stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE

ZC 86/72 AUGUSTUS

L.C.A. VAN LEEUWEN
CURSUS ALGEBRA 1971-1972

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

Inhoud

Cursus Algebra

door

L.C.A. van Leeuwen

I. Definitie van een groep en voorbeelden.

Het basis-begrip voor de groepentheorie is het begrip verzameling, dat we hier niet zullen definiëren. De objecten, die een gegeven verzameling bepalen, heten de elementen van die verzameling. Verzamelingen worden met hoofdletters aangeduid, hun elementen met kleine letters. Voor de volgende verzamelingen gebruiken we speciale letters:

Z is de verzameling van gehele getallen;
Q is de verzameling van rationale getallen;
R is de verzameling van reële getallen.

Als x een element is van A, dan noteren we dit met $x \in A$ (lees: x behoort tot A). Als x niet tot de verzameling A behoort, schrijven we: $x \notin A$.
De verzameling A heet een deelverzameling van de verzameling S als $a \in A$ impliceert $a \in S$. We noteren dit door $A \subseteq S$ (lees: A is bevat in S).
Als S een gegeven verzameling is, dan gebruiken we de notatie:
$A = \{a \in S \mid P(a)\}$ voor:
A is de verzameling van alle elementen in S waarvoor de eigenschap P geldt. Bezit geen element $a \in S$ de eigenschap P, dan is
$A = \{a \in S \mid P(a)\}$ de zg. lege verzameling, aangeduid door $\emptyset$.
De vereniging van de twee verzamelingen A en B (notatie: $A \cup B$) definieren we door:

$$A \cup B = \{x \mid x \in A \text{ of } x \in B\}.$$

Syll. ZC 86, afl. 1!

De doorsnede van de twee verzamelingen A en B, geschreven als $A \cap B$, is per definitie

$$A \cap B = \{x \mid x \in A \text{ en } x \in B\}.$$

Nog een constructie van een verzameling uit twee gegeven verzamelingen is het Cartesisch product.
Laat A en B twee verzamelingen zijn. Het Cartesisch product van A en B is de verzameling

$$A \times B = \{(x,y) \mid x \in A \text{ en } y \in B\}.$$

Dus $A \times B$ is de verzameling van alle geordende paren (x,y) met $x \in A$ en $y \in B$. Het paar (x_1,y_1) is gelijk aan het paar (x_2,y_2) dan en slechts dan als $x_1 = x_2$ en $y_1 = y_2$.
Als S een willekeurige verzameling is, noemen we een afbeelding van $S \times S$ in S een binaire bewerking (operatie) op S. Als $\tau: S \times S \to S$ een binaire operatie is, dan voegt τ aan elk geordend tweetal elementen $x,y \in S$ één derde element $(x,y)\tau \in S$ toe.
Na deze voorbereidingen kunnen we nu de definitie van een groep geven.

Definitie 1.1. Laat G een niet-lege verzameling zijn en τ een binaire operatie op G, d.w.z. $\tau: G \times G \to G$. We noteren het element $(a,b)\tau$ door $a * b$. De verzameling G met de operatie $*$ heet een groep als voldaan is aan de volgende axioma's:

(1) $*$ is associatief, d.w.z., $a * (b*c) = (a*b) * c$ voor alle $a,b,c \in G$.

(2) er is een element $e \in G$ zodat $a * e = e * a = a$ voor alle $a \in G$ (het bestaan van een neutraal element in G).

(3) voor iedere $a \in G$ bestaat er een element $\bar{a} \in G$, zodat geldt: $a * \bar{a} = \bar{a} * a = e$ (het bestaan van een inverse $\bar{a}$ voor iedere a in G).

Geldt voor een verzameling V dat $a * b \in V$ voor alle $a,b \in V$ en een operatie $*$, op V gedefinieerd, dan noemt men V gesloten onder $*$. Iedere verzameling is gesloten met betrekking tot een binaire operatie, die er op is gedefinieerd. Dus als G een groep is met de operatie $*$, dan is G

gesloten onder de operatie *.
Is, behalve aan (1), (2), (3) nog voldaan aan
* is commutatief: $a * b = b * a$ voor alle $a,b \in G$,
dan noemt men G met de operatie * een commutatieve (of abelse) groep.
Om een groep te definiëren, kunnen we met minder volstaan dan de eisen (1), (2) en (3), Het is nl. voldoende om i.p.v. (2) en (3) het bestaan van een links-neutraal element resp. links-inverse te eisen:

(2') er is een element e, zodat $e * a = a$ voor alle $a \in G$.

(3') bij elke a is er een $\vec{a} \in G$, zodat $\vec{a} * a = e$.

Men kan nu aantonen, dat uit (1), (2') en (3') volgt dat e ook rechts-neutraal element is ($a*e=a$) en dat $\vec{a}$ rechts-inverse is ($a*\vec{a}=e$), zodat (1), (2) en (3) volgen. Omgekeerd impliceert het stelsel (1), (2), (3) natuurlijk dat (1), (2'), (3') geldig is. Men noemt de axiomastelsels (1), (2), (3) en (1), (2'), (3') gelijkwaardig.
Als de bewerking * wordt vervangen door +, spreekt men over een additieve groep. Het neutrale element e wordt dan vervangen door 0 en heet nul-element:

$a + 0 = 0 + a = a$; $\vec{a}$ vervangt men door $-a$:

$a + (-a) = (-a) + a = 0$.

In het geval dat * vervangen wordt door ·, spreekt men over een multiplicatieve groep. Men heeft:

$a \cdot e = e \cdot a = a$ voor alle $a \in G$ en men vervangt $\vec{a}$ door a^{-1}:

$a \cdot a^{-1} = a^{-1} \cdot a = e$.

Vele auteurs laten, bij multiplicatieve groepen, ook het bewerkingteken weg:

$(ab)c = a(bc)$

$ae = ea = a$

$aa^{-1} = a^{-1}a = e$.

Als het duidelijk is, welke de groeps-operatie is, spreekt men over de groep G i.p.v. de groep G met de operatie $*$.

Voorbeelden.

1. Z, Q en R vormen additieve groepen t.o.v. de gewone optelling. Deze groepen zijn abels.

2. De verzamelingen $Q \setminus \{0\}$, $R \setminus \{0\}$ vormen multiplicatieve groepen t.o.v. de gewone vermenigvuldiging. Ook deze groepen zijn abels.

3. Laat $x \in R \setminus \{0\}$. Beschouw de functies

$$f_1(x) = x,\ f_2(x) = \frac{1}{x},\ f_3(x) = -x,\ f_4(x) = -\frac{1}{x}$$

met definitie-gebied $R - \{0\}$. T.o.v. de operatie $(f_i * f_k)(x) = f_i(f_k(x))$ voor $1 \leq i, k \leq 4$ vormen deze functies een commutatieve groep met 4 elementen. Bij een eindige groep noemt men het aantal elementen de orde van de groep. Bovenstaande groep is dus een groep van de orde 4.

4. Een ander voorbeeld van een comm. groep van de orde 4 is het volgende.
Beschouw van een vierkant de 4 rotaties d_0, $d_{\pi/2}$, d_π en $d_{3\pi/2}$ om het centrum over resp. 0, $\pi/2$, π en $3\pi/2$, die het vierkant in zich zelf overvoeren.
Voor deze verzameling is de groepsoperatie "het na elkaar uitvoeren van de rotaties", bijv.

$$d_{\pi/2} * d_\pi = d_{3\pi/2},\ d_{3\pi/2} * d_\pi = d_{\pi/2} \text{ etc.}$$

Men heeft, als we $d_{\pi/2}$ voorstellen door d:

$$d_{\pi/2} = d,\ d_\pi = d^2,\ d_{3\pi/2} = d^3,\ d_0 = d^4.$$

5. Beschouw de functies

$$f_1(x) = x,\ f_2(x) = \frac{1}{x},\ f_3(x) = 1-x,$$

$$f_4(x) = \frac{x-1}{x},\ f_5(x) = \frac{x}{x-1} \text{ en } f_6(x) = \frac{1}{1-x}$$

met definitie-gebied $R \setminus \{0,1\}$.
De groepsoperatie is dezelfde als in voorbeeld 3. T.o.v. deze operatie vormen de functies een niet-abelse groep van de orde 6. Men heeft bijv.

$$(f_2 \circ f_6)(x) = f_2(f_6(x)) = f_2(\tfrac{1}{1-x}) = 1-x = f_3(x)$$

en

$$(f_6 \circ f_2)(x) = f_6(f_2(x)) = f_6(\tfrac{1}{x}) = \frac{1}{1-1/x} = \frac{x}{x-1} = f_5(x).$$

Dus $f_2 \circ f_6 \neq f_6 \circ f_2$.

6. Laat k een vast geheel getal zijn. Dan is $Z_k = \{n \mid n \in Z;\ n = k\text{-voud}\}$ een groep t.o.v. de gewone optelling van gehele getallen.

Definitie. Laat $n > 0$ een vast geheel getal zijn. We definiëren $a \equiv b \bmod n$ voor $a,b \in Z$ als $n \mid a - b$. Lees voor "$a \equiv b \bmod n$": a is congruent met b modulo n. De relatie heet congruentie modulo n. Bijv. $41 \equiv 3 \bmod 19$, $-9 \equiv 21 \bmod 10$ enz.
De congruentie-relatie (modulo n) heeft de volgende eigenschappen:

a) Congruentie modulo n bepaalt een equivalentie-relatie op de verzameling Z.
b) Deze equivalentie-relatie heeft n verschillende equivalentie-klassen.
c) Als $a \equiv b \bmod n$ en $c \equiv d \bmod n$, dan is $a + c \equiv b + d \bmod n$ en $ac \equiv bd \bmod n$.

Eigenschap a) is direct duidelijk. Geef de equivalentie-klasse, waartoe a behoort, aan door [a]. Dus, voor $b \in Z$, geldt $b \in [a] \longleftrightarrow b \equiv a \bmod n$. Volgens de delingsalgorithme geldt voor een willekeurige $c \in Z$ dat $c = kn + r$ met $0 \leq r < n$. Dus $c \in [r]$ en $[c] = [r]$. Er zijn dus ten hoogste n verschillende congruentie-klassen nl. [0], [1], ..., [n-1]. Deze zijn echter 2 aan 2 verschillend, want als $[i] = [j]$ met bijv. $0 \leq i < j < n$, dan is $n \mid (j-i)$, terwijl $0 < j-i < n$, hetgeen onmogelijk is. Dus zijn er precies n verschillende congruentie-klassen [0], [1], ..., [n-1].
Om c) te bewijze, stellen we dat $a \equiv b \bmod n$ en $c \equiv d \bmod n$, dus $n \mid (a-b)$ en $n \mid (c-d)$. Hieruit volgt $n \mid \{(a-b) + (c-d)\}$ of

$n \mid \{(a+c) - (b+d)\}$. Dan geldt $a + c \equiv b + d \bmod n$. Ook is $n \mid \{(a-b)c + (c-d)b\}$ of $n \mid (ac-bd)$, zodat $ac \equiv bd \bmod n$.
Laat $J_n = \{[0], [1], \ldots, [n-1]\}$. Voor $[i], [j] \in J_n$ definieert men: $[i] + [j] = [i+j]$. Deze "optelling" van congruentie-klassen is zinvol, want als $[i] = [i']$ en $[j] = [j']$, dan is $i \equiv i' \bmod n$ en $j \equiv j' \bmod n$, dus $i + j \equiv i' + j' \bmod n$ of $[i+j] = [i'+j']$. Er volgt $[i] + [j] = [i+j] = [i'+j'] = [i'] + [j']$.
J_n heet de verzameling van gehele getallen mod n. T.o.v. de juist gedefinieerde operatie vormt deze verzameling een commutatieve groep van de orde n.

7. Een permutatie van een verzameling A is een 1-1-afbeelding van A op zichzelf. Is A eindig, bijv. $A = \{a_1, a_2, \ldots, a_n\}$, dan noteert men een permutatie P van A door: $P = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{i_1} & a_{i_2} & \ldots & a_{i_n} \end{pmatrix}$, waarbij $a_1 \to a_{i_1}$ etc., $i_1, \ldots, i_n$ doorlopen de getallen 1, ..., n. Men kan de a weglaten en A opvatten als verzameling $\{1, 2, \ldots, n\}$, zodat $P = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$. Bijv. $A = \{1, 2, 3, 4\}$, dan is $P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ een permutatie van A. Het aantal verschillende permutaties van $(1,2,\ldots,n)$ is $n!$.

Permutaties kan men "samenstellen", hetgeen we toelichten aan de hand van een voorbeeld. Met $P_2 \circ P_1$ wordt bedoeld: pas eerst P_2 toe en op het resultaat P_1. Bijv. $A = \{1, 2, 3, 4, 5\}$;
$P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$, $P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$, dan is $P_2 \circ P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$.
Men kan aantonen, dat de permutaties van n elementen t.o.v. deze operatie $\circ$ van het samenstellen een groep vormen, de z.g. symmetrische groep S_n van de orde n! Het neutrale element van S_n is de identieke permutatie, die ieder element invariant laat. S_n is commutatief voor $n \leq 2$ (voor $n = 1$ bestaat de groep alleen uit het neutrale element) en niet-commutatief voor $n > 2$. In bovenstaand voorbeeld geldt: $P_1 \circ P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$, dus $P_2 \circ P_1 \neq P_1 \circ P_2$.

8. Uit twee gegeven groepen A en B kan men als volgt een nieuwe groep vormen:
De geordende paren (a,b), $a \in A$, $b \in B$ zijn de elementen van een groep, als we de groepsoperatie $*$ definiëren door

$$(a_1,b_1) * (a_2,b_2) = (a_1.a_2,\ b_1 \circ b_2),$$

waarin $.$ de operatie is in de groep A en $\circ$ de operatie in de groep B. De nieuwe groep heet het direkte product van A en B. Merk op dat de verzameling, waarop het direkte product is gedefinieerd, het Cartesisch product van de verzamelingen A en B is. Met weglaten van de groepsoperatie wordt het direkte product van de groepen A en B aangegeven door $A \times B$. $A \times B$ is een commutatieve groep dan en slechts dan als zowel A als B commutatieve groepen zijn. Als A en B eindig zijn met orden p resp. q, dan is $A \times B$ ook eindig en de orde van $A \times B$ is pq.

II. Elementaire gevolgen van de definitie van een groep.

Stelling 2.1. In iedere groep G bestaat één en precies één element e zodat $a*e = e*a = a$ voor alle $a \in G$.

Bewijs. Dat er zo'n element e is in G volgt uit de definitie van een groep. Stel nu e en e' zijn neutrale elementen in G, dan is $e'*e = e'$ en $e'*e = e$, dus $e = e'$.

Stelling 2.2. G is een groep en $a,b,c \in G$. Dan geldt:
$a*b = a*c \Longrightarrow b = c$ en $b*a = c*a \Longrightarrow b = c$
(vereenvoudigingswet).

Bewijs. Als $a*b = a*c$, dan is $\overrightarrow{a} * (a*b) = \overrightarrow{a} * (a*c)$ of
$(\overrightarrow{a}*a) * b = (\overrightarrow{a}*a) * c$ of $e*b = e*c$ i.e. $b = c$.
Evenzo $b*a = c*a \Longrightarrow (b*a) * \overrightarrow{a} = (c*a) * \overrightarrow{a} \Longrightarrow b * (a*\overrightarrow{a}) =$
$= c * (a*\overrightarrow{a}) \Longrightarrow b*e = c*e$ i.e. $b = c$.

Stelling 2.3. Als $a \in G$, G een groep, dan is er precies één element $\overrightarrow{a} \in G$ zodat $a*\overrightarrow{a} = \overrightarrow{a}*a = e$.

Bewijs. Stel $b*a = c*a = e$ en $a*b = a*c = e$ voor $a,b,c \in G$. Dan geldt, volgens St.2.2, $b = c$. Volgens de definitie van een groep voldoet $\overrightarrow{a}$ aan $a*x = x*a = e$. Dus $\overrightarrow{a}$ is het enige element in G dat voldoet.

Gevolg 2.4. (i) Als $a \in G$, dan is $(\overrightarrow{a})^{\rightarrow} = a$
(ii) Als $a,b \in G$, dan is $\overrightarrow{a*b} = \overrightarrow{b}*\overrightarrow{a}$.

Bewijs. (i) Het element $(\overrightarrow{a})^{\rightarrow}$ is het enige element in G dat voldoet aan $\overrightarrow{a}*x = x*\overrightarrow{a} = e$(st.2.3).
Ook geldt $\overrightarrow{a}*a = a*\overrightarrow{a} = e$. Dus $(\overrightarrow{a})^{\rightarrow} = a$.
(ii) Het bewijs van (ii) verloopt analoog.

Opmerking. Voor multiplicatieve groepen heeft men dus $(a^{-1})^{-1} = a$; voor additieve groepen geldt $-(-a) = a$ (iedere $a \in G$).
Evenzo heeft men voor mult. resp. add. groepen:
$(ab)^{-1} = b^{-1}a^{-1}$ resp. $-(a+b) = (-a) + (-b)$.

Er zijn vele andere mogelijke, logisch equivalente, definities van een groep.

De nu volgende stelling geeft zo'n alternatief.

Stelling 2.5. Laat G een niet-lege verzameling zijn en $\circ$ een binaire operatie op G die voldoet aan

a) $a \circ (b \circ c) = (a \circ b) \circ c$ voor alle $a,b,c \in G$.

b) de vergelijking $a \circ x = b$ heeft een oplossing in G voor alle $a,b \in G$.

c) de vergelijking $y \circ a = b$ heeft een oplossing in G voor alle $a,b \in G$.

Dan is G met de operatie $\circ$ een groep en iedere groep G met operatie $\circ$ voldoet aan a), b) en c).

Bewijs. Om st. 2.5 te bewijzen moet men aantonen dat het axioma-stelsel a), b), c) gelijkwaardig is met het stelsel 1), 2), 3) van definitie 1.1. Stel a), b) en c) zijn geldig. Wegens a) = 1) is aan 1) voldaan. Nu heeft $y \circ a = a$ een oplossing bijv. $y = e$, dus $e \circ a = a$. Kies b willekeurig in G. De vergelijking $a \circ x = b$ heeft een oplossing, bijv. $x_1 \in G$. Dan is $e \circ b = e \circ (a \circ x_1) = (e \circ a) \circ x_1 = a \circ x_1 = b$ voor iedere $b \in G$.

Ook de vergelijking $a \circ x = a$ heeft een oplossing bijv. $x = e_1$, dus $a \circ e_1 = a$. Kies b' willekeurig in G. De vergelijking $y \circ a = b'$ heeft een oplossing, bijv. $y_1 \in G$. Dan is $b' \circ e_1 = (y_1 \circ a) \circ e_1 = y_1 \circ (a \circ e_1) = y_1 \circ a = b'$ voor iedere $b' \in G$.

Kies nu $b = e_1$ en $b' = e \Longrightarrow e \circ e_1 = e_1$ en $e \circ e_1 = e$.

Hieruit volgt $e = e_1$, zodat $e \circ b = b \circ e = b$ voor iedere $b \in G$.

Dus aan 2) is voldaan.

Stel nu $a \circ x = e$ heeft oplossing x_1 en $y \circ a = e$ heeft oplossing y_1. Dan volgt: $y_1 = y_1 \circ e = y_1 \circ (a \circ x_1) = (y_1 \circ a) \circ x_1 = e \circ x_1 = x_1$.

Dus, bij gegeven $a \in G$, is er een element $\bar{a}$ zodat $a \circ \bar{a} = \bar{a} \circ a = e$.

Aan 3) is voldaan.

Omgekeerd, neem aan dat 1), 2) en 3) geldig zijn. Aan a) is voldaan. De vergelijking $a \circ x = b$ heeft als oplossing $x = \bar{a} \circ b$, want $a \circ (\bar{a} \circ b) = (a \circ \bar{a}) \circ b = e \circ b = b$. Evenzo heeft de vergelijking $y \circ a = b$ als oplossing $y = b \circ \bar{a}$. Dus aan b) en c) is voldaan. Hiermee is de stelling bewezen.

Veronderstel weer: G met de operatie $\circ$ is een groep. Dan is voldaan aan b) en c) van stelling 2.5. Men kan nu bewijzen, dat de vergelijkingen $a\circ x = b$ en $y\circ a = b$ eenduidig bepaalde oplossingen hebben.
Het element $\vec{a}\circ b$ voldoet aan $a\circ x = b$ Stel nu dat er nog een element $x' \in G$ is zodat $a\circ x' = b$. Dan is $a\circ x' = a \circ (\vec{a}\circ b)$, dus $x' = \vec{a}\circ b$ (vereenvoudigingswet). Evenzo bewijst men dat $y = b\circ\vec{a}$ het enige element in G is, dat voldoet aan $y\circ a = b$.
Als G een eindige groep is met bijv. n elementen, dan kan men de n^2 uitkomsten, die men verkrijgt door alle "producten" $a \circ b (a,b \in G)$ te bepalen, opschrijven in een tabel, de z.g. vermenigvuldigingstabel. Deze tabel wordt gemaakt door de elementen van G, bijv. $a_1, a_2, \ldots, a_n$, in dezelfde volgorde verticaal en horizontaal te noteren. Op de $(i,j)^e$-plaats in het schema, d.w.z. het snijpunt van de i^e rij en j^e kolom staat het element $a_i \circ a_j (1 \leq i \leq n,\ 1 \leq j \leq n)$.
In een vermenigvuldigingstabel van een groep G komt ieder element uit G precies één keer voor in iedere rij en in iedere kolom. Immers, stel bijv. dat het element $b \in G$ twee keer voorkomt in de kolom van a_i. Dan zijn er elementen a_j, a_k in G met $a_j \neq a_k$ en zodat $a_j\circ a_i = a_k \circ a_i = b$. Maar de vergelijking $x\circ a_i = b$ heeft slechts één oplossing in G, dus b komt slechts één keer voor.

<u>Voorbeeld</u>. $G = S_3$ met elementen

$a_1 = \binom{123}{123}$, $a_2 = \binom{123}{213}$, $a_3 = \binom{123}{132}$, $a_4 = \binom{123}{321}$, $a_5 = \binom{123}{231}$ en

$a_6 = \binom{123}{312}$ (zie voorbeeld 7 in §1).

De vermenigvuldigingstabel voor S_3 is:

0	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_6	a_5	a_4	a_3
a_3	a_3	a_5	a_1	a_6	a_2	a_4
a_4	a_4	a_6	a_5	a_1	a_3	a_2
a_5	a_5	a_3	a_4	a_2	a_6	a_1
a_6	a_6	a_4	a_2	a_3	a_1	a_5 .

Een eindige groep G is commutatief dan en slechts dan als de corresponderende tabel symmetrisch is t.o.v. de hoofddiagonaal. Zoals we reeds gezien hebben is S_3 niet commutatief.
Men kan aantonen dat alle groepen met minder dan 6 elementen commutatief zijn. Dus een niet-commutatieve groep moet noodzakelijk 6 of meer elementen bevatten. Het bewijs hiervan kan reeds nu gegeven worden, maar volgt later gemakkelijker uit dan verkregen hulpmiddelen.
Laat $n > 6$ een gegeven natuurlijk getal zijn. Bestaat er een niet-commutatieve groep van de orde n? Het antwoord is dat niet voor iedere $n > 6$ een dergelijke groep bestaat. Bijv.: elke groep van de orde 7, van de orde 9 enz. is abels.
Veronderstel dat A een eindige verzameling is met n elementen ($n > 2$). Men kan een tabel maken volgens het schema van de vermenigvuldigingstabel, zodat in iedere rij en in iedere kolom van deze tabel precies één element van A voorkomt. Is dit dan een verm. tabel of m.a.w. heeft men op A een groepsstructuur gedefinieerd? Aan b) en c) van stelling 2.5 is voldaan. De associatieve wet is in het algemeen echter niet geldig, zodat aan a) niet voldaan behoeft te zijn. Dus de verkregen tabel is in het algemeen geen verm. tabel.

Voorbeeld: $n = 3$

0	a_1	a_2	a_3
a_1	a_2	a_3	a_1
a_2	a_1	a_2	a_3
a_3	a_3	a_1	a_2

Elke groep van de orde 3 is abels, zodat de verm. tabel symmetrisch is t.o.v. de hoofddiagonaal.
Nevenstaande tabel is dus geen groepstabel.

Men heeft bijv.: $(a_3^2)a_2 = a_2^2 = a_2$ en $a_3(a_3a_2) = a_3a_1 = a_3$.
Dus $(a_3^2)a_2 \neq a_3(a_3a_2)$, geen associativiteit.

III. Ondergroepen

Definitie 3.1. Laat $(G,*)$ een groep zijn en $H \subseteq G$ een niet-lege deelverzameling van G. Het paar $(H,*)$ (beperking van $*$ tot H) heet een ondergroep van $(G,*)$, als $(H,*)$ zelf een groep is.
Het is gemakkelijk in te zien dat iedere groep G tenminste twee ondergroepen heeft: de groep G zelf en de ondergroep bestaande uit één element, het neutrale element. Als H ondergroep is van G, maar $H \neq G$, d.w.z. $H \subset G$, dan heet H echte ondergroep van G. De groep G zelf en het neutrale element in G heten triviale ondergroepen van G.

Stelling 3.2. G is een groep en H is ondergroep van G.
Dan geldt:
a) het neutrale element van H is het neutrale element van G.
b) als $a \in H$ en $\overrightarrow{a}$ is de inverse van a in G, dan $\overrightarrow{a} \in H$ en $\overrightarrow{a}$ is de inverse van a in H.

Bewijs a) Als e het neutrale element in G is en e' dat van H, dan is $e' * e' = e'$ in H en dus in G. Dus in G geldt: $\overrightarrow{e'} * (e'*e') = \overrightarrow{e'} * e' = e$ of $(\overrightarrow{e'}*e') * e' = e$, zodat $e*e' = e$ of $e' = e$.

b) Stel $a \in H$ en b is de inverse van a in H. Dan is $a*b = e$, het neutrale element van zowel H als G. (a)). Dus in G geldt: $a*b = a*\overrightarrow{a}$, zodat $b = \overrightarrow{a}$ en $\overrightarrow{a} \in H$. Vaak ontstaat het probleem om te bepalen of een deelverzameling van elementen van een groep een ondergroep is t.o.v. de groepsoperatie. In het algemeen moeten dus de groepsaxioma's onderzocht worden voor de betreffende deelverzameling. Omdat de elementen van de deelverzameling elementen van de groep zijn, is de associatieve wet automatisch geldig. Men behoeft slechts het "gesloten zijn" d.w.z. $a*b \in H$ voor alle $a,b \in H$ aan te tonen en men moet aantonen dat $\overrightarrow{a} \in H$ voor iedere $a \in H$.
Als aan beide condities is voldaan, volgt direct, voor $a \in H$, dat $\overrightarrow{a} \in H$ en dus $a*\overrightarrow{a} = e \in H$. De voorwaarden zijn dus voldoende opdat H ondergroep is. Dat ze nodig zijn, is triviaal.
Men kan beide voorwaarden samenvatten in één enkele:

Stelling 3.3. H is een niet-lege deelverzameling van een groep G. Dan is H een ondergroep van G dan en slechts dan als $a,b \in H \Rightarrow a*\overrightarrow{b} \in H$ voor ieder paar $a,b \in H$.

Bewijs. Stel H is ondergroep van G. Dan volgt uit $a,b \in H$ dat $\overrightarrow{b} \in H$, dus $a*\overrightarrow{b} \in H$.
Omgekeerd, stel dat uit $a,b \in H$ volgt dat $a*\overrightarrow{b} \in H$. We tonen aan dat de groepsaxioma's gelden voor H.

1) H bevat e, het neutrale element van G. Want, omdat $H \neq \emptyset$, is er een element $a \in H$. Volgens onderstelling, met $b = a$, volgt $a*\overrightarrow{a} = e \in H$.
2) Voor iedere $a \in H$ geldt $\overrightarrow{a} \in H$. Want $e \in H$ (1)), dus voor iedere $a \in H$ volgt $e*\overrightarrow{a} = \overrightarrow{a} \in H$.
3) H is gesloten t.o.v. de binaire operatie in G, d.w.z. de binaire operatie van G, beperkt tot H, is een binaire operatie in H. Stel n.l. $a,b \in H$. Dan is $\overrightarrow{b} \in H$ (2)), dus, volgens onderstelling, $a*(\overrightarrow{b})^{\rightarrow} \in H$, d.w.z. $a*b \in H$. Omdat de associatieve wet geldt in H, is H een groep.

Hiermee is de stelling bewezen.

Voorbeelden 1) De verzameling van even getallen is een ondergroep van de additieve groep van alle gehele getallen. Want, als a en b even zijn, dan is a-b een even geheel getal.
2) Laat Z_6 de groep zijn van gehele getallen mod 6. De ondergroepen van Z_6 zijn: $E = \{[0]\}$, $A_1 = \{[0], [2], [4]\}$, $A_2 = \{[0], [3]\}$ en $A_3 = Z_6$.
3) E_2 is de verzameling van punten in het vlak met Cartesische coördinaten, d.w.z. $E_2 = \{(x,y) \mid x,y \in R\}$. Stel D_4 is de volgende verzameling van permutaties van E_2:

$d_0 = e$ (identieke functie): $(x,y) \to (x,y)$
$d_{\pi/2}$: $(x,y) \to (-y,x)$
d_{π} : $(x,y) \to (-x,-y)$
$d_{3\pi/2}$: $(x,y) \to (y,-x)$
v : $(x,y) \to (-x,y)$ (spiegeling in Y-as)
h : $(x,y) \to (x,-y)$ (spiegeling in X-as)
d_1 : $(x,y) \to (y,x)$ (spiegeling in $y = x$)
d_2 : $(x,y) \to (-y,-x)$ (spiegeling in $y = -x$).

Deze verzameling transformaties kan beschouwd worden als de verzameling van alle symmetrische bewegingen van een vierkant met middelpunt in O(0,0) en verticale en horizontale zijden.
De verzameling D_4 met het samenstellen van bewegingen als operatie (vgl. I, voorbeeld 4) is een groep, die de groep van symmetrieën van een vierkant wordt genoemd.
D_4 bevat 8 niet-triviale ondergroepen: $A_1 = \{d_0, d_{\pi/2}, d_\pi, d_{3\pi/2}\}$, $A_2 = \{d_0, d_\pi, v, h\}$, $A_3 = \{d_0, d_\pi, d_1, d_2\}$, $A_4 = \{d_0, d_\pi\}$, $A_5 = \{d_0, d_1\}$, $A_6 = \{d_0, d_2\}$, $A_7 = \{d_0, h\}$, $A_8 = \{d_0, v\}$.

Definitie 3.4. Het centrum van een groep $(G,*)$, aangeduid met $C(G)$, is de verzameling

$$C(G) = \{c \in G \mid c*x = x*c \text{ voor alle } x \in G\}.$$

Dus $C(G)$ bestaat uit die elementen van G, die met ieder element van G commuteren. Bijv., in de groep D_4 geldt $C(D_4) = \{d_0, d_\pi\} = A_4$.
Men ziet direct in dat een groep $(G,*)$ commutatief is dan en slechts dan als $C(G) = G$.

Stelling 3.5. $(C(G),*)$ is een ondergroep van $(G,*)$ voor iedere groep G.

Bewijs. $C(G) \neq \emptyset$, want het neutrale element $e \in G$ behoort tot $C(G)$. Stel $a, b \in C(G)$, dan geldt, per definitie, $a*x = x*a$ en $b*x = x*b$ voor iedere $x \in G$. Dus, voor een willekeurige $x \in G$ geldt:
$(a*\bar{b}) * x = a * (\bar{b}*x) = a * (\bar{x}*b)^{-} = a * (b*\bar{x})^{-} = a * (x*\bar{b}) = (a*x) * \bar{b} =$
$= (x*a) * \bar{b} = x * (a*\bar{b})$, waaruit volgt $a*\bar{b} \in C(G)$. Dus $(C(G),*)$ is ondergroep van $(G,*)$ volgens st. 3.3.

Stelling 3.6. $\{H_i,*\}_{i\in I}$ is een verzameling ondergroepen van $(G,*)$; de index-verzameling I is willekeurig. Dan is $(\bigcap_i H_i,*)$ ook een ondergroep.

Bewijs. Omdat de verzamelingen H_i alle het neutrale element van $(G,*)$ bevatten, geldt $\bigcap_i H_i \neq \emptyset$. Stel dat a en b twee willekeurige elementen zijn in $\bigcap_i H_i$. Dan geldt $a,b \in H_i$ voor iedere $i \in I$. $(H_i,*)$ is ondergroep, dus $a*\bar{b} \in H_i$ voor iedere $i \in I$, zodat $a*\bar{b} \in \bigcap_i H_i$.

Dan is $(\bigcap H_i,*)$ ondergroep van $(G,*)$ volgens st. 3.3.
In het algemeen is het niet juist, dat ook $(\bigcup_i H_i,*)$ een ondergroep van $(G,*)$ is. Voor een tegenvoorbeeld kan men de ondergroepen $A_1 = \{[0],[6]\}$ en $A_2 = \{[0],[4],[8]\}$ van de groep Z_{12} van gehele getallen mod. 12 nemen. De verzameling $A_1 \cup A_2 = \{[0],[4],[6],[8]\}$ is geen ondergroep van Z_{12}.

Stelling 3.7. Laten $(H_1,*)$ en $(H_2,*)$ ondergroepen zijn van de groep $(G,*)$. Dan is $(H_1 \cup H_2,*)$ ook een ondergroep dan en slechts dan als $H_1 \subseteq H_2$ of $H_2 \subseteq H_1$.

Bewijs. Stel dat $H_1 \subseteq H_2$ of $H_2 \subseteq H_1$. Kies $a,b \in H_1 \cup H_2$. Dan geldt $a,b \in H_1$ of $a,b \in H_2$. Omdat zowel H_1 als H_2 ondergroep is van G volgt hieruit $a*\bar{b} \in H_1$ of $a*\bar{b} \in H_2$, zodat $a*\bar{b} \in H_1 \cup H_2$. Dus $(H_1 \cup H_2,*)$ is ondergroep van G. Omgekeerd, veronderstel dat $H_1 \cup H_2$ ondergroep is van G. Neem aan dat $H_1 \not\subseteq H_2$ en $H_2 \not\subseteq H_1$. Dan zijn er elementen $a \in H_1$, $a \notin H_2$ en $b \in H_2$, $b \notin H_1$. Als $a*b \in H_1$ dan zou volgen $b = \bar{a} * (a*b) \in H_1$, hetgeen niet juist is. Dus $a*b \notin H_1$. De mogelijkheid $a*b \in H_2$ zou opleveren $a = (a*b) * \bar{b} \in H_2$, hetgeen eveneens niet juist is. Dus $a*b \notin H_2$. D.w.z. er geldt $a,b \in H_1 \cup H_2$, maar $a*b \notin H_1 \cup H_2$. Omdat $H_1 \cup H_2$ ondergroep is, is dit een contradictie. Dus de aanname $H_1 \not\subseteq H_2$ en $H_2 \not\subseteq H_1$ is onjuist, zodat $H_1 \subseteq H_2$ of $H_2 \subseteq H_1$.

Definitie 3.8. $(G,*)$ is een groep en H,K zijn niet-lege deelverzamelingen van G. Het product HK is per definitie de verzameling
$HK = \{h*k \mid h \in H, k \in K\}$.
Neem bijv. voor G de symmetrische groep S_3. Laat $H = \{a_1,a_2\}$ en $K = \{a_1,a_4\}$ zijn in S_3 (zie het voorbeeld op pag. 10). Op grond van de vermenigvuldigingstabel voor S_3 geldt $HK = \{a_1,a_2,a_4,a_5\}$. Omdat $a_2*a_2 = a_1$ en $a_4*a_4 = a_1$, a_1 het neutrale element van S_3, geldt $\bar{a}_2 = a_2 \in H$ en $\bar{a}_4 = a_4 \in K$, dus H en K zijn ondergroepen van S_3. HK is echter geen ondergroep van S_3, want bijv. $a_4*a_5 = a_3 \notin HK$, dus HK is niet gesloten t.o.v. *. Men heeft ook, uit de tabel, $KH = \{a_1,a_2,a_4,a_6\} \neq HK$. In het algemeen kan men nu bewijzen :

Stelling 3.9. HK is een ondergroep van $(G,*)$ dan en slechts dan als $HK = KH$ voor ondergroepen H en K van G.

Bewijs. Veronderstel eerst dat HK = KH, d.w.z. als $h \in H$ en $k \in K$ dan is $h*k = k_1*h_1$ voor elementen $k_1 \in K$, $h_1 \in H$ (het is niet nodig dat $k_1 = k$ of $h_1 = h$ is!). Omdat H en K ondergroepen zijn, is $e \in H$ en $e \in K$, dus $e = e*e \in HK$, zodat $HK \neq \emptyset$. Stel $a,b \in HK$, zodat $a = h*k$ en $b = h_1*k_1$ voor geschikte keuze van $h,h_1 \in H$ en $k,k_1 \in K$. Dan geldt $a*\overline{b} = (h*k) * (h_1*k_1)^{-} = h * ((k*\overline{k}_1) * \overline{h}_1)$. Omdat K gesloten is onder *, is $k*\overline{k}_1 \in K$, dus $(k*\overline{k}_1) * \overline{h}_1 \in KH$. Wegens KH = HK bestaan er elementen $h_2 \in H$ en $k_2 \in K$, die voldoen aan $(k*\overline{k}_1) * \overline{h}_1 = h_2*k_2$. Hieruit volgt dat $a*\overline{b} = h * (h_2*k_2) = (h*h_2) * k_2 \in HK$. Volgens st.3.3. is HK dus ondergroep van (G,*).

Omgekeerd, als HK ondergroep is van G, dan geldt voor ieder paar $h \in H$, $k \in K$ dat $\overline{h}*\overline{k} \in HK$ en dus $k*h = (\overline{h}*\overline{k})^{-} \in HK$. Men heeft dus $KH \subseteq HK$. Stel x is een willekeurig element in HK, dan is $\overline{x} \in HK$ en $\overline{x} = h*k$. Dus $x = (\overline{x})^{-} = (h*k)^{-} = \overline{k}*\overline{h} \in KH$, want K en H zijn ondergroepen van G. Dus volgt dat $HK \subseteq KH$. De conclusie is dat HK = KH, waarmee de stelling bewezen is.

Een belangrijk speciaal geval krijgt men als G een abelse groep is. In dat geval geldt voor ieder paar ondergroepen H en K van G, dat HK = KH (de commuterende eigenschap geldt hier elementsgewijs). Aan de voorwaarde van st. 3.9. is voldaan, zodat volgt:

Gevolg 3.10. Als H, K ondergroepen zijn van de abelse groep G, dan is HK een ondergroep van G.

IV Cyclische groepen en het isomorfie-begrip.

Definitie 4.1. $(G,*)$ is een willekeurige groep en S is een niet-lege deelverzameling van G.
Dat betekent het symbool (S):

$$(S) = \cap \{ H \mid S \subseteq H;\ (H,*) \text{ is ondergroep van } (G,*) \}.$$

De verzameling (S) is niet leeg, want G zelf voldoet aan de voorwaarden, die aan H gesteld zijn.
Omdat $S \subseteq H$ and $(S) = \cap H$ volgt dat $S \subseteq (S)$.
Een direct gevolg van stelling 3.6 is dat $((S),*)$ een ondergroep is van $(G,*)$. (S) wordt de ondergroep genoemd voortgebracht door de verzameling S.
Volgens definitie 4.1 geldt voor iedere ondergroep H van G, waarvoor $S \subseteq H$, dat $(S) \subseteq H$. Omdat ook $S \subseteq (S)$ noemt men (S) wel de kleinste ondergroep van G, die de verzameling S bevat. Het kan natuurlijk gebeuren dat $(S) = G$ en in zo'n geval zelgt men, dat de groep G wordt voortgebracht door de deelverzameling S. Bijv. de add.groep Z van de gehele getallen wordt voortgebracht door de verzameling Z_0 van de oneven gehele getallen.
Men kan (S) ook elementsgewijs beschrijven. Daartoe definiëren we: $\overrightarrow{S} = \{ \overrightarrow{a} \mid a \in S \}$. Dan geldt

$$(S) = \{a_1 * a_2 * \ldots * a_n \mid a_1, \ldots, a_n \in S \cup \overrightarrow{S};\ n \text{ geheel}, \geq 1 \}.$$

De verzameling rechts bestaat dus uit alle eindige "producten", waarvan de factoren òf elementen van S òf inversen van elementen van S zijn.
Geef dexe verzameling even aan met $[S]$.
Een schets van het bewijs verloopt dan als volgt:
$[S]$ is een ondergroep van G met de eigenschap $S \subseteq [S]$. Omdat (S) de kleinste ondergroep is, die S bevat, volgt hieruit $(S) \subseteq [S]$. De omgekeerde inclusie wordt afgeleid uit het feit dat iedere ondergroep, die de verzameling S bevat, ook noodzakelijk alle elementen van $[S]$ moet bevatten. Dus $[S] \subseteq \cap H = (S)$.

Een belangrijk speciaal geval ontstaan als S uit één enkel element a bestaat. Men noemt de ondergroep (a) dan de cyclische ondergroep met voortbrengende a. De cyclische ondergroep (a) is dus de doorsnede van alle ondergroepen die a bevatten of de kleinste ondergroep die a bevat. De elementen van (a) zijn eindige "producten" met factoren = a of = $\bar{a}$. Dus (a) = $\{ a^n \mid n \in Z\}$. Hierbij is $a^n = a * a *\ldots * a$ (n keer) voor $n \geq 1$, $a^0 = e$ en $a^{-n} = (a^n)^{\neg}$ voor $n \geq 1$. Met volledige inductie kan men bewijzen dat $(a^n)^{\neg} = (\bar{a})^n$ voor $n \geq 1$. Het is mogelijk dat de groep G gelijk is aan één van zijn cyclische ondergroepen, d.w.z. $G = (a)$ voor 'n element $a \in G$.

Definitie 4.2. G is een groep. Als er een element $a \in G$ is zodat $G = \{a^n \mid n \in Z\}$, dan heet G een cyclische groep, voortgebracht door a, en a heet een voortbrengende van G. We schrijven: $G = (a)$.

Merk op, dat als $G = (a)$, ieder element $g \in G$ geschreven kan worden in de vorm a^m voor 'n geheel getal m.

Een cyclische groep kan verschillende voortbrengenden hebben; men heeft altijd $(a) = (\bar{a})$.

In additieve schrijfwijze luidt de definitie:

G heet een cyclische groep, als er een element $a \in G$ is zodat $G = \{ n\,a \mid n \in Z \}$.

Bijv. Z met de optelling als operatie is een cyclische groep: $Z = (1) = (-1)$. Een ander voorbeeld van een cyclische groep is de commutatieve groep van 4 rotaties d_0, $d_{\pi/2}$, d_π en $d_{3\pi/2}$ van een vierkant om zijn centrum over resp. 0, $\pi/2$, π en $3\pi/2$ (voorbeeld 4, §1). Hier is $d_{\pi/2}$ een voortbrengende, dus $G = (d_{\pi/2})$.

Cyclische groepen zijn commutatief, dus de symmetrische groep S_3 bijv. is niet cyclisch.

Er zijn eindige en oneindige cyclische groepen. De structuur van deze beide soorten is volledig bekend d.w.z. we kunnen bekende groepen aangeven, zodat iedere cyclische groep in 1-1 verband gebracht kan worden met een bekende groep en zodat de resp. binaire operaties corresponderen. Een dergelijk verband noemt men een isomorfie.

Definitie 4.3. Twee groepen, $(G,\circ)$ en $(H,*)$, worden isomorf genoemd als er een 1-1-duidige afbeelding $f : G \to H$ van G op H (bijectie) bestaat zodanig dat voor alle $a, b \in G$ geldt

$$(a \circ b)f = af * bf.$$

Men zegt ook dat G isomorf is met H en schrijft $G \cong H$. De afbeelding f wordt een isomorfie genoemd.

Voorbeelden.

1. Z is de groep van de gehele getallen en Z_2 is de groep van de even getallen (voorbeeld 6, §1), beide met de optelling als operatie. Definiëer $f : Z \to Z_2$ door $(n)f = 2n$ voor alle $n \in Z$. Het is duidelijk dat f een 1-1-afbeelding en een op-afbeelding is. Omdat $(a+b)f = 2(a+b) = 2a + 2b = (a)f + (b)f$, is f een isomorfie en $Z \cong Z_2$.
2. De afbeelding $\phi : x \to e^x$ voor iedere $x \in R$ definiëert een isomorfie van de additieve groep R van de reële getallen op de multiplicatieve groep R^+ van de positieve reële getallen. Immers, als $(x)\phi = (y)\phi$, dan is $e^x = e^y$, dus $x = y$, zodat ϕ een 1-1-afbeelding is. Als $r \in R^+$, dan is $(\ln r)\,\phi = e^{\ln r} = r$, en $\ln r \in R$. Dus ϕ is een afbeelding op R^+. Tenslotte, voor $x, y \in R$ geldt: $(x+y)\,\phi = e^{x+y} = e^x e^y = (x\phi)\,(y\phi)$.

We bewijzen nu:

Stelling 4.4. Iedere oneindige cyclische groep is isomorf met de additieve groep Z van de gehele getallen. Iedere cyclische groep van de orde n is isomorf met de additieve groep $\overline{Z}_n$ van de gehele getallen modulo n.

Bewijs. Laat G een cyclische groep zijn met voortbrengende a, $G = (a)$. Dus $G = \{ a^n \mid n \in Z \}$. Als G oneindig is, dan zijn alle machten van a verschillend, d.w.z. als $h \neq k$, dan is $a^h \neq a^k$. Want stel $a^h = a^k$ en bijv. $h > k$. Dan is $a^h(a^k)^{-1} = a^h(\overline{a})^k = a^{h-k} = e$, het neutrale element van G, en $h - k > 0$. Laat m het kleinste positieve gehele getal zijn zodat $a^m = e$. We beweren dat G dan alleen de verschillende elementen $e, a, a^2, \ldots, a^{m-1}$ zou hebben. Want stel $a^n \in G$, dan bestaan er, volgens de delingsalgorithmus, gehele getallen q en r zodat $n = mq + r$ met $0 \leq r < m$. Dus $a^n = a^{mq+r} = (a^m)^q a^r = e^q a^r = a^r$ met $0 \leq r < m$. Dit zou betekenen, dat G eindig zou zijn. Dus alle machten van a zijn verschillend. Definiëer nu de afbeelding $\phi : G \to Z$ door $(a^n)\phi = n$ voor iedere $a^n \in G$. Als $(a^n)\phi = (a^m)\phi$, dan is $n = m$ en $a^n = a^m$, dus de afbeelding is 1-1. Het is duidelijk dat ϕ een op-afbeelding is. Tenslotte

is $(a^n a^m)\phi = (a^{n+m})\phi = n + m = a^n)\phi + (a^m)\phi$, zodat ϕ de operatie op G in tact laat. Dus ϕ is een isomorfie.
Als G eindig is, kunnen niet alle positieve machten van de voortbrengende a verschillend zijn, dus, voor positieve gehele getallen i en j met bijv. $i < j$, moet gelden $a^i = a^j$. Evenals in het vorige geval is er dan een kleinste positief geheel getal n zodat $a^n = e$. Hieruit volgt dan: $G = \{ e, a, a^2, \ldots, a^{n-1} \}$. Want, als i en j nu twee verschillende niet-negatieve gehele getallen kleiner dan n zijn, bijv. $i < j$, dan zou $a^i = a^j$ impliceren dan $a^{j-i} = e$, in tegenspraak met de minimaliteit van n. Dus de n elementen: $e, a, \ldots, a^{n-1}$ zijn alle verschillend. Verder geldt, voor een willekeurig geheel getal k, dat $k = qn + r$ met gehele getallen q en r en $0 \leq r < n$ (delingsalgorithmus). Dus $a^k = a^r$ met $0 \leq r < n$ en ieder element van G komt voor in het n-tal: $e, a, \ldots, a^{n-1}$. Definiëer nu de afbeelding ψ: $G \to \overline{Z}_n$ door $(a^i)\psi = [i]$ (zie voorbeeld 6, §1). Als $a^i = a^j$, dan is $a^{i-j} = e$, dus $i - j = qn$, q geheel, of $i \equiv j \bmod n$, zodat $[i] = [j]$. Omgekeerd volgt uit $[i] = [j]$, dat $a^i = a^j$. Dus ψ is 1-1. Merk op dat $(e)\psi = (a^0)\psi = [0]$. Ook is ψ een op-afbeelding. Bovendien is $(a^i a^j)\psi = (a^{i+j})\psi = [i+j] = [i] + [j] = (a^i)\psi + (a^j)\psi$. Dus ψ is een isomorfie. Hiermee is de stelling bewezen.

Omdat isomorfie van groepen een equivalentierelatie is, kan men een gegeven verzameling van groepen verdelen in disjuncte deelverzamelingen zodat elk 2-tal groepen in dezelfde deelverzameling isomorf zijn en geen twee groepen in verschillende deelverzamelingen isomorf zijn.
Bijv. beschouw de verzameling V van groepen van de orde 3. Men kan bewijzen dat elk paar groepen van de orde 3 isomorf is. Men zegt ook wel: er is slechts één groep van de orde 3, tot op isomorfie. In dit geval is er dus één equivalentieklasse. Niet alle groepen van de orde 4 zijn isomorf. Een cyclische groep van de orde 4 is isomorf met $\overline{Z}_4$ volgens stelling 4.4. In voorbeeld 3, §1 hebben we echter een niet-cyclische groep van de orde 4. Immers, $f_2^2 = f_1$, $f_3^2 = f_1$ en $f_4^2 = f_1$, f_1 het neutrale element, zodat geen van de elementen f_2, f_3, f_4 de groep voortbrengt. Deze groep is dus niet cyclisch. Als representant van de equivalentie-klasse van isomorfe groepen, waartoe deze groep behoort, neemt men de z.g. vier-groep van Klein V:

$V = \{ e, a, b, c \}$ met vermenigvuldigingstabel

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

De afbeelding α, gedefinieerd door

$$(f_1)\alpha = e, \quad (f_2)\alpha = a, \quad (f_3)\alpha = b, \quad (f_4)\alpha = c$$

is een isomorfie van de groep in voorbeeld 3, §1 op de vier-groep van Klein.

Men kan bewijzen dat er, tot op isomorfie, twee groepen van de orde 4 zijn. Dus elke groep van de orde 4 is òf isomorf met $\overline{Z}_4$ òf met V.

V. Normaaldeler en factorgroep.

Definitie 5.1. $(G,*)$ is een groep en $(H,*)$ is ondergroep van $(G,*)$.
Stel dat $a,b \in G$.
Dan is $a \equiv b \bmod H$ als $a*\overline{b} \in H$ (lees: a is congruent b modulo H).

Hulpstelling 5.2. De betrekking "$a \equiv b \bmod H$" is een equivalentie-relatie.

Bewijs. We moeten aantonen:

(1) $a \equiv a \bmod H$;

(2) $a \equiv b \bmod \longrightarrow b \equiv a \bmod H$;

(3) $a \equiv b \bmod H$, $b \equiv c \bmod H \longrightarrow a \equiv c \bmod H$.

ad(1): $a \equiv a \bmod H$ wegens $a*\overline{a} = e \in H$, e neutrale element van G (st.3.2).

ad(2): stel $a \equiv b \bmod H$, dus $a*\overline{b} \in H$. Nu is $(a*\overline{b})^{-} = b * \overline{a}$ (gevolg 2.4), dus ook $b*\overline{a} \in H$, want H is ondergroep. Dan is $b \equiv a \bmod H$.

ad(3): stel $a \equiv b \bmod H$ en $b \equiv c \bmod H$. Dan geldt $a*\overline{b} \in H$, $b*\overline{c} \in H$, dus $(a*\overline{b}) * (b*\overline{c}) = a * (\overline{b}*b) * \overline{c} = a * e * \overline{c} = a*\overline{c} \in H$, dus $a \equiv c \bmod H$.

Dus de congruentie mod H is een equivalentie-relatie.

Opmerking. Als $G = Z$ de additieve groep van de gehele getallen en $H = Z_n$ de ondergroep van de n-vouden is $(n \geq 2)$, dan betekent de relatie $a \equiv b \bmod H$ voor $a,b \in G$, dat $a-b \in H$ of dat $a - b$ een n-voud is (additieve notatie). Dit is de gewone getaltheoretische congruentie modulo n (zie voorbeeld 6,§1). Dus, in het algemene geval, is congruentie modulo H een generalisatie van een bekende relatie in een bekende groep. Een equivalentie-klasse met $a \in G$ als representant bestaat uit alle elementen $x \in G$ waarvoor geldt $a \equiv x \bmod H$ of $a*\overline{x} \in H$. Het is duidelijk dat $a * \overline{x} = h (h \in H) \longrightarrow \overline{x} = \overline{a} * h \longrightarrow x = \overline{h} * a$ en $\overline{h} \in H$. Omgekeerd geldt voor een element $y = h' * a$ $(h' \in H)$, dat $\overline{y} = \overline{a} * \overline{h'}$,

dus $a * \overline{y} = a * \overline{h'} \in H$, zodat y tot de equivalentie-klasse mod H met a als representant behoort. Met de notatie van definitie 3.8 kan men deze klasse nu aangeven door $Ha = \{h * a | h \in H\}$.

Definitie 5.3. $Ha = \{h * a | h \in H\}$ wordt een rechternevenklasse van H in G genoemd.
Voor iedere $a \in G$ kan men de rechternevenklasse Ha van a in G vormen en omdat Ha samenvalt met de equivalentie-klasse met a als representant, geldt dus $Ha = \{x \in G | a \equiv x \bmod H\}$. In het bijzonder geldt $a \in Ha$ voor iedere $a \in G$. De equivalentie-klassen mod H, dit zijn de rechternevenklassen Ha, bewerken een partitie van G in disjuncte deelverzamelingen. Hieruit volgt direct:
Twee rechternevenklassen van H in G vallen òf samen òf hebben geen element gemeen. Men heeft: Ha valt samen met Hb $(a,b \in G)$ dan en slechts dan als $b \in Ha$. Of ook: $b \in Ha \leftrightarrow a \equiv b \bmod H \leftrightarrow a * \overline{b} \in H$.
Volgens definitie 5.3 geldt $He = H$. Dus, voor $a \in G$, geldt: Ha valt samen met $H \leftrightarrow a \in H$.

Stelling 5.4. Er is een 1-1 verband tussen twee rechternevenklassen Ha en Hb van H in G $(a,b \in G)$.

Bewijs. De afbeelding ϕ: $h*a \to h*b$ $(h \in H, a,b \in G)$ definieert een bijectie van Ha op Hb. Het is duidelijk dat ϕ surjectief is. Stel nu $h_1 * b = h_2 * b$ met $h_1, h_2 \in H$, dan volgt $h_1 = h_2$ (vereenvoudigingswet), dus $h_1 * a = h_2 * a$. Dus ϕ is injectief.
Deze bijectieve eigenschap van rechternevenklassen is van belang voor eindige groepen G.
Stel H is een ondergroep van een eindige groep G. Dan heeft, volgens st. 5.4, elke rechternevenklasse van H in G hetzelfde aantal elementen. Dit aantal is gelijk aan het aantal elementen in de nevenklasse met e als representant, d.w.z. $He = H$. Dus het aantal elementen in een rechternevenklasse is gelijk aan de orde van H, aangeduid door O(H). Omdat G eindig is, is het aantal rechternevenklassen van H in G eindig. Ieder element $a \in G$ behoort tot één en precies één nevenklasse n.l. Ha. Stel het aantal nevenklassen is k, dan geldt dus $kO(H) = O(G)$. Hiermee is de stelling van Lagrange bewezen, die als volgt luidt:

Stelling 5.5. Als G een eindige groep is en H is een ondergroep van G, dan is O(H) een deler van O(G).

Definitie 5.6. G is een willekeurige groep en H is een ondergroep van G. De index van H in G is het aantal verschillende rechternevenklassen van H in G en wordt aangeduid door [G:H].
Als G een eindige groep is, geldt $[G:H] = \frac{O(G)}{O(H)}$ volgens de stelling van Lagrange. Het is heel goed mogelijk dat een oneindige groep G een ondergroep $H \neq G$ heeft, zodat de index [G:H] eindig is. Een voorbeeld hiervan is de groep Z van de gehele getallen met als ondergroep Z_n = groep van de n-vouden ($n \geq 2$). Hiervoor geldt $[Z:Z_n] = n$.
Als a een element is van de groep G, dan verstaan we onder de orde van a de orde van de cyclische ondergroep (a) van G met a als voortbrengende. We noteren: o(a) = orde van a.
Veronderstel nu dat G een eindige groep is. Dan is iedere cyclische ondergroep (a) van G ($a \in G$) ook eindig en de orde van de groep (a) is een deler van de orde van de groep G, of $o(a) | O(G)$.
Als o(a) = n, dan heeft de groep (a) precies n elementen: $(a) = \{e,a,a^2,\ldots,a^{n-1}\}$. Uit het bewijs van stelling 4.4 volgt dat n het kleinste positief gehele getal is, zodat $a^n = e$. Dus o(a) is het kleinste pos. gehele getal, zodat $a^{o(a)} = e$.

Gevolg 5.7. Als G een eindige groep is en $a \in G$, dan geldt $a^{O(G)} = e$.

Bewijs. Volgens het bovenstaande is $o(a) | O(G)$, dus bijv. $O(G) = mo(a)$.
Dan volgt $a^{O(G)} = a^{mo(a)} = (a^{o(a)})^m = e^m = e$.
Als toepassing van de stelling van Lagrange bewijzen we dat er precies 2 niet-isomorfe groepen van de orde 4 zijn.

Stelling 5.8. Iedere groep van de orde 4 is òf isomorf met de cyclische groep van de orde 4 of met de vier-groep V van Klein (zie §4).

Bewijs. $G = \{e,a,b,c\}$ is een groep van de orde 4, waarin e het neutrale element is. Omdat $o(a) | O(G) = 4$, $o(b) | 4$, $o(c) | 4$, hebben de elementen a, b en c òf orde 2 òf orde 4. Als één van deze drie de orde 4 heeft, dan is G cyclisch van de orde 4.

Dus, veronderstel dat geen van de elementen a, b en c de orde 4 heeft, d.w.z. $o(a) = o(b) = o(c) = 2$. Dan volgt $a^2 = b^2 = c^2 = e$.
Beschouw het product $a * b$. Als $a * b = e$, dan is $b = \bar{a} = a$, want $o(a) = 2$, in tegenspraak met $b \neq a$. Dus $a * b \neq e$. Als $a * b = a$, dan volgt $b = e$, contradictie. Als $a * b = b$, dan is $a = e$, contradictie. Daarom is de enige mogelijkheid dat $a * b = c$, hetgeen moet gelden, want $a * b \in G$.
In dit stadium ziet de vermenigvuldigingstabel voor G er als volgt uit:

*	e	a	b	c
e	e	a	b	c
a	a	e	c	
b	b		e	
c	c			e

Omdat ieder element van G in iedere rij en kolom moet voorkomen in de tabel, moet gelden $a * c = b$.
Gebruik makend van deze eigenschap, kan men de overige plaatsen in de tabel invullen en vindt men achtereenvolgens: $b * c = a$, $b * a = c$, $c * a = b$ en $c * b = a$. Men verkrijgt zo juist de vermenigvuldigingstabel van de vier-groep V van Klein (zie §4).

Stelling 5.9. Iedere groep G, waarvoor $O(G) = p$, p een priemgetal, is cyclisch.

Bewijs. Omdat $O(G) = p$, $p > 1$, heeft G een element $a \neq e$. Beschouw de cyclische ondergroep (a) met als voortbrengende a. Er geldt $o(a) \mid O(G) = p$, dus $o(a) = 1$ of $o(a) = p$. Volgens definitie van $o(a)$, volgt uit $o(a) = 1$ dat $a = e$, in tegenspraak met $a \neq e$. Dus $o(a) = p = O(G)$, zodat $(a) = G$ en G cyclisch is.
We kunnen nu gemakkelijk een bewering uit §2 bewijzen n.l.

Stelling 5.10. Een niet-commutatieve groep heeft tenminste 6 elementen.

Bewijs. Volgens st. 5.9. is een groep G met $O(G) = p$, p priemgetal, cyclisch en dus commutatief. Dus iedere groep met orde 2, 3 of 5 is commutatief. Volgens St. 5.8 is iedere groep G met $O(G) = 4$ óf cyclisch

òf isomorf met V, de vier-groep van Klein. Uit de tabel van V volgt, dat V commutatief is. Dus een groep van de orde 4 is commutatief. Hiermee is de stelling bewezen.
Een niet-commutatieve groep van de orde 6 is S_3, de symmetrische groep van de orde 3! = 6 (zie §2).

Opmerking. De omkering van de stelling van Lagrange is niet juist, d.w.z. een groep van de orde n behoeft niet een ondergroep van de orde k te hebben, waarin k een deler is van n. Er bestaat een groep van de orde 12 (een ondergroep van de symmetrische groep S_4), die geen ondergroepen van de orde 6 heeft.
(G,*) is een groep en (H,*) is ondergroep van (G,*). Definieer de relatie $\sim$ op G door: $a \sim b$ als $\vec{a} * b \in H$ $(a,b \in G)$. Evenals in hulpstelling 5.2 kan men gemakkelijk bewijzen dat $\sim$ een equivalentierelatie op G is.

Definitie 5.11. (G,*) is een groep, $a \in G$ en (H,*) is ondergroep van (G,*). Dan heet $aH = \{a * h | h \in H\}$ een linkernevenklasse van H in G.
We tonen nu aan dat de equivalentie-klassen van $\sim$ juist de linkernevenklassen van H in G zijn. Immers, stel $a \in G$ en a representeert de klasse $[a] = \{x \in G | x \sim a\}$. Als $y \in [a]$, dan is $y \sim a$, dus $\vec{y} * a = h'$, $h' \in H$, dus $\vec{y} = h' * \vec{a}$ of $y = a * \vec{h'} \in aH$, want H is ondergroep in G. Omgekeerd, als $x \in aH$, dan is $x = a * h$, $h \in H$, dus $\vec{x} = \vec{h} * \vec{a}$ en $\vec{x} * a = \vec{h} \in H$, zodat $x \sim a$ of $x \in [a]$.
Hieruit volgt, dat $[a] = aH$.
De linkernevenklassen bewerken dus een partitie van G in disjuncte deelverzamelingen. Hieruit volgt:
Twee linkernevenklassen van H in G vallen òf samen òf hebben geen element gemeen. Men heeft nu voor $a,b \in G$:
$aH = bH \leftrightarrow b \in aH \leftrightarrow a \sim b \pmod{H} \leftrightarrow \vec{a} * b \in H$.
Volgens definitie 5.11 geldt $eH = H$. Dus, voor $a \in G$ geldt:
$aH = H \leftrightarrow \vec{a} \in H$ of $a \in H$.
Juist zoals in stelling 5.4 kan men nu bewijzen dat er een 1-1 verband is tussen twee linkernevenklassen aH en bH van H in G$(a,b \in G)$.

Laat G een groep zijn en H een ondergroep van G. Dan is er een 1-1 afbeelding van de verzameling {gH} van linkervenklassen van H in G op de verzameling {Hg} van rechternevenklassen van H in G. De bedoelde afbeelding is ϕ: $gH \to H\overline{g}$. Het is duidelijk dat
$g_1H = gH \longrightarrow g_1 \sim g \pmod H \longrightarrow \overline{g}_1 * g \in H \longrightarrow \overline{g} * g_1 \in H \longrightarrow \overline{g} \equiv \overline{g}_1 \pmod H$
$\longrightarrow H\overline{g} \equiv H\overline{g}_1$ en omgekeerd. Omdat ϕ ook surjectief is, volgt dat ϕ een bijectie is.

Opmerking: $aH \to Ha$ ($a \in G$) is geen afbeelding, omdat $aH = a'H$ kan zijn ($a,a' \in G$), maar $Ha \neq Ha'$.
De index van H in G, [G:H], is dus ook gelijk aan het aantal verschillende linkernevenklassen van H in G (zie definitie 5.6).
Stel $G = S_3$ en H is de ondergroep $\{a_1,a_2\}$ (zie voorbeeld, §2). Omdat [G:H] = 3, zijn er drie rechternevenklassen van H in G en drie linkernevenklassen van H in G als volgt:

Rechter-nevenklassen	Linker-nevenklassen
$H = \{a_1,a_2\}$	$H = \{a_1,a_2\}$
$Ha_5 = \{a_5,a_4\}$	$a_5H = \{a_5,a_3\}$
$Ha_6 = \{a_6,a_3\}$	$a_6H = \{a_6,a_4\}$

Dus de rechternevenklasse Ha_5 is geen linkernevenklasse. Ook $N = \{a_1,a_5,a_6\}$ is een ondergroep van S_3. Omdat [G:N] = 2, zijn er twee rechter- en twee linkernevenklassen van N in G als volgt:

Rechter-nevenklassen	Linker-nevenklassen
$N = \{a_1,a_5,a_6\}$	$N = \{a_1,a_5,a_6\}$
$Na_2 = \{a_2,a_3,a_4\}$	$a_2N = \{a_2,a_4,a_3\}$.

Dus iedere linkernevenklasse van N in S_3 is een rechternevenklasse en omgekeerd. Ondergroepen, zoals N in S_3 waarvoor deze eigenschap geldt, zijn belangrijk.

Definitie 5.12. Een ondergroep (H,*) van de groep (G,*) heet een normaaldeler (of invariante ondergroep) als iedere linkernevenklasse van H in G een rechternevenklasse van H in G is.

Dus, als H normaaldeler is en aH is linkernevenklasse van H in G, dan bestaat er een element $b \in G$, zodat $aH = Hb$. omdat $a \in aH$ volgt hieruit dat $a \in Hb$. De rechternevenklassen Hb en Ha hebben het element a gemeen, dus $Hb = Ha$. M.a.w. als aH rechternevenklasse is van H in G, dan moet het de klasse Ha zijn. We kunnen nu definitie 5.12 opnieuw formuleren:

Een ondergroep $(H,*)$ is normaaldeler in de groep $(G,*)$ dan en slechts dan als $aH = Ha$ voor iedere $a \in G$.

Voor een normaaldeler H kan men dus eenvoudig over nevenklassen van H in G spreken zonder de toevoeging rechts of links. De triviale ondergroepen $\{e\}$ en G zijn normaaldelers in G. Iedere ondergroep van een commutatieve groep G is normaaldeler in G. Een criterium opdat een ondergroep H van een groep G normaaldeler is in G is de volgende

Stelling 5.13. De ondergroep $(H,*)$ is normaaldeler in de groep $(G,*)$ dan en slechts dan als voor ieder element $a \in G$ geldt: $aH\bar{a} \subseteq H$.

Bewijs. Neem eerst aan dat $aH\bar{a} \subseteq H$ voor iedere $a \in G$. We moeten bewijzen dat $aH = Ha$. Stel $a * h$ is een willekeurig element in aH. Omdat $aH\bar{a} \subseteq H$, is $a * h * \bar{a} = h_1$ voor 'n element $h_1 \in H$. Dus geldt dat $a * h = (a * h * \bar{a}) * a = h_1 * a \in Ha$ en dus is $aH \subseteq Ha$.
Kies nu $h * a$ willekeurig in Ha. Dan volgt dat $\bar{a} * h * a = \bar{a} * h * (\bar{a})^{-} \in H$, omdat $aH\bar{a} \subseteq H$ voor iedere $a \in G$. Dus $\bar{a} * h * a = h_2$, $h_2 \in H$ en $h * a = a * h_2 \in aH$ zodat $Ha \subseteq aH$. Dus $aH = Ha$.
Omgekeerd, stel $aH = Ha$ voor iedere $a \in G$. Laat $a * h_1 * \bar{a}$ een willekeurig element zijn in $aH\bar{a}$. Omdat $aH = Ha$ bestaat er een element $h_2 \in H$ zodat $a * h_1 = h_2 * a$. Bijgevolg is $a * h_1 * \bar{a} = (h_2 * a) * \bar{a} = h_2$, zodat $aH\bar{a} \subseteq H$. Hiermee is de stelling bewezen.

Als toepassing van st. 5.13 kan men nu bewijzen: Het centrum C(G) van een groep G is een normaaldeler in iedere groep G (definitie 3.4). Volgens st. 3.5 is C(G) een ondergroep van G. Stel $c \in C(G)$ en a is willekeurig in G, dan moet men aantonen dat $a * c * \bar{a} \in C(G)$. Er geldt echter $a * c = c * a$, want $c \in C(G)$. Dus $a * c * \bar{a} = c * a * \bar{a} =$
$= c * e = c \in C(G)$.

Men verifieert ook direct, dat de ondergroep $H = \{a_1, a_2\}$ in $G = S_3$ geen normaaldeler is, want bijv. $a_4 * a_2 * \overline{a_4} = a_6 * a_4 = a_3 \notin H$.
De betekenis van normaaldelers is dat zij ons in staat stellen nieuwe groepen te definiëren, die in nauwe betrekking staan tot de oorspronkelijke groep. Als $(H,*)$ normaaldeler is in de groep $(G,*)$, dan geven we de verzameling van verschillende nevenklassen van H in G aan door G/H:

$$G/H = \{aH \mid a \in G\}.$$

Een binaire operatie op G/H wordt gedefinieerd door:

$$(aH) \otimes (bH) = (a * b)H.$$

Omdat deze definitie gegeven is met behulp van representanten van nevenklassen, moeten we aantonen dat de "vermenigvuldiging" van nevenklassen onder $\otimes$ ondubbelzinnig is gedefinieerd, onafhankelijk van de keuze van de representanten in deze klassen. D.w.z., men moet laten zien dat als $aH = a_1H$ en $bH = b_1H$ dan ook $(a * b)H = (a_1 * b_1)H$ is. Uit $aH = a_1H$ volgt $\overline{a} * a_1 \in H$, uit $bH = b_1H$ volgt $\overline{b} * b_1 \in H$. Omdat H normaaldeler is in G, weten we dat $xH\overline{x} \subseteq H$ voor iedere $x \in G$ (st.5.13).
In het bijzonder geldt:
$\overline{b}Hb = \overline{b}H(\overline{b})^{-} \subseteq H$, dus $\overline{b} * (\overline{a} * a_1) * b \in H$ en dus ook $(a*b)^{-} * (a_1*b_1) =$
$= (\overline{b} * (\overline{a}*a_1) * b) * (\overline{b}*b_1) \in H$, want H is gesloten t.o.v. $*$. Dan volgt $(a*b)H = (a_1*b_1)H$.

Stelling 5.14. $(G,*)$ is een groep en $(H,*)$ is normaaldeler in $(G,*)$. Dan vormt het stelsel $(G/H,\otimes)$ een groep, die bekend staat als de factorgroep van G over H.

Bewijs. We hebben reeds gezien, dat $\otimes$ ondubbelzinnig is gedefinieerd en dat G/H gesloten is t.o.v. $\otimes$. De associatieviteit van de operatie $\otimes$ ziet men als volgt:
$[aH \otimes bH] \otimes cH = [(a*b)H] \otimes cH = ((a*b) * c)H = (a * (b*c))H =$
$aH \otimes [(b*c)H] = aH \otimes [bH \otimes cH]$ $(a,b,c, \in G)$.
De nevenklasse $H = eH$, e neutrale element in G, is het neutrale element voor de operatie $\otimes$, want $aH \otimes eH = (a*e)H = aH = (e*a)H = eH \otimes aH$.

De inverse van de nevenklasse aH is $\vec{a}H$, waarin $\vec{a}$ het inverse element is van a in $(G,*)$. Immers:
$aH \otimes \vec{a}H = (a*\vec{a})H = eH = (\vec{a}*a)H = \vec{a}H \otimes aH$.
Dus aan de axioma"s (1), (2) en (3) van definitie (1.1) is voldaan, zodat G/H met de operatie $\otimes$ een groep is.
Hiermee is de stelling bewezen.
Een direct gevolg van definitie 5.6 is

Gevolg 5.15. G is een eindige groep en H is normaaldeler in H, dan is $[G:H] = \frac{O(G)}{O(H)} = O(G/H)$.

Voorbeeld. Z is de additieve groep van de gehele getallen en Z_n is de ondergroep van de n-vouden ($n \geq 2$). Z is commutatief, dus Z_n is normaaldeler in Z. De nevenklassen van Z_n in Z hebben de vorm:

$$a + Z_n = \{a + kn \mid k \in Z\} = [a], \ (a \in Z).$$

M.a.w., de nevenklassen van Z_n zijn precies de congruentie-klassen modulo n (voorbeeld 6, §1). De compositie van nevenklassen in Z/Z_n wordt gegeven door: $(a+Z_n) \otimes (b+Z_n) = a + b + Z_n$ of in andere notatie: $[a] \otimes [b] = [a+b]$.
De factorgroep van Z over Z_n is dus niets anders als de groep $\vec{Z}_n$ van gehele getallen modulo n.

VI. Homomorfieën.

Definitie 6.1. $(G,*)$ en $(G',\circ)$ zijn twee groepen en f is een afbeelding van G in G', $f : G \to G'$. Dan heet f een homomorfie van G in G' als

$$(a*b)f = (a)f \circ (b)f$$

voor ieder paar elementen $a, b \in G$.
Merk op dat in het linkerlid de binaire operatie $*$ in G wordt gebruikt voor $a * b$ en in het rechterlid de operatie $\circ$ in G' voor de elementen $(a)f$ en $(b)f$ in G'. Men drukt de eigenschap van homomorfie vaak uit door: het beeld van het "product" onder f is gelijk aan het "product" van de beelden.

Voorbeelden.

1) $(G,*)$ is een willekeurige groep. Definieer de afbeelding $f : G \to G$ door $f = 1_G$ d.i. de identieke afbeelding op G te nemen; f is een homomorfie van G op zichzelf.
2) $(G,*)$ en $(G',\circ)$ zijn twee groepen met neutrale elementen e en e' resp. De afbeelding $f : G \to G'$, gegeven door $(a)f = e'$ voor alle $a \in G$, is een homomorfie van G in G'.
3) $(R,+)$ is de additieve groep van de reële getallen en $(R\setminus\{0\},.)$ is de groep van reële getallen $\neq 0$ met de gewone vermenigvuldiging als operatie. Definieer $\Phi : R \to R \setminus \{0\}$ door $(a)\Phi = 2^a$. Dan geldt

$$(a+b)\Phi = 2^{a+b} = 2^a \,.\, 2^b = (a)\Phi \,.\, (b)\Phi$$

voor ieder paar elementen $a, b \in R$. Dus Φ is een homomorfie. Omdat $2^a > 0$ voor iedere $a \in R$, is Φ niet surjectief, dus Φ is een homomorfie van R in $R \setminus \{0\}$, maar niet op $R \setminus \{0\}$.

4) $G = S_3 = \{a_1,a_2,a_3,a_4,a_5,a_6\}$ en $G' = \{a_1,a_2\}$ (zie §2).
Definiëer de afbeelding $f : G \to g'$ door $(a_2^i * a_5^j)f = a_2^i$.
Er geldt: $a_2^2 = a_1$ en $a_5^3 = a_1$, a_1 het neutrale element van S_3.
Dus $i = 0, 1$ en $j = 0, 1, 2$, waarbij $a_2 * a_5 = a_4$, $a_2 * a_5^2 =$
$= a_2 * a_6 = a_3$ en $a_1 * a_5^2 = a_1 * a_6 = a_6$, zodat S_3 wordt voortgebracht

---

door a_2 en a_5 of $S_3 = (a_2, a_5)$ (zie §4).
Men ziet gemakkelijk in, dat f een homomorfie is:
$(a_1)f = a_1$, $(a_2)f = a_2$, $(a_3)f = a_2$, $(a_4)f = a_2$, $(a_5)f = a_1$ en
$(a_6)f = a_1$.

5) G = Z = additieve groep van de gehele getallen en G' = $\overline{Z}_4$ = additieve groep van restklassen modulo 4.
Definieer de afbeelding f : Z $\to \overline{Z}_4$ door

(n)f = [2], als n oneven is

en (n)f = [0], als n even is.

f is een homomorfie van Z in $\overline{Z}_4$, maar f is niet surjectief.

Stelling 6.2. f is een homomorfie van de groep (G,*) in de groep (G',$\circ$). Dan geldt:

(a) (e)f = e', waarin e resp e' het neutrale element is in G resp. G'.

(b) als a $\in$ G, dan is $(\overline{a})f = (af)^{-1}$, d.w.z. het beeld van de inverse van a in G is de inverse van het beeld van (a)f in G'.

Bewijs.

(a) Voor iedere a $\in$ G geldt: a * e = e * a = a, dus a f = (a*e)f = = (af) $\circ$ (ef) en (af) $\circ$ e' = af, zodat (af) $\circ$ (ef) = (af) $\circ$ e'. Volgens de vereenvoudigingswet in (G',$\circ$) (st.2.2) volgt hieruit (e)f = e'.

(b) Voor iedere a $\in$ G geldt a * $\overline{a}$ = a * $\overline{a}$ = e, dus $(a*\overline{a})f = (\overline{a}f) \circ (af)$ en $(a*\overline{a})f$ = (e)f = e' (volgens a), dus (af) $\circ$ $(\overline{a}f)$ = e' en $(af) \circ (af)^{-1}$ = e' in (G',0).
Uit st.2.2 volgt weer: $(\overline{a})f = (af)^{-1}$. Hiermee is de stelling bewezen.

Als f : G $\to$ G' een homomorfie is, dan wordt de verzameling van beeldelementen onder f (in G') het beeld van f of Im f (lees: image f) genoemd. Dus Im f = {(a)f | a $\in$ G}. Men kan bewijzen dat Im f een ondergroep van G' is. D.w.z. het homomorfe beeld van een groep is een groep.

Stelling 6.3. f is een homomorfie van de groep (G,*) in de groep (G',$\circ$). Dan is Im f een ondergroep van G'.

Bewijs. Het is duidelijk dat Im f een niet-lege deelverzameling is van G'. Volgens st.3.3 moeten we aantonen, dat uit a', b' $\in$ Im f volgt dat $a' \circ \overline{b'} \in$ Im f. Als a' $\in$ Im f, dan is a' = (a)f voor 'n element a $\in$ G,

evenzo $b' \in \text{Im } f \Rightarrow b' = (b)f$ voor 'n element $b \in G$.
Dus $a' \circ \overline{b'} = (af) \circ (bf)^{-1} = (af) \circ (\overline{b}f)$ (st.6.2) $= (a*\overline{b})f \in \text{Im } f$.
Een homomorfie $f : G \to G'$ van een groep G in een groep G' bewerkstelligt dus een homomorfie $f' : G \to \text{Im } f$ van de groep G op de groep Im f.
Men behoeft slechts $(g)f' = (g)f$ voor iedere $g \in G$ te definiëren.
$f : G \to G'$ is een homomorfie op dan en slechts dan als $\text{Im } f = G'$.
Uit stelling 6.3 volgt in het bijzonder, dat, als $f : G \to G'$ een homomorfie is van een groep G in een groep G' en H is een ondergroep van G, de verzameling van beeldelementen (onder f) van de elementen van H een ondergroep H' is van G'. Hierbij is $H' = \{(h)f \mid h \in H\}$. Men zou dit ook als volgt kunnen formuleren: als men de homomorfie $f : G \to G'$ beperkt tot de ondergroep H van G, gaat f over in $f' : H \to H'$ en $H' = \text{Im } f'$.
Veronderstel weer, dat $f: G \to G'$ een gegeven homomorfie is van de groep G in de groep G'. Laat H' een willekeurige ondergroep zijn van G'. Dan definiëren we: $(H')f^{-1} = \{a \mid a \in G, (a)f \in H'\}$.

Stelling 6.4. f is een homomorfie van de groep $(G,*)$ in de groep $(G',\circ)$. Dan geldt:
(a) als $(H',\circ)$ ondergroep is in G', dan is $((H')f^{-1},*)$ ondergroep in G.
(b) als $(H',\circ)$ normaaldeler is in G', dan is $((H')f^{-1},*)$ normaaldeler in G.

Bewijs:
(a). $(H')f^{-1} \neq \emptyset$, want $e \in G$ en $(e)f = e'$ (st.6.2), dus $(e)f \in H'$. Dus $e \in (H')f^{-1}$. Stel nu dat $a, b \in (H')f^{-1}$. Dan geldt $(a)f, (b)f \in H'$. Dus $(a*\overline{b})f = (af) \circ (\overline{b}f) = (af) \circ (bf)^{-1} \in H'$, want H' is ondergroep van G'. Omdat $a * \overline{b} \in G$, volgt hieruit dat $a * \overline{b} \in (H')f^{-1}$, dus $(H')f^{-1}$ is ondergroep volgens st.3.3.
(b). $(H',\circ)$ is normaaldeler, dus ondergroep in G'. Dus volgens (a) is $(H')f^{-1}$ ondergroep in G.
Stel nu $h \in (H')f^{-1}$, dus $(h)f \in H'$ en laat a een willekeurig element van G zijn. Dan volgt: $(a*h*\overline{a})f = (af) \circ (hf) \circ (\overline{a}f) \in H'$, want $(h)f \in H'$ en H' is ondergroep in G'. Dus geldt: $a*h*\overline{a} \in (H')f^{-1}$. Omdat dit voor iedere $h \in (H')f^{-1}$ juist is, kan men schrijven: $a(H')f^{-1}\,\overline{a} \subseteq (H')f^{-1}$. Volgens st.5.13 betekent dit, dat $(H')f^{-1}$ normaaldeler is in G.

Definitie 6.5. f is een homomorfie van de groep $(G,*)$ in de groep $(G',\circ)$ en e' is het neutrale element van G'. Dan wordt de verzameling $K = \{x \mid x \in G \text{ en } xf = e'\}$ de kern van f genoemd en geschreven als $K = \text{kern } f$.
Men heeft dus: kern $f = (e')f^{-1}$.

Volgens §5 is de triviale ondergroep {e} van een groep G normaaldeler in G. Dus een direct gevolg van stelling 6.4(b) is
Stelling 6.6. f is een homomorfie van de groep $(G,*)$ in de groep $(G',\circ)$. Dan is kern f een normaaldeler in G.
Het kan gebeuren, dat f = G. In dit geval wordt ieder element van G door f afgebeeld of e', e' het neutrale element van G'. Dit is het geval in voorbeeld 2, §6. Het andere extreme geval doet zich voor, als kern f = {e}, e het neutrale element in G (zie voorbeeld 1, §6). Men kan nu bewijzen:
Stelling 6.7. f is een homomorfie van de groep $(G,*)$ in de groep $(G',\circ)$. Dan is f een injectieve afbeelding (1-1-verband) dan en slechts dan als kern f = {e}.
Bewijs. Veronderstel dat de afbeelding f een injectie is. We weten al dat $e \in$ kern f. Stel nu dat $a \in$ kern f, $a \neq e$, voor 'n element $a \in G$. Dan is $(a)f = e' = (e)f$, d.w.z. $(a)f = (e)f$, maar $a \neq e$. Dan is f geen 1-1-afbeelding, dus kern f = {e}.
Omgekeerd, stel dat kern f = {e}. Stel nu dat $a, b \in G$ met $(a)f = (b)f$. Hieruit volgt, dat $(a*\overline{b})f = (af) \circ (\overline{b}f) = (af) \circ (bf)^{-1} = (af) \circ (af)^{-1} = e'$, dus $a * \overline{b} \in$ kern f. Maar kern f = {e}, dus $a * \overline{b} = e$ of $a = b$. Dus f is een injectie. Hiermee is de stelling bewezen.
In het geval dat de homomorfie f injectief is, heeft men dus een 1-1-duidige afbeelding $f' : G \to \text{Im } f$ van G op Im f (bijectie), terwijl voor alle $a, b \in G$ geldt: $(a*b)f' = (af') \circ (bf')$. Volgens definitie 4.3 betekent dit dat de groepen $(G,*)$ en $(\text{Im } f,\circ)$ isomorf zijn. Omgekeerd, als $(G,*)$ en $(H,\circ)$ isomorfe groepen zijn, dan is er een 1-1-afbeelding $k : G \to H$ van G op H, die tevens homomorfie is (def.4.3). Volgens st.6.7 geldt dus kern k = {e}, e neutrale element van G. Men heeft dus:
Gevolg 6.8. Een homomorfie $\phi : G \to H$ van een groep G op een groep H met kern $\phi = K$ is een isomorfie van G op H dan en slechts dan als K = {e}.

In het geval, dat $\phi : G \to H$ een homomorfie van G in H is met kern $\phi = \{e\}$, noemt men ϕ ook een isomorfie van G <u>in</u> H.

Iedere homomorfie bepaalt dus een normaaldeler door middel van zijn kern. Van de andere kant toont de volgende stelling aan dat iedere normaaldeler in een groep aanleiding geeft tot een homomorfe afbeelding, de z.g. <u>natuurlijke afbeelding</u>.

<u>Stelling 6.9</u>. $(H,*)$ is normaaldeler in de groep $(G,*)$. Dan is de afbeelding $\nu : G \to G/H$ gedefiniëerd door

$$(a)\nu = aH$$

voor iedere $a \in G$ een homomorfie van G op de factorgroep $(G/H,\otimes)$. De kern van ν is precies de verzameling H.

<u>Bewijs</u>. Omdat ieder element $a \in G$ behoort tot één en precies één nevenklasse $aH \in G/H$ is de afbeelding ν zinvol. Men heeft nu voor $a, b \in G$: $(a*b)\nu = (a*b)H = (aH) \otimes (bH) = (a)\nu \otimes (b)\nu$ (zie §5). Dat ν een afbeelding op is, is triviaal, want ieder element van G/H is een nevenklasse aH met $a \in G$ en $(a)\nu = aH$. Dus ν is een homomorfie op.

Volgens st.5.14 is de nevenklasse $H = eH$, e neutrale element van G, het neutrale element in G/H.

Dus kern $\nu = \{a \mid a \in G, (a)\nu = H\}$

$\{a \mid a \in G, aH = H\} = H$ (zie §5, blz. 26).

Hiermee is de stelling bewezen.

De nu volgende stelling wordt wel de fundamentele stelling van homomorfieën genoemd.

<u>Stelling 6.10</u>. f is een homomorfie van de groep $(G,*)$ op de groep $(G',\circ)$ met kern K. Dan is

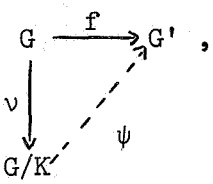
$$(G/K,\otimes) \text{ isomorf met } (G',\circ).$$

<u>Bewijs</u>. Beschouw het diagram:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle \nu}\downarrow & & \\ G/K & & \end{array}$$

waarin $(a)\nu = aK$ $(a \in G)$ de natuurlijke afbeelding is.

Merk op dat kern $f = K$ een normaaldeler is in G (st.6.6), dus de factor-

groep G/K bestaat. We willen het diagram aanvullen tot: 

zodat ψ de isomorfie van G/K op G' bewerkt.
Definiëer de afbeelding $\psi : G/K \to G'$ door

$$(aK)\psi = (a)f \text{ voor iedere } a \in G.$$

De eerste vraag is of ψ een zinvol gedefiniëerde afbeelding is. Stel dus $a'K = aK$ met $a, a' \in G$, dan is $a' = a * k$ met $k \in K$, dus $(a')f =$
$= (a*k)f = (af) \circ (kf) = (af) \circ e'$, e' neutrale element van G', want $k \in$ kern f. Dus $(a')f = (a)f$, zodat $(a'K)\psi = (a')f = (a)f = (aK)\psi$.
Vervolgens tonen we aan dat ψ een homomorfie is:

$$[aK) \otimes (a'K)]\psi = [(a*a')K]\psi = (a*a')f = (af) \circ (a'f) = (aK)\psi \circ (a'K)\psi.$$

Ook geldt ψ is surjectief, want als $g' \in G'$, dan is $g' = (g)f$, omdat f een op-afbeelding is $(g \in G)$, dus $g' = (g)f = (gK)\psi$. Dus ψ is een homomorfie van G/K op G'. Ook is ψ een 1-1-afbeelding, want als $(aK)\psi = e'$, dan is $e' = (a)f$, dus $a \in$ kern $f = K$. Maar $a \in K$ impliceert $aK = K$, dus de kern van $\psi = K$. Volgens st.6.7 volgt hieruit dat ψ een 1-1-afbeelding is. Hiermee is aangetoond dat de groepen $(G/K, \otimes)$ en $(G', \circ)$ isomorf zijn (def.4.3) en de stelling bewezen.

Men kan opmerken, dat de driehoek van afbeeldingen in het diagram commutatief is d.w.z. voor iedere $a \in G$ geldt $(a)(\nu \circ \psi) = (a)f$, want $(a)\nu = aK$ en $(aK)\psi = (a)f$, dus $(a)(\nu \circ \psi) = \{(a)\nu\}\psi = (a)f$. Er geldt ook, dat ψ de enige afbeelding is, waarvoor dit juist is. Stel n.l. $f = \nu \circ \alpha$ voor 'n afbeelding α: $G/K \to G'$. Dan is $(aK)\psi = (a)f = (a)(\nu \circ \alpha) = (aK)\alpha$ voor iedere nevenklasse $aK \in G/K$, dus $\psi = \alpha$.
Voorbeelden. 6) Z = additive groep van de gehele getallen en $G' = \{1, -1\}$ is multiplicatieve groep van de getallen 1 en -1.
Definieer $f : Z \to G'$ door $(n)f = 1$ als n even is $(n \in Z)$
en $(n)f = -1$ als n oneven is $(n \in Z)$.
Dan is f een homomorfie van Z op G' en
kern $f = Z_2$ = groep van de even gehele getallen.
Dus $Z/\text{kern } f = Z/Z_2 = \{Z_2, 1+Z_2\}$.

De fundamentele st. 6.10 zegt dan dat $^{Z}/_{Z_2} \cong G'$. Dit is ook duidelijk uit de vermenigvuldigingstabellen:

0	Z_2	$1+Z_2$
Z_2	Z_2	$1+Z_2$
$1+Z_2$	$1+Z_2$	Z_2

en

.	1	-1
1	1	-1
-1	-1	1

Het bewijs van stelling 6.10 geeft aan, dat de afbeelding ψ , die de isomorfie bewerkt (de geïnduceerde afbeelding) wordt gegeven door

$$(Z_2)\psi = (0+Z_2) = (0)f = 1$$

$$(1+Z_2)\psi = (1)f = -1.$$

7) $(G,*)$ is een willekeurige groep en a is een vast element in G. Definiëer de afbeelding $f : Z \to G$ door $(n)f = a^n$ voor iedere $n \in Z$. Men toont direct aan dat de zo gedefiniëerde f een homomorfie is van de additieve groep Z van de gehele getallen op de cyclistische ondergroep (a) van G:

$$(n+m)f = a^{n+m} = a^n * a^m = (n)f * (m)f.$$

Per definitie is $(a) = \{a^n \mid n \in Z\}$, dus f beeldt Z af op de groep (a) (zie §4). Volgens stelling 6.10 geldt dus $^{Z}/_{\text{kern } f} \cong (a)$, waarin kern $f = \{n \mid n \in Z, a^n = e\}$. Er zijn nu 2 mogelijkheden wat kern f betreft. De eerste is dat kern $f = \{0\}$, m.a.w. $a^n = e$ impliceert $n = 0$. In dit geval heeft een element van $^{Z}/_{\text{kern } f}$ de vorm: $n + \text{kern } f = n + 0 = n$, $n \in Z$. Dus de nevenklassen in $^{Z}/_{\text{kern } f}$ zijn juist de elementen van Z; men heeft $^{Z}/_{\text{kern } f} = Z$. De tweede mogelijkheid is, dat kern $f \neq \{0\}$. Er zijn dus gehele getallen $n \neq 0$ zodat $a^n = e$. Als $a^n = e$, dan is ook $a^{-n} = (\bar{a})^n = (a^n)^{-1} = e$, dus er is tenminste één $n > 0$ zodat $a^n = e$. Dan bestaat er ook een kleinste positief geheel getal, bijv. m, zodat $a^m = e$. Het is duidelijk, dat hieruit volgt dat $a^{km} = e$ voor ieder geheel getal k. Met behulp van de delingsalgorithmus vindt men, dat de gehele veelvouden van m juist alle exponenten n van a zijn met de eigenschap dat $a^n = e$ of m.a.w., dat kern $f = Z_m$, waarin Z_m de ondergroep in

Z is van de m-vouden. Dus in dit geval is $^{Z}/\text{kern } f = {}^{Z}/Z_m = \overline{Z}_m$ (zie voorbeeld in §5 na gevolg 5.15).

Samenvattend volgt uit het bovenstaande dat

(1) als de voorbrengende a van (a) niet van eindige orde is, dan (a) $\cong$ Z is en

(2) als a van eindige orde m is, dan (a) $\cong \overline{Z}_m$ is.

Hiermee is stelling 4.4 opnieuw bewezen.

8) $G = S_3$ en $N = \{a_1, a_5, a_6\}$ is normaaldeler in S_3 (zie blz.27). De nevenklassen N en Na_2 (of a_2N) zijn de elementen van G/N. Omdat $(Na_2) \otimes (Na_2) = N$ $(a_2^2=a_1)$, het neutrale element van G/N, volgt hieruit dat $G/N \cong$ de cyclische groep van de orde 2. Men kan ook 'n afbeelding $f : S_3 \to \overline{Z}_2$ definiëren door $(a_1)f = [0]$, $(a_2)f = [1]$. $(a_3)f = [1]$, $(a_4)f = [1]$, $(a_5)f = [0]$ en $(a_6)f = [0]$. Om aan te tonen dat f een homomorfie is, moet men bewijzen dat $(x \circ y)f = (x)f + (y)f$ voor alle $x, y \in S_3$. Omdat kern $f = \{a_1, a_5, a_6\} = N$, volgt uit stelling 6.10 dat $G/N \cong \overline{Z}_2$.

Het is eenvoudig in te zien dat een factorgroep van een commutatieve groep noodzakelijk commutatief is. Men kan de vraag stellen of een niet-commutatieve groep commutatieve factorgroepen kan hebben. Of, ook, wat volgens st.6.9 hetzelfde is, kan zo'n groep homomorf op een commutatieve groep worden afgebeeld?

Definitie 6.11. (G,*) is een gegeven groep. Als $a, b \in G$, dan is de commutator van a en b, per definitie, het element $a * b * \bar{a} * \bar{b}$.

Een standaard notatie is: $[a,b] = a * b * \bar{a} * \bar{b}$.

Er geldt: $a * b = b * a$ dan en slechts dan als $[a,b] = e$. De commutatoren vormen geen ondergroep in G, omdat zij niet gesloten zijn onder de operatie *. Daarom voeren we de ondergroep in, die wordt voortgebracht door de verzameling commutatoren. Deze ondergroep heet de commutator ondergroep van G en wordt genoteerd met [G,G] (zie voor de definitie §4).

De inverse van een commutator is weer 'n commutator: $[a,b]^{-1} = [b,a]$, zoals men onmiddellijk inziet. Dus in de definitie van [G,G] is het niet nodig expliciet de inversen op te nemen; de elementen van [G,G] bestaan uit producten van eindig veel commutatoren. D.w.z.

$$[G,G] = \{\Pi[a_i,b_i] \mid a_i, b_i \in G\}$$

waarin het symbool Π een eindig product met één of meer factoren voorstelt (zie [S] in §4).

Stelling 6.12. De groep [G,G] is normaaldeler in (G,*).

Bewijs. We weten al dat [G,G] ondergroep is in G.

Stel nu $a \in G$ en $c \in [G,G]$. Dan volgt:

$a * c * \bar{a} = (a*c*\bar{a}*\bar{c}) * c = [a,c] * c$. Het element $[a,c] * c$ is een eindig product van commutatoren en behoort dus tot [G,G]. Dus $a[G,G]\bar{a} \subseteq [G,G]$ voor iedere $a \in G$. Volgens st.5.13 is [G,G] dus normaaldeler in G.

Men kan nu de factorgroep G/[G,G] vormen.

Hiervoor geldt:

Stelling 6.13. H is normaaldeler in G. Dan is de factorgroep G/H commutatief dan en slechts dan als $[G,G] \subseteq H$.

Bewijs. Stel aH en bH zijn 2 willekeurige elementen in G/H. Omdat de nevenklasse eH = H het neutrale element is in G/H, is de groepsoperatie $\otimes$ in G/H commutatief dan en slechts dan als

$$H = [aH, bH] = (aH) \otimes (bH) \otimes (aH)^{-} \otimes (bH)^{-}$$

of, wat op hetzelfde neerkomt,

$$H = (a*b*\bar{a}*\bar{b})H.$$

Een nodige en voldoende voorwaarde opdat de laatste gelijkheid geldt, is $[a,b] = a * b * \bar{a} * \bar{b} \in H$. M.a.w. commutativiteit van de factorgroep G/H is equivalent met de eis dat de ondergroep H alle commutatoren van G bevat. Omdat [G,G] per definitie de kleinste ondergroep is met deze eigenschap (zie def.4.1), is de laatste voorwaarde equivalent met $[G,G] \subseteq H$.

Een speciaal geval is H = [G,G]:

Gevolg 6.14. Voor iedere groep G, is de factorgroep G/[G,G] commutatief.

Bijv. $N = \{a_1, a_5, a_6\} = [S_3, S_3]$ en $S_3/[S_3, S_3] \cong \bar{Z}_2$ (voorbeeld 8).

VII. Permutatiegroepen en de stelling van Cayley.

Definitie 7.1. S is een niet-lege verzameling. A(S) is de verzameling van alle 1-1-afbeeldingen van S op zichzelf.

Stelling 7.2. A(S) is een groep t.o.v. de operatie $\circ$: samenstellen van afbeeldingen.

Bewijs: We tonen aan dat de volgende eigenschappen gelden:

(1) $\sigma \in A(S), \tau \in A(S) \rightarrow \sigma \circ \tau \in A(S)$.

(2) $\sigma, \tau, \mu \in A(S) \rightarrow (\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$.

(3) er bestaat een element 1_S (de identieke afbeelding) in A(S) zodat $\sigma \circ 1_S = 1_S \circ \sigma = \sigma$ voor iedere $\sigma \in A(s)$

(4) voor iedere $\sigma \in A(S)$ bestaat een element $\sigma^{-1} \in A(S)$ (de inverse van σ) zodat $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1_S$.

ad (1). Per definitie is $\sigma \circ \tau$ de afbeelding van S in S waarvoor geldt $(s)(\sigma \circ \tau) = (s\sigma)\tau$. Als $S = \{s\}$, dan is $(s)\sigma = s$, $(s)\tau = s$ en $(s)(\sigma \circ \tau) = s$, dus $\sigma \circ \tau \in A(S)$. Stel nu $s_1, s_2 \in S$ en $s_1 \neq s_2$. Omdat σ een 1-1-afbeelding is, volgt $s_1\sigma \neq s_2\sigma$. Omdat τ ook 1-1 is en $s_1\sigma \neq s_2\sigma$ volgt $(s_1\sigma)\tau \neq (s_2\sigma)\tau$, dus $s_1(\sigma \circ \tau) = (s_1\sigma)\tau \neq (s_2\sigma)\tau = s_2(\sigma \circ \tau)$. Dus $\sigma \circ \tau$ is een 1-1-afbeelding. Stel $t \in S$. Omdat τ een op-afbeelding is, is er een element $s \in S$ met $(s)\tau = t$ (s is ook eenduidig wegens het 1-1-karakter van τ). Omdat τ een op-afbeelding is, is er een element $s_1 \in S$ met $s_1\sigma = s$; dan is $s_1(\sigma \circ \tau) = (s_1\sigma)\tau = (s)\tau = t$, dus $\sigma \circ \tau$ is een op-afbeelding. Dan is $\sigma \circ \tau \in A(S)$.

ad (2). Voor een willekeurig element $s \in S$ geldt
$s((\sigma \circ \tau) \circ \mu) = (s(\sigma \circ \tau))\mu = ((s\sigma)\tau)\mu$ en
$s(\sigma \circ (\tau \circ \mu)) = (s\tau)(\tau \circ \mu) = ((s\sigma)\tau)\mu$. Dus
$(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$.

ad (3). 1_S is de identieke afbeelding d.w.z. $s1_S = s$ voor iedere $s \in S$. Dus $s(\sigma \circ 1_S) = (s\sigma)1_S = s\sigma = (s1_S)\sigma = s(1_S \circ \sigma)$ voor iedere $s \in S$. Dan $\sigma \circ 1_S = \sigma = 1_S \circ \sigma$.

ad (4). Als $s \in S$ gegeven is, dan bestaat er, omdat σ een op-afbeelding is, een element $s_1 \in S$ zodat $s_1\sigma = s$.
Omdat σ ook 1 - 1 is, is s_1 eenduidig bepaald.

We definiëren de afbeelding $\sigma^{-1} : S \to S$ door $s_1 = (s)\sigma^{-1}$ dan en slechts dan als $s = s_1\sigma$.
Dan geldt, als $s \in S$ en $t = s\sigma$, dat $s = t\sigma^{-1}$.
Dus $s(\sigma\circ\sigma^{-1}) = (s\sigma)\sigma^{-1} = t\sigma^{-1} = s$, zodat $\sigma \circ \sigma^{-1} = 1_S$.
Evenzo $s(\sigma^{-1}\circ\sigma) = (s\sigma^{-1})\sigma = s_1\sigma = s$, zodat $\sigma^{-1} \circ \sigma = 1_S$.
Nu volgt uit $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1_S$, dat σ^{-1} een 1-1-afbeelding op is.
Merk eerst op dat σ^{-1} een op-afbeelding is, want als $t \in S$ gegeven is, dan is $t = t(\sigma\circ\sigma^{-1}) = (t\sigma)\sigma^{-1}$ en dus is t het beeld onder σ^{-1} van 't element $t\sigma$ in S.
Merk dan op dat σ^{-1} 1-1-afbeelding is, want als $s_1\sigma^{-1} = s_2\sigma^{-1}$, dan volgt $s_1 = s_1(\sigma^{-1}\circ\sigma) = (s_1\sigma^{-1})\sigma = (s_2\sigma^{-1})\sigma = s_2(\sigma^{-1}\circ\sigma) = s_2$.
Dus $\sigma^{-1} \in A(S)$.
Volgens definitie 1.1. is A(S) een groep. Hiermee is de stelling bewezen.

Als de verzameling S uit n elementen bestaat, is A(S) een eindige groep die n! elementen heeft. Immers iedere 1-1-afbeelding σ van S op zichzelf bepaalt een permutatie van de n elementen van S:

$$\begin{pmatrix} s_1 & \cdots & s_n \\ (s_1)\sigma & \cdots & (s_n)\sigma \end{pmatrix}$$ en omgekeerd is door iedere permutatie van

de n elementen van S een 1-1-afbeelding van S op zichzelf bepaald. Het aantal permutaties van n elementen is n! , dus $O(A(S)) = n!$
In dit geval noteert men de groep A(S) met S_n (zie voorbeeld 7, §1).
In plaats van de elementen $s_1, s_2, \ldots, s_n$ in S neemt men alleen de indices $1, 2, \ldots, n$ en een element van S_n is dus een permutatie van de getallen $1, \ldots, n$. S_n heet de symmetrische groep van de orde n! We hebben al gezien dat S_n niet abels is voor $n > 2$ (§1).
We bewijzen nu een stelling voor A(S), die bekend staat als de stelling van Cayley:

Stelling 7.3. Iedere groep G is isomorf met een ondergroep van A(S) voor een geschikte verzameling S.

Bewijs. $(G,*)$ is een groep, dus G, als verzameling opgevat, is niet leeg. Voor de verzameling S gebruiken we de elementen van G; d.w.z. stel $S = G$. Voor $g \in G$, definiëren we $\tau_g : S(=G) \to S(=G)$ door middel van $x\tau_g = x * g$ voor iedere $x \in G$. Als $y \in G$, dan is $y = (y*\bar{g}) * g = (y*\bar{g})\tau_g$, zodat τ_g de verzameling S op zichzelf afbeeldt. Bovendien is τ_g een 1-1-afbeelding, want als $x, y \in S$ en $x\tau_g = y\tau_g$ dan is $x * g = y * g$ en volgens st.2.2 (vereenvoudigingswet) volgt hieruit dat $x = y$. Dus voor iedere $g \in G$ is $\tau_g \in A(S)$. Als $g, h \in G$, beschouw dan t_{g*h}. Voor iedere $x \in S = G$ geldt: $x\tau_{g*h} = x * (g*h) = (x*g)*h = (x\tau_g)\tau_h = x(\tau_g \circ \tau_h)$. Hieruit volgt dat $\tau_{g*h} = \tau_g \circ \tau_h$. Definieer nu een afbeelding $\psi : G \to A(S)$ door middel van $(g)\psi = \tau_g$ voor iedere $g \in G$. Er volgt dat $(g*h)\psi = \tau_{g*h} = \tau_g \circ \tau_h = (g)\psi \circ (h)\psi$ en ψ is een homomorfie volgens definitie 6.1. De verzameling $K = \{g_0 \mid g_0 \in G \text{ en } (g_0)\psi = \tau_{g_0} = 1_S\}$ is volgens definitie 6.5 kern ψ. Voor iedere $x \in G$ geldt $x\tau_{g_0} = x1_S = x$. In het bijzonder, als e het neutrale element is van G, geldt $e\tau_{g_0} = e$. Maar ook $e\tau_{g_0} = e * g_0 = g_0$ volgens definitie van τ_g, dus $g_0 = e$ en $K = \text{kern } \psi = \{e\}$. Volgens gevolg 6.8 is ψ een isomorfie van G in A(S) en dus is G isomorf met Im ψ, hetgeen een ondergroep is van A(S) (st.6.3). Hiermee is de stelling bewezen.

Stelling 7.3 stelt ons in staat een abstracte groep te identificeren met een groep van bijectieve afbeeldingen van een verzameling S op zichzelf. Merk echter op, dat ψ een isomorfie in is, in het algemeen. Gebruikt men $S = G$ voor een eindige groep G met $O(G) = n$, dan vindt men dat $A(S) = S_n$ juist n! elementen heeft. Een eindige groep van de orde n is dus isomorf met een echte ondergroep van S_n voor $n > 2$.

We zullen nu de groep S_n wat nader onderzoeken.
Laat $S = \{1, 2, \ldots, n\}$. Als $\phi \in A(S) = S_n$, dan is ϕ een 1-1-afbeelding van S op zichzelf of een permutatie van de getallen $\{1, 2, \ldots, n\}$. Men kan ϕ "uitschrijven" door bijv. $\phi : 1 \to i_1, 2 \to i_2, \ldots, n \to i_n$ of in andere notatie

$$\phi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} .$$

Als $\theta,\psi \in S_n$, dan verstaat men onder $\theta \circ \psi$ of $\theta\psi$ de permutatie van S, die ontstaat door eerst θ en op het resultaat ψ toe te passen (zie st.7.2).
Bijv. $n = 4$: $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \Rightarrow \theta\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$.

Voor een willekeurige niet-lege verzameling S voeren we een relatie in.
Laat $\theta \in A(S)$. Als $a, b \in S$, dan definiëren we $a \equiv_\theta b$ dan en slechts dan als $b = a\theta^i$ voor 'n getal $i \in Z$.
De bewering is dat "$\equiv_\theta$" een equivalentie-relatie is op S.
Want (1) $a \equiv_\theta a$ omdat $a = a\theta^0 = a1_S$.

(2) als $a \equiv_\theta b$, dan is $b = a\theta^i (i \in Z)$, dus $a = b\theta^{-i}$ $(-i \in Z)$ en $b \equiv_\theta a$.

(3) als $a \equiv_\theta b$, $b \equiv_\theta c$, dan is $b = a\theta^i$, $c = b\theta^j = (a\theta^i)\theta^j = a\theta^{i+j}$, dus $a \equiv_\theta c$.

Deze equivalentie-relatie bewerkt een partitie van S in disjuncte deelverzamelingen, n.l. de equivalentie-klassen.
De equivalentie-klasse van $s \in S$ heet de <u>kring</u> (Eng. orbit) <u>van s onder θ</u>; de kring van s onder θ bestaat uit alle elementen van de vorm $s\theta^i$, $i = 0, \pm 1, \pm 2, \ldots$.
Hierbij is $\theta^0 = 1_S$.
We passen het begrip kring nu toe op de verzameling $S = \{1, 2, \ldots, n\}$.
Omdat S eindig is, zijn niet alle elementen $s\theta^i (s \in S, \theta \in A(S) = S_n)$ verschillend van s, d.w.z. $s = s\theta^i$ voor een geheel getal $i (\neq 0)$. Als $s = s\theta^i$ met $i < 0$, dan is $s\theta^{-i} = (s\theta^i)\theta^{-i} = s\theta^0 = s1_S = s$, en $-i > 0$.
Er is dus een kleinste positief geheel getal $l = l(s)$, dat van s afhangt zodat $s\theta^l = s$. De kring van s onder θ bestaat uit de elementen $\{s, s\theta, s\theta^2, \ldots, s\theta^{l-1}\}$.

<u>Voorbeeld</u>. $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$; $S = \{1, 2, 3, 4, 5, 6\}$.

Kring van 1 onder θ is $\{1(=1\theta^0), 1\theta^1 = 2\}$, $(1\theta^2 = 2\theta = 1)$.
Kring van 2 onder θ is dus ook $\{1, 2\}$. Kring van $3 = \{3\}$.
Kring van 4 onder θ is $\{4, 4\theta = 5, 4\theta^2 = 5\theta = 6\}$, $(4\theta^3 = 6\theta = 4)$.
We introduceren nu een speciaal type permutatie in de volgende definitie:
<u>Definitie 7.4.</u> Stel $n_1, n_2, \ldots, n_k$ zijn k verschillende getallen tussen 1 en n. Als een permutatie $\sigma \in S_n$ zodanig is, dat $(n_i)\sigma = n_{i+1}$ voor $1 \leq i < k$, $(n_k)\sigma = n_1$ en $(n_j)\sigma = n_j$ voor $n_j \in S \setminus \{n_1, n_2, \ldots n_k\}$ $(S=\{1,2,\ldots n\})$ dat heet σ een <u>cykel van lengte k</u> ofwel een <u>k-cykel.</u>

Een cykel is dus een toevoeging : $n_1 \to n_2 = (n_1)\sigma$, $n_2 \to n_3 = (n_2)\sigma = (n_1)\sigma^2$, ..., $n_{k-1} \to n_k = (n_{k-1})\sigma = (n_1)\sigma^{k-2}$, $n_k \to n_1 = (n_k)\sigma$, en de overige getallen in $S = \{1, 2, \ldots, n\}$ blijven onveranderd. De verzameling $\{n_1, n_2, \ldots, n_k\}$ is de kring van $n_i (i=1.,k)$ onder σ. De kring van $n_j \notin \{n_1, n_2, \ldots n_k\}$ onder σ bestaat alleen uit n_j. Voor de cykel σ van lengte k noteert men $\sigma = (n_1, n_2, \ldots, n_k)$.

Voorbeeld. In S_5 heeft men : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = (2\ 5\ 3)$ is een 3-cykel.

In S_6 is $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 5 & 1 \end{pmatrix} = (1\ 3\ 6)$ ook een 3-cykel.

De notatie voor een cykel is zo, dat ieder element in de cykel op de 1^e plaats geschreven kan worden bijv. $(2\ 5\ 3) = (5\ 3\ 2) = (3\ 2\ 5)$ in S_5. Omdat cykels een speciaal soort permutaties zijn, kan men cykels samenstellen. Het resultaat is een permutatie van S.

Stelling 7.5. $S = \{1, 2, \ldots, n\}$. Als $\sigma \in S_n$, dan kan σ geschreven worden als een product van disjuncte cykels in de volgende betekenis:

$$\sigma \to \tau_1 \circ \tau_2 \circ \ldots \circ \tau_p$$

waarin τ_i cykels $(i=1,2,\ldots p)$ en $\tau_i \cap \tau_j = \emptyset$ voor $i \neq j$.

Bewijs. Stel $i_1 \in S$ en $i_2 = (i_1)\sigma$, $i_3 = (i_2)\sigma$, ..., $i_{\alpha+1} = (i_\alpha)\sigma$, ... enz. Omdat S eindig is, bereiken we een punt, waarin het nieuwe gehele getal in deze rij gelijk is aan één van zijn voorgangers. Stel dat $i_{\alpha+1}$ de eerste is van $i_1, i_2, \ldots, i_\alpha, i_{\alpha+1}$, die gelijk is aan één van zijn voorgangers. De bewering is dat $i_{\alpha+1} = i_1$. Immers, als $i_{\alpha+1} \neq i_1$, dan is $i_{\alpha+1}$ één uit de rij $i_2, \ldots, i_\alpha$, bijv. $i_{\alpha+1} = i_\beta$ met $1 < \beta \leq \alpha$. Dan volgt $(i_{\beta-1})\sigma = i_\beta = i_{\alpha+1} = (i_\alpha)\sigma$. Maar $i_\alpha \neq i_{\beta-1}$, dus σ zou niet 1-1 zijn. Daarom is $i_{\alpha+1} = i_1$. Noem nu τ , de α-cykel: $\tau_1 = (i_1\ i_2\ \ldots\ i_\alpha)$.

Stel $j_1 \in S$, is 'n getal, dat verschillend is van $i_1, i_2, \ldots, i_\alpha$. Precies, als hierboven, kan men getallen $j_2 = (j_1)\sigma, \ldots, j_\beta = (j_{\beta-1})\sigma$ vinden met $j_1 = (j_\beta)\sigma$. Stel weer τ_2 de β-cykel: $\tau_2 = (j_1 j_2 \ldots j_\beta)$. Geen van de getallen $j_1, j_2, \ldots, j_\beta$ is gelijk aan één van de getallen $i_1, i_2, \ldots, i_\alpha$. Want stel j_s is de eerste uit $j_1, \ldots, j_\beta$ die gelijk is aan één van de getallen $i_1, i_2, \ldots, i_\alpha$ bijv. $j_s = i_r$. Wegens de constructie van j_1, is $s > 1$.

Dan is $(j_{s-1})\sigma = j_s = i_r = \begin{cases} (i_{r-1})\sigma & \text{als } r > 1 \\ (i_\alpha)\sigma & \text{als } r = 1 \end{cases}$.

Omdat σ een 1-1-afbeelding is, volgt dat $j_{s-1} = \begin{cases} i_{r-1} & \text{als } r > 1 \\ i_\alpha & \text{als } r = 1 \end{cases}$.

Dit is in tegenspraak met het feit dat j_{s-1} niet gelijk is aan één van de getallen $i_1, \ldots, i_\alpha$. Dus $\tau_1 \cap \tau_2 = \emptyset$.
Dan, op dezelfde manier, als $k_1 \notin \tau_1$, $k_1 \notin \tau_2$ ($k_1 \in S$), construeren we een j-cykel

$$\tau_3 = (k_1\ k_2\ \ldots\ k_\gamma) .$$

Geen van de getallen $k_1, \ldots, k_\gamma$ is gelijk aan één van de getallen $i_1, \ldots i_\alpha, j_1, \ldots, j_\beta$ wordt op dezelfde manier als hierboven bewezen.
Het is duidelijk dat op deze manier een partitie van S ontstaat in disjuncte cykels. Elk element van S behoort tot één en precies één cykel, omdat elke cykel de kring van elk van zijn elementen is onder σ.
Stel nu s is een willekeurig element van S en bijv. $s \in \tau_i$ ($1 \leq i \leq p$).
Dan $s \notin \tau_j$, $j \neq i$, ($j \in \{1, \ldots p\}$). Dus volgens definitie 7.4 is $(s)\tau_j = s$ en $(s)\ (\tau_1 \circ \tau_2 \ldots \circ \tau_p) = (s)\tau_i$. Omdat τ_i een kring is onder σ, geldt ook $(s)\tau_i = (s)\sigma$, want $s \in \tau_i$. Dus $(s)\ (\tau_1 \circ \tau_2 \ldots \circ \tau_p) = (s)\sigma$ zodat $\sigma = \tau_1 \circ \tau_2 \ldots \circ \tau_p$. Hiermee is de stelling bewezen.

Een speciaal soort cykels zijn de cykels van lengte 2.
Zo'n cykel heeft de vorm $\tau = (i\ j)$, $i \neq j$ en heet een <u>transpositie</u>.
Beschouw de k-cykel $(n_1 n_2 \ldots n_k)$. Men kan direct bewijzen, dat $(n_1 n_2 \ldots n_k) = (n_1 n_2)\ (n_1 n_3) \ldots (n_1 n_k)$. Deze ontbinding is niet eenduidig. Hiermee bedoelen we dat een k-cykel op meer dan één manier als een product van transposities geschreven kan worden. Bijv. (1 2 3) = (12) (3) = = (23) (21).Omdat, volgens st.7.5, iedere permutatie een product van disjuncte cykels is en iedere cykel een product van transposities, is het duidelijk dat

<u>Gevolg 7.6</u>. Iedere permutatie in S_n is een product van transposities.
Dus volgens §4 vormen de transposities in S_n een stelsel voortbrengenden van S_n.
Een transpositie kan niet de identieke afbeelding zijn. Dus als we 1_S schrijven als het product van u transposities, dan is $u \geq 2$. Bovendien als 1_S het product is van 2 transposities, dan moeten ze gelijk zijn.
We bewijzen nu

<u>Stelling 7.7</u>. Als 1_S geschreven kan worden als het product van

$u \geq 3$ transposities, dan kan 1_S geschreven worden als het product van $u - 2$ transposities.

Bewijs: Stel $1_S = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_u$, waarin de τ_i transposities zijn. Stel dat $\tau_j = (xy)$ en dat y niet voorkomt in één van de τ_h met $h < j$. Dan moet y voorkomen in een τ_k met $k > j$, want anders zou $y = (y)1_S = (y)\tau_j = x$ zijn.

Beschouw alle uitdrukkingen van 1_S als het product van u transposities, waarin de eerste j transposities zijn $\tau_1, \tau_2, \ldots, \tau_j$. Aan elke uitdrukking van deze vorm kunnen we het gehele getal toevoegen:

$$m = \min \{k \in Z \mid k > j \text{ en } y \in \tau_k\}.$$

Kies, onder al deze uitdrukkingen, er één met $m = m_0$ minimaal. Stel dat deze uitdrukking is

$$1_S = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_j \circ \ldots \circ \tau_u.$$

We beweren dat de minimale $m_0 = j + 1$. Want stel $m_0 > j + 1$ en laat $\tau_{m_0} = (yz)$. Volgens de definitie van m_0, komt y niet voor in τ_{m_0-1}. Als z niet voorkomt in τ_{m_0-1}, dan zijn τ_{m_0} en τ_{m_0-1} verwisselbaar, en dus

$$1_S = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_j \circ \ldots \circ \tau_{m_0-2} \circ \tau_{m_0} \circ \tau_{m_0-1} \circ \tau_{m_0+1} \circ \ldots \circ \tau_u,$$

hetgeen in strijd is met de keuze van m_0, want $y \in \tau_{m_0}$.

Als z voorkomt in τ_{m_0-1}, bijv. $\tau_{m_0-1} = (z\ w)$, hebben we

$$\tau_{m_0-1} \circ \tau_m = (z\ w) \circ (y\ z) = (y\ z) \circ (y\ w)$$

en dus

$$1_S = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_{m_0-2} \circ (y\ z) \circ (y\ w) \circ \tau_{m_0+1} \circ \ldots \circ \tau_u$$

hetgeen opnieuw in strijd is met de keuze van m_0.

Dus $m_0 = j + 1$, wegens $m_0 \geq j + 1$.

Stel nu dat $\tau_1 = (x_1\ x_2)$. Onder alle uitdrukkingen van 1_S als het product van u transposities met als eerste transpositie τ_1, kiezen we er één met minimale m, d.w.z. $m = 2$. Dus $x_2 \in \tau_2$ en $\tau_2 = (x_2\ x_3)$. Onder alle uitdrukkingen van 1_S als het product van u transposities met als eerste 2

transposities τ_1, τ_2, kiezen we er één met minimale m, d.w.z. m = 3. Dus $x_3 \in \tau_3$ en $\tau_3 = (x_3\ x_4)$ enz. Omdat het product van de u transposities $= 1_S$ is, kunnen we een geheel getal s vinden met $2 \leq s \leq u$ en een uitdrukking: $1_S = (x_1\ x_2) \circ (x_2\ x_3) \circ \ldots \circ (x_{s-1}\ x_s) \circ (x_s\ x_1) \circ$

$\circ\ \tau_{s+1} \circ \ldots \circ \tau_u$.

Dan geldt ook:

$$1_S = (x_2\ x_s) \circ (x_2\ x_{s-1}) \circ \ldots \circ (x_2\ x_3) \circ \tau_{s+1} \circ \ldots \circ \tau_u$$

hetgeen men inziet door achtereenvolgens het effect van 1_S op $x_1, x_2, \ldots, x_s$ in beide uitdrukkingen te beschouwen.
Omdat de laatste uitdrukking uit u - 2 transposities bestaat, is hiermee de stelling bewezen.

Gevolg 7.8. De identieke afbeelding 1_S kan nooit het product zijn van een oneven aantal transposities.

Stelling 7.9. Als $\phi \in S_n$ en als

$$\phi = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_s = \tau_1' \circ \tau_2' \circ \ldots \circ \tau_t',$$

waarin τ_i en τ_j' transposities zijn $(i=1,\ldots s; j=1,\ldots,t)$
dan is $S \equiv t \pmod 2$.

Bewijs. Uit de schrijfwijze voor ϕ volgt:

$$1_S = \phi \circ \phi^{-1} = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_s \circ (\tau_t')^{-1} \circ \ldots \circ (\tau_1')^{-1}$$

$$1_S = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_s \circ \tau_t' \circ \ldots \circ \tau_1'.$$

Volgens gevolg 7.8, is $s + t \equiv 0 \pmod 2$ of s + t is even, dus ook $2s - (s+t) = s - t$ is even of $s \equiv t \pmod 2$.

Definitie 7.10. Een permutatie $\phi \in S_n$ heet een oneven permutatie als ϕ geschreven kan worden als het product van een oneven aantal transposities en ϕ heet een even permutatie als ϕ geschreven kan worden als het product van een even aantal transposities.
Volgens st.7.9 is het voor een permutatie onmogelijk tegelijkertijd even en oneven te zijn en volgens gevolg 7.6 is iedere permutatie dus òf even òf oneven. Een even permutatie wordt van even pariteit genoemd, van een oneven permutatie is de pariteit oneven.

Het is gemakkelijk om de pariteit van een product van twee permutaties te bepalen uit die van hun factoren. Want, stel $\phi = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$ en $\sigma = \tau_1' \circ \tau_2' \circ \ldots \circ \tau_s'$, waarin τ_i, τ_j' transposities zijn, dan is $\phi \circ \sigma$ een product van r + s transposities. Dus de pariteit van $\phi \circ \sigma$ wordt gegeven door de volgende tabel:

ϕ	σ	$\phi \circ \sigma$
even	even	even
even	oneven	oneven
oneven	oneven	even
oneven	even	oneven

De verzameling S_n van permutaties van $S = \{1, 2, \ldots, n\}$ heeft een partitie in 2 klassen, de even en oneven permutaties. We bewijzen nu:

Stelling 7.11. Laat $n \geq 2$ en A_n is de verzameling van even permutaties in S_n. Dan is A_n normaaldeler in S_n en $[S_n : A_n] = 2$.

Bewijs. Stel dat $W = \{1, -1\}$ de multiplicatieve groep van de gehele getallen 1 en -1 is. Definieer een afbeelding $\psi : S_n \to W$ door $(\phi)\psi = 1$, als $\phi \in S_n$ even is en $(\phi')\psi = -1$ als $\phi' \in S_n$ oneven is. Volgens de tabel van de partiteiten is ψ een homomorfie van S op W. De kern van ψ is precies A_n. Dus volgens st.6.6 is A_n normaaldeler in S_n. Volgens st.6.10 geldt $S_n/A_n \tilde{=} W$. Dus volgens gevolg 5.15 geldt $[S_n : A_n] = \frac{O(S_n)}{O(A_n)} = O(S_n/A_n) = O(W) = 2$.

Dus A_n bevat $\frac{1}{2}n!$ elementen en $S \setminus A_n$, de verzameling van oneven permutaties, bevat $\frac{1}{2}n!$ elementen.

VIII. Automorfieën

Een bijzonder belangrijke klasse van homomorfieën zijn de isomorfieën van een groep G op zichzelf. Een dergelijke afbeelding is zowel een permutatie van de elementen van G als een homomorfie.

Definitie 8.1. G is een groep en f is een isomorfie van G op G. Dan heet f een automorfie van G. Een triviaal voorbeeld van een automorfie is de identieke afbeelding 1_G van de groep G op zichzelf. Iedere automorfie van een groep G is een permutatie van de elementen van G d.w.z. een 1-1-afbeelding van de verzameling G op zichzelf. Dus de automorfieën van G vormen een deelverzameling Aut(G) van de verzameling A(G) van alle 1-1-afbeeldingen van de verzameling G op zichzelf. Volgens st.7.2 is A(G) een groep t.o.v. de operatie: samenstellen van afbeeldingen.

Stelling 8.2. Aut(G) is een ondergroep van A(G).

Bewijs: Aut(G) is een niet-lege deelverzameling van A(G), want $1_G \in \mathrm{Aut}(G)$. Stel nu $f, g \in \mathrm{Aut}(G)$. Omdat $f, g \in A(G)$, is $f \circ g^{-1} \in A(G)$, want A(G) is een groep. Er geldt: $(a * b)(f \circ g^{-1}) = [(a * b)f]g^{-1} = [(a)f * (b)f]g^{-1}$ voor willekeurige elementen $a, b \in G$. Omdat f en g beide 1-1-afbeeldingen op (bijecties) zijn, bestaan er eenduidig bepaalde elementen $a', b' \in G$ zodat $(a)f = (a')g$ en $(b)f = (b')g$. Men heeft dus: $a' = [(a)f]g^{-1}$ en $b' = [(b)f]g^{-1}$. Dus $[(a)f * (b)f]g^{-1} = [(a')g * (b')g]g^{-1} = [(a' * b')g]g^{-1} = (a' * b')(g \circ g^{-1}) = (a' * b')1_G = a' * b' = [(a)f]g^{-1} * [(b)f]g^{-1}$. Dus $(a * b)(f \circ g^{-1}) = [(a)f]g^{-1} * [(b)f]g^{-1}$ voor ieder paar $a, b \in G$. Dan is $f \circ g^{-1}$ een homomorfie van G in zichzelf. Maar $f \circ g^{-1} \in A(G)$, dus de homomorfie is surjectief. Bovendien is $f \circ g^{-1}$ injectief, dus $f \circ g^{-1}$ is een isomorfie van G op zichzelf (gevolg 6.8). Dan is $f \circ g^{-1} \in \mathrm{Aut}(G)$. Volgens st.3.3. is Aut G dus een ondergroep van A(G).

Opmerking. Aut(G) is, in het algemeen, geen normaaldeler in A(G). Bijv. $Z_3 = \{[0],[1],[2]\}$ is de groep van gehele getallen modulo 3. Een automorfie f van Z_3 voert het element [0] in zichzelf over (st. 6.2). Verder is f bepaald door $\{[1]\}f$, want $\{[2]\}f = [1]f + [1]f$. Omdat

$[1]f \neq [0]$, heeft men óf $[1]f = [1]$ óf $[1]f = [2]$. In het eerste geval is f de identieke afbeelding 1_{Z_3}, in het tweede geval heeft men $[0]f = [0]$, $[1]f = [2]$, $[2]f = [1]$. Dus Aut $(Z_3) = \{1_{Z_3}, f\}$, waarbij $f^2 = 1_{Z_3}$. Omdat $O(Z_3) = 3$, is $A(Z_3) = S_3$. Stel $\sigma = ([0],[1],[2])$ is een element van $A(Z_3)$ (3-cykel). Dan is $\sigma^{-1} = ([0],[2],[1])$ en $\sigma \circ f \circ \sigma^{-1} = ([0],[1])$ (2-cykel) in $A(Z_3)$ voor $f \in \text{Aut}(Z_3)$. Dus $\sigma \circ f \circ \sigma^{-1} \notin \text{Aut}(Z_3)$. Wegens st.5.13 is $\text{Aut}(Z_3)$ geen normaaldeler in $A(Z_3)$.

Een bijzonder soort automorfieën zijn de z.g. inwendige automorfieën. Stel a is een vast element van de groep G. Definieer de afbeelding $\sigma_a : G \to G$ door

$$(x)\sigma_a = \overline{a} * x * a \text{ voor iedere } x \in G.$$

We zullen nu aan tonen dat σ_a een automorfie van G is. Vooreerst is σ_a een homomorfie: als $x_1, x_2 \in G$, dan geldt

$$(x_1 * x_2)\sigma_a = \overline{a} * (x_1 * x_2) * a =$$
$$= (\overline{a} * x_1 * a) * (\overline{a} * x_2 * a) = (x_1)\sigma_a * (x_2)\sigma_a.$$

Vervolgens is σ_a een surjectieve afbeelding: als x een willekeurig element van G is, dan is $(a * x * \overline{a})\sigma_a = x$. Tenslotte is σ_a ook injectief: stel $(x_1)\sigma_a = (x_2)\sigma_a$, dan is $\overline{a} * x_1 * a = \overline{a} * x_2 * a$. Door de vereenvoudigingswet (st.2.2) toe te passen, volgt hieruit $x_1 = x_2$. Dus σ_a is een automorfie van G. Afbeeldingen van de vorm $\sigma_a \in \text{Aut}(G)$, met $a \in G$, worden inwendige automorfieën van de groep G genoemd. Preciezer:
σ_a is de inwendige automorfie, geïnduceerd door het element a.

De verzameling van inwendige automorfieën van G noteren we:
$I(G) = \{\sigma_a \mid a \in G\}$.

Stelling 8.3. I(G) is een normaaldeler in Aut(G).

Bewijs: Stel $\sigma_a, \sigma_b \in I(G)$. Dan is, voor iedere $x \in G$:
$(x)(\sigma_a \circ \sigma_b) = ((x)\sigma_a)\sigma_b = (\overline{a} * x * a)\sigma_b = \overline{b} * (\overline{a} * x * a) * b =$
$= \overline{(a * b)} * x * (a * b)$, dus $\sigma_a \circ \sigma_b = \sigma_{a*b}$ voor $a, b \in G$. In het bijzonder volgt hieruit, voor het neutrale element $e \in G$: $\sigma_a \circ \sigma_e =$
$= \sigma_{a*e} = \sigma_a$ en $\sigma_e \circ \sigma_a = \sigma_{e*a} = \sigma_a$ voor iedere $\sigma_a \in I(G)$. Als $\overline{a}$ de inverse is van a in G, dan volgt ook: $\sigma_a \circ \sigma_{\overline{a}} = \sigma_{a*\overline{a}} = \sigma_e$ en

$\sigma_{\overline{a}} \circ \sigma_a = \sigma_{\overline{a}*a} = \sigma_e$. Nu is σ_e het neutrale element in Aut(G), want $(x)\sigma_e = \overline{e} * x * e = x$ voor iedere $x \in G$, dus $\sigma_e = 1_G$. Volgens st. 2.3 is er precies één element in Aut(G), dat de inverse is van $\sigma_a \in$ Aut(G). Hieraan voldoet $\sigma_{\overline{a}}$, dus $\sigma_{\overline{a}} = (\sigma_a)^{-1}$. Hieruit volgt nu, dat I(G) ondergroep is in Aut(G).

Om aan te tonen, dat I(G) normaaldeler is in Aut(G) moeten we laten zien, dat, als $f \in$ Aut(G), het product $f \circ \sigma_a \circ f^{-1} \in I(G)$ voor iedere $\sigma_a \in I(G)$. Er geldt: $(x)(f \circ \sigma_a \circ f^{-1}) = \{((x)f)\sigma_a\}f^{-1} = \{\overline{a} * (x)f * a\}f^{-1}$. Omdat $f^{-1} \in$ Aut(G) een homomorfie is, volgt:
$\{\overline{a} * (x)f * a\}f^{-1} = (\overline{a})f^{-1} * \{(x)f\}f^{-1} * (a)f^{-1} = (\overline{a})f^{-1} * x * (a)f^{-1}$.
In G geldt: $a * \overline{a} = \overline{a} * a = e$, dus als men hierop de homomorfie f^{-1} toepast: $(a)f^{-1} * (\overline{a})f^{-1} = (\overline{a})f^{-1} * (a)f^{-1} = (e)f^{-1} = e$ (st.6.2(a)), dus $(\overline{a})f^{-1} = \overline{(a)f^{-1}}$. Hieruit volgt $(x)(f \circ \sigma_a \circ f^{-1}) = \overline{(a)f^{-1}} * x * (a)f^{-1} = (x)\sigma_{(a)f^{-1}}$, voor iedere $x \in G$, zodat $f \circ \sigma_a \circ f^{-1} = \sigma_{(a)f^{-1}} \in I(G)$.

Volgens st.5.13 is I(G) dus normaaldeler in Aut(G).

Stelling 8.4. Voor iedere groep G geldt:

$$G/C(G) \cong I(G),$$

waarin C(G) het centrum van de groep G is (def. 3.4).

Bewijs: Definieer de afbeelding $\phi : G \to I(G)$ door $(a)\phi = \sigma_a$. Het is duidelijk dat ϕ een op-afbeelding is.
Er geldt: $(a * b)\phi = \sigma_{a*b} = \sigma_a \circ \sigma_b$ (bewijs st.8.3) $= (a)\phi \circ (b)\phi$. Dus ϕ is een homomorfie op. We willen aantonen dat Kern $\phi = C(G)$. Het neutrale element van I(G) is σ_e (bewijs st.8.3), dus kern $\phi = \{a \mid a \in G, (a)\phi = \sigma_e\}$ of Kern $\phi = \{a \mid a \in G, \sigma_a = \sigma_e\}$. Maar $\sigma_a = \sigma_e$ betekent $(x)\sigma_a = (x)\sigma_e$ voor iedere $x \in G$ of $\overline{a} * x * a = x$ voor iedere $x \in G$.
Dus $a \in G$ heeft de eigenschap: $a \in$ Kern ϕ dan en slechts dan als $x * a = a * x$ voor iedere $x \in G$ d.w.z. $a \in C(G)$. Dus Kern $\phi = C(G)$.
Pas nu de fundamentele st. 6.10 toe, dan volgt:

$$G/C(G) \cong I(G).$$

Gevolg 8.5. Als I(G) cyclisch is, dan is $I(G) = \{\sigma_e\}$.

Bewijs: Stel I(G) wordt voortgebracht door σ_a, $a \in G$. Wegens $(\sigma_a)^n = \sigma_{a^n}$ voor $n > 0$ en $(\sigma_a)^{-1} = \sigma_{\bar{a}}$, hebben de elementen van I(G) de vorm σ_{a^n}, n geheel. Als b een willekeurig element in G is, dan is $\sigma_b = \sigma_{a^k}$ voor een geheel getal k. Uit st.8.4 volgt $b \equiv a^k(C(G))$ of $b \in a^k C(G)$. Dus ieder element in G heeft de vorm $a^k * x$ met $k \in Z, x \in C(G)$. Uit $b_1 = a^{k_1} * x_1$ en $b_2 = a^{k_2} * x_2$ $(b_1, b_2 \in G)$ volgt $b_1 * b_2 = (a^{k_1} * x_1) * (a^{k_2} * x_2) = a^{k_1} * (x_1 * a^{k_2}) * x_2 = a^{k_1} * (a^{k_2} * x_1) * x_2 = a^{k_1+k_2} * x_1 * x_2$. Evenzo vindt men $b_2 * b_1 = a^{k_2+k_1} * x_2 * x_1$ en $x_1 * x_2 = x_2 * x_1$ wegens $x_1, x_2 \in C(G)$, dus $b_1 * b_2 = b_2 * b_1$. Dus G is abels. Dan is $C(G) = G$, dus wegens $G/C(G) \tilde{=} I(G)$, bestaat I(G) uit 1 element: $I(G) = \{\sigma_e\}$.

Voorbeelden.

1) $G = Z$, de additieve groep van de gehele getallen. Omdat Z cyclisch is met 1 als voortbrengende, is een automorfie ϕ van G bepaald door $(1)\phi$. Stel $(1)\phi = k$, $k \in Z$. Omdat ϕ surjectief is, moet er een geheel getal n zijn, zodat $(n)\phi = 1$ of $n\{(1)\phi\} = n.k = 1$. Dit is alleen mogelijk, als $k = \pm 1$. De afbeelding ϕ bepaald door $(1)\phi = 1$ is de identieke afbeelding; ook de afbeelding ϕ bepaald door $(1)\phi = -1$ is een automorfie van Z. Men heeft dus $Aut(Z) \tilde{=} Z_2$, de cyclische groep van de gehele getallen modulo 2.
2) $G = Z_n$, de additieve groep van de gehele getallen modulo n. Omdat [1] voortbrengende is van Z_n, is een automorfie ϕ van Z_n bepaald door $[1]\phi$. Elk element van Z_n heeft een orde, die een deler is van n (zie blz. 24). We beweren nu: <u>Als G een groep is en ϕ is een automorfie van G, en $a \in G$ heeft $o(a) > 0$, dan is $o((a)\phi) = o(a)$.</u>
   Stel n.l. $o(a) = k$, dan is $a^k = e$ en k is het kleinste pos. gehele getal met deze eigenschap. Dus $\{(a)\phi\}^k = (a^k)\phi = (e)\phi = e$. Als $\{(a)\phi\}^m = e$ voor 'n geheel getal m met $0 < m < k$, dan volgt $(a^m)\phi = \{(a)\phi\}^m = e$, dus $a^m = e$, want ϕ is injectief. Dit is echter in tegenspraak met $o(a) = k$. Dus $o((a)\phi) = k$. Hiermee is de bewering bewezen. Passen we dit toe op $G = Z_n$, dan volgt dat $o([1]\phi) = o([1]) = n$.

Stel nu $[1]\phi = [k]$ voor 'n geheel getal k met $0 < k < n$. Bewering: k en n zijn relatief priem of g.g.d.(k,n) = 1. Want als d/k, d/n, dan geldt: $n/d.\{[1]\phi\} = n/d.\{k[1]\} = k/d.\{n[1]\} = k/d.\{[0]\} = [0]$, dus de orde van [1] is een deler van n/d. Maar $o([1]\phi) = o([1]) = n$, dus d = 1. Omgekeerd, stel $0 < s < n$ en (n,s) = 1 voor $s \in Z$. Dan is de afbeelding $\psi : [k] \to s.[k]$ voor iedere $[k] \in Z_n$ een automorfie van Z_n. Wegens (n,s) = 1 bestaan er gehele getallen u en v zodat u.s + v.n = 1. Dus $[1] = \{u.s + v.n\}[1] = u.s[1] + v.n[1] = u.s[1]$, want $o([1]) = n$, d.w.z. $[1] = s.[u] = \{[u]\}\psi$, dus ψ is surjectief. Stel $s.[k] = [0]$, dus $s.k[1] = [0]$, dus n/s.k, want $o([1]) = n$. Maar (n.s) = 1, dus n/k en wegens $o \leq k < n$ volgt hieruit k = 0. Dus ψ is injectief. Dat ψ een homomorfie is van Z_n op zichzelf, is duidelijk, dus ψ is een automorfie.

Uit het voorgaande volgt dat er een 1-1-verband is tussen de elementen van Aut(G) en de elementen van de verzameling U_n van gehele getallen, kleiner dan n en relatief priem met n. Er is niet alleen een bijectief verband, Aut(G) is isomorf met de groep U_n. Geef de automorfie van Z_n, bepaald door $[1] \to [k]$, met $o < k < n$, (k,n) = 1, aan met ϕ_k. Als $\phi_j : [1] \to [j]$, dan is $\phi_j \circ \phi_k : [1] \to [j] \to [j][k] = [jk]$, dus $\phi_j \circ \phi_k = \phi_{jk}$. Het is duidelijk dat uit (k,n) = 1, (j,n) = 1 volgt dat (jk,n) = 1.

Als jk > n, reduceert men eerst modulo n, zodat $t \equiv jk(n)$ en $0 < t < n$. Dan geldt weer (t,n) = 1 wegens (jk,n) = 1. Men kan dus stellen dat het product van gehele getallen j en k met $0 < j, k < n$ en j,k relatief priem met n weer een geheel getal - eventueel na reductie modulo n - oplevert met deze eigenschappen. De vermenigvuldiging voldoet aan de associatieve wet. Het getal 1 heeft de eigenschap van neutraal element: 1.j = j.1 = j voor $0 < j < n$ en (j,n) = 1. Uit (j,n) = 1, $0 < j < n$ volgt dat er gehele getallen u en v bestaan met u.j + v.n = 1 of $uj \equiv 1(n)$. Hierbij kan men, zonodig, u reduceren mod n., zodat $0 < u < n$ is. Uit $uj \equiv 1(n)$ volgt dat (u,n) = 1. Dus voor iedere j met (j,n) = 1, $0 < j < n$ bestaat een inverse u met dezelfde eigenschappen.

<u>Volgens def. 1.1 vormen de gehele getallen j met $0 < j < n$ en (j,n) = 1 een groep U_n t.o.v. vermenigvuldiging mod n.</u>

Men kan de elementen van U_n ook als restklassen mod n d.w.z. als elementen

van Z_n opvatten. Ieder geheel getal j met $0 < j < n$ en $(j,n) = 1$ representeert één en precies één restklasse $[j]$ in Z_n. De afbeelding $[k] \to \phi_k$, voor $0 < k < n$, $(k,n) = 1$, is een isomorfie van U_n op $Aut(G)$, wegens $\phi_j \circ \phi_k = \phi_{jk}$. Dus $Aut(G) \cong U_n$.

3) $G = V_4$, de vier-groep van Klein; $V_4 = \{e, a_1, a_2, a_3\}$ met $a_1^2 = a_2^2 = a_3^2 = e$, $a_1 * a_2 = a_2 * a_1 = a_3$, $a_1 * a_3 = a_3 * a_1 = a_2$ en $a_2 * a_3 = a_3 * a_2 = a_1$.
Bij iedere automorfie $\phi \in Aut(V_4)$ gaat e in e over en ϕ bewerkt een permutatie van de elementen a_1, a_2 en a_3. Omgekeerd: stel ϕ is een permutatie van a_1, a_2, a_3 en $(e)\phi = e$. Dan is: $(a_i)\phi * (a_i)\phi = e$ en $a_i^2 = e$, dus $(a_i^2)\phi = e$, zodat $(a_i^2)\phi = (a_i)\phi * (a_i)\phi$. Als $a_i \neq a_j$, is $(a_i)\phi \neq (a_j)\phi$, dus $(a_i)\phi.(a_j)\phi = (a_k)\phi$ met $a_k \neq a_i$, $a_k \neq a_j$. Maar dan is $a_k = a_i * a_j$, dus $(a_i)\phi.(a_j)\phi = (a_i * a_j)\phi (i,j,k \in \{1,2,3\})$.
Ook: $(e)\phi * (a_i)\phi = (a_i)\phi * (e)\phi = (a_i)\phi (i = 1,2,3)$.
Dus ϕ is een isomorfie van V_4 op zichzelf. De automorfieën van V_4 corresponderen één-éénduidig met de permutaties van $\{a_1,a_2,a_3\}$ en $Aut(V_4) \cong S_3$.
Stel f is de inwendige automorfie van G, geïnduceerd door het element $a \in G$. Als S een deelverzameling is van G, dan is

$$\overline{a}\ S\ a = \{\overline{a}*s*a \mid s \in S\}$$

in overeenstemming met definitie 3.8. Dus f, gedefinieerd op elementen van G, kan worden uitgebreid tot deelverzamelingen van G. In het bijzondere geval, dat S ondergroep is van G, is $\overline{a}\ S\ a$ ook ondergroep van G. Immers, uit $\overline{a}*s_1*a$, $\overline{a}*s_2*a \in \overline{a}\ S\ a$ volgt:

$(\overline{a}*s_1*a) * (\overline{a}*\overline{s_2}*a) = \overline{a}*s_1*\overline{s_2}*a \in \overline{a}\ S\ a$, want $s_1*\overline{s_2} \in S$, omdat S ondergroep is van G.

$\overline{a}\ S\ a$ heet een geconjugeerde van S.
Als $\overline{a}\ S\ a = S$ volgt direct $Sa = aS$ en omgekeerd. Dus als $\overline{a}\ S\ a = S$ voor iedere $a \in G$, is S normaaldeler in G en omgekeerd (zie pag.28). De relatie: $\overline{a}\ S\ a = S$ voor iedere $a \in G$ betekent dat S invariant is onder de inwendige automorfie f. Dus:
<u>Een ondergroep S van G is een normaaldeler in G dan en slechts dan als S invariant is onder alle inwendige automorfieën van G.</u>
In dat geval valt S samen met alle geconjugeerden van S. Normaaldelers worden soms invariante ondergroepen genoemd.

IX. Definitie van een ring en voorbeelden

Definitie 9.1. R is een niet-lege verzameling en + en $\circ$ zijn twee binaire operaties op R, die we zullen aanduiden als "optelling" en "vermenigvuldiging" resp. De verzameling R met de operaties + en $\circ$, kortweg $(R,+,\circ)$ heet een ring als voldaan is aan de volgende voorwaarden:

(1) $(R,+)$ is een commutatieve groep.

(2) $\circ$ is associatief, d.w.z., $(a\circ b)\circ c = a\circ(b\circ c)$ voor alle $a,b,c \in R$.

(3) $a\circ(b+c) = (a\circ b)+(a\circ c)$ (linker distributieve wet) en $(a+b)\circ c = (a\circ c)+(b\circ c)$ (rechter distributieve wet) voor alle $a,b,c \in R$.

Als het duidelijk is, welke de ring-operaties zijn, spreekt men over de ring R i.p.v. de ring R met de operaties + en $\circ$. Evenals voor groepen, wordt voor het product de $\circ$ vaak weggelaten en schrijft men ab in plaats van $a\circ b$. Het neutrale element van $(R,+)$ wordt door 0 aangegeven en heet het nulelement van de ring. Als er een element $e \in R$ bestaat zodat $ae = ea = a$ voor alle $a \in R$, dan heet e een één-element van R. R heet een commutatieve ring, als $ab = ba$ voor alle $a,b \in R$. In het andere geval heet R een niet-commutatieve ring. R heet een ring met één-element, als R een één-element e heeft.

Er bestaat een zeer eenvoudige ring die alleen uit het neutrale element 0 bestaat. Hiervoor geldt: $0+0=0$, $0\circ 0 = 0$. Deze ring heet de triviale ring.

Stel R is een ring met één-element e. Als R niet de triviale ring is, dan zijn de elementen 0 en e verschillend. Immers uit $0+0=0$ volgt $0\circ a = (0+0)a = 0\circ a + 0\circ a$, dus uit de vereenvoudigingswet in $(R,+)$ volgt $0\circ a = 0$ voor alle $a \in R$. Als $0 = e$, dan is $a = e\circ a = 0\circ a = 0$ voor iedere $a \in R$. Maar R is niet de triviale ring, dus de aanname $e = 0$ leidt tot een tegenspraak. Dus $0 \neq e$.

Afspraak. We nemen aan dat iedere ring met één-element meer dan 1 element heeft. Dan is de mogelijkheid $0 = e$ uitgesloten.

Voorbeelden.

1. De stelsels $(Z,+,\circ)$, $(Q,+,\circ)$ en $(R,+,\circ)$ met de gebruikelijke optelling en vermenigvuldiging vormen ringen. Elk van deze ringen is commutatief

en heeft het gehele getal 1 als één-element.

2. $(Z_2+,\circ)$, met de gewone optelling en vermenigvuldiging is de ring van de even getallen. Deze ring heeft geen één-element.
3. S is een gegeven verzameling en P(S) is de collectie van alle deelverzamelingen van S. Het symmetrisch verschil van twee deelverzamelingen $A,B \subseteq S$ is de verzameling $A \Delta B$ met

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

(Als C en D willekeurige verzamelingen zijn, met $D \subseteq C$, definieert ment $C\setminus D$ door:

$$C\setminus D = \{x \mid x \in C \text{ en } x \notin D\}.)$$

Als we optelling en vermenigvuldiging in P(S) definiëren door:

$$A + B = A \Delta B, \quad A \circ B = A \cap B,$$

dan vormt het stelsel $(P(S),+,\circ)$ een commutatieve ring met één-element. De lege verzameling $\emptyset$ dient als nul-element, en S is het één-element. Iedere verzameling in P(S) is gelijk aan de additieve inverse van zichzelf: $A = \bar{A}$ voor iedere $A \in P(S)$. Immers:
$A + A = A \Delta A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset$.
$A + \emptyset = A \Delta \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A$ voor iedere $A \in P(S)$.
Evenzo: $\emptyset + A = A$ voor iedere $A \in P(S)$.
$A \circ S = A \cap S = A$ en $S \circ A = S \cap A = A$ voor iedere $A \in P(S)$.
De verificatie van de associatieve wetten (voor de optelling en vermenigvuldiging) en de distributieve wet laten we achterwege.

4. $(R,+,\circ)$ is een gegeven ring. Dan kunnen we de verzameling $M_n(R)$ van $n\times n$-matrices over R beschouwen. Als $I_n = \{1,2,\ldots,n\}$, dan is een element van $M_n(R)$ een functie $f: I_n \times I_n \to R$. In de praktijk identificeert men zo'n afbeelding f met zijn waarden $a_{ij} = (i,j)f$, die worden geschreven in een $n\times n$ rechthoekig schema

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \qquad (a_{ij} \in R).$$

Eenvoudigheidshalve zullen we de n×n-matrix met het element a_{ij} op de plaats (i,j) afkorten tot (a_{ij}).
De operaties, die nodig zijn om van $(M_n(R),+,\circ)$ een ring te maken, worden verschaft door de formules:

$$(a_{ij}) + (b_{ij}) = (a_{ij}+b_{ij}) \quad \text{en} \quad (a_{ij}) \circ (b_{ij}) = (c_{ij})$$

met

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \circ b_{kj}.$$

Het nul-element van deze ring is de n×n-matrix, waarvan alle elementen = 0 ($\in$ R) zijn; en $-(a_{ij}) = (-a_{ij})$. Omdat R associatief is t.o.v. +, is ook de optelling in $M_n(R)$ associatief. Stel (a_{ij}), (b_{ij}) en $(c_{ij}) \in M_n(R)$. Dan geldt $\{(a_{ij}) \circ (b_{ij})\} \circ (c_{ij}) = (d_{ij}) \circ (c_{ij})$, waarin $d_{ij} = \sum_{k=1}^{n} a_{ik} \circ b_{kj}$. Ook $(d_{ij}) \circ (c_{ij}) = (e_{ij})$ met $e_{ij} = \sum_{t=1}^{n} d_{it} \circ c_{tj}$. Dus

$$e_{ij} = \sum_{t=1}^{n} \left(\sum_{k=1}^{n} a_{ik} \circ b_{kt} \right) \circ c_{tj} = \sum_{k=1}^{n} \sum_{t=1}^{n} (a_{ik} \circ b_{kt}) \circ c_{tj} =$$

$$= \sum_{k=1}^{n} a_{ik} \circ \left(\sum_{t=1}^{n} b_{kt} \circ c_{tj} \right) = \sum_{k=1}^{n} a_{ik} \circ f_{kj}, \text{ als } f_{kj} = \sum_{t=1}^{n} b_{kt} \circ c_{tj}.$$

Dus $(e_{ij}) = (a_{ij}) \circ (f_{ij}) = (a_{ij}) \circ \{(b_{ij}) \circ (c_{ij})\}$.
Hieruit volgt: $\{(a_{ij}) \circ (b_{ij})\} \circ (c_{ij}) = (a_{ij}) \circ \{(b_{ij}) \circ (c_{ij})\}$, zodat de associatieve wet ook voor de vermenigvuldiging in $M_n(R)$ geldt. De beide distributieve wetten in $M_n(R)$ volgen uit de overeenkomstige wetten in R. Dus $(M_n(R),+,\circ)$ is een ring.
De ring $M_n(R)$ is niet commutatief voor n > 1. Als R een één-element e heeft, is de matrix met e's op de hoofddiagonaal (d.w.z. $a_{ii} = e$) en 0 op de andere plaatsen een één-element voor de ring $M_n(R)$. Met behulp van het Kronecker symbool δ_{ij}, gedefinieerd door

$$\delta_{ij} = \begin{cases} 1 & \text{als } i = j \\ 0 & \text{als } i \neq j \end{cases} \qquad (i,j=1,2,\ldots,n)$$

kan het één-element van $M_n(R)$ geschreven worden als (δ_{ij}).

5. X is een willekeurige niet-lege verzameling en $(R,+,\circ)$ is een ring. Met map(X,R) bedoelen we de verzameling bestaande uit alle afbeeldingen van X in R; in formule:

$$\text{map}(X,R) = \{f \mid f: X \to R\}.$$

De elementen van map(X,R) kunnen worden samengesteld door algebraïsche bewerkingen op de functiewaarden uit te voeren. Precieser: de "puntsgewijze" som $f + g$ en het product $f \circ g$ van $f,g \in \text{map}(X,R)$ zijn resp. de afbeeldingen van X in R, die voldoen aan

$$(x)(f+g) = (x)f + (x)g, \quad (x)(f\circ g) = (x)f \circ (x)g,$$

voor alle $x \in X$.
De gedefinieerde optelling en vermenigvuldiging in map(X,R) maken deze verzameling tot een ring. Het nul-element van deze ring is de constante functie f, met $(x)f = 0 \in R$ voor iedere $x \in X$. De inverse $-f$ van $f \in \text{map}(X,R)$ wordt gekarakteriseerd door de regel $(x)(-f) = \overline{(x)f}$ (in R).
De algebraïsche eigenschappen van map(X,R) worden bepaald door wat er gebeurt in de ring $(R,+,\circ)$. Bijv. als R een één-element e heeft, dan heeft de ring map(X,R) ook een één-element; n.l. de constante functie f met $(x)f = e$ voor iedere $x \in X$. Evenzo, als R commutatief is, is map(X,R) ook commutatief.

6. $R = \{(a,b) \mid a,b \in Z\}$.
Voor (a,b) en (c,d) definiëren we een optelling en vermenigvuldiging op R als volgt:

$$(a,b) + (c,d) = (a+c,b+d)$$
$$(a,b) \circ (c,d) = (ac-bd,ad+bc).$$

Men kan aantonen dat R t.o.v. deze bewerkingen een ring is. Het nulelement van R is (0,0), $0 \in Z$ en de additieve inverse van $(a,b) \in R$ is $(-a,-b)$. Deze ring heeft een één-element, n.l. (1,0), $1 \in Z$:

$$(1,0) \circ (c,d) = (c,d)$$

en $(c,d) \circ (1,0) = (c,d)$ voor iedere $(c,d) \in R$.

Merk op, dat de additieve groep van R het direkte product $Z \times Z$ is (zie p.7).
I.p.v. de schrijfwijze (a,b) kan men ook de notatie $a + bi$ gebruiken, waarin $i^2 = -1 \in Z$. De optelling en vermenigvuldiging worden dan resp. aangeduid door

$$(a+bi) + (c+di) = a + c + (b+d)i$$

$$(a+bi) \circ (c+di) = ac - bd + (ad+bc)i.$$

Het product van $a + bi$ en $c + di$ wordt berekend door eerst te vermenigvuldigen volgens de distributieve en associatieve wetten, dan $ai = ia$ voor ieder reëel getal a te gebruiken en tenslotte het formele element i^2 door -1 te vervangen.
De aldus verkregen ring (die dus overeenkomt met de ring R hierboven) is een ring van speciale complexe getallen; de getallen $a + bi$, $a,b \in Z$, noemt men gehele getallen van Gauss. De ring van de gehele getallen van Gauss wordt vaak aangeduid door $Z[i]$. Het is een commutatieve ring met één-element $1 + 0i = 1$ $(\in Z)$.

7. In voorbeeld 6 op p.5 zijn de congruentie-klassen van gehele getallen modulo n ingevoerd, waarin $n > 0$ een vast geheel getal is. Voor ieder geheel getal a werd de equivalentie-klasse, waartoe a behoort, aangegeven door $[a]$:

$$[a] = \{x \in Z \mid x \equiv a(\mathrm{mod}\ n)\} = \{a + kn \mid k \in Z\}.$$

De verzameling van alle equivalentie-klassen van gehele getallen modulo n zullen we aanduiden met J_n. Op pag. 5 is aangetoond dat de klassen $[0],[1],\ldots,[n-1]$ precies alle elementen van J_n zijn. Op pag. 6 is een optelling voor de elementen van J_n gedefinieerd: $[i] + [j] = [i+j]$ voor $[i],[j] \in J_n$. T.o.v. deze operatie vormt J_n een commutatieve groep. Aan het eerste axioma in de definitie 9.1 is door $(J_n,+)$ dus voldaan.
We definiëren nu een vermenigvuldiging op J_n:

$$[i] \circ [j] = [ij] \quad \text{voor } [i],[j] \in J_n.$$

Het is duidelijk, dat $\circ$ een binaire operatie is. Deze vermenigvuldiging is zinvol, want als $[i] = [i']$ en $[j] = [j']$ dan is $i \equiv i' \bmod n$ en $j \equiv j' \bmod n$, dus $ij \equiv i'j' \bmod n$ volgens eigenschap c) op p. 5. Hieruit volgt $[ij] = [i'j']$. Dus $[i] \circ [j] = [ij] = [i'j'] = [i'] \circ [j']$. De associatieve wet in J_n voor de vermenigvuldiging is geldig, want $\{[i] \circ [j]\} \circ [k] = [ij] \circ [k] = [(ij)k] = [i(jk)] = [i] \circ [jk] = [i] \circ \{[j] \circ [k]\}$. Evenzo gelden de beide distributieve wetten:

$$[i] \circ \{[j] + [k]\} = [i] \circ [j+k] = [i(j+k)] = [ij+ik] = [ij] + [ik] = [i] \circ [j] + [i] \circ [k]$$

en

$$\{[i] + [j]\} \circ [k] = [i+j] \circ [k] = [(i+j)k] = [ik+jk] = [ik] + [jk] = [i] \circ [k] + [j] \circ [k].$$

Dus J_n voldoet aan het 2^e en 3^e axioma in definitie 9.1. Dan is $(J_n,+,\circ)$ een ring.
De klassen $[0]$ en $[1]$ fungeren als nul-element resp. één-element in deze ring, terwijl $[n-a] = [-a]$ de additieve inverse is van $[a]$ in J_n. Omdat $[i] \circ [j] = [j] \circ [i]$ voor alle $[i],[j] \in J_n$, is J_n een commutatieve ring.

X. Elementaire gevolgen van de definitie van een ring

Stelling 10.1. R is een ring. Voor alle $a,b,c \in R$ geldt:

1) $0 \circ a = a \circ 0 = 0$,

2) $a \circ (-b) = (-a) \circ b = -(a \circ b)$

3) $(-a) \circ (-b) = a \circ b$ en

4) $a \circ (b-c) = a \circ b - a \circ c$, $(b-c) \circ a = b \circ a - c \circ a$,

waarin 0 het nul-element is van R, $-a$ de additieve inverse is van a en $b-c = b+(-c)$.

Bewijs

1) Uit $0+0 = 0$ volgt $0 \circ a = (0+0) \circ a = 0 \circ a + 0 \circ a$. Dus uit de vereenvoudigingswet voor de additieve groep $(R,+)$ volgt $a \circ 0 = 0$. Evenzo geldt $a \circ 0 = a \circ (0+0) = a \circ 0 + a \circ 0 \rightarrow a \circ 0 = 0$ (§2, st. 2.2).
2) Uit $b+(-b) = 0$ volgt $a \circ (b+(-b)) = a \circ b + a \circ (-b) = a \circ 0 = 0$ (1), dus $a \circ (-b) = -(a \circ b)$, want de additieve inverse is eenduidig bepaald. Evenzo: $a+(-a) = 0 \rightarrow 0 = 0 \circ b = (a+(-a)) \circ b = a \circ b + (-a) \circ b$, dus $(-a) \circ b = -(a \circ b)$.
3) $(-a) \circ (-b) = -\{(-a) \circ b\}$ volgens (2) $= -\{-(a \circ b)\}$ (2) $= a \circ b$.
4) $a \circ (b-c) = a \circ (b+(-c)) = a \circ b + a \circ (-c) = a \circ b + (-(a \circ c)) = a \circ b - a \circ c$.
   $(b-c) \circ a = (b+(-c)) \circ a = b \circ a + (-c) \circ a = b \circ a + (-(c \circ a)) = b \circ a - c \circ a$.

We zullen nu het begrip "nuldeler" invoeren.

Definitie 10.2. R is een ring en $a(\neq 0) \in R$. Dan heet a een linker- (rechter-) nuldeler van R als er een element $b \neq 0$ in R bestaat zodat $a \circ b = 0$ ($b \circ a = 0$). Een nuldeler is elk element van R dat òf een linker- òf een rechter-nuldeler is.

Volgens def. 10.2 is 0 geen nuldeler en als R een één-element e bevat, dan is e geen nuldeler.

Een voorbeeld van een ring met nuldelers is J_n, waarin $n > 1$ een samengesteld getal is; als $n = n_1 n_2$ in Z ($0 < n_1, n_2 < n$), dan is het product $[n_1] \circ [n_2] = [n] = [0]$ in J_n (zie voorbeeld 6, pag. 59).

Als R een ring is zonder nuldelers kan men uit de betrekking $a \circ b = 0$ $(a,b \in R)$ concluderen dat òf $a = 0$ òf $b = 0$.

Stelling 10.3. Een ring R heeft geen nuldelers dan en slechts dan als hij voldoet aan de vereenvoudigingswet voor de vermenigvuldiging; d.w.z. voor alle $a,b,c \in R$ geldt: $a \neq 0$, $ab = ac \Longrightarrow b = c$ en
$a \neq 0$, $ba = ca \Longrightarrow b = c$.

Bewijs. Stel R heeft geen nuldelers en $ab = ac$, $a \neq 0$. Dan is
$a(b-c) = 0 \rightarrow b-c = 0$, dus $b = c$.
Evenzo: $ba = ca$, $a \neq 0 \rightarrow (b-c)a = 0$, $a \neq 0 \rightarrow b-c = 0$ of $b = c$.
Omgekeerd, stel R voldoet aan de vereenvoudigingswet. Neem aan $ab = 0$ met $a \neq 0$. Dan is $ab = a0 \rightarrow b = 0$.
Evenzo: $ab = 0$, $b \neq 0 \rightarrow ab = 0b$, $b \neq 0 \rightarrow a = 0$.
Dus er zijn geen nuldelers in R.

Definitie 10.4. Een integriteitsgebied is een commutatieve ring met één-element en zonder nuldelers.
Een voorbeeld van een integriteitsgebied is de ring Z van de gehele getallen. Ook de ringen Q (rationale getallen) en R (reële getallen) zijn integriteitsgebieden. Uit stelling 10.3 volgt dat de vereenvoudigingswet voor de vermenigvuldiging geldt in een integriteitsgebied.

Definitie 10.5. $(R,+,\circ)$ is een ring en $S \subseteq R$ is een niet-lege deelverzameling van R. Als het systeem $(S,+,\circ)$ zelf een ring is, met de optelling en vermenigvuldiging in S dezelfde als in R (beperking tot S), dan heet $(S,+,\circ)$ een deelring van $(R,+,\circ)$.
Volgens def. 9.1 is S een deelring van R, als $(S,+,)$ een ondergroep is van $(R,+)$, de vermenigvuldiging een binaire operatie is op S en voldoet aan de associatieve wet en de beide distributieve wetten. Omdat aan de laatste eis voor elementen van S, als elementen van R, is voldaan, kunnen we deze weglaten in de definitie van een deelring. Dus:
Het systeem $(S,+,\circ)$ vormt een deelring van de ring $(R,+,\circ)$ dan en slechts dan als

1) S een niet-lege deelverzameling is van R,
2) $(S,+)$ een ondergroep is van $(R,+)$, en
3) de verzameling S gesloten is t.o.v. vermenigvuldiging.

Uit §3, st. 3.3 volgt dat (S,+) een ondergroep is van (R,+) als S een niet-lege deelverzameling is van R en a-b $\in$ S voor a,b $\in$ S. Hierdoor is het mogelijk het begrip deelring van een ring op de volgende wijze te karakterizeren:

Stelling 10.6. R is een ring en S is een niet-lege deelverzameling in R. Dan is S een deelring van R dan en slechts dan als

1) $a,b \in S \rightarrow a-b \in S$ (gesloten onder verschil)
2) $a,b \in S \rightarrow a \circ b \in S$ (gesloten onder vermenigvuldiging).

Bewijs. Als S een deelring is van R, dan is S een ring, dus 1) en 2) zijn geldig, omdat + en $\circ$ binaire operaties zijn op S en
$a-b = a+(-b)$ $(-b \in S)$.
Omgekeerd volgt uit 1) en 2) dat S een deelring is. Voor a,b $\in$ S geldt
$a+b = a+(-(-b)) = a-(-b) \in S$, want $b \in S \rightarrow b-b = 0 \in S$ en
$b \in S \rightarrow 0-b = -b \in S$.
Ook $a,b \in S \rightarrow a \circ b \in S$, dus + en $\circ$ zijn binaire operaties op S. $S \neq \emptyset$ en 1) geldt, dus (S,+) is een groep, en $(S,+) \subseteq (R,+)$, dus (S,+) is een commutatieve ondergroep van (R,+).
De associatieve wet en de distributieve wetten gelden in S, omdat ze geldig zijn in R.
Uit §3, st. 3.2 volgt dat het nul-element van S gelijk is aan dat van R en dat de additive inverse van een element a van de deelring S hetzelfde element is als de inverse van a, a opgevat als element van R.

Voorbeeld

1. Iedere ring R heeft twee deelringen, n.l. de verzameling {0}, bestaande uit het nulelement van R en R zelf. Deze twee deelringen heten de triviale deelringen van R. S deelring van R en $S \neq R$, dus $S \subset R$, dan heet S echte deelring van R.
2. De verzameling Z_2 van even getallen is een deelring van de ring Z van de gehele getallen.
   Immers: $2n - 2m = 2(n-m) \in Z_2$
   $(2n)(2m) = 2(2nm) \in Z_2$.

Uit dit voorbeeld blijkt dat in een ring met één-element, een deelring niet het één-element behoeft te bevatten.

Definitie 10.7. R is een willekeurige ring. Het centrum van R is als volgt gedefinieerd:

$$\text{cent } R = \{a \in R \mid ar = ra, \forall r \in R\}.$$

Het is duidelijk dat een ring R commutatief is dan en slechts dan als cent R = R.

Stelling 10.8. R is een willekeurige ring. Dan is cent R een deelring van R.

Bewijs. cent $R \neq \emptyset$, want $0 \in$ cent R. Stel nu, dat $a,b \in$ cent R. Dan is $ar = ra$, $br = rb$, $\forall r \in R$. Dus, voor een willekeurig element $r \in R$, geldt:

$$(a-b)r = ar-br = ra-rb = r(a-b),$$

zodat $a-b \in$ cent R. Evenzo geldt:

$$(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab),$$

dus $ab \in$ cent R. Volgens st. 10.6 is cent R een deelring van R.

Er is al opgemerkt dat, als een ring een één-element heeft, dit niet juist behoeft te zijn voor deelringen. Men heeft ook andere mogelijkheden:

1) Een deelring heeft een één-element, maar de hele ring niet.
2) Zowel de ring als één van zijn deelringen bezitten één-elementen, maar deze zijn verschillend.

In elk van de gevallen 1) en 2) is het één-element van de deelring een nuldeler in de omvattende ring. Immers, stel $e' \neq 0$ is het één-element van de deelring S. We nemen verder aan, dat e' niet als één-element voor de hele ring R fungeert. Dus bestaat er een element $a \in R$ met $a \circ e' \neq a$. Het is duidelijk dat $(a \circ e') \circ e' = a \circ (e' \circ e') = a \circ e'$, want S is gesloten t.o.v. vermenigvuldiging en $e' \circ e' = e'$ in S. Dus $(a \circ e' - a) \circ e' = 0$. Nu is $a \circ e' - a \neq 0$ en $e' \neq 0$, dus de ring R heeft nuldelers en in het bijzonder is e' een nuldeler.

Voorbeeld

3. Beschouw de verzameling $R = Z \times Z_2$ (Cartesisch product). Men kan R een ring-structuur geven door optelling en vermenigvuldiging componentsgewijze te definiëren:

$$(a,b) + (c,d) = (a+c,\ b+d)$$
$$(a,b)(c,d) = (ac,\ bd).$$

Dat aan de ring-axioma's is voldaan, volgt uit het feit, dat Z en Z_2 ringen zijn. Het nul-element van R is (0,0), de inverze van (a,b) is (-a, -b).
De verzameling $Z \times \{0\} = \{(a,0) \mid a \in Z\}$ vormt een deelring S van R.
Immers: S is niet-leeg, $((0,0) \in S)$. Uit $(a,0),(b,0) \in S$ volgt: $(a,0)-(b,0) = (a-b,0) \in S$ en $(a,0)(b,0) = (ab,0) \in S$. S heeft (1,0) als één-element, want $(1,0)(a,0) = (a,0)(1,0) = (a,0)$ voor iedere $(a,0) \in S$. Maar R heeft geen één-element. Stel (a,b) is één-element van R, dan is $(a,b)(1,0) = (a,0) = (1,0)$, dus $a = 1$.
Maar $(1,b)(1,2) = (1,2b) = (1,b)$, zodat $b = 1$, hetgeen niet kan wegens $b \in Z_2$.
Als men $R = Z \times Z$ kiest met componentsgewijze optelling en vermenigvuldiging, dan is $Z \times \{0\}$ een deelring van R met één-element (1,0). Maar dit één-element is verschillend van dat van R, omdat (1,1) het één-element is van R, zoals direct uit de vermenigvuldiging blijkt. Het element (1,0) moet een nuldeler zijn in R; inderdaad geldt $(1,0)(0,1) = (0,0)$, waarin (0,0) het nul-element is van R.

Als R een willekeurige ring is en n een positief geheel getal, dan definiëren we de <u>n^e macht van a</u> $(a \in R)$ inductief als volgt:

$$a' = a, \quad a^n = a^{n-1} \circ a.$$

Hieruit volgen de gebruikelijke regels voor exponenten:

$$a^n \circ a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \qquad n,m > 0,\ n,m \in Z.$$

Kies m vast en pas inductie toe naar n:

$$a^1 \circ a^m = a \circ a^m = a^{m+1};$$

stel $\quad a^j \circ a^m = a^{m+j}, \qquad m,j > 0,\ m,j \in Z.$

Dan is $\quad a^{j+1} \circ a^m = (a^j \circ a) \circ a^m = a^j \circ (a \circ a^m) = a^j \circ (a^m \circ a) =$

$= (a^j \circ a^m) \circ a = a^{m+j} \circ a = a^{m+j+1}.$

$$(a^1)^m = a^m = a^{1 \circ m};$$

stel $\quad (a^j)^m = a^{jm}, \qquad m,j > 0,\ m,j \in Z.$

Dan is $\quad (a^{j+1})^m = (a^{j \circ a})^m = (a^j)^m \circ a^m = a^{jm} \circ a^m = a^{jm+m} = a^{(j+1)m}.$

In het algemeen volgt uit $a \circ b = b \circ a$ $(a,b \in R)$, dat alle machten van a commuteren met alle machten van b, dus $(a \circ b)^n = a^n \circ b^n$ voor ieder positief geheel getal n.
R is een gegeven ring met één-element e. Dan heet een element $a \in R$ een <u>eenheid</u>, als a een inverse $a^{-1} \in R$ bezit t.o.v. de vermenigvuldiging, d.w.z.

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Als a een eenheid is, is a^{-1} eenduidig bepaald. Stel n.l.

$$a \circ b = a \circ c = e \Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$$

of

$$e \circ b = e \circ c \Rightarrow b = c.$$

T.o.v. de vermenigvuldiging in R vormen de eenheden in R een groep R^*. R^* is zeker niet leeg, want e en -e behoren tot R^*.
Als a een eenheid is in R, dus als a^{-1} bestaat in R, kunnen negatieve machten van a ingevoerd worden. Men definieert: $a^{-n} = (a^{-1})^n$ voor $n > 0$, $n \in Z$. Per definitie is $a^0 = e$. Daarmee heeft het symbool a^n betekenis voor ieder geheel getal n, als men zich beperkt tot a is eenheid.
Voor ieder positief geheel getal n, definiëren we het <u>n^e natuurlijke veelvoud na</u> recursief als volgt:

$$1a = a \quad \text{en} \quad na = (n-1)a+a, \text{ als } n > 1.$$

We spreken af: $0a = 0$ (eerste 0 = getal 0, tweede 0 = nul-element van R) en $(-n)a = -(na)$, $n > 0$, $n \in Z$.
Hiermee is de definitie van na uitgebreid tot alle gehele getallen n.
Voor gehele veelvouden gelden identiteiten:

$$(n+m)a = na+ma$$

$$(nm)a = n(ma)$$

$$n(a+b) = na+nb$$

voor $a,b \in R$ en willekeurige gehele getallen n en m.
We zullen de laatste formule aantonen. Voor $n = 1$ geldt:

$$1(a+b) = a+b = 1a+1b;$$

stel $\quad j(a+b) = ja+jb, \qquad j \geq 1, \ j \in Z.$

Dan is $\quad (j+1)(a+b) = j(a+b)+(a+b) = ja+jb+a+b = ja+a+jb+b =$

$$= (j+1)a+(j+1)b.$$

Dus $n(a+b) = na+nb$ voor iedere $n \in Z$, $n > 0$.
Ook is $0(a+b) = 0 = 0a+0b$. Tenslotte is

$$(-n)(a+b) = -(n(a+b)) = -(na+nb) = -(nb)-(na) =$$

$$= (-n)(a)+(-n)(b) \qquad \text{voor } n \in Z, \ n > 0.$$

Dus de formule is juist voor iedere $n \in Z$.
Uit de distrinutieve wetten volgen nog:

$$n(ab) = (na)b = a(nb)$$

$$(na)(mb) = (nm)(ab)$$

voor $a,b \in R$ een willekeurige gehele getallen n en m.

Opmerking. De uitdrukking na moet niet worden beschouwd als een ringproduct; in feite is het mogelijk dat n niet tot R behoort. Het symbool

na is alleen een gemakkelijke manier om een zekere som van elementen van R aan te duiden. Als R een één-element e heeft, is het mogelijk na als een product van twee ring-elementen voor te stellen n.l.
$na = n(ea) = (ne)a$, met $ne, a \in R$.

XI. Idealen

Deelringen zijn, als men verder geen beperkingen oplegt, te algemeen om gewenste resultaten, zoals de fundamentele homomorfie-stelling voor ringen, af te leiden. We zullen daarom in dit hoofdstuk onze aandacht beperken tot een klasse van deelringen met een sterkere eis van gesloten zijn t.o.v. de vermenigvuldiging, n.l. het gesloten zijn t.o.v. vermenigvuldiging met een willekeurig ring-element.

Definitie 11.1. Een deelring I van een ring R heet een twee-zijdig ideaal in R als $r \in R$ en $a \in I$ impliceren dat zowel $ra \in I$ als $ar \in I$. Anders gezegd, als één van de factoren in een product van 2 ring-elementen uit R tot I behoort, dan moet het product tot I behoren.
In verband met stelling 10.6 kan men definitie 11.1 vervangen door

Definitie 11.2. I is een niet-lege deelverzameling van een ring R. Dan is I een twee-zijdig ideaal in R als geldt:

1) $a, b \in I \Rightarrow a - b \in I$, en
2) $r \in R, a \in I \Rightarrow ra \in I$ en $ar \in I$.

Als de voorwaarde 2) wordt verzwakt in deze zin dat men alleen eist dat het product $ra \in I$ voor iedere keuze van $r \in R$ en $a \in I$, dan spreekt men van een links-ideaal; rechts-idealen worden analoog gedefinieerd. Als R een commutatieve ring is, is er geen onderscheid tussen links-, rechts- en tweezijdige idealen.
Afspraak. In het vervolg zullen we met de term "ideaal" steeds een twee-zijdig ideaal bedoelen.

Voorbeelden.

1) Z is de ring van de gehele getallen.
   Stel (n) is de verzameling nZ van alle gehele veelvouden van n;
   d.w.z. $(n) = \{nm \mid m \in Z\}$.
   Dan is (n) een ideaal in Z;
   $$nm - nk = n(m-k),$$
   $$k(nm) = n(km), \qquad m,k \in Z.$$

Syll. ZC 86, afl.11

In het bijzonder geldt (2) = 2Z, de ring van de even getallen is een ideaal in Z. Merk op, dat (0) = {0} en (1) = Z (triviale idealen).

Niet iedere deelring van een ring is een ideaal. Bijv., K is de ring van reële getallen. Dan is Z een deelring van K, maar Z is geen ideaal in K.

Immers, $\frac{1}{2} \in K$, $1 \in Z$, maar $\frac{1}{2}.1 \notin Z$.

2) We beschouwen de ring

$$\text{map } (X,R) = \{f \mid f : X \to R\}$$

van voorbeeld 5 op pag.58. R is een ring en X is een willekeurige niet-lege verzameling.

Kies x vast in X.

Definieer $I_x = \{f \mid f \in \text{map } (X,R);\ (x)f = 0\}$.

Kies $f, g \in I_x$ en h willekeurig in map (X,R).

Dan volgt:

$$(x)\ (f-g) = (x)f - (x)g = 0 - 0 = 0,$$
$$(x)\ (f\circ h) = (x)f \circ (x)h = 0 \circ (x)h = 0,$$
$$(x)\ (h\circ f) = (x)h \circ (x)f = (x)h \circ 0 = 0.$$

Dus $f - g$, $f \circ h$ en $h \circ f$ behoren alle tot I_x, zodat I_x een ideaal is in map (X,R).

Algemener: S is een willekeurige niet-lege deelverzameling in X.

Definieer:

$$I = \{f \mid f \in \text{map } (X,R);\ (x)f = 0 \text{ voor alle } x \in S\}.$$

Dan is I een ideaal in map (X,R). Omdat $I = \bigcap_{x \in S} I_x$ hebben we een situatie, waarin de doorsnede van idealen weer een ideaal is. Dit geldt echter algemeen (zie st.11.5).

Voordat we het volgende voorbeeld geven, eerst een stelling voor ringen met één-element.

<u>Stelling 11.3.</u> R is een ring met één-element e. I is een <u>echt</u> (rechts-, links-, 2-zijdig) ideaal in R. Dan heeft geen enkel element van R een

inverse t.o.v. de vermenigvuldiging; d.w.z. $I \cap R^* = \emptyset$ (zie pag.66).

Bewijs. Stel $a \neq 0 \in I$ en a^{-1} bestaat in R, of a is eenheid in R. (De stelling is triviaal, als $I = \{0\}$). Dan volgt $e = a^{-1} \circ a \in I$ (def.11.2). Dus ook $r = r \circ e \in I$ (def.11.2) voor iedere $r \in R$. Dus $R \subseteq I$ en $I = R$. Dit is in tegenspraak met het gegeven, dat I een echte deelverzameling is van R.
Een direct gevolg is

Gevolg 11.4. R is een ring met één-element. Dan bevat geen enkel echt (rechts-, links-, 2-zijdig) ideaal het één-element.

Voorbeelden.

3) Z[i] is de ring van de gehele getallen van Gauss. (zie pag.59). Definieer

$$I = \{a + bi \mid a \equiv 0(2) \text{ en } b \equiv 0(2)\}.$$

Dan is I een niet-lege deelverzameling van Z[i]. Uit $a_1 \equiv 0(2)$ en $a_2 \equiv 0(2)$ volgt $a_1 - a_2 \equiv 0(2)$ en $a_1 r \equiv 0(2)$ met $a_1, a_2, r \in Z$. Dus

$$a_1 + b_1 i,\ a_2 + b_2 i \in I \Rightarrow (a_1+b_1 i) - (a_2+b_2 i) = (a_1-a_2) + (b_1-b_2)i \in I$$

en

$$a_1 + b_1 i \in I,\ r + si \in Z[i] \Rightarrow (a_1+b_1 i) \circ (r+si) =$$

$$= (a_1 r - b_1 s) + (a_1 s + b_1 r)\, i \in I.$$

Evenzo geldt: $(r+si) \circ (a_1+b_1 i) \in I$. Dus I is een ideaal in Z[i]. Evenals in de ring Z gebruikt men de notatie $I = (2)$.

4) $M_n(R)$ is de ring van $n \times n$-matrices over R. (zie pag.56). We willen aantonen dat $M_n(R)$ geen niet-triviale idealen heeft, als R de ring is van de reële getallen.
Hiertoe voeren we in: $E_{ij} = (e_{ij})$ met $e_{ij} = 1$, $e_{kt} = 0$ voor $k \neq i$ en/of $t \neq j$. Dus E_{ij} is de $n \times n$-matrix met 1 op de plaats(i,j) en op alle andere plaatsen 0.
Stel $I \neq \{0\}$ is een ideaal in de ring $M_n(R)$. I bevat een matrix

$(a_{ij}) \neq$ nul-matrix met bijv. $a_{rs} \neq 0$. Omdat I een ideaal is in $M_n(R)$, is het product

$$E_{rr}\ (b_{ij})\ (a_{ij})\ E_{ss}$$

een element van I, waarin de matrix (b_{ij}) gedefinieerd is door:
$b_{ii} = a_{rs}^{-1}$ voor $i = 1, 2, \ldots, n$ en $b_{jk} = 0$ voor $j \neq k$.
Als $(c_{ij}) = E_{rr}\ (b_{ij})$, dan is $c_{kl} = \sum_{i=1}^{n} e_{ki}\ b_{il}$, maar $e_{ki} = 0$ voor $k \neq r$ en/of $i \neq r$, dus $c_{kl} = 0$ voor $k \neq r$; $c_{rl} = \sum_{i=1}^{n} e_{ri}\ b_{il} = e_{rr}\ b_{rl}$, want $e_{ri} = 0$ voor $i \neq r$. Ook is $b_{rl} = 0$ voor $r \neq 1$, dus $c_{rl} = 0$ voor $r \neq 1$. Tenslotte is $c_{rr} = e_{rr}\ b_{rr} = a_{rs}^{-1}$.
Als $(d_{ij}) = (c_{ij})\ (a_{ij})$, dan is $d_{kl} = \sum_{i=1}^{n} c_{ki}\ a_{il}$. Wegens $c_{ki} = 0$ voor $k \neq r$, is $d_{kl} = 0$ voor $k \neq r$; $d_{rl} = \sum_{i=1}^{n} c_{ri}\ a_{il} = c_{rr}\ a_{rl}$, want $c_{ri} = 0$ voor $i \neq r$.
Als $(f_{ij}) = (d_{ij})\ E_{ss}$, dan is $f_{kl} = \sum_{i=1}^{n} d_{ki}\ e'_{il}$ met $e'_{il} = 0$ voor $i \neq s$ en/of $1 \neq s$. Dus $f_{kl} = 0$ voor $1 \neq s$.
Ook is $f_{ks} = \sum_{i=1}^{n} d_{ki}\ e'_{is} = d_{ks}\ e'_{ss}$, want $e'_{is} = 0$ voor $i \neq s$.
Dus $f_{rs} = d_{rs}\ e'_{ss} = d_{rs} = c_{rr}\ a_{rs} = a_{rs}^{-1}\ a_{rs} = 1$.
Voor $k \neq r$ is $d_{ks} = 0$, dus voor $k \neq r$ is $f_{ks} = 0$.
Hiermede is aangetoond dat

$$E_{rr}\ (b_{ij})\ (a_{ij})\ E_{ss} = E_{rs},$$

zodat $E_{rs} \in I$. Gemakkelijk toont men aan dat

$$E_{ij} = E_{ir}\ E_{rs}\ E_{sj} \qquad (i,j=1,2,\ldots,n)$$

zodat alle n^2 matrices E_{ij} bevat zijn in I. Het één-element (δ_{ij}) van $M_n(r)$ kan geschreven worden als

$$(\delta_{ij}) = E_{11} + E_{22} + \ldots + E_{nn},$$

hetgeen ledit tot de conclusie, dat $(\delta_{ij}) \in I$. Volgens gevolg 11.4 is $I = M_n(R)$. Dus $M_n(R)$ bevat geen echte idealen $\neq 0$, waarmee de bewering is aangetoond.

Een ring $R \neq \{0\}$ noemt men <u>enkelvoudig</u> als R geen twee-zijdige idealen heeft anders dan $\{0\}$ en R. De matrix-ring $M_n(R)$ is een enkelvoudige ring.

<u>Opmerking.</u> $M_n(R)$ heeft geen echte 2-zijdige idealen $\neq 0$, maar $M_n(R)$ heeft echte rechts- (links-)idealen $\neq 0$. Bijv. in de ring $M_2(R)$ vormt de verzameling van alle matrices van de vorm $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, a, b $\in$ R een rechts-ideaal, maar geen links-ideaal. Evenzo is de verzameling van alle matrices van de vorm $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$, c, d $\in$ R een links-ideaal, maar geen rechts-ideaal.

<u>Stelling 11.5.</u> Laat $\{I_i\}$ een willekeurige verzameling idealen zijn in de ring R, waarin i een index-verzameling doorloopt. Dan is $\bigcap_i I_i$ ook een ideaal in R.

<u>Bewijs.</u> $\bigcap_i I_i$ is niet leeg, want elk van de idealen I_i bevat het nul-element van R. Stel nu dat a, b $\in \bigcap_i I_i$ en r $\in$ R. Dan geldt a, b $\in I_i$ voor een willekeurige i uit de index-verzameling. Dus $a - b \in I_i$, $ar \in I_i$ en $ra \in I_i$, want I_i is ideaal in R (def.11.2). Omdat dit geldt voor iedere i, volgt hieruit dat $a - b \in \bigcap_i I_i$, $ar \in \bigcap_i I_i$ en $ra \in \bigcap_i I_i$. Dus $\bigcap_i I_i$ is een ideaal in R.

Laat R een willekeurige ring zijn en S een niet-lege deelverzameling van R. Evenals voor groepen (pag.17) definiëren we het symbool (S) als volgt:

$$(S) = \cap \{I \mid S \subseteq I;\ I \text{ is ideaal in } R\}.$$

De verzameling (S) is niet leeg, want R is ideaal in R en $S \subseteq R$. Omdat $S \subseteq I$ voor ieder ideaal I in de definitie van (S) en $(S) = \cap I$ volgt dat $S \subseteq (S)$.
Een direct gevolg van stelling 11.5 is dat (S) een ideaal is in R, dat

bekend staat als het ideaal, voortgebracht door de verzameling S.
Uit de definitie van (S) volgt, dat voor ieder ideaal I in R met $S \subseteq I$ geldt dat $(S) \subseteq I$. Omdat ook $S \subseteq (S)$ noemt men (S) wel het kleinste ideaal van R, dat de verzameling S bevat. Soortgelijke redeneringen gelden voor de eenzijdige idealen in R, die door S worden voorgebracht. In het algemeen is de beschrijving van (S) elementsgewijs ingewikkelder dan in het geval van groepen. Als S uit een eindig aantal elementen, bijv. $a_1, a_2, \ldots, a_n$, bestaat, wordt het ideaal (S) aangegeven door $(a_1, a_2, \ldots, a_n)$. Een dergelijk ideaal heet eindig voortgebracht en de elementen heten voortbrengenden. Een ideaal (a), dat wordt voortgebracht door precies één ring-element, heet een hoofdideaal.
Het hoofdideaal (a) is dus de doorsnede van alle idealen die a bevatten of het kleinste ideaal dat a bevat. Het rechts-ideaal $(a)_r$, voortgebracht door a, is de doorsnede van alle rechts-idealen die a bevatten. Omdat $(a)_r$ gesloten is t.o.v. vermenigvuldiging van rechts, bevat $(a)_r$ alle producten $ar (r \in R)$ evenals de elementen $na (n \in Z)$, en dus alle elementen van de vorm $ar + na (r \in R, n \in Z)$. Stel $I = \{ar + na \mid r \in R; n \in Z\}$. Dan geldt:

$$(ar_1+n_1a) - (ar_2+n_2a) = a(r_1-r_2) + (n_1-n_2)a, \quad r_1, r_2 \in R, n_1, n_2 \in Z$$

en $(ar_1+n_1a)r = (ar_1)r + n_1(ar) = a(r_1r+n_1r), \quad r \in R,$

dus I is een rechts-ideaal in R (def.11.2) en $I \subseteq (a)_r$. Omdat

$a = a.0 + 1.a \in I$, geldt ook $(a)_r \subseteq I$. Dus $I = (a)_r$, zodat

$$(a)_r = \{ar + na \mid r \in R; n \in Z\}.$$

Als R een één-element e heeft, is de term na overbodig, en we kunnen de uitdrukking ar + na eenvoudiger schrijven als:
$ar + na = ar + a(ne) = a(r+ne) = ar'$, waarin $r' = r + ne$ een ring-element is. Dus de verzameling $(a)_r$ bestaat uit alle rechter-veelvouden van a door elementen van R, ook wel aangeduid door aR:

$$(a)_r = aR = \{ar \mid r \in R\}.$$

Analoge opmerkingen gelden voor links-idealen en voor het links-ideaal $(a)_l$.

Opmerking. De verzameling $aR = \{ar \mid r \in R\}$ is een rechts-ideaal in R, ook als de ring geen één-element heeft. Dit ideaal behoeft echter a niet te bevatten, bijv. $4Z_2 = \{4.(2n) \mid n \in Z\}$ is ideaal in Z_2, de ring van even getallen.
Laat (a) het hoofdideaal zijn, voortgebracht door $a \in R$. Dan bevat (a) de elementen ras, ra, as en na voor iedere keuze van $r, s \in R$, $n \in Z$. Iedere eindige som van de vorm $\sum r_i a s_i (r_i, s_i \in R)$ behoort tot (a). Dus (a) bevat alle elementen van de gedaante:

$$ma + ra + as + \sum_{\text{eindig}} r_i a s_i, \qquad r, s, r_i, s_i \in R, n \in Z.$$

De verzameling $J = \{na + ra + as + \sum_{\text{eindig}} r_i a s_i \mid r, s, r_i, s_i \in R; n \in Z\}$ is een ideaal in R en $J \subseteq (a)$. Omdat $a \in J$, geldt ook $(a) \subseteq J$. Dus $J = (a)$, zodat

$$(a) = \{na + ra + as + \sum_{\text{eindig}} r_i a s_i \mid r, s, r_i, s_i \in R;\ n \in Z\}.$$

Als R een één-element e heeft, reduceert deze omschrijving van (a) tot:

$$(a) = \{ \sum_{\text{eindig}} r_i a s_i \mid r_i, s_i \in R\}.$$

Voor commutatieve R geldt, in het algemeen,

$$(a) = \{na + ra \mid r \in R, n \in Z\}.$$

Voor commutatieve ringen met één-element geldt:

$$(a) = aR = Ra.$$

Definitie 11.6. Een ring R heet een hoofd-ideaalring als ieder ideaal I van R hoofdideaal is.

Stelling 11.7. De ring Z is een hoofdideaalring.

Bewijs. We tonen aan dat ieder ideaal I in Z de vorm I = (n) met n geheel, $n \geq 0$, heeft.
Als I = {0}, dan is de stelling juist, want het nul-ideaal {0} is het hoofdideaal voortgebracht door 0.
Stel $I \neq \{0\}$ en $m(\neq 0) \in I$. Dan ook $0 - m = -m \in I$, dus I bevat een positief geheel getal (I is niet leeg). Laat n het kleinste positief gehele getal zijn in I. Omdat I een ideaal is in Z, behoort ieder geheel veelvoud van n tot I, dus $(n) \subseteq I$.
Stel k is willekeurig element in I. Volgens de delingsalgorithmus bestaan er gehele getallen q en r met $k = qn + r$ en $0 \leq r < n$. Dus $r = k - qn \in I$, want $k \in I$ en $qn \in I$. Als $r > 0$, dan hebben we een tegenspraak met de aanname dat n het kleinste positief gehele getal is in I. Dus $r = 0$ en $k = qn \in (n)$. Hieruit volgt $I \subseteq (n)$, zodat $(n) = I$.

XII. Homomorfieën van ringen.

Definitie 12.1. R en R' zijn gegeven ringen. Een ring-homomorfie van R in R' is een afbeelding f: R → R' zodat

$$(a+b)f = (a)f + (b)f$$
$$(ab)f = (a)f(b)f$$

voor ieder paar elementen a, b ∈ R. Een homomorfie, die een bijectie is van de verzameling R op de verzameling R' heet een isomorfie. Als f een homomorfie is van R in R', dan heet de verzameling $(R)f = \{(r)f \mid r \in R\}$ het homomorfe beeld van R onder f. Als R = R', zegt men dat f: R → R een homomorfie is van R in zichzelf. Een homomorfie f: R → R van R in zichzelf wordt ook wel endomorfie van R genoemd. Een isomorfie f: R → R van R op R heet een automorfie van R.

Voorbeelden.

1) R en R' zijn willekeurige ringen en f: R → R' is de afbeelding, waarvoor geldt (r)f = 0 voor iedere r ∈ R. Dus:

$$(a+b)f = 0 = 0+0 = (a)f + (b)f$$
$$(ab)f = 0 = 0.0 = (a)f \circ (b)f \qquad (a,b \in R),$$

zodat f een homomorfie is. Deze homomorfie is de triviale homomorfie.

2) $\bar{Z}_n$ is de ring van gehele getallen modulo n, n > 0, n vast en geheel (zie voorbeeld 7, pag. 59). Z is de ring van gehele getallen. Definieer f: Z → $\bar{Z}_n$ door te stellen a ↦ [a], waarin a ∈ Z, d.w.z. ieder geheel getal wordt afgebeeld op de restklasse modulo n, die het bevat. Dan geldt:

$$(a+b)f = [a+b] = [a] + [b] = (a)f + (b)f$$
$$(ab)f = [ab] = [a] \circ [b] = (a)f \circ (b)f$$

voor ieder paar a, b ∈ Z. Dus f is een homomorfie.

3) Map (X,R) = {f | f: X → R} is de ring van afbeeldingen van een niet-lege verzameling X in een ring R (zie voorbeeld 5, pag. 58).

Definieer ϕ_a: Map (X,R) $\to$ R door $(f)\phi_a = (a)f$ voor iedere $f \in$ map (X,R); a is een vast element uit X. Dan geldt:

$$(f+g)\phi_a = (a)(f+g) = (a)f + (a)g = (f)\phi_a + (g)\phi_a$$
$$(fg)\phi_a = (a)(f\circ g) = (a)f \circ (a)g = (f)\phi_a \circ (g)\phi_a$$

voor ieder paar f, g $\in$ map (X,R). Dus ϕ_a is een homomorfie, de z.g. evaluatie-homomorfie in a.

4) $Z[i] = \{a+bi \mid a,b \in Z\}$ is de ring van de gehele getallen van Gauss (zie voorbeeld 6, pag. 59). $\bar{Z}_2 = \{[0],[0]\}$ is de ring van de restklassen modulo 2. Definieer de afbeelding f: $Z[i] \to \bar{Z}_2$ door het voorschrift:

$(a+bi)f = [0]$, als $a \equiv b(2)$ is
$(c+di)f = [1]$, als $c \not\equiv d(2)$ is.

Er geldt: $\{(a+bi) + (c+di)\}f = \{(a+c) + (b+d)i\}f$.

a) Als $a \equiv b(2)$, $c \equiv d(2)$, dan is $a+c \equiv b+d(2)$, dus
$\{(a+c) + (b+d)i\}f = [0] = [0] + [0] = (a+bi)f + (c+di)f$.

b) Als $a \equiv b(2)$, $c \not\equiv d(2)$, dan is $a + c \not\equiv b+d(2)$, dus
$\{(a+c) + (b+d)i\}f = [1] = [0] + [1] = (a+bi)f + (c+di)f$.

c) Als $a \not\equiv b(2)$, $c \equiv d(2)$, dan is $a+c \not\equiv b+d(2)$, dus
$\{(a+c) + (b+d)i\}f = [1] = [1] + [0] = (a+bi)f + (c+di)f$.

d) Als $a \not\equiv b(2)$, $c \not\equiv d(2)$, dan is $a+c \equiv b+d(2)$ dus
$\{(a+c) + (b+d)i\}f = [0] = [1] + [1] = (a+bi)f + (c+di)f$.

Voor de vermenigvuldiging geldt:

$$(a+bi) \circ (c+di) = ac - bd + (ad+bc)i.$$

Nu is
$$(ac-bd)^2 = a^2c^2 + b^2d^2 - 2abcd$$
$$(ad+bc)^2 = a^2d^2 + b^2c^2 + 2abcd \quad +$$
$$(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2).$$

Het produkt $(a^2+b^2)(c^2+d^2)$ is dan en slechts dan oneven als beide factoren oneven zijn. Ook geldt:

$a^2 + b^2$ oneven $\iff$ $a \not\equiv b(2)$
$c^2 + d^2$ oneven $\iff$ $c \not\equiv d(2)$

Dus $(ac-bd)^2 + (ad+bc)^2$ oneven $\Longleftrightarrow$ a $\nmid$ b(2) en c $\nmid$ d(2).
Ook: $(ac-bd)^2 + (ad+bc)^2$ oneven $\Longleftrightarrow$ (ac-bd) $\nmid$ (ad+bc)(2).
Dus (ac-bd) $\nmid$ (ad+bc)(2) $\Longleftrightarrow$ a $\nmid$ b(2) en c $\nmid$ d(2).
Dan volgt ((a+bi) $\circ$ (c+di)f = {ac-bd+(ad+bc)i}f = [1] , (a+bi)f = = [1] en (c+di)f = [1].
Wegens [1] $\circ$ [1] = [1] en [1] $\circ$ [0] = [0] $\circ$ [1] = [0] $\circ$ [0] = [0] is ((a+bi) $\circ$ (c+di)f = (a+bi)f $\circ$ (c+di)f in alle gevallen.
Dus f is een homomorfie van Z [i] op $\bar{Z}_2$.

Stelling 12.2. f: R $\to$ R' is een homomorfie van de ring R in de ring R'. Dan geldt:
1) (0)f = 0
2) (-a)f = -(a)f voor iedere a $\in$ R. Als R en R' resp. het eenheidselement e, e' hebben en f is een homomorfie op i.e. Im f = R', dan geldt:
3) (e)f = e'
4) $(a^{-1})f = (a)f^{-1}$ voor iedere eenheid a in R.

Bewijs. Uit (0)f = (0+0)f = (0)f + (0)f volgt (0)f = 0.
Uit (a)f + (-a)f = (a+(-a))f = (0)f = 0 volgt (-a)f = -(a)f.
Wat (3) betreft, stel a $\in$ R zodat (a)f = e', dan volgt: (e)f = = (a)f $\circ$ (e)f = (a $\circ$ e)f = e'.
Tenslotte volgt uit (a)f $\circ$ $(a^{-1})f = (a \circ a^{-1})f = (e)f = e'$, dat $(a)f^{-1} = (a^{-1})f$, voor ieder element a in R, dat eenheid is.

Opmerking. Op grond van 2) in stelling 12.2 geldt ook (a-b)f = (a)f + (-b)f = (a)f - (b)f voor iedere keuze van a, b $\in$ R. Dus een ring-homomorfie respecteert verschillen, sommen en produkten.

Stelling 12.3. f: R $\to$ R' is een homomorfie van de ring R in de ring R'. Dan geldt:
1) Voor iedere deelring S van R, is (S)f een deelring van R'.
2) Voor iedere deelring S' van R' is $(S')f^{-1} = \{S \mid s \in R \text{ en } (s)f \in S'\}$ een deelring van R.

Bewijs. 1) Per definitie is $(S)f = \{(a)f \mid a \in S\}$.
Stel nu $(a)f, (b)f \in (S)f$. Dan $a, b \in S$, dus $a-b$ en $a \circ b$ behoren tot S (st.10.6). Dus

$$(a)f - (b)f = (a-b)f \in (S)f$$
$$\text{en } (a)f \circ (b)f = (ab)f \in (S)f$$

Wegens $S \neq \emptyset$ is $(S)f \neq \emptyset$, dus $(S)f$ is deelring van R' (St.10.6)
2) Stel nu $a, b \in (S')f^{-1}$, dus $(a)f, (b)f \in S'$. Omdat S' deelring is van R', volgt direct dat

$$(a-b)f = (a)f - (b)f \in S'$$
$$\text{en } (a \circ b)f = (a)f \circ (b)f \in S'.$$

Dit betekent dat $a-b, a \circ b \in (S')f^{-1} \Longrightarrow (S')f^{-1}$ is deelring van R. Immers $(S')^{f-1} = \emptyset$, want $0 \in R$ en $(0)f = 0 \in S'$, dus $0 \in (S')f^{-1}$. Hiermee is de stelling bewezen. Deel 2) van st.12.3. blijft gelden, als we "deelring" vervangen door "ideaal". Preciezer geformuleerd: Als I' een ideaal is in R', dan is de deelring $(I')f^{-1}$ een ideaal in R. Immers: $(I')f^{-1}$ is deelring van R volgens st.12.3. Stel dat $a \in (I')f^{-1}$, dus $(a)f \in I'$ en kies 'n element $r \in R$. Dan geldt: $(ar)f = (a)f \circ (r)f \in I'$ en $(ra)f = (r)f \circ (a)f \in I'$, m.a.w. $ar \in (I')f^{-1}$ en $ra \in (I')f^{-1}$. Volgens def. 11.2 is $(I')f^{-1}$ dan ideaal in R.
Zonder verdere beperkingen kan men niet bewijzen, dat $(I)f$ een ideaal is in R', als I ideaal is in R. Men heeft nodig dat $r' \circ (a)f \in (I)f$ voor alle $r' \in R'$ en $a \in I$. Een voldoende voorwaarde is, dat $r' \in R'$ vervangen kan worden door $(r)f$, $r \in R$, zodat men kan gebruiken dat I ideaal is in R. Het antwoord is dus duidelijk: neem voor f een surjectie. Dus:

Gevolg 12.4.

1) Voor ieder ideaal I' van R' geldt dat de deelring $(I')f^{-1}$ ideaal is in R.
2) Als $(R)f = R'$, dan is, voor ieder ideaal I in R, de deelring $(I)f$ een ideaal in R'.

Definitie 12.5. f is een homomorfie van de ring R in de ring R'. De kern van f, aangeduid door ker f, bestaat uit die elementen van R, die door f op het nul-element van de ring R' worden afgebeeld:

$$\ker f = \{a \in R \mid (a)f = 0\}.$$

Uit stelling 12.2 volgt dat ker f een niet-lege deelverzameling is van R, omdat $0 \in \ker f$. Behalve in het geval van de triviale homomorfie, is de kern steeds een echte deelverzameling van R.

Stelling 12.6. De kern van een homomorfie f van een ring R in een ring R' is een ideaal in R.

Bewijs. We hebben gezien dat de verzameling {0}, bestaande uit het nul-element van R', een deelring is in R', een z.g. triviale deelring (p.63). Omdat $r' \circ 0 = 0 \circ r' = 0$ voor iedere $r' \in R'$, is deze deelring {0} ook ideaal in R' (def.11.2). Uit de definitie van ker f volgt: $\ker f = (0)f^{-1}$, dus ker f is ideaal in R volgens gevolg 12.4 (1).

Stelling 12.7. Een homomorfie f van een ring R in een ring R' is injectief dan en slechts dan als $\ker f = \{0\}$.

Bewijs. Stel dat de afbeelding f injectief is. Omdat $(0)f = 0$, volgt uit $(a)f = 0 = (0)f$ voor een element $a \in R$, dat $a = 0$. Dus $\ker f = \{0\}$. Omgekeerd, stel dat $\ker f = \{0\}$. Als $a, b \in R$ met $(a)f = (b)f$, dan volgt $(a-b)f = (a)f - (b)f = 0$, dus $a-b \in \ker f = \{0\}$. Daarom is $a = b$ en f injectief. Hiermee is de stelling bewezen.

Definitie 12.8. R en R' zijn gegeven ringen. Dan is R isomorf met R', aangeduid door $R \cong R'$, als er een homomorfie f van R op R' bestaat, die een bijectieve afbeelding is.

Uit de definitie volgt direct, dat, als $R \cong R'$, ook geldt $R' \cong R$. Immers als $f: R \to R'$ een bijectie en een homomorfie is, dan geldt dit ook voor $f^{-1}: R' \to R$. Men zegt daarom, dat twee ringen R en R' isomorf zijn zonder aan te geven dat R isomorf is met R' of R' isomorf is met R.

Twee isomorfe ringen, ofschoon in het algemeen formeel niet identiek, zijn vanuit algebraïsch standpunt identiek: er bestaat een afbeelding, die de algebraïsche structuur van een ring op de ander overbrengt. In het geval dat de homomorfie $f: R \to R'$ injectief is, heeft men een bijectie $f': R \to \text{Im } f$ van R op Im f (in R'). Voor alle $a,b \in R$ geldt: $(a+b)f' = (a+b)f = af + bf = af' + bf'$ en $(ab)f' = (ab)f = (af)(bf) = (af')(bf')$. Dus f' is een homomorfie. De ringen R en Im f zijn dus isomorf. Omgekeerd, als R en R' isomorfe ringen zijn, dan is er een bijectie $g: R \to R'$ van R op R', die tevens homomorfie is (def.12.8). Volgens st.12.7 geldt dus $\ker g = \{0\}$. Men heeft dus

Gevolg 12.9. Een homomorfie $f: R \to R'$ van een ring R op een ring R' met $\ker f = K$ is een isomorfie van R op R' dan en slechts dan als $K = \{0\}$.

Voorbeeld. R is een ring met één - element e en de afbeelding $f: Z \to R$ wordt gegeven door $(n)f = ne$, $n \in Z$. Dan is f een homomorfie van Z in R:

$$(n+m)f = (n+m)e = ne + me = (n)f + (m)f$$
$$(nm)f = (nm)e = n(me) = (ne)(me) = (n)f \circ (m)f.$$

Ker f is een ideaal in Z (st.12.6) en Z is een hoofdideaalring (st.11.7) dus

$$\ker f = \{n \in Z \mid ne = 0\} = (t),$$

t geheel, $t \geq 0$. In het speciale geval, dat $t = 0$, volgt $\ker f = \{0\}$, dus f is injectief. Men heeft dan $Z \cong \text{Im } f \ (\subseteq R)$ en men noemt f een isomorfie van Z in R. In dit geval bevat R dus een deelring Im f, die isomorf is met de ring van de gehele getallen.

XIII Factorringen en homomorfie-stellingen.

R en R' zijn gegeven ringen en f: R → R' is een ring-homomorfie van R op R'. Wegens (R)f = R', bepaalt ieder ideaal I van de ring R een ideaal (I)f in de ring R' (gevolg 12.4). Men zou kunnen denken dat in dit geval de idealen van R één-éénduidig corresponderen met die van R' volgens de afbeelding f. Dit is echter, in het algemeen, niet juist. Immers, stel I en J zijn idealen in R, waarvoor geldt: $I \subseteq J \subseteq I + \ker f$, waarbij $I + \ker f = \{i + a \mid i \in I, a \in \ker f\}$, dan geldt $(I)f \subseteq (J)f \subseteq (I+\ker f)f = (I)f$, dus $(I)f = (J)f$. Idealen I en J in R, die verschillend zijn, kunnen dus hetzelfde beeld hebben in R'.
Men kan dit verbeteren door òf te eisen, dat $\ker f = \{0\}$ òf door alleen idealen I in R te beschouwen waarvoor geldt $\ker f \subseteq I$. In beide gevallen volgt dat $I \subseteq J \subseteq I + \ker f \subseteq I$, zodat I = J. Als $\ker f = \{0\}$ dan is de afbeelding f een bijectie en $R \cong R'$ (gevolg 12.9). Het is duidelijk dat er dan ook een bijectief verband tussen de idealen van R en die van R' bestaat. We zullen nu het tweede geval: $\ker f \subseteq I$ nader onderzoeken.

Hulpstelling 13.1. f : R → R' is een homomorfie van R op R'. Als I een ideaal is in de ring R met $\ker f \subseteq I$, dan geldt $I = ((If)f^{-1})$.

Bewijs. Stel a is een element in R met $a \in ((I)f)f^{-1}$,
dus $(a)f \in (I)f$. Dan is $(a)f = (r)f$ voor een element $r \in I$. Dus $(a-r)f = 0$ of $a - r \in \ker f \subseteq I$. Hieruit volgt $a \in I$, zodat $((I)f)f^{-1} \subseteq I$. Omdat $I \subseteq ((I)f)f^{-1}$ altijd geldt, volgt hieruit dat $I = ((I)f)f^{-1}$.

Stelling 13.2. (Correspondentie-stelling)
f : R → R' is een homomorfie van de ring R op de ring R'. Dan is er een bijectief verband tussen die idealen I van R waarvoor geldt $\ker f \subseteq I$ en de verzameling van alle idealen I' in R'; de correspondentie wordt gegeven door I' = (I)f, als I ideaal is in R met $\ker f \subseteq I$.

Bewijs. We tonen eerst aan dat de genoemde correspondentie surjectief is, d.w.z. dat ieder ideaal in R' beeldelement is. M.a.w., als I' een

---

ideaal is in R', moeten we een ideaal I in de ring R bepalen met ker f $\subseteq$ I en zodat (I)f = I'. Men kan I = (I')f^{-1} nemen. Volgens gevolg 12.4 (1) is (I')f^{-1} een ideaal in R. Omdat 0 $\in$ I', is ker f = = (0)f^{-1} $\subseteq$ (I')f^{-1}. Ook volgt (I)f = ((I')f^{-1})f. Uit de definitie van (I')f^{-1} volgt dat ((I')f^{-1})f $\subseteq$ I'. Nu is f een op-afbeelding, dus bij i' $\in$ I' bestaat r $\in$ R zodat (r)f = i'. Maar dan is r $\in$ (I')f^{-1}, dus i' $\in$ ((I')f^{-1})f, zodat I' $\subseteq$ ((I')f^{-1})f en I' = ((I')f^{-1})f = (I)f. Vervolgens tonen we de injectiviteit van de correspondentie aan. Stel dus dat I en J idealen zijn in R met ker f $\subseteq$ I, ker f $\subseteq$ J en zodat (I)f = (J)f. Uit hulpstelling 13.1 volgt nu:

$$I = ((I)f)f^{-1} = ((J)f)f^{-1} = J.$$

Dus de correspondentie is bijectief: I $\Longleftrightarrow$ (I)f met ker f $\subseteq$ I, waarmee de stelling is bewezen.
Men kan nog opmerken, dat de correspondentie inclusie-behoudend is; d.w.z. als I $\subseteq$ J voor idealen I en J in R met ker f $\subseteq$ I, ker f $\subseteq$ J, dan is (I)f $\subseteq$ (J)f. Omgekeerd, als I' $\subseteq$ J' voor idealen I', J' in R', dan is (I')f^{-1} $\subseteq$ (J')f^{-1} in R.
Het begrip ideaal heeft een equivalentie-relatie tot gevolg. Evenals in de groepentheorie met betrekking tot groep en ondergroep is ingevoerd (zie def.5.1., p.22) kan men met betrekking tot ring en ideaal definiëren: R is een ring en I is een ideaal in R. Stel a, b $\in$ R. Dan is a $\equiv$ b mod I als a - b $\in$ I.
De betrekking "a $\equiv$ b mod I" is een equivalentie-relatie. Het bewijs hiervan wordt aan de lezer overgelaten.
De relatie "$\equiv$ mod I" induceert een partitie van R in equivalentieklassen, die we nu nader bekijken.

Stelling 13.3. Als I een ideaal is in de ring R, dan is de equivalentie-klasse van b $\in$ R voor de relatie $\equiv$ mod I de verzameling

$$b + I = \{b + i \mid i \in I\}.$$

Bewijs. Stel [b] = $\{x \in R \mid x \equiv b \bmod I\}$. Als a = b + i behoort tot b + I, dan is a - b = i $\in$ I. Volgens definitie van $\equiv$ mod I betekent dit

dat $a \equiv b \bmod I$, dus $a \in [b]$, zodat $b + I \subseteq [b]$. Omgekeerd, als $x \in [b]$, dan geldt $x \equiv b \bmod I$, dus $x - b = i$ voor een element $i \in I$, zodat $x = b + i \in b + I$. Dus de inclusie $[b] \subseteq b + I$ is ook geldig en $[b] = b + I$.

Het is gebruikelijk om een verzameling van de vorm $b + I$ een restklasse van I in R en het element b een representant van de klasse $b + I$ te noemen.

De volgende stelling geeft enkele basis-eigenschappen van restklassen. Deze eigenschappen zijn een direct gevolg van bekende eigenschappen van equivalentie-klassen.

Stelling 13.4. R is een ring en I is ideaal in R. Stel $a, b \in R$.
Dan geldt:

1) $a + I = I$ dan en slechts dan als $a \in I$.
2) $a + I = b + I$ dan en slechts dan als $a - b \in I$.
3) òf $a + I = b + I$ òf $(a+I) \cap (b+I) = \emptyset$.

Bewijs. 1) Stel $a + I = I \Longrightarrow a = a + 0 \in a + I = I$.
Stel $a \in I$. Dan is $a + i \in I$ voor iedere $i \in I$, dus $a + I \subseteq I$.
Ook is $i = a + (i-a) \in a + I$ voor iedere $i \in I$, dus $I \subseteq a + I$.
Dus $I = a + I$.

2) Stel $a + I = b + I \Longrightarrow a \in a + I = b + I \Longrightarrow a \equiv b \bmod I \Longrightarrow a - b \in I$.
Stel $a - b \in I$. Dus $a \equiv b \bmod I$ of $a \in b + I$, dus $a + I \subseteq b + I$.
Evenzo $b \equiv a \bmod I$ of $b \in a + I$, zodat $b + I \subseteq a + I$.
Dus $a + I = b + I$.

3) Stel $(a+I) \cap (b+I) \neq \emptyset$, bijv. $c \in (a+I) \cap (b+I)$.
Dus $c \in a + I$ en $c \in b + I$ of $c = a + i_1 = b + i_2$, $i_1, i_2 \in I$.
Dan $a - b = i_2 - i_1 \in I$, dus $a + I = b + I$ volgens 2).

Evenals in de groepentheorie met betrekking tot normaaldelers, kan men de verzameling van verschillende restklassen van I in R een ring-structuur geven. We zullen het symbool R/I gebruiken om de verzameling van alle restklassen van I in R aan te geven, d.w.z.

$$R/I = \{a + I \mid a \in R\}.$$

Op R/I worden twee binaire operaties + en $\circ$ gedefinieerd door:

$$(a+I) + (b+I) = (a+b) + I$$

$$(a+I) \circ (b+I) = ab + I.$$

Men moet nu aantonen, dat deze "optelling" en "vermenigvuldiging" van restklassen mod I ondubbelzinnig is gedefinieerd, d.w.z. onafhankelijk van de keuze van de representanten in deze klassen.
Stel daarom $a + I = a' + I$ en $b + I = b' + I$. Dus $a - a' \in I$ en $b - b' \in I$ (st. 13.4), of $a - a' = i_1$ en $b - b' = i_2$, $i_1, i_2 \in I$. Dan volgt $(a+b) - (a'+b') = (a-a') + (b-b') = i_1 + i_2 \in I$, dus $(a+b) + I = (a'+b') = I$ (st. 13.4). Het resultaat is dus dat $(a+I) + (b+I) = (a'+I) + (b'+I)$. Met betrekking tot de vermenigvuldiging van restklassen mod I, merken we op dat $ab - a'b' = a(b-b') + (a-a')b' = ai_2 + i_1 b' \in I$, omdat $ai_2 \in I$ en $i_1 b' \in I$. Dus $ab + I = a'b' + I$ of $(a+I) \circ (b+I) = (a'+I) \circ (b'+I)$. De definitie van vermeningvuldiging is zinvol.

Stelling 13.5. R is een ring en I is een ideaal in R. Dan is R/I, met de gedefinieerde optelling en vermenigvuldiging, een ring, die bekend staat als de factorring of restklassenring van R naar I.

Bewijs. (R/I,+) is een commutatieve groep wordt op dezelfde manier bewezen, als in st.5.14 (p.29 en 30). De commutativiteit van de optelling volgt uit:

$$(a+I) + (b+I) = (a+b) + I = (b+a) + I = (b+I) + (a+I).$$

De associativiteit van de vermenigvuldiging is een gevolg van de associativiteit in R:

$$\{(a+I) \circ (b+I)\} \circ (c+I) = \{ab + I\} \circ (c+I) = (ab)c + I = a(bc) + I =$$

$$= (a+I) \circ \{bc + I\} = (a+I) \circ \{(b+I) \circ (c+I)\}.$$

De distributieve wetten zijn eveneens een gevolg van dezelfde wetten in R.
We merken nog op, dat de restklasse $I = 0 + I$ het nul-element in R/I is

en dat de additieve inverse van a + I ($a \in R$) de klasse -a + I is. In st.12.6 hebben we gezien, dat bepaalde idealen voorkomen als kernen van homomorfieën. We zullen nu aantonen, dat ieder ideaal inderdaad op deze manier ontstaat.

Stelling 13.6. I is een ideaal in de ring R. Dan is de afbeelding: $nat_I : R \to R/I$ gedefinieerd door $(a)nat_I = a + I$ een homomorfie van R op de factorring R/I. De kern van nat_I is precies de verzameling I.

Bewijs. Voor iedere $a \in R$ geldt: $a = a + 0 \in a + I$ en wegens st.13.4 behoort a dus tot precies één restklasse. Dus de afbeelding nat_I is zinvol. Er geldt: $(a+b)nat_I = (a+b) + I = (a+I) + (b+I) = (a)nat_I + (b)nat_I$ en $(ab)nat_I = ab + I = (a+I) \circ (b+I) = (a)nat_I \circ (b)nat_I$. Dus nat_I is een ring-homomorfie. Ieder element van R/I is een restklasse a + I, met $a \in R$ en per definitie is $(a)nat_I = a + I$, dus nat_I is surjectief. Tenslotte geldt: $ker(nat_I) = \{a \in R \mid (a)nat_I = I\}$

$$= \{a \in R \mid a + I = I\} = I$$

wegens stelling 13.4. Hiermee is de stelling bewezen. Men noemt de afbeelding nat_I, die aan ieder element in R de restklasse in R/I toevoegt waarvan het een representant is, de natuurlijke afbeelding van R op de factorring R/I.

Voorbeeld. Z is de ring van de gehele getallen en n is een positief geheel getal. Beschouw het hoofdideaal (n) in Z. De restklassen van (n) in Z hebben de vorm: $a + (n) = \{a + kn \mid k \in Z\}$, waaruit blijkt, dat de restklassen van (n) precies de congruentie-klassen modulo n zijn. Wat eerder werd ingevoerd als de operaties voor de congruentieklassen modulo n resp. als het samenstellen van nevenklassen(zie voorbeeld 6, §1 resp. voorbeeld p.30) kan nu worden beschreven als het samenstellen van restklassen in Z/(n):

$$(a+(n)) + (b+(n)) = a + b + (n)$$

$$(a+(n)) \circ (b+(n)) = ab + (n).$$

$(Z/(n),+)$ valt samen met wat op p.30 is genoemd: Z/Z_n.

Kortom, de ring $\overline{Z}_n$ van gehele getallen modulo n, $n > 0$, kan opgevat worden als de factorring van Z naar (n).
De afbeelding $nat_{(n)} : Z \to \overline{Z}_n$, gedefinieerd door $a \to [a] = a + (n)$, is de natuurlijke afbeelding van Z op de factorring $\overline{Z}_n$, (vgl. voorbeeld 2, p.77).
We passen nu de correspondentie-stelling toe op het geval, dat we beginnen met een ideaal I in R en voor de homomorfie f de natuurlijke afbeelding $nat_I : R \to R/I$ nemen. Omdat $ker(nat_I) = I$ (st.13.6) moet de formulering iets gewijzigd worden:

Stelling 13.7. Laat I een ideaal zijn in de ring R. Dan bestaat er een bijectief verband tussen die idealen J van R waarvoor geldt $I \subseteq J$ en de verzameling van alle idealen J' van de factorring R/I, J' wordt gegeven door $(J)nat_I = J'$, met J ideaal in R en $I \subseteq J$.

Nu is $(J)nat_I = \{j + I \mid j \in J\} = J/I$, omdat I ook ideaal in J is. Anders gezegd: de idealen van R/I hebben de vorm J/I, waarin J een ideaal is in R en $I \subseteq J$. Als toepassing hiervan bewijzen we de volgende bewering:
De ring $\overline{Z}_n$ van gehele getallen modulo n heeft precies één ideaal voor iedere positieve deler m van n, en geen andere idealen.
Omdat $\overline{Z}_n = Z/(n)$, is er volgens st.13.7 een bijectief verband tussen die idealen van de ring Z die (n) bevatten en de verzameling van idealen van $\overline{Z}_n$. De idealen van Z zijn precies de hoofdidealen (m), waarin (m) een niet-negatief geheel getal is (st.11.7). Er is dus een bijectief verband tussen de idealen van $\overline{Z}_n$ en die idealen (m) van Z, waarvoor geldt $(m) \supseteq (n)$. Als $(m) \supseteq (n)$, dan is $n \in (n) \subseteq (m)$, dus m is een deler van n. Omgekeerd, als m deler is van n, dan is ieder n-voud ook een m-voud (in Z), dus $(n) \subseteq (m)$. Hiermee is de bewering bewezen.

Stelling 13.8. (Ontbinding van homomorfieën). $f : R \to R'$ is een homomorfie van de ring R op de ring R' en I is een ideaal van R met $I \subseteq \ker f$. Dan bestaat er een eenduidig bepaalde homomorfie $\overline{f} : R/I \to R'$ met de eigenschap dat $f = nat_I \circ \overline{f}$.

Bewijs. We definiëren eerst een afbeelding

$\overline{f} : R/I \to R'$, de z.g. geïnduceerde afbeelding, door

$$(a+I)\overline{f} = (a)f \qquad (a \in R).$$

De eerste vraag is, of $\overline{f}$ zinvol gedefinieerd is. D.w.z. we moeten aantonen dat de definitie onafhankelijk is van de keuze van de representanten. Stel $a + I = b + I$, dus $a - b \in I$ (st.13.4) en $I \subseteq \ker f$, zodat $a - b \in \ker f$ en $(a)f = (a-b+b)f = (a-b)f + (b)f = (b)f$, dus $(a+I)\overline{f} = (a)f = (b)f = (b+I)\overline{f}$. De afbeelding is dus zinvol.
Vervolgens tonen we aan, dat $\overline{f}$ een homomorfie is

$$\{(a+I) + (b+I)\}\overline{f} = (a+b+I)\overline{f} = (a+b)f = (a)f + (b)f = (a+I)\overline{f} = (b+I)\overline{f}$$

en, evenzo,

$$\{(a+I) \circ (b+I)\}\overline{f} = (ab+I)\overline{f} = (ab)f = (a)f \circ (b)f = (a+I)\overline{f} \circ (b+I)\overline{f}.$$

Voor ieder element $a \in R$ geldt:

$$(a)f = (a+I)\overline{f} = \{(a)nat_I\}\overline{f} = (a)\ (nat_I \circ \overline{f}),$$

dus $f = nat_I \circ \overline{f}$.
Blijft nog over aan te tonen, dat deze ontbinding eenduidig is. Stel dus dat $f = nat_I \circ g$ voor nog een afbeelding $g: R/I \to R'$. Dan geldt

$$(a+I)\overline{f} = (a)f = (a)\ (nat_I \circ g) = (a+I)g$$

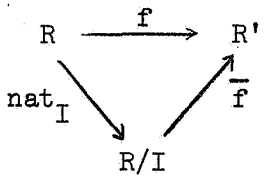
voor iedere restklasse $a + I \in R/I$. Dus $g = \overline{f}$. De geïnduceerde afbeelding is dus de enige afbeelding van de factorring R/I in R', die voldoet aan $f = nat_I \circ \overline{f}$, (Merk op, dat $\overline{f}$ surjectief is).

Gevolg 13.9. De geïnduceerde afbeelding $\overline{f}$ is een isomorfie dan en slechts dan als $\ker f \subseteq I$.

Bewijs. We beschrijven $\ker \overline{f}$ expliciet:

$$\begin{aligned} \ker \overline{f} &= \{a + I \mid (a+I)\overline{f} = 0\} \\ &= \{a + I \mid (a)f = 0\} \\ &= \{a + I \mid a \in \ker f\} = (\ker f)nat_I. \end{aligned}$$

Volgens gevolg 12.9 is een noodzakelijke en voldoende voorwaarde, opdat $\overline{f}$ een isomorfie is, dat ker $\overline{f}$ = I. Dit betekent hier, dat (ker f)nat_I = I, hetgeen weer equivalent is met de inclusie ker f $\subseteq$ I (st.13.4).
Hiermee is gevolg 13.9 bewezen.
De gelijkheid f = $nat_I \circ \overline{f}$ wordt soms genoemd een "ontbinding" van de homomorfie f via de afbeelding nat_I. In een diagram heeft men:



Bij gegeven homomorfie f en ideaal I in R met I $\subseteq$ ker f is er één en slechts één afbeelding $\overline{f}$, die het diagram commutatief maakt.
In het geval I = ker f, zijn zowel st.13.8 als gevolg 13.9 toepasbaar.
Dus f induceert een afbeelding $\overline{f}$, zodat $\overline{f}$: R/I $\to$ R' een isomorfie is.
Hiermee is de volgende stelling bewezen:

Stelling 13.10. (Fundamentele homomorfie-stelling).
Als f : R $\to$ R' een homomorfie is van de ring R op de ring R', dan is R/ker f $\cong$ R'.

Voorbeelden.

1) f : R $\to$ R' is de triviale homomorfie, d.w.z. (r)f = 0 voor iedere r $\in$ R. Dan is ker f = R en R/ker f = R/R $\cong$ Im f = (0).
2) Map(X,R) = {f | f : X $\to$ R} is de ring van afbeeldingen van een niet-lege verzameling X in een ring R en ϕ_a: Map (X,R) $\to$ R door (f)ϕ_a = (a)f is de evaluatie-homomorfie in a. Dan is ker ϕ_a = {f $\in$ Map(X,R) | (a)f = 0}, d.w.z. de afbeeldingen, die 0 zijn in "het punt a". Er geldt:
$$\text{Map}(X,R)/\ker \phi_a \cong \text{Im } \phi_a.$$
3) Z[i] is de ring van de gehele getallen van Gauss en $\overline{Z}_2$ = {[0], [1]} is de ring van restklassen mod 2. Dan is de afbeelding f : Z[i] $\to$ $\overline{Z}_2$

met $(a+bi)f = [0]$, als $a \equiv b(2)$ en

$(c+di)f = [1]$, als $c \not\equiv d(2)$ is, een homomorfie (zie voorbeeld 4, p.78).

Ker $f = \{a + bi \mid a \equiv b(2)\}$ en $Z[i]/\ker f \tilde{=} \overline{Z}_2$.

Representanten van de 2 restklassen in $Z[i]/\ker f$ zijn bijv.

$0 = 0 + 0 \circ i$ en $1 = 0 + 1 \circ i$, zodat

$Z[i]/\ker f = \{\ker f,\ 1 + \ker f\}$.

XIV. Integriteitsgebieden en lichamen

Definitie 14.1. Een ring F wordt een lichaam genoemd als de verzameling $F \setminus \{0\}$ een commutatieve groep is t.o.v. de vermenigvuldiging in F (het neutrale element van deze groep wordt met e genoteerd).
Uit de definitie volgt dat een lichaam tenminste één element verschillend van 0 bevat, want $F \setminus \{0\} \neq \emptyset$, omdat de elementen van $F \setminus \{0\}$ een groep vormen (definitie 1.1). In de ring F geldt $a \circ 0 = 0 \circ a = 0$ voor iedere $a \in F$ (st.10.1), dus voor ieder paar elementen $a, b \in F$ geldt: $a \circ b = b \circ a$ en niet alleen voor de elementen $\neq 0$. Evenzo volgt uit $e \circ 0 = 0 \circ e = 0$, dat e een één-element is voor de ring F. Men kan een lichaam dus ook definiëren door:
Een lichaam is een commutatieve ring met één-element, waarin ieder element $\neq 0$ een inverse heeft t.o.v. de vermenigvuldiging.
Ieder element $\neq 0$ in een lichaam F is dus een eenheid in F (zie blz.66). De groep F^* van de eenheden in F komt overeen met $F \setminus \{0\}$.
Als men de eis van de commutativiteit weglaat in de definitie van een lichaam, heet het stelsel een delingsring. D.w.z. een ring R is een delingsring, als de elementen $\neq 0$ in R een (niet noodzakelijk commutatieve) groep vormen met betrekking tot de vermenigvuldiging.

Voorbeelden.

1) De verzameling Q van rationale getallen, de verzameling R van reële getallen, en de verzameling $F = \{a + b\sqrt{2} \mid a, b \in Q\}$ vormen lichamen. In alle gevallen zijn de binaire operaties de gewone optelling en vermenigvuldiging. Een inverse van $a + b\sqrt{2}$ ($a, b \in Q$, a en b niet beide 0) is $\frac{1}{a^2-2b^2}(a-b\sqrt{2})$.
2) Beschouw de verzameling $C = R \times R = \{(x,y) \mid x \in R \text{ en } y \in R\}$, R de verzameling van de reële getallen, het z.g. Cartesisch product (blz.2). We definiëren een optelling en vermenigvuldiging op C als volgt:

$$(a,b) + (c,d) = (a+c, b+d)$$

$$(a,b)\,(c,d) = (ac-bd, ad+bc).$$

Men kan bewijzen dat C met deze operaties een commutatieve ring met één-element is (vgl. voorbeeld 6 in §9, blz.58). Het paar (1,0) is een één-element voor de vermenigvuldiging, en (0,0) is het nul-element van C. Stel nu $(a,b) \in C$ en $(a,b) \neq (0,0)$, dus of $a \neq 0$ of $b \neq 0$, zodat $a^2 + b^2 > 0$. Dan bestaat $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$ in C en dit element heeft de eigenschap:

$$(a,b)\ (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) = (\frac{a^2+b^2}{a^2+b^2}, \frac{a(-b)+ab}{a^2+b^2}) = (1,0) \quad \text{(St.10.1)}.$$

Dus ieder element $\neq 0$ in C heeft een inverse t.o.v. de vermenigvuldiging, en C is een lichaam.
C bevat een deelring, die isomorf is met het lichaam van de reële getallen. De verzameling

$$R \times \{0\} = \{(a,0) \mid a \in R\}$$

is een deelring van C. Immers, $R \times \{0\} \neq \emptyset$, want $(0,0) \in R \times \{0\}$. Uit $(a,0)$ en $(b,0) \in R \times \{0\}$ volgt dat $(a,0) - (b,0) = (a-b,0) \in R \times \{0\}$ en $(a,0)\cdot(b,0) = (ab,0) \in R \times \{0\}$. Dus $R \times \{0\}$ is een deelring van C.
De afbeelding $f : R \to R \times \{0\}$, gedefinieerd door $a \mapsto (a,0)$ is een isomorfie van R op $R \times \{0\}$, zoals gemakkelijk is aan te tonen. Dus $R \tilde{=} R \times \{0\}$.
Het verschil tussen R en $R \times \{0\}$ is een verschil in notatie; we kunnen het reële getal a identificeren met het geordende paar $(a,0) = (a)f$.
In deze zin kan R als deelring van C beschouwd worden.
Een willekeurig element $(a,b) \in C$ kan geschreven worden als $(a,b) =$
$= (a,0) + (b,0)\cdot(0,1)$, waarin $(0,1)^2 = (0,1) \circ (0,1) = (-1,0)$. We voeren het symbool i in als afkorting van (0,1) : $(a,b) = (a,0) + (b,0)i$.
Tenslotte worden paren van de vorm (a,0) vervangen door hun 1^e component a. Dit kan, wegens $R \tilde{=} R \times \{0\}$. Een representatie van (a,b) wordt dan:

$$(a,b) = a + bi, \text{ met } i^2 = -1.$$

M.a.w., het lichaam C, zoals het hier werd gedefinieerd, is een versie van het bekende stelsel van complexe getallen.

De paren (a,b) met a en b $\in$ Z, vormen een deelring van C, zoals direct duidelijk is (Z is verzameling van de gehele getallen). Deze deelring is de ring Z[i] van de gehele getallen van Gausz:

$$Z[i] = \{a + bi \mid a, b \in Z\}$$

met optelling en vermenigvuldiging, zoals op blz.59 is aangegeven.

3) $H = \{(a,b,c,d) \mid a, b, c, d \in R\}$ is de verzameling van geördende 4-tallen van reële getallen.
Optelling en vermenigvuldiging in H zijn gedefinieerd door:

$$(a,b,c,d) + (a',b',c',d') = (a+a',b+b',c+c',d+d')$$

$$(a,b,c,d)\,(a',b',c',d') = (aa'-bb'-cc'-dd', ab'+ba'+cd'-dc', ac'-bd'+ca'+db', ad'+bc'-cb'+da').$$

Een eenvoudige, maar taaie berekening toont aan dat het systeem $(H,+,\circ)$ een ring is, die bekend staat als de ring van de reële quaternionen.
Het element (0,0,0,0) is nul-element, (1,0,0,0) is één-element. We introduceren nu de symbolen:

i = (0,1,0,0), j = (0,0,1,0) en k = (0,0,0,1). Dan gelden hiervoor de volgende eigenschappen:

$$i^2 = j^2 = k^2 = -1$$

$$ij = k,\quad jk = i,\quad ki = j,\quad ji = -k,\quad kj = -i,\quad ik = -j.$$

Dus de commutatieve wet voor de vermenigvuldiging geldt niet in H, zodat H geen lichaam is.
Evenals in voorbeeld 2, kan men ieder quaternion schrijven in de vorm:

$$(a,b,c,d) = (a,0,0,0) + (b,0,0,0)i + (c,0,0,0)j + (d,0,0,0)k.$$

De deelring $S = \{(r,0,0,0) \mid r \in R\}$ is isomorf met R, analoog aan de situatie in voorbeeld 2. Hierdoor kan men de notatie vereenvoudigen door (r,0,0,0) te vervangen door het element r zelf. Dan kunnen de reële quaternionen verder beschouwd worden als de verzameling

$$H = \{a + bi + cj + dk \mid a, b, c, d \in R\} \text{ met}$$

$(a+bi+cj+dk) + (a'+b'i+c'j+d'k) = (a+a') + (b+b')i + (c+c')j + (d+d')k$

en $(a+bi+cj+dk) \circ (a'+b'i+c'j+d'k) =$

$(aa'-bb'-cc'-dd') + (ab'+a'b+cd'-dc')i + (ac'-bd'+ca'+db')j +$

$+ (ad'+bc'-cb'+da')k.$

Men telt op en vermenigvuldigt als bij polynomen en gebruikt de eigenschappen van i, j en k. H is een 4-dimensionale vectorruimte over R met {1, i, j, k} als basis.
Stel nu $q = a + bi + cj + dk \neq 0$ (d.w.z. tenminste één van de elementen $a,b,c,d \neq 0$). De geconjugeerde van q wordt gedefinieerd door $\overline{q} = a - bi - cj - dk$. Dan is $q\overline{q} = \overline{q}q = a^2 - (bi+cj+dk)^2 = a^2 + b^2 + c^2 + d^2 \neq 0$, dus q heeft een inverse t.o.v. de vermenigvuldiging:

$$q^{-1} = (a^2+b^2+c^2+d^2)^{-1} \circ \overline{q}.$$

Hiermee is aangetoond dat H een delingsring is.
De elementen van H van de vorm $(a,b,0,0) = a + bi$, de z.g. speciale quaternionen, vormen een deelring van H, die isomorf is met C (voorbeeld 2).

Stelling 14.2. Een lichaam F is een integriteitsgebied.

Bewijs. Ieder lichaam is een commutatieve ring met één-element (def. 14.1), dus we moeten alleen laten zien dat F geen nuldelers heeft (zie def.10.4). Stel $a, b \in F$ en $ab = 0$. Als $a \neq 0$, dan heeft a een inverse t.o.v. de vermenigvuldiging: $a^{-1} \in F$. Dan volgt: $0 = a^{-1} \circ 0 = a^{-1}(ab) = e \circ b = b$, dus F heeft geen nuldelers.
De omkering geldt niet. Er bestaan integriteitsgebieden, die geen lichamen zijn, bijv. de ring Z van de gehele getallen.
Een integriteitsgebied met een eindig aantal elementen is echter een lichaam. We bewijzen:

Stelling 14.3. Een integriteitsgebied R met een eindig aantal idealen is een lichaam.

Bewijs. Stel $a \neq 0 \in R$. Beschouw de verzameling van hoofdidealen (a^n),

met n geheel, n > 0:

$$(a^n) = Ra^n = \{ra^n \mid r \in R\} \qquad \text{(blz.75)}.$$

Omdat R een eindig aantal verschillende idealen heeft, volgt hieruit dat $(a^m) = (a^n)$ voor zekere positieve gehele getallen m en n met $m < n$. Dus $a^m \in (a^m)$, want $a^m = ea^m$, $e \in R$, en dus $a^m \in (a^n)$. Dus bestaat er een element $r' \in R$ met $a^m = r'a^n$. R heeft geen nuldelers (def.10.4), dus R voldoet aan de vereenvoudigingswet voor de vermenigvuldiging (st.10.3):

$$a^m = r'a^n = r'a^{n-m} \circ a^m,\ a^m \neq 0 \ \text{(want } a \neq 0) \Longrightarrow e = r'a^{n-m}.$$

Dus $e = (r'a^{n-m-1}) \circ a$. R is een commutatieve ring, zodat $e = (r'a^{n-m-1}) \circ a = a \circ (r' a^{n-m-1})$ met $n \geq m + 1$, en a^{-1} bestaat in R : $a^{-1} = r' \circ a^{n-m-1}$.
Ieder element $a \neq 0$ in R heeft een mult.inverse $\Longrightarrow$ R is een lichaam.

Gevolg 14.4.
Ieder eindig integriteitsgebied is een lichaam.
Men kan ook bewijzen, dat iedere eindige delingsring een lichaam is, maar het bewijs is niet elementair en wordt achterwege gelaten.

$\overline{Z}_n$ is de ring van de gehele getallen modulo n, (n geheel, n > 0) en een commutatieve ring met één-element [1] (voorbeeld 7, pag.59). Men kan de vraag stellen: Voor welke waarden van n, als ze er zijn, is $\overline{Z}_n$ een lichaam? Hiervoor geldt de volgende stelling:

Stelling 14.5. Een element $[a] \in \overline{Z}_n$ ($[a] \neq [0]$) heeft een multiplicatieve inverse in $\overline{Z}_n$ dan en slechts dan als a en n relatief priem zijn, d.w.z. g.g.d.(a,n) = 1.

Bewijs. Als a en n relatief priem zijn, bestaan er gehele getallen r en s zodat ar + ns = 1. Hieruit volgt dat [1] = [ar + ns] = [ar] + [ns] = = [ar] + [0] = [a] [r], dus [r] is een multiplicatieve inverse van [a]. Omgekeerd, neem aan dat [a] ($\neq$[0]) een eenheid is in $\overline{Z}_n$, bijv. met inverse $[b] \in \overline{Z}_n$. Dan geldt [ab] = [a] [b] = [1], zodat $ab \equiv 1 \pmod{n}$ en er een geheel getal k bestaat met ab - 1 = kn. Maar dan is ab + n(-k) = 1, dus g.g.d. (a,n) = 1.

Gevolg 14.6. De nuldelers van $\overline{Z}_n$ zijn precies de elementen $\neq [0]$ in $\overline{Z}_n$, die geen inverse hebben.

Bewijs. Als $[a] \neq [0]$ nuldeler is en $[b]$ is een inverse van $[a]$, dan is $[a][b] = [1]$. Ook is er een element $[c] \neq [0]$ in $\overline{Z}_n$ met $[c][a] = [0]$, dus $[c][a][b] = [c] = [0]$. Tegenspraak. Dus $[a]$ heeft geen inverse. Omgekeerd, stel $[a] \neq [0]$ heeft geen inverse in $\overline{Z}_n$, dus g.g.d. $(a,n) = d$, met $1 < d < n$ (st.14.5). Dus $a = rd$ en $n = sd$ voor geschikte gehele getallen r en s. Dus $[a] \circ [s] = [as] = [rds] = [rn] = [0]$. Wegens $n = sd$, is $0 < s < n$, dus $[s] \neq [0]$. Dan is $[a]$ nuldeler in $\overline{Z}_n$.
Samenvattend hebben we het volgende resultaat:

Stelling 14.7. De ring $\overline{Z}_n$ van gehele getallen modulo n is een lichaam dan en slechts dan als n een priemgetal is. Als n een samengesteld getal is, is $\overline{Z}_n$ geen integriteitsgebied en de nuldelers van $\overline{Z}_n$ zijn die elementen $[a]$ $(\neq [0])$ waarvoor geldt g.g.d. $(a,n) \neq 1$.
Ieder lichaam heeft tenminste 2 elementen, want $e \neq 0$ (blz.55). Er is een lichaam, dat precies 2 elementen heeft volgens st.14.7, n.l. de ring $\overline{Z}_2$.
Als toepassing hiervan nemen we de volgende bewering:
Als er een homomorfie $f : Z \to F$ bestaat van de ring Z van gehele getallen op een lichaam F, dan is F noodzakelijk een eindig lichaam, waarvan het aantal elementen een priemgetal is.
Wegens $f : Z \to F$ is een surjectieve homomorfie, volgt uit de fundamentele st. voor ringhomomorfieën, dat $Z/\ker f \tilde{=} F$. Maar $\ker f = (n)$ voor een positief geheel getal n, want Z is een hoofdideaalring (st.11.7).
Merk hierbij op, dat $n \neq 0$ is, anders zou $Z \tilde{=} F$ zijn, hetgeen onmogelijk is. Nu is $Z/(n) = \overline{Z}_n$, zoals we eerder zagen, dus $\overline{Z}_n \tilde{=} F$, zodat F precies n elementen heeft. Omdat $\overline{Z}_n$ een lichaam is, moet n een priemgetal zijn (st.14.7).
We definiëren nu de z.g. ϕ-functie van Euler:

$\phi : Z \to Z$ (we noteren hier het functie-voorschrift vóór het argument) door $\phi(1) = 1$ en $\phi(n) =$ aantal elementen in de ring $\overline{Z}_n$, dat een mult. inverse heeft, ook wel invertibele elementen genoemd; (voor ieder geheel getal $n > 1$).

Bijv. $\phi(6) = 2$, $\phi(9) = 6$, $\phi(12) = 4$.
Wegens st.14.5 kan $\phi(n)$ ook gekarakterizeerd worden door de volgende eigenschap:
$\phi(n)$ is het aantal positieve getallen $< n$, dat relatief priem is met n.
Dit is ook juist voor $n = 1$.
Als p een priemgetal is, is $\phi(p) = p - 1$.

Hulpstelling 14.8. Als U_n de deelverzameling van $\overline{Z}_n$ is gedefiniëerd door

$$U_n = \{[a] \in \overline{Z}_n \mid \text{g.g.d. } (a,n) = 1\}$$

dan is U_n, met de vermenigvuldiging van $\overline{Z}_n$, een eindige groep van de orde $\phi(n)$.

Bewijs. Wegens st.14.5 bestaat U_n uit de invertibele elementen van $\overline{Z}_n$ of ook de eenheden van $\overline{Z}_n$. T.o.v. de vermenigvuldiging in $\overline{Z}_n$ vormen de eenheden een groep (blz.66). Dus U_n is een groep, waarvan de orde juist $\phi(n)$ is.

Opmerking. De groep U_n is dezelfde als die van blz.53, waar is aangetoond dat $U_n \tilde{=} \text{Aut } G$ voor $G \equiv \overline{Z}_n$.
Dit leidt tot een klassiek resultaat van Euler met betrekking tot de ϕ-functie.

Stelling 14.9. (Euler-Fermat). Als n een positief geheel getal is en a is relatief priem met n, dan geldt:

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Bewijs. De klasse $[a] \in \overline{Z}_n$ kan beschouwd worden als een element van U_n. Omdat U_n een eindige groep is met $O(U_n) = \phi(n)$ (hulpst.14.8), volgt hieruit

$$[a^{\phi(n)}] = [1] \text{ (gevolg 5.7) of } a^{\phi(n)} = [1] \text{ of } a^{\phi(n)} \equiv 1 \pmod{n}.$$

Wat betreft de idealen in een ring, hebben lichamen de eenvoudigste structuur: een lichaam F heeft alleen de triviale idealen $\{0\}$ en F. Het zijn dus enkelvoudige ringen (blz.73). We bewijzen

Stelling 14.10. Laat R een commutatieve ring zijn met één-element. Dan is R een lichaam dan en slechts dan als R geen idealen heeft anders dan {0} en R, de z.g. triviale idealen.

Bewijs. Stel R is een lichaam en I is een ideaal in R, zodat $I \neq \{0\}$ en $I \neq R$. Dan is er een element $a \neq 0$ in R zodat $a \in I$. Dus a heeft een mult. inverse a^{-1} in R. Dit is in tegenspraak met $I \cap R^* = \emptyset$ (st. 11.3). Dus $I = \{0\}$ of $I = R$. Omgekeerd, neem aan dat de ring R geen andere idealen heeft dan {0} en R. Als $a \in R$ een gegeven element is $(\neq 0)$, beschouw het hoofdideaal $(a) = Ra = \{ra \mid r \in R\}$. Dan is $(a) \neq \{0\}$, want $a = ea \in (a)$ en $a \neq 0$. Dus, uit de veronderstelling volgt, $(a) = R$. In het bijzonder geldt, omdat $e \in (a)$, dat er een element $r' \in R$ is met $r'a = e$. Ook geldt $ar' = e$, want R is commutatief. Dus r' is een mult. inverse van a. Uit def. 14.1 volgt, dat R een lichaam is.

XV. Maximale en priem-idealen.

Definitie 15.1. Een ideaal I in de ring R heet een maximaal ideaal, als $I \neq R$ en uit $I \subset J \subset R$ voor een ideaal J in R volgt $J = R$.

Stelling 15.2. I is een echt ideaal in de ring R, d.w.z. $I \neq R$. Dan is I maximaal ideaal dan en slechts dan als $(I,a) = R$ voor ieder element a in R met $a \notin I$. Hierin is (I,a) het ideaal dat wordt voortgebracht door de verzameling $I \cup \{a\}$.

Bewijs. Volgens definitie (pag.73) geldt:

$$(I,a) = \cap \{J \mid I \cup \{a\} \subseteq J;\ J \text{ is ideaal in } R\}.$$

Er geldt: $I \subset (I,a) \subseteq R$. Dus als I maximaal ideaal is, volgt uit definitie 15.1, dat $(I,a) = R$. Omgekeerd, stel dat J een ideaal is in R met de eigenschap $I \subset J \subseteq R$. Als a een element van J is, met $a \notin I$, dan geldt $I \subset (I,a) \subseteq J$. Wegens $(I,a) = R$ volgt hieruit dat $J = R$. Dus I is maximaal ideaal in R.

Voorbeelden.

1) In de ring Z van de gehele getallen corresponderen de maximale idealen met de priemgetallen.
   D.w.z.: het hoofdideaal (n), $n > 1$, is maximaal dan en slechts dan als n een priemgetal is.

   Bewijs. Stel (n) is een maximaal ideaal in Z. Als het gehele getal $n(>1)$ niet priem is, dan is $n = n_1 n_2$ met $1 < n_1 < n_2 < n$ bijv. Dit impliceert dat voor de idealen (n_1) en (n_2) geldt:

$$(n) \subset (n_1) \subset Z, \quad (n) \subset (n_2) \subset Z,$$

   hetgeen in tegenspraak is met de maximaliteit van (n). Omgekeerd, neem aan dat het gehele getal n priem is. Als het hoofdideaal (n)

niet maximaal is in Z, dan geldt òf (n) = Z òf er bestaat een echt ideaal (m) in Z met (n) $\subset$ (m) $\subset$ Z. Uit (n) = Z volgt, dat 1 een veelvoud is van het priemgetal n, hetgeen onmogelijk is. Uit (n) $\subset$ (m) volgt dat n = km voor een geheel getal k > 1; dit levert ook een tegenspraak, omdat n een priemgetal is. Dus (n) is maximaal ideaal.

2) We beschouwen de ring

$$\text{map } (R,R) = \{f \mid f : R \to R\}$$

met R = lichaam van de reële getallen.
Beschouw $I_0 = \{f \mid f \in \text{map } (R,R);\ (0)f = 0\}$. Dan is I_0 een ideaal in map (R,R) (voorbeeld 2, §11, pag.70). De bewering is, dat I_0 een maximaal ideaal is. Stel $f \notin I_0$ en $1_R : R \to R$ is de identieke afbeelding op R, d.w.z. $(x)1_R = x$ voor iedere $x \in R$. Nu is $(x)\ (1_R^2+f^2) = (x)1_R^2 + (x)f^2 = \{(x)1_R \circ (x)1_R\} + \{(x)f \circ (x)f\} =$ $= x^2 + \{(x)f\}^2$. Er geldt: $x^2 + \{(x)f\}^2 \neq 0$ voor iedere $x \in R$. Immers voor x = 0 is $(0)f \neq 0$, want $f \notin I_0$ en voor $x \neq 0$ is $x^2 \neq 0$. Dus $(x)\ (1_R^2+f^2) \neq 0$ voor iedere $x \in R$. Dan bestaat de inverse afbeelding $(1_R^2+f^2)^{-1} : R \to R$ in map (R,R), gedefinieerd door $(x)\ (1_R^2+f^2)^{-1} = x\{(x)\ (1_R^2+f^2)\}^{-1}$. Men heeft: $(x)\ (1_R^2+f^2) \circ$ $\circ\ (x)\ (1_R^2+f^2)^{-1} = x = (x)1_R$ voor iedere $x \in R$. Dus de afbeelding $1_R^2 + f^2$ is een invertibel element of een eenheid in map (R,R).
Beschouw nu het ideaal $(1_R,f)$ in map (R,R), d.w.z. het ideaal voortgebracht door 1_R en f : $(1_R,f) = \{r \circ 1_R + s \circ f \mid r, s \in \text{map } (R,R)\}$. Omdat $1_R \in I_0$ wegens $(0)1_R = 0$, volgt $(1_R,f) \subseteq (I_0,f) \subseteq \text{map } (R,R)$. Als $(1_R,f)$ een echt ideaal in map (R,R) is, dan heeft geen element van $(1_R,f)$ een inverse t.o.v. de vermenigvuldiging (st.11.3). Maar $1_R^2 + f^2 \in (1_R,f)$ en $1_R^2 + f^2$ is eenheid in map (R,R), dus $(1_R,f)$

is geen echt ideaal, zodat ook (I_0,f) = map (R,R). Wegens st.15.2 is I_0 dus maximaal ideaal.

3) R is een lichaam (def.14.1), dan zijn (0) en (1) de enige idealen in R (st.14.10). Omdat $R \neq \{0\}$, is $(0) \neq R$. Er is geen ideaal J in R met $(0) \subset J \subset R$ of uit $(0) \subset J \subseteq R$ voor een ideaal J volgt $J = (1) = R$. Dus (0) is maximaal ideaal in R.

Stelling 15.3. R is een commutatieve ring met één-element. I is een echt ideaal in de ring R. Dan is I een maximaal ideaal dan en slechts dan als de factorring R/I een lichaam is.

Bewijs. Neem aan dat I een maximaal ideaal is in R. Omdat R een commutatieve ring is met één-element e, is ook de factorring R/I een commutatieve ring met één-element e + I. Om aan te tonen dat R/I een lichaam is, is het voldoende aan te tonen dat ieder element $\neq 0$ in R/I een inverse t.o.v. de vermenigvuldiging heeft (§14). Neem aan dat $a + I \neq I$, dus $a \notin I$ (st.13.4). Omdat I maximaal ideaal is, geldt dat $R = (I,a)$ (st.15.2), dus $R = (I,a) = \{i + ra \mid i \in I, r \in R\}$. D.w.z. ieder element van R, in het bijzonder het één-element $e \in R$, kan geschreven worden als $e = i' + r'a$ voor geschikte keuze van $i' \in I$, $r' \in R$. Hieruit volgt dat $e - r'a \in I$. Dus ook $e + I = r'a + I$ (st.13.4) = $= (r'+I)(a+I)$, zodat de inverse van $a + I$ in R/I bestaat: $r' + I = (a+I)^{-1}$. Dus R/I is een lichaam. Omgekeerd, neem aan dat R/I een lichaam is en J is een ideaal in R met $I \subset J \subseteq R$. We willen aantonen dat $J = R$, want dan is I maximaal in R (def.15.1). Omdat $I \subset J$, bestaat er een element $a \in J$ met $a \notin I$. Dus, de restklasse $a + I \neq I$, I het nul-element in R/I. Omdat R/I een lichaam is, moet $a + I$ een inverse hebben t.o.v. de vermenigvuldiging : $(a+I)(b+I) = ab + I = e + I$ voor een restklasse $b + I \in R/I$. Dan volgt $e - ab \in I \subset J$. Maar ook $ab \in J$, want J is ideaal in R en $a \in J$. Dus $e = (e-ab) + ab \in J$. Maar dan is $J = R$ (gevolg 11.4), zodat I maximaal is.

Voorbeeld. Z[i] is de ring van de gehele getallen van Gauss. $I = \{a + bi \mid a \equiv 0(2) \text{ en } b \equiv 0(2)\}$. Dan is I ideaal in Z[i] (voorbeeld 3, p.71). Ook geldt $Z[i] / I \tilde{=} \overline{Z}_2$, waarin $\overline{Z}_2$ het lichaam van de restklassen modulo 2 is (voorbeeld, §13). Dus I is maximaal ideaal in Z[i].

De aanname dat R een één-element heeft is essentieel in st.15.3. Beschouw daartoe de ring Z_2 van even gehele getallen, een commutatieve ring zonder één-element. In deze ring is het hoofdideaal (4), voortgebracht door het gehele getal 4, een maximaal ideaal. Hierin is

$$(4) = \{4(2j) + 4k \mid j, k \in Z\} = 4Z \quad \text{(zie p.75)}.$$

Stel n.l. dat n een element is van Z_2 en $n \notin (4)$. Dan is n een even geheel getal, dat niet door 4 deelbaar is. Dus n kan geschreven worden in de vorm $n = 4m + 2$, m geheel. Hieruit volgt: $2 = 4(-m) + n \in ((4),n)$ in Z_2, want $(4) = 4Z$. Nu is $Z_2 = (2) = ((4),n)$, dus volgens st.15.2 is (4) een maximaal ideaal in Z_2.

In de factorring $Z_2 / (4)$ geldt:

$$(2+(4))(2+(4)) = 4 + (4) = (4).$$

Dus de ring $Z_2 / (4)$ bezit nuldelers en kan geen lichaam zijn, want een lichaam is een integriteitsgebied (st.14.2).
Ook de aanname, dat R commutatief is, kan niet gemist worden in st.15.3. De matrix-ring $M_n(R)$ (n geheel, $n \geq 2$) is een enkelvoduige ring (p.73), d.w.z. $M_n(R)$ heeft geen idealen anders dan (0) en $M_n(R)$. Dus (0) is maximaal ideaal in $M_n(R)$, maar $M_n(R) / (0) \cong M_n(R)$ is geen lichaam, omdat $M_n(R)$, zoals bekend, nuldelers heeft.

We zullen nu de z.g. priemidealen beschouwen.

Definitie 15.4. Een ideaal I in de ring R, R een commutatieve ring met één-element, is een priemideaal als, voor $a, b \in R$,

$$ab \in I \Longrightarrow a \in I \text{ of } b \in I.$$

Het klassieke voorbeeld van een priemideaal in de ring Z is het hoofdideaal (p), waarbij p een priemgetal is.

Stelling 15.5. Een commutatieve ring R met één-element is een integriteitsgebied dan en slechts dan als het nul-ideaal (0) een priemideaal is.

Bewijs. R is een integriteitsgebied dan en slechts dan als R geen nuldelers bezit. Als (0) priemideaal is, volgt uit ab = 0 dat a = 0 of b= 0(a,b∈R), dus R heeft geen nuldelers. Omgekeerd is het duidelijk dat R heeft geen nuldelers impliceert dat (0) priemideaal is in R.
In het geval R = Z, de ring van de gehele getallen, kunnen we alle priem-idealen expliciet bepalen. De priemidealen zijn (p), p priem, (0) en Z. Z is priemideaal in Z (triviaal) en (0) is priemideaal in Z wegens st.15.5. Als p een priemgetal is, dan volgt uit ab $\in$ (p), dus p deler van ab, dat p deler is van a of p deler van b, dus a $\in$ (p) of b $\in$ (p). Dus (p) is priemideaal.
Omgekeerd, stel n($\neq$0,1) is een samengesteld getal, d.w.z. $n = n_1 n_2$, met $1 < n_1 n_2 < n$. Dan geldt $n_1 n_2 = n \in (n)$. Maar noch n_1 noch n_2 is een geheel veelvoud van n, dus $n_1 \notin (n)$ en $n_2 \notin (n)$. Hieruit volgt, dat (n) geen priemideaal is.
Men kan opmerken, dat (0) een priemideaal is in Z, maar geen maximaal ideaal. Voor een voorbeeld van een ring, die een niet-triviaal priemideaal bevat dat niet maximaal is, nemen we R = Z × Z, met de operaties componentsgewijs (zie voorbeeld 3, p.65). Dan geldt dat de verzameling Z × {0} = {(n,0) | n $\in$ Z} een ideaal is in R.
Immers Z × {0} is een deelring van R (p.65) en als (a,b) $\in$ R, dan is (a,b) (n,0) = (n,0) (a,b) = (na,0) $\in$ Z × {0} voor iedere (n,0) $\in$ Z × {0}. Ook is Z × {0} priemideaal in R. Uit (a,b) (c,d) $\in$ Z × {0} volgt (ac,bd) $\in$ Z × {0}, dus bd = 0, zodat b = 0 of d = 0, dus (a,b) $\in$ Z × {0} of (c,d) $\in$ Z × {0}.
Z × {0} is echter niet maximaal in R, want

$$Z \times \{0\} \subset Z \times Z_2 \subset R,$$

waarin $Z \times Z_2 = \{(a,b) \mid a \in Z, b \in Z_2\}$ een ideaal is in R.
In analogie met st.15.3 kunnen priemidealen gekarakteriseerd worden door:

Stelling 15.6. R is een commutatieve ring met één-element. Dan is I een priemideaal dan en slechts dan als de factorring R/I een integriteitsgebied is.

Bewijs. Neem aan dat I priemideaal is in R.
Omdat R een commutatieve ring is met één-element e, is ook de factorring R/I een commutatieve ring met één-element e + I. Om aan te tonen dat R/I een integriteitsgebied is, moet men alleen laten zien, dat R/I geen nuldelers heeft. Stel dus dat (a+I) (b+I) = I, (I is het nulelement in R/I). Dit is equivalent met ab + I = I of ab $\in$ I (st.13.4). Omdat I priemideaal is, moet tenminste één van de factoren a of b in I liggen. Dit betekent dat of a + I = I of b + I = I, dus R/I heeft geen nuldelers.
Neem nu aan dat R/I een integriteitsgebied is en ab $\in$ I. Dit betekent, dat (a+I) (b+I) = ab + I = I. Volgens de veronderstelling volgt hieruit dat a + I = I of b + I = I (R/I heeft geen nuldelers). Dus of a $\in$ I of b $\in$ I, zodat I een priemideaal is in R.

Stelling 15.7. In een commutatieve ring R met één-element is ieder maximaal ideaal een priemideaal.

Bewijs. Stel I is een maximaal ideaal in R, dan is R/I een lichaam (st.15.3.). Dus R/I is een integriteitsgebied (st.14.2). Dus I is een priemideaal (st.15.6).

Opmerking. Als de ring R geen één-element heeft is de stelling niet juist. Een voorbeeld is de ring Z_2 van even getallen, waarin (4) een maximaal ideaal is, maar geen priemideaal. Immers 2.2 $\in$ (4), terwijl 2 $\notin$ (4).
Ofschoon priemidealen en maximale idealen in een ring R in het algemeen niet samenvallen, is een klasse van ringen aan te geven, waarvoor ieder niet-triviaal priem-ideaal een maximaal ideaal is.

Stelling 15.8. R is een integriteitsgebied, waarin ieder ideaal hoofdideaal is, een z.g. hoofdideaalring. Een niet-triviaal ideaal (a) in R is priemideaal dan en slechts dan als het een maximaal ideaal is.

Bewijs. In R zijn (0) en R priemidealen; met niet-triviaal ideaal (a) wordt een ideaal $\neq$ 0 en $\neq$ R bedoeld. Omdat een macimaal ideaal priemideaal is (st.15.7), behoeven we alleen te bewijzen dat uit (a) is priemideaal volgt (a) is maximaal ideaal. Stel I is een ideaal in R

met $(a) \subset I \subseteq R$. Omdat R een hoofdideaalring is, bestaat er een element $b \in R$ met $I = (b)$. Uit $a \in (a) \subset (b)$ volgt $a = rb$ voor zeker element $r \in R$. Wegens (a) is priemideaal volgt uit $rb \in (a)$ dat $r \in (a)$ of $b \in (a)$. Uit $b \in (a)$ volgt $(b) \subseteq (a)$, hetgeen onmogelijk is. Dus $r \in (a)$, zodat $r = sa$ voor zeker element $s \in R$. Dus $a = rb = (sa)b$ of $(sb-e)a = 0$, e is één-element van R. Nu is $a \neq 0$, want (a) is niet-triviaal, en R heeft geen nuldelers, want R is integriteitsgebied, dus $e = sb$. Dit betekent dat $e \in (b) = I$, zodat $I = R$ (gevolg 11.4). Hieruit volgt dat (a) een maximaal ideaal is en stelling 15.8 is bewezen. Een voorbeeld van een ring R, die aan de voorwaarden van st.15.8 voldoet is de ring Z van de gehele getallen. In Z vallen dus samen:

a) priemidealen (p), met $p \neq 0$, $p \neq 1$, p priem;

b) maximale idealen.

XVI. Veeltermringen.

R is een ring in Z_+ is de verzameling van niet-negatieve gehele getallen. Een oneindige rij van elementen van R is een afbeelding $f : Z_+ \to R$. Als $r_j = f(j)$, $j = 0,1,2,\ldots$, noteren we f door middel van $(r_0,r_1, \ldots, r_n, \ldots)$ en we noemen r_j de j^e term van de rij.

Definitie 16.1. R is een ring. Een oneindige rij $(a_0,a_1,a_2, \ldots,a_n, \ldots)$ van elementen van R, met ten hoogste een eindig aantal termen $\neq 0$, heet een veelterm over R.
Bijv., als R = Z, dan zijn $(1,0,2,1,0, \ldots,0, \ldots)$ en $(0,0,1,0,0, \ldots,0,\ldots)$ veeltermen over R, maar $(0,1,0,1, \ldots,0,1, \ldots)$ is geen veelterm over R.
Een onmiddellijk gevolg van definitie 1.1 is, dat er voor iedere veelterm f een geheel getal d bestaat, dat van f afhangt, zodat $a_n = 0$ voor alle $n > d$. Als $a_d \neq 0$, maar $a_n = 0$ voor alle $n > d$, dan heet d de graad van de veelterm f. In het bijzonder is de graad van de nul-veelterm $(0,0, \ldots)$ niet gedefinieerd. De nul-veelterm en de veeltermen van de graad 0 worden constanten genoemd, veeltermen van de graad 1 heten lineair, veeltermen van de graad 2 kwadratisch, enz.
Omdat een veelterm een rij is (d.w.z. een afbeelding), is $(a_0,a_1,\ldots,a_n,\ldots) = (b_0,b_1,\ldots,b_n,\ldots)$ dan en slechts dan als $a_i = b_i$, $i = 0, 1, 2, \ldots$
We zullen nu een optelling en vermenigvuldiging van veeltermen definiëren.

Definitie 16.2.

Optelling:
$$(a_0,a_1,\ldots,a_n,\ldots) + (b_0,b_1,\ldots,b_n,\ldots) = (a_0+b_0,a_1+b_1,\ldots a_n+b_n,\ldots)$$

Vermenigvuldiging:
$(a_0,a_1,\ldots,a_n,\ldots)\ (b_0,b_1,\ldots,b_n,\ldots) = (c_0,c_1,\ldots,c_n,\ldots)$ waarin
$$c_r = a_0b_r + a_1b_{r-1} + a_2b_{r-2} + \ldots + a_{r-1}b_1 + a_rb_0 = \sum_{i=0}^{r} a_ib_{r-i} .$$

In het bijzonder geldt:

$c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0$. We merken op dat $\sum_{i=0}^{r} a_ib_{r-i} = \sum_{\substack{i+j=r \\ i\geq 0, j\geq 0}} a_ib_j$, hetgeen we zullen schrijven als $\sum_{i+j=r} a_ib_j$.

De algemene term c_r is dus gegeven door $c_r = \sum_{i+j=r} a_ib_j$, waarbij gesommeerd wordt over alle paren i en j met $0 \leq i \leq r$, $0 \leq j \leq r$ en zodat $i + j = r$.

Stelling 16.3. De verzameling van veeltermen f, met de boven gedefinieerde optelling en vermenigvuldiging, is een ring, de veeltermring over R.

Bewijs. We tonen eerst aan dat optelling en vermenigvuldiging binaire operaties zijn op de niet-lege verzameling van veeltermen f. Stel $f = (a_0,a_1,\ldots)$ en $g = (b_0,b_1,\ldots)$. Laat de graad van f = p en de graad van g = q zijn. Dan geldt voor $n > \max(p,q)$ dat $a_n + b_n = 0 + 0 = 0$. Dus $f + g = (a_0+b_0,a_1+b_1,\ldots)$ is een veelterm over R. Stel nu $fg = (c_0,c_1,\ldots)$. Beschouw de n^e term $c_n = \sum_{i+j=n} a_ib_j$ voor $n > p + q$.

Als j groter is dan q, dan is $b_j = 0$, terwijl als i groter is dan p, $a_i = 0$ is. Om dus een term $\neq 0$ in $\sum_{i+j=n} a_ib_j$ te krijgen, moet $i \leq p$ en $j \leq q$ zijn. Maar dan is $i + j \leq p + q < n$, dus $i + j \neq n$. Hieruit volgt $c_n = 0$ voor $n > p + q$. Dus ook $fg = (c_0,c_1,\ldots)$ is een veelterm over R. T.o.v. de optelling vormen de veeltermen een commutatieve groep. Uit de definitie van de optelling volgt direct dat als $\hat{0}$ de nulveelterm is,

$$f + \hat{0} = \hat{0} + f = f \text{ voor iedere veelterm } f.$$

De inverse van $f = (a_0,a_1,a_2,\ldots)$ is $-f = (-a_0,-a_1,-a_2,\ldots)$ en -f is een veelterm, want $a_n = 0$ dan en slechts dan als $-a_n = 0$ in R. De associativiteit van de optelling volgt uit de associativiteit van de optelling in R.

Nu tonen we aan dat de vermenigvuldiging van veeltermen associatief is. Stel $f = (a_0,a_1,\ldots)$, $g = (b_0,b_1,\ldots)$ en $h = (c_0,c_1,\ldots)$ zijn veeltermen .

We moeten aantonen dat $f(gh) = (fg)h$. We berekenen de r^e term van beide producten. Laat de p^e term van (gh)zijn $d_p = \sum_{p+j=p} b_i c_j$. Dan is de r^e term van $f(gh)$: $\sum_{p+q=r} a_q d_p = \sum_{p+q=r} a_q \left(\sum_{i+j=p} b_i c_j \right) = \sum_{i+j+q=r} a_q (b_i c_j)$, waarbij in de laatste som gesommeerd wordt over alle tripels gehele getallen i, j en q met $0 \leq i, j, q \leq r$ en zodat $i + j + q = r$. Op een geheel analoge manier vindt men dat de r^e term van $(fg)h$ gelijk is aan

$$\sum_{j+t=r} \left(\sum_{i+q=t} a_q b_i \right) c_j = \sum_{q+i+j=r} (a_q b_i) c_j .$$

Omdat de vermenigvuldiging in R associatief is, geldt $a_q(b_i c_j) = (a_q b_i)c_j$, dus de r^e termen in beide producten stemmen overeen. Dan is $f(gh) = (fg)h$.
Tenslotte tonen we de distributieve wetten aan. De r^e term van $f(g+h)$ is $\sum_{i+j=r} a_i(b_j+c_j)$, terwijl de r^e term van $fg + fh$ is $\sum_{i+j=r} a_i b_j + \sum_{i+j=r} a_i c_j$.
Dus $f(g+h) = fg + fh$ wegens $a_i(b_j+c_j) = a_i b_j + a_i c_j$ in R. Evenzo volgt $(f+g)h = fh + gh$.
Volgens def.9.1 is de verzameling van veeltermen f een ring.

Notatie. De veeltermring over R geven we aan met R[x].

Stelling 16.4. R is een ring. Dan kan R ingebed worden in R[x].

Bewijs. Definieer een afbeelding $\phi : R \to R[x]$ door middel van $\phi(r) = (r,0,0,\ldots,0,\ldots)$ voor iedere $r \in R$. Dan is $\phi(r+s) = (r+s,0,0,\ldots,0,\ldots) = (r,0,\ldots,0,\ldots) + (s,0,\ldots,0,\ldots) = \phi(r) + \phi(s)$ en
$\phi(rs) = (rs,0,0,\ldots,0,\ldots) = (r,0,\ldots,0,\ldots)\,(s,0,\ldots,0,\ldots) = \phi(r)\phi(s)$.
Dus ϕ is een homomorfie van R in R[x]. Als $\phi(r) = (r,0,\ldots,0,\ldots) = (0,0,\ldots,0,\ldots)$, dan is $r = 0$, dus kern $\phi = (0)$. Dus ϕ is een isomorfie - in (st.127), of R kan ingebed worden in R[x].
De constante veeltermen vormen een deelring R' van R[x], die isomorf is met de ring R onder de afbeelding $\phi^{-1} : (r,0,\ldots,0,\ldots) \to r$. We zullen R met deze deelring R' van R[x] identificeren. Met het identificeren wordt bedoeld, dat de elementen van R' (in R[x]) de namen van de elementen van R krijgen, zoals bepaald wordt door de isomorfie ϕ^{-1}. Optelling en vermenigvuldiging van elementen van R met elementen van R[x] komen overeen

met de bewerkingen op de corresponderende elementen van R' en de elementen van R[x].

Bijv. $f = (a_0,a_1,\ldots,a_n,\ldots) \in R[x]$, $r \in R$. Met het element $r \in R$ correspondeert $\phi(r) = (r,0,\ldots,0,\ldots) \in R'$ en $rf = r(a_0,a_1,\ldots,a_n,\ldots) = (r,0,\ldots,0,\ldots)(a_0,a_1,\ldots a_n,\ldots) = (ra_0,ra_1,\ldots,ra_n,\ldots)$. Ook $r + f = (r,0,\ldots,0) + (a_0,a_1,\ldots,a_n,\ldots) = (r+a_0,a_1,\ldots,a_n,\ldots)$.
We mogen nu R als deelring van R[x] beschouwen.

Stelling 16.5. De veeltermring R[x] is een integriteitsgebied dan en slechts dan als R een integriteitsgebied is.

Bewijs. Als R[x] integriteitsgebied is, dan geldt dit ook voor R, want R is een deelring van R[x] en het is duidelijk dat het eenheidselement in R[x] van de vorm $(a,0,\ldots,0,\ldots)$ is en dus a het eenheidselement in R is. Wegens het identificeren vallen eenheidselement van R[x] en eenheidselement van R dus samen.
Omgekeerd, stel dat R een integriteitsgebied is. Omdat $r \in R$, is het duidelijk dat $(e,0,\ldots,0,\ldots)$ het eenheidselement voor de veeltermring R[x] is. De commutativiteit van de vermenigvuldiging in R[x] volgt direct uit die van R, want $\sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i = \sum_{j+i=k} b_j a_i =$

$= \sum_{i+j=k} b_i a_j$ voor a_i, b_i, a_j, $b_j \in R$. Dus

$(a_0,a_1,\ldots,a_n,\ldots)(b_0,b_1,\ldots,b_n,\ldots) = (b_0,b_1,\ldots,b_n)(a_0,a_1,\ldots,a_n,\ldots)$.
Stel $f \neq 0$, $g \neq 0$ in R[x]. Laat de graad van $f = n_1$ en de graad van $g = n_2$ zijn. Als $f = (a_0,a_1,\ldots)$ en $g = (b_0,b_1,\ldots)$, dan is $a_{n_1} \neq 0, b_{n_2} \neq 0$, maar $a_k = 0$ voor $k > n_1$ en $b_k = 0$ voor $k > n_2$.
Dan geldt in f.g dat de $(n_1+n_2)^e$ term wordt gegeven door

$\sum_{i+j=n_1+n_2} a_i b_j = a_{n_1} b_{n_2} \neq 0$, want R is integriteitsgebied. Dus R[x] heeft geen nuldelers. Dan is R[x] integriteitsgebied (def.10.4).
Met betrekking tot de graad van de veeltermen $f \neq 0$ in R[x] geldt de volgende stelling, waarvan het bewijs uit dat van stelling 16.3 en stelling 16.5 volgt.

Stelling 16.6.

a) Als $f \neq 0$, $g \neq 0 \in R[x]$, dan is voor $f+g \neq 0$:
graad $(f+g) \leq \max(\text{graad } f, \text{graad } g)$.
(Gelijkheid geldt als graad $f \neq$ graad g is).

b) Als $f \neq 0$, $g \neq 0 \in R[x]$, dan is voor $fg \neq 0$:
graad $(fg) \leq$ graad f + graad g.
Als R een integriteitsgebied is, geldt b) met gelijkteken.

Gevolg 16.7. R is een integriteitsgebied. Dan zijn de eenheden in R[x] de constante veeltermen $(a,0,0,\ldots)$ met a eenheid in R.

Bewijs. Zoals we gezien hebben is $(e,0,0,\ldots)$ het eenheidselement in R[x] met $e(\in R)$ eenheidselement in R. Als $f.g = (e,0,0,\ldots)$ voor $f, g \in R[x]$, dan is graad f + graad $g = 0$ (st.16.6(b)), dus graad $f =$ = graad $g = 0$ en f en g zijn constante veeltermen: $f = (a,0,0,\ldots)$ en $g = (b,0,0,\ldots)$ met $ab = 1$. Dus a is eenheid in R(zie blz.66). Omgekeerd volgt direct dat als a een eenheid is in R, $(a,0,\ldots)$ een eenheid is in R[x]. De eenheden van R en die van R[x] kan men weer identificeren, zodat beide samenvallen.

We zullen nu een notatie invoeren, die ons in staat stelt veeltermen in hun gewone vorm te zien.
Definieer x als de veelterm $(0,e,0,\ldots,0,\ldots)$, waarin $e \in R$ het eenheidselement in R is.

Stelling 16.8. Voor ieder geheel getal $n \geq 0$ geldt:
$x^2 = (0,0,\ldots,0,e,0,\ldots)$, waarin e als n^e term voorkomt en de overige termen = 0 zijn.
Iedere veelterm $(b_0,b_1,\ldots,b_k,0,0,\ldots)$ kan geschreven worden in de vorm: $b_0 + b_1x + b_2x^2 + \ldots + b_kx^k$.

Bewijs. Voor $n = 0$ geldt $x^0 = (e,0,0,\ldots)$, het eenheidselement in R[x]. $x^1 = x = (0,e,0,\ldots,0)$, dus de stelling is juist voor $n = 0$ en $n = 1$. Stel nu dat $x^n = (0,0,\ldots,0,e,0,\ldots)$, waarin e als n^e term voorkomt. Dan is $x^{n+1} = x^n . x = (0,0,\ldots,0,e,0,\ldots)\ (0,e,0,\ldots) =$ $= (0,\ldots,0,0,e,0,\ldots)$, waarin e nu de $n+1^e$ term is. Dus volgens inductie is het eerste deel van de stelling juist.

$(b_0,b_1,\ldots,b_k,0,0,\ldots) = (b_0,0,\ldots,0,\ldots) + (0,b_1,0,\ldots) + \ldots +$
$+ (0,0,\ldots,0,b_k,0,\ldots,0,\ldots)$ en voor iedere b_i geldt:
$(0,0,\ldots,0,b_i,0,\ldots) = b_i(0,\ldots,0,e,0,\ldots) = b_i x^i (i=0,1,\ldots,k)$.
Dus $(b_0,b_1,\ldots,b_k,0,0,\ldots) = b_0x^0+b_1x+\ldots+b_kx^k = b_0 + b_1x + \ldots + b_kx^k$.
Hiermee is de stelling bewezen.

Opmerking. In de bovengenoemde definitie van x is vooropgesteld dat R een eenheidselement bezit. Als R een willekeurige ring is, niet noodzakelijk met eenheidselement, kan men R inbedden in een ring R^* met eenheidselement. Hierbij is $R^* = \{(r,n) \mid r \in R, n \in Z\}$. Optelling en vermenigvuldiging in R^* zijn gedefinieerd door

$$(a,n) + (b,m) = (a+b,n+m),$$

$$(a,n)(b,m) = (ab+ma+nb,nm).$$

De additieve groep van R^* is het direkte product van R en Z (blz.7), (0,1) is het eenheidselement van R^*. Als we (r,0) met r idenrificeren, kan R beschouwd worden als een deelring van R^*. Het gevolg is dat men de veeltermring R[x], zoals gedefinieerd is in definities 16.1 en 16.2, kan inbedden in de ring $R^*[x]$. Dan is R[x] een deelring van $R^*[x]$ en ieder element van R[x] heeft de vorm

$$a_0 + a_1x + \ldots + a_nx^n,\ a_i \in R. \text{ (stelling 16.8)},$$

ondanks het feit dat x geen element van R[x] hoeft te zijn.
Er geldt: $x \in R[x]$ dan en slechts dan als R een eenheidselement heeft.

Voorbeeld.
We beschouwen de ring Z[x], Z de ring van de gehele getallen.
In deze ring vormen de veeltermen, deelbaar door x, een ideaal: het hoofdideaal (x).
Stel $f(x), g(x) \in Z[x]$ en $f(x)\,g(x) \in (x)$. Dan is $x \mid f(x)g(x)$, dus $x \mid f(x)$ of $x \mid g(x)$ zodat $f(x) \in (x)$ of $g(x) \in (x)$. Hieruit volgt dat (x) een priemideaal is (def.15.4). Een andere manier om dit in te zien is via de afbeelding $\phi : Z[x] \to Z$, die gedefinieerd is door $\phi(f(x)) = f(0)$ voor iedere $f(x) \in Z[x]$. Men toont gemakkelijk aan dat ϕ een

homomorfie en surjectief is. Dus $\frac{Z[x]}{\text{kern } \phi} \tilde{=} Z$ (fundam.homomorfie-st.).
Hierin is kern $\phi = \{f(x) \mid f(0) = 0\}$, d.w.z. de veeltermen in Z[x] met constante = 0 of kern $\phi = (x)$, dus $\frac{Z[x]}{(x)} \tilde{=} Z$. Z is integriteitsgebied, dus $\frac{Z[x]}{(x)}$ is integriteitsgebied. Dan volgt dat (x) priemideaal is (st.15.6).
Beschouw nu 't ideaal $(x,2) = \{xf(x) + 2g(x) \mid f(x), g(x) \in Z[x]\}$.
Iedere veelterm uit (x,2) heeft <u>even</u> constante term en omgekeerd behoort iedere veelterm met even constante tot (x,2). Het is duidelijk dat $(x) \subseteq (x,2)$, maar $2 \notin (x)$ en $2 \in (x,2)$, dus $(x) \subset (x,2)$.
We tonen aan dat (x,2) een maximaal ideaal is.
Men heeft $(x,2) \neq Z[x]$, want $1 \notin (x,2)$. De afbeelding $\overline{\phi} : Z[x] \to \overline{Z}_2$ met $f(x) \mapsto \overline{f(0)}$ is een surjectieve homomorfie van Z[x] op de ring van restklassen mod.2. $\overline{\phi}$ voegt aan een veelterm $f(x) \in Z[x]$ toe: $\overline{0}$ resp. $\overline{1}$, voor: f(x) heeft <u>even</u> constante resp. <u>oneven</u> constante. Kern $\overline{\phi} = (x,2)$, dus $\frac{Z[x]}{(x,2)} \tilde{=} \overline{Z}_2$ (st.13.10). Nu is $\overline{Z}_2$ een lichaam (st.14.7), dus (x,2) is maximaal ideaal in Z[x] (st.15.3).
Omdat in Z[x] het priemideaal (x) niet maximaal is, is Z[x] geen hoofdideaalring op grond van stelling 15.8.
Men kan bewijzen:
F is een lichaam. Dan is F[x] een hoofdideaalring.
We gaan hier niet verder op in.