homomorfisme, dan geldt (als e_i het eenheids-element in G_i is $(i = 1, 2)$)

1. $\varphi(e_1) = e_2$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$

Bewijs: 1. Voor elke $g \in G_1$ geldt

$$\varphi(g) = \varphi(g * e_1) = \varphi(g) \circ \varphi(e_1)$$

met als gevolg $\varphi(e_1) = e_2$.

2. $a \in G \Rightarrow e_2 = \varphi(e_1) = \varphi(a * a^{-1}) =$

$$\varphi(a) \circ \varphi(a^{-1}) \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}.$$

Opgave: De afbeelding φ: $G \to G/H$ met $\varphi(a) = a * H$ is een homomorfisme als H een normaaldeler is van G.

Definitie 10. Onder de kern K van een homomorfisme φ: $(G_1,*) \to (G_2,o)$ verstaan we de verzameling van alle elementen $g \in G_1$ die door φ op e_2 worden afgebeeld:

$$K = \{g \mid g \in G_1, \varphi(g) = e_2\}.$$

Stelling 4. De kern K van een homomorfisme φ is een ondergroep van G.

Bewijs: $g \in K \Rightarrow \varphi(g) = e_2 \Rightarrow \varphi(g^{-1}) = e_2^{-1} = e_2$.

Dus $a,b \in K \Rightarrow \varphi(a * b^{-1}) = \varphi(a) \circ \varphi(b^{-1}) =$

$$= e_2 \circ e_2 = e_2 \Rightarrow a * b^{-1} \in K.$$

Stelling 5. Is φ een homomorfisme van $G_1 \to G_2$ (G_1, G_2 groepen) dan is de kern K van φ een normaaldeler van G_1.

Bewijs: $k \in K \Rightarrow \varphi(a * k * a^{-1}) = \varphi(a) * \varphi(k) * \varphi(a^{-1}) =$

$= \varphi(a) * \varphi(a^{-1}) = \varphi(e_1) = e_2 \Rightarrow a * k * a^{-1} \in K.$

Permutatiegroepen

Zij X een verzameling en P(X) de verzameling van alle 1-1 duidige afbeeldingen (permutaties) van X op zichzelf, dan kunnen we P(X) tot een groep maken door de compositie g_1 o g_2 van twee permutaties $g_1, g_2 \in P(X)$ als volgt te definiëren

$$(g_1 \text{ o } g_2)(x) = g_1(g_2(x)) \quad \text{voor alle } x \in X.$$

(Ga dit na; welke permutatie is het eenheidselement?)

Voorbeeld 5. Zij $X = \{1,2,3\}$, dan bestaat P(X) uit de volgende elementen (permutaties)

$$e = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

(de "groepsvermenigvuldiging" is expliciet aangegeven in voorbeeld 3).

Voorbeeld 6. De permutatiegroep van $X = \{1,2,3,4\}$ bevat de volgende permutatiegroep

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

als Abelse, niet cyclische ondergroep.

Deze groep heet de Viergroep van Klein. De groepstabel heeft de volgende gedaante

o	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Definitie 11. Onder een automorfisme van een lichaam k verstaan we een 1-1 duidige afbeelding φ van k op zichzelf, zodanig dat voor alle $a,b \in k$ geldt:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(a.b) = \varphi(a) \,.\, \varphi(b)$$

Opgave: Bewijs dat $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(-a) = -\varphi(a)$ en $a \neq 0 \Rightarrow$
$\Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}$.

Voorbeeld 7. De afbeelding φ met $\varphi(a+b\sqrt{2}) = a-b\sqrt{2}$ $(a,b \in Q)$ is een automorfisme van $Q(\sqrt{2})$.

Opgave: Bepaal alle automorfismen van de lichamen Q, $Q(i\sqrt{2})$, $Q(\sqrt[3]{2})$, $Q(i, \sqrt{2})$.

Toon aan, dat voor elk automorfisme φ van k geldt:

$\varphi(r) = r$ als $r \in Q$.

Stelling 6a. De automorfismen van een lichaam k vormen een groep G(k); deze automorfismengroep is een ondergroep van de permutatiegroep P(k).

Het bewijs wordt aan de lezer overgelaten.

Definitie 12. Is $k_1 \supset k$, dan heet elk automorfisme van k_1 dat alle elementen van k invariant laat, een k-automorfisme van k_1.

Stelling 6b. Alle k-automorfismen van k_1 vormen een groep $G(k_1/k)$. Deze groep heet de Galoisgroep van k_1 over k.

Het bewijs wordt aan de lezer overgelaten.

Opgave: Bepaal de Galoisgroep van

1. $Q(i, \sqrt{2})$ over $Q(i)$
2. C over R.

Stelling 7. Zij H een collectie automorfismen van K.

Dan is:

$$K_H \overset{\text{def}}{=} \left\{ x \;\middle|\; x \in K, \sigma(x) = \tau(x) \text{ voor alle } \sigma, \tau \in H \right\}$$

een lichaam.

K_H heet het invariante lichaam van K onder H; elk element $x \in K_H$ heet een invariant van K onder H.

Opmerking: Bevat H de identieke afbeelding dan geldt voor elke invariant $x \in K_H$ van K onder H: $\sigma(x) = x$ voor elke $\sigma \in H$.

Bewijs: Het is duidelijk dat $0 \in K_H$ en $1 \in K_H$.

Zij $x_1, x_2 \in K_H$ en $\sigma, \tau \in H$; dan is

$$\sigma(x_1+x_2) = \sigma(x_1) + \sigma(x_2) = \tau(x_1) + \tau(x_2) = \tau(x_1+x_2) \quad \text{en}$$

$$\sigma(x_1 . x_2) = \sigma(x_1) . \sigma(x_2) = \tau(x_1) . \tau(x_2) = \tau(x_1 . x_2).$$

Voor elke $x \in K_H$ geldt:

$$\sigma(-x) = -\sigma(x) = -\tau(x) = \tau(-x);$$

is $x \neq 0$ dan is

$$\sigma(x^{-1}) = \frac{1}{\sigma(x)} = \frac{1}{\tau(x)} = \tau(x^{-1}).$$

Stelling 8. In de lineaire ruimte Hom (K,K) over K (vergelijk §4, stelling 7) is elk stelsel H van automorfismen van K een lineair onafhankelijk stelsel.

Bewijs: Elk automorfisme σ van K is, als element van Hom (K,K), ongelijk aan het nulelement van Hom (K,K), zodat de stelling juist is voor n = 1.

Veronderstel nu dat de stelling juist is voor n = 1, 2, ..., r-1 ($r \geq 2$); zij nu $\sigma_1, \ldots, \sigma_r$ een r-tal (verschillende) automorfismen van K dat lineair afhankelijk is.

Dan bestaat er in K een r-tal scalairen $\alpha_1, \alpha_2, \ldots, \alpha_r$ zodanig dat

$$\alpha_1\sigma_1 + \alpha_2\sigma_2 + \ldots + \alpha_r\sigma_r = 0,$$

terwijl op grond van de inductieveronderstelling geen dezer α's gelijk is aan 0.

Dus:

$$\beta_1\sigma_1 + \beta_2\sigma_2 + \ldots + \beta_{r-1}\sigma_{r-1} + \sigma_r = 0, \beta_i = \alpha_r^{-1} \cdot \alpha_i \neq 0 \quad (1)$$

Nu is $\sigma_i \neq \sigma_j$ als $i \neq j$, zodat er een $a \in K$ ($a \neq 0$) bestaat met $\sigma_1(a) \neq \sigma_r(a)$.

Voor elke $x \in K$ is het beeld van $ax \in K$, onder het homomorfisme $\beta_1\sigma_1 + \ldots + \sigma_r$ ($= 0 \in \text{Hom } (K,K)$) gelijk aan 0, zodat

$$\beta_1\sigma_1(a)\sigma_1 + \beta_2\sigma_2(a)\sigma_2 + \ldots + \sigma_r(a)\sigma_r = 0;$$

hierin is wegens $a \neq 0$, $\sigma_r(a) \neq 0$, zodat we kunnen schrijven

$$\sigma_r^{-1}(a)\beta_1\sigma_1(a)\sigma_1 + \ldots + \sigma_r = 0. \quad (2)$$

Uit (1) en (2) volgt nu:

$$\{\beta_1 - \sigma_r^{-1}(a)\beta_1\sigma_1(a)\}\sigma_1 + \ldots + \{\beta_{r-1} - \sigma_r^{-1}(a)\beta_{r-1}\sigma_{r-1}(a)\}\sigma_{r-1} = 0 \quad (3)$$

waarbij de coëfficiënt van σ_1 ongelijk is aan 0; immers indien $\beta_1 - \sigma_r^{-1}(a)\beta_1\sigma_1(a) = 0$ zou zijn, dan zou wegens $\beta_1 \neq 0$ gelden

$\sigma_1(a) = \sigma_r(a)$, hetgeen in tegenspraak is met de keuze van a.
Uit (3) volgt nu dat de r-1 (verschillende) automorfismen $\sigma_1, \sigma_2, \ldots, \sigma_{r-1}$ lineair afhankelijk zijn, wat in strijd is met onze inductieveronderstelling.

Conclusie: het stelsel $\sigma_1, \sigma_2, \ldots, \sigma_r$ is lineair onafhankelijk. Elk eindig stelsel verschillende automorfismen van K is dus lineair onafhankelijk. Op grond van §3, stelling 1, Gevolg 1, kunnen we nu zeggen dat elk stelsel H bestaande uit automorfismen van K, lineair onafhankelijk is over K.

Stelling 9. Is H een stelsel automorfismen van K, bestaande uit de n (verschillende) elementen $\sigma_1, \ldots, \sigma_n$, dan geldt:

$$\left[K : K_H\right] \geqslant n.$$

Bewijs: Veronderstel dat $\left[K : K_H\right] = r < n$. We zullen aantonen dat deze veronderstelling tot een tegenspraak leidt. Uit $\left[K : K_H\right] = r$ volgt dat K eindig dimensionaal is over K_H; zij

$$\omega_1, \omega_2, \ldots, \omega_r \in K$$

een basis van K over K_H.
In het stelsel lineaire vergelijkingen

$$\left.\begin{aligned}
&\sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \ldots + \sigma_n(\omega_1)x_n = 0\\
&\sigma_1(\omega_2)x_1 + \sigma_2(\omega_2)x_2 + \ldots + \sigma_n(\omega_2)x_n = 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\sigma_1(\omega_r)x_1 + \sigma_2(\omega_r)x_2 + \ldots + \sigma_n(\omega_r)x_n = 0
\end{aligned}\right\} \qquad (1)$$

hebben we meer onbekenden dan vergelijkingen zodat er (zie §6, stelling 1) een niet triviale oplossing $x_1, x_2, \ldots, x_n \in K$ bestaat.

Elk element $a \in K$ is te schrijven als

$$a = \alpha_1\omega_1 + \alpha_2\omega_2 + \ldots + \alpha_r\omega_r,\ \alpha_i \in K_H.$$

Vermenigvuldigen we in (1) de i-de vergelijking met $\sigma_1(\alpha_i)$, dan verkrijgen we op grond van $\sigma_1(\alpha_i) = \sigma_j(\alpha_i)$ (immers $\alpha_i \in K_H$) en $\sigma_j(\alpha_i)\sigma_j(\omega_i) = \sigma_j(\alpha_i\omega_i)$:

$$\sigma_1(\alpha_1\omega_1)x_1 + \ldots + \sigma_n(\alpha_1\omega_1)x_n = 0$$

$$\sigma_1(\alpha_2\omega_2)x_1 + \ldots + \sigma_n(\alpha_2\omega_2)x_n = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_1(\alpha_r\omega_r)x_1 + \ldots + \sigma_n(\alpha_r\omega_r)x_n = 0$$

Door optelling volgt hieruit

$$\sigma_1(a)x_1 + \sigma_2(a)x_2 + \ldots + \sigma_n(a)x_n = 0,$$

want

$$\sigma_i(\alpha_1\omega_1) + \sigma_i(\alpha_2\omega_2) + \ldots + \sigma_i(\alpha_r\omega_r) =$$

$$= \sigma_i(\alpha_1\omega_1 + \ldots + \alpha_r\omega_r) = \sigma_i(a).$$

Aangezien $a \in K$ willekeurig gekozen was, geldt dus

$$x_1\sigma_1 + x_2\sigma_2 + \ldots + x_n\sigma_n = 0, \qquad x_i \in K$$

Hierin zijn niet alle x'en gelijk aan nul, zodat het stelsel $H = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ lineair afhankelijk is, hetgeen in tegenspraak is met stelling 8.

In de stellingen 7, 8 en 9 bestond H uit een <u>willekeurig stel</u> verschillende automorfismen van K; is H in het bijzonder een ondergroep van de Galoisgroep G (K/k) dan geldt de volgende stelling.

<u>Stelling 10</u>. Heeft de <u>ondergroep</u> H van G(K) de orde n dan geldt

$$\left[K : K_H\right] = n.$$

Bewijs: Laat H bestaan uit de elementen $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Omdat H een groep is, bevat H de identieke afbeelding I van K op K; neem b.v. $\sigma_1 = I$. Het invariantenlichaam K_H bestaat nu dus uit alle $x \in K$ waarvoor geldt

$$(x =)\sigma_1(x) = \sigma_2(x) = \ldots = \sigma_n(x);$$

elk k-automorfisme uit H laat dus elk element $x \in K_H$ <u>op zijn plaats</u>.

Veronderstellen we nu $\left[K : K_H\right] > n$; dan bestaan er n+1 elementen $a_1, a_2, \ldots, a_{n+1}$ in K die t.o.v. K_H lineair onafhankelijk zijn.

Het stelsel vergelijkingen

$$\left.\begin{aligned} x_1\sigma_1(a_1) + x_2\sigma_1(a_2) + \ldots + x_{n+1}\sigma_1(a_{n+1}) &= 0 \\ x_1\sigma_2(a_1) + x_2\sigma_2(a_2) + \ldots + x_{n+1}\sigma_2(a_{n+1}) &= 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ x_1\sigma_n(a_1) + x_2\sigma_n(a_2) + \ldots + x_{n+1}\sigma_n(a_{n+1}) &= 0 \end{aligned}\right\} \quad (0)$$

heeft, zoals bekend, binnen K een niet triviale oplossing $x_1, x_2, \ldots, x_{n+1}$.

Wegens $\sigma_1 = I$ is dan

$$x_1a_1 + x_2a_2 + \ldots + x_{n+1}a_{n+1} = 0 ,$$

zodat <u>niet alle</u> getallen x_i tot K_H kunnen behoren (immers de $a_i \in K$ zijn lineair onafhankelijk over K_H).

Van alle niet triviale oplossingen kiezen we er één met zo weinig mogelijk van 0 verschillende elementen:

$$\alpha_1, \alpha_2, \ldots, \alpha_r, 0, 0, \ldots, 0 \quad (\alpha_i \neq 0,\ i=1,2,\ldots,r).$$

Nu is $r \neq 1$, want $r = 1$ zou tot gevolg hebben

$$\alpha_1\sigma_1(a_1) = 0 \Rightarrow \sigma_1(a_1) = 0 \Rightarrow a_1 = 0$$

terwijl in feite $a_1 \neq 0$.

Zonder beperking der algemeenheid mogen we verder stellen $\alpha_r = 1$ (ga dit na), zodat

$$\alpha_1\sigma_i(a_1) + \alpha_2\sigma_i(a_2) + \ldots + \alpha_{r-1}\sigma_i(a_{r-1}) + \sigma_i(a_r) = 0 \quad (1)$$

voor $i = 1, 2, \ldots, n$; ook hier behoren $\alpha_1, \alpha_2, \ldots, \alpha_{r-1}$ niet allemaal tot K_H.

Zij $\alpha_1 \notin K_H$, dan is er een σ_k waarvoor

$$\sigma_k(\alpha_1) \neq \alpha_1.$$

Op grond van het feit dat H een groep is, geldt, dat

$$H = \left\{\sigma_k\sigma_1, \sigma_k\sigma_2, \ldots, \sigma_k\sigma_n\right\}.$$

Beschouw nu het beeld van de uitdrukkingen in (1) onder de afbeelding σ_k:

$$\sigma_k(\alpha_1).\sigma_k\sigma_j(a_1)+\sigma_k(\alpha_2).\sigma_k\sigma_j(a_2)+\ldots+\sigma_k(\alpha_{r-1}).\sigma_k\sigma_j(a_{r-1}) +$$

$$+ \sigma_k\sigma_j(a_r) = 0.$$

Voor zekere j is nu $\sigma_k\sigma_j = \sigma_i$, zodat

$$\sigma_k(\alpha_1)\sigma_i(a_1)+\sigma_k(\alpha_2)\sigma_i(a_2)+\ldots+\sigma_k(\alpha_{r-1})\sigma_i(a_{r-1})+\sigma_i(a_r)=0. \quad (2)$$

Uit (1) en (2) leidt men af

$$\left\{\alpha_1 - \sigma_k(\alpha_1)\right\}\sigma_i(a_1) + \ldots + \left\{\alpha_{r-1} - \sigma_k(\alpha_{r-1})\right\}\sigma_i(a_{r-1}) = 0$$

met $\alpha_1 - \sigma_k(\alpha_1) \neq 0$, met als gevolg dat het stelsel (0) een niet triviale oplossing heeft met minder dan r van nul verschillende elementen.

Dit is in tegenspraak met de keuze van r.

Conclusie: $\left[K : K_H\right] \leqq n$.

Met behulp van stelling 9 volgt nu direkt dat

$$\left[K : K_H\right] = n.$$

Stelling 11. Zij H een eindige ondergroep van de orde n van G(K) en zij σ een automorfisme van K, dat elk element van K_H op zichzelf afbeeldt; dan is $\sigma \in H$.

Bewijs. Stel $\sigma \notin H$; dan bestaat $H \cup \{\sigma\}$ uit n+1 verschillende automorfismen van K, zodat volgens stelling 9

(1) $[K : K_{H \cup \{\sigma\}}] \geqslant n+1$. Maar, volgens de definitie van σ is $K_{H \cup \{\sigma\}} = K_H$, zodat volgens stelling 10

(2) $[K : K_{H \cup \{\sigma\}}] = n$.

De veronderstelling $\sigma \notin H$ leidt dus tot een tegenspraak. Dus $\sigma \in H$.

Stelling 12. Zijn H_1 en H_2 eindige ondergroepen van G(K) met $K_{H_1} = K_{H_2}$ dan is $H_1 = H_2$.

Bewijs. Volgt onmiddellijk uit stelling 11.

Gevolg. Is H een eindige ondergroep van G(K) dan geldt $G(K/K_H) = H$.

Opgaven. 1) Bewijs dat $G(K) = G(K/Q)$.

2) $K_{G(K)} \supset Q$.

3) Geef een voorbeeld waarin $K_{G(K)} \neq Q$.

In het voorgaande is aangetoond, dat met elke ondergroep H van G(K) ondubbelzinnig een lichaam $K_H \subset K$ correspondeert, zodanig dat $G(K/K_H) = H$.

Omgekeerd kan men de vraag stellen, of ook elk deellichaam L van K ondubbelzinnig correspondeert met G(K/L) zodanig dat $K_{G(K/L)} = L$. Dat dit niet het geval is blijkt uit het volgende voorbeeld:

$$K = Q(\sqrt[3]{2}), \quad L = Q.$$

Men gaat gemakkelijk na, dat in dit geval G(K/L) slechts uit de identieke afbeelding bestaat; dit heeft tot gevolg dat

$$K_{G(K/L)} = K \neq L.$$

In de volgende paragraaf zullen we nagaan voor welke lichamen $L \subset K$ wel geldt

$$K_{G(K/L)} = L.$$

§8. Normale uitbreidingen, splijtlichamen

Definitie 1. Een eindige uitbreiding N van k heet een normale uitbreiding van k als elk irreducibel polynoom $p(x) \in k[x]$, dat een nulpunt in N heeft, binnen $N[x]$ volledig in lineaire factoren te ontbinden is (d.w.z. als $p(x) = 0$ in N een wortel heeft, dan liggen alle wortels van deze vergelijking in N).

Stelling 1. Is $k \subset L$ zodanig dat

$$L_{G(L/k)} = k,$$

dan is L een normale uitbreiding van k.

Bewijs. Stel L is niet normaal over k; dan is er in $k[x]$ een irreducibel polynoom $p(x)$ met $p(\vartheta) = 0$ voor zekere $\vartheta \in L$, terwijl $p(x)$ binnen $L[x]$ niet volledig in lineaire factoren ontbindbaar is.
Voor $p(x)$ kunnen we dus schrijven

$$p(x) = q(x).(x-\vartheta_1)(x-\vartheta_2) \ldots (x-\vartheta_r); \vartheta_1 = \vartheta \text{ en } \vartheta_i \in L,$$

waarbij $q(x) \in L[x]$ $(q(x) \notin k[x])$ (ga dit na) minstens de graad 2 heeft en de ϑ's alle in L gelegen wortels van $p(x) = 0$ zijn. Voor elke $\sigma \in G(L/k)$ geldt

$$\sigma(\vartheta_i) = \vartheta_j$$

met als gevolg dat $p(x) \in k[x]$ en $(x-\vartheta_1)(x-\vartheta_2) \ldots (x-\vartheta_r)$ invariant zijn onder σ, zodat ook $q(x)$ invariant is onder σ.
Daar $q(x) \notin k[x]$, bevat $q(x)$ een coëfficiënt $a_s \notin k$, die onder alle automorfismen $\sigma \in G(L/k)$ invariant blijft. Het invariantenlichaam $L_{G(L/k)}$ is dus echt groter dan k, wat in tegenspraak is met het gegeven.
Conclusie: L is een normaal over k.

Stelling 2. Zij N een normale uitbreiding van k en zij L een lichaam tussen k en N

$$k \subset L \subset N.$$

Dan is N ook een normale uitbreiding van L.

Bewijs. Zij $p(x)$ een irreducibel polynoom uit $L[x]$ en zij $p(\beta) = 0$ met $\beta \in N$. We moeten nu aantonen dat alle wortels van $p(x) = 0$ in N liggen.

N is een eindige uitbreiding van k, met als gevolg dat elk element van N algebraïsch is over k. Zij $q(x) \in k[x]$ het minimaal polynoom (over k) van β. Nu is $k[x] \subset L[x]$, zodat $q(x) \in L[x]$. Daar $p(\beta) = q(\beta) = 0$ en $p(x)$ irreducibel is (over L), is $q(x)$ een veelvoud van $p(x)$. Elke wortel van $p(x) = 0$ is dus ook wortel van $q(x) = 0$; alle wortels van $q(x) = 0$ liggen in N, dus ook alle wortels van $p(x) = 0$ liggen in N.

Stelling 3. Zij $k \subset L \subset K$, terwijl L een normale uitbreiding is van k. Dan is $G(K/L)$ een normaaldeler van $G(K/k)$.

Bewijs. Zij $\ell \in L$ en zij $p(x) \in k[x]$ het minimaal polynoom van ℓ over k. Dan is

$$0 = p(\ell) = \alpha_0 + \alpha_1 \ell + \ldots + \alpha_r \ell^r, \quad \alpha_i \in k.$$

Zij nu $\tau \in G(K/k)$; dan is

$$0 = \tau(0) = \tau(p(\ell)) = \alpha_0 + \alpha_1 \tau(\ell) + \ldots + \alpha_r (\tau(\ell))^r = p(\tau(\ell)).$$

Omdat L normaal is over k, geldt dus $\tau(\ell) \in L$. Is $\sigma \in G(K/L)$, dan geldt dus

$$(\sigma \circ \tau)(\ell) = \sigma(\tau(\ell)) = \tau(\ell),$$

met als gevolg $(\tau^{-1} \circ \sigma \circ \tau)(\ell) = \tau^{-1}(\tau(\ell)) = \ell$. Het automorfisme $\tau^{-1} \circ \sigma \circ \tau$ laat dus L invariant, zodat

$$\tau^{-1} \circ \sigma \circ \tau \in G(K/L).$$

Definitie 2. De lichamen k_1 en k_2 heten isomorf als er een 1-1 duidige afbeelding σ van k_1 op k_2 bestaat, zodanig dat voor alle $\alpha, \beta \in k_1$ geldt

$$\begin{cases} \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) \\ \sigma(\alpha . \beta) = \sigma(\alpha) . \sigma(\beta). \end{cases}$$

Stelling 4. Zij k een lichaam en $p(x) \in k[x]$ een irreducibel polynoom; zijn ϑ en η twee wortels van $p(x) = 0$, dan bestaat er tussen $k(\vartheta)$ en $k(\eta)$ een isomorfisme σ, zodanig dat $\sigma(\vartheta) = \eta$ en $\sigma(\alpha) = \alpha$ voor alle $\alpha \in k$.

Bewijs. Heeft p(x) de graad n, dan is

$1, \eta, \eta^2, \ldots, \eta^{n-1}$ een basis voor $k(\eta)$ over k

en $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$ een basis voor $k(\vartheta)$ over k.

Beschouw nu de afbeelding

$$\sigma : k(\vartheta) \to k(\eta)$$

met

$$\alpha_0 + \alpha_1\vartheta + \ldots + \alpha_{n-1}\vartheta^{n-1} \xrightarrow{\sigma} \alpha_0 + \alpha_1\eta + \ldots + \alpha_{n-1}\eta^{n-1};$$

deze afbeelding is 1-1 duidig en op (ga dit na).
Verder is

$$\sigma(\alpha+\beta) = \sigma\Big(\sum_{i=0}^{n-1} \alpha_i\vartheta^i + \sum_{i=0}^{n-1} \beta_i\vartheta^i\Big) = \sigma\Big(\sum_{i=0}^{n-1} (\alpha_i + \beta_i)\vartheta^i\Big) =$$

$$= \sum_{i=0}^{n-1} (\alpha_i + \beta_i)\eta^i = \sum_{i=0}^{n-1} \alpha_i\eta^i + \sum_{i=0}^{n-1} \beta_i\eta^i = \sigma(\alpha) + \sigma(\beta);$$

men gaat gemakkelijk na dat ook $\sigma(\alpha.\beta) = \sigma(\alpha) \,.\, \sigma(\beta)$.

Stelling 5. Zijn L en L^* deellichamen van een lichaam N, terwijl σ een isomorfisme is tussen L en L^*.
Is $k \overset{\text{def}}{=} \{x \mid x \in L \cap L^*, \sigma(x) = x\}$, en is N normaal over k, dan bestaat er een automorfisme σ^* van N zodanig dat $\sigma^*(\ell) = \sigma(\ell)$ voor alle $\ell \in L$.

Bewijs. N is normaal over k, zodat N ook normaal is over L en L^* $(k \subset L \subset N;\ k \subset L^* \subset N)$.
Zij ϑ een willekeurig element van N, dan heeft ϑ over L een minimaal polynoom $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in L[x]$. Met behulp van het automorfisme σ kan men L[x] als volgt afbeelden op $L^*[x]$:

$$p(x) \xrightarrow{\sigma} p^*(x) = x^n + \sigma(a_{n-1})x^{n-1} + \ldots + \sigma(a_1)x + \sigma(a_0).$$

Indien p(x) irreducibel is over L, is $p^*(x)$ irreducibel over L^* (ga dit na). Zij $q(x) \in k[x]$ het minimaalpolynoom van ϑ over k; dan is $q^*(x) = q(x)$; $q(x) = 0$ heeft de wortel ϑ; dus p(x) deelt q(x), met als gevolg dat $p^*(x)$ ook $q^*(x) = q(x)$ deelt. Daar q(x) binnen $N[x]$ in lineaire factoren te ontbinden is, moet ook $p^*(x) = 0$ alle wortels in N hebben. Zij η een wortel van $p^*(x) = 0$. Dan kunnen we een afbeelding σ^* definiëren: $\sigma^*(\vartheta) = \eta$ en $\sigma^*(\ell) = \sigma(\ell)$; voor alle $\ell \in L$.

We bewijzen nu eerst, dat deze afbeelding kan worden uitgebreid tot een isomorfisme van $L(\vartheta)$ op $L^*(\eta)$.

$\{1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}\}$ is een basis van $L(\vartheta)$ over L

en $\{1, \eta, \eta^2, \ldots, \eta^{n-1}\}$ is een basis van $L^*(\eta)$ over L^*.

Een willekeurig element van $L(\vartheta)$ ziet er als volgt uit:

$\beta = b_0 + b_1\vartheta + \ldots + b_{n-1}\vartheta^{n-1}$. Deze wordt door σ^* afgebeeld op

$\beta^* = \sigma(b_0) + \sigma(b_1)\eta + \ldots + \sigma(b_{n-1})\eta^{n-1}$.

$$\sigma^*(\beta+\gamma) = \sigma^*\Big(\sum_{i=0}^{n-1} b_i\vartheta^i + \sum_{i=0}^{n-1} c_i\vartheta^i\Big) = \sigma^*\Big(\sum_{i=0}^{n-1} (b_i + c_i)\vartheta^i\Big) = \sum_{i=0}^{n-1} \sigma(b_i+c_i)\eta^i =$$

$$= \sum_{i=0}^{n-1} \sigma(b_i)\eta^i + \sum_{i=0}^{n-1} \sigma(c_i)\eta^i = \sigma^*(\beta) + \sigma^*(\gamma).$$

Om te bewijzen, dat $\sigma^*(\beta.\gamma) = \sigma^*(\beta).\sigma^*(\gamma)$ is het voldoende te bewijzen dat $\sigma^*(\beta\vartheta) = \sigma^*(\beta)\sigma^*(\vartheta)$ (ga dit na).

$$\sigma^*(\beta\vartheta) = \sigma^*\Big(\sum_{i=0}^{n-1} b_i\vartheta^{i+1}\Big) = \sigma^*\Big(\sum_{i=1}^{n-1} b_{i-1}\vartheta^i + b_{n-1}\vartheta^n\Big) = \text{(na ontwikkeling}$$

van ϑ^n met behulp van $p(\vartheta) = 0$) $= \sigma^*(-a_0.b_{n-1} - a_1b_{n-1}\vartheta + b_0\vartheta - a_2b_{n-1}\vartheta^2 + b_1\vartheta^2 - \ldots$

$\ldots - a_{n-1}b_{n-1}\vartheta^{n-1} + b_{n-2}\vartheta^{n-1}) = -\sigma(a_0).\sigma(b_{n-1}) - \sigma(a_1)\sigma(b_{n-1})\eta +$

$+ \sigma(b_0)\eta - \ldots - \sigma(a_{n-1})\sigma(b_{n-1})\eta^{n-1} + \sigma(b_{n-2})\eta^{n-1}.$

$$\sigma^*(\beta).\sigma^*(\vartheta) = \Big(\sum_{i=0}^{n-1} \sigma(b_i)\eta^i\Big)\eta = \sum_{i=0}^{n-1} \sigma(b_i)\eta^{i+1} = \sum_{i=1}^{n-1} \sigma(b_{i-1})\eta^i + \sigma(b_{n-1})\eta^n =$$

$$= -\sigma(a_0)\sigma(b_{n-1}) - \sigma(a_1)\sigma(b_{n-1})\eta + \sigma(b_0)\eta - \ldots - \sigma(a_{n-1})\sigma(b_{n-1})\eta^{n-1} +$$

$$+ \sigma(b_{n-2})\eta^{n-1}.$$

Conclusie: $\sigma^*(\beta\vartheta) = \sigma^*(\beta)\sigma^*(\vartheta)$.

Dus: σ^* is een isomorfisme tussen $L(\vartheta)$ en $L^*(\eta)$.
Daar N van eindige graad is, kan men door dit proces een eindig aantal malen toe te passen, een voortzetting verkrijgen van σ, die op geheel N gedefiniëerd is; maar dat is dan tevens een automorfisme van N, dat aan de gestelde eisen voldoet.
De stellingen 4 en 5 leveren samen enige informatie over het bestaan van automorfismen in normale uitbreidingen. Wanneer men een irreducibel polynoom heeft, dat binnen een normale uitbreiding uiteen valt, dan is er altijd wel een automorfisme te vinden, dat de wortels in elkaar overvoert. Dit heeft tot gevolg dat we nu de stellingen 1 en 3 kunnen omkeren.

Stelling 6. Zij k een lichaam, en zij N een normale uitbreiding van k; dan geldt voor het invariantenlichaam van de Galoisgroep G(N/k)

$$N_{G(N/k)} = k.$$

Bewijs. Stel het invariantenlichaam $N_{G(N/k)}$ bevat een element ϑ dat niet in k zit, dan heeft ϑ een minimaalpolynoom $p(x) \in k[x]$, terwijl $p(x)$ niet lineair is maar binnen N wel in lineaire factoren uiteen valt. $p(x)$ heeft dus binnen N een wortel $\vartheta_1 \neq \vartheta$.
Volgens stelling 4 is er nu een isomorfisme van $k(\vartheta)$ naar $k(\vartheta_1)$, en volgens stelling 5 is er een automorfisme van N, dat ϑ in ϑ_1 overvoert. Dit is in tegenspraak met de keuze van ϑ; dus men kan niet een ϑ vinden, die invariant is, en niet in k zit.
Gevolg: $N_{G(N/k)} = k$.

Stelling 7. Zij k een lichaam, en zij N een normale uitbreiding van k. Zij H een normaaldeler van de Galoisgroep G(N/k); dan is N_H een normale uitbreiding van k.

Bewijs. Stel N_H is niet normaal, dan is er een polynoom $p(x) \in k[x]$, dat irreducibel is over k, en dat in N_H een nulpunt ϑ heeft, maar niet in N_H in lineaire factoren uiteen valt. Daar N normaal is over k, valt $p(x) \in k[x]$ binnen $N[x]$ wel in lineaire factoren uiteen; er is dus een η zodanig dat $\eta \in N$, $\eta \notin N_H$, $p(\eta) = 0$.

Er bestaat dus een automorfisme τ van N, dat $\vartheta \in N_H$ afbeeldt op het element $\eta \notin N_H$. Er is dus een element $\sigma \in H$, dat η afbeeldt op een element $\zeta \neq \eta$. Maar wegens de eenduidigheid van het automorfisme τ is dus $\tau^{-1}(\zeta) \neq \tau^{-1}(\eta) = \vartheta \in N_H$.
Dus nu geldt: $\tau^{-1} \circ \sigma \circ \tau(\vartheta) \neq \vartheta$ zodat $\tau^{-1} \circ \sigma \circ \tau \notin H$; H is dus geen normaaldeler van G(N/k).

Definitie 3. Zij H een ondergroep van een groep G. Dan heet het aantal linker nevenklassen aH (met $a \in G$) de index van H t.o.v. G.

Opgaven.

1) Bewijs, dat het geen verschil maakt of de index m.b.v. de linker-, of m.b.v. de rechternevenklassen wordt gedefiniëerd.

2) Zij G een groep, en H een ondergroep, dan is: orde(H).index(H) = orde(G).

De resultaten van deze stellingen kunnen als volgt worden samengevat:

Stelling 8. Hoofdstelling der Galoistheorie.

Zij k een lichaam, en N een normale uitbreiding van k.

1) Dan is aan elk lichaam L met $k \subset L \subset N$ één en slechts één ondergroep $G(N/L) \subset G(N/k)$ toegevoegd, zodanig dat $N_{G(N/L)} = L$.

2) Het lichaam L is dan en slechts dan een normale uitbreiding van k als G(N/L) een normaaldeler is in G(N/k).

3) Voor elke L geldt: $[L : k]$ = index van G(N/L) en $[N : L]$ = orde van G(N/L).

Bewijs. 1) stellingen 1, 2 en 6.
2) stellingen 3 en 7.
3) §7 stelling 10 en definitie index.

Definitie 4. Onder het splijtlichaam t.o.v. k van het polynoom $f(x) \in k[x]$ verstaan we de kleinste uitbreiding S van k die alle wortels van $f(x) = 0$ bevat.

Opmerking. In dit splijtlichaam is f(x) volledig te ontbinden in lineaire factoren.
(We veronderstellen de hoofdstelling der algebra bekend).

Stelling 9. Elke normale uitbreiding N van k is splijtlichaam t.o.v. k voor zeker polynoom $f(x) \in k[x]$.
(Hierbij behoeft f(x) niet irreducibel te zijn over k).

Bewijs: N is een normale uitbreiding van k en is dus eindig dimensionaal over k. Zij $\{\eta_1, \eta_2, \ldots, \eta_n\}$ een basis van N over k. Zij $p_i(x) \in k[x]$ het minimaal polynoom van η_i. Aangezien dit polynoom irreducibel is en een wortel (n.l. η_i) in N heeft, is het binnen N geheel in lineaire factoren te ontbinden.
Het product

$$p(x) = p_1(x).p_2(x).p_3(x). \ldots p_n(x)$$

is dus binnen N geheel in lineaire factoren te ontbinden; N omvat dus het splijtlichaam S van p(x): $N \supset S$.
Anderzijds moet het splijtlichaam S van p(x) alle wortels van $p(x) = 0$, dus zeker de elementen η_i bevatten; daar de elementen η_i het lichaam N opspannen, moet wel gelden $S \supset N$. Conclusie: $N = S$.

Stelling 10. Het splijtlichaam S van $f(x) \in k[x]$ is een normale uitbreiding van k.

Bewijs: Zij p(x) een irreducibel polynoom uit $k[x]$ en zij $\beta \in S$ een wortel van $p(x) = 0$; we moeten nu aantonen dat alle wortels van $p(x) = 0$ in S liggen. Daar $\beta \in S$, is β te schrijven als

$$\beta = r(\alpha_1, \alpha_2, \ldots, \alpha_m)$$

waarbij $\alpha_1, \alpha_2, \ldots, \alpha_m$ alle wortels zijn van $f(x) = 0$ en $r(x_1, x_2, \ldots, x_m)$ een polynoom is met coëfficiënten uit k (vergelijk §6, stelling 5).

Permuteren we in $r(\alpha_1, \alpha_2, \ldots, \alpha_m)$ de α's dan verkrijgen we m! getallen $\beta_j \in S$. Beschouw nu het polynoom

$$q(x) = (x-\beta_1)(x-\beta_2) \ldots (x-\beta_{m!}) \quad (\beta_1 = \beta).$$

Dit polynoom is symmetrisch in de β's; de β's ontstaan uit elkaar door de α's te permuteren, zodat elke coëfficiënt van q(x) een symmetrische veelterm in de α's is.
De hoofdstelling van de symmetrische funkties (zie appendix bij §8) zegt, dat dan elke coëfficiënt van q(x) te schrijven is als een veelterm in de elementaire symmetrische funkties van de α's, met coëfficiënten uit k (immers, de coëfficiënten van $r(x_1, x_2, \ldots, x_m)$ zijn ook elementen van k).
De elementaire symmetrische funkties in de α's zijn, zoals bekend, juist de coëfficiënten van $f(x) \in k[x]$ en zijn dus elementen van k; dus $q(x) \in k[x]$.
Nu is $q(\beta) = p(\beta) = 0$; p(x) is irreducibel, zodat p(x) een deler is van q(x). Alle wortels van p(x) komen dus voor onder de β's en liggen dus alle in S.

Appendix

Symmetrische veeltermen (funkties)

Definitie. Een polynoom $\varphi(x_1, x_2, \ldots, x_n)$ heet symmetrisch indien het polynoom bij elke permutatie van de variabelen $x_1, x_2, \ldots, x_n$ in zichzelf overgaat.

Voorbeelden.

$$\sigma_1 = \sigma_1(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \ldots + x_n.$$

$$\sigma_2 = \sigma_2(x_1, x_2, \ldots, x_n) = x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n.$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n = \sigma_n(x_1, x_2, \ldots, x_n) = x_1x_2 \ldots x_n.$$

Deze polynomen σ_i heten de elementaire symmetrische veeltermen.

Andere voorbeelden zijn:

$$x_1^2 + x_2^2 + \ldots + x_n^2 \quad (= \sigma_1^2 - 2\sigma_2)$$

$$x_1^2 x_2 x_3 \ldots x_n + \ldots + x_1 x_2 x_3 \ldots x_n^2 \quad (= \sigma_1 \sigma_n)$$

$$x_1^3 + x_2^3 + \ldots + x_n^3 \quad (= \sigma_1^3 - 3\sigma_1\sigma_2 - 6\sigma_3 \quad \text{voor } n \geqslant 3).$$

Stelling. Hoofdstelling der symmetrische veeltermen

Elke symmetrische veelterm $\varphi(x_1, x_2, \ldots, x_n)$ met coëfficiënten uit het lichaam k is te schrijven als een veelterm $\psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ eveneens met coëfficiënten uit k.

Bewijs: Men ordene het polynoom $\varphi(x_1, x_2, \ldots, x_n)$ lexicografisch: d.w.z. men plaatse de term

$$a\, x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

voor de term

$$b\, x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n}$$

indien het eerste verschil $\alpha_i - \beta_i$ dat niet 0 is, positief is.
Voor de eerste term $a x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ van φ geldt dan, wegens het symmetrisch zijn van φ, dat $\alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_{n-1} \geqslant \alpha_n$.
Is g de graad van φ (d.w.z. g is het maximum, over alle termen van φ, van de som van de bijbehorende exponenten β_i), dan heeft

$$\varphi_1(x_1, x_2, \ldots, x_n) = \varphi(x_1, x_2, \ldots, x_n) - a\sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \ldots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}$$

hoogstens de graad g, terwijl de eerste term van φ_1 lexicografisch later komt dan de eerste term van φ.
We kunnen dus schrijven

$$\varphi = a\, \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \ldots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n} + \varphi_1.$$

Behandelen we φ_1 op dezelfde wijze als φ, dan ontstaat een term

$$b\,\sigma_1^{\beta_1-\beta_2}\,\sigma_2^{\beta_2-\beta_3}\,\ldots\,\sigma_{n-1}^{\beta_{n-1}-\beta_n}\,\sigma_n^{\beta_n} \qquad (b \in k)$$

en een polynoom φ_2 (met coëfficiënten uit k) zodanig dat

1. $\varphi = a\,\sigma_1^{\alpha_1-\alpha_2}\,\ldots\,\sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\,\sigma_n^{\alpha_n} + b\,\sigma_1^{\beta_1-\beta_2}\,\ldots\,\sigma_{n-1}^{\beta_{n-1}-\beta_n}\,\sigma_n^{\beta_n} + \varphi_2$

2. de graad van φ_2 hoogstens gelijk is aan de graad van φ_1
3. de eerste term van φ_2 lexicografisch later komt dan de eerste term van φ_1.

Dit proces is voortzetbaar, maar zal zeker na een eindig aantal stappen afbreken, omdat bij gegeven graad g slechts een eindig aantal mogelijke lexicografische opvolgers van de eerste term van φ bestaat. Het symmetrische polynoom φ is dus te schrijven als

$$\psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

waarbij ψ een (in het algemeen niet symmetrisch) polynoom is met coëfficiënten uit k.

§9. Constructies met passer en lineaal.

In deze paragraaf zal de onoplosbaarheid van een aantal beroemde klassieke meetkundige problemen worden bewezen. Hiermee wordt bedoeld: de onmogelijkheid om uitgaande van een willekeurig stelsel meetkundige gegevens de gevraagde constructie uit te voeren met behulp van een passer en een lineaal.

Het betreft hier de volgende problemen:

a) Het Delische probleem (de verdubbeling van de kubus).

b) De trisectie van de hoek.

c) De quadratuur van de cirkel.

d) De constructie van de regelmatige n-hoek.
(Voor welke n is de regelmatige n-hoek construeerbaar?)

Alvorens deze problemen afzonderlijk te bespreken dienen wij eerst te onderzoeken wat door middel van passer en lineaalconstructies verkregen kan worden en wat niet.

In het Euclidische vlak denken wij ons naast de gegeven meetkundige objecten (punten, lijnen, hoeken, en cirkels) een Carthesisch coördinatenstelsel. Hiermede kunnen wij alle gegevens en gevraagde figuren representeren door getallen en vergelijkingen. De voorwaarden waaraan de te construeren objecten dienen te voldoen laten zich nu algebraïsch uitdrukken.

De eerste stelling geeft een voldoende voorwaarde opdat een oplossing x van een probleem zich laat construeren met passer en lineaal uitgaande van de gegevens $a_1, a_2, \ldots, a_k$.

Stelling 1: Als een oplossing x van een probleem reëel is en zich laat berekenen uitgaande van de gegevens $a_1\ a_2 \ldots a_k$ door de volgende bewerkingen: "optellen, aftrekken, vermenigvuldigen, delen, en vierkantswortel trekken", dan is x uit $a_1 \ldots a_k$ te construeren met behulp van passer en lineaal.

Bewijs: Denk het Euclidische vlak als complex z-vlak waarin de oorsprong en het punt z=1 gegeven zijn. Als a en b twee gegeven complexe getallen zijn dan kunnen a+b en a-b gevonden worden door parallelogram constructies.

Het product a.b is bepaald door Arg(ab) = Arg(a) + Arg(b) (wat

neerkomt op het overbrengen van een hoek) en de evenredigheid $1 : |a| = |b| : |ab|$ waarvoor een bekende evenredigheidsconstructie bestaat.

Deling komt neer op $\mathrm{Arg}(\frac{a}{b}) = \mathrm{Arg}(a) - \mathrm{Arg}(b)$ en de evenredigheid $|b| : 1 = |a| : |\frac{a}{b}|$.

Tenslotte komt het trekken van een vierkantswortel neer op de betrekkingen: $\mathrm{Arg}(\sqrt{a}) = \frac{1}{2}\mathrm{Arg}(a)$ (een bisectrice constructie) en de evenredigheid: $1 : |\sqrt{a}| = |\sqrt{a}| : |a|$ waarvoor een constructie met een loodlijn binnen een cirkel bekend is.

Opmerking 1: Uit het bewijs volgt dat zodra het vlak genormeerd is door het punt z=0 en z=1 aan te wijzen, ieder punt met rationale coördinaten oonstrueerbaar is.

Opmerking 2: De voorwaarde waaraan de x uit stelling 1 voldoet laat zich ook formuleren als volgt:
x zit in een lichaam K dat uit het lichaam $k = Q(a_1, a_2, \ldots, a_k)$ verkregen wordt door eindig veel kwadratische uitbreidingen. Hieruit volgt $[K : k] = 2^m$.

Van stelling 1 geldt ook een omkering:

Stelling 2: Laat x een getal zijn dat zich uit $1, a_1, a_2, \ldots, a_n$ laat construeren met passer en lineaal. Dan zit x in een lichaam K dat uit $k = Q(a_1, a_2, \ldots, a_n)$ verkregen wordt door eindig veel kwadratische uitbreidingen.

Bewijs: Beschouw het Euclidische vlak met daarin een Carthesisch coördinatenstelsel. We mogen al die punten bepaald denken waarvan de coördinaten in k zitten.
In dit vlak bekijken we de elementaire constructies.

a) Het kiezen van een punt. Als het punt bepaald is zitten beide coördinaten in k. Als we een onbepaald punt (x,y) kiezen komt dit neer op een transcendente uitbreiding van k die geen invloed uitoefent op het probleem.
b) Het trekken van een lijn door twee punten (x_1,y_1) en (x_2,y_2). Deze lijn heeft de vergelijking:

$$(x_1 - x_2)(y - y_1) = (y_1 - y_2)(x - x_1)$$

Dit is een lineaire vergelijking met coëfficiënten in k.

c) Het snijden van twee lijnen: $a_1x + b_1y + c_1 = 0$
$a_2x + b_2y + c_2 = 0$

Als $a_1, a_2, b_1, b_2, c_1, c_2 \in k$ dan zitten ook de coördinaten van de oplossing in k.

d) Constructie van een cirkel met gegeven middelpunt en straal.

$$(x - x_0)^2 + (y - y_0)^2 = r^2.$$

De coëfficiënten van deze kwadratische vergelijking zitten in k.

e) Snijden van lijn en cirkel: $x^2 + y^2 + ax + by + c = 0$
$y = mx + p$

Als a, b, c, m, $p \in k$ dan zitten de coördinaten van de oplossingen in een lichaam dat kwadratisch is over k.

f) Het snijpunt van twee cirkels.

Deze constructie laat zich reduceren tot e),

immers $\left.\begin{aligned} x^2 + y^2 + a_1x + b_1y + c_1 &= 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 &= 0 \end{aligned}\right\}$ komt neer op

$$\left.\begin{aligned} x^2 + y^2 + a_1x + b_1y + c_1 &= 0 \\ (a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) &= 0 \end{aligned}\right\}$$

Combinatie van de stellingen 1 en 2 leert dus:

Stelling 3: Een onbekende x laat zich door constructie met passer en lineaal construeren uit de gegevens $(1, a_1, a_2, \ldots, a_k)$ dan en slechts dan als x in een lichaam K zit dat verkregen wordt door eindig vele kwadratische uitbreidingen van het lichaam $k = Q(a_1, a_2, \ldots, a_k)$.

Opmerking 3: $[K : k] = 2^m$ hieruit volgt in het bijzonder $[k(x) : k] = 2^n$. Op grond van deze nodige voorwaarde kunnen we de onoplosbaarheid van een aantal problemen reeds bewijzen.

Een kwadratische uitbreiding van een lichaam k is als splijtlichaam van een kwadratisch polynoom altijd normaal over k. Hieruit volgt dat als K uit k verkregen wordt door een serie kwadratische uitbreidingen er een serie tussenlichamen is aan te wijzen:

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \ldots \subseteq k_n = K$$

hierbij is k_{i+1} normaal over k_i. Door hierna nog eens eindig veel kwadratische uitbreidingen uit te voeren kunnen we tot een lichaam L komen dat K omvat en normaal is over k. Zo vinden we de rij tussenlichamen:

$$k = k_0 \subseteq k_1 \subseteq \ldots \subseteq k_n = K \subseteq k_{n+1} \subseteq \ldots \subseteq k_r = L$$

Nu kunnen we de hoofdstelling der Galoistheorie toepassen.
Met de boven geschreven rij correspondeert een rij ondergroepen:

$$G(L/k) \supseteq G(L/k_1) \supseteq \ldots \supseteq G(L/K) \supseteq G(L/k_{n+1}) \supseteq \ldots \supseteq G(L/L) = E$$

aangezien voor iedere i k_{i+1} kwadratisch (dus normaal) is over k_i volgt:

$G(L/k_{i+1}) \trianglelefteq G(L/k_i)$ en

$G(L/k_i)/G(L/k_{i+1}) \cong G(k_{i+1}/k_i) \cong C_2$ (een cyclische groep van de orde 2)

Het boven geschetste betoog is omkeerbaar:
Zij L normaal over k en laat G(L/k) een rij normaaldelers bezitten:

$$E \trianglelefteq N_{r-1} \trianglelefteq N_{r-2} \trianglelefteq \ldots \trianglelefteq N_0 = G(L/k).$$

terwijl voor iedere i $N_{i+1}/N_i \cong C_2$, dan correspondeert hiermede een rij tussenlichamen:

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \ldots \subseteq k_r = L$$

zodanig dat: $G(K_{i+1}/k_i) \cong N_i/N_{i+1} \cong C_2$ zodat voor iedere i k_{i+1} kwadratisch is over k_i.
De groepentheorie leert ons dat bij iedere groep van de orde 2^n een rij normaaldelers als bovengenoemd is te vinden:
Hieruit volgt dus de stelling:

Stelling 4: Zij L normaal over k. Dan is L op te bouwen door eindig veel kwadratische uitbreidingen dan en slechts dan als $[L:k]$ een macht van twee is.

Stelling 3 laat zich nu opnieuw formuleren:

Stelling 3*: Een onbekende x laat zich door constructie met passer en lineaal construeren uit de gegevens $(1, a_1, a_2, \ldots, a_k)$ dan en slechts dan als x in een normale uitbreiding L van $k = Q(a_1, a_2, \ldots a_k)$ zit met $[L:k] = 2^m$.

We kunnen nu de gevraagde onmogelijkheidsbewijzen zonder moeite geven.

a) Het Delische probleem.

Gegeven een ribbe van een kubus a.
Gevraagd de ribbe van een kubus met inhoud $2a^3$.
Hier wordt in feite gevraagd het getal $\sqrt[3]{2}$ te construeren. (We mogen a=1 veronderstellen)
Aangezien $[Q(\sqrt[3]{2}) : Q] = 3$ is het Delische probleem onoplosbaar.

b) De trisectie van een hoek.

Gegeven een hoek 3α.
Gevraagd de hoek α te construeren.
Als hoek 3α gegeven is betekent dit in feite dat het getal $\cos 3\alpha$ gegeven is. Gezocht wordt $\cos \alpha$. Hiervoor geldt de algebraïsche vergelijking:

$$4\cos^3 \alpha - 3\cos \alpha - \cos 3\alpha = 0.$$

Aangezien het polynoom $4x^3 - 3x - \beta$ voor algemene β irreducibel is, is de gevraagde uitbreiding van $Q(\cos 3\alpha)$ een kubische uitbreiding.
De trisectie van de hoek is dus onmogelijk.

Opmerking 4: Voor die speciale hoeken γ waarvoor het polynoom $4x^3 - 3x - \cos \gamma$ wel reducibel is (bv. $\gamma = \frac{\pi}{2}$) is de trisectie natuurlijk wel mogelijk.

c) De quadratuur van de cirkel.

Gegeven een cirkel met straal r.
Gevraagd de zijde van een vierkant met oppervlakte πr^2.
In feite wordt hier gevraagd naar een constructie van het getal π.
Nu is π een transcendent getal dus π ligt in geen enkele algebraïsche uitbreiding van Q.
Ook de quadratuur van de cirkel is dus onoplosbaar.

d) De constructie van de regelmatige n-hoek.

Hier wordt gezocht naar de constructie van een hoek van $\frac{2\pi}{n}$ radialen. We moeten dus construeren het getal $\cos\frac{2\pi}{n} = \frac{1}{2}(e^{\frac{2\pi i}{n}} + e^{\frac{-2\pi i}{n}})$. Dit komt neer op de constructie van de primitieve n^e eenheidswortel $\zeta_n = e^{\frac{2\pi i}{n}}$. Dit komt neer op een lichaamsuitbreiding met de graad $\varphi(n)$ waarbij $\varphi(n)$ de indicator van Euler is (zie opmerking). $\varphi(n)$ is gegeven door de priemfactor ontbinding van n.

Als $n = 2^l \cdot p_1^{\nu_1} \cdot p_2^{\nu_2} \cdot \ldots \cdot p_k^{\nu_k}$ $p_1 \ldots p_k$ priemgetallen ≥ 3 dan is $\varphi(n) = 2^{l-1} \cdot p_1^{\nu_1 - 1} \cdot \ldots \cdot p_k^{\nu_k - 1} \cdot (p_1 - 1) \ldots (p_k - 1)$

Als $\varphi(n)$ een macht van twee is dan moet dus gelden:

$\nu_1 = \nu_2 = \ldots = \nu_k = 1$ en $p_1 = 2^{k_1} + 1$ $p_2 = 2^{k_2} + 1$ etc.

Als 2^m+1 priem is moet m zelf een macht van 2 zijn. De enige priemgetallen van deze vorm (priemgetallen van Fermat) die bekend zijn, zijn:

$3 = 2 + 1$ $5 = 2^2 + 1$ $17 = 2^{2^2} + 1$ $257 = 2^{2^3} + 1$ en

$65537 = 2^{16} + 1$.

Als n dus behalve factoren 2 alleen deze factoren enkelvoudig bevat is de regelmatige n-hoek construeerbaar. Zo zijn de regelmatige 3, 4, 5, 6, 8, 10, 12, 15, en 17-hoek construeerbaar maar de 7 of 9-hoek niet.

Opmerking 5: Een primitieve n^e eenheidswortel is een wortel van $x^n - 1 = 0$ die geen wortel is van $x^d - 1 = 0$ voor een deler d van n. De n^e eenheidswortels vormen een cyclische groep van de orde n waarvan de $\varphi(n)$ voortbrengenden juist de primitieve eenheidswortels zijn. Iedere n^e eenheidswortel is primitieve d^e eenheidswortel voor precies één deler d van n.

Als $\Phi_d(x) = \prod(x - \xi_{d_i})$ waarbij ξ_{d_i} de primitieve d^e eenheidswortels doorloopt ($\varphi(d)$ stuks) dan geldt:

$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$. Hieruit volgt door inductie dat $\Phi_n(x)$ een geheel polynoom is voor iedere n. De graad van $\Phi_n(x)$ is juist $\varphi(n)$. Tenslotte kan bewezen worden dat $\Phi_n(x)$ irreducibel is. Hieruit volgt dat $[Q(e^{\frac{2\pi i}{n}}) : Q] = \varphi(n)$.

§10. Oplosbaarheid van vergelijkingen door middel van radikalen.

Definitie 1. Zij k een lichaam en f(x) een polynoom uit $k[x]$ van de vorm $(x^n - a_1)(x^n - a_2) \ldots (x^n - a_r)$, $a_i \in k$, $i = 1, \ldots, r$. Als k een primitieve n^e eenheidswortel bevat, dan heet het ontbindingslichaam (d.i. het splijtlichaam) K van f(x) over k een Kummer uitbreiding van k.

Stelling 1. Als K een Kummer uitbreiding is van k dan is

1e) K een normale uitbreiding van k,

2e) de Galoisgroep G van K over k is abels.

Bewijs.

1e) Zie §8, stelling 10.

2e) Laat α_i een wortel zijn van $x^n - a_i$, $i = 1, \ldots, r$ en ξ een primitieve n^e eenheidswortel, $\xi \in k$.
Dan zijn de elementen $\alpha_i\xi, \alpha_i\xi^2, \ldots, \alpha_i\xi^n$ de n verschillende wortels van $x^n - a_i$, $i = 1, \ldots, r$ en $K = k(\alpha_1, \ldots, \alpha_r)$.
Stel nu dat φ en ψ twee automorfismen zijn uit G. Zowel φ als ψ beelden dan iedere α_i af op een wortel van $x^n - a_i$, dus er zijn getallen φ_i en ψ_i zó dat

$$\varphi(\alpha_i) = \alpha_i \xi^{\varphi_i}$$

$$\psi(\alpha_i) = \alpha_i \xi^{\psi_i}.$$

Dus $(\varphi.\psi)(\alpha_i) = \varphi(\psi(\alpha_i)) = \varphi(\alpha_i\xi^{\psi_i}) = \alpha_i\xi^{\varphi_i}\xi^{\psi_i} = \alpha_i\xi^{\varphi_i+\psi_i}$

en $(\psi.\varphi)(\alpha_i) = \psi(\varphi(\alpha_i)) = \psi(\alpha_i\xi^{\varphi_i}) = \alpha_i\xi^{\psi_i}\xi^{\varphi_i} = \alpha_i\xi^{\psi_i+\varphi_i}$.

Er geldt dus dat $\varphi.\psi(\alpha_i) = (\psi.\varphi)(\alpha_i)$, $i = 1, \ldots, r$.
Daar $\alpha_1, \ldots, \alpha_r$ een stel voortbrengenden is van K over k geldt dus dat $\varphi.\psi = \psi.\varphi$.

Stelling 2. Als K het ontbindingslichaam is van $f(x) = x^p - a$ en als k een primitieve p^e eenheidswortel bevat, waarbij p een priemgetal is, dan is K = k, of $x^p - a$ is irreducibel en de Galoisgroep G van K over k is een cyclische groep van de orde p.

Bewijs. Laat α een wortel zijn van x^p-a en ξ een p^e eenheidswortel. Dan zijn $\alpha\xi, \alpha\xi^2, \ldots, \alpha\xi^p$ alle wortels van x^p-a, zó dat $K = k(\alpha)$ en $[K : k] \leq p$. De orde van G is dus kleiner of gelijk aan p. Voor iedere $\varphi \in G$ is er een r, $0 < r \leq p$, zó dat $\varphi(\alpha) = \alpha\xi^r$. Dus $\varphi^p(\alpha) = \alpha(\xi^r)^p = \alpha$.
De orde van φ is dus een deler van p. Als φ niet de identieke afbeelding is, dan heeft φ dus juist een orde p en bestaat G dus uit de machten van φ.

Definitie 2. Een uitbreiding K van een lichaam k heet een uitbreiding door middel van radikalen als er lichamen $k = K_0, K_1, \ldots, K_r = K$ bestaan, zo dat $K_i = K_{i-1}(\alpha_i)$, $i = 1, \ldots, r$, waarbij α_i wortel is van een vergelijking van de vorm $x^{n_i} - a_i = 0$, $a_i \in K_{i-1}$.

$$k = K_0 \subset K_1 \subset \ldots\ldots \subset K_r = K.$$

Opmerking. Wij zullen steeds aannemen dat het grondlichaam k primitieve $n_i$de eenheidswortels bevat voor $i = 1, 2, \ldots, r$.
Dan is ieder lichaam K_i een normale uitbreiding van K_{i-1}. K hoeft dan echter nog geen normale uitbreiding van k te zijn.
Wel kunnen wij K dan uitbreiden tot een lichaam L zo dat L een uitbreiding is van k, door middel van radikalen en zó dat L normaal is over k.

Stelling 3. Iedere uitbreiding K van k door middel van radikalen is bevat in een normale uitbreiding L van k door middel van radikalen.

Bewijs. Stel $k \subset K_1 \subset \ldots \subset K_r = K$.
Wij zullen deze stelling bewijzen door inductie naar r.
Als r = 1, dan $K = K_1 = k(\alpha_1)$, waarbij α_1 wortel is van $x^{n_1} - a_1$.
Daar k een primitieve $n_1$de eenheidswortel bevat is K_1 normaal over k.
Laat nu de stelling bewezen zijn voor alle rijen met lengte r-1.
Dan is er dus een normale uitbreiding L van k zó dat $K_{r-1} \subset L$ en L een uitbreiding door middel van radikalen is van k.
Zij nu $K = K_r = K_{r-1}(\alpha_r)$ waarbij α_r wortel is van $x^{n_r} - a_r$, $a_r \in K_{r-1}$.
Laat $a_r, a_r^1, \ldots, a_r^s$ alle wortels zijn van het minimale polynoom van

a_r over k. Daar $a_r \in K_{r-1} \subset L$ en L normaal over k geldt ook $a_r^i \in L$, $i = 1, \ldots, s$.

Zij nu $f(x) = (x^{n_r} - a_r)(x^{n_r} - a_r^1) \ldots (x^{n_r} - a_r^s) \in L[x]$ en laat E het ontbindingslichaam zijn van f over L.

Dan is $L \subset L_1 = L(\alpha_r) \subset L_2 = L_1(\alpha_r^1) \subset \ldots \subset L_r(\alpha_r^s) = E$, waarbij α_r^i wortel is van $x^{n_r} - a_r^i$.

E is dus een uitbreiding door middel van radikalen van L en dus ook van k. Verder geldt dat $K_{r-1}(\alpha_r) = K \subset L(\alpha_r) \subset E$.

Daar ieder automorfisme uit de Galoisgroep van L over k de elementen $a_r, a_r^1, \ldots, a_r^s$ permuteert, liggen de coëfficiënten van f(x) in k en is E dus het ontbindingslichaam van een polynoom uit $k[x]$.

E is dus normaal over k.

Definitie 3. Zij f(x) een polynoom uit $k[x]$ en α een wortel van f(x). Als α bevat is in een uitbreiding K door middel van radikalen van k dan zeggen wij dat α uitgedrukt kan worden in radikalen.

Als alle wortels van f uitgedrukt kunnen worden in radikalen dan heet f oplosbaar door middel van radikalen.

Opmerking 1. Het is duidelijk dat als f irreducibel is en minstens één wortel van f uitgedrukt kan worden in radikalen, dan is f oplosbaar door middel van radikalen. Immers als α wortel is van f en $\alpha \in K$, waarbij K een uitbreiding is van k door middel van radikalen, dan is er volgens stelling 3 een normale uitbreiding L van k door middel van radikalen die K omvat.

Daar $\alpha \in L$, ligt iedere wortel van f in L.

Opmerking 2. Een wortel α van het polynoom $f(x) \in k[x]$ kan uitgedrukt worden in radikalen als α zich uit de coëfficiënten van f berekenen laat door middel van rationale operaties en worteltrekken.

α is dus een uitdrukking van de vorm

$$\alpha = \sqrt[n]{\ldots \sqrt[m]{\ldots} + \sqrt[r]{\ldots} + \ldots}$$

Zoals bekend is, is iedere vergelijking van de tweede, derde of vierde graad oplosbaar met behulp van radikalen. Voor vergelijkingen met hogere graad is dit niet meer het geval.

Stelling 4. Als het polynoom $f(x) \in k[x]$ oplosbaar is door middel van radikalen, dan bevat de Galoisgroep G van f(x) een rij ondergroepen $G = G_0 \supset G_1 \supset \ldots \supset G_n = E$ zo dat G_i een normaaldeler is van G_{i-1} en zó dat de factorgroep G_{i-1}/G_i abels is.

Bewijs. Laat L een normale uitbreiding door middel van radikalen zijn van k, zo dat het ontbindingslichaam K van f bevat is in L.

$$k \subset K_1 \subset K_2 \subset \ldots \subset K_r = L.$$

Daar voor iedere i K_i een Kummer uitbreiding is van K_{i-1} is de Galoisgroep van K_i over K_{i-1} abels (Stelling 1). Met de rij $k \subset K_1 \subset K_2 \subset \ldots \subset K_r = L$ correspondeert een rij ondergroepen.

$$G(L/k) \supset G(L/K_1) \supset G(L/K_2) \supset \ldots \quad G(L/K_r) = E.$$

Daar K_i normaal is over K_{i-1} is $G(L/K_i)$ een normaaldeler van $G(L/K_{i-1})$.
Verder is $G(L/K_{i-1})/G(L/K_i) \cong G(K_i/K_{i-1})$ en dus abels.
Zij nu G de Galoisgroep van K over k. Dan geldt daar $k \subset K \subset L$ en K normaal is over k dat G(L/K) een normaal deler is van G(L/k) en de Galoisgroep G is isomorf met

$$G(L/k) \Big/ G(L/K)$$

G is dus een homomorf beeld van G(L/k). Zij nu φ de homomorfe afbeelding van G(L/k) op G. Dan geldt

$$\varphi(G(L/k)) = G \supset G_1 = \varphi(G(L/K_1)) \supset G_2 = \varphi(G(L/K_2)) \supset \ldots \supset G_r = \varphi(E) = E.$$

Iedere G_i is normaaldeler van G_{i-1} en G_{i-1}/G_i is abels.

Opmerking 1 Met behulp van deze stelling kan men nu het bestaan aantonen van hogere machtsvergelijkingen die niet oplosbaar zijn door middel van radikalen. Laat nl. f(x) een polynoom zijn uit $k[x]$

zó dat de Galoisgroep van f gelijk is aan G.
Stel dat het niet mogelijk is in G een rij ondergroepen te vinden die voldoen aan de voorwaarden van stelling 4, dan is f(x) niet oplosbaar door middel van radikalen. Men kan bewijzen dat ook het omgekeerde geldt.
Heeft men dus een polynoom met Galoisgroep G zo dat er wel een dergelijke rij ondergroepen bestaat, dan is f(x) oplosbaar met behulp van radikalen. Een groep die aan de voorwaarden van stelling 4 voldoet heet oplosbaar.

Opmerking 2. De aanname dat k genoeg n^{de} eenheidswortels bevat is in de bovenstaande stelling niet nodig. Immers laat K het ontbindingslichaam zijn van f en laat f oplosbaar zijn door middel van radikalen. Door aan K een primitieve n^{de} eenheidswortel ξ te adjungeren krijgen wij een lichaam K* dat nog steeds normaal is over k. K* kunnen wij ook krijgen door eerst aan k ξ te adjungeren, $k^* = k(\xi)$ en daarna de radikalen $k \subset k^* \subset K^*$. Zij nu G* de groep van K* over k*, G de groep van K* over k en G^0 de groep van k* over k. Dan is G^0 abels en $G^0 = G/G^*$. Daar G* oplosbaar is, is ook G oplosbaar.
De factorgroep G/H met H de groep van K* over K is isomorf met de Galoisgroep van f en dus is deze oplosbaar. (G/H is homomorf beeld van G).

Voorbeeld. Zij K het lichaam van de rationale getallen en $f(x) = x^5 - 4x + 2$.
Uit het irreducibiliteitscriterium van Eisenstein volgt dat f(x) irreducibel is over k.
Gemakkelijk kan men tevens bewijzen dat f(x) precies 3 reële wortels heeft, zeg α_1, α_2, α_3. Dan zijn de twee andere wortels α_4 en α_5, twee complexe getallen zó dat $\bar{\alpha}_4 = \alpha_5$.
Zij nu G de Galoisgroep van f en K het ontbindingslichaam.
G kan dan opgevat worden als een ondergroep van de symmetrische groep S_5. De wortels van f(x) worden immers door iedere $\varphi \in G$ gepermuteerd.

Zij nu $g(\alpha_1, \ldots, \alpha_5)$ een willekeurig element van K (d.i. een polynoom in $\alpha_1, \ldots, \alpha_5$ met coëfficiënten uit k) en laat φ de afbeelding zijn van K in K gedefiniëerd door $\varphi(g(\alpha_1, \ldots, \alpha_5)) = \bar{g}(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_5)$. Daar alle coëfficiënten van g evenals $\alpha_1, \alpha_2, \alpha_3$ reëel zijn is $\bar{g}(\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_5) = g(\alpha_1, \alpha_2, \alpha_3, \alpha_5, \alpha_4)$.
Men kan nu gemakkelijk bewijzen dat φ een automorfisme is van K over k en dat dus de permutatie (45) bevat is in G. Verder is G opgevat als permutatie groep transitief (d.w.z. voor ieder tweetal getallen x en y, $1 \leq x \leq 5$, $1 \leq y \leq 5$, is er een $\varphi \in G$ met $\varphi(x) = y$).
Uit deze twee eigenschappen volgt nu dat $G = S_5$.

Lemma 1. Iedere transitieve ondergroep G van de symmetrische groep S_5 die een willekeurige transpositie (xy) bevat is gelijk aan S_5.

Bewijs. Stel dat $(12) \in G$. Voor iedere transpositie (xy) en iedere permutatie σ geldt $\sigma^{-1}.(xy).\sigma = (\sigma(x)\sigma(y))$.
Uit de transitiviteit van G volgt dan dat elk van de getallen 1, 2, 3, 4 of 5 in minstens één transpositie uit G voorkomt.
Wij kunnen nu 2 gevallen onderscheiden.

1e) éénzelfde getal komt in 3 transposities voor,
b.v. (12), (13), (14) $\in$ G. Maar dan ook een transpositie met 5 in G, b.v. $(52) \in G$.
Maar dan ook $(52)(12)(52) = (15) \in G \Rightarrow G = S_5$.

2e) éénzelfde getal komt in hoogstens 2 transposities voor b.v. $(12), (13) \in G$.
Daar ook $(12)(13)(12) = (23) \in G$, moet dus $(45) \in G$. Daar G transitief is, is er een $\sigma \in G$ met $\sigma(4) = 1$, $\sigma^{-1}(45)\sigma = (\sigma(4)\sigma(5)) = (1\ \sigma(5)) \in G$.
Dus $\sigma(5) = 2$ of $\sigma(5) = 3$; wegens de symmetrie mogen we aannemen $\sigma(5) = 2$.
Maar dan is $\sigma(13)\sigma^{-1} = (\sigma^{-1}(1)\ \sigma^{-1}(3)) = (4x) \in G$, terwijl $x = 1$, 2, of 3.
Dit is in strijd met het feit dat de getallen 1, 2 en 3 in hoogstens twee transposities voorkomen.

Wij hebben nu dus een polynoom $f(x) = x^5 - 4x + 2 \in k[x]$ zó dat de Galoisgroep van f de symmetrische groep S_5 is. Wij bewijzen nu dat S_5 niet oplosbaar is, en dat f dus niet oplosbaar is met behulp van radikalen (stelling 4).

Lemma 2. Als een ondergroep H van S_5 iedere permutatie van de vorm (xyz) bevat en als N een normaaldeler is van H zó dat H/N abels is, dan bevat N iedere permutatie van de vorm (xyz).

Bewijs. We zullen bewijzen dat $(123) \in N$. Zij f de homomorfe afbeelding van H op H/N. Stel $f((412)) = x$ en $f((253)) = y$. Dan is $xy = yx$ dus $xyx^{-1}y^{-1} = E$.
Hieruit volgt dat $(412)\,(253)\,(412)^{-1}(253)^{-1} \in N$.
Maar $(412)\,(253)\,(412)^{-1}(253)^{-1} = (123)$. Dus $(123) \in N$.

Lemma 3. S_5 is niet oplosbaar.

Bewijs. Zij $S_5 = G_0 \supset G_1 \supset G_2 \supset \ldots \; G_n = E$ een rij ondergroepen van S_5 zo dat G_i normaaldeler is van G_{i-1} en G_{i-1}/G_i abels is.
Daar $G_0 = S_5$ alle permutaties van de vorm (xyz) bevat, bevat ook G_1 alle permutaties van de vorm (xyz) en dus ook verder iedere G_i (lemma 2), $i = 2, \ldots, n$.
De rij G_i kan dus niet eindigen met een groep G_n die alleen uit de identiteit bestaat.

§11. Primitieve eenheidswortels en cyclotome polynomen

We bekijken over het lichaam der complexe getallen de volgende vergelijking:

$$x^n - 1 = 0.$$

Uit de Analyse is bekend dat de n complexe wortels gegeven worden door:

$$\zeta_{n,0} = 1 \quad \zeta_{n,1} = e^{\frac{2\pi 1}{n}} \cdots \zeta_{n,k} = e^{\frac{2\pi k 1}{n}} \cdots \zeta_{n,n-1} = e^{\frac{2\pi(n-1)1}{n}}$$

(ga na dat de bovengenoemde complexe getallen aan de vergelijking voldoen en onderling ongelijk zijn).

Definitie: Het getal $\zeta_{n,k} = e^{\frac{2\pi 1 k}{n}}$ heet een n^e eenheidswortel. Als n en k onderling ondeelbaar zijn heet $\zeta_{n,k}$ een primitieve n^e eenheidswortel.

Bezitten n en k een grootste gemene deler d die groter is dan 1 dan geldt:

$$\zeta_{n,k} = e^{2\pi 1 \frac{k}{n}} = e^{2\pi 1 \frac{k/d}{n/d}} = \zeta_{\frac{n}{d},\frac{k}{d}}.$$

Aangezien ((k/d), (n/d)) = 1 is $\zeta_{n,k}$ een n/d^e primitieve eenheidswortel. Duidelijk is dat n/d een deler van n is.

Hieruit volgt: Iedere n^e eenheidswortel is primitieve d^e eenheidswortel voor één en hoogstens één deler van n. Omgekeerd is voor iedere deler d van n een d^e eenheidswortel tevens een n^e eenheidswortel.

Combinatie van deze twee uitspraken geeft:

Prop. 1: De verzameling van de n^e eenheidswortels is de vereniging van de verzamelingen der primitieve d^e eenheidswortels als d de delers van n (incluis 1 en n zelve) doorloopt.

Prop. 2: De n^e eenheidswortels vormen onder vermenigvuldiging (als complexe getallen) een cyclische groep van de orde n.

Bewijs: Uit $(\zeta_{n,k})^n = (\zeta_{n,1})^n = 1$ volgt dat

$$(\zeta_{n,k} \cdot \zeta_{n,1}^{-1})^n = (\zeta_{n,k})^n \cdot ((\zeta_{n,1})^n)^{-1} = 1 \cdot 1^{-1} = 1 \quad \text{dus}$$

$\zeta_{n,k} \cdot \zeta_{n,1}^{-1}$ is weer een n^e eenheidswortel.

Hieruit volgt dat de n^e eenheidswortels een ondergroep vormen van de vermenigvuldiging groep der complexe getallen. Uit het feit dat $\zeta_{n,1} = e^{2\pi i/n}$ een genererend element is volgt dat het een cyclische groep is.

Aangezien we alle wortels van $x^n - 1 = 0$ gevonden hebben kunnen we schrijven:

$$x^n - 1 = (x-1)(x-\zeta_{n,1})(x-\zeta_{n,2})\ldots(x-\zeta_{n,n-1}).$$

In het rechterlid groeperen we nu de termen $(x-\zeta_{n,k})$ als $\zeta_{n,k}$ de verzameling der primitieve d^e eenheidswortels doorloopt en dit doen we voor iedere deler d van n. Volgens prop. 1 krijgen we iedere term precies één keer.
Stel

$$\Phi_d = \prod_{(n,k)=\frac{n}{d}} (x - \zeta_{n,k}).$$

Dan volgt:

$$x^n - 1 = \prod_{d/n} \Phi_d.$$

Φ_d is een polynoom met complexe coëfficiënten.
We zullen aantonen dat al deze coëfficiënten geheel zijn.

Prop. 3: Φ_k is een polynoom uit $\mathbb{Z}[x]$ voor ieder natuurlijk getal k.

Het bewijs gaat met volledige inductie:

Aangezien $\Phi_1(x) = x - 1$ is de stelling juist voor $k = 1$.

Stel ik heb de stelling bewezen voor $k < n$ dan geldt:

$$x^n - 1 = \prod_{\substack{d/n \\ d \neq n}} \Phi_d(x) \cdot \Phi_n(x)$$

$x^n - 1$ en $\prod_{\substack{d/n \\ d \neq n}} \Phi_d(x)$ zijn polynomen in $\mathbb{Z}[x]$.

Verder volgt uit de definitie van $\Phi_d(x)$ dat de coëfficiënt van de hoogste term altijd 1 is. Ik kan dus binnen $\mathbb{Z}[x]$ het delingsalgorithme uitvoeren en aldus $\Phi_n(x)$ uitrekenen. Op deze wijze kan ik constateren dat ook $\Phi_n(x)$ een polynoom met gehele coëfficiënten is.

Bij het bewijs van de irreducibiliteit van $\Phi_n(x)$ worden enige eigenschappen van congruenties modulo een priemgetal p gebruikt. Wij zullen deze eigenschappen hier noemen en afleiden.

Definitie: Stel $f(x)$ en $g(x) \in \mathbb{Z}[x]$ dan heten $f(x)$ en $g(x)$ congruent modulo p (noteer $f(x) \equiv g(x) \pmod p$) indien geldt:

$$f(x) - g(x) = p \cdot h(x) \quad \text{waarbij } h(x) \in \mathbb{Z}[x].$$

Eigenschappen:

Als $f(x) \equiv g(x) \pmod p$ en $h(x) \equiv k(x) \pmod p$ dan geldt:

$$f(x) + h(x) \equiv g(x) + k(x) \pmod p$$
$$f(x) - h(x) \equiv g(x) - k(x) \pmod p$$
$$f(x) \cdot h(x) \equiv g(x) \cdot k(x) \pmod p$$

In het algemeen geldt voor iedere geheeltallige veelterm Q

$$Q(f(x)) \equiv Q(g(x)) \pmod p.$$

Een tweede belangrijke eigenschap is

$$(f(x) + g(x))^p \equiv (f(x))^p + (g(x))^p \pmod p$$

immers: $(f(x) + g(x))^p = (f(x))^p + \binom{p}{1}(f(x))^{p-1} g(x) + \ldots + \binom{p}{p-1} f(x)$
$(g(x))^{p-1} + (g(x))^p$

en $\binom{p}{1} \ldots \binom{p}{p-1}$ zijn allen deelbaar door p.

Evenzo geldt: $(f(x) + g(x) + h(x))^p \equiv (f(x))^p + (g(x) + h(x))^p \equiv$
$\equiv (f(x))^p + (g(x))^p + (h(x))^p \pmod p$.

In het algemeen geldt: Als F een geheeltallige veelterm is in $f_1(x), \ldots, f_k(x)$ dan geldt:

$$\left[F(f_1(x), \ldots, f_k(x))\right]^p \equiv F((f_1(x))^p, \ldots, (f_k(x))^p) \pmod p$$

(Schrijf F uit als som van enkelvoudige termen (dus $2f_1 = f_1 + f_1$) en pas daarop bovenstaande regel toe).

De kleine stelling van Fermat is een speciaal geval van bovengenoemde stelling:
Voor $a \in N$ geldt: $a^p \equiv a \pmod p$.

Immers $a^p = (\underbrace{1 + 1 + \ldots + 1}_{a\text{-keer}})^p \equiv \underbrace{1^p + 1^p + \ldots + 1^p}_{a\text{-keer}} = a \pmod p$

<u>Stelling</u>: $\Phi_n(x)$ is irreducibel over de gehele getallen voor iedere natuurlijke n.

<u>Bewijs</u>: Laat f(x) een irreducibele factor zijn van $x^n - 1$, $f(x) \in \mathbb{Z}[x]$.
Ik schrijf nu

$f(x) = \prod_{j=1}^{k} (x - \varepsilon_j)$ waarbij ε_j n^e eenheidswortels zijn.

Uitgeschreven: $f(x) = x^k + a_1 x^{k-1} + \ldots + a_k$.
a_k is als product van n^e eenheidswortels zelf weer een eenheidswortel en is bovendien geheel dus $a_k = \pm 1$.
Zij nu $g(x) = \prod_{j=1}^{k} (x - \varepsilon_j^p) = x^k + b_1 x^{k-1} + \ldots + b_k$ waarbij
p een priemgetal is dat geen deler van n is.

Nu is $b_k = a_k^p = \pm 1$.
De b_1 zijn gehele symmetrische veeltermen in de ε_j^p dus gehele symmetrische veeltermen in de ε_j. Dan zijn de b_1 volgens de hoofdstelling over de symmetrische polynomen gehele veeltermen van de a_1 dus zeker geheel.

Ik kan de stelling over de congruenties toepassen.

$$b_j = \sigma_j(\varepsilon_1^p, \ldots, \varepsilon_k^p) \equiv (\sigma_j(\varepsilon_1, \ldots, \varepsilon_k))^p = a_j^p \equiv a_j \pmod p$$

Hieruit volgt $f(x) = g(x) + p \cdot h(x)$.
$f(x)$ is irreducibel. $f(x)$ is dus een deler van $g(x)$ of $f(x)$ en $g(x)$ zijn onderling deelbaar.
Veronderstel $f(x)$ en $g(x)$ onderling ondeelbaar. Aangezien alle wortels van $g(x)$ n^e eenheidswortels zijn is $g(x)$ evenals $f(x)$ een deler van $x^n - 1$.

$x^n - 1 = f(x) \cdot g(x) \cdot k(x)$. Afgeleide nemen geeft:
$nx^{n-1} = f'(x) \cdot g(x) \cdot k(x) + f(x) \cdot g'(x) \cdot k(x) +$
$+ f(x) \cdot g(x) \cdot k'(x)$.

Dus $n \cdot x^{n-1} = f'(x) \cdot ((f(x) - p \cdot h(x)) \cdot k(x) +$
$+ f(x) \cdot g'(x) \cdot k(x) + f(x) \cdot g(x) \cdot k'(x)$. Omordenen geeft:
$n \cdot x^{n-1} = f(x) \cdot Q(x) + p \cdot R(x)$. Hierbij mag ik veronderstellen dat alle coëfficiënten in $Q(x)$ onderling ondeelbaar zijn met p.

$$n \cdot x^{n-1} = (x^k + a_1 x^{k-1} + \ldots \pm 1)(c_p x^r + \ldots + c_s x^s) + p \cdot R(x).$$

Er zijn nu twee mogelijkheden:

1e) $Q(x) = 0$. Dan geldt: $n \cdot x^{n-1} = p \cdot r(x)$.
Dit is in strijd met p geen deler van n.

2e) $Q(x) \neq 0$. Nu zijn er in het rechterlid twee coëfficiënten aan te wijzen die niet deelbaar zijn door p (nl. die van de graad k+r en van de graad s) terwijl links maar één coëfficiënt is die niet door p deelbaar is. De afgeleide identiteit voert dus tot een tegenspraak.

We mogen dus niet veronderstellen dat f(x) en g(x) onderling ondeelbaar zijn. Aangezien f(x) een deler van g(x) moet zijn terwijl de graad gelijk is en ze beiden een coëfficiënt 1 hebben voor de hoogste term zijn f(x) en g(x) gelijk.

Nu volgt de irreducibiliteit van $\Phi_n(x)$.
Aangezien die irreducibele factor f(x) van $\Phi_n(x)$ waarvan $e^{\frac{2\pi i}{n}}$ een wortel is ook $e^{\frac{2\pi i}{n}\cdot p_1 \cdot p_2 \cdots p_s}$ als wortels heeft (waarbij p_i geen geen deler van n is) zijn alle primitieve n^e eenheidswortels wortel van deze irreducibele factor.
Dus $f(x) \mid \Phi_n(x)$ en $\Phi_n(x) \mid f(x)$ zodat $f(x) = \Phi_n(x)$ waarmede het bewijs is voltooid.

Tenslotte de Galoisgroep $G\left[Q(e^{\frac{2\pi i}{n}})/Q\right]$.

Ieder automorfisme voert de primitieve eenheidswortel $e^{\frac{2\pi i}{n}}$ over in een andere primitieve eenheidswortel $e^{\frac{2\pi i}{n}.k}$ (waarbij (k,n) = 1). Deze operatie bepaalt het gehele automorfisme. Voor iedere k die met n onderling ondeelbaar is geeft deze operatie een automorfisme van $Q(e^{\frac{2\pi i}{n}})$. Noem dit automorfisme σ_k.
Dan kan men eenvoudig inzien:

$$\sigma_k = \sigma_{k'} \iff k \equiv k' \pmod{n}$$

en

$$\sigma_k \cdot \sigma_m = \sigma_{k.m}$$

Hieruit valt af te leiden dat de automorfismengroep homeomorf is met de multiplicatieve groep van onderling ondeelbare restklassen modulo n. Dit is als bekend uit de getallentheorie een abelse groep van $\varphi(n)$ elementen. Hierbij is $\varphi(n)$ de indicator van Euler.

§12. Vraagstukken over lineaire algebra en Galoistheorie

I. Vectorruimten

1) V is de vectorruimte, bestaande uit alle homogene tweedegraads-veeltermen in x en y, met coëfficiënten uit R.
Het endomorfisme σ is gedefiniëerd door $\sigma(f) = (x+y)\frac{\partial f}{\partial x} + (x-y)\frac{\partial f}{\partial y}$.

a) Welke dimensie heeft V? geef een basis voor V.

b) Bepaal Im σ en Ker σ.

c) Los op: $\sigma(f) = x^2 + y^2$
$\sigma(g) = x^2 - y^2$.

2) Gegeven het stelsel vergelijkingen:

$$\begin{aligned} x + (2\alpha-3)y + (\alpha-2)z - t &= 2 \\ (\alpha+1)x + (\alpha-3)y - 2z + (1-\alpha)t &= 0 \\ x - 2y - 2z &= -2 \\ (1-\alpha)x + (3\alpha-3)y + (2\alpha-2)z - t &= 4 \end{aligned}$$

a) Voor welke waarden van α is er niet precies één oplossing? Bepaal in deze gevallen alle oplossingen van het stelsel vergelijkingen.

3) De afbeelding σ: $R^3 \to R^3$ zij als volgt gedefiniëerd:

$\sigma(x_1, x_2, x_3) = (3x_1-x_2, x_1+x_2, x_1)$.

a) Bewijs dat σ een lineaire afbeelding is.

b) Geef de matrix aan die bij σ behoort.

4) Zij σ de lineaire afbeelding van R^3 in R die bepaald wordt door:

Ker $\sigma = \{(x,y,z)/x + 2y + z = 0\}$
$\sigma((1,1,1)) = 1$.

Bepaal $\sigma((3,6,2))$.

II. Groepentheorie.

1) Bewijs dat de matrices van de vorm $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ (met $r \in R$) met de matrixvermenigvuldiging als operatie een groep vormen.
Met welke groep is deze groep isomorf?

2) Men beschouwt in R^2 de transformaties $f_{n,m}$ gedefiniëerd door:

$$f_{n,m}((x,y)) = ((-1)^n x+m, y+n), \text{ n en m geheel.}$$

Bewijs dat deze transformaties een groep vormen.

3) Gegeven zijn de volgende groepen:
A is de optelgroep der gehele getallen.
B is de multplicatieve groep der positieve reële getallen.
C is de optelgroep der reële getallen.
D is de oneindige cyclische groep.
E is de optelgroep der rationale getallen.

Welke van deze groepen zijn isomorf?.

4) Bepaal alle ondergroepen van de symmetrische groep S_3.

5) Zij G de groep van alle congruente afbeeldingen van het vlak op zichzelf, en zij H_1 de ondergroep van alle rotaties om de oorsprong, en H_2 de ondergroep van alle translaties.

a) Is H_1 normaaldeler van G?
b) Is H_2 normaaldeler van G?

Aanwijzing: Bewijs eerst, dat elke congruente afbeelding φ te schrijven is als het product van 1) een spiegeling s om de x-as; 2) een rotatie r om de oorsprong en 3) een translatie t; dus $\varphi = t \cdot r \cdot s$.

6) Zij G de groep van alle congruente afbeeldingen van een kubus op zichzelf, die één hoekpunt invariant laten.

Geef een voorstelling van G als permutatiegroep van de hoekpunten.

7) Zij G de multiplicatieve groep van alle rationale getallen van de vorm $2^k\ 3^m\ 5^n$ (k, m en n geheel) en laat H de ondergroep zijn, die bestaat uit alle getallen 2^k.

Beschrijf de nevenklassen van H in G.
Waarmee is de factorgroep G/H isomorf?

III. Galoistheorie

1) Bewijs, dat de Galoisgroep van de vergelijking $x^4 - 5 = 0$ t.o.v. Q(i) cyclisch is. Beschrijf de Galoisgroep t.o.v. Q.

2) Laat zien, dat de vergelijking $x^3 - 3x + 1 = 0$ normaal is, door de wortels rationaal in één er van uit te drukken. Beschrijf de automorfieën van het ontbindingslichaam.

3) Bewijs, dat de vergelijking $x^4 - 2x^3 + 9$ irreducibel is over Q.

4) Bewijs, dat de symmetrische groep S_3 oplosbaar is.

5) Als f(x) een irreducibele veelterm van de derde graad voorstelt, wat zijn dan de mogelijkheden van de Galoisgroep van f(x).

6) Bepaal de graden van de ontbindingslichamen van de volgende polynomen over Q:

a) $x^4 + 4x^3 + 6x^2 + 4x + 2$.
b) $x^4 - 6x^3 + 4x^2 - 6x + 3$.
c) $x^4 - 2x^3 + 5x^2 - 4x + 6$.

d) $x^3 - 3x^2 - 10x + 24$.

e) $x^3 - 2x^2 + x - 1$.

7) Bewijs, dat het ontbindingslichaam van een polynoom van de graad n hoogstens de graad $n!$ heeft.

8) Beschrijf volledig de correspondentie Ondergroepen-Deellichamen van het lichaam $Q(i, \sqrt[4]{3})$ over Q.

9) Bewijs, dat $Q(\beta)$ niet normaal is over Q, als β een willekeurige wortel is van $x^4 - 32x + 2 = 0$.

IV. Construeerbaarheid

1) Voor welke van de volgende hoeken is de trisectie mogelijk?

a) $\frac{\pi}{85}$ rad.

b) arc cos $\frac{11}{25}$ $\sqrt{5}$

c) arc cos -115/128

d) $\frac{\pi}{3}$ rad.

e) arc cos 3/16

f) $\frac{7\pi}{13}$ rad.

g) $\frac{13\pi}{8738}$ rad.

2) Constructie van de vijfhoek. Stel $z_i = e^{\frac{2\pi i}{5}}$.
Bewijs dat: $z_1 + z_2 + z_3 + z_4 = -1$ en dat $(z_1+z_4)(z_2+z_3) = -1$.
Laat zien hoe hieruit een constructie van de vijfhoek is af te leiden.

Oplossingen.

I.

1) a) Dim V = 3; Basis: x^2; xy; y^2.

   b) Im σ = H(x^2+xy; xy-y^2); Ker σ = H(x^2 - 2xy - y^2).

   c) xy$\oplus$H(x^2-2xy+y^2); geen oplossing.

2) a) α = 0; α = 1; α = 2.

   b) α = 0: geen oplossing; α = 1: geen oplossing;

   α = 2: (2,0,3,0)$\oplus$H(1,0,1,1).

3) b) $\begin{pmatrix} 3 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

4) $4\frac{1}{4}$.

II.

1) Isomorf met R.

2) $f_{l,p} \circ f_{n,m} = f_{l+n,(-1)^l m+p}$.

3) A $\simeq$ D (beschouw in A 1 als generator). B $\simeq$ C (logarithme).

4) (1); (1),(12); (1),(13); (1),(23); (1),(123),(132); en S_3 zelf.

5) a) neen; b) ja.

6) Als $\begin{matrix} EFGH \\ ABCD \end{matrix}$ de kubus is, met A invariant, dan S_3 over (B,D,E).

7) a) De nevenklassen zijn van de vorm: $2^k\ 3^m\ 5^n$, met vaste n en m en variabele k. De factorgroep is isomorf met de groep $3^n\ 5^m$.

III.

1) De ondergroep van S_4 die gegenereerd wordt door de elementen (1234) en (12) is isomorf met de gevraagde groep.

2) $x_i = x_1$; $x_2 = x_1^2 - 2$; $x_3 = x_1^4 - 4x_1^2 + 2$.
   De Galoisgroep is isomorf met de even permutaties van S_3: A_3.

4) $S_3 \supset A_3 \supset \{e\}$.

5) S_3 of A_3.

6) a) 4; b) 4; c) 2; d) 1; e) 6.

IV.

1) a) ja; b) ja; c) ja; d) nee; e) ja; f) ja; g) ja.

2) Door constructie van (z_1+z_4) en (z_2+z_3) uit de vergelijking $x^2 - x - 1 = 0$.

Colloquium "Lineaire algebra en Galois-theorie"

Geschiedkundig Supplement

Bijeenkomst van 16 maart 1966

Spreker: Tj.S. Visser

1811 - E. GALOIS - 1832

Literatuur:

(1) D.S. Kasir, The Algebra of Omar Khayyam (New York, 1931)

(2) E. Bortolotti, I contributi del Tartaglia, del Cardano, del Ferrari, e della scuola matematica bolognese alla teoria algebrica delle equazioni cubiche (Imola, 1926)

(3) F. Viète (Vieta, décodeerde voor Henri IV secrete spaanse dépeches) In artem analyticam isagoge (1591)

(4) J.L. Lagrange, Réflexions sur la résolution algébrique des équations, 1770-1 in de Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin

(5) N.H. Abel, Unmöglichkeit der Auflösung der Gleichungen fünften Grades durch Wurzelzeichen (Crelle's Journal, Bd I, 1826)

(6) E. Galois, Mémoire sur la théorie des équations (met Discours préliminaire) (1830; publ. Liouville 1846; zie ook (7) -)

(7) R. Bourgne et J.P. Azra, Ecrits et mémoires mathématiques d'Evariste Galois. Edition critique et intégral de ses manuscripts et publications (Parijs, 1962. Met voorwoord van Dieudonné)

(8) G. Verriest, Evariste Galois et la théorie des équations algébriques (Leuven, 1934)

(9) (G. Boole, Mathematical Analysis of Logic) (1848)

(10) F. Klein, Vorlesungen über das Ikosaëder und die Auflösung der Gleichung vom fünften Grade (Heidelberg, 1884)

(11) G.A. Miller, History of the theory of Groups to 1900

(12) E.T. Bell, Men of Mathematics (New York, 1937)
(13) D.J. Struik, A concise history of mathematics (New York, 1948)
(14) G. Helmberg, Mathematicus Scribens; oratie Eindhoven, 1966

Enige citaten

- E. Galois, Discours préliminaire, zie (6): "Si maintenant vous me donnez une équation que vous aurez choisie à votre gré et que vous désiriez connaître si elle est ou non soluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot, les calculs sont impraticables".
- Verriest over Galois, zie (8), blz. 58: "Tant par le résultat obtenu que par les considérations qui y conduisent, (sa) découverte est peut-être la plus grande qui ait jamais été faite dans le domaine de l'algèbre".
- Dieudonné over Galois in (7), Voorwoord: "Ses idées sont à la source même de l'Algèbre moderne".
  "On est frappé de l'allure étrangement moderne de sa pensée, son insistance sur le caractère conceptuel des mathématiques, son aversion pour les longs calculs masquant les idées directrices, son souci de grouper les problèmes selon leurs affinités profondes de structure ( ), tout cela nous est maintenant familier".
  "Il était parvenu à l'essentiel de la théorie des intégrales abéliennes, telle que Riemann devait les développer 25 ans plus tard".
- G.A. Miller in Finite Groups, blz. 85 (1916): "Abel and Galois solved two fundamental problems in the theory of equations by means of substitution groups, and thus they directed attention to the usefulness of this subject (Cf Part III)". Noot van Tj.S.V.: in dat Part III behandelen Miller c.s. de 3 antieke problemen; de buigpunten van een kubiek; de 28 bitangenten aan een quartiek; de 27 rechten op het derdegraads oppervlak. Verg. ook (10).

- Struik, zie (13), blz. 223/4: "This mess ("ce gâchis") contained no less than the theory of groups, the key to modern algebra and to modern geometry".
  "We may speculate on the possibility that if Galois had lived, modern mathematics might have received its deepest inspiration from Paris and the school of Lagrange rather than from Göttingen and the school of Gauss".
- Klein in "Entwicklung", I, blz. 89, over Galois:
  "Des Ausgabe (Liouville's, in 1846, Tj.S.V.) ist ein Porträt der jugendlichen Autors beigegeben, dessen Knabenhaft kecker, fast mutwilliger Ausdruck den seltsamsten Gegensatz bildet zu dem wunderbar tiefgehenden, dabei völlig klaren, reif durchgebildeten Text des Werkes. Dieser Gegensatz veranschaulicht der inneren Widerspruch, an dem Galois zugrunde gegangen ist. Eine unerhörte Frühreife, verbunden mit einem nicht zu bändigendem Temperament, dass sich keiner Ordnung, keiner Regel fügen wollte, eine Leidenschaftlichkeit des Wesens, die sich selbst verzehrte, lassen ihn als den typischen Vertreter des ungeordneten, echt französischen Genies erscheinen".
  Noot van Tj.S.V.: het portret is van een 15-jarige, zie (7). Wie zich verbaast over de lichtzinnige algemeenheid van Klein's slotwoorden, bedenke dat de Vorlesung, in zijn woning en voor een kleine kring, gehouden werd in oorlogsjaar 1915.
- Verriest in (8), blz. 45: "..... en arithmétique on fait des opérations déterminées sur des nombres déterminés, en algèbre on fait des opérations déterminées sur des nombres non déterminés, dans la théorie des groupes abstraits on étudie des opérations non déterminées effectuées sur des objects non déterminés".

Enige jaartallen

ca 100 : 2-de graads vergelijking reeds bij Heron, Alexandrië.
ca 1000: de dichter, astronoom en wiskundige Omar Khayyam (= Tentmakers) te Merv, Perzië, over de 3-de graads vergelijking.
ca 1150: Gerhard van Cremona vertaalt te Toledo veel uit het arabisch, o.a. over algebra.

ca 1500 : Europa leert boekdrukkunst en ontdekt Amerika.
1515 : Scipio del Ferro, van de befaamde universiteit te Bologna, vindt de oplossing der 3-de graads vergelijking.
1535 : Tartaglia (= de Stotteraar) idem.
1545 : Cardano idem; noemt Tartaglia.
1540 : Tartaglia lost de 4-de graads vergelijking op.
1770 : Lagrange publiceert (4).
1777 : Gauss geboren.
1789 : Cauchy geboren.
1801 : Gauss en de regelmatige 17-hoek.
ca 1820 : Rage der 5-de graads vergelijking (verg. de pi-rage).

1802-1829: Niels Henrik Abel, Noor.
1811-1832: (mei): Evariste Galois.

1815 : Boole geboren, Brit.
1826 : Abel publiceert (5).
1830 : Galois stuurt (6) in.
1846 : Liouville publiceert (6), na veel vlijt en aandrang van broer A. Galois en vriend A. Chevalier.
(1848 : Boole's brochure (9) -)
(1870 : G. Cantor begint te publiceren over Verzamelingenleer.)

Wat Abel en Galois gemeen hadden

Tijdvak der romantiek. Merkwaardige moeder (A: mooi en vrolijk als haar zoon; G: geleerd en paradoxaal; overleefde haar zoon 40 jaar). Lazen jong Lagrange en "losten" met 16 jaar de 5-de graads vergelijking "op", doch natuurlijk fout.
A overleed aan armoe en tering, G aan domheid en onrust (verg. (12): Genius and Poverty; Genius and Stupidity).
Wat A bewees voor de 5-de graads vergelijking, bewees G voor elke graad, tevens aanwijzend wanneer "oplossing" toch weer wel mogelijk.
Van beiden gingen waardevolle manuscripten teloor op een hooggeleerde tafel; o.a. op Cauchy's tafel.(A 24-10-1826 aan Holmboe: "Cauchy est fou" (C is gek)).

A had als grote vriend Crelle; G als bescheiden vrienden leraar Richard en makker Chevalier.
Beiden openden een weg in de functie-theorie, verg. Abel met Jacobi en Galois met Riemann.

- S. Lie over A en G (in 1897): Die Mathematiker unserer Zeit werden erst durch das Studium von Abel's durchsichtigen und tiefen Untersuchungen in den Stand gesetzt, Galois' ebenso schwer zugaengliche als tiefe Ideen zu verstehen.

Het Frans heeft voor wortel en wortel naar behoren twee woorden: racine en radical.

Uit het korte leven van Evariste Galois

1811: oktober, geb. te Bourg-la Reine bij Parijs.
Vader hield een jongens-pensionaat.
1815: (de 100 dagen) Vader wordt burgemeester.
1828: Eerste publicatie, als lyceïst; door Cauchy zoekgemaakt.
1829: Tweemaal afgewezen voor de beroemde Ecole Polytechnique.
1829: naar de Ecole normale.
1830: vandaar verwijderd.
1830: Secretaris der Académie overlijdt waardoor weer een manuscript zoek.
1830: in conflict met de politieke politie, En zie (6).
1831: Poisson stuurt manuscript terug als onbegrijpelijk.
1831: 8 maanden in het gevang, bespot door geboefte.
1832: wegens slechte gezondheid op erewoord beperkt vrij.
1832: nacht van 29 op 30 mei: schrijft inderhaast zijn wetenschappelijk testament (aan Chevalier, bestemd voor Jacobi en Gauss. - Zie in (7) de 7 blz. die beginnen met blz. 173. P.M.: "ce gâchis"; gâchis = rommel; smeerboel; metselspecie.)
1832: 30 mei: blijft na duel liggen met buikwond;
31 mei: sterft aan buikvliesontsteking in het ziekenhuis.
Tot zijn jongere broer: "Ne pleure pas, j'ai besoin de tout mon courage pour mourir à vingt ans".

Dichtregels van G. tussen zijn calculaties:
"L'éternel cyprès m'environne: / Plus pâle que la pâle automne, /
Je m'incline vers le tombeau".

Over de onbekende, x (zie M. Cantor, Geschichte, I)

Arabisch : sjai (ding); dzjidz (wortel).
Hindoe : yaavat - taavat.
Latijn : tantum quantum (!); ook radix.
Italiaans: cosa (de "cossisten").