TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

VERZAMELINGSLEER

met opgaven

Prof. Dr. J.J. Seidel

Drs. C.P. van Nieuwkasteele

Voorjaarssemester 1973

Technische Hogeschool
Eindhoven

Dictaatnummer 2.219.1
Prijs f.5,50

Onderafdeling der Wiskunde
en Informatica

Verzamelingsleer

met opgaven

Voorjaarssemester 1973

Prof.dr. J.J. Seidel
Drs. C.P. van Nieuwkasteele

Verzamelingsleer

voorjaarssemester 1979

Literatuur:

[1] S.T.M. Ackermans - J.H. van Lint, Algebra en Analyse, Wolters-Noordhoff (1970).

[2] H. Freudenthal, Exacte logica, Erven F. Bohn (1961).

[3] P.R. Halmos, Intuitieve verzamelingenleer, Aula (1968), Naïve set theory, van Nostrand (1964).

Inhoudsopgave blz.

Hoofdstuk I. Logica

1.1. Beweringen

Wij beschouwen allerlei beweringen (proposities), die waar of onwaar zijn. Tertium non datur.

Voorbeeld 1. Eindhoven ligt in België; is onwaar.

Voorbeeld 2. $2 \times 2 = 4$; is waar.

Voorbeeld 3. $3 \times 6 < 7$; is onwaar.

Uit beweringen p en q kunnen nieuwe beweringen worden gevormd met behulp van bewerkingen.

Negatie. Is p een bewering, dan is $\neg p$ (spreek uit niet-p) de negatie van p; de bewering $\neg p$ is waar als p onwaar is, en is onwaar als p waar is.

Voorbeeld 4. $\neg (2 + 2 = 4)$ is hetzelfde als $(2 + 2 \neq 4)$, en is onwaar.

Conjunctie. De bewering $p \wedge q$ (spreek uit p en q) is slechts waar als p en q beide waar zijn.

Voorbeeld 5. $(2 + 2 = 4) \wedge (3 \times 6 < 7)$ is onwaar.

Voorbeeld 6. $(2 + 2 = 4) \wedge$ (Eindhoven ligt in Brabant) is waar.

Voorbeeld 7. Een serieschakeling van twee schakelaars p en q sluit, als zowel p als q sluiten (dus als $p \wedge q$ sluit).

Disjunctie. De bewering $p \vee q$ (spreek uit p of q) is slechts waar als p en q niet beide onwaar zijn, dus als

$$\neg ((\neg p) \wedge (\neg q))$$

waar is. Met andere woorden, $p \vee q$ is waar als p of q waar is (waarin "of" niet in uitsluitende zin is bedoeld).

Voorbeeld 8. $(2 + 2 = 4) \vee (3 \times 6 < 7)$ is waar.

Voorbeeld 9. $(2 + 2 = 4) \vee (3 \times 6 > 7)$ is waar.

Voorbeeld 10. $(2 + 2 = 5) \vee (3 \times 6 < 7)$ is onwaar.

Voorbeeld 11. Een parallelschakeling van twee schakelaars p en q sluit, als p sluit, als q sluit, als p en q sluiten (dus als $p \vee q$ sluit).

Implicatie. De bewering $p \Rightarrow q$ is slechts onwaar als p waar en q onwaar is, dus is waar als

$$(\neg p) \vee q$$

waar is.

Voorbeeld 12. $(2 + 2 = 4) \Rightarrow$ (elk paard heeft 7 poten) is onwaar.

Voorbeeld 13. $(2 + 2 = 5) \Rightarrow$ (elk paard heeft 7 poten) is waar.

Voorbeeld 14. $(2 + 2 = 5) \Rightarrow$ (elk paard heeft 4 poten) is waar.

Voorbeeld 15. $(2 + 2 = 4) \Rightarrow$ (elk paard heeft 4 poten) is waar.

Gelijkwaardigheid. De bewering $p \Leftrightarrow q$ is slechts waar als p en q beide waar, en als p en q beide onwaar zijn.

Voorbeeld 16. $(2 + 2 = 4) \Leftrightarrow$ (Eindhoven ligt in Brabant) is waar.

Voorbeeld 17. $(2 + 2 = 5) \Leftrightarrow$ (elk paard heeft 7 poten) is waar.

Voorbeeld 18. $(2 + 2 = 4) \Leftrightarrow (3 \times 6 < 7)$ is onwaar.

De hierboven gegeven definities laten zich overzichtelijk samenvatten met behulp van waarheidstafels (1 betekent waar, 0 betekent onwaar):

p	$\neg p$
1	0
0	1

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Waarheidstafels kunnen worden gebruikt om te bewijzen dat bepaalde beweringen waar zijn in alle gevallen. Men spreekt dan van een tautologie.

Voorbeeld 19. $p \vee (\neg p)$ is waar in alle gevallen, want

p	$\neg p$	$p \vee (\neg p)$
1	0	1
0	1	1

Voorbeeld 20. $(p \wedge (p \Rightarrow q)) \Rightarrow q$ is waar in alle gevallen, want

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

Voorbeeld 21. $((p \wedge q) \vee r) \Leftrightarrow ((p \vee r) \wedge (q \vee r))$ is waar in alle gevallen, want

p	q	r	$p \wedge q$	L	$p \vee r$	$q \vee r$	R	$L \Leftrightarrow R$
1	1	1	1	1	1	1	1	1
0	1	1	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	1	0	1	1	1	1	1	1
1	0	0	0	0	1	0	0	1
0	1	0	0	0	0	1	0	1
0	0	1	0	1	1	1	1	1
0	0	0	0	0	0	0	0	1

1.2. Predicaten

Voor de variabele x substitueren wij dingen uit een bepaalde totaliteit U. Een predicaat P(x) is een uitdrukking in x, waaruit een bewering ontstaat wanneer voor x wordt gesubstitueerd een ding uit U.

Voorbeeld 1.

U	P(x)	onwaar voor:	waar voor:
reële getallen	x is positief	$x = -3$	$x = 7$
reële getallen	$(x + 1)(x - 2) = 0$	$x = 3$	$x = 2$
T.H. gemeenschap	x is rector	x = Jansen	x = Van der Leeden
Nederlanders	x woont in Eindhoven	x = Juliana	x = Van der Lee
Metalen	x is rood	x = ijzer	x = koper
natuurlijke getallen	x is priem	$x = 6$	$x = 7$
reële getallen	$(x + 2)^2 = x^2 + 4x + 4$	geen enkele x	elke x
reële getallen	$(x + 2)^2 = x^2 + 4x + 5$	elke x	geen enkele x.

Uit de predicaten P(x) en Q(x), met x uit dezelfde totaliteit U, worden de volgende predicaten gevormd:

$$\neg P(x),\ P(x) \wedge Q(x),\ P(x) \vee Q(x),\ P(x) \Rightarrow Q(x),\ P(x) \Leftrightarrow Q(x)\ .$$

Voorbeeld 2. $\neg (x > 0)$ is slechts waar voor $x \leq 0$.

Voorbeeld 3. $(x > 0) \wedge (x < 2)$ is slechts waar voor $0 < x < 2$.

Voorbeeld 4. $(x > 0) \vee (x = 0)$ is slechts waar voor $x \geq 0$.

Voorbeeld 5. $(x > 0) \vee (-3 < x < 3)$ is slechts waar voor $x > -3$.

Voorbeeld 6. $(x \geq 0) \Rightarrow (x = 3)$ is waar voor $x = 3$, is onwaar voor $x = 2$, is waar voor elke negatieve x.

In bovenstaande voorbeelden was U de totaliteit der reële getallen. Laat nu U zijn de totaliteit der mensen.

Voorbeeld 7. (x is bakker) $\Rightarrow$ (x is vrouw) is waar als voor x een vrouwelijke bakker wordt gesubstitueerd, maar is ook waar als voor x een niet-bakker wordt gesubstitueerd.

Voorbeeld 8. (x is bakker met 5 armen) $\Rightarrow$ (x is hoogleraar) is altijd waar.

Opmerking. Wij herhalen dat, als voor x wordt gesubstitueerd een a uit de totaliteit U, de bewering P(a) $\Rightarrow$ Q(a) altijd waar is behalve als P(a) waar is en Q(a) niet waar is.

1.3. Quantoren

$\forall_{x\in U}(P(x))$ is de bewering: P(x) is waar voor alle x uit de totaliteit U. Deze bewering is waar of niet.

$\exists_{x\in U}(P(x))$ is de bewering: er is een x uit de totaliteit U waarvoor P(x) waar is. Deze bewering is waar of niet.

$\exists!_{x\in U}(P(x))$ is de bewering: er is één x uit de totaliteit U waarvoor P(x) waar is. Deze bewering is waar of niet.

In de volgende voorbeelden is U de totaliteit der reële getallen.

Voorbeeld 1. $\forall_{x\in\mathbb{R}}(x^2 - 1 = (x + 1)(x - 1))$ is waar.

Voorbeeld 2. $\forall_{x\in\mathbb{R}}(x^2 > 0)$ is onwaar.

Voorbeeld 3. $\exists_{x\in\mathbb{R}}(x^2 - 1 = 0)$ is waar.

Voorbeeld 4. $\exists_{x\in\mathbb{R}}(x^2 + 1 = 0)$ is onwaar.

Voorbeeld 5. $\exists_{x\in\mathbb{R}}\ \exists_{y\in\mathbb{R}}\ (x > y)$ is waar,

$\forall_{x\in\mathbb{R}}\ \exists_{y\in\mathbb{R}}\ (x > y)$ is waar,

$\exists_{x\in\mathbb{R}}\ \forall_{y\in\mathbb{R}}\ (x > y)$ is onwaar.

Zij nu U de totaliteit der mensen.

Voorbeeld 6. $\forall_{x\in U}$ (x is sterfelijk) is waar,

$\exists_{x\in U}$ (x is onsterfelijk) is onwaar.

Voorbeeld 7. $\exists!_{x\in U}$ (x is koningin van Engeland) is waar.

De negatie van de bewering $\forall_{x\in U}(P(x))$ is de bewering $\exists_{x\in U}(\neg P(x))$ en er geldt:

$$(\neg \forall_{x\in U}(P(x)) \iff (\exists_{x\in U}(\neg P(x))) \ .$$

De negatie van de bewering $\exists_{x\in U}(P(x))$ is de bewering $\forall_{x\in U}(\neg P(x))$ en er geldt:

$$(\neg \exists_{x\in U}(P(x))) \iff (\forall_{x\in U}(\neg P(x))) \ .$$

Voorbeeld 8. $(\neg \forall_{x\in\mathbb{R}}(x^2 > 0)) \iff (\exists_{x\in\mathbb{R}}(\neg (x^2 > 0)))$.

Voorbeeld 9. $(\neg \exists_{x\in U}$ (x is onsterfelijk)) $\iff (\forall_{x\in U}$ $(\neg$ (x is onsterfelijk))).

Hoofdstuk II. Verzamelingen

2.1. Het begrip verzameling

Voorbeelden van verzamelingen zijn de volgende.
Een mand appels, een zootje vis, een gezelschap studenten, een verzameling postzegels, een club voetballers, een federatie voetbalclubs, een klasse leerlingen, een school klassen, een school haringen, een hoop mieren, een stel mierenhopen, een lijn punten, een waaier lijnen, een totaliteit dingen.

Wij veronderstellen de begrippen "verzameling" en "is element van" als intuïtief bekend. Notaties:

$$a \in A \ , \quad a \notin A$$

voor "a is element van de verzameling A", resp. "a is niet element van de verzameling A.

Voorbeeld 1. De verzameling $\mathbb{N}$ der natuurlijke getallen;

$$1 \in \mathbb{N} \ , \quad 2 \in \mathbb{N} \ , \quad 87 \in \mathbb{N} \ , \quad 0 \notin \mathbb{N} \ , \quad -3 \notin \mathbb{N} \ .$$

Voorbeeld 2. De verzameling $\mathbb{Z}$ der gehele getallen;

$$2 \in \mathbb{Z} \ , \quad -1 \in \mathbb{Z} \ , \quad 0 \in \mathbb{Z} \ , \quad -87 \in \mathbb{Z} \ , \quad \tfrac{1}{2} \notin \mathbb{Z} \ .$$

Voorbeeld 3. De verzameling $\mathbb{Q}$ der rationale getallen;

$$1 \in \mathbb{Q} \ , \quad \tfrac{1}{2} \in \mathbb{Q} \ , \quad -\frac{7}{5} \in \mathbb{Q} \ , \quad \frac{10}{5} \in \mathbb{Q} \ , \quad \sqrt{2} \notin \mathbb{Q} \ .$$

Voorbeeld 4. De verzameling $\mathbb{R}$ der reële getallen;

$$-23 \in \mathbb{R} \ , \quad \pi \in \mathbb{R} \ , \quad \sqrt{2} \in \mathbb{R} \ , \quad i \notin \mathbb{R} \ .$$

Voorbeeld 5. De lege verzameling $\emptyset$.

Voorbeeld 6. De verzameling $\{2,3\}$ bestaat uit de getallen 2 en 3.

Voorbeeld 7. De verzameling $\{2,\{3\}\}$ bestaat uit het getal 2 en de verzameling bestaande uit het getal 3.

Voorbeeld 8. Zij KNVB de verzameling van de voetbalclubs in Nederland. Beschouw elke voetbalclub als de verzameling van zijn voetballers. Dan geldt

Van Beveren $\in$ PSV, PSV $\in$ KNVB, van Beveren $\notin$ KNVB, KNVB $\cap$ {PSV} = {PSV} .

2.2. Inclusie

A is deel van B, notatie $A \subset B$, wanneer voor elke $a \in A$ geldt $a \in B$. Twee verzamelingen A en B zijn gelijk, notatie A = B, wanneer geldt $A \subset B$ en $B \subset A$.

Eigenschappen: $A \subset A$; als $A \subset B$ en $B \subset C$, dan $A \subset C$.

Voorbeeld 1. $\emptyset \subset \{5,6\} \subset \{5,6,87\} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Voorbeeld 2. $\{5,6\} = \{5,5,5,6\}$.

Voorbeeld 3. De verzameling van alle delen van $\{1,2,3\}$ is

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} .$$

Teneinde bepaalde moeilijkheden *) te vermijden, zullen wij slechts verzamelingen beschouwen die deel zijn van een verzameling U, het universum. Wij nemen aan dat er voor elk element x van U twee mogelijkheden zijn, ten aanzien van een verzameling A, namelijk

$$x \in A \quad \text{en} \quad x \notin A .$$

2.3. Aanduiding van een verzameling met een predicaat

Een predicaat P(x), met individuenverzameling I, wordt een bewering wanneer voor x wordt gesubstitueerd een element van I.

De verzameling van alle $x \in I$, waarvoor P(x) waar is, wordt genoteerd door

$$P = \{x \in I \mid P(x)\} .$$

*) Zie ook 2.8, blz. 13.

Voorbeeld 1. $\{x \in \mathbb{R} \mid (x + 1)(x - 2) = 0\} = \{-1,2\}$.

Voorbeeld 2. $\{x \in \mathbb{N} \mid (x + 1)(x - 2) = 0\} = \{2\}$.

Voorbeeld 3. $\{x \in \mathbb{R} \mid -3 < x \leq 1\}$.

Voorbeeld 4. $\{x \in \mathbb{R} \mid \exists_{y \in \mathbb{R}} (x = y^2)\} = \{x \in \mathbb{R} \mid x \geq 0\}$.

Voorbeeld 5. Zij A en B punten van het vlak. $\{P \in \text{vlak} \mid PA = PB\}$ is de middelloodlijn van AB.

Voorbeeld 6. $\{(x,y) \in \text{vlak} \mid x^2 + y^2 = 9\}$ is een cirkel.

Voorbeeld 7. $\{x \in U \mid x \in A\} = A$.

2.4. Bewerkingen met verzamelingen

Zij A en B verzamelingen, beide deel van de verzameling U.
De vereniging $A \cup B$ is de verzameling die bestaat uit de elementen van A en de elementen van B:

$$A \cup B := \{x \in U \mid (x \in A) \vee (x \in B)\} .$$

De doorsnede $A \cap B$ is de verzameling die bestaat uit de elementen die zowel element van A als element van B zijn:

$$A \cap B := \{x \in U \mid (x \in A) \wedge (x \in B)\} .$$

Het complement A^* van A (t.o.v. U) is de verzameling van de elementen van U die niet element van A zijn:

$$A^* := \{x \in U \mid x \notin A\} .$$

Voorbeeld 1. $U = \mathbb{R}$, $A = \{x \in \mathbb{R} \mid x > 0\}$, $B = \{x \in \mathbb{R} \mid x \leq 1\}$, dan $A \cup B = \mathbb{R}$, $A \cap B = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$, $A^* = \{x \in \mathbb{R} \mid x \leq 0\}$.

Voorbeeld 2. Zij U de verzameling van de mensen, A de verzameling van de manlijke mensen, B de verzameling van de volwassen mensen. Dan is $A \cap B$ de verzameling van de mannen, en $(A \cup B)^*$ de verzameling van de meisjes.

Voorbeeld 3. $U = \mathbb{R}$, $A = \{x \in \mathbb{R} \mid x \geq 0\}$, $B = \{x \in \mathbb{R} \mid x \leq 0\}$, $C = \{x \in \mathbb{R} \mid x < 0\}$, dan $A \cup B = \mathbb{R}$, $A \cap B = \{0\}$, $A \cup C = \mathbb{R}$, $A \cap C = \emptyset$, $B \cup C = B$, $B \cap C = C$.

Twee verzamelingen heten disjunct wanneer hun doorsnede leeg is.

Er is een nauw verband tussen de hierboven ingevoerde bewerkingen $\cup$, $\cap$, * voor verzamelingen, en de in 1.2. besproken bewerkingen $\vee$, $\wedge$, $\neg$ voor predicaten.

Zij $P(x)$ en $Q(x)$ twee predicaten met dezelfde individuenverzameling U. Zij

$$P := \{x \in U \mid P(x)\} \ , \ Q := \{x \in U \mid Q(x)\} \ .$$

Dan geldt:

(1) $P^* = \{x \in U \mid \neg P(x)\}$,

(2) $P \cap Q = \{x \in U \mid P(x) \wedge Q(x)\}$,

(3) $P \cup Q = \{x \in U \mid P(x) \vee Q(x)\}$,

(4) $P^* \cup Q = \{x \in U \mid P(x) \Rightarrow Q(x)\}$,

(5) $(P^* \cup Q) \cap (P \cup Q^*) = \{x \in U \mid P(x) \Leftrightarrow Q(x)\}$.

Wij bewijzen enkele van deze formules.

(1) Zij $x \in P^*$, dan $x \notin P$, dan $P(x)$ onwaar, dan $\neg P(x)$ waar, dus $x \in$ rechts.
Zij $x \in U$ en $\neg P(x)$ waar, dan $P(x)$ onwaar, dan $x \notin P$, dus $x \in P^*$.

(3) Zij $x \in P \cup Q$, dan $(x \in P) \vee (x \in Q)$, dan ($P(x)$ waar) $\vee$ ($Q(x)$ waar), dan $(P(x) \vee Q(x))$ waar, dus $x \in$ rechts.
Zij $x \in U$ en $(P(x) \vee Q(x))$ waar, dan ($P(x)$ waar) $\vee$ ($Q(x)$ waar), dan $(x \in P) \vee (x \in Q)$, dus $x \in P \cup Q$.

(4) Zij $x \in P^* \cup Q$, dan $(x \in P^*) \vee (x \in Q)$, dan ($P(x)$ onwaar) $\vee$ ($Q(x)$ waar), dan $(P(x) \Rightarrow Q(x))$ waar, dus $x \in$ rechts.
Zij $x \in U$ en $(P(x) \Rightarrow Q(x))$ waar, dan ($Q(x)$ waar) $\vee$ ($P(x)$ onwaar), dan $(x \in Q) \vee (x \in P^*)$, dus $x \in Q \cup P^*$.

2.5. Eigenschappen der bewerkingen

Vereniging en doorsnede van verzamelingen voldoen aan de volgende eigenschappen:

$A \cup B = B \cup A$, $A \cap B = B \cap A$, de commutatieve wet.

$(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$, associatieve wetten.

$A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.

Als $A \subset B$, dan $A \cup B = B$ en $A \cap B = A$.

$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ } distributieve wetten.

Het complement voldoet aan de volgende eigenschappen:

$(A^*)^* = A$, $U^* = \emptyset$, $\emptyset^* = U$, als $A \subset B$ dan $B^* \subset A^*$,

$A \cup A^* = U$, $A \cap A^* = \emptyset$,

$(A \cup B)^* = A^* \cap B^*$, $(A \cap B)^* = A^* \cup B^*$.

Sommige van deze eigenschappen zijn triviaal, andere laten zich bewijzen via het in de vorige paragraaf aangeduide verband met de propositiecalculus (rekening met beweringen). Wij geven een voorbeeld van het laatste.

Bewijs van $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.
Voer in de volgende predicaten, alle met individuenverzameling U.

$$A(x) : \Leftrightarrow (x \in A) \quad , \quad B(x) : \Leftrightarrow (x \in B) \quad , \quad C(x) : \Leftrightarrow (x \in C) \ .$$

Wegens 1.1, voorbeeld 21, weten wij dat voor $x \in U$

$$((A(x) \wedge B(x)) \vee C(x)) \Leftrightarrow ((A(x) \vee C(x)) \wedge (B(x) \vee C(x)))$$

altijd waar is. Daarom geldt

$$\{x \in U \mid (A(x) \wedge B(x)) \vee C(x)\} = \{x \in U \mid (A(x) \vee C(x)) \wedge (B(x) \vee C(x))\} \ ,$$

en dit is gelijkwaardig met het gestelde.

2.6. Nog enkele bewerkingen

Het verschil $A \setminus B$ van de verzamelingen A en B is de verzameling die als elementen heeft de elementen van A die niet tevens element van B zijn:

$$A \setminus B := A \cap B^* = \{x \in U \mid (x \in A) \wedge (x \notin B)\} .$$

Triviaal is

$$U \setminus A = A^* , \quad A \setminus A = \emptyset , \quad A \setminus \emptyset = A , \quad A \setminus A^* = A .$$

Iets minder triviaal zijn

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C) , \quad A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) .$$

Bewijs:

$$A \setminus (B \cap C) = A \cap (B \cap C)^* = A \cap (B^* \cup C^*) =$$

$$= (A \cap B^*) \cup (A \cap C^*) = (A \setminus B) \cup (A \setminus C) .$$

Niet geldt $(A \setminus B) \setminus C = A \setminus (B \setminus C)$, zoals blijkt uit het volgende voorbeeld:

$$A := \{x \in \mathbb{R} \mid x > -1\}, \; B := \{x \in \mathbb{R} \mid x < 1\}, \; C := \{x \in \mathbb{R} \mid -2 < x < 2\}.$$

Het symmetrische verschil $A \div B$ van de verzamelingen A en B is de verzameling bestaande uit de elementen die tot precies één van de beide verzamelingen A en B behoren:

$$A \div B := (A \setminus B) \cup (B \setminus A) .$$

Er geldt $A \div B = (A \cup B) \setminus (A \cap B)$,

immers $(A \setminus B) \cup (B \setminus A) = (A \cap B^*) \cup (B \cap A^*) =$

$$= (A \cup B) \cap U \cap U \cap (B^* \cup A^*) = (A \cup B) \cap (A \cap B)^* =$$

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

Eenvoudige eigenschappen zijn:

$$A \div B = B \div A , \quad A \div A = \emptyset , \quad A \div \emptyset = A ,$$

$$A \div A^* = U , \quad (A \div B) \div C = A \div (B \div C) .$$

2.7. Vereniging en doorsnede van een willekeurige collectie verzamelingen

Zij I een verzameling, en zij aan ieder element $i \in I$ toegevoegd een verzameling A_i. Wij definiëren

$$\bigcup_{i\in I} A_i := \{x \in U \mid \exists_{i\in I}(x \in A_i)\} ,$$

$$\bigcap_{i\in I} A_i := \{x \in U \mid \forall_{i\in I}(x \in A_i)\} .$$

Wanneer $I = \{1,2,\ldots,n\}$ een eindige verzameling is, dan staat hier

$$\bigcup_{i\in I} A_i = A_1 \cup A_2 \cup \ldots \cup A_n , \quad \bigcap_{i\in I} A_i = A_1 \cap A_2 \cap \ldots \cap A_n .$$

Wanneer $I = \mathbb{N}$, dan schrijft men

$$\bigcup_{i\in I} A_i = \cup_{i=1}^{\infty} A_i , \quad \bigcap_{i\in I} A_i = \cap_{i=1}^{\infty} A_i .$$

De volgende eigenschap geldt:

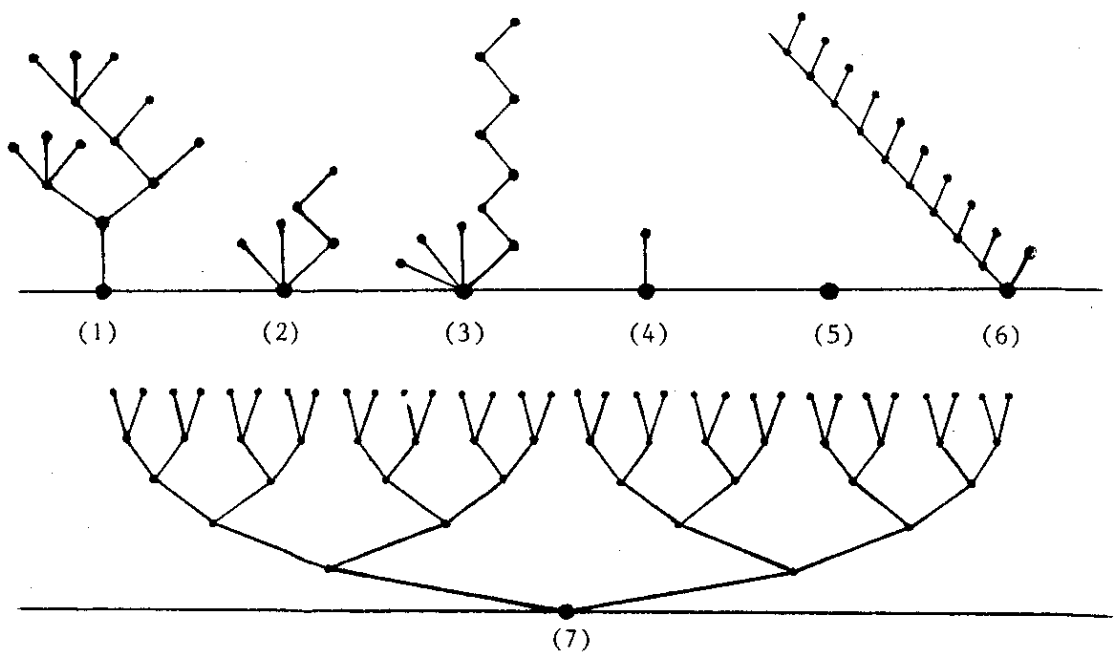
$$\left(\bigcup_{i\in I} A_i\right)^* = \bigcap_{i\in I} A_i^* , \quad \left(\bigcap_{i\in I} A_i\right)^* = \bigcup_{i\in I} A_i^* .$$

Bewijs:

$\neg$ (x is element van tenminste één A_i) $\Leftrightarrow$ (x is element van geen enkele A_i)

$\Leftrightarrow$ (x is element van elke A_i^*) .

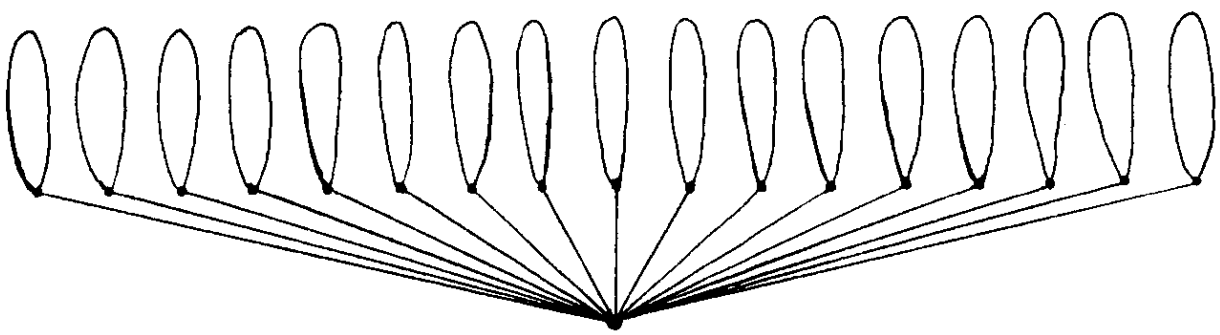
2.8. De paradox van Russell



Wij beschouwen alle mogelijk bomen. Elke boom begint met een wortel. Boom (5) heeft geen tak. Boom (6) is bedoeld oneindig veel takken te hebben. Zo ook de binaire boom (7). Boom (6) en boom (7) hebben de eigenschap, dat er op de eerste etage een boom staat die dezelfde is als (isomorf is met) de hele boom.

Definitie. Een boom B heet verboden als hij een met B isomorfe subboom op de eerste etage bevat.

Beschouw nu de verzameling van alle niet-verboden bomen. Maak een nieuwe boom als volgt, door al deze niet-verboden bomen op de eerste etage te plaatsen:



Is deze nieuwe boom verboden of niet?

Stel de nieuwe boom is verboden. Dan staat er eenzelfde boom op de eerste etage. Daar staan echter slechts de niet-verboden bomen.

Stel de nieuwe boom is niet-verboden. Dan komt deze boom op de eerste etage voor. Maar dan is de nieuwe boom verboden.

Zo bereiken wij een paradox. De "verklaring" is, dat wij niet ongebreideld mogen verzamelen. De verzamelingsleer moet zorgvuldiger worden opgezet.

Hoofdstuk III. Afbeeldingen en relaties

3.1. Cartesisch product

Het Cartesisch product van de verzamelingen A en B (notatie $A \times B$) is de verzameling van alle geordende paren (a,b) waarbij $a \in A$ en $b \in B$:

$$A \times B := \{(a,b) \mid a \in A,\ b \in B\} .$$

Voorbeeld 1. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is het platte vlak uit de analytische meetkunde.

Voorbeeld 2. $\mathbb{Z} \times \mathbb{Z}$ is de verzameling van de roosterpunten in $\mathbb{R}^2$.

Voorbeeld 3. Zij $A := \{a_1,\ldots,a_n\}$, $B := \{b_1,\ldots,b_m\}$. Het aantal elementen van $A \times B$ is nm.

Het Cartesisch product $A \times B \times C$ is de verzameling van de geordende drietallen (a,b,c) met $a \in A$, $b \in B$, $c \in C$. Wij schrijven $A^3 := A \times A \times A$.

Voorbeeld 4. Zij $F := \{0,1\}$, dan bestaat F^n uit alle rijen met n plaatsen, elk gevuld met 0 of 1. F^n heeft 2^n elementen. F^3 kan worden gebruikt voor de duale voorstelling van de getallen: 0 = 000, 1 = 001, 2 = 010, 3 = 011, 4 = 100, 5 = 101, 6 = 110, 7 = 111.

Voorbeeld 5. $F := \{0,1,2,3,4,5,6,7,8,9\}$. Wij kunnen F^4 gebruiken voor de decimale voorstelling van de getallen 0 tot en met 9999.

3.2. Afbeeldingen

Zij $A \times B$ het Cartesisch product van de verzamelingen A en B.
Een afbeelding F van A in B, notatie $F : A \nrightarrow B$, is een deel F van $A \times B$ met de eigenschap:

$$\forall_{a \in A}\ \exists!_{b \in B}\ ((a,b) \in F) .$$

b, notatie $b = F(a)$, is het beeld van $a \in A$ onder F, en a is een origineel van b onder F.

Opmerking. Dit is de precisering van de zin: F is een voorschrift volgens hetwelk aan elke $a \in A$ wordt toegevoegd één $b = F(a) \in B$.

Opmerking. In het begrip afbeelding vervalt het verschil tussen de begrippen functie en grafiek.

Voorbeeld 1. $\{(1,1),(2,1),(3,2),(4,3)\}$ is een afbeelding van $\{1,2,3,4\}$ in $\mathbb{Z}$.

Voorbeeld 2. Een oneindige rij $a_1,a_2,a_3,\ldots$ is een afbeelding van $\mathbb{N}$ in $\mathbb{R}$.

Voorbeeld 3. Een telefoonboek is een afbeelding van de verzameling der telefoonbezitters in $\mathbb{N}$.

Voorbeeld 4. De functie sin is een afbeelding van $\mathbb{R}$ in $\mathbb{R}$. De functie log is een afbeelding van $\{x \in \mathbb{R} \mid x > 0\}$ in $\mathbb{R}$.

Voorbeeld 5. Een predicaat P is een afbeelding van de individuenverzameling I in $\{0,1\}$.

Voorbeeld 6. De identieke afbeelding I van A op A is gedefinieerd door $I = \{(x,x) \mid x \in A\}$. Deze afbeelding beeldt elke $a \in A$ op zichzelf af.

Zij $F : A \to B$ een afbeelding. Zij $A' \subset A$ en $B' \subset B$.
$F(A') := \{F(a) \in B \mid a \in A'\}$ is het beeld van A'.
$F^{\leftarrow}(B') := \{a \in A \mid F(a) \in B'\}$ is het volledig origineel van B'.

Voorbeeld 7. Beschouw de afbeelding $\sin : \mathbb{R} \to \mathbb{R}$. $A' = \{x \in \mathbb{R} \mid 0 \leq x \leq \pi\}$, dan $\sin(A') = \{y \in \mathbb{R} \mid 0 \leq y \leq 1\}$,

$$\sin^{\leftarrow}(\{\tfrac{1}{2}\}) = \{\frac{\pi}{6} , \frac{5\pi}{6} , \frac{13\pi}{6} , \frac{17\pi}{6} ,\ldots\} .$$

$B' = \{y \in \mathbb{R} \mid 0 \leq y \leq 1\}$ dan $\sin^{\leftarrow}(B') = \{x \mid 0 \leq x \leq \pi\} \cup \{x \mid 2\pi \leq x \leq 3\pi\} \cup \ldots$

Voorbeeld 8. Beschouw de afbeelding $\log : \{x \in \mathbb{R} \mid x > 0\} \to \mathbb{R}$.

$$\log^{\leftarrow}(\{0\}) = \{1\} .$$

$$\log(\{x \mid 0 < x \leq 1\}) = \{y \mid y \leq 0\} .$$

$$\log^{\leftarrow}(\{y \mid y \geq 0\}) = \{x \mid x \geq 1\} .$$

3.3. Afbeeldingen op, één-éénduidigheid, inverse en samengestelde afbeeldingen

Zij $F : A \to B$ een afbeelding van A in B, dus

$$\forall_{a \in A} \exists!_{b \in B} ((a,b) \in F) .$$

$F : A \to B$ heet een afbeelding van A op B, als bovendien geldt

$$\forall_{b \in B} \exists_{a \in A} ((a,b) \in F) ,$$

m.a.w. als $F(A) = B$.

Voorbeeld 9. $\sin : \mathbb{R} \to \mathbb{R}$ is een afbeelding in, en niet op.
$\sin : \mathbb{R} \to \{y \in \mathbb{R} \mid -1 \leq y \leq 1\}$ is een afbeelding op.
$\log : \{x \in \mathbb{R} \mid x > 0\} \to \mathbb{R}$ is een afbeelding op.

$F : A \to B$ heet één-éénduidig als

$$\forall_{b \in F(A)} \exists!_{a \in A} ((a,b) \in F) ,$$

m.a.w. als $\forall_{a \in A} \forall_{a' \in A} (F(a) = F(a') \Rightarrow a = a')$.
$F : A \to B$ heet één-éénduidig op als

$$\forall_{b \in B} \exists!_{a \in A} ((a,b) \in F) .$$

Opmerking. Soms noemt men een afbeelding op: surjectief, een één-éénduidige afbeelding: injectief, en een één-éénduidige afbeelding op: bijectief.

Voorbeeld 10. $\sin : \mathbb{R} \to \mathbb{R}$ is niet één-éénduidig.
$\log : \{x \mid x > 0\} \to \mathbb{R}$ is één-éénduidig op.

Voorbeeld 11. $\arcsin : \{x \mid -1 \leq x \leq 1\} \to \{y \mid -\frac{\pi}{2} \leq y \leq \frac{\pi}{2}\}$ is één-éénduidig op.

Stelling. Als $F : A \to B$ één-éénduidig op is, dan is

$$G : B \to A, \text{ met } G := \{(b,a) \mid b \in B, a \in A, (a,b) \in F\} ,$$

een afbeelding die één-éénduidig op is.

Bewijs. $F \subset A \times B$ en de gedefinieerde $G \subset B \times A$ liggen gespiegeld t.o.v. de diagonaal I:

$$\forall_{a \in A} \forall_{b \in B} (((a,b) \in F) \iff ((b,a) \in G)) .$$

F is een afbeelding die één-éénduidig op is:

$$\forall_{b \in B} \exists!_{a \in A} ((a,b) \in F) .$$

Hieruit volgt

$$\forall_{b \in B} \exists!_{a \in A} ((b,a) \in G) .$$

Dit betekent dat $G : B \to A$ een afbeelding is. Deze afbeelding is één-éénduidig op, omdat bovendien geldt

$$\forall_{a \in A} \exists!_{b \in B} ((b,a) \in G) .$$

Notatie. G heet de inverse van F, schrijf $G = F^{-1}$. Als $F(a) = b$, dan $G(b) = a$.

Voorbeeld 12. log en e-macht zijn inverse afbeeldingen:

$$y = \log x , \quad x = e^y .$$

Opmerking. Let op dat slechts de inverse is gedefinieerd van afbeeldingen die één-éénduidig op zijn.

Voorbeeld 13. $\sin : \mathbb{R} \to \{y \in \mathbb{R} \mid -1 \leq y \leq 1\}$ heeft geen inverse.

Voorbeeld 14. Van $y = 1 - \sqrt{x}$ en $z = \log y$ is $z = \log(1 - \sqrt{x})$ de samengestelde functie, op $\{x \in \mathbb{R} \mid 0 \leq x < 1\}$.

Zij $F : A \to B$ en $G : B \to C$ afbeeldingen. De samengestelde afbeelding $G \circ F : A \to C$ wordt gedefinieerd door

$$\forall_{a \in A} ((G \circ F)(a) := G(F(a))) .$$

Voorbeeld 15. De afbeeldingen $F : \mathbb{R} \to \mathbb{R}$ en $G : \mathbb{R} \to \mathbb{R}$ worden gedefinieerd door:

$$\forall_{x \in \mathbb{R}} \; (F(x) := \sin x, \; G(x) := x^2) \; .$$

Zij hebben als samengestelden:

$$(G \circ F)(x) = (\sin x)^2 \quad \text{en} \quad (F \circ G)(x) = \sin(x^2) \; .$$

3.4. De karakteristieke functie van een verzameling

Zij U een verzameling en zij $W := \{0,1\}$.
De karakteristieke functie χ_A van de verzameling $A \subset U$ is de afbeelding $\chi_A : U \to W$ gedefinieerd door

$$\chi_A(x) = 1 \text{ als } x \in A, \; \chi_A(x) = 0 \text{ als } x \notin A \; .$$

De verzameling A is bepaald door zijn karakteristieke functie, immers

$$A = \overleftarrow{\chi_A}(\{1\}) \; .$$

Eigenschappen van karakteristieke functies:

$$\chi_{A^*} = 1 - \chi_A \; ,$$

$$\chi_{A \cap B} = \chi_A \chi_B = \min(\chi_A, \chi_B) \; ,$$

$$\chi_{A \cup B} = \chi_A + \chi_B - \chi_A \chi_B = \max(\chi_A, \chi_B) \; ,$$

$$\chi_{A \setminus B} = \chi_A - \chi_A \chi_B \; ,$$

$$\chi_{A \div B} = \chi_A + \chi_B - 2\chi_A \chi_B \; .$$

Eén herleiding:

$$\chi_{A \cup B} = 1 - \chi_{(A \cup B)^*} = 1 - \chi_{A^* \cap B^*} = 1 - \chi_{A^*} \chi_{B^*} =$$

$$= 1 - (1 - \chi_A)(1 - \chi_B) = \chi_A + \chi_B - \chi_A \chi_B \; .$$

Voorbeeld.

$$\chi_{A \div A} = \chi_A + \chi_A - 2 \, \chi_A^2 = \chi_A + \chi_A - 2 \, \chi_A = 0 \; .$$

3.5. Relaties

Een relatie R op een verzameling V is een deel van $V \times V$. De elementen $x \in V$ en $y \in V$ zijn in de relatie R, schrijf $x \sim y$, wanneer $(x,y) \in R$. Een relatie heet

reflexief, wanneer $\forall_{x \in V} (x \sim x)$,
symmetrisch, wanneer $\forall_{x \in V} \forall_{y \in V} ((x \sim y) \Rightarrow (y \sim x))$,
transitief, wanneer $\forall_{x \in V} \forall_{y \in V} \forall_{z \in V} (((x \sim y) \wedge (y \sim z)) \Rightarrow (x \sim z))$.

Voorbeelden. De verzameling is steeds $\mathbb{R}$.

relatie $x \sim y$	reflexief	symmetrisch	transitief
$x = y + 1$	-	-	-
$x > y$	-	-	+
$x \neq y$	-	+	-
$x \leq y < x + 2$	+	-	-
$xy > 0$	-	+	+
$x \geq y$	+	-	+
$\lvert x - y \rvert < 1$	+	+	-
$x = y$	+	+	+

3.6. Equivalentierelaties

Een relatie, die reflexief, symmetrisch en transitief is, heet een equivalentierelatie.

Voorbeeld 1. Zij $V := \mathbb{R}$. De relatie $x - y \in \mathbb{Z}$ is een equivalentierelatie.

Voorbeeld 2. Zij V de verzameling van de driehoeken in het vlak. De congruentie van driehoeken is een equivalentierelatie.

Voorbeeld 3. Zij V de verzameling der rechten in het vlak. De relatie gedefinieerd door evenwijdigheid (en samenvallen) is een equivalentierelatie.

Voorbeeld 4. Zij $V := \mathbb{Z}$. De relatie ($x - y$ is een 5-voud) is een equivalentierelatie.

Zij $\sim$ een equivalentierelatie, gedefinieerd op een verzameling V. De bij $a \in V$ behorende equivalentieklasse $K\ell(a)$ is gedefinieerd door

$$K\ell(a) := \{x \in V \mid x \sim a\} .$$

Voorbeeld 1. $K\ell(\frac{1}{3}) = \{\frac{1}{3}, \frac{4}{3}, \frac{7}{3}, \ldots, -\frac{2}{3}, -\frac{5}{3}, \ldots\}$.

Voorbeeld 2. $K\ell(\Delta) = \{$alle driehoeken die congruent zijn met $\Delta\}$.

Voorbeeld 3. $K\ell(\ell) = \{\ell$ en alle rechten die evenwijdig zijn aan $\ell\}$.

Voorbeeld 4. $K\ell(2) = \{2,7,12,\ldots,-3,-8,\ldots\} = K\ell(7) = K\ell(-3)$.

Stelling. De diverse equivalentieklassen verdelen V in niet-lege, disjuncte delen, met de eigenschap dat de elementen van elk equivalent paar in eenzelfde deel liggen en dat de elementen van elk niet-equivalent paar in verschillende delen liggen.

Voorbeeld 1. Bij elke a uit $0 \leq a < 1$ behoort een equivalentieklasse $K\ell(a) = \{a + z \mid z \in \mathbb{Z}\}$, en er geldt:

$$\mathbb{R} = \bigcup_{0 \leq a < 1} K\ell(a), \quad \forall_{0 \leq a < 1} \, (K\ell(a) \neq \emptyset) ,$$

$$\forall_{\substack{0 \leq a,b < 1 \\ a \neq b}} \, (K\ell(a) \cap K\ell(b) = \emptyset) .$$

Voorbeeld 3. Bij elke rechte ℓ door de oorsprong behoort een klasse $K\ell(\ell)$ van de met ℓ evenwijdige lijnen. Deze klassen zijn niet leeg, onderling disjunct, en hun vereniging is de verzameling der rechten in het vlak.

Voorbeeld 4. Bij elk der getallen 0,1,2,3,4 behoort een klasse, namelijk:

$K\ell(0) = \{5$-vouden$\}$, $K\ell(1) = \{5$-vouden $+1\}$, $K\ell(2) = \{5$-vouden $+2\}$,

$K\ell(3) = \{5$-vouden $+3\}$, $K\ell(4) = \{5$-vouden $+4\}$.

Dit zijn alle klassen.

Bewijs stelling. Zij $\sim$ een equivalentierelatie op V. Zij $K\ell(a)$ de equivalentieklasse van $a \in V$. Dan geldt:

$\forall_{a\in V}\ (K\ell(a) \neq \emptyset)$, omdat $a \in K\ell(a)$ wegens reflexiviteit.

$V = \bigcup_{a\in V} K\ell(a)$, omdat $V \subset \bigcup_{a\in V} K\ell(a)$ wegens $a \in K\ell(a)$, en

$V \supset \bigcup_{a\in V} K\ell(a)$ wegens $K\ell(a) \subset V$.

Voor $a \in V$, $b \in V$ geldt:

$$K\ell(a) \cap K\ell(b) = \emptyset \quad \text{of} \quad K\ell(a) = K\ell(b) \ ;$$

het bewijs luidt als volgt.
Neem $c \in K\ell(a)$, dan $c \sim a$. Neem $x \in K\ell(a)$, dan $x \sim a$ en (symmetrie) $a \sim x$. Dan ook (transitiviteit) $c \sim x$ en $x \sim c$. Wegens

$$\forall_{x\in V}\ ((x \sim a) \Longleftrightarrow (x \sim c))$$

geldt dus $K\ell(a) = K\ell(c)$. Wanneer nu $c \in K\ell(a) \cap K\ell(b)$, dan volgt $K\ell(a) = K\ell(c) = K\ell(b)$. Hiermee is de stelling bewezen.

Voorbeeld 5. In $\mathbb{R}^2$ is de relatie $\sim$ gedefinieerd als volgt. Twee punten zijn equivalent als zij dezelfde afstand tot de oorsprong hebben:

$$\forall_{(x,y)\in \mathbb{R}^2}\ \forall_{(u,v)\in \mathbb{R}^2}\ (((x,y) \sim (u,v)) :\Longleftrightarrow (x^2 + y^2 = u^2 + v^2)) \ .$$

Dit is een equivalentierelatie. De equivalentieklassen zijn de cirkels met middelpunt in de oorsprong.

Voorbeeld 6. $\forall_{x\in \mathbb{R}}\ \forall_{y\in \mathbb{R}}\ ((x \sim y) :\Longleftrightarrow \exists_{a\in \mathbb{R}}\ ((a \neq 0) \wedge (ax = y)))$ is een equivalentierelatie. De equivalentieklassen zijn $\{0\}$ en $\mathbb{R} \setminus \{0\}$.

Voorbeeld 7. Zij $F : A \to B$ een afbeelding

$$\forall_{x\in A}\ \forall_{y\in A}\ ((x \sim y) :\Longleftrightarrow (F(x) = F(y)))$$

is een equivalentierelatie. De equivalentieklassen zijn de verzamelingen $F^{\leftarrow}(\{b\})$, met $b \in F(A)$.

3.7. Het Galois lichaam GF(p), p priem

Zij p een priemgetal. Twee gehele getallen heten congruent modulo p als hun verschil een p-voud is.

Voorbeeld 1. $17 \equiv 2 \pmod 5$, omdat $17 - 2 = 5.3$.

Voorbeeld 2. $92 \equiv 1 \pmod 7$, omdat $92 - 1 = 7.13$.

Congruentie mod p definieert een relatie op $\mathbb{Z}$:

$$\forall_{x\in\mathbb{Z}} \forall_{y\in\mathbb{Z}} ((x \equiv y \pmod p) :\Longleftrightarrow (\exists_{v\in\mathbb{Z}} (x - y = pv))) .$$

Deze relatie is een equivalentierelatie, immers $x \equiv x \pmod p$, omdat $x - x = p.0$.

Als $x \equiv y \pmod p$, dan $x - y = pv$, dan $y - x = p.(-v)$, dus $y \equiv x \pmod p$.

Als $x \equiv y$ en $y \equiv z$, dan $x - y = pv$ en $y - z = pw$, dan $x - z = p(v + w)$, dus $x \equiv z \pmod p$.

De equivalentieklassen zijn de volgende verzamelingen:

$$Kl(0) = \{\ldots,-2p,-p,0,p,2p,3p,\ldots\} ,$$

$$Kl(1) = \{\ldots,-2p+1,-p+1,1,p+1,2p+1,3p+1,\ldots\} ,$$

$$Kl(2) = \{\ldots,-2p+2,-p+2,2,p+2,2p+2,3p+2,\ldots\} ,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots ,$$

$$Kl(p-1) = \{\ldots,-p-1,-1,p-1,2p-1,3p-1,4p-1,\ldots\} .$$

In overeenstemming met de stelling van 3.6 wordt $\mathbb{Z}$ door deze equivalentieklassen verdeeld in disjuncte delen. Voor de equivalentieklassen definieren wij optelling en vermenigvuldiging als volgt:

$$Kl(a) + Kl(b) := Kl(a + b) ,$$

$$Kl(a) \,.\, Kl(b) := Kl(ab) .$$

Dit zijn zinvolle definities, omdat het volgende geldt:

Als $a \equiv a'$, $b \equiv b'$, dan $a + b \equiv a' + b'$.

Bewijs: als $a - a' = pv$, $b - b' = pw$, dan $a + b - a' - b' = p(v + w)$.

Als $a \equiv a'$, $b \equiv b'$, dan $ab = a'b'$.

Bewijs: als $a = a' + pv$, $b = b' + pw$, dan $ab = a'b' +$ p voud.

Voor de zojuist gedefinieerde optelling en vemenigvuldiging van equivalentieklassen geldt een aantal eigenschappen die de verzameling der equivalentieklassen tot een lichaam maken. Dit is het Galois lichaam GF(p). Wij stellen de opsomming van deze eigenschappen uit, en bewijzen hier slechts de belangrijkste eigenschap:

Stelling. Uit $K\ell(a) \cdot K\ell(b) = K\ell(0)$ volgt $K\ell(a) = K\ell(0)$ of $K\ell(b) = K\ell(0)$.

Bewijs. $K\ell(a) \cdot K\ell(b) = K\ell(ab)$. Uit $K\ell(ab) = K\ell(0)$ volgt $ab \equiv 0 \pmod p$, dus $ab = pv$, dus p deelbaar op ab. Omdat p priem is, volgt dat p deelbaar is op a of op b, dus

$$a \equiv 0 \pmod p \quad \text{of} \quad b \equiv 0 \pmod p .$$

Dit betekent $K\ell(a) = K\ell(0)$ of $K\ell(b) = K\ell(0)$.

Het Galois lichaam GF(p) heeft p elementen, namelijk de equivalentieklassen modulo p. Wij kunnen deze equivalentieklassen optellen en vermenigvuldigen. Deze rekening illustreren wij in de volgende voorbeelden. Daarin worden de equivalentieklassen $K\ell(0)$, $K\ell(1)$,..., $K\ell(p-1)$ voorgesteld door de getallen $0,1,\ldots,p-1$, waarmee dan moet worden gerekend modulo p.

Voorbeeld 3. GF(5) heeft 5 elementen, voorgesteld door $GF(5) = \{0,1,2,3,4\}$, met optelling en vermenigvuldiging als volgt:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Voorbeeld 4. $GF(2) = \{0,1\}$ met

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Voorbeeld 5. GF(3) = (0,+,-) met

+	0	+	-
0	0	+	-
+	+	-	0
-	-	0	+

×	0	+	-
0	0	0	0
+	0	+	-
-	0	-	+

Hoofdstuk IV. Groepen

Literatuur:

[1] S.T.M. Ackermans - J.H. van Lint, Algebra en Analyse, Wolters-Noordhoff (1970).

[4] G. Birkhoff - S. MacLane, A survey of modern algebra, MacMillan (1948).

[5] A.I. Malcev, Groups and other algebraic systems, Mathematics, its content, methods, meaning, Vol. I, part 6, chapter 20, Amer. Math. Soc. (1963).

[6] W. Peremans, Syllabus Groepentheorie, T.H. Eindhoven.

4.1. Inleiding

Groepentheorie is ontstaan als "algebra van symmetrieën". Voorbeelden van symmetrieën zijn de spiegelingen (ten opzichte van een vlak, van een rechte, van een punt), de rotaties (om een punt, om een as), de translaties, en andere meetkundige regelmatigheden. Symmetrieën komen evenzeer voor in de algebra en in andere onderdelen van de wiskunde. De groepentheorie biedt een methode ter beschrijving van regelmatigheden, en wordt als zodanig in een aantal wetenschappen gebruikt.

Voorbeeld 1. Het vierkant heeft 8 symmetrieën: D_0, $D_{\frac{1}{2}\pi}$, D_π, $D_{3/2\pi}$, de draaiingen over 0°, 90°, 180°, 270°, resp., R_h, R_v, R_d, R_e, de reflecties om de horizontale, de verticale, en de beide diagonale assen.
In de verzameling van deze symmetrieën wordt de algebraïsche bewerking der vermenigvuldiging ingevoerd. Het product van twee symmetrieën is de symmetrie die wordt verkregen door ze na elkaar uit te voeren:

$$R_h D_{\frac{1}{2}\pi} = R_e \ , \quad D_{\frac{1}{2}\pi} R_h = R_d \ , \quad D_{\frac{1}{2}\pi}^2 = D_\pi \ .$$

Het product van twee symmetrieën is een symmetrie. Het product is niet onafhankelijk van de volgorde. De symmetrieën van het vierkant vormen een groep van de orde 8. De draaiingen vormen daarvan een ondergroep van de orde 4.

Voorbeeld 2. De veelterm $x_1^3 + 2x_2 + x_3^3 + 2x_4$ is symmetrisch in x_1, x_3 en ook in x_2, x_4. De eigenschappen van de veelterm zijn dezelfde onder de permutaties

$$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}.$$

De permutaties kunnen na elkaar worden uitgevoerd en hebben een product:

$$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}.$$

De permutaties vormen een groep van de orde 4.

Voorbeeld 3. $\{x \in \mathbb{C} \mid x^4 - 2x^2 + 9 = 0\} = \{i + \sqrt{2}, i - \sqrt{2}, -i + \sqrt{2}, -i - \sqrt{2}\}$. De wortels worden gepermuteerd onder de volgende symmetrieën van het complexe vlak:

$$S\begin{cases}\sqrt{2} \to -\sqrt{2}\\ i \to i\end{cases}, \quad T\begin{cases}\sqrt{2} \to \sqrt{2}\\ i \to -i\end{cases}, \quad ST\begin{cases}\sqrt{2} \to -\sqrt{2}\\ i \to -i\end{cases}, \quad I\begin{cases}\sqrt{2} \to \sqrt{2}\\ i \to i\end{cases}.$$

Deze symmetrieën vormen een groep van de orde 4, genaamd de Galois groep van de vergelijking.

Bovenstaande voorbeelden betreffen verzamelingen van symmetrieën, waarin bij elk tweetal symmetrieën een "productsymmetrie" behoort, met zekere eigenschappen. Voor het begrip groep behoeven wij ons echter niet te beperken tot verzamelingen waarvan de elementen symmetrieën zijn. Wij zullen meer algemeen beschouwen verzamelingen waarin bij elk tweetal elementen een element (hun product) behoort, met zekere eigenschappen.

Voorbeeld 4. De verzameling der vectoren van $\mathbb{R}_3$ wordt een groep, wanneer bij elk paar vectoren $\underline{a}$ en $\underline{b}$ als hun "product" wordt gedefinieerd de vector $\underline{a} + \underline{b}$.

4.2. Productoperatie

Een verzameling met productoperatie is een paar (V,φ) van een verzameling V en een afbeelding $\varphi: V \times V \to V$. Met andere woorden, aan elk geordend paar elementen $(a,b) \in V \times V$ wordt toegevoegd een element $\varphi(a,b) \in V$.

Voorbeeld 1. $(\mathbb{R},.)$. Hier is $V := \mathbb{R}$ en $\varphi(a,b) := a.b$, de gewone vermenigvuldiging.

Voorbeeld 2. $(\mathbb{R},+)$. Hier is $V := \mathbb{R}$ en $\varphi(a,b) := a+b$, de gewone optelling.

Voorbeeld 3. $(\mathbb{R}^2,+)$. Hier is $V := \mathbb{R}^2$ en $\varphi(\underline{a},\underline{b}) := \underline{a}+\underline{b}$, de optelling van vectoren.

Voorbeeld 4. (V,o). Hier is V de verzameling der reguliere lineaire afbeeldingen $\mathbb{R}^2 \to \mathbb{R}^2$, en $\varphi(\alpha,\beta) = \alpha \circ \beta$ de samengestelde afbeelding (eerst β, dan α).

Voorbeeld 5. $(\mathbb{R},\text{gemidd.})$. Hier is $V := \mathbb{R}$ en $\varphi(a,b) := \frac{1}{2}(a+b)$, het gemiddelde van a en b.

In de volgende definities schrijven wij ab in plaats van $\varphi(a,b)$; wij werken dus met $(V,)$.

Definitie. $(V,)$ heet commutatief, als $\forall_{a\in V} \forall_{b\in V} (ab = ba)$.
Voorbeelden 1, 2, 3 en 5 zijn commutatief, voorbeeld 4 niet.

Definitie. $(V,)$ heet associatief, als $\forall_{a\in V} \forall_{b\in V} \forall_{c\in V} ((ab)c = a(bc))$.
Voorbeelden 1, 2, 3 en 4 zijn associatief, voorbeeld 5 niet.

Definitie. $(V,)$ heeft een eenheid e, als $\exists_{e\in V} \forall_{a\in V} (ea = ae = a)$.
Voorbeelden 1, 2, 3 en 4 hebben een eenheid, namelijk resp. 1, 0, $\underline{0}$, identiteit. Voorbeeld 5 heeft geen eenheid.

Opmerking. Als er een eenheid is, dan is er één eenheid (bewijs!).

Definitie. In $(V,)$, voorzien van eenheid e, heeft $a \in V$ een inverse, als

$$\exists_{b \in V} \ (ab = ba = e) \ .$$

In voorbeelden 1, 2, 3 en 4 is de inverse van $a \neq 0$, a, $\underline{a}$, α resp. $\frac{1}{a}$, $-a$, $-\underline{a}$, α^{-1}. In voorbeeld 1 heeft 0 geen inverse.

4.3. Semigroepen

Een semigroep is een verzameling met productoperatie, die associatief is.

Voorbeeld 1. $(\mathbb{N},+)$ is een commutatieve semigroep. Er is geen eenheid.

Voorbeeld 2. $(\mathbb{N} \cup \{0\},+)$ is een commutatieve semigroep met eenheid 0. Merk op dat 3 geen inverse heeft.

Voorbeeld 3. $(\mathbb{N},.)$ is een commutatieve semigroep met eenheid 1. Merk op dat 3 geen inverse heeft.

Voorbeeld 4. Zij A een singuliere matrix. De verzameling van de machten van A, met de matrixvermenigvuldiging, is een commutatieve semigroep. Merk op dat I als eenheid kan worden genomen, maar dat er geen inversen zijn.

Voorbeeld 5. Zij V de verzameling van alle rijtjes van nullen en enen. Als productoperatie nemen wij de concatenatie, dat is, het aan elkaar plakken van rijtjes, bijvoorbeeld

$$(1,0,1,1,0,1,0,0) \circ (1,1,0,0,0) = (1,0,1,1,0,1,0,0,1,1,0,0,0) \ .$$

Dit geeft een semigroep die niet commutatief is. Het lege rijtje kan als eenheid worden genomen. Er zijn geen inversen.

4.4. Groepen

Een verzameling met productoperatie $(V,)$ heet een groep, wanneer geldt

G_1 : $(V,)$ is associatief,

G_2 : er is een eenheid,

G_3 : elk element van V heeft een inverse.

De groep heet Abels, wanneer hij commutatief is.

Voorbeelden van 4.2. Voorbeelden 2 en 3 zijn Abelse groepen, voorbeeld 4 is een niet-Abelse groep, voorbeelden 1 en 5 zijn geen groep.

Stelling. Zij $(G,)$ een groep, dan geldt

$$\forall_{a\in G}\, \forall_{b\in G}\, \exists!_{x\in G}(ax = b) \ , \quad \forall_{a\in G}\, \forall_{b\in G}\, \exists!_{y\in G}\, (ya = b) \ .$$

Bewijs. $a^{-1}b$ voldoet, want $a(a^{-1}b) = (aa^{-1})b = eb = b$.
Stel $ax = b = ax'$, dan $a^{-1}ax = a^{-1}ax'$, dus $ex = ex'$, dus $x = x'$.
Het bewijs van de tweede bewering gaat net zo.

Voorbeeld 1. $(\mathbb{R} \setminus \{0\},)$, met de gewone vermenigvuldiging, heet de multiplicatieve groep der reëlen $\neq 0$. De eenheid is 1. De getallen a en 1/a zijn elkaars inverse.

Voorbeeld 2. $(\mathbb{Q},+)$, met de gewone optelling, heet de additieve groep der rationale getallen. De eenheid is 0. De getallen a en -a zijn elkaars inverse.

Voorbeeld 3. Voor p priem is $(GF(p),+)$ een groep, met eenheid $K\ell(0)$, waarin $K\ell(a)$ en $K\ell(-a)$ elkaars inverse zijn.

Voorbeeld 4. Zij $p \in \mathbb{N}$. De complexe getallen

$$e^{\frac{2\pi i}{p}} \ , \ e^{\frac{4\pi i}{p}} \ , \ldots , \ e^{\frac{2\pi(p-1)i}{p}} \ , \ e^{2\pi i} \ ,$$

met de gewone vermenigvuldiging, vormen een groep, met eenheid $e^{2\pi i} = 1$,

waarin $e^{\frac{2\pi ki}{p}}$ en $e^{\frac{2\pi(p-k)i}{p}}$ elkaars inverse zijn.

Definitie. $(V,\times)$ en $(V',\star)$ zijn groepen. Een afbeelding $F : V \to V'$ heet een isomorfisme als

i) F is één-éénduidig op,

ii) $\forall_{a\in V}\, \forall_{b\in V}(F(a \times b) = F(a) \star F(b))$.

$(V,\times)$ en $(V',\star)$ heten isomorf, notatie $V \cong V'$, als er zo'n isomorfisme bestaat.

Definitie. $(V,\times)$ en $(V',*)$ zijn groepen. Een afbeelding $F : V \to V'$ heet een homomorfisme als

$$\forall_{a\in V}\,\forall_{b\in V}(F(a \times b) = F(a) * F(b)) .$$

$(V,\times)$ heet homomorf in (op) $(V',*)$, als er zo'n homomorfisme in (op) bestaat.

Voorbeeld 5. De voorbeelden 3 en 4 betreffen isomorfe groepen. Inderdaad, $F(x) := e^{\frac{2\pi ix}{p}}$ beeldt de equivalentieklassen mod p één-éénduidig af op de complexe getallen van voorbeeld 4, en er geldt

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

Ook de groep der draaiingen die de regelmatige p-hoek in zichzelf overvoert, is isomorf met de groepen van voorbeelden 3 en 4.

Voorbeeld 6. Noem $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. De groepen $(\mathbb{R}^+,\cdot)$ en $(\mathbb{R},+)$ zijn isomorf. Inderdaad, $\log : \mathbb{R}^+ \to \mathbb{R}$ is één-éénduidig op, en heeft de eigenschap $\log(a.b) = \log a + \log b$.

Voorbeeld 7. $(\mathbb{R}\setminus\{0\},\cdot)$ is homomorf op $(\mathbb{R}^+,\cdot)$. Inderdaad, $F(x) = |x|$, met $|x\cdot y| = |x|\cdot|y|$, voldoet.

Voorbeeld 8. Zij E de eenheidscirkel in het complexe vlak. $(\mathbb{R},+)$ is homomorf op $(E,\cdot)$, onder

$$F(x) = e^{2\pi ix} .$$

Voorbeeld 9. Zij V een vectorruimte, W een deelruimte, en $P : V \to W$ de projectie op deze deelruimte. $(V,+)$ is homomorf of $(W,+)$, onder de afbeelding P.

Voorbeeld 10. Een reguleire lineaire afbeelding A van een vectorruimte V is een isomorfisme van $(V,+)$ met zichzelf, daar

$$A(\underline{x} + \underline{y}) = A\underline{x} + A\underline{y} .$$

Een singuliere A is een homomorfisme van $(V,+)$ in zichzelf, en een homomorfisme van $(V,+)$ op (beeldruimte,+).

4.5. Eindige groepen

Definitie. Een groep (G,), waar G een eindige verzameling is, heet een eindige groep. Het aantal elementen van G heet de orde van de groep.

Voorbeeld 1. {e} is een groep als we definiëren ee = e.

Voorbeeld 2. {e,a} is een groep als we definiëren

ee = e, ea = ae = a, aa = e .

Voorbeeld 3. De op isomorfie na enige groep G = {e,a,b} is die met producttafel

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Voorbeeld 4. Er zijn, op isomorfie na, twee groepen van de orde 4. De producttafels zijn de volgende

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

De cyclische groep van orde 4

	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 viergroep van Klein

De eerste groep is isomorf met de groep van de draaiingen van het vierkant; de tweede groep is isomorf met de groepen van 4.1, voorbeelden 2 en 3.

Stelling. Zij (G,) een eindige Abelse groep van de orde n. Dan geldt

$$\forall_{a \in G} \; (a^n = e) \; .$$

Bewijs. Zij $G = \{a_1, a_2, \ldots, a_n\}$. Op grond van de vorige stelling is ook $\{aa_1, aa_2, \ldots, aa_n\} = G$, omdat al deze elementen verschillend zijn: uit $aa_i = aa_j$ volgt $a_i = a_j$. Dus geldt

$$a_1 a_2 \ldots a_n = aa_1 aa_2 \ldots aa_n \; ,$$

$$e = a^n \; .$$

Opmerking. In 4.8 zullen wij zien dat de voorgaande stelling geldt voor willekeurige (ook niet Abelse) eindige groepen van de orde n.

Definitie. Zij (G,) een groep. De orde van het element $a \in G$ is de kleinste positieve macht t zodat geldt $a^t = e$.

Stelling. De orde van een element van een eindige groep is een deler van de orde van de groep.

Bewijs. Schrijf $n = qt + r$, $0 \leq r < t$, dan

$$e = a^n = a^{qt}.a^r = (a^t)^q.a^r = e^q.a^r = ea^r = a^r \; .$$

Maar t was de kleinste positieve macht met $a^t = e$, dus $r = 0$ en $n = qt$.

Definitie. Een groep heet cyclisch, wanneer alle elementen kunnen worden geschreven als machten van één element.

Voorbeeld 5. Elke eindige Abelse groep met een priemgetal als orde is cyclisch.

Voorbeeld 6. Het eerste voorbeeld van voorbeeld 4 is cyclisch. Het tweede voorbeeld van voorbeeld 4 is niet cyclisch.

4.6. (Z mod n,+) en (Z mod n,.)

Zij n een natuurlijk getal.

Definitie.

$$\forall_{a\in\mathbb{Z}}\forall_{b\in\mathbb{Z}}((a \equiv b \bmod n) :\Longleftrightarrow (\exists_{v\in\mathbb{Z}}(a - b = nv))\ .$$

Congruentie mod n is een equivalentierelatie. Net als in 3.7 definiëren wij voor de equivalentieklassen een optelling en een vermenigvuldiging door

$$Kl(a) + Kl(b) := Kl(a + b)\ ,\quad Kl(a).Kl(b) := Kl(ab)\ .$$

Voorbeeld 1. Zij n = 6. Dan geldt:

$$Kl(4) + Kl(3) = Kl(1)\ ,\quad Kl(4).Kl(3) = Kl(0)\ .$$

De verzameling der equivalentieklassen modulo n duiden wij aan met Z mod n.

Stelling. $\forall_{n\in\mathbb{N}}$ ((Z mod n,+) is een Abelse groep).

Bewijs. Volgt uit de volgende eigenschappen van Z:

$a + b = b + a$, $(a + b) + c = a + (b + c)$, $a + nv \equiv a \pmod n$,

$a + (n - a) \equiv 0 \pmod n$.

Stelling. $\forall_{n\in\mathbb{N}}$ ((Z mod n,) is een commutatieve semigroep met eenheid).

Bewijs. Volgt uit de volgende eigenschappen van Z:

$$ab = ba\ ,\quad (ab)c = a(bc)\ ,\quad a\ 1 = a\ .$$

Voorbeeld 2. (Z mod 6,) is niet een groep, want er is geen x met $2x \equiv 1 \pmod 6$.

Stelling. Zij p een priemgetal. Dan is ($\mathbb{Z}$ mod p \ {0},) een groep.

Bewijs. Zij $a \not\equiv 0 \bmod p$. Voor $x \not\equiv y \bmod p$ geldt $ax \not\equiv ay \bmod p$, omdat $a(x - y) \equiv 0 \bmod p$ tengevolge heeft $x - y \equiv 0 \bmod p$. Daar dus alle ax verschillend zijn mod p, en er slechts p - 1 mogelijkheden zijn, heeft $ax \equiv 1 \bmod p$ een oplossing in $\mathbb{Z}$ mod p \ {0}.

Voorbeeld 3. (vergelijk 3.7, blz. 24). (GF(p),+) is een Abelse groep.

Voorbeeld 4. (GF(p) \ {0},) is een Abelse groep. Er geldt

$$\forall_{a \in GF(p)\setminus\{0\}} \; (a^{p-1} = 1) \; ,$$

m.a.w.

$$\forall_{a \not\equiv 0 \bmod p} \; (a^{p-1} \equiv 1 \bmod p) \; ,$$

de stelling van Fermat.

4.7. Permutatiegroepen

Zij $V = \{a_1, a_2, \ldots, a_n\}$ een eindige verzameling. Een permutatie van V is een één-éénduidige afbeelding van V op zichzelf. Wij duiden een permutatie aan door onder elkaar te schrijven de indices van de elementen van V en die van hun beelden.

Voorbeeld 1. De permutatie $a_1 \to a_3$, $a_2 \to a_2$, $a_3 \to a_4$, $a_4 \to a_1$ wordt aangeduid door

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} .$$

Het product $\rho \circ \sigma$ van de permutaties ρ en σ van V is de productafbeelding (eerst σ, dan ρ). Dit product is i.h.a. niet commutatief.

Voorbeeld 2.

$$\rho \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

$$\sigma \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Voorbeeld 3. De identieke permutatie ι, en de inverse ρ^{-1} van een permutatie ρ:

$$\iota = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

Stelling van Cayley. Elke eindige groep van de orde n is isomorf met een groep van permutaties van een verzameling van n elementen.

Bewijs. Zij $(G,)$ met $G = \{a_1, a_2, \ldots, a_n\}$ een groep. Aan $a \in G$ voegen wij toe de permutatie

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ aa_1 & aa_2 & \cdots & aa_n \end{pmatrix}.$$

Dan is aan $ab \in G$ toegevoegd het product van de permutaties die aan $a \in G$ en aan $b \in G$ zijn toegevoegd, wegens

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ aa_1 & aa_2 & \cdots & aa_n \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ ba_1 & ba_2 & \cdots & ba_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ aba_1 & aba_2 & \cdots & aba_n \end{pmatrix}.$$

Hieruit volgt dat de beschouwde permutaties een groep vormen, die isomorf is met $(G,)$.

Voorbeeld 4. De cyclische groep van de orde 4, zie 4.5, voorbeeld 4, kan worden opgevat als de groep der draaiingen van $\mathbb{R}_2$ die een vierkant invariant laten.

Voorbeeld 5. De viergroep van Klein, zie 4.5, voorbeeld 4, kan worden opgevat als de groep der spiegelingen van $\mathbb{R}_2$ (t.o.v. de x-as, t.o.v. de y-as, t.o.v. de oorsprong) die een rechthoek invariant laten.

Opmerking. Alle symmetrieën van het vierkant vormen een permutatiegroep van de orde 8. Alle permutaties van de verzameling van 4 elementen vormen een permutatiegroep van de orde 24.

De groep van alle permutaties van een verzameling van n elementen heeft de orde n!, en heet de symmetrische groep S_n.

De groep van alle even permutaties van een verzameling van n elementen heeft de orde $\frac{1}{2}n!$, en heet de alternerende groep A_n.

Opmerking. De permutatie

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$$

heet een even permutatie wanneer

$$\prod_{1 \le i < j \le n} (a_j - a_i) > 0 \ .$$

4.8. Ondergroepen

Zij (G,) een groep, en zij $H \subset G$. Wanneer (H,) zelf weer een groep is, dan heet (H,) een ondergroep van (G,).

Voorbeeld 1. $(\mathbb{Z},+)$ is een ondergroep van $(\mathbb{R},+)$.

Voorbeeld 2. $(\mathbb{R}^2,+)$ is isomorf met een ondergroep van $(\mathbb{R}^3,+)$.

Voorbeeld 3. $(GF(2),+)$ is niet een ondergroep van $(\mathbb{Z},+)$, omdat de bewerkingen + in beide groepen verschillen.

Stelling. Zij (G,) een groep; zij $H \neq \emptyset$ en $H \subset G$. Opdat (H,) een ondergroep is van (G,) is nodig en voldoende dat

$$\forall_{a \in H} \forall_{b \in H} (ab^{-1} \in H) .$$

Bewijs. De noodzakelijkheid is triviaal. We nemen nu aan dat de voorwaarde geldt, en bewijzen dat (H,) een groep is. De associativiteit geldt vanzelf. Het eenheidselement e van (G,) ligt in H, immers neem b = a. Met a en e ligt ook $ea^{-1} = a^{-1}$ in H, dus er is een inverse. Met a en b ligt ook $a(b^{-1})^{-1} = ab$ in H. Dit bewijst dat (H,) een groep, dus een ondergroep van G is.

Zij (G,) een groep, met ondergroep (H,). Definieer de relatie $\sim$ door

$$\forall_{x \in G} \forall_{y \in G}((x \sim y) :\Leftrightarrow (xy^{-1} \in H)) .$$

Dit is een equivalentierelatie wegens

$$xx^{-1} = e,\ yx^{-1} = (xy^{-1})^{-1},\ xy^{-1}yz^{-1} = xz^{-1} .$$

De equivalentieklasse van $a \in G$ is

$$\{x \in G \mid xa^{-1} \in H\} = \{ha \in G \mid h \in H\} ,$$

en wordt genoteerd met Ha. Merk op dat He = H.

Stelling (Lagrange). Voor een eindige groep G met ondergroep H geldt

$$(\text{orde } G) = (\text{orde } H) \times (\text{aantal equivalentieklassen}) .$$

Bewijs. Ha heeft evenveel elementen als H. Inderdaad, uit $h_1a = h_2a$ volgt $h_1 = h_2$. De equivalentieklassen hebben dus evenveel elementen. Hieruit volgt de bewering.

Stelling (Fermat). Voor een eindige groep G van de orde n geldt

$$\forall_{a \in G}(a^n = e) .$$

Bewijs. De verzameling van de machten van $a \in G$ vormt een cyclische ondergroep

$$H = \{a, a^2, \ldots, a^t = e\} \ , \quad t = \text{orde van } a \ .$$

Volgens de vorige stelling is t deelbaar op n. Omdat $a^t = e$ geldt ook $a^n = e$.

De stelling van Lagrange kan worden gebruikt bij eindige permutatiegroepen. Laat g en h permutaties zijn van een eindige verzameling Ω, en laat e de identieke permutatie zijn van Ω. Wij noteren het beeld van $\alpha \in \Omega$ onder g door α^g. Dan geldt voor alle $\alpha, \beta \in \Omega$:

$$\alpha^e = \alpha \ , \ (\alpha^g)^h = \alpha^{gh} \ , \ (\beta = \alpha^{g^{-1}}) \Leftrightarrow (\beta^g = \alpha) \ .$$

Zij G een groep van permutaties van Ω. De <u>stabilisator</u> G_α van $\alpha \in \Omega$ wordt gedefinieerd door

$$G_\alpha := \{g \in G \mid \alpha^g = \alpha\} \ .$$

De stabilisator G_α is een ondergroep van G omdat uit $\alpha^g = \alpha$, $\alpha^h = \alpha$ volgt $\alpha^{g^{-1}} = \alpha$, $\alpha^{gh} = \alpha$. Voor ons geval luidt de hierboven ingevoerde equivalentieregel

$$\forall_{g \in G} \forall_{h \in G} ((g \sim h) :\Leftrightarrow (gh^{-1} \in G_\alpha) \Leftrightarrow (\alpha^{gh^{-1}} = \alpha) \Leftrightarrow (\alpha^g = \alpha^h)) \ ,$$

dus $g, h \in G$ zijn equivalent wanneer zij α in hetzelfde beeld overvoeren. Er zijn dus evenveel equivalentieklassen als elementen in

$$\text{Baan}(\alpha) := \{\alpha^g \in \Omega \mid g \in G\} \ ,$$

De stelling van Lagrange levert dus:

<u>Stelling</u>. Zij G een permutatiegroep van een eindige verzameling Ω, en zij $\alpha \in \Omega$. Dan geldt

$$(\text{orde } G) = (\text{orde } G_\alpha) \quad (\text{aantal elementen in Baan}(\alpha)) \ .$$

Deze stelling wordt bijzonder eenvoudig in het geval dat G een <u>transitieve</u> permutatiegroep van Ω is, d.w.z. wanneer

$$\forall_{\alpha \in \Omega} \forall_{\beta \in \Omega} \exists_{g \in G} (\alpha^g = \beta) \ ,$$

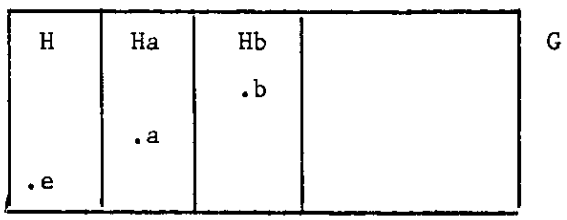
omdat dan $\text{Baan}(\alpha) = \Omega$.

Voorbeeld 4. De symmetriegroep van het regelmatig viervlak is S_4, de symmetrische groep op de 4 hoekpunten, van de orde 24. De ondergroep der symmetrieën, die een hoekpunt in zichzelf overvoeren, is S_3, de symmetrische groep op de 3 overige hoekpunten.

Voorbeeld 5. De symmetriegroep van de kubus heeft 8.6 = 48 elementen. Inderdaad, de symmetriegroep is transitief, en de stabilisator van een punt van de kubus is isomorf met S_3.

Voorbeeld 6. De symmetriegroep van de icosaeder heeft 12 × 10 = 120 elementen.

4.9. Normale ondergroepen



Wij vragen ons af of wij van de verzameling equivalentieklassen van de vorige § een groep kunnen maken door een geschikte vermenigvuldiging te definiëren. Dit is niet altijd het geval. De moeilijkheid is dat de gelijkheid $h_1ah_2b = hab$ niet steeds waar is. Deze moeilijkheid doet zich niet voor wanneer

$$\forall_{g\in G}\,\forall_{h\in H}\,\exists_{h'\in H}(gh = h'g) \ .$$

Definitie. Een ondergroep (H,) van (G,) heet een normale ondergroep wanneer

$$\forall_{g\in G}(gH = Hg) \ .$$

Voorbeeld 1. In een Abelse groep G is elke ondergroep H een normale ondergroep.

Voorbeeld 2. In de symmetrische groep S_3 wordt een niet-normale ondergroep gevormd door

$$\begin{pmatrix}1 & 2 & 3\\ & & \\ 1 & 2 & 3\end{pmatrix} \text{ en } \begin{pmatrix}1 & 2 & 3\\ & & \\ 2 & 1 & 3\end{pmatrix},$$

omdat

$$\begin{pmatrix}1 & 2 & 3\\ & & \\ 1 & 3 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ & & \\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ & & \\ 3 & 1 & 2\end{pmatrix},$$

maar

$$\begin{pmatrix}1 & 2 & 3\\ & & \\ 2 & 1 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ & & \\ 1 & 3 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ & & \\ 2 & 3 & 1\end{pmatrix}.$$

Zij (H,) een normale ondergroep van de groep (G,).

Definitie. De factorgroep (G/H,·) is de groep gevormd door de equivalentieklassen

$$\{Ha \mid a \in G\}$$

met de productoperatie

$$Ha \cdot Hb := Hab .$$

Inderdaad vormen de equivalentieklassen een groep, met eenheid H, terwijl Ha^{-1} als inverse van Ha optreedt.

Stelling. Zij (H,) een normale ondergroep van (G,). Dan is (G,) homomorf op (G/H,·).

Bewijs. Het verlangde homomorfisme is de afbeelding

$$\forall_{a \in G}(F(a) := Ha) ,$$

die voldoet wegens Hab = Ha·Hb .

Voorbeeld 3. (Z,+) is een Abelse groep. De zesvouden vormen een normale ondergroep H. De equivalentieklassen mod 6 vormen de factorgroep (Z/H,+), die isomorf is met (Z mod 6,+).

Voorbeeld 4. Zij (V,),met $V = \{a, a^2, a^3, a^4, a^5, a^6 = 1\}$ een cyclische groep van de orde 6. Hiervan is (W,) met $W = \{1, a^2, a^4\}$ een normale ondergroep.

De factorgroep V/W heeft de elementen W en aW.

Voorbeeld 5. De eenheidscirkel in het vlak is isomorf met de factorgroep $\mathbb{R}/\mathbb{Z}$.

Voorbeeld 6. De torus is isomorf met $\mathbb{R}^2/\mathbb{Z}^2$.

Voorbeeld 7. Zij $A_1A_2A_3A_4$ een regelmatig viervlak, en zijn k,ℓ,m de middenverbinders der overstaande ribben. De groep S_4 der symmetrieën van het viervlak heeft de orde 24. De groep S_3 der symmetrieën van de middenverbinders heeft de orde 6. De homomorfie van S_4 met S_3 wordt gedemonstreerd in de figuur. Inderdaad, de middenverbinders zijn invariant bij de volgende permuaties van de hoekpunten

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}.$$

Deze permutaties vormen een normale ondergroep van S_4, die isomorf is met de viergroep K_4 van Klein. De factorgroep van S_4 naar K_4 is S_3:

$$S_4/K_4 \cong S_3 .$$

Hoofdstuk V. Ringen en lichamen

5.1. Definities

Beschouw een verzameling V met twee productoperaties. Schrijf (V,+,.), noem de operatie + de opteloperatie en de operatie . de vermenigvuldigingsoperatie.

Definitie. (V,+,.) heet een ring wanneer is voldaan aan de volgende voorwaarden:

(V,+) is een commutatieve groep,
(V,.) is een semigroep,
$\forall_{a,b,c\in V}$ ((a + b).c = a.c + b.c, c.(a + b) = c.a + c.b).

Definitie. (V,+,.) heet een lichaam wanneer is voldaan aan de volgende voorwaarden:

(V,+) is een commutatieve groep,
(V \ {0},.) is een groep,
$\forall_{a,b,c\in V}$ ((a + b).c = a.c + b.c, c.(a + b) = c.a + c.b).

Het is duidelijk dat een lichaam een ring is. Omgekeerd echter is niet elke ring tevens een lichaam.

Voorbeeld 1. $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, met de gewone optelling en vermenigvuldiging, zijn lichamen.

Voorbeeld 2. ($\mathbb{Z}$,+,) is een ring, en geen lichaam.

Voorbeeld 3. De verzameling der 2 × 2 matrices, met de gewone matrixoptelling en matrixvermenigvuldiging, is een ring en geen lichaam.

Voorbeeld 4. ($\mathbb{Z}$ mod 6,+,) is een ring, en geen lichaam. Inderdaad, $2x \equiv 1 \pmod 6$ heeft geen oplossing.

Voorbeeld 5. Voor p priem is GF(p) een lichaam, vgl. 3.7.

Definitie. Een ring [lichaam] heet commutatief als zijn multiplicatieve semigroep [groep] commutatief is.

Stelling. In een lichaam $(V,+,\ )$ geldt

$$\forall_{a,b\in V}\ ((ab = 0) \Rightarrow ((a = 0) \vee (b = 0))) .$$

Bewijs. Stel we hebben $a \in V$ en $b \in V$ met

$$(ab = 0) \wedge (a \neq 0) \wedge (b \neq 0) .$$

Dan bestaat a^{-1}, en er volgt een contradictie wegens

$$0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b .$$

Voorbeeld 6. $(\mathbb{Z} \bmod 6,+,\cdot)$ is geen lichaam, want $2.3 \equiv 0 \pmod 6$.

Voorbeeld 7. $(\mathbb{Z},+,\ )$ is geen lichaam, maar een ring. De in de stelling genoemde eigenschap geldt echter wel.

Definitie. Zij $(R,+,\ )$ een ring en zij $\emptyset \neq I \subset R$. Dan heet I een ideaal in de ring als

$$\forall_{a\in I}\ \forall_{b\in I}\ (a - b \in I)$$

en

$$\forall_{a\in I}\ \forall_{r\in R}\ ((ar \in I) \wedge (ra \in I)) .$$

Voorbeeld 8. In $(\mathbb{Z},+,\ )$ vormen de zesvouden een ideaal.

Een ideaal is een deelring. Merk op dat $(I,+)$ een normale ondergroep van de commutatieve groep $(R,+)$ is. Wij kunnen uit een ring R en een bijbehorend ideaal I maken de factorring R/I, net zoals wij uit een groep G en een normale ondergroep H hebben gemaakt de factorgroep G/H.
Definieer de relatie $\sim$ door

$$\forall_{r\in R}\ \forall_{s\in R}\ ((r \sim s) :\Leftrightarrow (r - s \in I)) .$$

Dit is een equivalentierelatie wegens

$$r - r = 0 \in I,\ s - r = -1(r - s),\ r - s + s - t = r - t .$$

De equivalentieklasse van $r \in R$ is

$$\{x \in R \mid x - r \in I\} = \{r + i \mid i \in I\}$$

en wordt genoteerd $r + I$. Zonder veel moeite volgt:

Stelling. Zij I een ideaal in de ring $(R,+,\ )$. De equivalentieklassen $r + I$, met optelling en vermenigvuldiging volgens

$$(r + I) + (s + I) := r + s + I,\ (r + I)(s + I) := rs + I$$

vormen een ring, genaamde de factorring R/I.

Voorbeeld 9. Zij $R = (\mathbb{Z},+,.)$. Zij I het ideaal van alle n-vouden. Dan is

$$R/I = (\mathbb{Z} \bmod n,+,.)\ .$$

5.2. Eindige lichamen

Een eindig lichaam is een lichaam met eindig veel, zeg q, elementen ($q \geq 2$).

Voorbeeld 1. Zij p priem. Het Galois lichaam GF(p) heeft p elementen.

Zij F een eindig lichaam met q elementen. Zij 0 het nulelement, en zij 1 het eenheidselement. Omdat F eindig veel elementen heeft moeten in de oneindige rij

$$1,\ 1 + 1,\ 1 + 1 + 1,\ 1 + 1 + 1 + 1,\ldots$$

tenminste twee elementen dezelfde zijn, dus moet een veelvoud van 1 gelijk aan 0 zijn.

Definitie. De karakteristiek p van F is het kleinste natuurlijke getal zodat de som van p enen nul is (schrijf $p1 = 0$).

Stelling. De karakteristiek van een eindig lichaam is een priemgetal.

Bewijs. Stel $p = mn$ met $1 < m < p$, $1 < n < p$. Dan $0 = mn1 = m1.n1$. Hieruit volgt $m1 = 0$ of $n1 = 0$, hetgeen onmogelijk is.

Gevolg. De som van p elementen $b \in F$ is 0.

Bewijs. $b + b + \ldots + b = 1b + 1b + \ldots + 1b = (1 + 1 + \ldots + 1)b$.

Gevolg. Als $nb = 0$, $b \in F$, $n \in \mathbb{N}$, dan $b = 0$ of $n = p$ voud.

Bewijs. Voor $b \neq 0$, $n = pv + r$, $0 \leq r < p$, volgt $rb = 0$ dus $r = 0$.

Stelling. Het aantal elementen van een eindig lichaam is een macht van de karakteristiek.

Bewijs. Zij q het aantal elementen, en zij p de karakteristiek van het lichaam F. Schrijf $1 = b_1$, en beschouw

$$\{m_1 b_1 \mid m_1 = 0,1,2,\ldots,p-1\} .$$

Wanneer dit F is, dan is $q = p$, en wij zijn klaar. Zij

$$b_2 \neq m_1 b_1,\ b_2 \in F ,$$

en beschouw

$$\{m_1 b_1 + m_2 b_2 \mid m_1 = 0,1,2,\ldots,p-1,\ m_2 = 0,1,2,\ldots,p-1\} .$$

Wanneer dit F is, dan $q = p^2$, en wij zijn klaar. Zij

$$b_3 \neq m_1 b_1 + m_2 b_2,\ b_3 \in F ,$$

en beschouw

$$\{m_1 b_1 + m_2 b_2 + m_3 b_3 \mid m_i = 0,1,2,\ldots,p-1\} .$$

Zo doorgaande vinden wij eindig veel elementen $b_1, b_2, \ldots, b_k$ van F. De elementen

$$m_1 b_1 + m_2 b_2 + \ldots + m_k b_k$$

zijn verschillend, omdat b_ℓ geen lineaire combinatie is van $b_1, b_2, \ldots, b_{\ell-1}$. Daarom is p^k het aantal elementen van F.

In 5.4 zullen wij een eindig lichaam met p^k elementen construeren. Zonder bewijs delen wij mee:

Stelling. Elk eindig lichaam is commutatief.

Stelling. Op isomorfie na is er slechts één lichaam met p^k elementen, p priem, $k \in \mathbf{N}$.

Stelling. De multiplicatieve groep van een eindig lichaam met q elementen is cyclisch van de orde $q - 1$.

De laatste stelling kan ook als volgt worden geformuleerd. Elk eindig lichaam F met q elementen bevat tenminste één element ε, genaamd primitief element, zodat

$$F \setminus \{0\} = \{\varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^{q-1} = 1\} .$$

Voorbeeld 2. In GF(5) is 2 primitief element, omdat

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1 .$$

5.3. Polynoomringen

Zij F een commutatief lichaam. Beschouw de polynomen in x met coëfficiënten in F, bijvoorbeeld (neem $n \geq m$)

$$a(x) := a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 , \quad a_i \in F,\ a_n \neq 0 ,$$

$$b(x) := b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 , \quad b_i \in F,\ b_m \neq 0 .$$

Twee polynomen zijn dezelfde wanneer hun coëfficiënten van gelijke machten van x gelijk zijn. Wij definiëren

$$a(x) + b(x) := \sum_{i=0}^{n} (a_i + b_i) x^i ,$$

$$a(x) \cdot b(x) := \sum_{k=0}^{m+n} c_k x^k = \sum_{k=0}^{m+n} \sum_{i=0}^{k} a_i b_{k-i} x^k ,$$

$$0(x) := 0 ,$$

$$1(x) := 1 .$$

Onder deze definities wordt de verzameling der polynomen in x een ring, notatie $(F[x],+,.)$. Deze ring is geen lichaam, omdat de vergelijking

$$a(x).X(x) = b(x)$$

niet voor alle $a(x)$ en $b(x)$ oplosbaar is. Inderdaad, de gebroken veeltermen behoren niet tot $R = (F[x],+,.)$. Wel heeft de ring R de eigenschap dat

$$\text{uit } a(x).b(x) = 0 \text{ volgt } a(x) = 0 \text{ of } b(x) = 0 \ .$$

Zij $f(x)$ een polynoom van de graad k. Zij I het ideaal dat bestaat uit alle veelvouden van $f(x)$, dus

$$I = \{r(x)\cdot f(x) \mid r(x) \in R\} \ .$$

De quotiëntring R/I bestaat uit de veeltermen modulo $f(x)$, dus uit de veeltermen van de vorm

$$c_0 + c_1x + c_2x^2 + \ldots + c_{k-1}x^{k-1} \ , \quad c_i \in F \ .$$

Definitie. $f(x)$ heet irreducibel over F, wanneer $f(x)$ niet te schrijven is als product van twee veeltermen (met coëfficiënten in F) van lagere graad.

Voorbeeld 1. $x^2 + 1$ is irreducibel over $\mathbb{R}$.

Voorbeeld 2. $x^2 - x - 1$ is irreducibel over GF(3).

Voorbeeld 3. $x^4 + x + 1$ is irreducibel over GF(2).

5.4. $GF(p^k)$

Zij p priem. De polynomen met coëfficiënten in GF(p) vormen de ring

$$R = (GF(p)[x],+,.) \ .$$

Zij $f(x)$ een polynoom van de graad k, dat irreducibel is over GF(p). Zij I het ideaal van de veelvouden van $f(x)$. De quotiëntring R/I bestaat uit de polynomen van de vorm

$$c_0 + c_1x + c_2x^2 + \ldots + c_{k-1}x^{k-1}, \quad c_i \in GF(p) \ ,$$

met optelling en vermenigvuldiging mod p en mod f(x). Er zijn eindig veel, namelijk p^k, van zulke polynomen. Als a(x) zo'n polynoom is, en c(x) doorloopt de eindig vele polynomen van R/I, dan doorloopt a(x)c(x) eveneens de eindig vele polynomen van R/I. Inderdaad, zou $a(x)c(x) \equiv a(x)d(x) \bmod f(x)$, dan zou

$$a(x)(c(x) - d(x)) = r(x)f(x) .$$

Dit kan niet als f(x) irreducibel is.
Er volgt, dat voor gegeven b(x) en a(x), niet 0, er een c(x) is zodat

$$a(x)c(x) \equiv b(x) \bmod f(x) .$$

Hiermee is bewezen dat R/I een lichaam is, en wel een lichaam met p^k elementen. Wij noemen dit lichaam $GF(p^k)$, het Galois lichaam met p^k elementen.

Voorbeeld 1. $GF(3^2)$.
De veelterm $x^2 - x - 1$ is irreducibel over GF(3). De volgende veeltermen van de graad 1 over GF(3) stellen tesamen $GF(3^2) \setminus \{0\}$ voor.

$$x^0 = 1 \qquad x^5 = 2x$$
$$x^1 = x \qquad x^6 = 2 + 2x$$
$$x^2 = 1 + x \qquad x^7 = 2 + x$$
$$x^3 = 1 + 2x \qquad x^8 = 1 .$$
$$x^4 = 2$$

Voorbeeld 2. $GF(2^4)$.
De veelterm $x^4 + x + 1$ is irreducibel over GF(2). De volgende veeltermen van de graad 3 over GF(2) stellen tesamen $GF(2^4) \setminus \{0\}$ voor.

$$x^0 = 1 \qquad x^8 = 1 + x^2$$
$$x^1 = x \qquad x^9 = x + x^3$$
$$x^2 = x^2 \qquad x^{10} = 1 + x + x^2$$
$$x^3 = x^3 \qquad x^{11} = x + x^2 + x^3$$
$$x^4 = 1 + x \qquad x^{12} = 1 + x + x^2 + x^3$$
$$x^5 = x + x^2 \qquad x^{13} = 1 + x^2 + x^3$$
$$x^6 = x^2 + x^3 \qquad x^{14} = 1 + x^3$$
$$x^7 = 1 + x + x^3 \qquad x^{15} = 1 .$$

Hoofdstuk VI. Vectorruimten en grafen

6.1. Vectorruimten over GF(q)

Zij $q = p^r$ de macht van een priemgetal p.
$V(2,q) := GF(q) \times GF(q)$ is de verzameling der geordende paren (x,y) met $x \in GF(q)$ en $y \in GF(q)$. De lineaire algebra van V(2,q) heeft veel gemeen met de gewone lineaire algebra van $\mathbb{R}^2$. Er zijn echter ook verschillen, onder andere omdat V(2,q) slechts een eindig aantal punten bezit.

Voorbeeld 1. In V(2,5) bezit de rechte $\{(x,y) \mid y = 2x + 1\}$ vijf punten, namelijk (0,1), (1,3), (2,0), (3,2), (4,4).

Voorbeeld 2. In V(2,5) zijn er zes rechten door 0, namelijk $y = 0$, $y = x$, $y = 2x$, $y = 3x$, $y = 4x$, $x = 0$.

Een rechte in V(2,q) is gedefinieerd door

$$\{(x,y) \mid ax + by + c = 0\} ,$$

voor $a,b,c \in GF(q)$, waarbij $(a,b,c) \neq (0,0,0)$ en $(a,b,c) \neq (0,0,c)$ en waarbij $(\lambda a, \lambda b, \lambda c)$ dezelfde rechte aanduidt als (a,b,c).

Stelling. V(2,q) heeft q^2 elementen en $q(q + 1)$ rechten. Elke rechte heeft q punten, door elk punt gaan $q + 1$ rechten.

Bewijs. Er zijn q^2 geordende paren (x,y), met $x,y \in GF(q)$, dus q^2 punten in V(2,q). Er zijn $q^3 - 1$ geordende drietallen $(a,b,c) \neq (0,0,0)$, dus er zijn $q^2 + q + 1$ verschillende vergelijkingen $ax + by + c = 0$. Daar $a = b = 0$ geen rechte definieert, zijn er $q^2 + q$ verschillende rechten. Elke rechte $y = mx + n$ heeft q punten. Dit geldt ook voor elke rechte $ax + c = 0$. De laatste bewering volgt door tellen, omdat elk paar verschillende rechten ofwel één, ofwel geen punten gemeen heeft.

Voorbeeld 3. In V(2,5) geldt

$$\{(x,y) \mid x^2 + y^2 + 1 = 0\} = \{(0,2), (0,3), (2,0), (3,0)\} .$$

In de beide volgende stellingen beperken wij ons tot $q = p^r$, p priem, $p \neq 2$.

Stelling. GF(q) \ {0} bevat $\frac{1}{2}(q-1)$ kwadraten en $\frac{1}{2}(q-1)$ niet-kwadraten.

Bewijs. In GF(q) volgt uit $x^2 = y^2$ dat $(x-y)(x+y) = 0$, dus dat $x = y$ of $x = -y$, wegens 5.1. Voor $x \in GF(q) \setminus \{0\}$ zijn x en $-x$ verschillend, en geldt $(-x)^2 = x^2$. Hieruit volgt de stelling.

Definitie. GL(2,q) is de groep der niet-singuliere lineaire afbeeldingen $A : V \to V$, d.i. de groep der niet-singuliere 2×2 matrices over GF(q).

Stelling. GL(2,q) heeft orde $(q^2-1)(q^2-q)$.

Bewijs. Er zijn $(q^2-1)(q^2-q)$ geordende paren onafhankelijke vectoren $\underline{a}$ en $\underline{b}$ in V82,q). Kies een vaste basis $\{\underline{e}_1, \underline{e}_2\}$. Neem $A\underline{e}_1 = \underline{a}$ en $A\underline{e}_2 = \underline{b}$.

Opmerking. GL(2,5) telt 480 elementen, GL(2,2) telt er 6.

Stelling. In V(2,q) geldt, voor alle $a \neq 0$ en alle b, dat

$$\{(x,y) \mid ax^2 + b = y^2\} \neq \emptyset .$$

Bewijs. Als y doorloopt GF(q), dan is $1 + \frac{1}{2}(q-1) = \frac{1}{2}(q+1)$ het aantal elementen van GF(q) dat door y^2 wordt doorlopen. Als x doorloopt GF(q), dan doorloopt x^2, dus ook ax^2, dus ook $ax^2 + b$, eveneens $\frac{1}{2}(q+1)$ elementen van GF(q). In totaal zijn er q elementen in GF(q). Voor zekere x en voor zekere y zijn $ax^2 + b$ en y^2 dus gelijk.

Opmerking. Deze stelling is de basis voor de theorie der kegelsneden in V(2,q). Ook hier wijkt dus V(2,q) af van de theorie in $\mathbf{R}^2$.

$V(n,q) := (GF(q))^n$ is de verzameling der geordende n-rijen $(x_1, x_2, \ldots, x_n)$, met $x_i \in GF(q)$, $i = 1,2,\ldots,n$.

Voorbeeld 4. V(3,2) heeft 8 binaire vectoren, met coördinaten 0 of 1. Elke rechte heeft 2 punten. Er zijn 7 rechten en 7 vlakken door de oorsprong.

Voorbeeld 5. V(4,2) heeft 16 vectoren, 15 rechten door 0 en 15 hypervlakken door 0. Er zijn 35 vlakken door 0. Inderdaad, kies een vector $\neq \underline{0}$; dit kan op 15 manieren. Kies een tweede vector $\neq \underline{0}$; dit kan op 14 manieren. Echter 15×14 is $6 \times$ het aantal vlakken door 0.

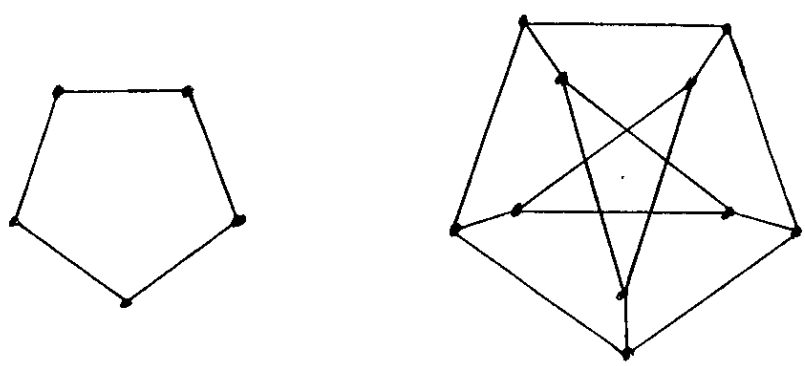
§ 6.2. Grafen

Definitie. Een *graaf* (Ω,E) is een verzameling Ω en een deel E van de verzameling $\Omega^{(2)}$ der ongeordende paren uit Ω.

Met andere woorden, een graaf is een verzameling van "hoekpunten", waarvan sommige paren "verbonden", en andere paren "niet verbonden" zijn. De verbindingen heten ook "ribben". Wij beperken ons tot eindige grafen, d.w.z. Ω is een eindige verzameling.

Grafen worden gebruikt bij electrische netwerken, transportnetwerken, chemische verbindingen, puzzles, spelletjes, kleuringsproblemen, toernooien, sociale relaties, marketing, groepentheorie, meetkunde, huwelijksproblemen, telefoonnetten, blokdiagrammen, prioriteitenschema's, hierarchieën, etc., etc.

Voorbeeld 1. De vijfhoeksgraaf en de Petersengraaf:



Een graaf op n hoekpunten wordt beschreven door zijn n × n *verbindingsmatrix* $A = [a_{ij}]$ met $a_{ii} = 0$, $a_{ij} = 1$ voor verbonden hoekpunten $i \neq j$, $a_{ij} = 0$ voor niet-verbonden hoekpunten $i \neq j$.

Voorbeeld 2. In de volgende verbindingsmatrices stelt I de eenheidsmatrix voor, en J de matrix bestaande uit louter énen:

$$A_5 \quad \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad A_{10} \quad \begin{bmatrix} A_5 & I_5 \\ I_5 & J_5 - I_5 - A_5 \end{bmatrix}.$$

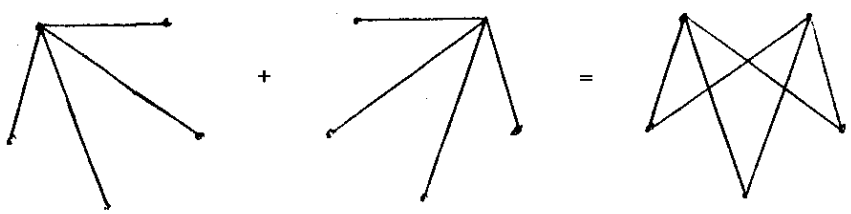
Een graaf op n hoekpunten kan ook worden voorgesteld door de karakteristieke functie van zijn ribbenverzameling, dus door een vector met $\frac{1}{2}n(n-1)$ coördinaten uit $\{0,1\}$.

Voorbeeld 3. De vijfhoeksgraaf en zijn complement worden voorgesteld door

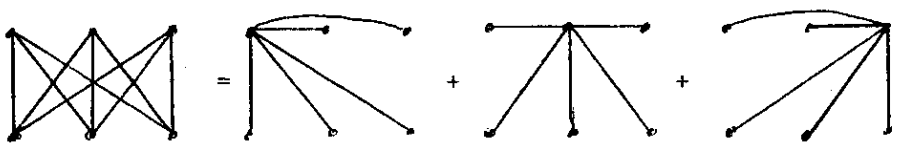
(1 0 0 1 1 0 0 1 0 1), resp. (0 1 1 0 0 1 1 0 1 0) .

De vectorruimte $V(\frac{1}{2}n(n-1),2)$ van dimensie $\frac{1}{2}n(n-1)$ over GF(2) stelt voor de verzameling van alle grafen op n hoekpunten. De optelling in $V(\frac{1}{2}n(n-1),2)$ vertaalt zich in de "optelling modulo 2" van grafen.

Voorbeeld 4.



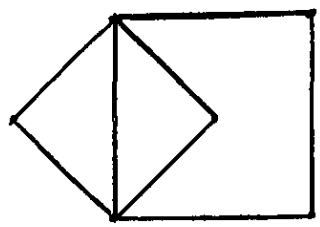
Voorbeeld 5.



Een *ster* is een graaf waarin één hoekpunt is verbonden met alle andere, onderling niet-verbonden, hoekpunten. Bij n punten behoren n sterren. De corresponderende vectoren van $V(\frac{1}{2}n(n-1),2)$ spannen een lineaire deelruimte P op. De vectoren van P corresponderen met de *volledige paargrafen:* verdeel de n punten in twee disjuncte deelverzamelingen A en B, en verbind elk punt van A met elk punt van B.

Een *Eulergraaf* is een graaf waarvoor het aantal verbindingen in elk hoekpunt even is. De mod 2 som van twee Eulergrafen is weer een Eulergraaf. Daarom vormen de met de Eulergrafen corresponderende vectoren van $V(\frac{1}{2}n(n-1),2)$ een lineaire deelruimte.

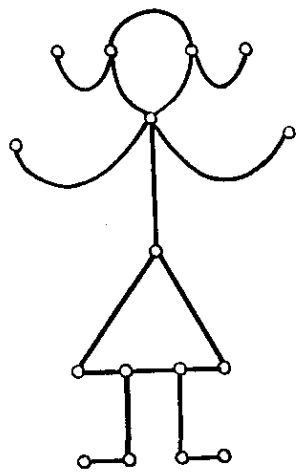
Voorbeeld van een Eulergraaf:

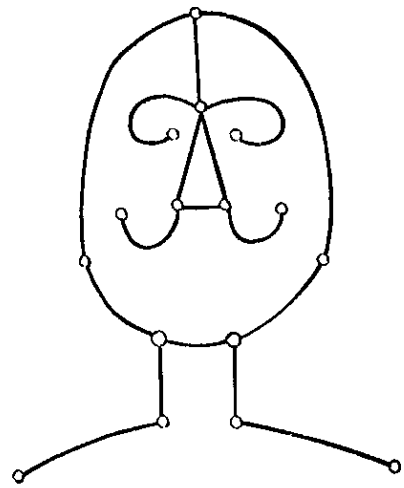


§ 6.3. Isomorfismen en automorfismen van grafen

Definitie. Twee grafen (Ω,E) en (Ω',E') heten *isomorf*, wanneer er een één-éénduidige afbeelding van Ω op Ω' bestaat die E in E' overvoert.

Voorbeeld 1. De volgende grafen zijn isomorf:





Definitie. Een *automorfisme* van een graaf (Ω,E) is een permutatie van Ω die E in zichzelf overvoert.

Een permutatie $g: \Omega \to \Omega$ is een één-éénduidige afbeelding van Ω op Ω. Deze permutatie is een automorfisme van (Ω,E) wanneer geldt:

$$\forall_{\alpha\in\Omega}\ \forall_{\beta\in\Omega}\ ((\{\alpha^g,\beta^g\} \in E) \Leftrightarrow (\{\alpha,\beta\} \in E)) \ .$$

Twee automorfismen g en h kunnen worden samengesteld tot $g \circ h$, dat weer een automorfisme is. De identiteit is een automorfisme. Hieruit volgt:

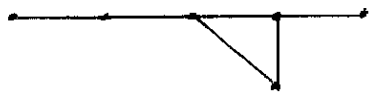
Stelling. De automorfismen van een graaf (Ω,E) vormen een groep, $\mathrm{Aut}(\Omega,E)$.

Het is duidelijk dat een graaf en zijn complement dezelfde automorfismengroep hebben.

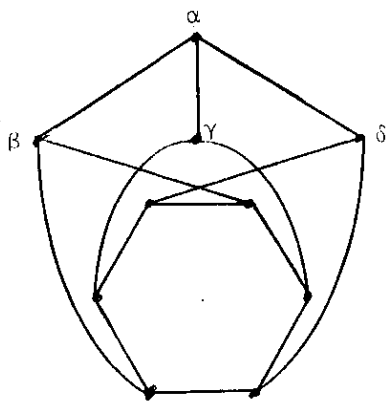
Voorbeeld 2. De vijfhoeksgraaf heeft 10 automorfismen. Dit kan men direct inzien, maar het volgt ook uit de stelling van Lagrange. Inderdaad, de automorfismengroep is transitief, en de stabilisator van een punt bevat 2 automorfismen.

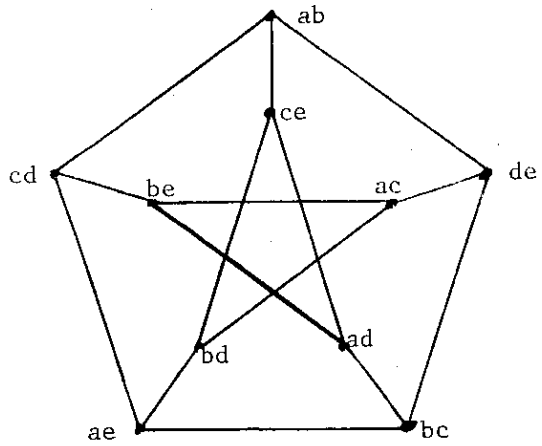
Voorbeeld 3. Elke graaf op $n \leq 5$ punten heeft meer dan één automorfisme.

Voorbeeld 4. De volgende graaf op 6 punten heeft slechts de identiteit als automorfisme:



Voorbeeld 5. De Petersengraaf heeft 120 automrofismen. Wij zullen dit op twee manieren aantonen.





Eerste methode, met gebruik van de stelling van Lagrange. Aut is transitief op de graaf, want elk punt is door een automorfisme over te voeren in elk ander. Wij bewijzen dat de stabilisator Aut_α van α de orde 12 heeft. Wij zien direct $3! = 6$ automorfismen, door de buren van α te permuteren. Er is echter behalve de identiteit nóg een automorfisme dat α, β, γ en δ in zichzelf overvoert, namelijk de antipodale spiegeling van de zeshoek. Daarom heeft Aut $10 \times 6 \times 2 = 120$ automorfismen.

Tweede methode: De hoekpunten van de Petersengraaf kunnen worden opgevat als de 10 ongeordende paren uit de verzameling van 5 symbolen {a,b,c,d,e}, waarbij twee paren verbonden worden als zij geen symbool gemeen hebben. Elke permutatie van {a,b,c d,e} geeft aanleiding tot een automorfisme van de graaf. Daarom geldt

$$\mathrm{Aut(Petersen)} \cong S_5 ,$$

met $5! = 120$ automorfismen.

Literatuur. R.J. Wilson, Introduction to graph theory, Oliver-Boyd (1972).

Hoofdstuk VII. Ordening

7.1. Partieel geordende verzamelingen

Een relatie op een verzameling V is een deel van $V \times V$. Een ordeningsrelatie, notatie $\geq$, is een relatie die de volgende eigenschappen bezit:

(1) $\quad \forall_{x \in V} \ (x \geq x)$,

(2) $\quad \forall_{x \in V} \forall_{y \in V} \forall_{z \in V} \ (((x \geq y) \wedge (y \geq z)) \Rightarrow (x \geq z))$,

(3) $\quad \forall_{x \in V} \forall_{y \in V} \ (((x \geq y) \wedge (y \geq x)) \Rightarrow (x = y))$.

Een partieel geordende verzameling (kort: poset) is een verzameling met een ordeningsrelatie. Soms stelt men een poset voor door een plaatje met de afspraak:

slechts (recht of schuin) verticaal verbonden elementen, en dezelfde elementen, staan in de relatie $\geq$;

hoger gelegen element $\geq$ lager gelegen element.

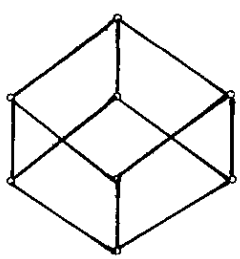


fig. 1

fig. 2

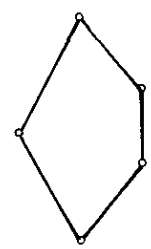


fig. 3

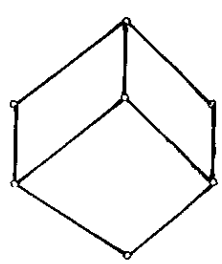


fig. 4

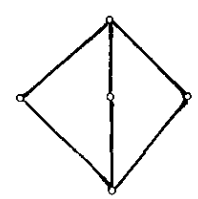


fig. 5

Een tralie (= lattice) is een poset waarin elk paar $x \in V$, $y \in V$ een grootste kleinere $x \cap y \in V$, en een kleinste grotere $x \cup y \in V$ heeft.

Opmerking. De notatie $\cap$ en $\cup$ is zo gekozen dat de huidige begrippen generalisaties zijn van de in hoofdstuk II behandelde doorsnede $\cap$ en vereniging $\cup$ van verzamelingen, zie 7.2, voorbeeld 2.

7.2. Voorbeelden

Voorbeeld 1. Neem $V = \mathbb{N}$ en definieer

$$\forall_{a\in\mathbb{N}} \forall_{b\in\mathbb{N}} ((a \geq b) :\Longleftrightarrow (a \text{ is deelbaar door } b)) .$$

Dit is een ordeningsrelatie. Blijkbaar geldt:

$$a \cap b = \text{ggd}(a,b) , \quad a \cup b = \text{kgv}(a,b) .$$

De delers van het getal 30 worden voorgesteld door figuur 1. De delers van het getal 8 worden voorgesteld door figuur 2.

Voorbeeld 2. Zij V de verzameling van de deelverzamelingen van een universum U. Definieer

$$\forall_{A\in V} \forall_{B\in V} ((A \geq B) :\Longleftrightarrow (A \supset B)) .$$

Dit is een ordeningsrelatie. Blijkbaar is $A \cap B$ de doorsnede, en $A \cup B$ de vereniging van A en B.

Voorbeeld 3. Zij V de verzameling van de convexe deelverzamelingen van $\mathbb{R}^2$. Definieer

$$\forall_{A\in V} \forall_{B\in V} ((A \geq B) :\Longleftrightarrow (A \supset B)) .$$

Dit is een ordeningsrelatie. In dit voorbeeld is $A \cap B$ de doorsnede, en $A \cup B$ het convexe omhulsel van A en B.

Voorbeeld 4. Zij $V = \mathbb{R}$ en zij $\geq$ de relatie "groter dan of gelijk aan". Dit is een ordeningsrelatie. De getallen 1, 3, 25 en 87 in deze relatie worden voorgesteld door figuur 2.

Voorbeeld 5. Zij V de verzameling van de lineaire deelruimten van een gegeven vectorruimte. Zij $\geq$ de relatie "bevatten als deelruimte". Dit is een ordeningsrelatie. In figuur 1 worden voorgesteld de oorsprong 0, drie onafhankelijke rechten door 0, de drie door de paren der rechten opgespannen vlakken, de door de rechten opgespannen ruimte. In figuur 5 worden voorgesteld drie verschillende rechten door 0 in een vlak.

Voorbeeld 6. Zij V de verzameling van de punten, de rechten, de vlakken van de Euclidische ruimte, en de lege verzameling. Zij $\geq$ de relatie "bevatten". Dit is een ordeningsrelatie. In figuur 3 wordt het axioma van Euclides voorgesteld: in een vlak, door een punt buiten een rechte, gaat één rechte, die met de gegeven rechte niets gemeen heeft. In figuur 4 worden voorgesteld twee evenwijdige rechten in een vlak, gesneden door een derde rechte.

Voorbeeld 7. Zij V de verzameling der reële functies op $\mathbb{R}$. Laat $f \geq g$ betekenen

$$\forall_{x \in \mathbb{R}} \; (f(x) > g(x)) \; .$$

Dit is een ordeningsrelatie. Voor de functies e en f zijn de functies $e \cup f$ en $e \cap f$ bepaald door

$$\forall_{x \in \mathbb{R}} \; ((e \cup f)(x) = \max(e(x),f(x)), \; (e \cap f)(x) = \min(e(x),f(x)) \; .$$

Voorbeeld 8. Zij V de verzameling van de ondergroepen van een groep. Laat $\geq$ betekenen: "bevatten als ondergroep". Dit is een ordeningsrelatie. In figuur 5 worden voorgesteld de groep van Klein $\{e,a,b,c\}$, en de ondergroepen $\{e,a\}$, $\{e,b\}$, $\{e,c\}$, $\{e\}$.

Voorbeeld 9. Zij V de verzameling der punten van $\mathbb{R}^2$. Zij $\geq$ gedefinieerd door

$$((a_1,a_2) \geq (b_1,b_2)) :\Leftrightarrow ((a_1 > b_1) \vee ((a_1 = b_1) \wedge (a_2 \geq b_2)))$$

waarin $>$ de gewone ordening van $\mathbb{R}$ is. Deze lexicografische ordening is een ordeningsrelatie.

7.3. Tralies

In 7.1 werd de definitie, en in 7.2 werd een aantal voorbeelden van tralies gegeven. In een tralie $(V,\geq)$ wordt het verband tussen de ordeningsrelatie $\geq$, de grootste kleinere $\cap$, en de kleinste grotere $\cup$ gegeven door

$$\forall_{x\in V}\,\forall_{y\in V}\,((x \geq y) \Longleftrightarrow (x \cap y = y) \Longleftrightarrow (x \cup y = x)) .$$

Figuur 3 en figuur 5 tonen aan dat niet in elke tralie geldt:

$$\forall_{x,y,z\in V}\,((x \cup (y \cap z) = (x \cup y) \cap (x \cup z)) \wedge (x \cap (y \cup z) =$$

$$= (x \cap y) \cup (x \cap z))) .$$

Wanneer deze eigenschap wel geldt, dan heet het tralie distributief, zie figuur 1.

Voorbeeld 4 en voorbeeld 7 (van 7.2) tonen aan dat niet in elke tralie geldt:

$$\exists_{I\in V}\,\forall_{x\in V}\,(I \geq x) , \quad \exists_{0\in V}\,\forall_{x\in V}\,(x \geq 0) ,$$

met andere woorden, dat niet elk tralie een grootste element I en een kleinste element 0 heeft.

Een gecomplementeerd tralie is een tralie met grootste en kleinste element, waarin bovendien geldt:

$$\forall_{x\in V}\,\exists_{x^*\in V}\,((x \cup x^* = I) \wedge (x \cap x^* = 0)) .$$

In figuur 4 en figuur 2 bestaat wel een grootste en een kleinste element, maar het betreffende tralie is niet gecomplementeerd. Voorbeelden 1, 2, 5 en 6 (van 7.2) betreffen gecomplementeerde tralies.

7.4. Boole algebra's en Boole ringen

Een Boole algebra is een tralie dat distributief en gecomplementeerd is.

Voorbeeld 1. Figuur 1 betreft een Boole algebra, figuren 2, 3, 4 en 5 niet.

Voorbeeld 2. De deelverzamelingen van een universum U, met $\supset$ als ordeningsrelatie, vormen een Boole algebra. Inderdaad, de doorsnede $\cap$ en de vereniging $\cup$ voldoen aan de distributieve wet; er is een grootste U en een kleinste $\emptyset$; elke deelverzameling A heeft een complement A^* dat voldoet aan $A \cap A^* = \emptyset$, $A \cup A^* = U$.

Zij $(V,\geq)$ een Boole algebra. Definieer een optelling en een vermenigvuldiging door

$$\forall_{a\in V} \forall_{b\in V} (a + b := (a \cap b^*) \cup (b \cap a^*) , \quad ab := a \cap b) .$$

De verkregen $(V,+,)$ is een commutatieve ring, waarin I het eenheidselement, en 0 het nulelement is, en waarin $a + a = 0$. Inderdaad, de ringeigenschappen gelden wegens (onder andere)

$$a + 0 = (a \cap I) \cup (0 \cap a^*) = a, \quad a.I = a \cap I = a ,$$

$$ab + ac = (a \cap b \cap (a^* \cup c^*)) \cup (a \cap c \cap (a^* \cup b^*)) =$$

$$= (a \cap b \cap c^*) \cup (a \cap c \cap b^*) =$$

$$= a \cap ((b \cap c^*) \cup (c \cap b^*)) = a(b + c) .$$

De ring $(V,+,)$ heeft bovendien de eigenschap dat elk element idempotent is, dat is, dat

$$\forall_{a\in V} (a^2 = a)$$

geldt.

Een ring met eenheidselement, waarin elk element idempotent is, heet een Boole ring.
Wij hebben dus bewezen:

Stelling. Zij $(V,\geq)$ een Boole algebra. Onder

$$\forall_{a\in V} \forall_{b\in V} (a + b := (a \cap b^*) \cup (b \cap a^*) , \quad ab := a \cap b)$$

is $(V,+,)$ een Boole ring.

Uit een Boole ring is omgekeerd een Boole algebra te verkrijgen, wegens

Stelling. Zij $(V,+,\ )$ een Boole ring. Onder

$$\forall_{a\in V}\ \forall_{b\in V}\ (a \cap b := ab,\ a \cup b := a + b + ab,\ \ a^* := I + a)$$

is $(V,\cap,\cup,*)$ een Boole algebra.

Bewijs door verificatie.

Voorbeeld 4. $(GF(2))^4$ is de verzameling der 4-rijtjes van nullen en enen uit GF(2). De 4-rijtjes vormen een Boole ring onder de componentgewijze optelling en vermenigvuldiging mod 2:

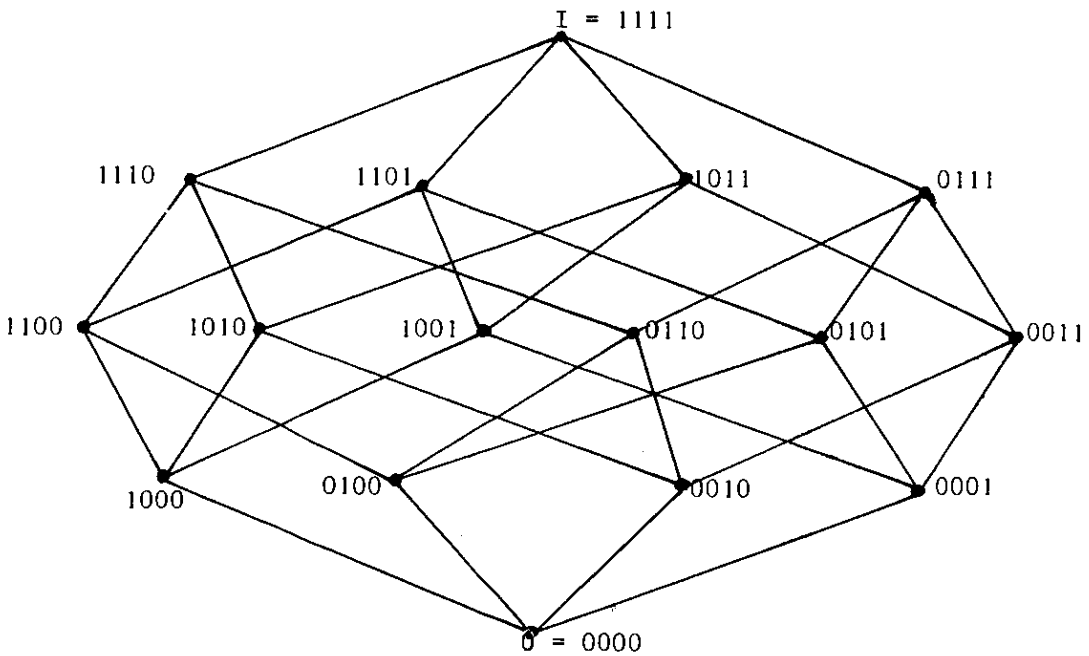
$$a = (1,1,0,0),\ b = (1,0,1,0),\ a + b = (0,1,1,0),\ ab = (1,0,0,0)\ .$$

Merk op dat inderdaad geldt $a^2 = a$ en $a + a = 0$, met

$$0 = (0,0,0,0)\ ,\quad I = (1,1,1,1)\ .$$

$(GF(2))^4$ is ook een Boole algebra, met

$$a \cup b = (1,1,1,0),\ a \cap b = (1,0,0,0),\ a^* = (0,0,1,1),\ b^* = (0,1,0,1)\ .$$



Voorbeeld 5. $(GF(2))^n$, de verzameling der n-rijtjes van nullen en enen uit GF(2), is een Boole ring onder de componentgewijze mod 2 optelling en vermenigvuldiging:

$$a + b := (a_1 + b_1, \ldots, a_n + b_n), \quad ab := (a_1b_1, \ldots, a_nb_n) \bmod 2 ,$$

voor $a = (a_1,\ldots,a_n)$ en $b = (b_1,\ldots,b_n)$. Ook is $(GF(2))^n$ een Boole algebra, onder

$$(a \geq b) :\Leftrightarrow \forall_{1\leq i\leq n} (a_ib_i = b_i)$$

met

$$a^* = (1 + a_1, \ldots, 1 + a_n), \quad a \cap b = (a_1b_1, \ldots, a_nb_n) ,$$

$$a \cup b = (a^* \cap b^*)^* = (a_1 + b_1 + a_1b_1, \ldots, a_n + b_n + a_nb_n) .$$

Voorbeeld 6. Zij $P = (p_1,\ldots,p_n)$ een verzameling van n elementen. De verzameling V der deelverzamelingen van P heeft 2^n elementen. V is een Boole algebra onder de relatie $\subset$, bevatten.
V is een Boole ring onder de bewerkingen

$$AB = A \cap B, \quad A + B = A \div B .$$

Opmerking. De voorbeelden 5 en 6 zijn isomorf. Inderdaad, $(GF(2))^n$ is te beschouwen als de verzameling der karakteristieke functies van de deelverzameling van P.

Stelling. Een eindige Boole algebra [Boole ring] is isomorf met de Boole algebra [Boole ring] der deelverzamelingen van een eindige verzameling.

Zie [1], p. 160, voor het bewijs van deze stelling. De stelling spreekt uit dat de voorbeelden 5 en 6 niet slechts voorbeelden zijn, maar representatief zijn voor de eindige Boole algebra's. Een gevolg is, dat het aantal elementen van een eindige Boole algebra [Boole ring] een macht van 2 is, en dat eindige Boole algebra's [Boole ringen] eenvoudig te beschrijven zijn met n-rijtjes van nullen en enen uit GF(2).

Opmerking. Ook de propositielogica kan worden geïnterpreteerd als Boole algebra. Beschouw de beweringsveranderlijken $p_1,\ldots,p_n$. Zij W de verzameling van alle predicaten die uit $p_1,\ldots,p_n$ kunnen worden opgebouwd met de bewerkingen $\wedge$, $\vee$, $\neg$. Twee predicaten L en R heten gelijkwaardig wanneer $L \leftrightarrow R$ altijd waar is (voor elke substitutie voor $p_1,\ldots,p_n$). Dit is een equivalentierelatie op W. De verzameling V van alle equivalentieklassen, voorzien van de bewerkingen $\wedge$, $\vee$, $\neg$, is isomorf met de Boole algebra genoemd in de voorbeelden 5 en 6. Voor het bewijs zie [1], p. 158. Vergelijk ook Hoofdstuk I.

Opgaven Verzamelingsleer

Hoofdstuk 1: Logica

Bewijs dat de volgende propositievormen tautologiëen zijn.

1. $((p \vee q) \vee r) \Longleftrightarrow (p \vee (q \vee r))$.

2. $((p \vee q) \wedge r) \Longleftrightarrow ((p \wedge r) \vee (q \wedge r))$.

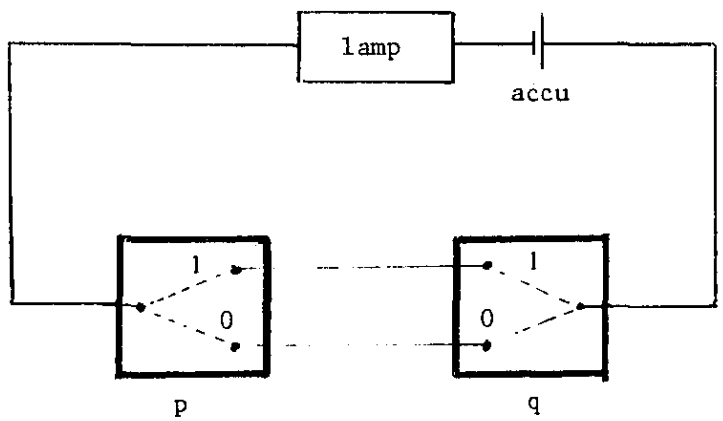
3. $(p \wedge (p \Rightarrow q)) \Longleftrightarrow (p \wedge q)$.

4. $(\neg(p \wedge q)) \Longleftrightarrow (\neg p \vee \neg q)$.

5. $(p \wedge (p \Rightarrow q)) \Rightarrow q$.

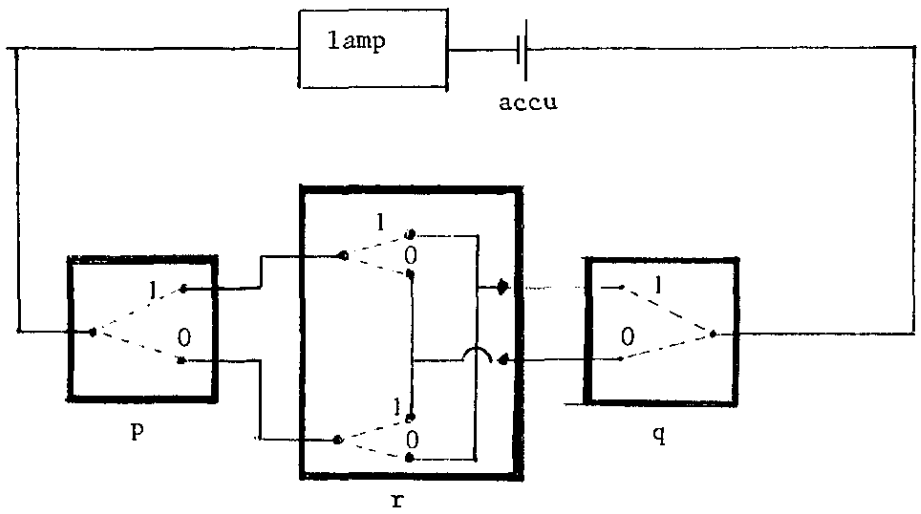
Elektrische schakelingen (opgaven 6 en 7).
Een schakeling bevat, behalve een spanningsbron en een lamp, enige schakelaars.
Afspraak: de schakeling heet "waar" als de lamp brandt.
De schakelaars p, q en r hebben elk twee standen: waar en onwaar, corresponderend met 1 of 0.
p en q hebben 1 ingang en 2 uitgangen, terwijl de schakelaar r twee ingangen heeft, maar 4 uitgangen, die gedeeltelijk met elkaar verbonden zijn.

6.



Bepaal de propositievorm, behorend bij deze hotelschakeling.

7.



Bepaal de propositievorm, behorend bij deze drievoudige hotel-schakeling.

In de opgaven 8 t/m 12 is U de totaliteit der reële getallen. Onderzoek voor welke waarde(n) van de variabele(n) de predicaten (of combinaties van predicaten) waar of onwaar zijn.

8. $P(x) :\Leftrightarrow (x-2)(x-3) = x^2 - 5x + 6$.

9. $P(x) :\Leftrightarrow (x-2)(x-3) = x^2 + x - 6$.

10. $P(x,y) :\Leftrightarrow x + y = 3$
    $Q(x,y) :\Leftrightarrow 3x - y = 5$
    } onderzoek $P(x,y) \wedge Q(x,y)$.

11. $P(x) :\Leftrightarrow x > 0$
    $Q(x) :\Leftrightarrow x \leq 3$
    } onderzoek: a) $P(x) \wedge Q(x)$
    b) $P(x) \vee Q(x)$.

12. $P(x) :\Leftrightarrow 0 \leq x \leq 3$; $Q(x) :\Leftrightarrow 1 \leq x \leq 5$

    Onderzoek: a) $P(x) \wedge Q(x)$
    b) $P(x) \vee Q(x)$
    c) $P(x) \Leftrightarrow Q(x)$
    d) $P(x) \Rightarrow Q(x)$.

13. Maak met behulp van quantoren de predicaten uit opgave 8 respectievelijk 9 tot ware beweringen.

Onderzoek of de beweringen in opgave 14 t/m 17 waar dan wel onwaar zijn.

14. a) $\forall_{x\in\mathbb{R}} \exists_{y\in\mathbb{R}} (x^2 > y)$

    b) $\exists_{x\in\mathbb{R}} \forall_{y\in\mathbb{R}} (x^2 > y)$

    c) $\forall_{y\in\mathbb{R}} \exists_{x\in\mathbb{R}} (x^2 > y)$

    d) $\exists_{y\in\mathbb{R}} \forall_{x\in\mathbb{R}} (x^2 > y)$

15. $\forall_{x\in\mathbb{R}} \forall_{y\in\mathbb{R}} ((x+y=3) \Rightarrow (2=3))$.

16. $\forall_{x\in\mathbb{R}} ((x^2>x) \Leftrightarrow ((x>1) \vee (x<0)))$.

17. $\forall_{a\in\mathbb{R}} \forall_{b\in\mathbb{R}} ((\exists_{x\in\mathbb{R}} (x^2 + ax + b = 0)) \Leftrightarrow (a^2 - 4b \geq 0))$.

18. Schrijf de volgende bewering met behulp van quantoren: "Er is geen grootste reëel getal".

19. Schrijf de bewering $\exists!_{x\in U}(P(x))$ zonder ! teken.

Hoofdstuk II: Verzamelingen

In onderstaande opgaven zijn alle verzamelingen deelverzamelingen van het universum U (tenzij anders vermeld).

Bewijs met behulp van waarheidstabellen:

1. $(A \cup B)^* = A^* \cap B^*$ en $(A \cap B)^* = A^* \cup B^*$.

2. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Bewijs met behulp van de eigenschappen der bewerkingen:

3. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

4. $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

5. $A \cap (B \setminus C) = (A \cap B) \setminus C$.

6. $((A \setminus B) \setminus C) \subset (A \setminus (B \setminus C))$.

7. Als $C \subset A$ èn $C \subset B$ dan $C \subset (A \cap B)$.

8. $A := \{0,1,2,3,4,5,6,7\}$.
   $B := \{1,3,5,7,8,9,10\}$.
   $C := \{0,2,4,6,8,10,12\}$.
   Bepaal: $(A \setminus B) \setminus C$; $A \setminus (B \setminus C)$;
   $A \cap B$; $(A \cap B) \cup C$;
   $(A \cup C) \cap (B \cup C)$; $A \div B$.

9. Bepaal $\{x \in \mathbb{R} \mid ((x-1)(x+2) = 0) \wedge (x \geq 0)\}$.
   Bepaal $\{x \in \mathbb{R} \mid x^2 + x + 1 = 0\}$.

10. De verzameling E der even positieve getallen wordt aldus geschreven:
    a) $E = \{x \in \mathbb{R} \mid (x = 2n) \wedge (n \in \mathbb{N})\}$.
    b) $E = \{2x \in \mathbb{R} \mid x \in \mathbb{N}\}$.
    c) $E = \{x \in \mathbb{R} \mid (x:2) \in \mathbb{N}\}$.

    Welke van de drie schrijfwijzen is fout? Verbeter de notatie.

11. Schrijf met behulp van de verzamelingsnotatie de rechte in R^2 die door de punten (0,1) en (2,0) gaat.

12. a) Schrijf met behulp van de verzamelingsnotatie de cirkel (in R^2) met middelpunt (a,b) en straal r.
    b) Schrijf met behulp van de verzamelingsnotatie de cirkels die straal r hebben.
    c) Schrijf met behulp van de verzamelingsnotatie alle cirkels.

13. S is de verzameling der vierhoeken.
    P " " " " parallellogrammen.
    L " " " " ruiten.
    R " " " " rechthoeken.
    V " " " " vierkanten.

    Ga na of de volgende beweringen waar dan wel onwaar zijn:

    a) $R \subset P$

    b) $L \supset P$

    c) $S \subset V$

    d) $L \setminus R = L \cap R$.

14. U is het universum; $A := \{x \in U \mid A(x)\}$; $B := \{x \in U \mid B(x)\}$.
    Er zijn "vertalingen" mogelijk van predicaten met A(x) en B(x) in de taal der verzamelingen.
    Onderzoek de onderstaande vertalingen op juistheid:

    a) $\forall_{x \in U}(A(x) \Rightarrow B(x))$; $A \subset B$

    b) $\forall_{x \in U}(A(x) \Leftrightarrow B(x))$; $A = B$

    c) $\nexists_{x \in U}(A(x) \Leftrightarrow B(x))$; $(A : B) \neq U$.

15. Vertaal de volgende zin:
    "Opdat x positief is, is het niet voldoende dat x^2 positief is." .

16. Schets $\{(x,y \in \mathbb{R}^2 \mid (x \neq 0) \Rightarrow \forall_{n \in \mathbb{N}}(-n|x| \leq y + |x| \leq 0)\}$.

Hoofdstuk III: Afbeeldingen en relaties

1. Bewijs de volgende eigenschappen van het Cartesisch produkt:
   a) $U \times (V \cap W) = (U \times V) \cap (U \times W)$
   b) $U \times (V \cup W) = (U \times V) \cup (U \times W)$.

2. Als $U := V \cap W$, bewijs dan:
   a) $U \times U = (V \times V) \cap (W \times W)$
   b) $U \times U = (V \times W) \cap (W \times V)$.

3. V is een verzameling en P(V) is de verzameling van alle deelverzamelingen. Onderzoek of de volgende uitspraak juist is:

$$\forall_{A \in P(V)} \forall_{B \in P(V)} ((A \times B = B \times A) \iff (A = B)).$$

4. $A := \{1,2,3,4\}$; $B := \{1,2,3\}$.
   Zij F een deelverzameling van $A \times B$, gegeven door:

$$F = \{(1,1), (2,1), (3,2), (4,3)\}.$$

   a) Bewijs dat F een afbeelding van A in B is.
   b) Is de afbeelding op?
   c) Is de afbeelding één-éénduidig?
   d) Bepaal $F^{\leftarrow}(\{1\})$.

5. l en m zijn rechten in het platte vlak. Aan elk punt P van l voegt men zijn orthogonale projectie op m toe. Onder welke voorwaarde is deze toevoeging een één-éénduidige afbeelding van l op m en wat is dan de inverse?

6. Schets de volgende deelverzamelingen van $\mathbb{R}^2$ en onderzoek welke afbeeldingen van $\mathbb{R}$ in $\mathbb{R}$ zijn:
   a) $\{(x,x+1) \mid x \in \mathbb{R}\}$
   b) $\{(x,x^2) \mid x \in \mathbb{R}\}$
   c) $\{(x,\sqrt{x^2+1}) \mid x \in \mathbb{R}\}$
   d) $\{(x,y) \in \mathbb{R}^2 \mid |x+y| = 1\}$
   e) $\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 = 1\}$.

7. Onderzoek of de volgende deelverzamelingen van $\mathbb{R}^2$ afbeeldingen zijn van $\mathbb{R}$ in $\mathbb{R}$:
   a) $\{(x^3,x) \mid x \in \mathbb{R}\}$
   b) $\{(x^2,x) \mid x \in \mathbb{R}\}$

8. Voor een vaste $\underline{a} \in \mathbb{R}^2$ wordt de afbeelding $T_{\underline{a}} : \mathbb{R}^2 \to \mathbb{R}^2$ aldus gedefinieerd:

$$\forall_{\underline{x} \in \mathbb{R}^2} \ (T_{\underline{a}} \ \underline{x} = \underline{x} + \underline{a}).$$

a) Bewijs dat $T_{\underline{a}}$ één-éénduidig en op is.

b) Bewijs dat $T_{\underline{a}}^{-1} = T_{-\underline{a}}$.

9. A is een lineaire afbeelding: $\mathbb{R}^2 \to \mathbb{R}^2$, gegeven door:

$$A \binom{1}{0} = \binom{-1}{-2} \quad \text{en} \quad A \binom{0}{1} = \binom{2}{4} .$$

a) is A één-éénduidig?

b) Bepaal $A^{\leftarrow}(\{\binom{3}{6}\})$.

10. Een afbeelding F: $\mathbb{R}^2 \to \mathbb{R}^2$ wordt aldus gedefinieerd:

$$\forall_{(x,y) \in \mathbb{R}^2} \ (F(x,y) = (x,0)).$$

Is deze afbeelding één-éénduidig? Is de afbeelding op?

11. Een afbeelding F : $\mathbb{R}^2 \to \mathbb{R}$ wordt aldus gedefinieerd:

$$\forall_{(x,y) \in \mathbb{R}^2} (F(x,y) = x).$$

Is deze afbeelding één-éénduidig? Is de afbeelding op?

12. $A = \{x \in \mathbb{R} \mid 1 \leq x < 2\}$ en $B = \{x \in \mathbb{R} \mid x \leq -1\}$.
Geef een één-éénduidige afbeelding van A op B.

13. F is een afbeelding $\mathbb{R}^2 \to \mathbb{C}$, gedefinieerd door:

$$\forall_{(x,y) \in \mathbb{R}^2} \ (F(x,y) = x \ e^{2\pi i y}).$$

Is deze afbeelding één-éénduidig? Is de afbeelding op?

14. G is een afbeelding: $\{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \leq y < 1\} \to \mathbb{C}$, gedefinieerd door:

$$\forall_{(x,y) \in \mathbb{R} \times \mathbb{R}} \ (G(x,y) = xe^{2\pi i y}) .$$

Is deze afbeelding één-éénduidig? Is de afbeelding op?

15. F is een afbeelding van A naar B; $A_1 \subset A$; $A_2 \subset A$; $B_1 \subset B$; $B_2 \subset B$.
Bewijs dat

a) $F(A_1 \cup A_2) = F(A_1) \cup F(A_2)$.

b) $F(A_1 \cap A_2) \subset (F(A_1) \cap F(A_2))$.

c) $F^{\leftarrow}(B_1 \cup B_2) = F^{\leftarrow}(B_1) \cup F^{\leftarrow}(B_2)$.

d) $F^{\leftarrow}(B_1 \cap B_2) = F^{\leftarrow}(B_1) \cap F^{\leftarrow}(B_2)$.

e) Zoek een voorbeeld waaruit blijkt dat in b) de inclusie echt kan zijn.

16. F is een afbeelding van A naar B; $A_1 \subset A$; $B_1 \subset B$.
Bewijs dat

a) $F^{\leftarrow}(F(A_1)) \supset A_1$.

b) $F(F^{\leftarrow}(B_1)) \subset B_1$.

c) Zoek bij a) en b) voorbeelden waaruit blijkt dat de inclusies echt kunnen zijn.

17. De afbeelding F: $\mathbb{R} \to \mathbb{R}^2$ wordt gedefinieerd door:

$$\forall_{x \in R} \; (F(x) = (x+1, 2x))$$

en de afbeelding G : $\mathbb{R}^2 \to \mathbb{R}$ wordt gedefinieerd door:

$$\forall_{(x,y) \in \mathbb{R}^2} (G(x,y) = y).$$

Bepaal $(G \circ F)^{\leftarrow} (\{x \mid 0 \leq x \leq 2\})$.

18. F is een afbeelding $\mathbb{R} \to \mathbb{R}^2$ en G een afbeelding $\mathbb{R} \to \mathbb{R}^2$, gedefinieerd door:

$$\forall_{x \in \mathbb{R}} \; (F(x) = (x, x^2)) \; ;$$

$$\forall_{x \in \mathbb{R}} \; (G(x) = (x^2, x)) \; .$$

Onderzoek of de volgende bewering waar dan wel onwaar is:

$$\forall_{A \subset \mathbb{R}} \; (G^{\leftarrow}(F(A)) = F^{\leftarrow}(G(A))).$$

19. F is een één-éénduidige afbeelding van A op B;
G is een één-éénduidige afbeelding van B op C.
Bewijs dat $G \circ F$ een één-éénduidige afbeelding van A op C is en bewijs ook dat $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$.

20. $V := \{(x,y) \in \mathbb{R}^2 \mid x^2 - y^2 \geq 0\}$.

F is een afbeelding : $V \to \mathbb{R}^2$, gedefinieerd door

$$\forall_{(x,y)\in V}(F(x,y) := (e^{x+y}, e^{x-y})) .$$

a) Bepaal en teken F(V).

b) Bepaal en teken $F^{\leftarrow}(W)$ voor $W := \{(u,v) \in \mathbb{R}^2 \mid \frac{1}{e} \leq uv < e\}$.

c) Onderzoek of F één-éénduidig is.

21. Bewijs met behulp van karakteristieke functies dat voor de verzamelingen A en B geldt:

a) Als $A \cup B = B$ dan is $A \subset B$.

b) Als $A \cap B = A$ dan is $A \subset B$.

c) $A \setminus (B \setminus A) = A$.

22. Zij A een niet-lege deelverzameling van een universum U.
We definiëren een relatie aldus

$$\forall_{x\in U} \forall_{y\in U}((x \sim y) :\Leftrightarrow (\chi_A(x) = \chi_A(y))) .$$

Bewijs dat dit een equivalentierelatie is en bepaal de equivalentieklassen.

23. In Z wordt een relatie gedefinieerd:

$$\forall_{a\in Z} \forall_{b\in Z}((a \sim b) :\Leftrightarrow (a^2 + a = b^2 + b)) .$$

Ga na of dit een equivalentierelatie is en zo ja, bepaal de equivalentieklassen.

24. V is de verzameling van alle reële functies op het interval [0,1].
Een relatie wordt aldus gedefinieerd

$$\forall_{f\in V} \forall_{g\in V}((f \sim g) :\Leftrightarrow (f - g \text{ is continu op } [0,1])) .$$

a) Bewijs dat dit een equivalentierelatie is.

b) Bewijs dat de functies die continu zijn op [0,1] juist een equivalentieklasse vormen.

25. Op $\mathbb{R}^2 \setminus \{(0,0)\}$ wordt de relatie $\sim$ gedefinieerd door

$$\forall_{(a,b)\in\mathbb{R}^2\setminus\{(0,0)\}} \forall_{(c,d)\in\mathbb{R}^2\setminus\{(0,0)\}} (((a,b) \sim (c,d)) \leftrightarrow (ad = bc)) .$$

a) Bewijs dat $\sim$ een equivalentierelatie is.

b) Bepaal de equivalentieklassen.

26. Beschouw de verzameling van kwadratische vormen in x van de gedaante $ax^2 + bx + c$, waarbij a, b, c en x elementen van GF(2) zijn.
Twee kwadratische vormen staan in relatie als hun nulpuntenverzameling in GF(2) dezelfde is.
Onderzoek of dit een equivalentierelatie is en zo ja, bepaal dan de equivalentieklassen.

27. a) Bepaal $\{x \in GF(3) \mid x^2 + x + 1 = 0\}$

b) " $\{x \in \mathbb{Z} \mid x^2 - 2 = 0\}$

c) " $\{x \in \mathbb{R} \mid x^2 - 2 = 0\}$

d) " $\{x \in GF(7) \mid x^2 - 2 = 0\}$.

28. Ontbind in faktoren: $x^3 + x^2 + x + 1$ als de nulpunten respectievelijk elementen zijn van $\mathbb{R}$, $\mathbb{C}$, GF(2) en GF(5).

29. Beschouw de lineaire ruimte van dimensie 2 over het lichaam GF(5).

a) Hoeveel punten telt deze ruimte?

b) Hoeveel punten bevat een rechte door O?

c) Hoeveel rechten door O zijn er?

d) Bepaal voor elk element q van GF(5) de punten van de ruimte die liggen op de kromme, bepaald door $x_1^2 + x_2^2 = q$.

30. Als opgave 29, maar nu over GF(p), waarbij p oneven priem is.
Beantwoord de vragen a t/m c.
Bewijs dat voor elk element q van GF(p) er minstens één punt is dat op de kromme bepaald door $x_1^2 + x_2^2 = q$ ligt.

Hoofdstuk IV: Groepen (deel 1)

1. V is een niet-lege verzameling. P(V) is de verzameling van alle deelverzamelingen van V.
   In P(V) beschouwen we achtereenvolgens de operaties:
   a) $\cap$
   b) $\cup$
   c) $\setminus$
   d) :

   Ga na welke van deze operaties commutatief zijn, welke associatief.
   Ga na in welke gevallen er een eenheidselement is en welke elementen in deze gevallen een inverse hebben.

2. $\mathbb{R}^+ := \{x \in \mathbb{R} \mid x > 0\}$.
   In $\mathbb{R}^+$ beschouwen we de operatie φ: $\mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$, gedefinieerd door:

$$\varphi((a,b)) := \frac{1}{\frac{1}{a} + \frac{1}{b}} .$$

   Bewijs dat $(\mathbb{R}^+, \varphi)$ een commutatieve semi-groep is. Is er een eenheidselement?

3. We beschouwen de verzameling $\mathbb{R}^3$ met als operatie het vectorproduct.
   a) Is dit product associatief?
   b) Is het product commutatief?
   c) Heeft $(\mathbb{R}^3, x)$ een eenheidselement?

4. $\mathbb{Z}^+ := \{x \in \mathbb{Z} \mid x > 0\}$.
   $V := \{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+\}$.

   In V wordt de matrixvermenigvuldiging als operatie gedefinieerd.
   Bewijs dat (V,) een commutatieve semi-groep is. Is er een eenheidselement? Welke elementen hebben een inverse?

5. $V := \{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+\}$.

   $W := \{\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+\}$.

   In $V \cup W$ wordt de matrixvermenigvuldiging als operatie gedefinieerd.
   Bewijs dat ($V \cup W$,) een semi-groep is. Is hij commutatief? Is er een eenheidselement? Zijn er elementen met een inverse?

6. Bewijs dat ($\mathbb{Z}$ mod 8,) een commutatieve semi-groep is met eenheids-element. Welke elementen hebben een inverse?

7. $m \in \mathbb{N}$. Beschouw voor $1 \leq i \leq m$ de verzameling

$$A_i := \{x \in \mathbb{Z} \mid x \equiv i \pmod{m}\}.$$

Zij $W = \{A_i \mid 1 \leq i \leq m\}$.
Op W wordt een operatie $\cdot$ gedefinieerd door:

$$\forall_{A_i \in W} \forall_{A_j \in W} (A_i \cdot A_j := \{x \in \mathbb{Z} \mid x \equiv ij \pmod{m}\}).$$

a) Bewijs dat $(W,\cdot)$ een semi-groep is.
b) Als g.g.d. $(i,m) = 1$, dan is g.g.d. $(x,m) = 1$ voor alle x in A_i. Bewijs dit.
c) Zij $W' = \{A_i \in W \mid \text{g.g.d. } (i,m) = 1\}$.
Bewijs dat $(W',\cdot)$ een Abelse groep is.

8. In Z wordt een operatie $*$ gedefinieerd door

$$\forall_{a \in \mathbb{Z}} \forall_{b \in \mathbb{Z}} (a * b = a + b - 2).$$

Bewijs dat $(\mathbb{Z},*)$ een Abelse groep is.

9. Onderzoek welke van de volgende verzameling met operatie groep zijn.
a) $(\{x + y\sqrt{2} \mid x \in \mathbb{Q}, y \in \mathbb{Q}\}, +)$
b) $(\{x + y\sqrt{2} \mid x \in Q, y \in Q, xy \neq 0\},)$

10. $V = \{(a,b) \mid a \in GF(3), b \in GF(3), (a,b) \neq (0,0)\}$.
In V wordt de operatie $*$ aldus gedefinieerd:

$$(a,b) * (c,d) = (ac + 2bd, ad + bc).$$

Bewijs dat $(V,*)$ een commutatieve groep is.

11. De wortels van de vergelijking $z^n = 1$ (in $\mathbb{C}$) vormen een multiplicatieve groep die isomorf is met ($\mathbb{Z}$ mod n,+).
Bewijs dit.

12. Bepaal de groep der symmetrieën van een gelijkzijdige driehoek en maak de groepentabel. Bepaal alle ondergroepen.

13. Voor i = 1,2,3,4 is f_i een afbeelding van $\mathbb{R}\setminus\{0\}$ op $\mathbb{R}\setminus\{0\}$, gedefinieerd door

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

Op de verzameling $V = \{f_1, f_2, f_3, f_4\}$ wordt de operatie $*$ gedefinieerd door

$$\forall_{x \in \mathbb{R}} ((f_j * f_i)x = f_j(f_i x)).$$

Bewijs dat $(V,*)$ een groep is. Met welke groep is deze groep isomorf?

14. De machten van de permutatie $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ vormen een groep.

Bewijs dit en zoek een groep die isomorf is met deze groep.

15. G is een verzameling met de productoperatie $*$.

Er is gegeven dat:

1) $*$ is associatief.

2) $\exists_{e_\ell \in G} \forall_{a \in G} (e_\ell * a = a)$.

3) $\forall_{a \in G} \exists_{a_\ell^{-1} \in G} (a_\ell^{-1} * a = e_\ell)$.

Bewijs dat

a) e_ℓ ook rechtereenheidselement is, d.w.z.:

$$\forall_{a \in G} (a * e_\ell = a),$$

b) er precies één eenheidselement is,

c) a_ℓ^{-1} ook rechter inverse is van a, d.w.z.:

$$\forall_{a \in G} (a * a_\ell^{-1} = e),$$

d) elk element precies één inverse heeft.

Hoofdstuk IV: Groepen (deel 2)

1. Zijn a en b elementen van een groep (G,) dan hebben ab en ba dezelfde orde. Bewijs dit.

2. Zijn a en b elementen van een groep (G,), a van orde n en b van orde m, dan is de orde van het element ab een deler van mn als gegeven is dat ab = ba. Bewijs dit.

3. Een cyclische groep (G,) met een niet eindig aantal elementen is isomorf met $(\mathbb{Z},+)$. Bewijs dit.

4. Elke ondergroep van een cyclische groep (G,) is ook cyclisch. Bewijs dit.

5. Bepaal alle ondergroepen van ($\mathbb{Z}$ mod 24,+).

6. a) Zijn (A,) en (B,) ondergroepen van (G,), dan is ook (A $\cap$ B,) ondergroep van (G,). Bewijs dit.

   b) Zijn (A,) en (B,) normale ondergroepen van (G,) dan is (A $\cap$ B,) ook normale ondergroep van (G,). Bewijs dit.

7. Zij (G,) een groep en (H,) een ondergroep.
   In G wordt de relatie gedefiniëerd:

   $$\forall_{x\in G}\ \forall_{y\in G}\ ((x \sim y) :\Longleftrightarrow (x^{-1}y \in H)).$$

   a) Bewijs dat dit een equivalentierelatie is.
   b) Bewijs dat aH de equivalentieklasse van a is (a $\in$ G).

8. Is H ondergroep van G, dan heet Ha een rechter nevenklasse van H, aH een linker nevenklasse van H.
   S_3 bevat als ondergroep de groep H, bestaande uit de elementen $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ en $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$. Bepaal de rechter en de linker nevenklassen van H.

9. Is (H,) een ondergroep van (G,) dan geldt:
   $\forall_{a\in G}\ \forall_{b\in G}$ (HaHb = Hab) dan en slechts dan als H normale ondergroep van G is. Bewijs dit.

10. Is S_n de symmetrische groep van de permutaties van n elementen, bewijs dan dat deze een ondergroep heeft die isomorf is met S_{n-1}.

11. a) Zij H een ondergroep van S_4 die isomorf is met S_3. Bepaal de linker- en de rechter-nevenklassen van H.
    b) V_4 is de permutatiegroep van de symmetrieën van een rechthoek. Bewijs dat V_4 isomorf is met een normale ondergroep van S_4.
    c) Bewijs dat $S_4/V_4 \cong S_3$.

12. Bewijs dat een groep waarvan de orde oneven is geen element heeft van orde 2.

13. Is (G,) een groep, $a \in G$ en $H = \{x \in G \mid xa = ax\}$, bewijs dan dat (H,) ondergroep van (G,) is. Is (H,) noodzakelijk commutatief?

14. (H,) en (K,) zijn normale ondergroepen van (G,) zó dat $H \cap K = \{e\}$ (e is eenheidselement van G).
    Bewijs dat

$$\forall_{h \in H} \forall_{k \in K} (hk = kh) \ .$$

15. $G := \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, c \in \mathbb{Z}, d \in \mathbb{Z}, |ad - bc| = 1 \}$

    $H := \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \mid ad - bc = 1 \}$.

    a) Toon aan dat G met de gebruikelijke matrixvermenigvuldiging een groep is.
    b) Bewijs dat H een ondergroep is van G.
    c) Laat zien dat H een normale ondergroep is van G.

Hoofdstuk V: Ringen en lichamen

1. V is een niet-lege verzameling, P(V) de verzameling van alle deelverzamelingen van V.
   Bewijs dat $(P(V), \div, \cap)$ een commutatieve ring met eenheidselement is.

2. a) $(R, +,)$ is een ring en S een niet-lege deelverzameling van R.
   $(S, +,)$ is een onderring van R dan en slechts dan als:

   $$\forall_{a\in S}\ \forall_{b\in S}\ ((a-b\in S) \wedge (ab\in S)).$$ Bewijs dit.

   b) Indien $(R, +,)$ een lichaam is en S een niet-lege deelverzameling van R, stel dan zelf de nodige en voldoende voorwaarde op voor de uitspraak:
   S is deellichaam van R.

3. Zijn $(S_1, +,)$ en $(S_2, +,)$ twee onderringen van de ring $(R, +,)$ dan is ook $(S_1 \cap S_2, +,)$ onderring van $(R, +,)$. Bewijs dit.

4. $V = \{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \in \mathbb{Z},\ b \in \mathbb{Z}\}$; + is de matrix optelling, $*$ de matrixvermenigvuldiging.
   a) Bewijs dat $(V, +, *)$ een commutatieve ring is met eenheidselement.
   b) Is $I = \{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \in \mathbb{Z}\}$, dan is $(I, +, *)$ een ideaal van $(V, +, *)$; bewijs dit.
   c) Bewijs dat V/I isomorf is met de ring der gehele getallen.

5. Bepaal alle idealen in de ring $(\mathbb{Z} \bmod 18, +,)$ en de bijbehorende factorringen. Welke hiervan zijn lichamen?

6. Zij $(R, +,)$ een lichaam. Bepaal alle idealen van R.

7. Zij $(R, +,)$ een ring met eenheidselement zonder nuldelers, d.w.z.:

   $$\forall_{a\in R}\ \forall_{b\in R}\ ((ab = 0) \Rightarrow ((a = 0) \vee (b = 0))).$$

   Heeft R eindig veel elementen, dan is R een lichaam. Bewijs dit.

8. In $\mathbb{R} \times \mathbb{R}$ worden twee bewerkingen gedefinieerd, nl. $\oplus$ en $*$ door:

   $$\forall_{(a,b)\in \mathbb{R}^2}\ \forall_{(c,d)\in \mathbb{R}^2}\ ((a,b) \oplus (c,d) := (a+c,\ b+d))$$

   $$\forall_{(a,b)\in \mathbb{R}^2}\ \forall_{(c,d)\in \mathbb{R}^2}\ ((a,b) * (c,d) := (ac-bd,\ bc+ad)).$$

   Bewijs dat $(\mathbb{R} \times \mathbb{R}, \oplus, *)$ een lichaam is dat isomorf is met $(\mathbb{C}, +,)$.

9. Beschouw de polynoomring $(\mathbb{R}[x], +,)$.

   a) Bewijs dat $x^2 + 1$ irreducibel is in $\mathbb{R}[x]$.

   b) Zij I het ideaal $\{r(x)(x^2+1) \mid r(x) \in \mathbb{R}[x]\}$.
   Bewijs dat $(\mathbb{R}[x]/I, +,)$ een commutatief lichaam is.

   c) Bewijs dat het lichaam uit b) isomorf is met $(\mathbb{C}, +,)$.

10. Bewijs dat $(\{a + b\sqrt{2} \mid a \in \mathbb{Q}, b \in \mathbb{Q}\}, +,)$ een commutatief lichaam is.

11. Beschouw de polynoomring $(\mathbb{Q}[x], +,)$.

   a) Bewijs dat $x^2 - 2$ irreducibel is in $\mathbb{Q}[x]$.

   b) Zij I het ideaal: $\{r(x)(x^2-2) \mid r(x) \in \mathbb{Q}[x]\}$.
   Bewijs dat $(\mathbb{Q}[x]/I, +,)$ een commutatief lichaam is door een isomorfie met het lichaam in opg. 10 te zoeken.

12. Zij $(R, +,)$ een commutatief lichaam van de karakteristiek p.

   a) Bewijs:
   $$\forall_{a\in R} \forall_{b\in R} ((a+b)^p = a^p + b^p) .$$

   b) Bewijs:
   $$\forall_{a\in R} \forall_{b\in R} ((a-b)^p = a^p - b^p).$$

13. Bewijs dat elk element van het lichaam $GF(p^k)$ oplossing is van de vergelijking $x^{p^k} - x = 0$.

14. Onderzoek in $(GF(2)[x], +,)$ het al of niet reducibel zijn van de polynomen:

   a) $x^3 + x + 1$

   b) $x^4 + x^3 + 1$

   c) $x^4 + x^2 + 1$.

15. Beschouw de polynoomring $(GF(2)[x], +,)$.

   a) Bewijs dat alle irreducibele polynomen van de graad 4 delers zijn van $x^{15} + 1$.

   b) Bewijs dat de onder a) genoemde polynomen in $(GF(2^4)[x], +,)$ te ontbinden zijn in factoren van de eerste graad.

16. a) Bewijs dat $x^2 + 1$ in $(GF(3)[x], +,)$ irreducibel is en construeer het lichaam $GF(3^2)$.
Zij α een primitief element van $GF(3^2)$.

b) Ontbind in $GF(3)[x]$ het polynoom $x^4 + 1$ in twee irreducibele polynomen en toon aan dat α een nulwaarde is van één van deze factoren.

17. Zij α een primitief element van $GF(27)$.
Bewijs dat $(x-\alpha^2)(x-\alpha^6)(x-\alpha^{18})$ een polynoom is in $GF(3)[x]$ en dat dit polynoom een irreducibele factor van $1 + x + x^2 + \ldots + x^{12}$ is.

Hoofdstuk VI: Vectorruimten over GF(q), grafen

1. a) Beschouw V(2,5), de vectorruimte van dimensie 2 over GF(5). Zij de rechte ℓ gegeven door $\ell = \{\underline{x} \in V(2,5) \mid \exists_{\lambda \in GF(5)} \ (\underline{x} = \lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix})\}$.

   i) Bepaal de punten op ℓ.

   ii) Bepaal een parametervoorstelling van de rechten die evenwijdig aan ℓ zijn en geef aan welke punten erop liggen.

   b) Zij ℓ een rechte in V(2,q), ($q = p^k$, p priem).

   i) Bepaal het aantal rechten in V(2,q) die evenwijdig aan ℓ zijn.

   ii) Wat is het verband tussen dit aantal en het totaal aantal rechten in V(2,q)?

2. Beschouw V(3,q), de vectorruimte van dimensie 3 over GF(q) ($q = p^k$, p priem).

   a) Bepaal het aantal rechten door een gegeven punt.

   b) Zij W een vlak in V(3,q). Bepaal het aantal rechten in W die door één punt van W gaan en bepaal het totaal aantal rechten in W.

   c) Bepaal het aantal vlakken in V(3,q) door een gegeven punt.

   d) Bepaal het aantal vlakken in V(3,q) door een gegeven rechte ℓ.

   e) Bepaal het totaal aantal vlakken in V(3,q).

3. a) Bepaal de verzameling $C := \{(x,y) \in V(2,7) \mid x^2 + y^2 = -3\}$.

   b) Beschouw alle rechten door $(2,0) \in C$.
   Toon aan dat er één rechte door (2,0) is die "de cirkel C" in één punt "snijdt" en dat de overige rechten C in twee punten "snijden".

   c) Beschouw alle rechten door (0,0). Welke rechten hebben 0,1 of 2 "snijpunten" met C?

4. a) Bepaal de verzameling $C := \{(x,y) \in V(2,5) \mid x^2 + y^2 = 1\}$.

   b) Laat zien dat een rechte door $(0,1) \in C$, de "cirkel C snijdt" in één of twee punt(en).

   c) Welke rechten door (0,2) snijden C in respectievelijk 0,1 of 2 punten?

5. V(3,4) is de vectorruimte van dimensie 3 over GF(4) met

$$GF(4) = (\{0,\alpha,\alpha+1,1\},+(\text{mod } 2),(\text{mod } 2),\ \cdot\ (\text{mod } 2,\text{mod}(\alpha^2+\alpha+1))) .$$

a) Vlak W: $\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}\alpha\\1\\\alpha+1\end{pmatrix} + \lambda\begin{pmatrix}1\\0\\\alpha\end{pmatrix} + \mu\begin{pmatrix}0\\\alpha+1\\\alpha\end{pmatrix}$, $\lambda,\mu \in GF(4)$.

b) Rechte ℓ: $\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}0\\0\\\alpha+1\end{pmatrix} + \nu\begin{pmatrix}1\\\alpha+1\\\alpha\end{pmatrix}$, $\nu \in GF(4)$

Onderzoek of ℓ evenwijdig is aan W en zo niet, bepaal dan het snijpunt van ℓ en W.

b) A: V(3,4) $\to$ V(3,4) is een lineaire afbeelding met matrix (t.o.v. een basis)

$$A = \begin{pmatrix}1 & \alpha & 0\\ \alpha+1 & 0 & \alpha\\ 0 & \alpha+1 & 1\end{pmatrix} .$$

Laat zien dat de beeldruimte van A een vlak W' evenwijdig aan W is en dat de nulruimte van A een rechte ℓ' evenwijdig aan ℓ is.

6. A en B zijn lineaire afbeeldingen V(2,5) $\to$ V(2,5) met matrices:

$$A = \begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix} \quad \text{en} \quad B = \begin{pmatrix}2 & 3\\ 1 & 4\end{pmatrix} .$$

a) Onderzoek of A en B reguliere afbeeldingen zijn.

b) Bepaal de beeldruimten en nulruimten van A en B.

c) Bepaal de eigenwaarden en eigenruimten onder A en B.

d) Bepaal het beeld van $\{\begin{pmatrix}x_1\\x_2\end{pmatrix} \mid x_1^2 + x_2^2 = 0\}$ onder A en B.

7. A: V(3,3) $\to$ V(3,3) is een lineaire afbeelding met matrix

$$A = \begin{pmatrix}1 & 0 & 2\\ 2 & 1 & 0\\ 0 & 1 & 1\end{pmatrix} .$$

a) Toon aan dat A een reguliere lineaire afbeelding is.

b) Bepaal de matrix A^{-1} van de inverse afbeelding A^{-1}.

c) Bepaal de eigenwaarden en eigenvectoren van A.

8. In V(2,3) worden een optelling $\oplus$ en vermenigvuldiging $\otimes$ gedefinieerd door

$$\forall_{(a,b)\in V(2,3)}\ \forall_{(c,d)\in V(2,3)}\ ((a,b) \oplus (c,d) := (a+c,\ b+d),$$

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

a) Toon aan dat $(V(2,3),\oplus,\otimes)$ een lichaam is met 9 elementen (GF(9)).

b) Laat zien dat $(V(2,3),\oplus,\otimes)$ isomorf is met $(GF(3)[x]/I,+,\ )$ waarbij

$$I = \{r(x)(x^2+1) \mid r(x) \in GF(3)[x]\} .$$

9. V(2,q) is met de optelling $\oplus$ gedefinieerd door

$$\forall_{(a,b)\in V(2,q)}\ \forall_{(c,d)\in V(2,q)}\ ((a,b) \oplus (c,d) := (a+c,\ b+d))$$

een commutatieve groep.

a) Zij $(v,w) \in V(2,q)$.

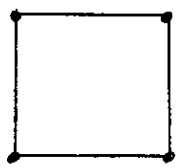
$$W := \{(x,y) \in V(2,q) \mid \exists_{\lambda\in GF(q)}\ (x,y) = \lambda(v,w)\} .$$

Toon aan $(W,\oplus)$ is een normale ondergroep.

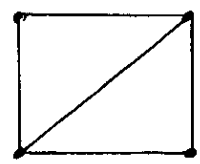
b) Bepaal de factorgroep $V(2,q)/W$.

10. Bepaal het aantal automorfismen van de volgende grafen (of hun complement):

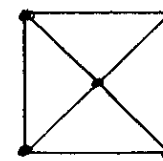
a)



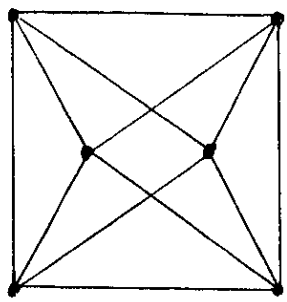
b)



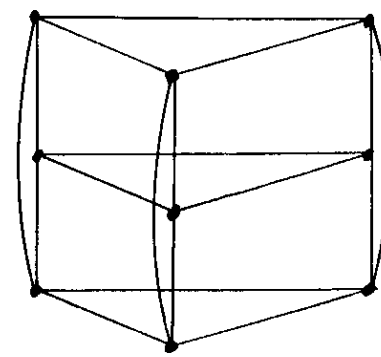
c)



d)



e)



11. Bedenk een graaf met 6 punten die als enig automorfisme de identiteit heeft (zie ook in de syllabus, § 6.3).

Hoofdstuk VII: Ordening

1. Bewijs dat in een tralie T geldt:

   a) $\forall_{x \in T} (x \cap x = x)$

   b) $\forall_{x \in T} (x \cup x = x)$.

2. Bewijs dat in een tralie T geldt:

   a) $\forall_{x \in T} \forall_{y \in T} (x \cap (x \cup y) = x)$

   b) $\forall_{x \in T} \forall_{y \in T} (x \cup (x \cap y) = x)$.

3. Bewijs dat in een tralie T geldt:

$$\forall_{x \in T} \forall_{y \in T} \forall_{z \in T} (x \cap (y \cap z) = (x \cap y) \cap z)$$
$$\forall_{x \in T} \forall_{y \in T} \forall_{z \in T} (x \cup (y \cup z) = (x \cup y) \cup z) .$$

4. Als $x \cap y$ de ggd en $x \cup y$ het kgv is van de natuurlijke getallen x en y, bewijs dan:

   a) $\forall_{x \in \mathbb{N}} \forall_{y \in \mathbb{N}} \forall_{z \in \mathbb{N}} (x \cap (y \cup z) = (x \cap y) \cup (x \cap z))$

   b) $\forall_{x \in \mathbb{N}} \forall_{y \in \mathbb{N}} \forall_{z \in \mathbb{N}} (x \cup (y \cap z) = (x \cup y) \cap (x \cup z))$.

5. Bewijs dat in een Boole algebra V geldt:

$$\forall_{x \in V} \exists!_{x^* \in V} (x \cup x^* = I, x \cap x^* = 0) .$$

6. Bewijs dat in een Boole algebra geldt:

   a) $\forall_{a \in V} \forall_{b \in V} ((a \cap b)^* = a^* \cup b^*)$

   b) $\forall_{a \in V} \forall_{b \in V} ((a \cup b)^* = a^* \cap b^*)$.

7. In een Boole ring B geldt:

   a) $\forall_{a \in B} \; (a + a = 0)$

   b) $\forall_{a \in B} \forall_{b \in B} \; (ab = ba)$.

8. a) Is V een niet-lege verzameling en P(V) de verzameling van alle deelverzamelingen, dan is $(P(V), \div, \cap)$ een Boole ring.
   Bewijs dit.

   b) Definieer op P(V) de operaties $\wedge$ en $\vee$ door

   $$\forall_{a \in P(V)} \forall_{b \in P(V)} \; (a \wedge b := a \cap b)$$

   $$\forall_{a \in P(V)} \forall_{b \in P(V)} \; (a \vee b := a \div b \div (a \cap b))$$

   $$\forall_{a \in V} \; (a^* = V \div a)$$

   dan is $P(V), \wedge, \vee, *)$ een Boole algebra onder $\supset$.
   Bewijs dit.

9. Bewijs dat het aantal deelverzamelingen van een verzameling met n elementen 2^n is.