Discrete Wiskunde

Prof. Dr. Ann Dooms

2023 - 2024

Voorwoord

Deze tekst is het cursusmateriaal bij het vak "Discrete Wiskunde" dat aan de VUB gedoceerd wordt in eerste bachelor Wiskunde, tweede Bachelor en Schakelprogramma Computerwetenschappen.

Op het examen wordt vooral gepeild naar het begrip van de cursus en de wiskundige technieken die aan de basis liggen. Alle stellingen, lemma's, gevolgen etc. moeten gekend zijn, met bewijs. De bewijzen die niet in de cursus staan zou de student zelf moeten kunnen vinden en kunnen dus ook op het examen aan bod komen. In de cursusfiche vind je meer details over het opzet van het examen.

Achteraan deze nota's vind je een korte bibliografie met referentiewerken die naast deze tekst kunnen geraadpleegd worden. Zij bevatten nog meer voorbeelden en oefeningen.

Hierbij wens ik de voormalige titularis van dit vak, Prof. Dr. Philippe Cara, en Tom Deneckere, te bedanken voor het opstellen van deze prachtige cursus, alsook Jan Broekaert, Caroline Verhoeven, Frank De Geeter, Adriaan Leijnse en Tomas Everaert die doorheen de jaren aan de tekst hebben meegewerkt.

Prof. Dr. Ann Dooms

Inhoudsopgave

Hoofdstuk 1

Inleidende begrippen

We frissen enkele basisbegrippen op en we maken notationele afspraken.

1.1 Logica

De wiskunde is opgebouwd uit "logische redeneringen". Deze redeneringen worden in het algemeen bestudeerd in de wiskundige discipline die "logica" heet. Logica komt uitgebreid aan bod in de cursus "Logica en Formele Systemen" (Prof. Dr. De Troyer). Wij zullen de taal en notatie van de zogenaamde predikatenlogica gebruiken om redeneringen neer te schrijven. We herhalen hier enkele notaties en begrippen:

- **propositie**: een bewering p die ofwel **waar**, ofwel **onwaar** is
- **conjunctie**: $p \wedge q$ ("p en q") en **disjunctie**: $p \vee q$ ("p of q")
- **implicatie**: $p \Rightarrow q$ ("Als p dan q")

  Voorbeeld. "x is deelbaar door 10 $\Rightarrow$ x is even"

- **equivalentie**: $p \Leftrightarrow q$ ("p is equivalent met q") betekent $(p \Rightarrow q) \wedge (q \Rightarrow p)$

  Voorbeeld. "n^2 even $\Leftrightarrow$ n even"

- **negatie**: $\neg p$

  Voorbeeld. "Het regent niet."

Opmerking.

De negatie van de implicatie is niet hetzelfde als contrapositie!

- **negatie van de implicatie**: $\neg(p \Rightarrow q)$ is equivalent met $p \wedge \neg q$
- **contrapositie van de implicatie**: $p \Rightarrow q$ is equivalent met $\neg q \Rightarrow \neg p$

Voorbeeld. Om te bewijzen dat "n^2 even $\Rightarrow$ n even" is het gemakkelijker te bewijzen dat "n oneven $\Rightarrow$ n^2 oneven".

1.2 Verzamelingen

Een fundamenteel begrip in de wiskunde is **verzameling**. Het is echter moeilijk dit begrip precies te definiëren. Verzamelingen laten toe alle (wiskundige) objecten met dezelfde kenmerken te groeperen of te verzamelen.

Voorbeeld. De verzameling **priemgetallen** groepeert alle positieve gehele getallen die juist twee verschillende delers bezitten.

Een object uit een gegeven verzameling heet een **element**. We noteren verzamelingen meestal met Latijnse hoofdletters: $A, B, C, \ldots, X, Y, Z$. Sommige verzamelingen verdienen een speciaal symbool:

- $\mathbb{N} = \{0, 1, 2, \ldots\}$: de natuurlijke getallen
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$: de gehele getallen
- $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \wedge b \neq 0\}$: de rationale getallen
- $\mathbb{R}$: de reële getallen
- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$: de complexe getallen

Merk op: Een verzameling kan gedefinieerd worden door haar elementen op te sommen tussen accolades. We kunnen ook een algemene beschrijving geven van haar elementen zoals in het voorbeeld van $\mathbb{Q}$. Hierbij moet je het verticale streepje "|" lezen als "waarvoor geldt". Het symbool "$\in$" betekent "is element van" of "behoort tot". Meer voorbeelden:

- $\mathbb{R}_0 = \{x \in \mathbb{R} \mid x \neq 0\}$
- $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$
- $\mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x > 0\}$

Als A **eindig** is (d.w.z. A bevat een eindig aantal elementen) noteren we het aantal elementen in A met $|A|$ of $\#A$. De **lege verzameling** $\emptyset$ bevat geen elementen. De uitspraak $\neg(x \in A)$ korten we af tot $x \notin A$, "x behoort niet tot A".

1.3 Kwantoren

Sommige uitspraken of eigenschappen zijn geldig *voor alle* objecten in een gegeven verzameling. Om dit te noteren gebruiken we de **kwantor** "voor alle": $\forall$.

Voorbeeld. $\forall\, x \in \mathbb{R} : x^2 \geq 0$.

Het dubbelpunt ":" betekent in een logische uitspraak "geldt".

Er is ook een kwantor "er bestaat" indien men wil zeggen dat een eigenschap geldt *voor minstens één* element in een gegeven verzameling.

Voorbeeld. $\exists\, x \in \mathbb{R} : x^2 = x$.

Soms wil men benadrukken dat er *slechts één element* bestaat met de gegeven eigenschap.

Voorbeeld. $\exists!\, x \in \mathbb{R}_0^+ : x^2 = x$.

1.4 Meerdere kwantoren en negaties

De volgorde van kwantoren heeft belang! Bijvoorbeeld

$$\forall\, x \in \mathbb{R} : \exists\, y \in \mathbb{R}^+ : x^2 = y$$

is waar, terwijl

$$\exists\, y \in \mathbb{R}^+ : \forall\, x \in \mathbb{R} : x^2 = y$$

onwaar is.

Opmerking. De letters die we gebruiken als **variabelen** hebben uiteraard geen belang:

$$\forall\, \beta \in \mathbb{R} : \exists\, b \in \mathbb{R}^+ : \beta^2 = b$$

is dezelfde uitspraak als de eerste, maar anders geschreven.

Negaties van uitspraken zijn zeer belangrijk. Denk bijvoorbeeld aan het bewijs door contrapositie.

De negatie van $\forall\, x \in X : p(x)$ is $\exists\, x \in X : \neg p(x)$ en de negatie van $\exists\, x \in X : p(x)$ is $\forall\, x \in X : \neg p(x)$.

Voorbeeld. De negatie van

$$\forall\, \varepsilon \in \mathbb{R}_0^+ : \exists\, \delta \in \mathbb{R}_0^+ : \forall\, x \in X : (|x-a| < \delta) \Rightarrow (|f(x) - f(a)| < \varepsilon)$$

is

$$\exists\, \varepsilon \in \mathbb{R}_0^+ : \forall\, \delta \in \mathbb{R}_0^+ : \exists\, x \in X : (|x-a| < \delta) \wedge (|f(x) - f(a)| \geq \varepsilon)$$

1.5 Deelverzamelingen en gelijke verzamelingen

Indien elk element van een verzameling A ook behoort tot een verzameling B, zeggen we dat A een **deelverzameling** is van B of dat B de verzameling A *omvat*.

Symbolisch:

$$A \subset B \Leftrightarrow \forall\, a \in A : a \in B$$

Voor $A \subset B$ schrijven we ook $B \supset A$. We hebben steeds $B \subset B$ en $\emptyset \subset B$. Alle andere deelverzamelingen heten **echte deelverzamelingen** van B.

Voorbeelden.

- $\{1, 2, 3\} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $\mathbb{Z} \not\subset \mathbb{R}^+$

Twee verzamelingen A en B zijn **gelijk** indien ze dezelfde elementen hebben. Dit is het geval als en slechts als $(A \subset B) \wedge (B \subset A)$. We noteren (uiteraard) $A = B$. Gevolg: $A \neq B$ indien $(A \not\subset B) \vee (B \not\subset A)$, d.w.z. $(\exists\, a \in A : a \notin B) \vee (\exists\, b \in B : b \notin A)$.

De verzameling van alle deelverzamelingen van een gegeven verzameling X noteren we $\mathcal{P}(X)$. Er geldt dus

$$\mathcal{P}(X) = \{S \text{ verzameling } \mid S \subset X\}$$

1.6 Bewerkingen met verzamelingen

De **doorsnede** van A en B is de verzameling $A \cap B = \{x \in A \mid x \in B\}$. Twee verzamelingen A en B heten **disjunct** indien $A \cap B = \emptyset$, d.w.z. ze hebben geen elementen gemeenschappelijk.

De **unie** van A en B is $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$. Het **verschil** van A en B is de verzameling $A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\}$.

Voorbeeld. Stel $A = \{1, 2, 3\}$ en $B = \{2, 3, 4, 5\}$. Dan geldt: $A \cap B = \{2, 3\}$, $A \cup B = \{1, 2, 3, 4, 5\}$, $A \setminus B = \{1\}$ en $B \setminus A = \{4, 5\}$

Als $A \subset B$, dan heet $B \setminus A$ het **complement** van A t.o.v. B. Soms speelt een wiskundige theorie zich volledig af in een gegeven verzameling U. In dat geval worden alle complementen berekend t.o.v. U (tenzij anders vermeld natuurlijk). Voor $A \subset U$ noteert men dan kort A^c, $\bar{A}$ of $\complement A$ voor het complement $U \setminus A$. De verzameling U noemt men het **universum** van de theorie.

1.7 Oneindige unies en doorsneden

Zij I een verzameling. Onderstel dat voor elke $i \in I$ een verzameling A_i gegeven is. Zo bekomen we een verzameling $\mathcal{A} = \{A_i \mid i \in I\}$ van verzamelingen **geïndexeerd** door I.

Voorbeeld. Stel $I = \{3, 4, 5, 6, 7\}$ en $A_i = \{1, 2, 3, \ldots, i\}$. Dan is $A_3 = \{1, 2, 3\}$, $A_4 = \{1, 2, 3, 4\}$ enz. Stel $J = \mathbb{N}_0$, $B_j = [0, \frac{1}{j}]$, een gesloten interval in $\mathbb{R}$. Dan is $B_1 = [0, 1]$, $B_2 = [0, \frac{1}{2}]$ enz.

De doorsnede van alle verzamelingen geïndexeerd door I definiëren we als

$$\bigcap \mathcal{A} = \bigcap_{i \in I} A_i = \{x \mid \forall\, i \in I : x \in A_i\}$$

en analoog definiëren we de unie

$$\bigcup \mathcal{A} = \bigcup_{i \in I} A_i = \{x \mid \exists\, i \in I : x \in A_i\}.$$

Voorbeeld. We keren terug naar de vorige voorbeelden. Er geldt:

$$\bigcup_{i \in I} A_i = A_7 \quad , \quad \bigcap_{i \in I} A_i = A_3$$

$$\bigcup_{j \in J} B_j = [0, 1] \quad , \quad \bigcap_{j \in J} B_j = \{0\}.$$

1.8 Cartesisch product

Zijn A, B twee verzamelingen. Het **cartesisch product** van A en B is de verzameling

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

De elementen van $A \times B$ heten **koppels**. Als $(a, b), (c, d) \in A \times B$ dan geldt $(a, b) = (c, d) \iff (a = c) \wedge (b = d)$. Als $a \neq b$ geldt $(a, b) \neq (b, a)$. In het algemeen zijn dus $A \times B$ en $B \times A$ verschillend. Als $A, B \subset U$ dan geldt $A \times B \subset U \times U$ en niet $A \times B \subset U$!

Als A en B eindig zijn geldt $|A \times B| = |A| \cdot |B|$.

Voorbeelden.

- Stel $A = \{2, 3\}$ en $B = \{4, 5, 6\}$. Vul dan zelf aan:
  - $A \times B = \ldots$
  - $B \times A = \ldots$
- Stel $A = [1, 3]$ en $B = [1, 2]$. Dan geldt $A \times B \subset \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Notatie. $A \times A$ noteren we kort A^2. Ook het Cartesisch product $A \times A \times \cdots \times A$ van n keer dezelfde verzameling schrijven we A^n.

1.9 Relaties

Een **relatie** van een verzameling A naar een verzameling B is per definitie een deelverzameling $\mathcal{R}$ van het cartesisch product $A \times B$.
Notatie. Als $(a, b) \in \mathcal{R}$, schrijven we $a\mathcal{R}b$.

Voorbeeld. Beschouw de verzameling $A = \{1, 2, 3, 4\}$ en de relatie "is kleiner dan of gelijk aan" op A. Dan is:

$$\begin{aligned} \mathcal{R} &= \{(a, b) \in A \times A \mid a \leq b\} \\ &= \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\} \end{aligned}$$

De **inverse relatie** $\mathcal{R}^{-1}$ van $\mathcal{R}$ is per definitie

$$\mathcal{R}^{-1} := \{(b, a) \mid (a, b) \in \mathcal{R}\}.$$

Dit is een relatie van B naar A.

Voorbeeld. Terugkerend naar het vorige voorbeeld geldt:

$$\mathcal{R}^{-1} = \{(1,1), (2,1), (3,1), (4,1), (2,2), (3,2), (4,2), (3,3), (4,3), (4,4)\}.$$

1.10 Functies

Zijn A, B verzamelingen. Een **functie** van A naar B is een relatie van A naar B waarbij elk element van A **precies één keer** voorkomt als eerste component van een koppel in de relatie. De verzameling A heet het **domein** van de functie en B is het **codomein**. Meestal noteren we functies met kleine letters en vermelden we duidelijk domein en codomein. Als $f \subset A \times B$ een functie is, noteren we $f : A \longrightarrow B$.

Voorbeeld. Als $A = \{1, 2, 3\}$ en $B = \{a, b, c, d\}$, dan is $f = \{(1, a), (2, b), (3, b)\}$ een functie en $\mathcal{R} = \{(1, a), (2, b), (2, a), (3, d)\}$ is een relatie maar geen functie.

Het woord **afbeelding** is een synoniem voor functie.

Zij $f : A \longrightarrow B$ een functie. Indien $(a, b) \in f$ noteren we $f(a) = b$. Het element $b \in B$ heet **beeld** van a door f en a heet een **origineel** van b voor f. We zeggen ook dat f het element a op het element b **stuurt**, notatie: $a \mapsto b$. Merk op: niet alle elementen van het codomein hebben een origineel, maar elk element van het domein heeft wel een beeld.

Voor vele functies bestaat er een "formule" om het beeld van een willekeurig element van het domein te berekenen. Dit heet het **functievoorschrift**. De volledige notatie voor een functie wordt dan:

$$f : A \longrightarrow B : a \longmapsto f(a)$$

waarbij $f(a)$ het functievoorschrift voorstelt.

Voorbeelden.

- $f \colon \mathbb{R} \longrightarrow \mathbb{R} \colon x \longmapsto x^2 + 5$
- $g \colon \mathbb{R} \longrightarrow \mathbb{R} \colon x \longmapsto \begin{cases} 5x & \text{als} \quad x \geq 0 \\ -2x & \text{als} \quad x < 0 \end{cases}$

Opmerking. Een functie wordt dus gedefinieerd door drie gegevens: domein, codomein en functievoorschrift, allen even belangrijk!

1.11 Beeld en invers beeld

Voor een functie $f : A \longrightarrow B$ en $S \subset A$ definiëren we het **beeld van** S door f als

$$\begin{aligned} f(S) &:= \{f(s) \mid s \in S\} \\ &:= \{b \in B \mid \exists\, s \in S, f(s) = b\} \end{aligned}$$

Dus geldt zeker $f(S) \subset B$.

De verzameling $f(A)$, het beeld van het hele domein van f, noemen we het **beeld van** f en noteren we ook als $\operatorname{Im} f$. Het beeld van f is dus een deel van het codomein.

Voorbeeld. Zij $f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2$. Dan is $f([-1, 2]) = [0, 4]$ en $\operatorname{Im} f = \mathbb{R}^+$. Uit dit voorbeeld leren we dat $\operatorname{Im} f$ dus in het algemeen niet gelijk is aan het codomein van f. Verwar dus niet beeld en codomein!

Nog steeds voor $f : A \longrightarrow B$ maar nu $T \subset B$, definiëren we het **invers beeld** van T onder f als

$$f^{-1}(T) := \{a \in A \mid f(a) \in T\}.$$

Merk op dat $f^{-1}(T)$ een notatie is en niet impliceert dat er voor f een inverse functie bestaat.

Als T een **singleton** $\{b\}$ is, schrijven we $f^{-1}(b)$ i.p.v. $f^{-1}(\{b\})$.

Voorbeeld. Met f zoals in het vorige voorbeeld hebben we: $f^{-1}(4) = \{-2, 2\}$, $f^{-1}(-1) = \emptyset$ en $f^{-1}(f([0, 1])) = f^{-1}([0, 1]) = [-1, 1]$.

In het algemeen geldt: $\forall\, S \subset A : f^{-1}(f(S)) \supset S$ en, zoals het voorbeeld toont, niet $f^{-1}(f(S)) = S$. We bewijzen dit even.

Bewijs. Zij $f : A \longrightarrow B$ een functie en $S \subset A$. We moeten bewijzen:

$$\forall\, s \in S : s \in f^{-1}(f(S)).$$

Dit is equivalent met

$$\forall\, s \in S : f(s) \in f(S) = \{f(t) \mid t \in S\},$$

wat duidelijk voldaan is. □

Je zal andere gelijkaardige eigenschappen in de oefeningen bewijzen.

1.12 Geïnduceerde functies, restrictie en corestrictie

Wanneer een functie $f\colon A \longrightarrow B$ gegeven is, kan je gemakkelijk een functie van $A \times A$ naar $B \times B$ definiëren: we beelden (a, a') gewoon af op $(f(a), f(a'))$. Algemeen kan je functies $A^n \longrightarrow B^n$ maken voor alle machten n. Je kan ook een functie maken op de delenverzameling $\mathcal{P}(A)$ van A. Door $\mathcal{P}(A) \longrightarrow \mathcal{P}(B)\colon S \longmapsto f(S)$.

We noteren al deze functies afgeleid uit f meestal nog altijd met f en noemen ze de functies door f **geïnduceerd** op $A \times A$ (of op A^n of op $\mathcal{P}(A)$).

We kunnen ook beslissen om de functie $f\colon A \longrightarrow B$ te bekijken op een deelverzameling X van A. Dan spreken we van de **restrictie** of **beperking** van f tot X. We noteren deze functie met $f|_X$. Er geldt dus

$$f|_X\colon X \longrightarrow B\colon x \longmapsto f(x)$$

We kunnen ook het codomein van de functie f beperken. Zij $Y \subset B$ zó dat $\forall\, a \in A\colon f(a) \in Y$. Dan is de **corestrictie** van f tot Y de functie

$$f|^Y\colon A \longrightarrow Y\colon x \longmapsto f(x)$$

We kunnen natuurlijk ook domein en codomein tegelijk beperken zodat we een functie $f|_X^Y\colon X \longrightarrow Y$ bekomen met voor elke $x \in X\colon f|_X^Y(x) = f(x)$.

1.13 Injecties en surjecties

Definitie 1. *Een functie $f : A \longrightarrow B$ heet **injectief** indien elk element van B hoogstens één keer voorkomt als tweede component van een koppel in f.*

Anders gezegd: elk element van B heeft hoogstens één origineel. Nog anders gezegd: indien twee elementen van A hetzelfde beeld hebben, moeten ze gelijk zijn. In symbolen: $f : A \longrightarrow B$ is injectief $\iff \forall a, b \in A : (f(a) = f(b)) \Rightarrow (a = b)$.

Voorbeeld. $f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2$ is *niet* injectief. Immers $1^2 = (-1)^2$ maar $1 \neq -1$. Anderzijds is $g : \mathbb{R}^+ \longrightarrow \mathbb{R} : x \mapsto x^2$ *wel* injectief want $a^2 = b^2 \iff a = \pm b$, maar aangezien $a, b \in \mathbb{R}^+$, geldt $a = b$.

We zien dat we een functie injectief kunnen maken door punten uit het domein weg te laten. De functie g uit het voorbeeld is gewoon de restrictie van f tot $\mathbb{R}^+$, of $f|_{\mathbb{R}^+}$.

Definitie 2. *Een functie $f : A \longrightarrow B$ is **surjectief** indien* $\operatorname{Im} f = B$.

Anders gezegd: elk element van het codomein heeft minstens één origineel. Symbolisch: $\forall\, b \in B : \exists\, a \in A : f(a) = b$.

Voorbeeld. $g : \mathbb{R}^+ \longrightarrow \mathbb{R} : x \longmapsto x^2$ is *niet* surjectief. De corestrictie $g|^{\mathbb{R}^+}$ is dat wel.

Door het codomein te beperken kan je een functie dus surjectief maken.

Een functie die tegelijk surjectief en injectief is, heet **bijectief**. Een functie is bijectief $\iff \forall\, b \in B : \exists!\, a \in A : f(a) = b$.

Voorbeeld. $h : \mathbb{R}^+ \longrightarrow \mathbb{R}^+ : x \longmapsto x^2$ is bijectief.

Een bijectie van een verzameling naar zichzelf heet een **permutatie**. Een zeer belangrijke permutatie is de **identieke permutatie** of de **identiteit**. Deze beeldt elk element af op zichzelf. We noteren de identieke permutatie van een verzameling X als 1_X. Er geldt dus $\forall\, x \in X : 1_X(x) = x$ of

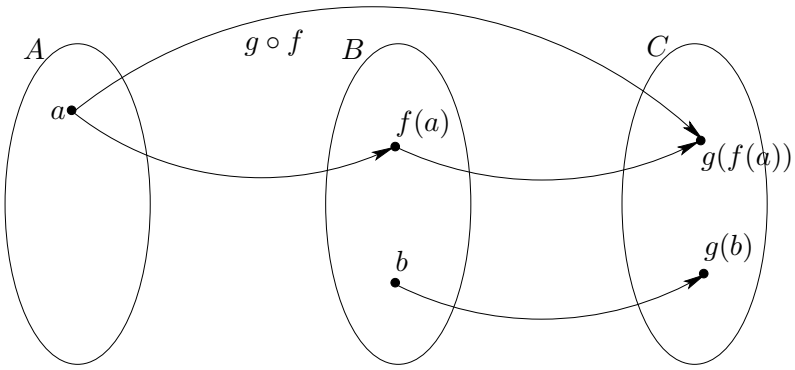
$$1_X : X \longrightarrow X : x \longmapsto x$$

Opmerking. Andere notaties voor de identieke permutatie op X zijn i_X, Id_X of id_X.

1.14 De samenstelling van functies

Beschouw twee functies $f : A \longrightarrow B$ en $g : B \longrightarrow C$, waarbij het domein van g het codomein van f is. Dan kunnen we op elk beeld $f(a)$ de functie g toepassen. Zo definiëren we een nieuwe functie van A naar C die we $g \circ f$ noteren (lees "g na f" omdat we eerst f toepassen en dan g). Dus:

$$g \circ f : A \longrightarrow C : a \mapsto g(f(a)).$$



Voorbeeld. Stel $f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x - 1$ en $g : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2$. Dan zijn:

$$\begin{aligned} &g \circ f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto g(x-1) = (x-1)^2 \\ &f \circ g : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2 - 1 \\ &f \circ f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x - 2 \\ &g \circ g : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^4 \end{aligned}$$

We merken op dat $f \circ g \neq g \circ f$, dus de volgorde heeft belang.

Eigenschap 1. *De samenstelling van functies is associatief: voor elke drie functies*

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

geldt

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Bewijs. Domeinen en codomeinen zijn duidelijk gelijk. Zij $a \in A$, dan

$$\begin{aligned}(h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a))) \\ &= (h \circ g)(f(a)) \\ &= ((h \circ g) \circ f)(a).\end{aligned}$$

□

1.15 Inverse functies

Definitie 3. *Zij $f : A \longrightarrow B$ een functie. Indien een functie $g : B \longrightarrow A$ voldoet aan*

$$f \circ g = 1_B \text{ en } g \circ f = 1_A$$

*dan heet g een **invers** voor f. We zeggen dan ook dat f **inverteerbaar** is.*

Niet alle functies hebben een invers. Een inverse g van $f : A \longrightarrow B$ moet een functie zijn van B naar A. Dus moet voor elke $b \in B$ precies één beeld $g(b) \in A$ voorzien worden. Bovendien moet gelden $(f \circ g)(b) = 1_B(b) = b$. Bijgevolg moet $g(b) \in f^{-1}(b)$. Opdat $g : B \longrightarrow A$ een functie zou zijn is dus nodig dat $\forall\, b \in B : f^{-1}(b) \neq \emptyset$. Dit komt erop neer dat f surjectief moet zijn.

Als $f : A \longrightarrow B$ surjectief is, zouden we als volgt een inverse $g : B \longrightarrow A$ kunnen construeren: voor elke $b \in B$ *kiezen* we een beeld $g(b)$ in $f^{-1}(b)$. Maar is zulke g dan een invers van f?

De voorwaarde $g \circ f = 1_A$ dwingt de injectiviteit van f. Inderdaad: als f niet injectief is, bestaan er $a \neq a' \in A$ met $f(a) = f(a')$. Stel $b := f(a)$, dan geldt $a, a' \in f^{-1}(b)$. Kiezen we dan als beeld van b door g het element a, dan hebben we $g(b) = a$, maar ook $g(b) = g(f(a')) = (g \circ f)(a') = 1_A(a') = a'$. Dus $a = a'$, wat in tegenspraak is met $a \neq a'$.

Als f een bijectie is, is $\forall\, b \in B : f^{-1}(b)$ een singleton. Er is dus geen keuze voor het construeren van de inverse g. De functie $g : B \longrightarrow A$ is dan wel degelijk een inverse van f.

We hebben bewezen:

Stelling 1. *Enkel bijectieve functies hebben een invers.*

Eigenschap 2. *Een functie heeft hoogstens één invers.*

Bewijs. Zij $f : A \longrightarrow B$ en zijn $g : B \longrightarrow A$ en $g' : B \longrightarrow A$ twee inversen. Dan geldt, $\forall\, b \in B$:

$$\begin{aligned} g(b) &= g(1_B(b)) \\ &= g((f \circ g')(b)) \\ &= (g \circ f \circ g')(b) \\ &= (g \circ f)(g'(b)) \\ &= 1_A(g'(b)) \\ &= g'(b). \end{aligned}$$

Vermits de domeinen en codomeinen van g en g' gelijk zijn, hebben we $g = g'$. □

Nu we weten dat elke inverteerbare functie *juist* één invers heeft, kunnen we spreken over *het* invers van een functie f in plaats van over *een* invers. We noteren de inverse functie f^{-1}. Verwar dit niet met inverse beelden die voor alle functies gedefinieerd zijn, niet enkel voor bijecties.

Voorbeeld. $h : \mathbb{R}^+ \longrightarrow \mathbb{R}^+ : x \mapsto x^2$ is een bijectie. Haar inverse is $h^{-1} : \mathbb{R}^+ \longrightarrow \mathbb{R}^+ : x \mapsto \sqrt{x}$.

1.16 Oefeningen

1. ○ Zij $p(x) =$"x is deelbaar door 10" en $q(x) =$"x is even".

   - schrijf $p(x)$ en $q(x)$ met symbolen
   - Geef de negatie van $p(x)$
   - Geef de conjunctie van $p(x)$ en $q(x)$
   - Schrijf "$q(x)$ impliceert $p(x)$", en de contrapositie ervan
   - Schrijf de equivalentie van $p(x)$ en $q(x)$ op

   Zeg van deze uitspraken of ze waar zijn of niet.

2. ◐ Stel de waarheidstafel op van de exclusieve of (Xor). Ken je een uitdrukking die equivalent is?

3. ○ Geef de waarheidstafels van

   - $(p \Rightarrow q) \Rightarrow (q \Rightarrow p)$
   - $q \Leftrightarrow (\neg p \vee \neg q)$
   - $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

4. ○ Toon aan dat $\neg(p \vee q)$ en $\neg p \wedge \neg q$ logisch equivalent zijn. Wat kan je zeggen over $\neg(p \wedge q)$ en $\neg p \vee \neg q$?

5. ○ Toon aan dat $p \Leftrightarrow q$ en $(p \Rightarrow q) \wedge (q \Rightarrow p)$ logisch equivalent zijn.

6. ◐ Het aantal rijen van een waarheidstabel hangt af van het aantal samenstellende uitspraken. Wat is het verband?

7. ○ Schrijf de waarheidstafels op voor volgende logische uitspraken en leid er een equivalente vorm voor de uitspraak uit af:

   - $\neg(\neg p)$
   - $\neg(p \wedge q)$
   - $\neg(p \vee q)$
   - $\neg(p \Leftarrow q)$
   - $\neg(p \Leftrightarrow q)$

8. ◐ Een tautologie (of logische wet) is een uitspraak die steeds waar is. Toon aan dat volgende beweringen tautologieën zijn en interpreteer:

- $\neg(p \wedge (\neg p))$
- $p \vee (\neg p)$
- $(p \wedge p) \Leftrightarrow p$
- $(p \wedge q) \Leftrightarrow (q \wedge p)$
- $(p \vee (q \vee r)) \Leftrightarrow ((p \vee q) \vee r)$
- $\neg(\neg p) \Leftrightarrow p$
- $p \Rightarrow (q \Rightarrow p)$
- $\neg p \Rightarrow (p \Rightarrow q)$
- $(p \Rightarrow q) \vee (q \Rightarrow p)$

9. ○ Is $p \Rightarrow (q \Rightarrow p)$ logisch equivalent met $(p \Rightarrow q) \Rightarrow p$?

10. ○ Noteer volgende oefeningen met behulp van kwantoren. Bepaal eventueel of de bewering waar of vals is. Schrijf de negatie van de bewering op met kwantoren en met woorden.

    (a) "Alle mensen zijn slim."

    (b) "Er zijn mensen die groot zijn."

    (c) "Er zijn mensen die groot zijn en lang haar hebben."

    (d) "Niet alle mensen hebben kort haar."

    (e) "Alle wegen leiden naar Rome."

    (f) "Voor elke mens geldt: als hij groot is, dan is hij niet klein."

    (g) "Een geheel getal is positief."

    (h) "Elk natuurlijk getal is even."

    (i) "Sommige reële getallen zijn positief."

11. ○ Schrijf alle deelverzamelingen van $\{1, 2, 3\}$.

12. ◐ Hoeveel deelverzamelingen heeft een verzameling met 2 elementen? Met 3 elementen? Met n elementen?

13. ◐ Wanneer behoort een element niet tot $A \cap B$? Vul aan: $x \notin A \cap B \Leftrightarrow \ldots$

14. ◐ analoog: $x \notin A \cup B \Leftrightarrow \ldots$

15. ◐ analoog: $x \notin A \backslash B \Leftrightarrow \ldots$

16. ◐ Toon aan dat

    - $B \supset A \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A$
    - $A \cup (A \cap B) = A$
    - $A \cap (A \cup B) = A$

17. ◐ Wanneer is $x \notin \bigcup_{i \in I} A_i$?

18. ◐ Geef de betekenis in woorden van de volgende uitspraken. Zeg of ze waar of onwaar zijn. Geef de negatie in symbolen en woorden.

    - $\forall\, x \in \mathbb{Z}, \exists\, y \in \mathbb{Z} : x < y$
    - $\exists\, x \in \mathbb{Z}, \exists\, y \in \mathbb{N} : x > y$
    - $\exists\, x \in \mathbb{Z}, \forall\, y \in \mathbb{Z} : x < y$
    - $\forall\, \varepsilon > 0, \exists\, \delta > 0, \forall\, x \in \mathbb{R} : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon$

19. ○ Zij $A = \{2, 3\}$, $B = \{4, 5, 6\}$ en $C = \{a, b, c, d\}$. Geef $A \times B$, $B \times A$, $A \times C$, $C \times B$, A^2, $C \times \{a\}$.

20. ○ Zij $A = \{1, 2, 3, 4\}$ en beschouw de relatie $\mathcal{R}$: "is kleiner dan of gelijk aan" op A. Geef de elementen van $\mathcal{R}$. Geef de inverse relatie van $\mathcal{R}$.

21. ◐ Zij $f : A \longrightarrow B$ een functie en $S_1, S_2 \subset A$. Bewijs dat

    (a) $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$
    (b) $f(S_1 \cap S_2) \subset f(S_1) \cap f(S_2)$

    Zoek voorbeelden die dit illustreren.

22. ◐ Zij $f : A \longrightarrow B$ een functie die niet noodzakelijk inverteerbaar is, en $S \subset A$ en $T, T_1, T_2 \subset B$. Bewijs dat

    (a) $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$
    (b) $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap$
    (c) $f(f^{-1}(T)) \subset T$
    (d) $f^{-1}(f(S)) \supset S$

    Zoek voorbeelden die dit illustreren.

23. ◐ Toon aan: $f : A \longrightarrow B$ is injectief $\iff$ $\forall b \in B : f^{-1}(b)$ bevat hoogstens één element.

24. ◐

    (a) Zij $f : A \longrightarrow B$. Toon aan dat $f \circ 1_A = f = 1_B \circ f$.
    (b) Toon aan dat de samenstelling van 2 injecties opnieuw een injectie is.
    (c) Toon aan dat de samenstelling van 2 surjecties opnieuw een surjectie is.

25. ○ Zij $f(x) = \sqrt{x}$, $g(x) = x/4$ en $h(x) = 4x - 8$. Zoek het functievoorschrift voor:

    (a) $h \circ g \circ f$ (c) $g \circ h \circ f$ (e) $f \circ g \circ h$
    (b) $h \circ f \circ g$ (d) $g \circ f \circ h$ (f) $f \circ h \circ g$

26. ○ Zij $f(x) = x - 3$, $g(x) = \sqrt{x}$, $h(x) = x^3$ en $j(x) = 2x$. Schrijf de volgende functies als een samenstelling van de bovenstaande:

    (a) $\sqrt{x-3}$ (e) $\sqrt{(x-3)^3}$ (i) x^9
    (b) $2\sqrt{x}$ (f) $(2x-6)^3$ (j) $x - 6$
    (c) $x^{1/4}$ (g) $2x - 3$ (k) $2\sqrt{x-3}$
    (d) $4x$ (h) $x^{3/2}$ (l) $\sqrt{x^3 - 3}$

27. ◐ Toon aan voor inverteerbare functies f en g:

    (a) $(f^{-1})^{-1} = f$ (b) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

28. ◐ Onderzoek of volgende functies inverteerbaar zijn. Zo ja, bepaal de inverse functies. Zo nee, definieer een bijectie $\tilde{f}$ met hetzelfde voorschrift als f en bepaal $(\tilde{f})^{-1}$.

    (a) $f : \mathbb{R} \to \mathbb{R} : x \mapsto |x|$ (e) $f : \mathbb{R} \to \mathbb{R} : x \mapsto \sqrt[3]{2x} + 2$
    (b) $f : \mathbb{R} \to \mathbb{R} : x \mapsto x + 1$ (f) $f : \mathbb{R} \to \mathbb{R} : x \mapsto 1$
    (c) $f : \mathbb{R} \to \mathbb{R} : x \mapsto 2x + 3$ (g) $f : \mathbb{R}_0 \to \mathbb{R} : x \mapsto \frac{2x-3}{x}$
    (d) $f : \mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto \sqrt{x}$ (h) $f : \mathbb{R} \to \mathbb{R} : x \mapsto \sin x$

29. ◐ Zij $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : h(x, y) = 2x + 3y$. Bepaal het beeld van h. Is h injectief? Surjectief?

30. ◐ Bewijs: $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$ als f injectief is (zie oef. 21). Geef een voorbeeld van een functie waarbij $f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2)$.

31. ◐ Bepaal of volgende functies injectief zijn. Geef hun beeld.

    (a) $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto 2x + 1$ (d) $f : \mathbb{R} \to \mathbb{R} : x \mapsto e^x$
    (b) $f : \mathbb{Q} \to \mathbb{Q} : x \mapsto 2x + 1$ (e) $f : [-\pi/2, \pi/2] \to \mathbb{R} : x \mapsto \sin x$
    (c) $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto x^3 - x$

(f) $f : [0, \pi] \to \mathbb{R} : x \mapsto \sin x$

32. ◐ Stel $f : A \to B$, met $A = X \cup Y$ en $X \cap Y = \emptyset$. Als $f_{|X}$ en $f_{|Y}$ injectief zijn, wat kan je dan zeggen van f?

33. ○ Bepaal voor elk van de volgende functies $f : \mathbb{Z} \to \mathbb{Z}$ of ze injectief of surjectief zijn. Indien niet surjectief, bepaal $f(\mathbb{Z})$:

(a) $f(x) = x + 7$ (c) $f(x) = -x + 5$ (e) $f(x) = -x^2 + x$
(b) $f(x) = 2x - 3$ (d) $f(x) = x^2$ (f) $f(x) = x^3$

34. ○ Zelfde vraag als oefening 33, waarbij f als een functie van $\mathbb{R}$ naar $\mathbb{R}$ beschouwd wordt.

35. ◐ Toon aan: als A en B verzamelingen zijn, dan geldt: $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$. [examen augustus 2005]

36. ◐ Vul aan (gebruik $\subset$, $\supset$ of $=$) en bewijs: als A en B verzamelingen zijn, dan geldt:

$$(A \times B) \cup (B \times A) \quad \ldots \quad (A \cup B) \times (A \cup B).$$

[examen augustus 2005]

Hoofdstuk 2

Eenvoudige principes van discrete wiskunde

2.1 De duiventil

We weten allemaal zeer goed dat als we 25 duiven in 20 hokjes moeten verdelen, er minstens één hokje zal zijn met meer dan één duif.

Stelling 2 (Principe van de **duiventil**)**.** *Als we n identieke objecten verdelen over k dozen met $n > k$, dan is er minstens één doos met minstens twee objecten.*

Bewijs. Uit het ongerijmde (U.H.O.)

Veronderstel van niet. Dan is er in elke doos hoogstens één object. Zij m het aantal lege dozen (met nul objecten dus). Dan zijn er in totaal $k - m$ dozen met elk juist één object. Vermits alle objecten verdeeld werden, geldt

$$n = k - m \leq k < n$$

en dat is een tegenspraak. □

Toepassing. Bekijk de rij 7, 77, 777, 7777, ... van natuurlijke getallen die enkel het cijfer 7 bevatten. Is één van die getallen deelbaar door 2013? We gaan bewijzen dat het antwoord ja is. Sterker zelfs:

Gevolg 1. *In de eerste* 2013 *elementen van bovenstaande rij zit minstens één veelvoud van* 2013*.*

Bewijs. We noteren de eerste elementen van de rij $a_1, a_2, \ldots, a_{2013}$.

Voor twee getallen a en b kunnen we steeds quotiënt q en rest r bepalen zodat $a = qb + r$ met $0 \leq r < b$. Doe dit nu voor alle getallen in de rij. Dus $\forall i \in \{1, \ldots, 2013\}$ bepalen we q_i en r_i zó dat $a_i = 2013q_i + r_i$.

Als er een i bestaat met $r_i = 0$, dan is a_i deelbaar door 2013 en is er niets meer te bewijzen. Veronderstel nu, uit het ongerijmde, dat geen enkele r_i nul is. Dan is $\{r_1, r_2, \ldots, r_{2013}\}$ een deelverzameling van $\{1, 2, \ldots, 2012\}$, de mogelijke niet-nulle resten bij deling door 2013. De duiventil leert ons dat minstens twee resten gelijk zijn. Dus $\exists i \neq j \in \{1, \ldots, 2013\}$ met $r_i = r_j$. We mogen, zonder de algemeenheid te schaden, aannemen dat $a_i > a_j$. Bekijk nu het verschil $a_i - a_j$: enerzijds is

$$\begin{array}{rcccl} & a_i & = & 77\ldots7777\ldots77 \\ - & a_j & = & \qquad\qquad 77\ldots77 \\ \hline a_i & - \; a_j & = & \underbrace{77\ldots77}_{a_{i-j}}00\ldots00 \end{array}$$

of dus $a_i - a_j = \underbrace{77\ldots77}_{a_{i-j}} \times 10^j$.

Anderzijds is $a_i - a_j = (2013q_i + r_i) - (2013q_j + r_j) = 2013(q_i - q_j) + 0$, aangezien $r_i = r_j$. Dus $a_i - a_j = a_{i-j} \times 10^j$ is een veelvoud van 2013.

Dit wil zeggen dat $a_{i-j} \times 10^j$ deelbaar is door 2013, maar vermits 10^j geen enkele deler gemeenschappelijk heeft met 2013, moet a_{i-j} een veelvoud zijn van 2013. We bekomen een tegenspraak en dus is het gestelde bewezen. □

Voorbeeld. In een groep van 100 mensen zijn er minstens 9 die hun verjaardag vieren in dezelfde maand. Inderdaad; onderstel dat er geen 9 hun verjaardag in dezelfde maand hebben, dan zijn er hoogstens $8 \times 12 = 96$ mensen. Strijdig!

Notatie. Zij $x \in \mathbb{R}$. Dan noteren we:

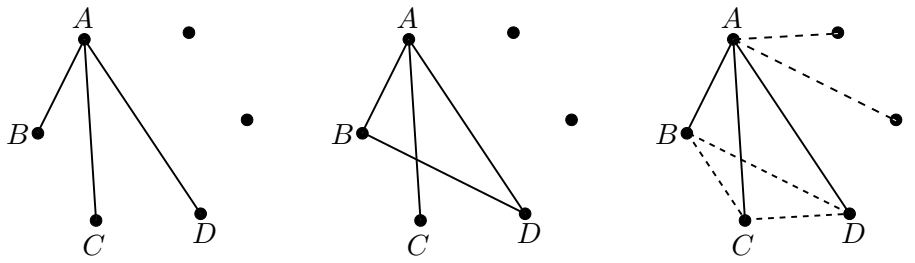
$$\lceil x \rceil = \text{kleinste geheel getal} \geq x$$

$$\lfloor x \rfloor = \text{grootste geheel getal} \leq x$$

Het voorbeeld illustreert de **veralgemeende duiventil**. Als je n identieke objecten verdeelt over k dozen, dan is er minstens één doos met minstens $\lceil \frac{n}{k} \rceil$ objecten. Het bewijs is analoog met dat van de "gewone" duiventil.

Voorbeeld. In een groepje van 6 mensen zijn elke twee individu's ofwel vrienden ofwel vijanden. Men kan met zekerheid zeggen dat er in deze groep drie mensen zijn die ofwel 2 aan 2 vijanden zijn, ofwel 2 aan 2 vrienden.

Bewijs. Zij A één van die personen. De overblijvende 5 personen vallen uiteen in 2 groepen, de vrienden van A en de vijanden van A. Door het veralgemeend principe van de duiventil bevat één van die twee groepen minstens $\lceil \frac{5}{2} \rceil = 3$ personen. Onderstel dat we dus minstens 3 vrienden hebben (het geval dat er minstens 3 vijanden zijn verloopt analoog). We noemen B, C, D drie van die vrienden (zie figuur 2.1). Als twee van de drie bevriend zijn is het bewijs gedaan. Als geen twee van de drie bevriend zijn, hebben we drie personen gevonden die 2 aan 2 vijanden zijn. □



Figuur 2.1: Illustratie van het bewijs. In de derde tekening zijn voor de duidelijkheid de vijanden verbonden met streepjeslijnen.

Opmerking. In dit bewijs gebruikten we een voorstelling van het probleem met punten en verbindingen. Zulks heet een **graaf**. We zullen dit concept nauwkeurig definiëren en bestuderen in Hoofdstuk **??**.

2.2 Eenvoudige teltechnieken

Laat ons terugdenken aan het bewijs van het veralgemeende principe van de duiventil. We tellen de objecten in de verschillende dozen op en komen zo tot een contradictie omdat het totaal aantal objecten niet bereikt is. Als we objecten tellen in dozen komt het er eigenlijk op neer dat we elementen tellen in disjuncte verzamelingen.

2.2.1 Tellen

Twee eindige verzamelingen A en B evenveel elementen hebben als en slechts als er een bijectie $A \longleftrightarrow B$ bestaat.

We gaan nu meer formeel definiëren wat we bedoelen met "aantal elementen in een eindige verzameling". Als we elementen van een verzameling

A tellen, gaan we ze eigenlijk nummeren: je neemt een *eerste* element weg uit de verzameling, dan een *tweede* enz. tot er geen meer zijn.

Dit resulteert in een bijectie f tussen de verzameling $\{1, 2, \ldots, n\}$ en A met $f(i) = i$-de element van A in onze selectie.

Notatie. $[n] := \{1, 2, \ldots, n\}$. Meer algemeen is $[1..n] = [n]$, maar ook $[0..n] = \{0, 1, \ldots, n\}$ en $[-k..l] = \{-k, -k+1, \ldots, l-1, l\}$.

Definitie 4. *Een verzameling A heeft $n \in \mathbb{N}$ elementen indien er een bijectie bestaat van $[n]$ naar A. Deze bepaalt een* ***ordening*** *of* ***nummering*** *van A.*

Notatie. Als $|A| = n$ en $f : [n] \longrightarrow A$ een nummering is, dan schrijven we dikwijls a_i i.p.v. $f(i)$.

Hoeveel deelverzamelingen heeft een eindige verzameling X? We kunnen de elementen van X nummeren : $X = \{x_1, x_2, \ldots, x_n\}$. We stellen ons dus eigenlijk de vraag op hoeveel manieren we een aantal elementen uit X kunnen kiezen om een deelverzameling te vormen. Het eerste element x_1 kan geselecteerd worden of niet. Er zijn dus twee keuzes. Ook x_2 kan wel of niet tot de deelverzameling behoren. We zien dus dat er voor elk element apart kan beslist worden om het in de deelverzameling te stoppen of niet. We moeten dus n keer kiezen tussen twee mogelijkheden. In totaal zijn er dus 2^n deelverzamelingen van X. We hebben net bewezen

Stelling 3. *Voor elke eindige verzameling X geldt*

$$|\mathcal{P}(X)| = 2^{|X|}$$

Opmerking. Deze stelling verklaart waarom sommige auteurs de notatie 2^X gebruiken in plaats van $\mathcal{P}(X)$ om de verzameling van deelverzamelingen van X aan te duiden.

2.2.2 Somprincipe

Stelling 4 (Somprincipe). *Zijn $A_1, A_2, \ldots, A_k$ twee aan twee disjuncte eindige verzamelingen. Dan geldt:*

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.$$

Bewijs. Dit is intuïtief weer zeer vanzelfsprekend. We hebben bijecties $f_i : [n_i] \longrightarrow A_i$ voor $i \in [k]$. Merk op dat

$$[\sum_{i=1}^{k} n_i] = [1..n_1] \cup [(n_1+1)..(n_1+n_2)] \cup \cdots \cup [(\sum_{i=1}^{k-1} n_i) + 1.. \sum_{i=1}^{k} n_i].$$

Definieer

$$f : [\sum_{i=1}^{k} n_i] \longrightarrow A_1 \cup A_2 \cup \cdots \cup A_k$$

door

$$f(i) = f_j(i - \sum_{l=1}^{j-1} n_l) \quad \text{als} \quad i \in [(\sum_{l=1}^{j-1} n_l) + 1 .. \sum_{l=1}^{j} n_l].$$

Verifieer zelf dat f een bijectie is. Vergeet hierbij niet dat alle verzamelingen disjunct zijn. □

Later zullen we dit veralgemenen en ook niet-ledige doorsneden toelaten.

2.3 Teltechnieken met producten

2.3.1 Dubbeltellen

Je gaat met vrienden iets drinken. Iedereen trakteert een rondje. Op het einde van de avond willen jullie weten hoeveel glazen water er in totaal gedronken zijn. Dit kan je enerzijds te weten komen door aan iedereen te vragen hoeveel glazen water hij gedronken heeft die avond en dan alles op te tellen. Of je kan aan iedereen vragen hoeveel watertjes hij betaalde in zijn ronde en dan alles optellen.

We kunnen dus hetzelfde op twee manieren tellen.

Stelling 5 (Principe van de **dubbeltelling**)**.** *Zij A en B twee (eindige) verzamelingen. Zij $S \subset A \times B$. Stel voor elke $a \in A$: $k_a := |\{(a,b) \mid b \in B \text{ en } (a,b) \in S\}|$ en voor elke $b \in B$: $r_b := |\{(a,b) \mid a \in A \text{ en } (a,b) \in S\}|$. Dan geldt:*

$$\sum_{a \in A} k_a = |S| = \sum_{b \in B} r_b.$$

Bewijs. Stel $K_a := \{(a,b) \mid b \in B \text{ en } (a,b) \in S\}$. De verzamelingen $(K_a)_{a \in A}$ zijn disjunct. Dus

$$|S| = |\bigcup_{a \in A} K_a| = \sum_{a \in A} k_a.$$

Analoog met $R_b := \ldots$ voor de rijen. □

Gevolg 2. *Als alle k_a gelijk zijn aan een zekere constante k en alle r_b gelijk zijn aan r dan geldt $k|A| = r|B|$.*

Toepassing. De dodecaëder heeft 30 ribben want er zijn 12 zijvlakken met elk 5 ribben en elke ribbe ligt op 2 zijvlakken. We tellen de koppels (ribbe, zijvlak) op twee manieren:

$$\#\text{ribben} \times 2 = 12 \times 5.$$

2.3.2 Woorden

Zij $f : [m] \longrightarrow Y$ een functie. Deze bepaalt m elementen van Y, namelijk $f(1), f(2), \ldots, f(m)$. Ook elk m-tupel in Y^m bepaalt een functie $[m] \longrightarrow Y$. Als je bijvoorbeeld het m-tupel $(y_1, y_2, \ldots, y_m)$ neemt, stel dan gewoon $f(i) := y_i$.

Een **woord** van **lengte** m over het alfabet Y is gewoon een m-tupel elementen uit Y. Elk woord bepaalt dus een functie en omgekeerd.

Stelling 6. *Zijn X, Y eindige verzamelingen, met $|X| = m$ en $|Y| = n$. Dan geldt:*

$$\#\{\textit{functies } f : X \longrightarrow Y\} = n^m.$$

Bewijs. Elke functie komt overeen met een m-tupel van Y en we weten

$$|Y^m| = |\underbrace{Y \times Y \times \cdots \times Y}_{m \text{ keer}}| = |Y|^m.$$

□

Voorbeeld. Het aantal woorden van lengte 3 in ons alfabet is 26^3.

Opmerking. Een woord maken komt erop neer dat we uit ons alfabet *achtereenvolgend* een letter kiezen. *Herhalingen* zijn toegestaan. Je kan je ook inbeelden dat de letters van het alfabet gedrukt staan op 26 bollen in een bokaal. Je neemt dan telkens een bol, kijkt naar de letter die erop staat en *legt hem dan terug.*

Voorbeeld. Het aantal deelverzamelingen van een verzameling met n elementen is 2^n.

2.3.3 Injecties tellen

Als we geen herhaling toelaten, bekijken we woorden waarin de functie $[m] \longrightarrow Y$ injectief is. Hoe tellen we het aantal injectieve functies?

Stelling 7. *Het aantal geordende keuzes van m objecten uit n zonder herhaling is*

$$n(n-1)(n-2)\cdots(n-m+1).$$

Bewijs. Om zo een woord te vormen moeten we achtereenvolgend m verschillende elementen van Y kiezen. Voor de eerste letter zijn er n keuzes, voor de tweede $n-1$ (want we mogen om het even welke letter nemen behalve die die we als eerste kozen). Voor de derde letter $n-2$ keuzes enz. tot we de laatste letter kiezen uit de $n-m+1$ die overblijven. □

Notatie. De **faculteit** (Engels: "factorial", Frans: "factorielle") van een natuurlijk getal $n \in \mathbb{N}$ is het getal

$$n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$$

Per definitie stellen we $0! = 1$ (we zullen dit later motiveren).

Het aantal keuzes in stelling 7 is bijgevolg kort te noteren als

$$\frac{n!}{(n-m)!}.$$

Voorbeeld. Op hoeveel manieren kan ik 6 studenten uit de klas kiezen en in een rij tegen het bord zetten?

2.3.4 Bijecties tellen

Wat als in vorige stelling $n = m$? Dan staat er: we kunnen op $n!$ verschillende manieren n objecten kiezen waarbij de volgorde van belang is. Dit betekent dat we de bijecties $[n] \longleftrightarrow Y$ tellen, want als $f : [n] \to Y$ injectief is met $|Y| = n$, dan is f een bijectie (oefening). Een selectie van n objecten uit n kunnen we zien als een **(her)ordening** van die objecten.

Een bijectie $f : Y \longrightarrow Y$ van een verzameling naar zichzelf noemt men een **permutatie**. Een permutatie $f : Y \longrightarrow Y$ is een (her)ordening van Y. Vermits $|Y| = n$, hebben we een bijectie (of ordening) $g : [n] \longrightarrow Y$. We kunnen dus ook spreken van een **permutatie** van n objecten.

De samenstelling $f \circ g : [n] \longrightarrow Y$ is ook een ordening van Y. Twee ordeningen $f, g : [n] \longleftrightarrow Y$ geven ook aanleiding tot een permutatie $Y \longleftrightarrow Y$. Inderdaad: vermits f en g bijecties zijn, zijn ze inverteerbaar. $g \circ f^{-1} : Y \longleftrightarrow Y$ is dan een permutatie.

2.3.5 Deelverzamelingen tellen

Zij A een verzameling en $k \in \mathbb{N}$. Een **k-deelverzameling** van A is een deelverzameling met k elementen.

Gegeven is $|A| = n$. Hoeveel k-deelverzamelingen heeft A?

Kiezen we k elementen uit A *met* ordening, dan zullen we eenzelfde deelverzameling meerdere keren kiezen. Beschouw de verzameling

$$S = \{(B, f) \mid B \subset A, |B| = k \text{ en } f \text{ een ordening van } B\}.$$

Dan kunnen we $|S|$ op twee manieren tellen: enerzijds

$$|S| = x \times k!$$

met x het aantal k-deelverzamelingen van A en $k!$ het aantal ordeningen van een gegeven k-deelverzameling. Anderzijds is

$$|S| = 1 \times \frac{n!}{(n-k)!}$$

want we kunnen op $n!/(n-k)!$ manieren k elementen kiezen uit A met volgorde. Natuurlijk bepaalt elk van die keuzes *juist* één k-deelverzameling. We hebben dus

$$x = \frac{n!}{(n-k)!\,k!}.$$

Voor $n \geq k$ noteren we

$$\frac{n!}{(n-k)!\,k!}$$

als

$$\binom{n}{k}.$$

We hebben bewezen:

Stelling 8. *Het aantal keuzes van k elementen uit een verzameling van n elementen, zonder volgorde en zonder herhaling, bedraagt*

$$\binom{n}{k}.$$

We merken ook nog op dat

$$\binom{n}{n-k} = \binom{n}{k}.$$

Notatie. De verzameling van alle k-deelverzamelingen van A noteren we $\binom{A}{k}$ zodat $\left|\binom{A}{k}\right| = \binom{|A|}{k}$.

Eigenschap 3 (Identiteit van Pascal)**.** *Zij $n, k \in \mathbb{N}_0$ met $k \leq n$. Dan geldt*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Bewijs. We zouden dit kunnen bewijzen aan de hand van de definitie (oefening), maar we geven hier een interessanter bewijs. We weten dat $\binom{n}{k}$ gelijk is aan het aantal k-deelverzamelingen in een verzameling A met n elementen. Kies nu een a vast in A. Dan is de verzameling van k-deelverzamelingen van A de disjuncte unie van

$$D_\in := \{B \in \binom{A}{k} \mid a \in B\} \quad \text{en} \quad D_\notin := \{B \in \binom{A}{k} \mid a \notin B\}.$$

We hebben dus $\binom{n}{k} = \left|\binom{A}{k}\right| = |D_\in| + |D_\notin|$. Dan bepalen we $|D_\in|$ als volgt: een element van $D_\in$ is een k-deelverzameling van A die a bevat. Zulke verzameling kunnen we maken door in $A \setminus \{a\}$ een verzameling met $k-1$ elementen te kiezen en hier a aan toe te voegen. Dit kan op $\binom{n-1}{k-1}$ manieren. De verzamelingen in $D_\notin$ bestaan uit k elementen gekozen uit $A \setminus \{a\}$. Dus is $|D_\notin| = \binom{n-1}{k}$. □

Deze stelling geeft aanleiding tot de beroemde **driehoek van Pascal**[1]:

$$\begin{array}{ccccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & \\
 & & \cdots & & \cdots & & \cdots & & \cdots & & \cdots & & & &
\end{array}$$

of

$$\begin{array}{ccccccccccccccc}
 & & & & & & 1 & & & & & & & & \\
 & & & & & 1 & & 1 & & & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & \\
\cdots & & \cdots & & \cdots & & \cdots & & \cdots & & \cdots & & \cdots & & \cdots
\end{array}$$

waarbij de getallen op de zijkant altijd 1 zijn, en de andere getallen telkens de som zijn van de twee getallen die op de rij erboven links en rechts ervan staan.

[1] (her)ontdekt door de Franse wiskundige Blaise Pascal (1623–1662) in 1653. Eerder ontdekt door de Chinese wiskundige Yang Hui in 1261.

2.3.6 Herhalingscombinaties

Stel $A = \{a, b, c, d\}$. De keuze *bcadabd* is equivalent met de keuze *aabbcdd* wanneer de volgorde geen rol speelt. Hoeveel mogelijkheden zijn er zo?

We moeten hier dus de woorden tellen die bestaan uit een aantal a's, gevolgd door een aantal b's, dan een aantal c's enz. zodat er in totaal 7 letters zijn. Let wel, het aantal in kwestie kan soms nul zijn: *bbbbbbb* is ook een woord van zeven letters met herhaling!

Een voorstelling van *aabbcdd* is •• | •• | • | ••. In totaal hebben we dus 10 tekens waarvan elk een • of een | is. We zetten een • voor elke letter en een | als de letter verandert. Dus | •• || • • • • • stelt het woord *bbddddd* voor: er zijn geen a's omdat er voor de eerste | geen • staat, en geen c's omdat er tussen de tweede en de derde | geen • staan.

In het algemeen hebben we n objecten waarin we k keer kiezen met terugleggen en geen rekening houden met de volgorde. Het aantal manieren om dat te doen is het aantal manieren om $n-1$ streepjes te plaatsen als er $n+k-1$ plaatsen beschikbaar zijn. Dit is dus $\binom{n+k-1}{n-1}$. We weten $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$ zodat het aantal **herhalingscombinaties** van k objecten uit n gelijk is aan

$$\binom{n+k-1}{k}.$$

We tonen nog even een interessante eigenschap van de getallen $\binom{n}{k}$.

Eigenschap 4. *Voor $n \in \mathbb{N}$ geldt*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0.$$

Bewijs. We weten dat $\binom{n}{0} = \binom{n-1}{0} = \binom{n}{n} = \binom{n-1}{n-1} = 1$ zodat het linkerlid via de Pascal-identiteit kan herschreven worden als

$$1 - \left[1 + \binom{n-1}{1}\right] + \left[\binom{n-1}{1} + \binom{n-1}{2}\right] - \cdots + (-1)^{n-1}\left[\binom{n-1}{n-2} + 1\right] + (-1)^n \times 1.$$

De tweede term tussen de eerste vierkante haken valt weg tegen de eerste term tussen de tweede vierkante haken. Analoog valt de tweede term tussen de tweede haken weg tegen de eerste term tussen de derde haken, enz. Uiteindelijk blijft er over

$$1 - 1 + (-1)^{n-1} \times 1 + (-1)^n \times 1 = 0.$$

□

2.4 Het binomium van Newton

We kennen reeds zeer lang volgende formules: $(a+b)^2 = a^2 + 2ab + b^2$ en $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. Algemeen geldt:

Stelling 9 (**Binomium van Newton**).

$$\begin{aligned}(a+b)^n &= \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \cdots + \binom{n}{n}a^0 b^n \\ &= \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i\end{aligned}$$

Bewijs. De macht

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ keer}}$$

werken we uit aan de hand van de distributiviteit. De term met $a^{n-i}b^i$ ontstaat door in i factoren $(a+b)$ de b te kiezen (en in de overige natuurlijk de a). De coëfficiënt die hoort bij $a^{n-i}b^i$ is bijgevolg gelijk aan het aantal keuzes van i objecten uit n. Dat is $\binom{n}{i}$. □

Je kan dus de driehoek van Pascal gebruiken om de coëfficiënten van elke macht te vinden in $(a+b)^n$.

De naam *binomium* komt van *binoom*, een geleerd woord voor tweeterm (een ander woord voor veelterm is trouwens *polynoom*). Daarom heten de getallen $\binom{n}{k}$ ook **binomiaal-coëfficiënten**.

Voorbeeld. De letters a en b in het binomium kunnen om het even wat zijn. Bijvoorbeeld:

$$(1-x)^7 = 1 - 7x + 21x^2 - 35x^3 + 35x^4 - 21x^5 + 7x^6 - x^7.$$

Het binomium kan ook gebruikt worden om andere eigenschappen van binomiaalcoëfficiënten aan te tonen.

Stelling 10. *Voor alle $n \in \mathbb{N}$ geldt:*

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

Bewijs. We weten dat $(1+x)^n(1+x)^n = (1+x)^{2n}$. We passen nu op het rechterlid het binomium toe:

$$(1+x)^n(1+x)^n = \binom{2n}{0} + \binom{2n}{1}x + \cdots + \binom{2n}{n}x^n + \cdots + \binom{2n}{2n}x^{2n}.$$

De coëfficiënt van de term in het midden van het rechterlid is het rechterlid van wat we willen bewijzen.

Nu zijn twee veeltermen gelijk als en slechts als de coëfficiënten van de overeenkomstige machten van x gelijk zijn. We gaan dus de coëfficiënt zoeken van x^n in $(1+x)^n(1+x)^n$. We krijgen een bijdrage tot de coëfficiënt van x^n telkens wanneer we in de eerste factor de term met x^k vermenigvuldigen met de term met x^{n-k} in de tweede factor. Hierbij is $0 \leq k \leq n$.

Het binomium leert ons dat

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$$

zodat de bijdrage tot de coëfficiënt van x^n die komt van $x^k x^{n-k}$ gelijk moet zijn aan

$$\binom{n}{k} \times \binom{n}{n-k} = \binom{n}{k}^2.$$

We krijgen in totaal als coëfficiënt voor x^n dus $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2$. □

2.5 Inclusie en exclusie

We weten dat $|A \cup B| = |A| + |B|$ als $A \cap B = \emptyset$. Als $A \cap B \neq \emptyset$, dan worden de elementen van $A \cap B$ dubbel geteld in $|A| + |B|$ terwijl ze maar één keer in $A \cup B$ zitten. Dit kunnen we goedmaken door $|A \cap B|$ af te trekken:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Voor drie verzamelingen geldt:

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &\quad -|A \cap B| - |A \cap C| - |B \cap C| \\ &\quad +|A \cap B \cap C|. \end{aligned}$$

Algemeen geldt de volgende

Stelling 11 (**Principe van inclusie en exclusie**). *Zijn $A_1, A_2, \ldots, A_n$ eindige verzamelingen en stel $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$. Dan hebben we*

$$\left|\bigcup \mathcal{A}\right| = |A_1 \cup A_2 \cup \cdots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n$$

met

$$\alpha_i = \sum_{\mathcal{B} \in \binom{\mathcal{A}}{i}} \left|\bigcap \mathcal{B}\right|.$$

Bewijs. Zij $x \in \bigcup \mathcal{A}$, dan $\exists k \in \mathbb{N}_0$ zodat x behoort tot juist k van de n verzamelingen in $\mathcal{A}$. Dus

$$\begin{array}{rccl}
\text{levert } x \text{ een bijdrage} & k & \text{in} & \alpha_1 = |A_1| + |A_2| + \cdots + |A_n| \\
& \binom{k}{2} & \text{in} & \alpha_2 \\
& \binom{k}{3} & \text{in} & \alpha_3 \\
& \vdots & \vdots & \vdots \\
& \binom{k}{k} & \text{in} & \alpha_k \\
& 0 & \text{in} & \alpha_{k+1} \\
& \vdots & \vdots & \vdots \\
& 0 & \text{in} & \alpha_n.
\end{array}$$

In totaal hebben we een bijdrage

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k-1}\binom{k}{k} = 1$$

(zie Stelling 4 op pagina 28). □

Voorbeeld. In de klas zijn er 73 studenten. 52 spelen piano, 25 viool en 20 fluit. 17 spelen piano en viool, 12 spelen piano en fluit, 7 viool en fluit en 1 enkele speelt alle drie de instrumenten. Hoeveel studenten spelen geen van de 3 instrumenten?

De oplossing:

$$\begin{aligned}
73 - |A_P \cup A_V \cup A_F| &= 73 - (52 + 25 + 20 - 17 - 12 - 7 + 1) \\
&= 73 - 62 \\
&= 11.
\end{aligned}$$

2.6 Oefeningen

1. ○ Toon aan: in elke groep van 13 personen zijn er zeker 2 die in dezelfde maand verjaren.

2. ◐ Toon aan dat in een groep mensen altijd zeker 2 mensen hetzelfde aantal vrienden in die groep hebben [We nemen aan dat als x een vriend is van x', ook x' een vriend is van x].

3. ○ Een geblinddoekte man heeft een hoop sokken: 10 bruine en 10 grijze. Hoeveel moet hij er nemen om zeker een passend paar te hebben? Hoeveel moet hij er nemen om zeker een grijs paar te hebben?

4. ◐ Stel dat we vijf punten kiezen in een gelijkzijdige driehoek met zijde 1. Toon aan dat er minstens één paar punten is waarvan de onderlinge afstand ten hoogste 1/2 is.

5. ◐ Toon aan: in elke verzameling van 12 gehele getallen zitten er altijd 2 waarvan het verschil deelbaar is door 11.

6. ◐ Toon aan: als $S \subset \mathbb{N}$ en $|S| = 37$ dan bevat S twee elementen die bij deling door 36 dezelfde rest opleveren.

7. ◐ Toon aan dat, als je 101 getallen selecteert uit $\{1, 2, 3, \ldots, 200\}$, er zeker 2 bij zijn zodat het ene deler is van het andere.

8. ● Zij X een deelverzameling van $\{1, 2, 3, \ldots, 2n\}$, en zij $Y = \{1, 3, 5, \ldots, 2n-1\}$. Definieer $f : X \to Y : f(x) =$ de grootste oneven deler van x. Toon aan: als $|X| \geq n + 1$, dan is f geen injectie. Leid daaruit af dat in dat geval X twee getallen x_1 en x_2 bevat zodat $x_1 | x_2$.

9. ● Toon aan dat het mogelijk is een deelverzameling X van $\{1, 2, 3, \ldots, 2n\}$ te vinden met $|X| = n$ zodat geen enkel element van X een ander element van X deelt.

10. ○ Als je 500000 'woorden' hebt van 4 of minder letters, kan het dan dat ze allemaal verschillend zijn?

11. ○ Toon aan: elke deelverzameling van 6 elementen uit $\{1, 2, \ldots, 9\}$ moet 2 elementen bevatten met als som 10.

12. ○ Zij $S = \{3, 7, 11, \ldots, 95, 99, 103\}$. Hoeveel elementen van S moeten we selecteren zodanig dat er zeker 2 zijn met som 110?

13. ● Zet de elementen van $\{1, 2, \ldots, 10\}$ op een cirkel. Toon aan dat er altijd 3 naast elkaar staan waarvan de som 18 of meer is.

14. ○ Bepaal in elk van de volgende gevallen het gepaste getal n, en schrijf de formule op van een bijectie $f : [n] \to X$.

    (a) $X = \{2, 4, 6, 8, 10\}$

    (b) $X = \{-3, -8, -13, -18, -23, -28\}$

    (c) $X = \{10, 17, 26, 37, 50, 65, 82, 101\}$

    (d) $X = \{k \in \mathbb{N} \mid \text{de } k\text{-de dag van deze maand is een maandag}\}$

15. ◐ Toon aan: als $|X| = n$ en er bestaat een bijectie van X naar Y, dan is $|Y| = n$.

16. ○ In een gemengde groep zitten 32 jongens. Elk van de jongens kent 5 meisjes van de klas, en elk meisje kent 8 jongens van de klas. Hoeveel meisjes zitten er in de klas?

17. ◐ Is het mogelijk om een aantal deelverzamelingen van [8] te vinden met de volgende eigenschappen?

    - elke deelverzameling bevat 3 elementen
    - elk element van [8] behoort tot juist 5 van de deelverzamelingen.

18. ○ Hoeveel vlaggen van drie gelijke verticale banden kan je maken als je de kleuren rood, wit, blauw en groen mag gebruiken? [Een van de repen wordt beschouwd als de 'binnenste', of 'die aan de kant van de mast'.]

19. ○ Toon aan dat er meer dan 10^{76} deelverzamelingen zijn van de verzameling van deelverzamelingen van de verzameling [8].

20. ○ Hoeveel woorden van 4 letters uit een alfabet van 10 letters kan je maken als elke letter hoogstens 1 keer mag gebruikt worden?

21. ◐ Stel

$$(n)_m = \frac{n!}{(n-m)!}$$

    Toon aan dat $(n)_m \times (n-m)_{r-m} = (n)_r$, $n > r > m$, door het resultaat te interpreteren in termen van geordende selecties.

22. ○ Een comité kiest een voorzitter, een secretaris en een penningmeester. Als het comité 9 leden telt, op hoeveel manieren kan dat dan? (Bespreek grondig van welke veronderstellingen je vertrekt.)

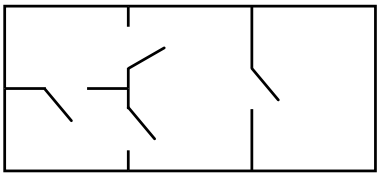
23. ◐ Een dominoblokje kan voorgesteld worden als $[x \mid y]$, met $x, y \in [0..6]$. Toon aan dat er 28 blokjes zijn (en geen 49).

24. ◐ Op hoeveel manieren kunnen we een wit en een zwart vakje kiezen op een schaakbord op zo'n manier dat de 2 vakjes niet in dezelfde rij of kolom staan? [768]

25. ○ Er zitten m meisjes en n jongens in een klas. Op hoeveel manieren kan je ze in een rij zetten als alle meisjes samen moeten staan?

26. ● Bereken het aantal permutaties σ van $[n]$ waarvoor $\sigma \circ \sigma = 1$.

27. ◐ De kamers van een flat (zie tekening) worden geverfd, zo dat 2 kamers die met elkaar verbonden zijn een andere kleur krijgen. Hoeveel mogelijkheden heb je met n kleuren?



Figuur 2.2: Plan van de flat van vraag 27

28. ● Veronderstel dat we 'veralgemeende dominoblokjes' hebben, van de vorm $[x \mid y]$ met $x, y \in [0..n]$. Zij $0 \leq k \leq n$. Toon aan dat het aantal blokjes waarvoor $x + y = n - k$ gelijk is aan het aantal waarvoor $x + y = n + k$. [In beide gevallen bekom je $\lceil (n - k + 1)/2 \rceil$.]

29. ◐ Stel met u_n het aantal woorden van n letters in het alfabet $\{0, 1\}$ voor met de eigenschap dat het woord geen 2 opeenvolgende nullen bevat. Toon aan:

$$u_1 = 2, \quad u_2 = 3 \quad \text{en} \quad u_n = u_{n-1} + u_{n-2} \text{ voor } n \geq 3.$$

[In hoofdstuk 6 zal je meer zulke problemen oplossen.]

30. ◐ In 1303 bewees de Chinees Chu Shih-Chieh, voor elke $r, n \in \mathbb{N}$ met $n \geqslant r$, volgende identiteit.

$$\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1}$$

Kan jij dat ook?

31. ◐ Toon aan:

(a) $\binom{s-1}{0} + \binom{s}{1} + \binom{s+1}{2} + \cdots + \binom{s+n-2}{n-1} + \binom{s+n-1}{n} = \binom{s+n}{n}$

(b) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$

32. ● Zij $n \in \mathbb{N}_0$. Bewijs dat

$$\sum_{r=1}^{n} r\binom{n}{r} = n \cdot 2^{n-1}.$$

[Hint: $r\binom{n}{r} = n\binom{n-1}{r-1}$ en oefening 31b.]

33. ● Gebruik de technieken van oefening 32 om volgende identiteiten te bewijzen.

(a) $\displaystyle\sum_{r=1}^{n} r^2\binom{n}{r} = n(n+1)2^{n-2}$

(b) $\displaystyle\sum_{r=1}^{n} r^3\binom{n}{r} = n^2(n+3)2^{n-3}$

Kan je een formule bedenken (en bewijzen) voor $\sum_{r=1}^{n} r^k\binom{n}{r}$ met $k \in \mathbb{N}$ en $k > 3$?

34. ● Zij X een verzameling met n elementen. Leg uit waarom

$$|\mathcal{P}(X)| = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}$$

en geef zo een (ander) bewijs van oefening 31b.

35. ◐ Toon aan: als 3 identieke dobbelstenen geworpen worden zijn er 56 mogelijke uitkomsten. Hoeveel zijn er bij n identieke dobbelstenen?

36. ● *[Multinomiaalcoëfficiënten]* Neem $n, m \in \mathbb{N}$, $m > 0$ en $n_1, n_2, \ldots, n_m$ natuurlijke getallen met $n_1+n_2+\cdots+n_m = n$. Toon aan dat het aantal manieren om n verschillende objecten te verdelen over m genummerde dozen, zo dat doos nummer i juist n_i objecten bevat, gelijk is aan

$$\frac{n!}{n_1!n_2!\cdots n_m!}.$$

Bewijs dat dit ook juist de coëfficiënt is van $x_1^{n_1}x_2^{n_2}\cdots x_m^{n_m}$ in de ontwikkeling van $(x_1 + x_2 + \cdots + x_m)^n$. Vergelijk dit met het binomium van Newton dat de ontwikkeling van $(x_1 + x_2)^n$ geeft. Deze gelijkenis leidt ons tot een naam voor de coëfficiënten in de ontwikkeling van $(x_1 + x_2 + \cdots + x_m)^n$. We noemen ze **multinomiaalcoëfficiënten** en noteren ze, ook analoog met binomiaalcoëfficiënten, met

$$\binom{n}{n_1, n_2, \ldots, n_m} := \frac{n!}{n_1!n_2!\cdots n_m!}.$$

In deze nieuwe notatie hebben we dat

$$\binom{n}{k} = \binom{n}{k, n-k}$$

voor de binomiaalcoëfficiënten.

37. ◐

(a) Stel dat we $(x + y + z)^n$ uitwerken. Hoeveel termen bevat de expansie?

(b) Bereken de coëfficiënt van $x^5y^3z^2$ in de expansie van $(x+y+z)^{10}$.

38. ● Toon aan dat het aantal n-tallen $(x_1, \ldots, x_n)$ elementen van $\mathbb{N}$ dat voldoet aan

$$x_1 + \cdots + x_n = r$$

gelijk is aan $\binom{n+r-1}{r}$.

39. ◐ Bereken de coëfficiënt van

(a) x^5 in $(1 + x)^{11}$

(b) a^2b^8 in $(a + b)^{10}$

(c) a^6b^6 in $(a^2 + b^3)^5$

(d) x^3 in $(3 + 4x)^6$

40. ◐ Gebruik het binomium van Newton om eigenschap 4 op blz. 28 te bewijzen.

41. ● Gegeven zijn twee positieve reële getallen p en q met $p+q=1$ en twee natuurlijke getallen k en n met $k \leqslant n$. Bewijs dat

$$\sum_{j=k}^{n} \binom{n}{j} p^j q^{n-j} \leqslant \binom{n}{k} p^k.$$

42. ◐ Toon aan dat $\forall n \in \mathbb{N}_0$:

$$\sum_{\substack{k \text{ even} \\ 0 \leqslant k \leqslant n}} \binom{n}{k} = \sum_{\substack{k \text{ oneven} \\ 0 \leqslant k \leqslant n}} \binom{n}{k} = 2^{n-1}.$$

[Hint: eigenschap 4 en oefening 31b.]

43. ◐ Toon aan[2] dat

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots + \binom{m}{r}\binom{n}{0}.$$

[Hint: $(1+x)^m(1+x)^n = (1+x)^{m+n}$.]

44. ◐ In een klas van 67 wiskundestudenten zijn er 47 die Frans kennen, 35 die Duits kennen en 23 die zowel Frans als Duits kennen. Hoeveel kennen er geen van beide? Als bovendien 20 studenten Russisch kennen, van wie 12 ook Frans en 11 ook Duits kennen en 5 studenten kennen de drie talen, hoeveel zijn er dan die geen van de drie kennen?

45. ◐ Hoeveel woorden kan je maken met de letters A, E, M, O, U, Y (elk 1 keer gebruiken) als de opeenvolgingen ME en YOU niet mogen voorkomen?

46. ● Noem d_n het aantal 'derangements' van $[n]$ (een **derangement** is een permutatie waarbij geen enkel element op zichzelf wordt afgebeeld). Bepaal d_4. [9]

47. ● Bepaal d_n (zie oef 46). Bewijs dat $d_n = \left[\frac{n!}{e}\right]$, waarbij $[x]$ staat voor het geheel getal dat het dichtst bij x ligt.

48. ◐ 4 mensen in een gebouw met tien etages stappen op de gelijkvloerse verdieping in de lift. Op hoeveel manieren is het mogelijk dat

[2] Deze identiteit werd voor het eerst bewezen door de Franse wiskundige A.T. Vandermonde (1735–1796) in 1772.

(a) iedereen op dezelfde etage uitstapt?

(b) er Ã©Ã©n persoon op een bepaalde etage uitstapt en de drie andere samen op een andere?

(c) er twee personen elk op een andere etage uitstappen en de twee resterende samen op nog een andere?

(d) er twee personen op Ã©Ã©n etage uitstappen en de twee andere op een andere?

(e) iedereen op een andere etage uitstapt?

49. ◐ Toon aan: als je in een vierkant met zijde 1 meter tien punten zet, dan zijn er minstens twee die dichter dan 0.5 meter bij elkaar liggen. [examen januari 2005]

50. ◐ Op vrijdag 14 januari 2005 gaan proffen en assistenten van het departement wiskunde naar restaurant "Le Mess" voor het traditionele nieuwjaarsetentje. Voor het voorgerecht kunnen ze kiezen tussen een vispasteitje of een salade met avocado en garnalen. Voor het hoofdgerecht zijn er drie mogelijkheden: filet mignon met pepersaus en frietjes, kabeljauwfilet met gestoomde groenten of Gentse waterzooi. Voor het dessert tenslotte kan er gekozen worden tussen ijs met aardbeien of Apfelstrudel.

(a) Vanaf hoeveel inschrijvingen is het onvermijdelijk dat 2 mensen exact hetzelfde menu bestellen (ga ervan uit dat iedereen zowel een voorgerecht, een hoofdgerecht en een dessert neemt)?

(b) De secretaresse maakt een lijstje met daarop alle gerechten en hoeveel mensen dat gerecht nemen. Als er 11 mensen inschrijven, en als iedereen drie gangen neemt, hoeveel verschillende lijstjes kan de secretaresse dan zo bekomen?

(c) Van de 11 personen die aan het dinertje deelnemen zijn er 4 gespecialiseerd in algebra, 4 in topologie en 4 in statistiek. Er zijn 2 mensen die zowel de statistiek als de topologie bemeesteren, en telkens 1 persoon voor de combinaties topologie-algebra en statistiek-algebra. Niemand beschouwt zichzelf als een specialist in de drie richtingen. Hoeveel personen op het dinertje zijn in geen van deze drie vakken gespecialiseerd?

[examen januari 2005]

51. ◐ In hoeveel permutaties van de letters van het alfabet komt geen enkel van volgende patronen voor: KAT, HOND, MUIS? [examen augustus 2005]

52. ◐ In hoeveel permutaties van de letters van het alfabet komt geen enkel van volgende patronen voor: KAT, HOND, MUIS, SPIN? [examen augustus 2005]

53. ◐ Een auditorium heeft 800 plaatsen. Hoeveel van die plaatsen moeten bezet zijn als je zekerheid wilt dat twee studenten in het auditorium dezelfde beginletters van voor- en achternaam hebben? [examen augustus 2005]

54. ◐ Hoeveel telefoonnummers van 10 cijfers bevatten elk oneven cijfer minstens één keer? [examen januari 2006]

55. ◐ Zes koppels organiseren een aantal diners. Zij nemen steeds plaats aan een rechthoekige tafel met 6 plaatsen aan elke kant. De plaatsen zijn genummerd en ze zorgen ervoor dat niemand ooit recht tegenover zijn partner zit. Hoeveel diners kunnen de koppels organiseren als zij willen dat nooit alle 12 personen op dezelfde plaatsen zitten als op één van de voorgaande diners? [examen augustus 2006]

Hoofdstuk 3

Gehele getallen

3.1 Ring

Zij R een verzameling voorzien van twee bewerkingen

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

die voldoen aan volgende eigenschappen:

1. $(R, +)$ is een **abelse** of **commutatieve** groep:
   - De optelling is **associatief**
   $$\forall a, b, c \in R : (a + b) + c = a + (b + c)$$
   - De optelling heeft een **neutraal element**
   $$\exists n \in R : \forall a \in R : a + n = a = n + a$$
   - Elk element a heeft een **invers** of **symmetrisch element** t.o.v. de optelling (dat we noteren als $-a$)
   $$\forall a \in R : \exists b \in R : a + b = n = b + a$$
   - De optelling is **commutatief**
   $$\forall a, b \in R : a + b = b + a$$

2. $(R, .)$ is een **monoide**:

- De vermenigvuldiging is associatief

$$\forall a, b, c \in R : (a.b).c = a.(b.c)$$

- De vermenigvuldiging heeft een neutraal element

$$\exists e \in R : \forall a \in R : a.e = a = e.a$$

3. De vermenigvuldiging is **distributief** t.o.v. de optelling

$$\begin{aligned} \forall a, b, c \in R : \quad & a.(b + c) = a.b + a.c \\ & (a + b).c = a.c + b.c \end{aligned}$$

We zeggen dat $(R, +, .)$ een **ring met eenheid** is. Wanneer ook de vermenigvuldiging commutatief is, spreken we van een **commutatieve ring met eenheid**.

Notatie. We schrijven $a - b$ voor $a + (-b)$. $a - b$ is dus kort voor "a plus het symmetrisch element van b".

Eigenschap 5. *De symmetrische en neutrale elementen zijn uniek.*

Bewijs. Oefening. □

Eigenschap 6. $\forall m, n \in R : m - (-n) = m + n.$

Bewijs. Als we bewijzen dat $-(-n) = n$ is het in orde, want $m-(-n) = m+(-(-n))$. Maar vermits symmetrische elementen uniek zijn is dit duidelijk want $n + (-n) = 0$. □

3.1.1 De ring van gehele getallen

De verzameling van alle gehele getallen uitgerust met $+$ en $\cdot$ is een ring met 0 als neutraal element voor de optelling en 1 als neutraal element voor de vermenigvuldiging die we noteren als $(\mathbb{Z}, +, \cdot)$.

3.1.2 Andere voorbeelden van ringen

Veeltermen

De verzameling van veeltermen met reële coëfficiënten en onbekende X is

$$\mathbb{R}[X] := \left\{ \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}, \forall i \in [0..n] : a_i \in \mathbb{R} \right\}.$$

Op deze verzameling definiëren we een optelling door

$$\left(\sum_{i=0}^{n} a_i X^i\right) + \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) X^k$$

waarbij we veronderstellen dat $a_k = 0$ voor $k > n$ en $b_k = 0$ voor $k > m$. We definiÃ«ren ook een vermenigvuldiging door

$$\left(\sum_{i=0}^{n} a_i X^i\right) . \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{m+n} c_k X^k$$

waarbij

$$c_k = \sum_{\substack{i\in[0..n]\\ j\in[0..m]\\ i+j=k}} a_i b_j .$$

De formule voor c_k drukt gewoon uit dat je de som neemt van alle producten van termen uit de eerste en de tweede veelterm die X^k opleveren.

Met deze definities is $(\mathbb{R}[X], +, .)$ een ring. Analoog zijn ook $(\mathbb{Z}[X], +, .)$ en $(\mathbb{Q}[X], +, .)$ ringen. Verifieer dit zelf als oefening.

Matrices

Een voorbeeld van een niet-commutatieve ring is de verzameling van alle reÃ«le $(n \times n)$-matrices, voor een gegeven $n \in \mathbb{N}_0$, met de optelling en de vermenigvuldiging die we gewoon zijn. Verifieer eveneens zelf.

3.2 Welorde

De elementen van $\mathbb{Z}$ zijn ook **geordend** door de relatie $\leq$. Deze heeft ook enkele goed gekende eigenschappen:

- $\leq$ is **reflexief**

$$\forall a \in \mathbb{Z} : a \leq a$$

- $\leq$ is **antisymmetrisch**

$$\forall a, b \in \mathbb{Z} : (a \leq b) \wedge (b \leq a) \Rightarrow (a = b)$$

- $\leq$ is **transitief**

$$\forall a, b, c \in \mathbb{Z} : (a \leq b) \wedge (b \leq c) \Rightarrow (a \leq c)$$

- Bovendien geldt:

$$\forall a, b, c \in \mathbb{Z} : a \leq b \Rightarrow a + c \leq b + c$$

en

$$\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{N} : a \leq b \Rightarrow a.c \leq b.c$$

Eigenschap 7. *Als $a \leq b$, dan $-b \leq -a$.*

Bewijs. Trek van beide leden a af. Je krijgt: $0 \leq b - a$. Trek vervolgens van beide leden b af: $-b \leq -a$. □

Definitie 5. *Zij V een verzameling met $S \subset V$. $x \in V$ heet een **ondergrens** van S indien $\forall s \in S : x \leq s$. Het **infimum** van S is de grootste ondergrens van S.*

Voorbeeld. $S = \{-5, 3, 10, 20\}$ heeft vele ondergrenzen, bijvoorbeeld $-6, -200, -5, \ldots$. Het infimum is -5. Merk op dat in dit voorbeeld het infimum van S zelf tot S behoort.

Definitie 6. *Indien het infimum van een verzameling S zelf tot S behoort, dan noemen we het een **minimum**.*

De volgende bijzondere eigenschap van $\mathbb{Z}$ is in feite een axioma.

Principe van de Welgeordendheid.
Elke niet-lege deelverzameling van $\mathbb{Z}$ die een ondergrens heeft, heeft ook een minimum.

3.3 Bewijs per inductie

Voorbeeld. Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

We merken eerst op dat voor $n = 1$, het kleinste element van $\mathbb{N}_0$, de eigenschap waar is:

$$1 = 1^2.$$

Dan gaan we ervan uit dat de eigenschap geldt voor $n = k$ en we bewijzen hieruit dat de eigenschap dan ook moet waar zijn voor $n = k + 1$. Dus nemen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ en dan tonen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$. Gebruikmakend van de aanname, wordt het linkerlid $k^2 + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2$.

Kunnen we uit deze algemene redenering afleiden dat de eigenschap geldt voor alle $n \in \mathbb{N}$?

Principe van Bewijs per Inductie.
Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. ***Basis van de inductie.*** *Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).*

2. *Onderstel dat de **inductiehypothese** geldt, i.e. wanneer $P(k)$ waar is voor een willekeurige $k \in \mathbb{N}$, dan is $P(k+1)$ dat ook (deze stap heet de **inductiestap**).*

Dan is $P(n)$ waar voor alle $n \in \mathbb{N}$.

Bewijs. Onderstel van niet. Zij $S = \{n \in \mathbb{N} \mid \neg P(n) \text{ waar}\}$, dan is deze verzameling niet leeg. Vermits $S \subset \mathbb{N}$ heeft S een ondergrens (bijvoorbeeld -1). Door de welgeordendheid van de gehele getallen heeft S een minimum, m. Door de basis van de inductie weten we dat $0 \notin S$ en dus $m \geq 1$. Omdat m een minimum is, hebben we zeker $(m - 1) \notin S$ zodat $P(m - 1)$ waar is, maar de inductiestap verzekert dan dat $P(m)$ ook waar is, wat een tegenspraak oplevert. □

Voor een bewijs per inductie, moet je dus de basis en de inductiehypothese verifiëren.

3.4 Quotiënt en rest

Als we 46 delen door 6, weten we dat de deling 'niet opgaat' en dat er een **rest** is van 4 met **quotiënt** 7. We kunnen dit samenvatten als $46 = 6 \cdot 7 + 4$ of '46 is een veelvoud van 6 plus 4'. In het algemeen geldt:

Stelling 12. *Gegeven $a \in \mathbb{Z}$ en $b \in \mathbb{N}_0$, dan $\exists q, r \in \mathbb{Z}$: $a = bq + r$ met $0 \leq r < b$.*

Bewijs. Stel

$$R := \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}.$$

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$. Als $a < 0$ dan hebben we $a = ba + (1-b)a$ zodat $(1-b)a \in R$, want $(1-b)a \in \mathbb{N}$ omdat $1 - b \leq 0$ en $a < 0$.

Uit het welordeningsprincipe kunnen we besluiten dat R een kleinste element r heeft. Dan geldt: $\exists y \in \mathbb{Z} : a = by + r$ zodat we $q := y$ kunnen nemen.

Er blijft te tonen dat $0 \leq r < b$. Door de definitie van R is $0 \leq r$ in orde. Indien $r \geq b$, dan is $r - b \geq 0$ en uit $a = by + r \iff a = b(y+1) + (r-b)$ volgt dan $r - b \in R$ en dat is strijdig, want r was het kleinste element van R. □

Stelling 13. *r en q in de vorige stelling zijn uniek.*

Bewijs. Bewijs uit het ongerijmde. Onderstel dat

$$\exists q \neq q' \in \mathbb{Z}, \exists r \neq r' \in [0..b-1] : bq + r = a = bq' + r'.$$

Veronderstel dat $q' < q$, zodat $q - q' \geq 1$. Dan krijgen we:

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b \geq b.$$

Strijdig. Bijgevolg is $q' < q$ niet waar. Analoog toon je dat $q' > q$ ook niet kan. Uiteindelijk moet dus $q' = q$ en dan ook $r = r'$. □

Een belangrijke toepassing van de vorige stellingen is onze (decimale) schrijfwijze voor getallen. Gegeven een natuurlijk getal x en een 'basis' $t \geq 2$, dan kunnen we herhaaldelijk de stelling toepassen:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ &\vdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n \end{aligned}$$

met elke $r_i \in [0..t-1]$ en $q_n = 0$.

Substitutie van de laatste vergelijking in de voorlaatste enz. geeft

$$x = r_n t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0$$

zodat de schrijfwijze voor x in basis t gelijk is aan

$$r_n r_{n-1} \ldots r_1 r_0.$$

Notatie. We noteren de schrijfwijze van een getal x in basis t als $(x)_t$.

Voorbeeld. Een computer rekent in basis 2. Hoe berekenen we $(386)_2$?

$$\begin{array}{rcrcc} 386 & = & 193 \cdot 2 & + & 0 \\ 193 & = & 96 \cdot 2 & + & 1 \\ 96 & = & 48 \cdot 2 & + & 0 \\ 48 & = & 24 \cdot 2 & + & 0 \\ 24 & = & 12 \cdot 2 & + & 0 \\ 12 & = & 6 \cdot 2 & + & 0 \\ 6 & = & 3 \cdot 2 & + & 0 \\ 3 & = & 1 \cdot 2 & + & 1 \\ 1 & = & 0 \cdot 2 & + & 1 \end{array}$$

Dus $(386)_2 = 110000010$.

Definitie 7. *We zeggen dat een geheel getal b een **veelvoud** is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z} : b = ka$. We zeggen in dat geval ook dat a het getal b **deelt** en schrijven $a \mid b$. Ook zeggen we dat a een **factor** of een **deler** is van b of dat b **deelbaar** is door a. Als $a \neq 0$, noteren we het getal $k \in \mathbb{Z}$ waarvoor $b = ka$ met $\frac{b}{a}$. Natuurlijk bestaat $\frac{b}{a}$ voor elke keuze $b \in \mathbb{Z}, a \in \mathbb{Z}_0$ maar in het algemeen behoort $\frac{b}{a}$ tot $\mathbb{Q}$ en niet tot $\mathbb{Z}$. Enkel als $a \mid b$ hebben we $\frac{b}{a} \in \mathbb{Z}$.*

Eigenschap 8. *Zij $n, d, c \in \mathbb{Z}$ met $c \neq 0 \neq d$. Er geldt*

$$d \mid n \wedge c \mid \frac{n}{d} \Rightarrow c \mid n \wedge d \mid \frac{n}{c}$$

Bewijs. $d \mid n \iff \exists k \in \mathbb{Z} : n = kd$ en $c \mid \frac{n}{d} \iff c \mid k \iff \exists l \in \mathbb{Z} : k = lc$. Bijgevolg is $n = lcd$ en dus volgt $c \mid n$ en aangezien $\frac{n}{c} = ld$ volgt ook $d \mid \frac{n}{c}$. □

3.5 Grootste gemene deler

Definitie 8. *Stel $a, b \in \mathbb{Z}$. Een geheel getal d heet een **grootste gemene deler (ggd)** van a en b indien $d \mid a$ en $d \mid b$ (gemene deler) èn $\forall c \in \mathbb{Z} : c \mid a \wedge c \mid b \Rightarrow c \mid d$ (grootste).*

Voorbeeld. $6 \mid 60$ en $6 \mid 84$ maar toch is 6 geen ggd van 60 en 84, want $12 \mid 60$ en $12 \mid 84$ maar $12 \nmid 6$.

Opmerking. Als d een ggd is, is ook $-d$ een ggd. We hebben:

Eigenschap 9. *Zijn $d \neq d'$ grootste gemene delers van a en b. Dan geldt $d = -d'$.*

Bewijs. Dit volgt uit $d \mid d'$ en $d' \mid d$. □

Definitie 9. De *grootste gemene deler van a en b is de unieke positieve grootste gemene deler van a en b. We noteren hem* $\text{ggd}(a, b)$.

Hoe berekenen we nu $\text{ggd}(a, b)$? Hiervoor hebben we nog volgende eigenschap nodig:

Eigenschap 10. *Stel $a = bq + r$. Dan is* $\text{ggd}(a, b) = \text{ggd}(b, r)$.

Bewijs. Stel $d \mid a$ en $d \mid b$. Dan zal ook $d \mid (a - bq)$ zodat $d \mid b$ en $d \mid r$. Omgekeerd: als $d \mid b$ en $d \mid r$ dan volgt $d \mid (bq + r)$ zodat $d \mid \text{ggd}(a, b)$. □

Voorbeeld. We bepalen $\text{ggd}(2406, 654)$. We passen hiervoor de voorgaande eigenschap herhaaldelijk toe:

$$\begin{array}{rcllcl}
2406 &=& 654.3 + 444 &\Rightarrow& \text{ggd}(2406, 654) &=& \text{ggd}(654, 444) \\
654 &=& 444.1 + 210 &\Rightarrow& &=& \text{ggd}(444, 210) \\
444 &=& 210.2 + 24 &\Rightarrow& &=& \text{ggd}(210, 24) \\
210 &=& 24.8 + 18 &\Rightarrow& &=& \text{ggd}(24, 18) \\
24 &=& 18.1 + 6 &\Rightarrow& &=& \text{ggd}(18, 6) \\
18 &=& 6.3 + 0 &\Rightarrow& &=& 6
\end{array}$$

Algemeen: als we hebben

$$\begin{array}{rcrcll}
a &=& bq_1 &+& r_1 & \text{met} \quad 0 \leq r_1 < b \\
b &=& r_1 q_2 &+& r_2 & 0 \leq r_2 < r_1 \\
r_1 &=& r_2 q_3 &+& r_3 & 0 \leq r_3 < r_2 \\
&\vdots& & & \vdots & \\
r_{k-4} &=& r_{k-3} q_{k-2} &+& r_{k-2} & 0 \leq r_{k-2} < r_{k-3} \\
r_{k-3} &=& r_{k-2} q_{k-1} &+& \boxed{r_{k-1}} & 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} &=& r_{k-1} q_k &+& 0 &
\end{array}$$

dan is

$$\begin{array}{rcl}
\text{ggd}(a, b) &=& \text{ggd}(r_{k-2}, r_{k-1}) \\
&=& r_{k-1} \\
&=& \text{de laatste niet-nulle rest.}
\end{array}$$

Dit algoritme heet het **Euclidisch algoritme**.

Stelling 14 (Bézout[1])**.** *Stel $a, b \in \mathbb{Z}, b \geq 0$ met $d = \text{ggd}(a, b)$, dan $\exists m, n \in \mathbb{Z} : d = ma + nb$. Ook is d het kleinste natuurlijk getal waarvoor dit kan.*

Bewijs. Voor $b = 0$ is de stelling triviaal.
Als $b \neq 0$, lezen we het resultaat van het Euclidisch algoritme van achter naar voor:

$$d = r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}.$$

Dus $d = m'r_{k-2} + n'r_{k-3}$, met $m' = -q_{k-1}$ en $n' = 1$. Nu substitueren we $r_{k-2} = r_{k-4} - r_{k-3}q_{k-2}$ zodat

$$\begin{aligned} d &= m'(r_{k-4} - r_{k-3}q_{k-2}) + n'r_{k-3} \\ &= (-m'q_{k-2} + n')r_{k-3} + m'r_{k-4} \\ &= m''r_{k-3} + n''r_{k-4}. \end{aligned}$$

Daarin substitueren we $r_{k-3} = r_{k-5} - r_{k-4}q_{k-3}$ enz. Uiteindelijk vinden we

$$d = m^{(k-3)}r_2 + n^{(k-3)}r_1$$

waaruit, via de substituties $r_2 = b - r_1q_2$ en $r_1 = a - bq_1$:

$$\begin{aligned} d &= m^{(k-3)}(b - r_1q_2) + n^{(k-3)}r_1 \\ &= (-m^{(k-3)}q_2 + n^{(k-3)})r_1 + m^{(k-3)}b \\ &= m^{(k-2)}r_1 + n^{(k-2)}b \\ &= m^{(k-2)}(a - bq_1) + n^{(k-2)}b \\ &= (-m^{(k-2)}q_1 + n^{(k-2)})b + m^{(k-2)}a \\ &= mb + na. \end{aligned}$$

Bewijs als oefening dat er geen kleiner getal $d' > 0$ bestaat waarvoor $\exists n', m' \in \mathbb{Z}$: $d' = m'a + n'b$. □

Voorbeeld. We passen de stelling van Bézout toe op het vorige voorbeeld:

$$\begin{array}{rcll} 6 &=& 24 - 18 & \\ &=& 24 - (210 - 8.24) & = 9.24 - 210 \\ &=& 9(444 - 2.210) - 210 & = 9.444 - 19.210 \\ &=& 9.444 - 19(654 - 444) & = 28.444 - 19.654 \\ &=& 28(2406 - 3.654) - 19.654 & = 28.2406 - 103.654 \end{array}$$

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $\text{ggd}(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

[1] Etienne Bézout (1730–1783), Frans wiskundige.

Definitie 10. $a, b \in \mathbb{Z}$ *heten* ***relatief priem*** *indien* $\text{ggd}(a, b) = 1$.

Eigenschap 11. $ggd(a, b) = 1 \Rightarrow \exists m, n \in \mathbb{Z} : ma + nb = 1$.

Gevolg 3. *Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma + nb$.*

Bewijs. Vermits alle getallen veelvouden zijn van $1 = \text{ggd}(a, b)$, volgt dit uit voorgaande eigenschap. □

Eigenschap 12. *Een positief rationaal getal heeft een* unieke *schrijfwijze als $\frac{a}{b}$ met a en b relatief priem en positief.*

Bewijs. Stel $\dfrac{a}{b} = \dfrac{a'}{b'}$ met $\text{ggd}(a, b) = 1 = \text{ggd}(a', b')$. Dan is $ab' = a'b$. Maar

$$\begin{aligned} b' &= 1.b' \\ &= (ma + nb)b' \\ &= mab' + nbb' \\ &= ma'b + nb'b \\ &= (ma' + nb')b. \end{aligned}$$

Dus $b \mid b'$. Analoog bewijs je dat $b' \mid b$ zodat uiteindelijk $b = b'$ en bijgevolg $a = a'$. □

3.6 Priemgetallen

De definitie kennen we allemaal: een **priemgetal** is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is *niet* priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Opmerking. 1 is geen priemgetal.

Priemgetallen hebben zeer veel toepassingen. Een van de meest gebruikte is het 'ontbinden in priemfactoren' om een getal beter te leren kennen, b.v. $825 = 3 \times 5^2 \times 11$. Als gevolg van de welordeningseigenschap van $\mathbb{Z}$, hebben we volgend gekend resultaat.

Stelling 15. *Elk natuurlijk getal groter dan* 1 *een ontbinding heeft in priemfactoren.*

Bewijs. Veronderstel even dat er minstens één getal is zonder factorisatie in priemgetallen. Dan is de verzameling A van alle getallen zonder factorisatie een niet-leeg deel van $\mathbb{N}$. Bijgevolg heeft A een minimum m. Indien m een priemgetal is, heeft m een triviale priemontbinding. Dus moet $m = m_1 m_2$ met $m_1, m_2 \in [2..m-1]$. Maar vermits m het kleinste element is van A, zullen m_1 en m_2 niet tot A behoren. Bijgevolg zijn deze getallen ontbindbaar. Maar als we deze twee ontbindingen naast elkaar schrijven, hebben we een ontbinding van m. Dit is in tegenspraak met $m \in A$. □

Opmerking. Hoewel we eenvoudig kunnen aantonen dat elk getal ontbindbaar is in priemfactoren, is het vinden van zulke ontbinding helemaal niet voor de hand liggend. Er bestaan momenteel geen efficiÃ≪nte algoritmen voor het vinden van priemfactorisaties.

We zullen nu aantonen dat de ontbinding van een gegeven getal uniek is (op de volgorde van de priemfactoren na). Eerst een hulpstelling:

Stelling 16. *Zij p een priemgetal. Indien p een product $x_1 x_2 \cdots x_n$ deelt, moet p ÃⓒÃⓒn van de factoren delen.*

Bewijs. Door inductie op het aantal factoren van $x_1 x_2 \cdots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

- $\boxed{n = 1}$ OK, triviaal
- $\boxed{n = k} \Rightarrow \boxed{n = k+1}$

  Onderstel dat $p \mid x_1 x_2 \cdots x_k x_{k+1}$ en stel $x := x_1 x_2 \cdots x_k$. Dan hebben we $p \mid x.x_{k+1}$.

  Indien $p \mid x$, hebben we door de inductiehypothese dat $\exists i \in [k] : p \mid x_i$.

  Indien $p \nmid x$ weten we dat $\text{ggd}(p, x) = 1$ omdat p priem is en dus maar twee delers heeft en p niet de ggd kan zijn. De stelling van Bezout levert $m, n \in \mathbb{Z}$ zo dat $1 = mp + nx$. Dan geldt:

$$\begin{aligned} x_{k+1} &= 1.x_{k+1} \\ &= (mp + nx)x_{k+1} \\ &= mpx_{k+1} + nxx_{k+1} \end{aligned}$$

  Vermits $p \mid mpx_{k+1}$ en $p \mid nxx_{k+1}$ (omdat $p \mid xx_{k+1}$), moet $p \mid x_{k+1}$.

□

Opmerking. p moet wel priem zijn. Anders is het niet moeilijk een tegenvoorbeeld te vinden, b.v. $6 \mid 8.3$, en toch is $6 \nmid 8$ en $6 \nmid 3$.

Stelling 17. *Een natuurlijk getal $n \geq 2$ heeft een unieke ontbinding in priemfactoren (op de volgorde van de factoren na).*

Bewijs. Als de stelling niet waar zou zijn, is er, door de welordeningseigenschap, een kleinste getal n met twee verschillende ontbindingen:

$$p_1 p_2 \cdots p_k = n = p'_1 p'_2 \cdots p'_l$$

met p_i en p'_j (niet noodzakelijk verschillende) priemgetallen voor $i \in [k]$ en $j \in [l]$.

Uit $n = p_1 p_2 \cdots p_k$ leiden we af dat $p_1 \mid n$ en dus $p_1 \mid p'_1 p'_2 \cdots p'_l$. De vorige stelling zegt dan dat $\exists j \in [l] : p_1 \mid p'_j$. Maar vermits p_1 en p'_j beide priemgetallen zijn (en 1 geen priemgetal is) wil dit zeggen dat $p'_j = p_1$.

Voor de eenvoud hernummeren we de priemfactoren $p'_1, p'_2, \ldots, p'_l$ zodanig dat de nieuwe $p'_1 = p_1$. Dan hebben we

$$\cancel{p_1} p_2 \cdots p_k = \cancel{p_1} p'_2 \cdots p'_l$$

zodat

$$p_2 \cdots p_k = p'_2 \cdots p'_l$$

hetgeen een tegenspraak is, want dan zou $p_2 \cdots p_k$ een getal kleiner dan n zijn met twee verschillende ontbindingen. □

Notatie. Meestal groeperen we gelijke factoren in de priemontbinding van een getal $n \in \mathbb{N}$. In het algemeen noteren we dus een priemontbinding als

$$n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$$

met $p_1, p_2, \ldots, p_k$ verschillende priemgetallen en $l_1, l_2, \ldots, l_k \in \mathbb{N}_0$.

Toepassing. Zijn m, n niet-nulle natuurlijke getallen, dan geldt $m^2 \neq 2n^2$.

Bewijs. Als $m = 1$ of $n = 1$ is de stelling duidelijk. We nemen dus $m, n \geq 2$.

Bekijken we de ontbinding van m en n: $m = 2^x h$ en $n = 2^y k$ met $x, y \in \mathbb{N}$ en h, k oneven (het zijn de producten van de priemfactoren $\neq 2$).

Dan is $m^2 = 2^{2x} h^2$ en $2n^2 = 2^{2y+1} k^2$. Deze twee getallen kunnen nooit gelijk zijn omdat we anders twee priemontbindingen zouden hebben voor m^2, Ã©Ã©n met een even aantal factoren 2 Ã©Ã©n met een oneven aantal. □

Een gevolg is dat $\forall m, n \in \mathbb{N}_0 : \left(\frac{m}{n}\right)^2 \neq 2$, nog een bewijs dat $\sqrt{2} \notin \mathbb{Q}$.

Soms lezen we in de krant dat het 'grootste priemgetal' is ontdekt. Dit is fout geformuleerd. Eigenlijk bedoelt men 'het grootste getal waarvan men tot nu toe zeker is dat het een priemgetal is'. Immers:

Stelling 18. *Er zijn oneindig veel priemgetallen.*

Bewijs. Veronderstel dat er maar $n \in \mathbb{N}$ priemgetallen $p_1, p_2, \ldots, p_n$ zijn. Beschouw het getal

$$m = p_1 p_2 \cdots p_n + 1.$$

Voor elk priemgetal p_i ($i \in [n]$) is $m - 1$ een veelvoud van p_i, dus $\forall i \in [n] : p_i \nmid m$. Maar m heeft een priemontbinding. Dus moeten er andere priemgetallen bestaan dan $p_1, p_2, \ldots, p_n$. □

Definitie 11. *Voor twee niet-nulle natuurlijke getallen m en n definieren we het* ***kleinste gemeen veelvoud*** *van m en n als het kleinste niet-nul natuurlijk getal dat een veelvoud is van zowel m als n. We noteren dit getal* $\mathrm{kgv}(m, n)$. *We hebben dus dat elk gemeen veelvoud van m en n deelbaar is door* $\mathrm{kgv}(m, n)$.

Lemma 1. *Zij m en n niet-nulle natuurlijke getallen en zij $P = \{p_1, p_2, \ldots, p_k\}$ de verzameling van alle priemgetallen die m of n delen. Dan hebben we*

$$m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \qquad en \qquad n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

voor zekere natuurlijke getallen $m_1, m_2, \ldots, m_k$ en $n_1, n_2, \ldots, n_k$.

Er geldt

$$\mathrm{ggd}(m, n) = \prod_{i=1}^{k} p_i^{\min\{m_i, n_i\}}$$

en

$$\mathrm{kgv}(m, n) = \prod_{i=1}^{k} p_i^{\max\{m_i, n_i\}}$$

Bewijs. Zij c een gemeenschappelijke deler van m en n. Dan moet elk priemgetal dat c deelt zeker behoren tot P. Dus geldt

$$c = \prod_{i=1}^{k} p_i^{c_i},$$

met voor elke $i \in [k]$, $c_i \leq m_i$ en $c_i \leq n_i$. Bovendien levert elke keuze van $c_i \in \mathbb{N}$ binnen deze beperkingen een gemeenschappelijke deler van m en n.

Hieruit volgt nu gemakkelijk dat de grootste gemeenschappelijke deler moet gelijk zijn aan $\prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}}$.

Het is ook duidelijk dat elk gemeenschappelijk veelvoud van m en n deelbaar moet zijn door $p_i^{\max\{m_i,n_i\}}$ voor elke $i \in [k]$. Het kleinste zulk veelvoud is juist $\prod_{i=1}^{k} p_i^{\max\{m_i,n_i\}}$. □

Opmerking. Sommige exponenten m_i of n_i in bovenstaand lemma kunnen nul zijn.

Gevolg 4. *Voor niet-nulle natuurlijke getallen n en m geldt steeds*

$$\text{ggd}(m,n) \cdot \text{kgv}(m,n) = mn.$$

Bewijs. Merk op dat $\min\{m_i,n_i\} = m_i$ impliceert dat $\max\{m_i,n_i\} = n_i$ en omgekeerd. Dus volgt uit vorig lemma dat

$$\text{ggd}(m,n) \cdot \text{kgv}(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}} \cdot \prod_{i=1}^{k} p_i^{\max\{m_i,n_i\}} = \prod_{i=1}^{k} p_i^{m_i+n_i} = m \cdot n.$$

□

Gevolg 5. *Voor niet-nulle natuurlijke getallen n en m zijn $\frac{m}{\text{ggd}(m,n)}$ en $\frac{n}{\text{ggd}(m,n)}$ steeds relatief priem.*

Bewijs. Rekening houdend met $\text{ggd}(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}}$, zien we dat

$$\frac{m}{\text{ggd}(m,n)} = \prod_{i=1}^{k} p_i^{m_i-\min\{m_i,n_i\}} \qquad \text{en dat} \qquad \frac{n}{\text{ggd}(m,n)} = \prod_{i=1}^{k} p_i^{n_i-\min\{m_i,n_i\}}$$

Bovendien is voor elke $i \in [k]$ het minimum van $\{m_i,n_i\}$ gelijk aan m_i of n_i zodat voor elke $i \in [k]$ minstens één van de exponenten $m_i - \min\{m_i,n_i\}$ of $n_i - \min\{m_i,n_i\}$ moet gelijk zijn aan nul. Dit betekent dat de priemfactor p_i niet voorkomt in de ontbinding van respectievelijk $\frac{m}{\text{ggd}(m,n)}$ of $\frac{n}{\text{ggd}(m,n)}$. Hierdoor hebben deze twee getallen geen enkele priemfactor gemeenschappelijk. □

3.7 De φ-functie van Euler

Definitie 12. *Voor een $n \in \mathbb{N}_0$ definiÃ«ren we $\varphi(n)$ als het aantal getallen in $[n]$ die relatief priem zijn met n.*

Laten we een kleine tabel maken voor de eerste 8 positieve natuurlijke getallen.

n	1	2	3	4	5	6	7	8
$\varphi(n)$	1	1	2	2	4	2	6	4

We merken op: voor p priem is $\varphi(p) = p - 1$.

Laten we $\varphi(12)$ berekenen. We krijgen $\varphi(12) = 4$.

Als we de som nemen van $\varphi(d)$ voor alle delers d van 12 krijgen we

$$\begin{array}{cccccccccccccc} & \varphi(1) & + & \varphi(2) & + & \varphi(3) & + & \varphi(4) & + & \varphi(6) & + & \varphi(12) & & \\ = & 1 & + & 1 & + & 2 & + & 2 & + & 2 & + & 4 & = & 12 \end{array}$$

Algemeen hebben we

Stelling 19. $\forall n \in \mathbb{N}_0 : \sum_{d|n} \varphi(d) = n.$

Bewijs. Stel

$$S := \{(d, f) \mid d \mid n, f \in [d], \text{ggd}(d, f) = 1\}.$$

Dan geldt

$$\begin{aligned} |S| &= \sum_{d|n} |\{f \mid (d, f) \in S\}| \\ &= \sum_{d|n} \varphi(d). \end{aligned}$$

We bewijzen nu $|S| = n$ door een bijectie $\beta : S \longrightarrow [n]$ te construeren. Stel

$$\beta(d, f) := f \times \frac{n}{d},$$

wat altijd een getal uit $[n]$ is (zie definitie van S). Nu is β injectief omdat

$$\begin{array}{rcl} \beta(d, f) & = & \beta(d', f') \\ & \Updownarrow & \\ f \times \frac{n}{d} & = & f' \times \frac{n}{d'} \\ & \Updownarrow & \\ \frac{f}{d} & = & \frac{f'}{d'} \end{array}$$

met $\text{ggd}(f, d) = \text{ggd}(f', d') = 1$. Uit Eigenschap 12 volgt dan $f' = f$ en $d' = d$.

β is ook surjectief. Zij immers $x \in [n]$ en stel

$$d_x = \frac{n}{\text{ggd}(n,x)} \in \mathbb{N} \quad \text{en} \quad f_x = \frac{x}{\text{ggd}(n,x)} \in \mathbb{N}.$$

Dan is $f_x \leq d_x$ (omdat $x \leq n$) en $\text{ggd}(d_x, f_x) = 1$ (wegens Gevolg 5). Nu geldt ook

$$\beta(d_x, f_x) = f_x \times \frac{n}{d_x} = \frac{x}{\cancel{\text{ggd}(x,n)}} \times \cancel{n} \times \frac{\cancel{\text{ggd}(x,n)}}{\cancel{n}} = x.$$

□

We kunnen ook een expliciete formule bekomen voor $\varphi(n)$, indien we de priemontbinding van n kennen. Laat ons bijvoorbeeld $\varphi(60)$ berekenen. We weten dat $60 = 2^2 \times 3 \times 5$. We zoeken de getallen $f \in [60]$ met $\text{ggd}(f, 60) = 1$. Dit zijn juist alle getallen in [60] die geen (priem)factor gemeenschappelijk hebben met 60. De getallen die wegvallen zijn dus alle veelvouden van 2, van 3 en van 5 tussen 1 en 60. Maar er zijn natuurlijk getallen die tegelijk een veelvoud zijn van 2 en van 3. We hebben hier een typisch probleem van inclusie en exclusie.

Noteer $A_d := \{x \in [60] \mid d \mid x\}$. Dan is

$$\begin{aligned}
\varphi(60) &= 60 - |A_2 \cup A_3 \cup A_5| \\
&= 60 - (|A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|) \\
&= 60 - (|A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}|) \\
&= 60 - (30 + 20 + 12 - 10 - 6 - 4 + 2) \\
&= 16.
\end{aligned}$$

Algemeen bewijzen we:

Stelling 20. *Zij $n \geq 2$ met als ontbinding in priemfactoren $n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$, dan geldt*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Bewijs. We stellen weer voor $d \mid n$: $A_d := \{x \in [n] \mid d \mid x\} = \{kd \mid k \in [\frac{n}{d}]\}$ zodat $|A_d| = \frac{n}{d}$. Zoals in het voorbeeld hebben we nu

$$\begin{aligned}
\varphi(n) &= n - |A_{p_1} \cup A_{p_2} \cup \cdots \cup A_{p_k}| \\
&= n - (\alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{k-1}\alpha_k)
\end{aligned}$$

met

$$\alpha_i = \sum_{\substack{\{j_1,j_2,\ldots,j_i\} \\ \in \binom{[k]}{i}}} |A_{p_{j_1}} \cap A_{p_{j_2}} \cap \cdots \cap A_{p_{j_i}}|,$$

de som van de cardinaliteiten van alle doorsnedes van i van de k verzamelingen. Dit kunnen we nog schrijven als

$$\begin{aligned} \alpha_i &= \sum_{\substack{\{j_1,j_2,\ldots,j_i\} \\ \in \binom{[k]}{i}}} \left| A_{p_{j_1} p_{j_2} \cdots p_{j_i}} \right| \\ &= \sum_{\substack{\{j_1,j_2,\ldots,j_i\} \\ \in \binom{[k]}{i}}} \frac{n}{p_{j_1} p_{j_2} \cdots p_{j_i}} \\ &= n \sum_{\substack{\{j_1,j_2,\ldots,j_i\} \\ \in \binom{[k]}{i}}} \frac{1}{p_{j_1} p_{j_2} \cdots p_{j_i}}. \end{aligned}$$

Dus

$$\begin{aligned} \varphi(n) &= n - \Big(n(\tfrac{1}{p_1} + \tfrac{1}{p_2} + \cdots + \tfrac{1}{p_k}) \\ &\quad -n(\tfrac{1}{p_1 p_2} + \tfrac{1}{p_1 p_3} + \cdots) \\ &\quad + \cdots \\ &\quad + (-1)^{k-1} n(\tfrac{1}{p_1 p_2 \cdots p_k}) \Big) \\ &= n \left(1 - \tfrac{1}{p_1}\right) \left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_k}\right). \end{aligned}$$

□

3.8 Equivalentierelaties en partities

Definitie 13. *Een relatie $\mathcal{R} \subset X \times X$ is een **equivalentierelatie** als ze*

1. *reflexief is:*

   $\forall x \in X : x \mathcal{R} x$

2. ***symmetrisch** is:*

   $\forall x, y \in X : x \mathcal{R} y \Rightarrow y \mathcal{R} x$

3. transitief is:

$$\forall x, y, z \in X : x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z.$$

Definitie 14. *Gegeven een verzameling V, definiëren we een **partitie** van V als een verzameling $\mathcal{A}$ van deelverzamelingen van V die voldoen aan volgende twee voorwaarden:*

(P1) $\forall A \neq B \in \mathcal{A}$: $A \cap B = \emptyset$

(P2) $\bigcup \mathcal{A} = V$

Stelling 21. *Een equivalentierelatie geeft steeds aanleiding tot een partitie.*

Bewijs. Stel voor $x \in X$:

$$E_x := \{y \in X \mid y\mathcal{R}x\}.$$

E_x heet de **equivalentieklasse** van x en x zelf heet **representant**. Dan is $\mathcal{E} = \{E_x \mid x \in X\}$ een partitie. Inderdaad,

- (P2) is voldaan omdat $\forall x \in X : E_x \subset X$, zodat $\mathcal{E} \subset X$ maar bovendien geeft de reflexiviteit van $\mathcal{R}$ dat $\forall x \in X : x \in E_x$, zodat $X \subset \mathcal{E}$.
- (P1) is ook voldaan. We bewijzen dat $E_x \cap E_y \neq \emptyset \Rightarrow E_x = E_y$. Zij namelijk $z \in E_x \cap E_y$. Dan $x\mathcal{R}z$ en $y\mathcal{R}z$ en bijgevolg $x\mathcal{R}y$ zodat $x \in E_y$. De transitiviteit toont aan dat $E_x \subset E_y$. Ook $y \in E_x$ zodat $E_y \subset E_x$.

□

Stelling 22. *Ook omgekeerd geeft elke partitie van een verzameling X aanleiding tot een equivalentierelatie.*

Bewijs. Zij $\mathcal{A}$ een partitie van X. Definieer, voor $x, y \in X$:

$$x\mathcal{R}y \iff \exists A \in \mathcal{A} : x, y \in A.$$

Ga zelf als oefening na dat dit een equivalentierelatie is. □

3.9 Congruenties

Definitie 15. *Zij $x_1, x_2 \in \mathbb{Z}, m \in \mathbb{N}_0$. x_1 en x_2 heten **congruent modulo** m indien $m \mid x_2 - x_1$. Het natuurlijk getal m heet de **modulus**. We schrijven $x_1 \equiv_m x_2$ of $x_1 \equiv x_2 \pmod{m}$.*

Eigenschap 13. *$\equiv_m$ is een equivalentierelatie.*

Bewijs. $\equiv_m$ is

- reflexief: $x \equiv_m x$ want $x - x = 0$ is een veelvoud van m;
- symmetrisch: $x \equiv_m y \Rightarrow y - x = km \Rightarrow x - y = (-k)m \Rightarrow y \equiv_m x$;
- transitief: $x \equiv_m y$ en $y \equiv_m z \Rightarrow y - x = km$ en $z - y = lm \Rightarrow z - x = (z - y) + (y - x) = (k + l)m$.

□

Stelling 23. *$\equiv_m$ is 'compatibel' met '$+$' en '$.$' in $\mathbb{Z}$, i.e.: $\forall x_1, x_2, y_1, y_2 \in \mathbb{Z}$ met $x_1 \equiv_m x_2$ en $y_1 \equiv_m y_2$:*

$$x_1 + y_1 \equiv_m x_2 + y_2$$

en

$$x_1 y_1 \equiv_m x_2 y_2.$$

Bewijs. Stel $x_2 - x_1 = km$ en $y_2 - y_1 = lm$. Dan geldt

$$(x_2 + y_2) - (x_1 + y_1) = (x_2 - x_1) + (y_2 - y_1) = km + lm = (k + l)m$$

en

$$\begin{aligned} x_2 y_2 - x_1 y_1 &= x_2 y_2 - x_1 y_2 + x_1 y_2 - x_1 y_1 \\ &= (x_2 - x_1) y_2 + (y_2 - y_1) x_1 \\ &= k m y_2 + l m x_1 \\ &= (k y_2 + l x_1) m \end{aligned}$$

□

Toepassing.(**De 9-proef**) Als een getal in basis 10 geschreven wordt als $x_n x_{n-1} \cdots x_0$ dan hebben we

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}.$$

Bewijs.

$$\begin{aligned} x - (x_0 + x_1 + \cdots + x_n) &= x_0 + x_1 \times 10 + \cdots + x_n \times 10^n \\ &\quad -x_0 - x_1 - \cdots - x_n \\ &= 9x_1 + 99x_2 + 999x_3 + \cdots + (10^n - 1)x_n. \end{aligned}$$

Maar er geldt duidelijk dat $9 \mid 10^i - 1 = \underbrace{99\cdots99}_{i \text{ keer}}$. Als we dan $\rho(x)$ schrijven voor $x_0 + x_1 + \cdots + x_n$, dan hebben we aangetoond:

$$\forall x \in \mathbb{Z} : x \equiv \rho(x) \pmod 9.$$

□

Dit wordt in de lagere school gebruikt om berekeningen na te kijken. Inderdaad, we weten dat $x \equiv \rho(x) \pmod 9$ en $y \equiv \rho(y) \pmod 9$. Als $xy = z$ moet dus

$$\rho(z) \equiv z \equiv xy \equiv \rho(x)\rho(y) \pmod 9.$$

Opgelet: het omgekeerde geldt niet noodzakelijk. Als de 9-proef klopt ben je dus nog niet zeker van je resultaat.

Voorbeeld. $54321 \times 98765 = 5363013565$ kan onmogelijk juist zijn, want $\rho(54321) = 15$, $\rho(98765)=35$ en $\rho(5363013565) = 37$. Wil de berekening kloppen, dan moet dus ook $15 \times 35 \equiv 37 \pmod 9$. Maar we mogen elk van deze getallen nog reduceren mod 9 om de berekeningen te vereenvoudigen. Dus

$$\begin{aligned} & 15 \times 35 \equiv 37 \pmod 9 \\ \iff\ & 6 \times 8 \equiv 1 \pmod 9 \\ \iff\ & 48 \equiv 1 \pmod 9 \\ \iff\ & 3 \equiv 1 \pmod 9 \end{aligned}$$

wat dus fout is.

3.10 Modulair rekenen

Vermits congruentie modulo m een equivalentierelatie is, kunnen we kijken naar de partitie die ontstaat. Bijvoorbeeld:

$$\begin{aligned}
E_0 &= \{0, m, 2m, -5m, \ldots\} \\
&= \{km \mid k \in \mathbb{Z}\} \\
&= \{\text{veelvouden van } m\} \\
E_1 &= \{1, m+1, -3m+1, \ldots\} \\
&= \{km+1 \mid k \in \mathbb{Z}\} \\
&= \{\text{gehele getallen waarvoor de rest bij deling door } m \text{ gelijk is aan } 1\} \\
E_2 &= \{km+2 \mid k \in \mathbb{Z}\} \\
&\vdots \\
E_{m-1} &= \{km+(m-1) \mid k \in \mathbb{Z}\} \\
E_m &= E_0.
\end{aligned}$$

We hebben m congruentieklassen. Ze vormen een partitie van $\mathbb{Z}$. De bewerkingen van $\mathbb{Z}$ induceren bewerkingen op deze m congruentieklassen:

$$E_k + E_l := E_{k+l}, \qquad E_k \times E_l := E_{k \times l}.$$

Natuurlijk moeten we nagaan dat deze bewerkingen niet afhangen van de keuze van de representanten in E_k en E_l.

Zij $E_k = E_{k'}$ en $E_l = E_{l'}$. We moeten bewijzen dat $E_{k+l} = E_{k'+l'}$. Maar dat is gewoon een gevolg van Stelling 23 omdat $k \equiv_m k'$ en $l \equiv_m l'$ en dus $k + l \equiv_m k' + l'$. Voor de vermenigvuldiging werken we volledig analoog.
Notatie. De verzameling $\{E_0, E_1, \ldots, E_{m-1}\}$ noteren we $\mathbb{Z}_m$.

Stelling 24. $(\mathbb{Z}_m, +, .)$ *is een commutatieve ring met eenheid.*

Bewijs. De bewerkingen zijn inwendig: $E_k + E_l \in \mathbb{Z}_m$ en $E_k \times E_l \in \mathbb{Z}_m$. De commutativiteit komt neer op $E_k + E_l = E_l + E_k$ en $E_k \times E_l = E_l \times E_k$, wat klopt door de overeenkomstige eigenschappen van $+$ en $\times$ in $\mathbb{Z}$. Verder moeten we nog aantonen dat

$$\begin{aligned}
&(E_k + E_l) + E_n = E_k + (E_l + E_n) \\
&(E_k \times E_l) \times E_n = E_k \times (E_l \times E_n) \\
&E_k + E_0 = E_k = E_0 + E_k \\
&E_k \times E_1 = E_k = E_1 \times E_k \\
&E_k \times (E_l + E_n) = E_k \times E_l + E_k \times E_n \\
&(E_k + E_l) \times E_n = E_k \times E_n + E_l \times E_n \\
&\forall E_k \in \mathbb{Z}_m : \exists\ -E_k = E_{-k} \in \mathbb{Z}_m : E_k + (-E_k) = E_0 = (-E_k) + E_k
\end{aligned}$$

We laten de bewijzen als oefening. □

Vereenvoudiging van notatie

Vermits de rekenregels in $(\mathbb{Z}_m, +, \times)$ dezelfde zijn als in $(\mathbb{Z}, +, \times)$, kunnen we zonder gevaar k noteren in plaats van E_k voor de restklasse van k modulo m. De context moet dan uitwijzen of we modulo m tellen of gewoon in $\mathbb{Z}$. $5 + 3$ zal dus een verkorte notatie zijn voor $E_5 + E_3$ in $\mathbb{Z}_6$ bijvoorbeeld. We zullen dan ook hebben $5 + 3 = 2$.

Toch even wijzen op een belangrijk verschil tussen $\mathbb{Z}$ en $\mathbb{Z}_m$. In $\mathbb{Z}$ geldt voor elke $a \neq 0$ dat $ab = ac \Rightarrow b = c$. Dit is niet langer waar in $\mathbb{Z}_m$. In $\mathbb{Z}_6$ bijvoorbeeld hebben we $3 \times 1 = 3 \times 5$, maar $1 \neq 5$.

Inverteerbare elementen in $\mathbb{Z}_m$

We hebben gezien dat $(\mathbb{Z}_m, +, \times)$ een commutatieve ring is met eenheid. Het verschil met veelgebruikte ringen zoals $(\mathbb{Q}, +, \times)$ of $(\mathbb{R}, +, \times)$ is dat sommige elementen niet inverteerbaar zijn.

Definitie 16. *$x \in \mathbb{Z}_m$ heet **inverteerbaar** indien er een $y \in \mathbb{Z}_m$ bestaat met $x \times y = 1$ (dus $x \times y \equiv_m 1$).*

Voorbeeld. In $\mathbb{Z}_6$ is 1 inverteerbaar, want $1 \times 1 = 1$. 2 is *niet* inverteerbaar want $2 \times 0 = 0$, $2 \times 1 = 2$, $2 \times 2 = 4$, $2 \times 3 = 0$, $2 \times 4 = 2$, $2 \times 5 = 4$. Dus $\nexists y \in \mathbb{Z}_6 : 2 \times y = 1$.

Lemma 2. *Zij $x \in \mathbb{Z}_m$ inverteerbaar. Dan is het invers van x uniek.*

Bewijs. Veronderstel dat y en z twee inversen zijn. Dus $xy = xz = 1$. Dan $y = y \times 1 = y(xz) = (yx)z = 1 \times z = z$. □

Bijgevolg kunnen we een notatie invoeren voor het uniek invers van $x \in \mathbb{Z}_m$, namelijk x^{-1}. Noteer ook $\mathcal{U}_m = \{x \in \mathbb{Z}_m \mid x \text{ inverteerbaar}\}$.

Stelling 25.

$$\forall x \in \mathbb{Z}_m : x \in \mathcal{U}_m \iff \text{ggd}(x, m) = 1.$$

Bewijs. $\boxed{\Rightarrow}$

$$\begin{aligned} x \in \mathcal{U}_m &\iff \exists\, y \in \mathbb{Z}_m : xy = 1 \\ &\iff \exists y \in \mathbb{Z}, \exists\, k \in \mathbb{Z} : xy - 1 = km \\ &\iff \exists y \in \mathbb{Z}, \exists\, k \in \mathbb{Z} : xy - km = 1 \end{aligned}$$

Een gemene deler van x en m is ook een deler van $xy - km$. Bijgevolg is $\text{ggd}(x, m) = 1$.

$\boxed{\Leftarrow}$ $\gcd(x,m) = 1 \Rightarrow \exists\, y,k \in \mathbb{Z} : xy + km = 1$ of $xy - 1 = -km$ of nog $m \mid xy - 1$ zodat $xy = 1$ in $\mathbb{Z}_m$.

□

Gevolg 6. $|\mathcal{U}_m| = \varphi(m)$.

Definitie 17. *Een ring met eenheid waarin* elk *niet-nul element inverteerbaar is, heet een* ***lichaam****. Indien de vermenigvuldiging bovendien commutatief is, spreekt men van een* ***veld****.*

Gevolg 7. *Voor p priem is elk van nul verschillend element in $\mathbb{Z}_p$ inverteerbaar. $(\mathbb{Z}_p, +, \times)$ is dus een veld.*

Lemma 3. *Als $x, y \in \mathcal{U}_m$, dan $xy \in \mathcal{U}_m$ en $(xy)^{-1} = y^{-1}x^{-1}$.*

Bewijs. $xy \times y^{-1}x^{-1} = xx^{-1} = 1$ en inversen zijn uniek. □

Stelling 26.

$$\forall y \in \mathcal{U}_m : y\mathcal{U}_m = \mathcal{U}_m.$$

Bewijs. Uit Lemma 3 volgt $y\mathcal{U}_m \subset \mathcal{U}_m$. Stel nu $x \in \mathcal{U}_m$. Dan is $x = y(y^{-1}x)$ en $y^{-1} \in \mathcal{U}_m$, want $y^{-1}y = 1$, zodat $y^{-1}x \in \mathcal{U}_m$. □

Stelling 27. *Zij $y \in \mathcal{U}_m$. Dan geldt: $y^{\varphi(m)} = 1$ in $\mathbb{Z}_m$.*

Bewijs. Nummer de elementen van $\mathcal{U}_m$. Dus $\mathcal{U}_m = \{u_1, u_2, \ldots, u_{\varphi(m)}\}$. Stel $u := u_1u_2 \cdots u_{\varphi(m)}$. Dan is u een element van $\mathcal{U}_m$, want het is een product van elementen van $\mathcal{U}_m$.

Vermits $y\mathcal{U}_m = \mathcal{U}_m$ zijn de elementen $yu_1, yu_2, \ldots, yu_{\varphi(m)}$ niets anders dan $u_1, u_2, \ldots, u_{\varphi(m)}$, eventueel in een andere volgorde geschreven. Bijgevolg geldt ook:

$$yu_1 \times yu_2 \times \cdots \times yu_{\varphi(m)} = u$$

of nog

$$y^{\varphi(m)}u_1u_2 \cdots u_{\varphi(m)} = u$$

of

$$\begin{aligned} & y^{\varphi(m)}u &=& u \\ \iff\quad & y^{\varphi(m)}uu^{-1} &=& uu^{-1} \\ \iff\quad & y^{\varphi(m)} &=& 1. \end{aligned}$$

□

Andere formuleringen van dezelfde stelling:

$$\forall y \in \mathbb{Z}, \forall m \in \mathbb{N}_0 : \text{ggd}(y, m) = 1 \Rightarrow y^{\varphi(m)} \equiv_m 1.$$

Dit resultaat heet de *Stelling van Euler*. Een speciaal geval is de *Kleine stelling van Fermat*:

Stelling 28. *Voor p priem hebben we*

$$\forall n \in \mathbb{N} : n^p \equiv_p n.$$

Bewijs. Als $p \nmid n$ is n inverteerbaar modulo p zodat $n^{\varphi(p)} \equiv_p 1$, of nog $n^{p-1} \equiv_p 1$, zodat $n^p \equiv_p n$.

Als $p \mid n$ is het duidelijk dat $n^p \equiv_p 0 \equiv_p n$. □

3.11 De Chinese reststelling

In de eerste eeuw stelde de Chinese wiskundige Sun-Tsu het volgende vraagstuk: "Van een getal weet men dat de rest bij deling door 3 gelijk is aan 2; wanneer men deelt door 5, vindt men als rest 3 en bij deling door 7 bedraagt de rest 2. Over welk getal gaat het?"

Het gaat hier eigenlijk om een *stelsel* van verschillende vergelijkingen waaraan het onbekende getal x moet voldoen:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

Dit probleem kan gemakkelijk opgelost worden aan de hand van de zogenaamde *Chinese reststelling*.

Stelling 29 (Chinese reststelling)**.** *Zij $m_1, m_2, \ldots, m_n$ paarsgewijs relatief prieme natuurlijke getallen en $a_1, a_2, \ldots, a_n$ willekeurige gehele getallen. Dan heeft het stelsel*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

een oplossing die uniek is modulo $m = m_1 m_2 \cdots m_n$. D.w.z. een unieke oplossing x met $0 \leqslant x < m$ en alle andere oplossingen congruent modulo m met deze x.

Bewijs. We geven een *constructief* bewijs. We gaan dus een algoritme geven om de oplossing werkelijk te construeren.

Voor $k \in [n]$ stellen we eerst $M_k := m/m_k$. Dit is het product van alle moduli, behalve m_k. Vermits alle moduli relatief priem zijn, hebben we zeker $\text{ggd}(m_k, M_k) = 1$. Stelling 25 zorgt dan voor een getal y_k met

$$M_k y_k \equiv 1 \pmod{m_k}$$

Stel nu

$$x := a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \in \mathbb{Z}.$$

We tonen nu dat deze x een oplossing is van het stelsel. Merk eerst op dat $M_j \equiv 0 \pmod{m_i}$ van zodra $i \neq j$. Als we dus x reduceren modulo m_k, blijft er alleen maar

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$$

over.

Onderstel nu dat y een andere oplossing is van het stelsel. Dan geldt voor elke $k \in [n]$ dat $m_k \mid x - y$. Vermits alle m_k relatief priem zijn, volgt hieruit $m \mid x - y$. □

Voorbeeld. We kunnen nu de vraag van Sun-Tsu oplossen.

We berekenen $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$ en $M_3 = m/7 = 15$. De inversen van M_k modulo m_k berekenen is ook niet moeilijk. We vinden $y_1 = 2$, $y_2 = 1$ en $y_3 = 1$. Hieruit vinden we

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}.$$

3.12 Public key cryptography

Als je geheime berichten wil versturen moet je een techniek afspreken om te *coderen*. Deze techniek noemen we een **cryptosysteem**.

Een bekend eenvoudig cryptosysteem bestaat erin om de letters te "verschuiven" in het alfabet. Als je bijvoorbeeld het bericht "`IK HEB EEN GEHEIM`" wil versturen, kan je elke letter drie plaatsen opschuiven in het alfabet. Je stuurt dus "`LN KHE HHQ JHKHLP`". Indien je als antwoord "`LN ZLO KHW ZHWHQ`" krijgt, kan je door de inverse operatie het bericht ontcijferen. Je krijgt "`IK WIL HET WETEN`".

Zulk eenvoudig systeem is doeltreffend indien men er zeker van is dat het bericht nooit zal onderschept worden door iemand die iets weet over de frequentie waarmee letters voorkomen in de Nederlandse taal. In onze berichten zie je bijvoorbeeld twee keer "`HHQ`". Er is veel kans dat dit "`EEN`" voorstelt.

Een ander nadeel van dit systeem is dat de twee personen die willen communiceren, op voorhand moeten afspreken hoeveel plaatsen zij elke letter opschuiven. Dit is wat men de *sleutel* van het cryptosysteem noemt. Deze sleutel moet geheim blijven. De sleutel uitwisselen tussen de twee personen die willen communiceren is dus een probleem bij dit soort cryptosysteem. Voor betalingen over internet moeten vele gebruikers communiceren met één bedrijf. Het is onbegonnen werk om voor elke gebruiker een sleutel mee te delen zonder dat hij kan onderschept worden. Gelukkig werd er in de jaren '70 door Rivest, Shamir en Adleman een systeem bedacht waarbij de sleutels niet meer geheim hoeven te zijn. Men spreekt van *Public Key Cryptography*.

Het systeem is gebaseerd op priemgetallen en modulair rekenen. Persoon A wil een geheim bericht naar persoon B sturen. Hiervoor gaat hij eerst zijn bericht (dat in letters geschreven is) vertalen naar getallen zodat er kan gerekend worden. Dit gebeurt via een standaard tabel die niet geheim hoeft te zijn. We kunnen bijvoorbeeld afspreken dat "A" wordt voorgesteld door het getal 1, "B" door 2, enz. De spatie is 0. Het bericht "`LUISTER GOED`" wordt dan bijvoorbeeld "`12 21 09 19 20 05 18 00 07 15 05 04`".

We gaan nu elke letter coderen door het te verheffen tot een vaste macht en dan het resultaat te reduceren modulo 33 (omdat er bijvoorbeeld 33 tekens zijn in ons eenvoudig systeem: letters plus wat leestekens). Laat ons bijvoorbeeld telkens de derde macht nemen. Dan is het gecodeerd bericht "`12 21 3 28 14 26 24 0 13 9 26 31`".

Dit was een voorbeeld met kleine getallen om te illustreren wat er gebeurt. In de praktijk gaan we te werk met veel grotere getallen. We moeten ook nog zien hoe deze machtsverheffing kan geïnverteerd worden om te decoderen.

Eén van de voornaamste eigenschappen waarop de veiligheid van het RSA cryptosysteem steunt, is de moeilijkheid om een willekeurig getal te ontbinden in priemfactoren. Het is bijvoorbeeld zeer gemakkelijk om de twee priemgetallen 71 en 59 met elkaar te vermenigvuldigen. We krijgen 4189. Probeer nu het omgekeerde: neem een vergelijkbaar getal, 4161, en probeer dat eens te ontbinden in priemfactoren.

Laat ons de methode van de machtsverheffing nu eens proberen met grotere getallen: we verheffen tot de macht 101 en reduceren modulo 1189. Vermits resten modulo 1189 groter kunnen worden dan 27 hebben we de

mogelijkheid om meer symbolen te gebruiken of meerdere letters ineens te coderen. In ons bericht "`12 21 09 19 20 05 18 00 07 15 05 04`" van hoger kunnen we de cijfers per drie groeperen zodat we "`122 109 192 005 180 007 150 504`" verkrijgen. Indien het aantal cijfers geen veelvoud is van drie, voegen we op het einde nullen toe om overal groepjes van drie cijfers te hebben.

We moeten nu dus 122^{101} berekenen. Dat is een ander paar mouwen... Zelfs met een rekenmachine zal dat niet lukken, tenzij we het slim aanpakken. We hebben hier immers te maken met een getal van 211 cijfers. Een eerste idee zou zijn om die macht stap voor stap te berekenen en steeds te reduceren modulo 1189. Op die manier krijgen we geen al te grote getallen.

Hier gaan we dan:

$$\begin{aligned} 122^2 &= 122 \cdot 122 = 14884 \equiv 616 \pmod{1189} \\ 122^3 &= 122^2 \cdot 122 \equiv 616 \cdot 122 = 75152 \equiv 245 \pmod{1189} \\ 122^4 &= 122^3 \cdot 122 \equiv 245 \cdot 122 = 29890 \equiv 165 \pmod{1189} \\ &\vdots \end{aligned}$$

Maar dat is ook nogal veel werk. Veel slimmer is om steeds te kwadrateren.

$$\begin{aligned} 122^2 &= \quad\quad = 14884 \equiv 616 \pmod{1189} \\ 122^4 &\equiv 616^2 = 379456 \equiv 165 \pmod{1189} \\ 122^8 &\equiv 165^2 = 27225 \equiv 1067 \pmod{1189} \\ 122^{16} &\equiv 1067^2 = 1138489 \equiv 616 \pmod{1189} \\ 122^{32} &\equiv 616^2 = 379456 \equiv 165 \pmod{1189} \\ 122^{64} &\equiv 165^2 = 27225 \equiv 1067 \pmod{1189} \end{aligned}$$

Nu geldt $101 = 1+4+32+64$ zodat $122^{101} = 122^1 \cdot 122^4 \cdot 122^{32} \cdot 122^{64} \equiv 122 \cdot 165 \cdot 165 \cdot 1067 = 3543987150 \equiv 245 \pmod{1189}$.

Dus met vijf kwadrateringen, een paar vermenigvuldigingen en reducties modulo 1189 hebben we het resultaat. Dit is veel efficiënter dan de honderd vermenigvuldigingen en reducties die we eerst gingen uitvoeren! Deze methode werkt steeds omdat we elke mogelijke exponent steeds kunnen schrijven als som van machten van 2. Dit komt er immers op neer dat we de exponent uitschrijven in basis 2 (zie blz. 46).

We beschrijven nu het RSA algoritme in het algemeen. Persoon B die berichten wil ontvangen kiest twee (grote) priemgetallen p en q en berekent

hun product $n := pq$. Hij bepaalt ook $b := (p-1)(q-1)$ en zoekt e met $\text{ggd}(e, b) = 1$. De informatie die publiek wordt gemaakt is n en e.

Indien persoon A een gecodeerd bericht wil sturen naar B zal hij eerst zijn bericht omzetten in getallen. Elk van die getallen m gaat hij dan coderen als volgt

$$c := m^e \pmod{n}$$

Het symbool c wordt dan verstuurd.

Wanneer B het bericht c ontvangt, moet hij dat decoderen. Hij maakt hiervoor gebruik van het feit dat $\text{ggd}(e, b) = 1$. Er is dus een invers d van e modulo b. Er bestaat dus een k met $ed = 1 + k(p-1)(q-1)$ zodat

$$c^d \equiv (m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} \pmod{n}$$

We veronderstellen nu even dat $\text{ggd}(m, p) = \text{ggd}(m, q) = 1$, wat geen grote beperking is. Dan kunnen we de uit de Stelling van Euler (Stelling 27) halen dat $m^{p-1} \equiv 1 \pmod{p}$ en $m^{q-1} \equiv 1 \pmod{q}$. Bijgevolg geldt

$$c^d \equiv m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1 \equiv m \pmod{p}$$

alsook

$$c^d \equiv m \cdot (m^{q-1})^{k(p-1)} \equiv m \cdot 1 \equiv m \pmod{q}.$$

Merk op dat indien m een veelvoud is van p of q, bovenstaande equivalenties geldig blijven. De onderstelling $\text{ggd}(m, p) = \text{ggd}(m, q) = 1$ was dus slechts tijdelijk nodig.

Uit de Chinese reststelling volgt nu dat

$$c^d \equiv m \pmod{pq}$$

Dus kan B decoderen door gewoon c^d te reduceren modulo n.

Merk op dat je ook gemakkelijk "met de hand" kan bewijzen dat $c^d \equiv m \pmod{pq}$.

In de praktijk worden priemgetallen van ongeveer tweehonderd cijfers gebruikt. Dan heeft n ongeveer vierhonderd cijfers en duurt de ontbinding in priemfactoren, met de beste algoritmen die tot nu toe bekend zijn, nog duizenden jaren. Men mag dus zeggen dat RSA cryptosystemen voorlopig veilig zijn. Bovendien bieden zij het grote voordeel dat de sleutel die dient voor het coderen publiek mag gemaakt worden zonder het systeem in gevaar te brengen.

3.13 Oefeningen

1. ◐ Bewijs dat

$$\forall n \in \mathbb{N}_0 \colon 1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1)$$

2. ◐ Bereken $S_n = 1^3 + 2^3 + \cdots + n^3$ voor $1 \leqslant n \leqslant 6$. Leid daaruit een formule af voor S_n. Bewijs je hypothese.

3. ◐ Zoek het kleinste natuurlijk getal n_0 waarvoor geldt dat $n! \geqslant 2^n$. Bewijs deze eigenschap voor alle $n \geqslant n_0$.

4. ○ Hoe ziet 2004 eruit in de stelsels met grondtal 2, 5 en 11?

5. ○ Toon aan: als $c \mid a$ en $c \mid b$, dan $\forall x, y \in \mathbb{Z} \colon c \mid (xa + yb)$.

6. ◐●

   (a) Zij $a \geqslant 10$ een geheel getal. Construeer b als volgt: vermenigvuldig het laatste cijfer van a met 5 en tel het resultaat op bij het getal dat je bekomt door het laatste cijfer van a weg te laten [voorbeeld: $a = 8429 \longrightarrow b = 5 \times 9 + 842 = 887$]. Toon nu aan: $7 \mid a \Leftrightarrow 7 \mid b$.

   (b) Omdat b doorgaans kleiner is dan a kunnen we het voorgaande gebruiken als test voor deelbaarheid door 7: je past het truukje steeds opnieuw toe op het getal dat je bekomt, tot je een resultaat bereikt waarvan je op het zicht ziet of het deelbaar is door 7.

   We willen nu een soortgelijke test ontwikkelen voor deelbaarheid door 13: gegeven een getal a construeren we b door het laatste cijfer van a te vermenigvuldigen met een getal m en dat resultaat op te tellen bij het getal dat je bekomt door in a het laatste cijfer weg te laten [dus: $a = 8429 \to b = 842 + 9m$]. Zoek nu m zodanig dat geldt: $13 \mid a \Leftrightarrow 13 \mid b$.

   [examen januari 2006]

7. ◐ Zij *abc* een getal van drie cijfers. Het *omgekeerde* van dat getal is *cba*. We noteren het omgekeerde van een getal x met $\bar{x}$. Onderstel nu dat x een getal is met drie cijfers waarvan het eerste en het laatste cijfer verschillend zijn. Dan geldt ofwel $x > \bar{x}$ ofwel $x < \bar{x}$. Zonder de algemeenheid te schaden veronderstellen we dat $x > \bar{x}$. Bereken nu $y := x - \bar{x}$ en dan $y + \bar{y}$. Welk resultaat krijg je? Probeer het op enkele voorbeelden en geef dan een bewijs.

8. ○ Bewijs dat $6 \mid (n^3 + 3n^2 + 2n)$, $\forall n \geqslant 0$.

9. ○ Zoek de grootste gemene deler van 721 en 448 en schrijf hem in de vorm $721m + 448n$ met $n, m \in \mathbb{Z}$.

10. ◐ Zij u en v gehele getallen. Toon aan : als er $n, m \in \mathbb{Z}$ bestaan zodat $mu + nv = 1$ dan is $\text{ggd}(u, v) = 1$.

11. ◐ Toon aan: $\text{ggd}(a, b) = d \Longrightarrow \text{ggd}(\frac{a}{d}, \frac{b}{d}) = 1$.

12. ○ Zoek $x, y \in \mathbb{Z}$ zodat $966x + 686y = 70$. [$x = -110$ en $y = 155$]

13. ○ Toon aan: als $n \geqslant 2$ en n is niet priem, dan bestaat er een priemgetal p met $p \mid n$ en $p^2 \leqslant n$. Leid hieruit af dat 467 priem is.

14. ◐ Toon aan : als $n, m \in \mathbb{Z}$, $m, n \geqslant 2$ en $m^2 = kn^2$ voor $k \in \mathbb{Z}$, dan is k een kwadraat.

15. ● Toon aan: als $2^n - 1$ priem is, dan is n priem. Zoek het kleinste getal n waarvoor het omgekeerde vals is (m.a.w. een priemgetal n zodat $2^n - 1$ niet priem is).

16. ○ Toon aan dat

$$1^4 + 2^4 + \cdots + n^4 = \frac{1}{30} n(n+1)(2n+1)(3n^2 + 3n - 1)$$

17. ◐ Toon aan dat $4^{2n} - 1$ deelbaar is door 15, voor elk niet-nul natuurlijk getal.

18. ◐ Zij $h > -1$ een reëel getal. Bewijs voor elk natuurlijk getal n volgende ongelijkheid:

$$1 + nh \leq (1 + h)^n$$

[examen januari 2005]

19. ◐ Bewijs dat voor elk natuurlijk getal $n > 0$ geldt

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = \frac{1}{4} n(n+1)(n+2)(n+3).$$

[examen januari 2005]

20. ◐ Zij $H_n = \sum_{i=1}^{n} \frac{1}{i}$. Toon aan dat $\sum_{n=1}^{k} H_n = (k+1)H_k - k$. [examen augustus 2005]

21. ○ Voor $n \in \mathbb{N}_0$ definiëren we

$$s_n = \sum_{k=1}^{n} \sum_{i=1}^{k} i.$$

Bewijs dat $s_n = \frac{1}{6}n(n+1)(n+2)$. [examen augustus 2006]

22. ◐ Voor een deelverzameling A van $\mathbb{N}_0$ definiëren we π_A als het product van alle elementen in A. Nu definiëren we voor $n \in \mathbb{N}_0$

$$s_n = \sum_{\emptyset \neq A \subset [1..n]} \frac{1}{\pi_A}.$$

We hebben dus bijvoorbeeld

$$s_3 = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 3} + \frac{1}{2 \cdot 3} + \frac{1}{1 \cdot 2 \cdot 3}.$$

(a) Wat is de waarde van s_3?

(b) Bepaal s_2 en s_4.

(c) Vind een algemene formule voor de waarde van s_n en bewijs deze.

[examen augustus 2006]

23. ○ Je beschikt over een onbeperkte hoeveelheid water, een afvoer, een container en twee emmertjes van 7 en 9 liter. Hoe kan je ervoor zorgen dat er 1 liter water in de container terecht komt?

24. ● Zoek alle getallen n met de volgende eigenschappen :

(a) $n \in \mathbb{N}_0$;

(b) elke priemfactor van n komt maar één keer voor in de ontbinding;

(c) als p priem is, geldt : $p \mid n \Leftrightarrow (p-1) \mid n$.

25. ◐ Toon aan : als n een positief geheel getal is, dan is geen enkel van de n opeenvolgende getallen beginnend met $(n+1)! + 2$ priem.

26. ● Toon aan : als $\text{ggd}(a, b) = 1$, dan is $\text{ggd}(a+b, a-b)$ ofwel 1 ofwel 2.

27. ○ Vind $\varphi(19)$, $\varphi(20)$ en $\varphi(21)$.

28. ● Toon aan : als x en n relatief priem zijn, dan zijn ook $n - x$ en n relatief priem. Leid daaruit af dat $\varphi(n)$ even is van zodra $n \geqslant 3$.

29. ● Toon aan : als p priem is en m is een positief geheel getal, dan geldt : een getal $1 \leqslant x \leqslant p^m$ is *niet* relatief priem met p^m als en slechts als het een veelvoud is van p. Leid hieruit af dat $\varphi(p^m) = p^m - p^{m-1}$.

30. ◐ Toon aan : als de factorisatie van n gegeven wordt door

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

dan is het aantal delers van n gelijk aan

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1).$$

31. ◐ Toon aan : als $\text{ggd}(m, n) = 1$, dan is $\varphi(mn) = \varphi(m)\varphi(n)$.

32. ○ Zij $X = \{1, 2, 5, 6, 7, 9, 11\}$ en schrijf $x \sim x'$ als $x - x'$ deelbaar is door 5. Verifieer dat $\sim$ een equivalentierelatie is en geef de partitie van X die deze equivalentierelatie induceert.

33. ○ Toon aan, zonder de vermenigvuldiging uit te voeren, dat

(a) $1234567 \times 90123 \equiv_{10} 1$

(b) $2468 \times 13579 \equiv_{25} -3$

34. ○ Gebruik de negenproef om te tonen dat twee van de volgende gelijkheden vals zijn. Wat kan je over de derde zeggen?

(a) $5783 \times 40162 = 233256846$

(b) $9787 \times 1258 = 12342046$

(c) $8901 \times 5743 = 52018443$

35. ○ Zoek $3^{15} \pmod{17}$ en $15^{81} \pmod{13}$.

36. ◐ Zij $(x_n x_{n-1} \ldots x_1 x_0)_{10}$ de voorstelling van het positieve getal x in het 10-delig stelsel. Toon aan dat $x \equiv x_0 - x_1 + x_2 \cdots + (-1)^n x_n \pmod{11}$. Gebruik dit resultaat om te testen of 1213141516171819 deelbaar is door 11.

37. ○ Maak de optellings- en vermenigvuldigingstabel van $\mathbb{Z}_6$.

38. ◐ Los het stelsel

$$\begin{cases} x + 2y &= 4 \\ 4x + 3y &= 4 \end{cases}$$

op in $\mathbb{Z}_7$ en $\mathbb{Z}_5$.

39. ◐ Los
$$x^2 + 3x + 4 = 0$$
op in $\mathbb{Z}_{11}$. [3 en 5]

40. ◐ Zoek de inverteerbare elementen van $\mathbb{Z}_6$, $\mathbb{Z}_7$ en $\mathbb{Z}_8$.

41. ◐ Toon aan:
    (a) 0 is nooit inverteerbaar in $\mathbb{Z}_m$, en 1 altijd.
    (b) Als x en y inverteerbaar zijn in $\mathbb{Z}_m$, dan zijn ook xy en x^{-1} inverteerbaar in $\mathbb{Z}_m$.

42. ○ Vind de inversen van
    (a) 2 in $\mathbb{Z}_{11}$
    (b) 7 in $\mathbb{Z}_{16}$
    (c) 7 in $\mathbb{Z}_{15}$
    (d) 5 in $\mathbb{Z}_{13}$

43. ○ Wat is de rest van 3^{47} bij deling door 23?

44. ◐ Stel dat a en b gehele getallen zijn, en p een priemgetal. Toon aan dat
$$(a+b)^p \equiv_p a^p + b^p$$

45. ● Zij p een priemgetal. Toon aan dat de vergelijking $x = x^{-1}$ in $\mathbb{Z}_p$ impliceert dat $x^2 - 1 = 0$. Leid hieruit af dat 1 en -1 de enige elementen van $\mathbb{Z}_p$ zijn die gelijk zijn aan hun eigen invers.

46. ● Toon aan dat voor p priem geldt
$$(p-1)! \equiv_p -1.$$

47. ● Zij $(a_i)_{i\in\mathbb{N}}$ een rij natuurlijke getallen met
$$a_i a_j = (a_{\text{kgv}(i,j)})^{\text{ggd}(i,j)}$$
Dan geldt dat ofwel
    (a) $a_1 = 1$, $a_i = 0$ voor alle $i > 2$ en a_2 is willekeurig; ofwel
    (b) er bestaat voor elk priemgetal p een getal $e(p) \in \mathbb{N} \cup \{\infty\}$ zodat $a_i = 0$ indien i deelbaar is door $p^{e(p)}$ voor een zeker priemgetal en $a_i = 1$ voor alle andere i.

48. ◐ De ISBN-code van een boek bestaat uit tien cijfers $x_1x_2\cdots x_{10}$ waarvoor volgende gelijkheid geldt

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$$

Door een beschadiging is het ISBN-nummer van een boek van de VUB-bibliotheek niet meer volledig leesbaar: er is één cijfer gewist. Als we dat cijfer voorstellen door x, zien we $020157x891$. Wat is x? [examen januari 2005]

49. ◐ Zoek het invers element van 25 in $\mathbb{Z}_{72}$. [examen augustus 2005]

50. ◐ Zij $n > 1$. Toon aan:

(a) Als $n = 2k$ en k is oneven, dan geldt $k^3 \equiv_n k$.

(b) Als $n = 4k$ dan geldt $(2k)^2 \equiv_n 0$.

(c) $\sum_{i=1}^{n-1} i^3 \equiv_n \begin{cases} \frac{n}{2} & \text{als } n \text{ een tweevoud is maar geen viervoud} \\ 0 & \text{in alle andere gevallen} \end{cases}$

[examen augustus 2005]

51. ○ Bepaal $\varphi(204)$, waarbij φ de φ-functie van Euler voorstelt. [examen januari 2006]

52. ◐ Gegeven is de vierkantsvergelijking

$$x^2 + 11x + 7 \equiv 0.$$

Bepaal alle oplossingen ervan in $\mathbb{Z}_{17}$ en in $\mathbb{Z}_{20}$. [examen augustus 2006] [In $\mathbb{Z}_{17}$: 9 en 14; in $\mathbb{Z}_{20}$: geen]

53. ◐ Gegeven is de vierkantsvergelijking

$$5x^2 + 4x + 1 \equiv 0.$$

Bepaal alle oplossingen ervan in $\mathbb{Z}_{17}$ en in $\mathbb{Z}_{20}$. [examen augustus 2006] [In $\mathbb{Z}_{17}$: 9 en 14; in $\mathbb{Z}_{20}$: geen]

54. ○ Vind een x die tegelijk voldoet aan volgende twee congruenties.

$$x \equiv 5 \pmod{8} \qquad x \equiv 73 \pmod{81}$$

55. ◐ Een groep van 17 piraten verovert een schat die bestaat uit een koffer vol met (identieke) goudstukken. Wanneer één van de piraten de buit eerlijk wil verdelen, blijven er 3 stukken over. Een andere piraat beschuldigt de verdeler ervan fout geteld te hebben en doodt hem in een duel. Nu worden de goudstukken opnieuw eerlijk verdeeld onder de 16 overblijvende piraten. Nu blijven er 10 stukken over. Weer wordt er gevochten en verliest een piraat het leven. Als men nu de goudstukken verdeelt in 15 gelijke stapels, blijft er geen stuk meer over. Wat is het kleinst mogelijk aantal goudstukken dat in de koffer heeft kunnen zitten?

56. ◐ Vind alle oplossingen van volgend stelsel.

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

57. ○ Bereken

$$30^{29} \pmod{51}, \qquad 7^{53} \pmod{123}, \qquad 11^{73} \pmod{187}, \qquad 19^{41} \pmod{91}.$$

58. ○ Vind voor volgende waarden van n de b van het RSA algoritme.

$$n = 85, \qquad n = 143, \qquad n = 323, \qquad n = 299$$

59. ◐ Je onderschept een geheime boodschap $c = 2$ en je weet dat de publieke sleutel van de ontvanger de waarden $n = 55$ en $e = 7$ heeft. Ontcijfer het bericht!

60. ● Ontcijfer het bericht "`0986 3029 1134 1105 1232 2281 2967 0272 1818 2398 1153`" als je weet dat de publieke sleutel $n = 3053$ en $e = 17$ is.

Hoofdstuk 4

Inleiding tot de grafentheorie

In Hoofdstuk 2 losten we reeds een probleem op door een grafische voorstelling met verbonden punten, welke ook nuttig is voor vele andere problemen. Daarom wijden we er nu een heel hoofdstuk aan.

4.1 Definities en terminologie

Definitie 18. *Een **graaf** bestaat uit een verzameling V wiens elementen we **toppen** noemen en een relatie $\to$ op V die we **adjacentierelatie** noemen. Een koppel (u, v) dat behoort tot de relatie $\to$ (d.w.z. $u \to v$) heet een **pijl**. De verzameling van pijlen noteren we met E.*

Meestal noteren we grafen met calligrafische letters $\mathcal{G}$, $\mathcal{H}$, ...

Bij ons zal de toppenverzameling van een graaf $\mathcal{G}$ meestal eindig zijn. De **orde** van $\mathcal{G}$ is dan $|V(\mathcal{G})|$, het aantal toppen in $\mathcal{G}$.

Nu kunnen we naargelang de eigenschappen van de adjacentierelatie verschillende soorten grafen onderscheiden.

Definitie 19. *Zij $\mathcal{G} = (V, \to)$ een graaf.*

*Indien de relatie $\to$ symmetrisch is, zegt men dat de graaf **ongericht** is. In dat geval schrijven we dikwijls $\sim$ in plaats van $\to$. Indien we willen benadrukken dat de graaf niet ongericht is, spreken we van een **gerichte graf**.*

*Indien $v \to v$ zeggen we dat de graaf een **lus** heeft in v. Een graaf zonder lussen noemen we **simpel** of **enkelvoudig**.*

Als er meerdere zulke grafen in het spel zijn, noteren we $V(\mathcal{G})$ om de toppenverzameling van $\mathcal{G}$ aan te duiden en $E(\mathcal{G})$ voor de pijlen. De letters V

en E komen van het Engels: een top is een "vertex" (meervoud "vertices") en een pijl een "edge".

Een ongerichte simpele graaf kunnen we ook zien als een koppel verzamelingen (V, E) waarbij V gestructureerd wordt door een verzameling E van 2-verzamelingen van V. We hebben dus $E \subset \binom{V}{2}$ en de elementen van E noemen we dan **bogen**. Twee toppen u, v van zulk een graaf (V, E) zijn dus adjacent indien $\{u, v\} \in E$. We zeggen dan ook dat u en v **buren** zijn. De **buurt** van een top v van een ongerichte simpele graaf $\mathcal{G}$ is de verzameling $\mathcal{G}_v$ van alle buren van v. We hebben dus

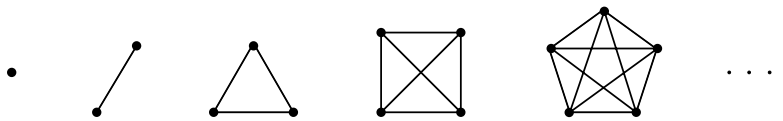
$$\mathcal{G}_v = \{x \in V(\mathcal{G}) \mid x \sim v\}$$

Een top zonder buren heet **geïsoleerd**.

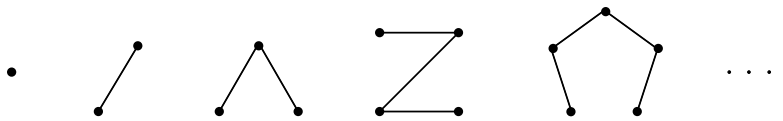
Opmerking. In de literatuur gebruikt men het woord "graf" vaak voor deze specifieke soort van ongerichte simpele grafen.

4.2 Belangrijke voorbeelden van ongerichte simpele grafen

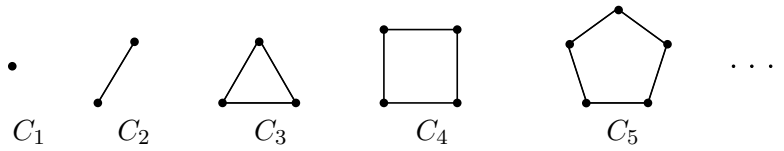
Complete grafen De complete graaf K_n heeft n toppen. Alle toppen zijn verbonden met alle overige toppen.



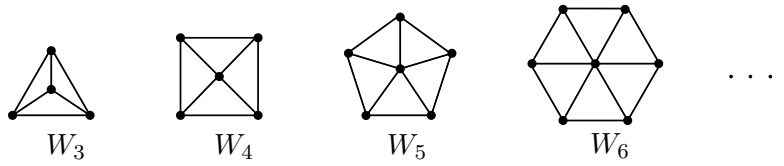
Paden Het pad P_n heeft n toppen $t_1, t_2, \ldots, t_n$ die zó verbonden zijn dat $t_i \sim t_{i+1}$ voor $i \in [n-1]$.



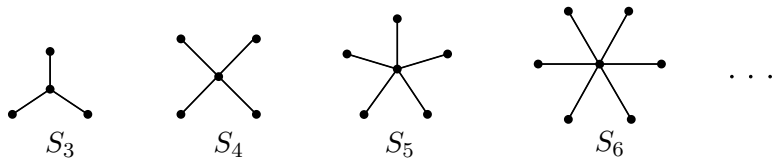
Cycli Een cyclus (of cykel) van lengte n is een graaf C_n met n toppen $t_0, t_1, \ldots, t_{n-1}$ die zó verbonden zijn dat $t_i \sim t_{i+1}$ voor $i \in \mathbb{Z}_n$, waarbij we de indices modulo n nemen.



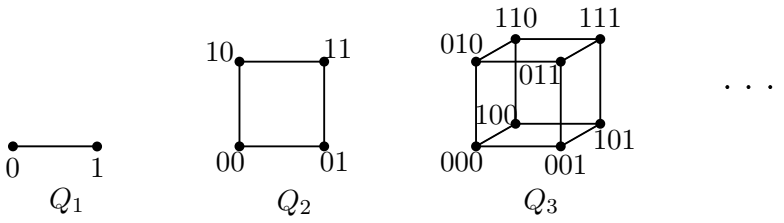
Wielen Het wiel W_n van orde n is een cyclus C_n met in het midden een top toegevoegd die verbonden is met alle toppen van de cyclus.



Sterren De ster S_n van orde n bekom je door in het wiel W_n de bogen van de cyclus weg te laten.



Kubussen Neem $\{0,1\}^n$ als toppenverzameling en maak twee toppen adjacent als ze verschillen in juist één coördinaat. We noteren de kubus in dimensie n met Q_n.



4.3 Verdere definities en eigenschappen

Definitie 20. *De* ***graad*** *van een top v in een ongerichte graaf $\mathcal{G}$ is het aantal bogen die v bevatten. Een lus tellen we twee keer. We noteren dit met* $\deg(v)$ *zodat geldt*

$$\deg(v) = |\mathcal{G}_v|.$$

Eigenschap 14 (Handshake)**.** *In een eindige ongerichte graaf $\mathcal{G}$ geldt steeds*

$$\sum_{v \in V(\mathcal{G})} \deg(v) = 2|E(\mathcal{G})|$$

Bewijs. Dubbeltelling: $\deg(v)$ is het aantal bogen die v bevatten en elke boog bevat juist twee toppen. □

Gevolg 8. *Een eindige ongerichte graaf heeft steeds een even aantal toppen van oneven graad.*

Bewijs. Omdat, wegens de vorige eigenschap, de som van alle graden even moet zijn. □

Een ander woord voor graad is **valentie**. Indien alle toppen van een ongerichte graaf dezelfde graad hebben, zeggen we dat de graf **regulier** is. Een **k-reguliere** graaf is een ongerichte graf waarin elke top graad k heeft.

Definitie 21. *In een gerichte graaf $\mathcal{G}$ definiëren we voor elke top v de **ingraad** en de **uitgraad** als het aantal pijlen dat in v respectievelijk aankomt en vertrekt. We noteren deze graden respectievelijk $\deg^+(v)$ en $\deg^-(v)$.*

*Een gerichte graaf heet **gebalanceerd** indien voor elke top v geldt dat $\deg^+(v) = \deg^-(v)$.*

Een **deelgraf** van een graaf $\mathcal{G}$ is een graaf $\mathcal{H}$ met $V(\mathcal{H}) \subset V(\mathcal{G})$ en $E(\mathcal{H}) \subset E(\mathcal{G})$. We spreken van een **opspannende deelgraf** indien $V(\mathcal{H}) = V(\mathcal{G})$. Zij $S \subset V(\mathcal{G})$. De **deelgraaf door $\mathcal{G}$ geïnduceerd op S** is de graaf met toppenverzameling S en de hierbij behorende pijlen (voor een ongerichte graaf hebben we dus de bogenverzameling $E(\mathcal{G}) \cap \binom{S}{2}$).

Een **wandeling** in een ongerichte graaf $\mathcal{G}$ is een rij van toppen

$$t_0, t_1, \ldots, t_k$$

zodanig dat $t_{i-1} \sim t_i$ voor elke $i \in [k]$. We spreken van een **gerichte wandeling** als $t_{i-1} \to t_i$.

De **lengte** van de wandeling is k, één minder dan het aantal toppen. De top t_0 heet **beginpunt** (of vertrekpunt) van de wandeling en t_k heet het **eindpunt** (of aankomstpunt). In een wandeling $t_0 \sim t_1 \sim \cdots \sim t_k$ zijn er dus k bogen van de vorm $\{t_{i-1}, t_i\}$ met $i \in [k]$. Als al die bogen verschillend zijn, wordt de wandeling een **pad** genoemd. Als $t_0 = t_k$ heet het pad **gesloten**. Een **simpel** of **enkelvoudig pad** is een pad waarin geen twee toppen gelijk zijn. Een gesloten pad dat na verwijderen van de top $t_0 = t_k$ een simpel pad wordt, heet een **cyclus**.

Een ongerichte graaf heet **samenhangend** indien er voor elk paar toppen $u, v \in V(\mathcal{G})$ een pad van u naar v bestaat. Een graaf die niet samenhangend is bestaat uit verschillende **samenhangscomponenten** waartussen geen bogen bestaan. Je kan dit ook als volgt bekijken: de relatie "... is verbonden met ... via een pad" is een equivalentierelatie op $V(\mathcal{G})$. De equivalentieklassen van die relatie zijn de samenhangscomponenten.

Een gerichte graaf $\mathcal{G}$ heet **samenhangend** indien de onderliggende graaf (verwijder alle pijlen op de bogen) samenhangend is. We zeggen dat $\mathcal{G}$ **sterk samenhangend** is indien er tussen elke twee toppen u en v een **gericht pad** bestaat. Dit wil natuurlijk zeggen dat er een opeenvolging van toppen en bogen $u = t_0, b_1, t_1, b_2, t_2, \ldots, b_k, t_k = v$ bestaat zodanig dat de boog b_i gericht is van t_{i-1} naar t_i en al zulke pijlen verschillend zijn.

Op een ongerichte graaf kunnen we ook een **afstand** definiëren. Voor $u, v \in V(\mathcal{G})$ stellen we $d(u, v)$ gelijk aan de lengte van de kortste wandeling van u naar v. Als er tussen u en v geen wandeling bestaat, schrijven we $d(u, v) = \infty$. We stellen ook voor elke top v dat $d(v, v) = 0$.

Eigenschap 15. *Voor een ongerichte graaf $\mathcal{G}$ geldt dat*

$$d\colon V(\mathcal{G}) \times V(\mathcal{G}) \longrightarrow \mathbb{N} \cup \{\infty\}\colon (u, v) \longmapsto d(u, v)$$

een metriek[1] *is.*

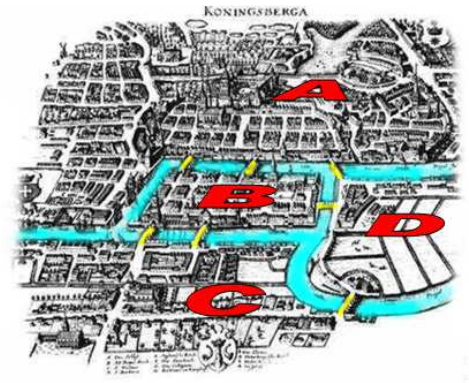
Bewijs. Het is duidelijk dat $d(u, v) = 0 \Leftrightarrow u = v$ en dat $d(u, v) = d(v, u)$ voor elk paar toppen $u, v \in V(\mathcal{G})$. Zij nu $u, v, w \in V(\mathcal{G})$ drie toppen met $d(u, v) = k$ en $d(v, w) = l$. Dit geeft een wandeling van u naar v en één van v naar w. Door deze na elkaar te volgen, krijgen we een wandeling van v naar w die lengte $k + l$ heeft. De afstand $d(u, w)$ zal dus ten hoogste $k + l$ bedragen. □

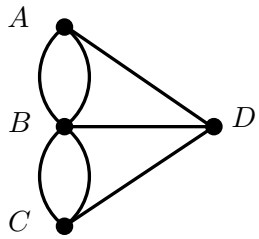
4.4 Bijzondere paden

4.4.1 Eulerpaden

Grafen werden uitgevonden door Leonhard Euler (1707–1783). Hij leefde op dat moment in Königsberg (nu Kaliningrad, Rusland) in Pruisen. De stad wordt in vier stukken verdeeld door de Pregel-rivier.

[1] Een metriek op een verzameling X is een afbeeling $\delta\colon X \times X \to \mathbb{R}^+$ die voldoet aan volgende drie eigenschappen: $\forall x \in X\colon \delta(x, x) = 0$; $\forall x, y \in X\colon \delta(x, y) = \delta(y, x)$ en $\forall x, y, z \in X\colon \delta(x, y) + \delta(y, z) \geqslant \delta(x, z)$.





Figuur 4.1: Een plattegrond van Königsberg ten tijde van Euler en daarnaast zijn grafische voorstelling.

Er zijn ook zeven bruggen over de rivier om de verschillende stadsgedeelten te verbinden. Op een dag was er een stoet die door de hele stad ging en Euler vroeg zich af of er een wandeling bestond voor de stoet zodanig dat elke brug juist één maal overgestoken werd en bovendien de wandeling terug zou komen naar het startpunt.

Euler stelde het probleem grafisch voor (zie Figuur 4.1) met zeven bogen en vier toppen, welke overeenkomen met de zeven bruggen en de vier stadsgedeelten. Het resultaat is geen graaf aangezien er "dubbele" bogen zijn en in een relatie komen de koppels immers hoogstens één keer voor.

Definitie 22. *Een* ***multigraf*** *is een graaf* $\mathcal{G} = (V, \to)$ *uitgebreid door middel van een functie* $\mu\colon V \times V \longrightarrow \mathbb{N}$ *die een* ***multipliciteit*** *toekent aan elke pijl. We interpreteren de functie* μ *als volgt:*

- $\mu(u, v) = 0$ *betekent dat* u *en* v *niet adjacent zijn;*
- $\mu(u, v) = k > 0$ *betekent dat er* k *pijlen zijn van* u *naar* v*.*

Pijlen die hetzelfde begin- en eindpunt hebben worden ***parallel*** *genoemd.*

Een multigraaf zonder parallelle pijlen is een graaf.

Oefening. Vertaal alle tot nu toe gedefinieerde begrippen (ongericht, boog, graad, wandeling, pad, samenhang, ...) voor multigrafen.

Definitie 23. *Een pad in een ongerichte multigraaf* $\mathcal{G}$ *heet een* ***Eulerpad*** *indien het elke boog van* $\mathcal{G}$ *precies één maal bevat. Een gesloten Eulerpad is*

*een **Eulercyclus**. Een multigraaf die een Eulercyclus bevat heet een **Eulergraaf**.*

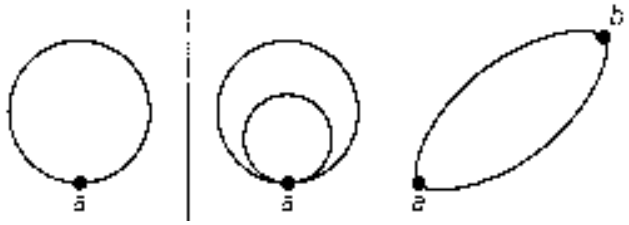
Stelling 30 (Euler, 1736)**.** *Zij $\mathcal{G}$ een ongerichte multigraaf zonder geïsoleerde toppen. Dan geldt dat $\mathcal{G}$ een Eulergraaf is **als en slechts als** $\mathcal{G}$ samenhangend is en alle toppen van $\mathcal{G}$ even graad hebben.*

Bewijs. $\boxed{\Rightarrow}$ Omdat $\mathcal{G}$ een Eulercyclus heeft, bestaat er $\forall a, b \in V$ een pad van a naar b, namelijk dat deel van de cyclus dat start in a en aankomt in b. Dus $\mathcal{G}$ is samenhangend.

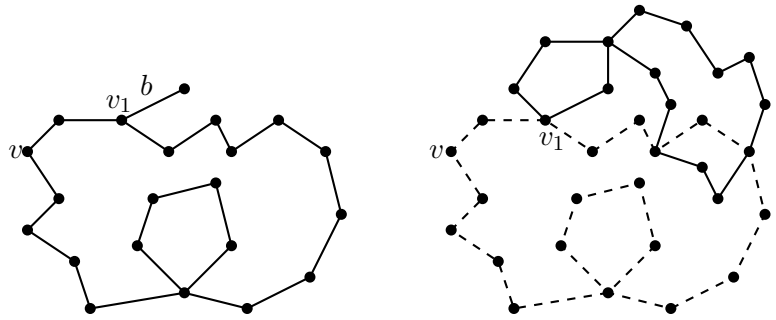
Kies een willekeurige top v in $\mathcal{G}$. Als we de Eulercyclus volgen, passeren we mogelijks verschillende keren in v. Elke doorgang in v gebruikt twee bogen: één om binnen te komen en één om terug buiten te gaan. Ook doorlopen we elke boog die v bevat juist één keer zodat $\deg(v)$ gelijk is aan tweemaal het aantal keer dat we in v komen, wat een even getal is.

$\boxed{\Leftarrow}$ We moeten een Eulercyclus construeren.

Als het aantal bogen in $\mathcal{G}$ 1 of 2 is, dan ziet $\mathcal{G}$ er als volgt uit:



We gaan nu verder per inductie en onderstellen dat het resultaat waar is wanneer er minder dan n bogen zijn. Wanneer $\mathcal{G}$ n bogen heeft, neem dan v een willekeurige top. Kies een boog die v bevat. Die heeft een ander uiteinde u. Kies nu een boog die u bevat, maar niet de boog die je juist gebruikte om uit v te vertrekken. Blijf zo bogen toevoegen, zonder tweemaal dezelfde te gebruiken. Doordat de graad van elke top even is, kunnen we steeds verder (telkens we in een top binnenkomen, is er nog een ongebruikte boog om buiten te gaan). Doe dit tot we terug in v aankomen, dan hebben we een gesloten pad P gemaakt dat vertrekt en aankomt in v en geen enkele boog tweemaal gebruikt. Als alle bogen van $\mathcal{G}$ tot P behoren, hebben we een Eulercyclus.



Als er nog bogen zijn die niet tot P behoren, moet er, wegens de samenhang van $\mathcal{G}$, een boog b bestaan die niet tot P behoort, maar wel een top v_1 van P bevat. Laten we nu alle bogen van P weg uit de graaf $\mathcal{G}$, dan houden we een graaf $\mathcal{G}'$ over waarin alle toppen nog steeds even graad hebben (we lieten per top een even aantal bogen weg). Misschien is $\mathcal{G}'$ niet samenhangend, maar dan beschouwen we de samenhangscomponent die v_1 bevat. Deze bevat een Eulercyclus P_1. Hetzelfde geldt voor alle resterende samenhangscomponenten. Zo krijgen we verschillende paden P_i in $\mathcal{G}$ die geen boog gemeenschappelijk hebben met P, maar wel allen een top v_i op P hebben. We kunnen alle paden combineren door in v te beginnen, het pad P te volgen tot in v_1, dan het pad P_1 te nemen tot we weer in v_1 komen, waar we weer het pad P volgen tot in v_2 waar we P_2 volgen, enzovoort. Omdat $\mathcal{G}$ eindig is, stopt het proces en bekomen we een Eulercyclus voor $\mathcal{G}$. □

Gevolg 9. *Een samenhangende ongerichte multigraaf $\mathcal{G}$ heeft een Eulerpad dat niet gesloten is* ***als en slechts als*** *$\mathcal{G}$ juist twee toppen heeft van oneven graad.*

Bewijs. $\boxed{\Rightarrow}$ Zij u en v de begin- en eindtop van het Eulerpad. De eerste boog van het pad geeft een bijdrage 1 tot de graad van u. Telkens het pad weer langs u gaat, neemt de graad met 2 toe. Dus zal de graad van u in het totaal oneven zijn. Analoog zal de graad van v oneven zijn omdat de laatste boog van het pad de graad met 1 laat toenemen. Alle overige toppen hebben duidelijk even graad.

$\boxed{\Leftarrow}$ Zij u en v de twee toppen met oneven graad. Voeg aan $\mathcal{G}$ de boog $\{u, v\}$ toe. Dan heeft elke top even graad en is vorige stelling van toepassing. We krijgen dus een gesloten Eulerpad. Als we hierin de boog $\{u, v\}$ weglaten, hebben we een Eulerpad in $\mathcal{G}$. □

4.4.2 Hamiltonpaden

William Rowan Hamilton (1805–1865) was een Iers wiskundige en vond in 1857 een spel uit. Op de toppen van een dodecaëder (regelmatig twaalfvlak) werden de namen van grote steden in de wereld aangebracht. Dan moest men een "reis rond de wereld" vinden die elke stad juist één keer bezoekt en enkel de ribben van de dodecaëder gebruikt als verbindingswegen tussen de steden.

Definitie 24. *Een simpel pad dat alle toppen van een multigraaf $\mathcal{G}$ bevat heet een **Hamiltonpad**. Een **Hamiltoncyclus** is een gesloten Hamiltonpad. Een multigraaf die een Hamiltoncyclus bevat heet een **Hamiltongraaf**.*

Lemma 4. *Als je k toppen uit een Hamiltongraaf $\mathcal{G}$ weglaat, samen met de aangrenzende bogen, dan valt $\mathcal{G}$ uiteen in hoogstens k samenhangscomponenten.*

Bewijs. Zij $\mathcal{H}$ een Hamiltoncyclus in $\mathcal{G}$. Noem de grafen die uit $\mathcal{G}$ en $\mathcal{H}$ respectievelijk ontstaan door weglaten van k toppen resp. $\mathcal{G}'$ en $\mathcal{H}'$. Voor $\mathcal{H}$ is de bewering zeker waar omdat $\mathcal{H}$ een cyclus is (en die valt uiteen in hoogstens k componenten). Maar $\mathcal{G}'$ bevat meer bogen dan $\mathcal{H}'$. Dus kan het aantal samenhangscomponenten van $\mathcal{G}'$ niet groter zijn dan dat van $\mathcal{H}'$. □

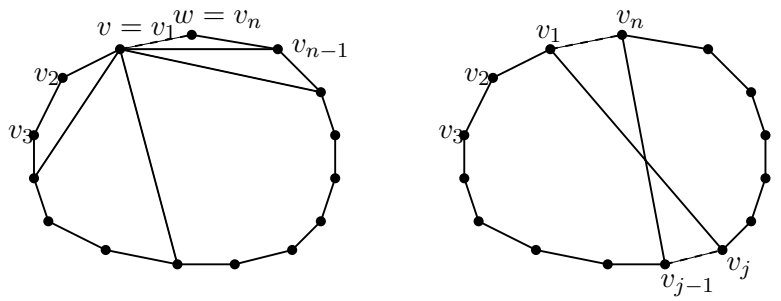
Stelling 31. *Zij $\mathcal{G}$ een multigraaf waarbij het verwijderen van n toppen leidt tot $m > n$ samenhangscomponenten, dan is $\mathcal{G}$ geen Hamiltongraaf.*

Stelling 32 (Dirac, 1952)**.** *Zij $\mathcal{G}$ een ongerichte simpele graaf met $n \geqslant 3$ toppen. Als alle toppen van $\mathcal{G}$ minstens graad $\frac{n}{2}$ hebben, dan heeft $\mathcal{G}$ een Hamiltoncyclus.*

Bewijs. Uit het ongerijmde.

Als de bewering uit de stelling onwaar is, moet er minstens één tegenvoorbeeld bestaan. Zij $\mathcal{G}'$ zo een tegenvoorbeeld met n toppen. Dus geldt voor elke $v \in V(\mathcal{G}')$ dat $\deg(v) \geqslant \frac{n}{2}$, maar er is geen Hamiltoncyclus. Voeg aan $\mathcal{G}'$ zoveel mogelijk bogen toe (door toppen te verbinden die niet adjacent zijn in $\mathcal{G}'$) zonder een Hamiltoncyclus te vormen. Noem deze graaf $\mathcal{G}$. Vermits er geen Hamiltoncyclus is in $\mathcal{G}$, is $\mathcal{G}$ zeker niet de complete graaf. Er moeten dus twee toppen v en w bestaan die niet verbonden zijn in $\mathcal{G}$. Vanwege de constructie van $\mathcal{G}$ zou het toevoegen van de boog $\{v, w\}$ een Hamiltoncyclus doen ontstaan. Dus bevat $\mathcal{G}$ een Hamiltonpad $v = v_1 \sim v_2 \sim \cdots \sim v_n = w$.

Figuur 4.2: "Reis rond de wereld" spel met een oplossing



Bekijk de verzameling $\mathcal{G}_v$ van buren van v. Deze heeft minstens $\frac{n}{2}$ elementen. Dan bekijken we de verzameling van opvolgers van een buur van w op het Hamiltonpad. Dus

$$S' := \{v_{i+1} \mid v_i \in \mathcal{G}_w\}.$$

We hebben zeker $w \in S'$ en stellen daarom $S := S' \setminus \{w\}$. Er geldt dan $|S| \geqslant \frac{n}{2} - 1$. De verzamelingen $\mathcal{G}_v$ en S zijn deelverzamelingen van $\{v_2, v_3, \ldots, v_{n-1}\}$ vermits v en w niet adjacent zijn.

De duiventil leert ons dat $|S \cap \mathcal{G}_v| \geqslant 1$. Dus bestaat er een top v_j met $v_j \sim v$ en $v_j \in S$, wat betekent dat $w = v_n \sim v_{j-1} \sim v_j$. Neem nu het pad $v = v_1 \sim v_j \sim v_{j+1} \sim \cdots \sim v_n \sim v_{j-1} \sim v_{j-2} \sim \cdots \sim v_1$. Dit is een Hamiltoncyclus, tegenspraak. □

4.4.3 Gerichte grafen

We hebben Euler- en Hamiltonpaden bestudeerd in ongerichte grafen. Bestaan er analoge begrippen of stellingen voor gerichte grafen?

Definitie 25. *Een gerichte (multi)graaf heet een **gerichte Eulergraaf** indien er een gesloten gericht pad is dat elke pijl juist één keer gebruikt.*

Stelling 33. *Een samenhangende gerichte (multi)graaf $\mathcal{G}$ is een gerichte Eulergraaf **als en slechts als** $\mathcal{G}$ sterk samenhangend en gebalanceerd is.*

Bewijs. $\boxed{\Rightarrow}$ Als er een Eulercyclus bestaat in $\mathcal{G}$ is het duidelijk dat dat de graaf gebalanceerd moet zijn omdat de cyclus in elke top evenveel moet binnenkomen als buitengaan. De Eulercyclus zorgt er ook voor dat er tussen elke twee toppen een gericht pad bestaat.

$\boxed{\Leftarrow}$ Je kan gewoon het ongerichte bewijs van Stelling 30 aanpassen. Doe dit zelf! □

Hamiltoncyclussen in gerichte grafen (dus gerichte cycli die elke top juist één keer bezoeken) zijn wat moeilijker. Hier beperken we ons tot een bijzondere soort gerichte grafen.

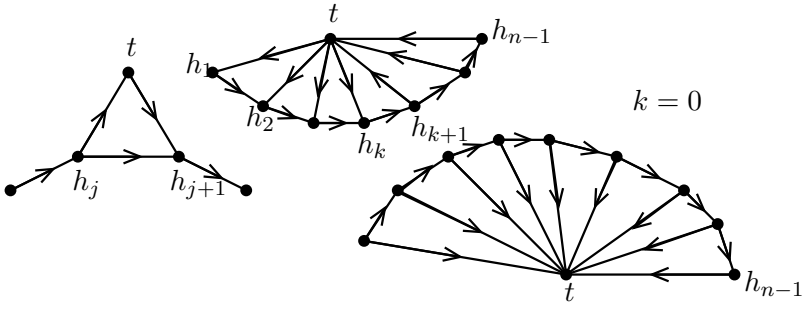
Een toernooi (bijvoorbeeld een schaaktoernooi, voetbaltoernooi, ...) kan aan de hand van een gerichte graaf gemodelleerd worden. We trekken een pijl van speler (of ploeg) u naar speler v indien u gewonnen heeft van v. Als iedereen tegen iedereen speelt, hebben we dus een complete graaf waar elke boog een oriëntatie krijgt.

Definitie 26. *Een **toernooi** is een gerichte simpele graaf die ontstaat door alle bogen van een complete graaf te oriënteren.*

Stelling 34. *Elk toernooi heeft een gericht Hamiltonpad.*

Bewijs. Bij inductie op n, het aantal toppen in het toernooi $\mathcal{T}$.

Als $n = 1$ of $n = 2$ is de stelling duidelijk waar. Onderstel nu dat de stelling geldt voor alle toernooien met $n - 1$ toppen. Kies een willekeurige top t en stel $\mathcal{T}'$ gelijk aan de graaf die ontstaat als je t en alle bogen waartoe t behoort verwijdert uit $\mathcal{T}$. Deze $\mathcal{T}'$ is een toernooi met $n-1$ toppen en heeft dus een Hamiltonpad $h_1 \to h_2 \to \cdots \to h_{n-1}$ wegens de inductiehypothese. Als er nu een $j \in [n-2]$ bestaat met $h_j \to t \to h_{j+1}$, dan is $h_1 \to h_2 \to \cdots \to h_j \to t \to h_{j+1} \to \cdots \to h_{n-1}$ een Hamiltonpad in $\mathcal{T}$. Als er zo geen j bestaat, dan is er zeker een $k \in \{0, 1, \ldots, n-1\}$ met $\forall j \leqslant k\colon t \to h_j$ en $\forall j > k\colon t \leftarrow h_j$. Maar dan is $t \to h_1$ (indien $k \neq 0$) een boog die een Hamiltonpad $t \to h_1 \to h_2 \to \cdots$ toelaat. In het geval $k = 0$ kunnen we t op het einde toevoegen: $h_1 \to h_2 \to \cdots \to h_{n-1} \to t$.

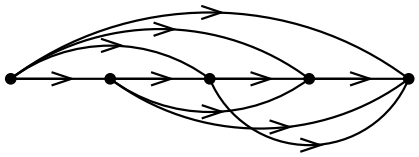


□

Stelling 35. *Een toernooi $\mathcal{T}$ heeft een gerichte Hamiltoncyclus **als en slechts als** $\mathcal{T}$ sterk samenhangend is.*

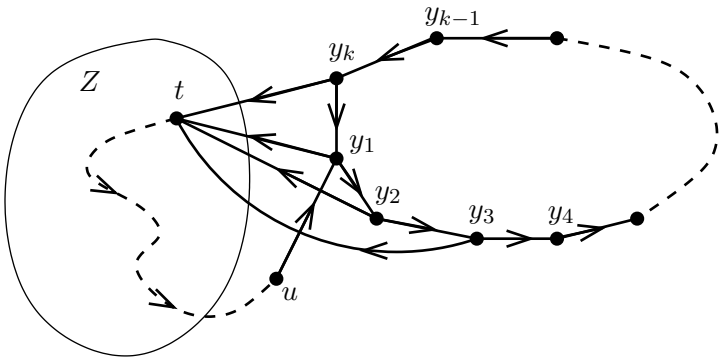
Bewijs. $\boxed{\Rightarrow}$ Als $\mathcal{T}$ een Hamiltoncyclus heeft, dan levert deze een gericht pad tussen elke twee toppen.

$\boxed{\Leftarrow}$ Onderstel dat $\mathcal{T}$ sterk samenhangend is. We bewijzen eerst dat $\mathcal{T}$ een gerichte cyclus bevat. Dit doen we uit het ongerijmde. Als $\mathcal{T}$ geen cyclus bevat dan geldt $\forall x, y, z \in \mathcal{T}\colon (x \to y \text{ en } y \to z) \Rightarrow x \to z$. Dan heet $\mathcal{T}$ een **transitief toernooi**. In zulk een toernooi kan je de punten van links naar rechts rangschikken zodat alle pijlen naar rechts wijzen. Zulk toernooi is duidelijk niet sterk samenhangend omdat er geen pad van rechts naar links gaat, tegenspraak.



Dus hebben we een cyclus $C = y_1 \to y_2 \to \cdots \to y_k \to y_1$. We veronderstellen dat hij maximale lengte heeft in $\mathcal{T}$ en toch geen Hamiltoncyclus is. Vermits $\mathcal{T}$ sterk samenhangend is, moet er een top t buiten C zijn die verbonden is met een top in C. Zonder de algemeenheid te schaden mogen we ervan uitgaan dat $y_1 \to t$ een pijl is. Als $t \to y_2$, zou $y_1 \to t \to y_2 \to y_3 \to \cdots$ een langere cyclus geven, tegenspraak. Dus moet de boog tussen t en y_2 anders gericht zijn: $y_2 \to t$. Analoog moet $\forall i \in [k]\colon y_i \to t$.

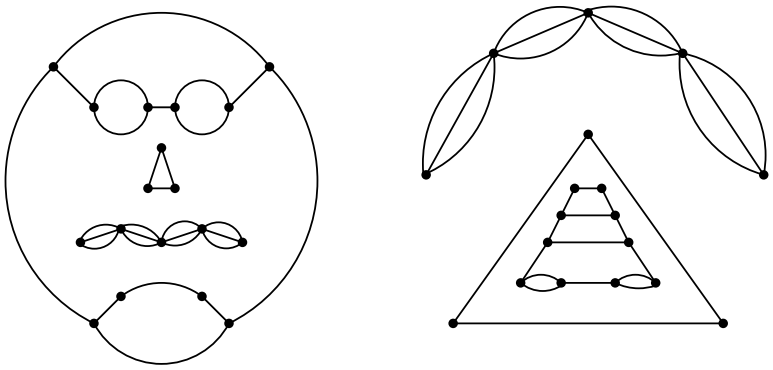
Stel nu even $Z := \{z \in V(\mathcal{T}) \setminus \{y_2\} \mid y_1 \to z\}$. Dan geldt, analoog aan voorgaande redenering, dat $\forall z \in Z\colon \forall i \in [k]\colon y_i \to z$. Maar vermits $\mathcal{T}$ sterk samenhangend is, moet er een pad van t naar y_1 bestaan. Dit pad moet minstens één top u buiten Z bevatten omdat je vanuit Z nooit (rechtstreeks) verbonden bent met y_1. Maar een top buiten Z is, door de definitie van Z en van toernooi, onmiddellijk verbonden met y_1 zodat $t \to \cdots \to u \to y_1 \to y_2 \to \cdots \to y_k \to t$ een cyclus is die langer is (minstens twee toppen meer) dan C. Dit is een tegenspraak. □



4.5 Isomorfismen tussen grafen

De wiskunde houdt zich bezig met de studie van bepaalde objecten en de relaties ertussen. Die objecten zijn meestal verzamelingen met een bijkomende structuur (een bewerking, meerdere bewerkingen, een verzameling van bogen, ...). Van fundamenteel belang zijn hierbij de afbeeldingen die een gegeven structuur bewaren. Dit zijn de zogenaamde *morfismen*. Wij bekijken nu het geval waar de objecten in kwestie grafen zijn.

Definitie 27. *Zij* (V, μ) *en* (W, φ) *twee multigrafen. Een afbeelding* $f : V \longrightarrow W$ *heet een* ***morfisme*** *indien zij voldoet aan* $\forall (u, v) \in V \times V$ *geldt dat* $\varphi(f(u), f(v)) = \mu(u, v)$.



Soms kan eenzelfde graaf op verschillende manieren getekend worden. Wanneer we bijvoorbeeld alle ongerichte simpele grafen met 6 toppen willen bepalen (doe dat eens!) door ze op een blad papier te tekenen, zal het snel gebeuren dat we eigenlijk twee keer dezelfde graaf tekenen, zonder dat te merken. Als we dus willen weten hoeveel "echt verschillende" grafen er zijn op 6 toppen, moeten we zeer voorzichtig te werk gaan. We preciseren nu wiskundig wanneer twee grafen eigenlijk dezelfde zijn.

Definitie 28. *Twee multigrafen* (V, μ) *en* (W, φ) *zijn* ***isomorf*** *als er een bijectief morfisme* $V \longrightarrow W$ *bestaat. Zulk een morfisme heet dan ook een* ***isomorfisme*** *tussen* (V, μ) *en* (W, φ).

Voor twee ongerichte simpele grafen $\mathcal{G} = (V, \sim_{\mathcal{G}})$ en $\mathcal{H} = (W, \sim_{\mathcal{H}})$ hebben we dus dat een isomorfisme een bijectie f is tussen de toppenverzamelingen V en W zodanig dat voor elk paar toppen $u, v \in V$ geldt $u \sim_{\mathcal{G}} v \Leftrightarrow f(u) \sim_{\mathcal{H}} f(v)$.
Notatie. Als twee grafen $\mathcal{G}$ en $\mathcal{H}$ isomorf zijn, noteren we $\mathcal{G} \cong \mathcal{H}$.

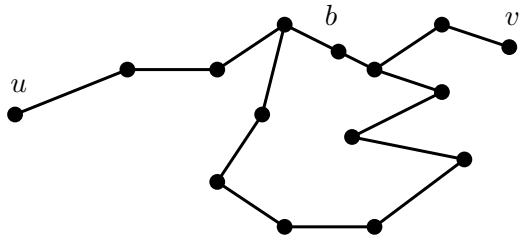
4.6 Bomen en bossen

Stelling 36. *Zij $\mathcal{G}$ een samenhangende simpele graaf. Dan zijn volgende twee eigenschappen equivalent*

*(1) $\mathcal{G}$ is **minimaal samenhangend***
(d.w.z. dat als je een boog weglaat, $\mathcal{G}$ niet meer samenhangend is)

(2) $\mathcal{G}$ heeft geen cyclus

Bewijs. $\boxed{(1) \Rightarrow (2)}$ Als $\mathcal{G}$ minimaal samenhangend is en toch een cyclus zou bevatten, dan kan je een boog b van deze cyclus weglaten zonder de samenhang te verliezen. Inderdaad: zij u en v toppen van $\mathcal{G}$. Ofwel was u met v verbonden via een pad dat b niet bevat en dan blijven ze verbonden. Indien het pad wel de boog b bevatte, kunnen we een nieuw pad maken door de rest van de cyclus te volgen, wat tot een tegenspraak leidt.



$\boxed{(2) \Rightarrow (1)}$ Bij contrapositie: $\neg(1) \Rightarrow \neg(2)$.
Onderstel dat $\mathcal{G}$ niet minimaal samenhangend is. Dan is er een boog $b = \{u, v\}$ die we niet nodig hebben voor de samenhang. Dus is er in de graaf $\mathcal{G}'$ die ontstaat uit $\mathcal{G}$ door het weglaten van de boog b, een pad van u naar v. Samen met b vormt dit pad een cyclus in $\mathcal{G}$. □

Definitie 29. *Een samenhangende ongerichte simpele graaf zonder cyclus noemen we een **boom**.*

Gevolg 10. *Een samenhangende ongerichte graaf is een boom **als en slechts als** elke twee toppen verbonden zijn door juist één pad.*

Bewijs. $\boxed{\Leftarrow}$ Als er voor elke twee toppen juist één verbinding is, is de graaf in kwestie minimaal samenhangend. Inderdaad: als je na het verwijderen van een boog $b = \{u, v\}$ nog een samenhangende graaf zou hebben, zou er buiten de boog b nog een pad van u naar v zijn, tegenspraak.

$\boxed{\Rightarrow}$ Zij $\mathcal{H}$ een boom en veronderstel dat er twee paden zijn tussen twee toppen u en v. Neem dan de stukken van die paden die niet samenvallen. Dit zijn cycli, tegenspraak.

□

Een beetje "experimenteren" met bomen toont ons snel dat er een verband is tussen het aantal toppen en het aantal bogen. We bewijzen de stelling na een kort lemma over bladeren.

Definitie 30. *Een top van graad* 1 *in een boom heet een* ***blad****.*

Lemma 5. *Een boom op* $n \geqslant 2$ *toppen heeft minstens twee bladeren.*

Bewijs. Neem een top t van de boom. Dan zijn er twee mogelijkheden:
$\boxed{t \text{ is geen blad}}$ Wandel dan vanuit t naar een buur, dan nog een buur, enz. zonder ooit een top tweemaal te bezoeken. Omdat de boom eindig is, stopt dit in een zekere top s. Dit moet een blad zijn, want als het proces gestopt zou zijn omdat s meerdere buren zou hebben die reeds eerder bezocht werden, betekent dit dat er meerdere paden van t naar s zijn, tegenspraak.

Om het tweede blad te vinden gebruiken we dat t geen blad is en dus $\deg(t) > 1$ zodat we vanuit t nog een wandeling kunnen maken op zoek naar een ander blad.
$\boxed{t \text{ is een blad}}$ Neem dan de enige buur van t in plaats van t. Deze top heeft graad $\geqslant 2$ tenzij de boom bestaat uit twee toppen die één boog vormen. Maar in dit geval geldt het lemma duidelijk. □

Stelling 37. *Een boom met* n *toppen heeft* $n - 1$ *bogen.*

Bewijs. Per inductie op n.

Voor $n = 1$ is de stelling duidelijk voldaan.

Onderstel dat de stelling waar is voor n toppen en zij $\mathcal{T}$ een boom met $n + 1$ toppen. Het lemma verzekert ons het bestaan van een blad t. Uit $\mathcal{T}$ laten we t samen met de unieke boog op t weg. Dit levert een graaf $\mathcal{T}'$ op die een boom is met n toppen en één boog minder dan $\mathcal{T}$. Deze heeft wegens de inductiehypothese $n - 1$ bogen. □

Definitie 31. *Wanneer* $\mathcal{G}$ *een gerichte graaf is, dan wordt* $\mathcal{G}$ *een* ***gerichte boom*** *genoemd als de ongerichte graaf geassocieerd met* $\mathcal{G}$ *een boom is.*

Een gerichte boom noemen we een ***gewortelde boom*** *als er een unieke top* t *is waarvoor de ingraad nul is en alle andere toppen ingraad één hebben. We noteren* $(\mathcal{G}, t)$*.*

We kunnen elke ongerichte boom wortelen door een willekeurige top als **wortel** te kiezen waardoor alle bogen een natuurlijke oriëntatie krijgen weg van die wortel.

Definitie 32. *Een **bos** is een ongerichte simpele graaf zonder cyclus.*

*Een **geworteld bos** is een bos waarin elke samenhangscomponent geworteld is.*

Opmerking. De samenhangscomponenten van een bos zijn dus bomen.

Eigenschap 16. *Zij $\mathcal{F}$ een bos met n toppen en k samenhangscomponenten. Dan heeft $\mathcal{F}$ juist $n-k$ bogen.*

Bewijs. We hebben k bomen met respectievelijk $n_1, n_2, \ldots, n_k$ toppen. Die hebben dus elk $n_i - 1$ bogen zodat het totaal aantal bogen $n_1 - 1 + n_2 - 1 + \cdots + n_k - 1 = (\sum_{i=1}^{k} n_i) - k = n - k$. □

Het aantal niet-isomorfe bomen tellen op n toppen is nogal moeilijk. Het aantal *genummerde bomen* tellen daarentegen is niet zo moeilijk.

Definitie 33. *Een **genummerde (of gelabelde) boom** is een boom met als toppenverzameling $[n]$ voor $n \in \mathbb{N} \setminus \{0,1\}$.*

Stelling 38 (Cayley)**.** *Voor elke $n \in \mathbb{N} \setminus \{0,1\}$ is het aantal genummerde bomen met n toppen gelijk aan n^{n-2}.*

Bewijs. Gegeven een boom met n toppen, dan kan je daarin twee (niet noodzakelijk verschillende) toppen als wortel kiezen (we noemen de boom **dubbel geworteld**). Er zijn dus n^2 manieren om de gegeven boom dubbel te wortelen. Als we t_n gelijk stellen aan het aantal genummerde bomen met n toppen, hebben we $n^2 t_n$ dubbel gewortelde genummerde bomen op n toppen.

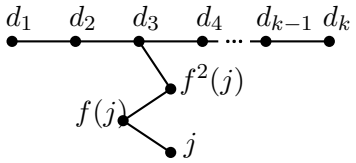
We tonen nu dat het aantal dubbel gewortelde bomen n^n bedraagt. Dit doen we door een bijectie te maken tussen die dubbel gewortelde bomen en de verzameling functies van $[n]$ naar $[n]$.

Zij $f\colon [n] \longrightarrow [n]$ een afbeelding en stel

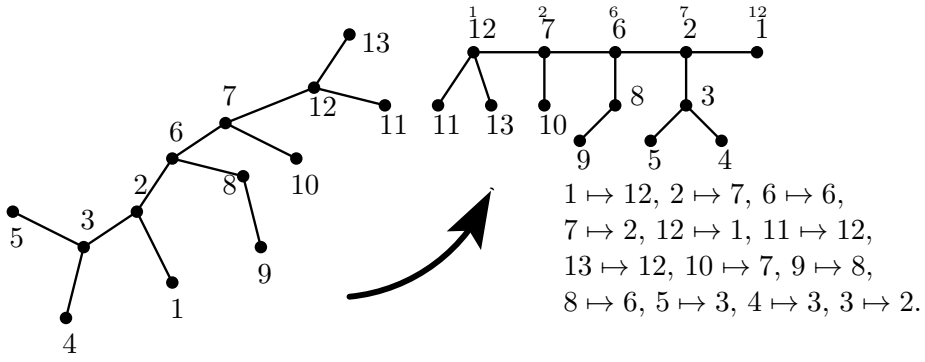
$$C := \{x \in [n] \mid \exists i \in \mathbb{N}_0\colon f^i(x) = x\},$$

welke we de *cyclische punten* van f noemen. We ordenen $C = \{c_1, c_2, \ldots, c_k\}$ zó dat $c_1 < c_2 < \cdots < c_k$. Stel nu voor elke $j \in [k]\colon d_j := f(c_j)$. Schrijf nu de getallen d_i naast de toppen van een pad P_k van lengte k. We nemen d_1

als eerste wortel en d_k als tweede. Voor $j \notin C$ maken we bogen $j \sim f(j)$. Dit geeft een dubbel gewortelde genummerde boom. Inderdaad: als we f verschillende keren laten inwerken op $j \notin C$, komen we uiteindelijk in een cyclisch punt terecht. Het pad $d_1 \sim d_2 \sim \cdots \sim d_k$ verzekert de samenhang zonder dat er cyclussen komen omdat deze van cyclische punten zouden komen en we hebben er juist voor gezorgd dat die in de graaf geen cyclus vormen.



Omgekeerd: een dubbel gewortelde genummerde boom tekenen we zó dat het pad tussen de twee wortels mooi recht ligt (dit zal overeenkomen met het pad P_k van hierboven). Voor j niet op dat rechte pad, stel je dan $f(j)$ gelijk aan de eerste buur van j op het unieke pad van j naar een top van het rechte pad. Op het rechte pad definiëren we het beeld van de i-de (te beginnen met de kleinste) top als die die op de i-de plaats staat op het rechte pad (te beginnen met de "linkse" wortel die nummer 1 krijgt).



□

Gevolg 11. *Het aantal gewortelde genummerde bomen op n toppen is n^{n-1}.*

Gevolg 12. *Het aantal gewortelde genummerde bossen op n toppen is $(n+1)^{n-1}$.*

Bewijs. Voeg een top toe aan het bos en verbind die met alle wortels van de resp. bomen. Nu hebben we een genummerde boom op $n+1$ toppen.

(Dit gaat ook omgekeerd: vertrek van een genummerde boom met $n+1$ toppen en neem top nummer 1 weg. Alle buren van deze top maak je

wortel van de samenhangscomponenten die overblijven. Dus is het aantal gewortelde genummerde bossen juist $(n+1)^{(n+1)-2} = (n+1)^{n-1}$). □

4.6.1 Opspannende bomen

Veronderstel dat we een netwerk moeten maken dat verschillende steden verbindt. Het netwerk moet zo zijn dat iedereen met iedereen in verbinding staat (eventueel met tussenstations). Een naïeve oplossing zou zijn om alle steden met elkaar te verbinden (een complete graaf), maar als we ook nog rekening moeten houden met de kostprijs van de verbindingen, moeten we anders te werk gaan.

Definitie 34. *Zij $\mathcal{G}$ een graaf en $w : E(\mathcal{G}) \longrightarrow \mathbb{R}^+$ een functie die aan elke pijl een **prijs** of **gewicht** toekent en welke we een **gewichtsfunctie** noemen. Een graaf samen met een gewichtsfunctie heet een **gewogen graaf**.*

Wat we meestal zoeken, is een opspannende deelgraaf met minimaal gewicht in een ongerichte graaf $\mathcal{G}$. Dit betekent dat de som van de gewichten van de pijlen van de opspannende deelgraaf minimaal is. Deze is zeker een boom omdat hij minimaal samenhangend moet zijn. We geven een algoritme.

Gierigheidsalgoritme (Kruskal).
Om een opspannende boom $\mathcal{T}$ van minimaal gewicht te vinden in een gewogen samenhangende ongerichte simpele graaf $(\mathcal{G}, w)$:

1. Neem een boog met kleinste gewicht om $\mathcal{T}$ te starten;
2. Neem een boog met kleinste gewicht in $\mathcal{G}$ die nog niet tot $\mathcal{T}$ behoort en geen cyclus creëert als je hem aan $\mathcal{T}$ toevoegt.
3. Ga naar (2) tot $\mathcal{T}$ een opspannende boom is.

Geeft dit algoritme nu de opspannende boom met het kleinste gewicht? Om hierop te antwoorden geven we eerst een lemma.

Lemma 6. *Zij $\mathcal{F}$ en $\mathcal{F}'$ twee bossen op dezelfde toppenverzameling en onderstel dat $\mathcal{F}$ minder bogen heeft dan $\mathcal{F}'$. Dan heeft $\mathcal{F}'$ een boog b die we kunnen toevoegen aan $\mathcal{F}$ zodanig dat $\mathcal{F} \cup \{b\}$ nog steeds een bos is.*

Bewijs. Uit het ongerijmde: onderstel dat er zo geen boog is. Dus om het even welke boog van $\mathcal{F}'$ je toevoegt aan $\mathcal{F}$, je verkrijgt telkens weer een cyclus. Dus alle bogen van $\mathcal{F}'$ verbinden toppen van eenzelfde samenhangscomponent van $\mathcal{F}$. Dan moet $\mathcal{F}'$ minstens evenveel componenten hebben

als $\mathcal{F}$. Als het aantal samenhangscomponenten van $\mathcal{F}$ gelijk is aan k, weten we dat $\mathcal{F}$ juist $n-k$ bogen heeft. Maar gegeven was dat $\mathcal{F}'$ *meer* bogen heeft dan $\mathcal{F}$, tegenspraak. □

Stelling 39. *Het gierigheidsalgoritme vindt steeds een opspannende boom met minimaal gewicht.*

Bewijs. Noem het resultaat van het gierigheidsalgoritme $\mathcal{T}$ en onderstel dat de graaf $\mathcal{G}$ een lichtere opspannende boom $\mathcal{H}$ heeft. Orden de bogen van $\mathcal{H}$ zó dat $w(h_1) \leqslant w(h_2) \leqslant \cdots \leqslant w(h_{n-1})$. We doen hetzelfde voor $\mathcal{T}$ zodat $w(t_1) \leqslant w(t_2) \leqslant \cdots \leqslant w(t_{n-1})$. Vermits het gierigheidsalgoritme begint met de allerlichtste boog, moet gelden

$$w(t_1) \leqslant w(h_1)$$

Zij i de eerste index waar $\mathcal{H}$ lichter wordt dan $\mathcal{T}$. Dus i is het kleinste getal zodat

$$\sum_{j=1}^{i} w(h_j) < \sum_{j=1}^{i} w(t_j)$$

Door onze veronderstelling bestaat zulke $i > 1$. Vermits i de eerste index is waar $\mathcal{H}$ lichter wordt, geldt zeker $w(h_i) < w(t_i)$ en ook

$$\sum_{j=1}^{i-1} w(h_j) \geqslant \sum_{j=1}^{i-1} w(t_j)$$

Stel $\mathcal{T}_{i-1}$ gelijk aan het bos dat geleverd wordt door het gierigheidsalgoritme na $i-1$ stappen. Stel ook $\mathcal{H}_i$ gelijk aan het bos dat bestaat uit de bogen $h_1, h_2, \ldots, h_i$. Volgens voorgaand lemma kunnen we een boog van $\mathcal{H}_i$ toevoegen aan $\mathcal{T}_{i-1}$ zodanig dat het nog een bos blijft. Deze boog is een zekere h_j met $j \leqslant i$. Maar nu geldt

$$w(h_j) \leqslant w(h_i) < w(t_i)$$

Dit toont dat het gierigheidsalgoritme nooit t_i zou kiezen in de i-de stap, maar eerder h_j die lichter is, tegenspraak. □

Gerelateerd hiermee is het zeer gekende ***handelsreizigersprobleem*** (***traveling salesman problem***) binnen de computerwetenschappen en operationeel onderzoek, nl. als er n steden gegeven zijn die een handelsreiziger moet bezoeken, samen met de afstand tussen ieder paar van deze steden, vind dan de kortste weg die kan worden gebruikt, waarbij iedere stad juist één keer wordt bezocht en die eindigt bij het beginpunt. Hier zoeken we dan eigenlijk een Hamilton cyclus met minimaal gewicht.

4.6.2 Het tellen van opspannende bomen

Hiervoor definiëren we een matrix om de graaf voor te stellen.

Zij $\mathcal{G}$ een gerichte multigraaf zonder lussen (dus gerichte simpele graaf wanneer er geen parallelle pijlen zijn). Zij $V(\mathcal{G}) = \{v_1, v_2, \ldots, v_n\}$ en $E(\mathcal{G}) = \{b_1, b_2, \ldots, b_m\}$ nummeringen van de toppen en pijlen van $\mathcal{G}$. De **incidentiematrix** van $\mathcal{G}$ is de $(n \times m)$-matrix $B_\mathcal{G}$ met

$$\begin{cases} b_{ij} := 1 & \text{als } v_i \text{ het eindpunt is van } b_j \\ b_{ij} := -1 & \text{als } v_i \text{ het beginpunt is van } b_j \\ b_{ij} := 0 & \text{in alle andere gevallen} \end{cases}$$

We geven een ietwat spectaculaire stelling.

Stelling 40 (Kirchhoff)**.** *Zij $\mathcal{G}$ een gerichte multigraaf zonder lussen en zij B de incidentiematrix van $\mathcal{G}$. Stel B_0 gelijk aan de matrix die ontstaat na verwijdering van om het even welke rij van B. Het aantal opspannende bomen in $\mathcal{G}$ is dan gelijk aan* $\det B_0 B_0^\top$.

Bewijs. Door hernummering van de n toppen kan je er steeds voor zorgen dat de weggelaten rij de laatste is. Als $m < n-1$ kan $\mathcal{G}$ zeker niet samenhangend zijn en zijn er dus geen opspannende bomen. Neem C een willekeurige $(n-1 \times n-1)$-deelmatrix van B_0. We bewijzen nu dat $|\det C| = 1$ als en slechts als de deelgraaf $\mathcal{G}_C$ bepaald door de kolommen van C (dit zijn juist $n-1$ pijlen van $\mathcal{G}$) een opspannende boom is. Anders is $\det C = 0$. We doen dit per inductie op n.

De basisstap van de inductie is voor $n = 2$. Voor zulke kleine grafen is de stelling duidelijk waar.

Onderstel in een eerste geval dat er in $\mathcal{G}_C$ een top v_i is van graad (= in- + uitgraad) 1. Dit betekent dat de i-de rij van C juist één niet-nul element bevat (en dat element is ± 1). We kunnen $\det C$ ontwikkelen volgens de i-de rij. Nu kunnen we de inductiehypothese gebruiken, want de cofactor die we moeten uitrekenen is de determinant van de matrix die overeenkomt met de graaf $\mathcal{G}_C$ waar we v_i uit hebben weggelaten. We noteren deze graaf $\mathcal{G}_C - v_i$. Dit is duidelijk een opspannende boom van $\mathcal{G} - v_i$ als en slechts als $\mathcal{G}_C$ een opspannende boom was van $\mathcal{G}$.

Als er nu geen top is van graad 1 in $\mathcal{G}_C$ (behalve misschien v_n, de top die we weglieten in B_0), dan kan $\mathcal{G}_C$ geen boom zijn en nog minder een opspannende boom. Maar $\mathcal{G}_C$ heeft wel $n-1$ pijlen en $n-1$ toppen. Dus moet $\mathcal{G}_C$ een top van graad nul hebben. Als dit niet v_n, de top van de weggelaten rij, is, dan heeft C een nulle rij zodat $\det C = 0$. Als v_n de

geïsoleerde top is, bevat elke kolom van C een $+1$ en een -1. Bijgevolg is de som van alle rijen van C de nulrij zodat de rijen van C lineair afhankelijk zijn en $\det C = 0$.

Nu gebruiken we de formule van Cauchy-Binet (zie Appendix A) die zegt dat

$$\det B_0 B_0^\top = \sum_{C \text{ een } (n-1\times n-1)\text{-deelmatrix van } B_0} (\det C)^2.$$

Maar we weten dat $(\det C)^2 = 1$ of 0, naargelang de kolommen van C een opspannende boom bepalen of niet. □

Als de graaf ongericht is, hebben we een analoge stelling. We definiëren hiervoor eerst een andere matrix.

Zij $\mathcal{G}$ een ongerichte simpele graaf met genummerde toppen en bogen $\{v_1, v_2, \ldots, v_n\}$ en $\{b_1, b_2, \ldots, b_m\}$ respectievelijk. De **Laplaciaanse matrix** $L_\mathcal{G}$ is de $(n \times n)$-matrix met

$$\begin{cases} l_{ij} := \deg(v_i) & \text{als } i = j \\ l_{ij} := -1 & \text{als } i \neq j \text{ en } v_i \sim v_j \\ l_{ij} := 0 & \text{in alle andere gevallen} \end{cases}$$

Stelling 41. *Het aantal opspannende bomen in een ongerichte simpele graaf is gelijk aan elke cofactor van $L_\mathcal{G}$.*

Bewijs. We maken van $\mathcal{G}$ een gerichte graaf $\mathcal{H}$ door elke boog $u \sim v$ te vervangen door twee pijlen $u \to v$ en $u \leftarrow v$.

Zij B_0 de incidentiematrix van $\mathcal{H}$, met de laatste rij weggelaten. We bewijzen dat $B_0 B_0^\top = 2L_{0\mathcal{G}}$, waarbij deze laatste matrix ontstaat uit $L_\mathcal{G}$ door de laatste rij en laatste kolom weg te laten. Op plaats (i, j) van $B_0 B_0^\top$ staat het scalair product van de i-de en de j-de rij van B_0 i.e. $\sum_{k=1}^{m} b_{ik} b_{jk}$. Als $i = j$ zal elke pijl die in v_i vertrekt of aankomt een bijdrage 1 hebben in dit product. In totaal hebben we dus $2\deg(v_i)$ op plaats (i, i). Voor $i \neq j$ zal elke pijl $v_i \to v_j$ en elke pijl $v_i \leftarrow v_j$ een bijdrage -1 hebben. Dit geeft dus -2 of 0 op plaats (i, j), naargelang v_i en v_j adjacent zijn of niet.

Nu geldt dus dat $\det B_0 B_0^\top = \det 2L_{0\mathcal{G}} = 2^{n-1} \det L_{0\mathcal{G}}$. Maar elke opspannende boom van $\mathcal{G}$ geeft aanleiding tot 2^{n-1} opspannende bomen in $\mathcal{H}$ omdat er 2^{n-1} manieren zijn om de bogen te oriënteren. □

Toepassing. Het aantal opspannende bomen in een complete graaf K_n met genummerde toppen is n^{n-2}.

Dit volgt uit

$$L_{K_n} = \begin{pmatrix} n-1 & -1 & -1 & \cdots & -1 \\ -1 & n-1 & -1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \cdots & n-1 \end{pmatrix}$$

Dit geeft ons een alternatief bewijs van de stelling van Cayley.

4.6.3 Samenhang van een graaf bestuderen

Definitie 35. *Zij $\mathcal{G}$ een multigraaf van orde n met genummerde toppen. Definieer de **adjacentiematrix** $A_\mathcal{G}$ van $\mathcal{G}$ als de $(n \times n)$-matrix met a_{ij} gelijk aan het aantal pijlen van de i-de naar de j-de top. Een lus wordt tweemaal geteld in een ongerichte graaf en éénmaal in een gerichte.*

De adjacentiematrix bevat veel informatie over de graaf $\mathcal{G}$.

Stelling 42. *Zij $k > 0$. Het element op plaats (i, j) in de k-de macht $A^k_\mathcal{G}$ geeft het aantal (gerichte) wandelingen van lengte k van top i naar top j.*

Bewijs. Per inductie op k. Voor $k = 1$ tellen we wandelingen van lengte 1, dus pijlen. De definitie van $A_\mathcal{G}$ doet de rest.

Onderstel dat de stelling waar is voor de k-de macht. Zij l een top van $\mathcal{G}$. Als er b_{il} wandelingen zijn van lengte k van i tot l en a_{lj} wandelingen van lengte 1 (t.t.z. pijlen) van l naar j, dan zijn er $b_{il}a_{lj}$ wandelingen van lengte $k+1$ van i tot j die langs l gaan. Dus is het aantal wandelingen van lengte $k+1$ tussen i en j in totaal gelijk aan

$$\sum_{l \in V(\mathcal{G})} b_{il}a_{lj} =: c_{ij}$$

De inductiehypothese levert dat b_{il} het element is op plaats (i, l) in $A^k_\mathcal{G}$ zodat c_{ij} juist het element is op plaats (i, j) van het matrixproduct $A^k_\mathcal{G}A_\mathcal{G} = A^{k+1}_\mathcal{G}$. □

Stelling 43. *Zij $\mathcal{G}$ een ongerichte multigraaf op n toppen met adjacentiematrix $A_\mathcal{G}$. Dan is $\mathcal{G}$ samenhangend **als en slechts als** $(I_n + A_\mathcal{G})^{n-1}$ enkel strikt positieve elementen heeft.*

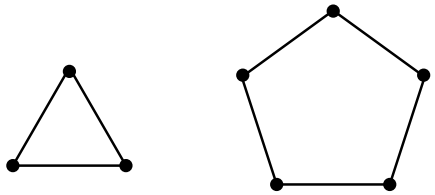
Bewijs. Merk op dat een pad tussen twee toppen van $\mathcal{G}$ ten hoogste $n-1$ bogen heeft. Dus is $\mathcal{G}$ samenhangend als en slechts als er $\forall i, j \in V(\mathcal{G})$ een $k \leqslant n-1$ is met een pad van lengte k van de i-de naar de j-de top. Dus $\forall i, j \in V(\mathcal{G})\colon \exists k < n\colon (A^k_\mathcal{G})_{ij} > 0$. Vermits $(I_n + A_\mathcal{G})^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} A^k_\mathcal{G}$, is de stelling bewezen. □

4.7 Bipartiete grafen

Definitie 36. *Een multigraaf heet **bipartiet** indien zijn toppenverzameling kan gepartitioneerd worden in twee delen zodat er geen enkele pijl is die toppen verbindt in hetzelfde deel.*

We kunnen de toppen van de graaf kleuren met twee kleuren zodat geen adjacente toppen dezelfde kleur hebben.

Het is eenvoudig na te gaan dat de driehoeksgraaf C_3 niet bipartiet is. Ook het pentagon C_5 niet. In het algemeen is een cyclus van oneven lengte niet bipartiet. Als een graaf een cyclus van oneven lengte omvat, is hij zeker niet bipartiet. Omgekeerd ook.



Stelling 44. *Een ongerichte multigraaf $\mathcal{G}$ is bipartiet **als en slechts als** $\mathcal{G}$ geen cyclus bevat van oneven lengte.*

Bewijs. $\boxed{\Rightarrow}$ We hebben dit reeds opgemerkt. Onderstel dat er een cyclus $v_1 \sim v_2 \sim \cdots \sim v_{2m+1}$ is en v_1 rood werd gekleurd. Dan moet v_2 blauw, v_3 rood, $\ldots$, v_{2m+1} rood. Maar dan mag v_1 niet adjacent zijn met v_{2m+1}, tegenspraak.

$\boxed{\Leftarrow}$ Gegeven is een graaf $\mathcal{G}$ zonder oneven cyclus. We kleuren $\mathcal{G}$ met 2 kleuren. Kies een top v en kleur hem rood. Kleur al zijn buren blauw. In het algemeen krijgt een top t de rode kleur als zijn afstand tot v even is en anders de blauwe kleur. We herhalen dit desnoods in elke samenhangscomponent.

We tonen aan dat deze kleuring de graaf bipartiet maakt. Veronderstel dat twee adjacente toppen x en y rood zijn. Dan is er een pad van even lengte van x tot v en een pad van even lengte van y tot v. Dit levert minstens een cyclus van oneven lengte, tegenspraak. Analoog als twee blauwe toppen adjacent zijn. □

Hoeveel bogen kan een bipartiete graaf hebben?

Stelling 45. *Zij $\mathcal{G}$ een bipartiete ongerichte graaf met n toppen. Dan heeft $\mathcal{G}$ ten hoogste $\frac{n^2}{4}$ bogen als n even is en ten hoogste $\frac{n^2-1}{4}$ als n oneven is.*

Bewijs. Kies $\mathcal{G}$ zó dat geen andere bipartiete graaf met n toppen meer bogen heeft. Stel r gelijk aan het aantal rode toppen en b het aantal blauwe. Doordat $\mathcal{G}$ maximaal is, is het duidelijk dat elke rode top verbonden is met elke blauwe. Dus heeft $\mathcal{G}$ juist rb bogen. Dit is gelijk aan $r(n-r)$. Zoek nu zelf $r \in [n]$ zodat de functie $f(r) = r(n-r)$ een maximum bereikt. □

Als een graaf meer bogen heeft, is hij niet bipartiet en bevat hij dus een cyclus van oneven lengte. Wij bewijzen meer.

Stelling 46. *Zij $\mathcal{H}$ een ongerichte simpele graaf met $2m$ toppen ($m \geqslant 2$) en minstens m^2+1 bogen. Dan bevat $\mathcal{H}$ een driehoeksgraaf.*

Bewijs. Per inductie op m.

Voor $m = 2$ krijgen we dat $\mathcal{H}$ een deelgraaf is van K_4 met minstens 5 bogen. Vorige stelling zegt dat $\mathcal{H}$ niet bipartiet is en dus een cyclus heeft van oneven lengte. Dit moet een driehoek zijn omdat $\mathcal{H}$ maar vier toppen heeft.

Als de stelling waar is voor alle grafen met minder dan $2m$ toppen, nemen we in $\mathcal{H}$ twee adjacente toppen u en v. Als $\deg(u) + \deg(v) > 2m$ hebben deze toppen een gemeenschappelijke buur die een driehoek geeft. Als $\deg(u) + \deg(v) \leqslant 2m$, zal het verwijderen van u en v, samen met alle bogen waartoe ze behoren, het aantal bogen doen afnemen met ten hoogste $2m-1$. Het resultaat is dus een graaf met $2m-2$ toppen en minstens $m^2+1-(2m-1) = m^2-2m+2 = (m-1)^2+1$ bogen. Deze graaf bevat wegens de inductiehypothese een driehoek. □

We kunnen zonder teveel moeite Stelling 45 veralgemenen tot een iets grotere klasse van grafen. We weten dat een bipartiete graaf nooit een driehoeksgraaf kan bevatten. Een driehoeksgraaf komt voor in elke complete graaf K_r voor $r > 2$ zodat een bipartiete graaf geen deelgraaf K_r kan hebben voor $r > 2$. Er bestaan wel grafen zonder K_r die niet bipartiet zijn (denk aan C_5).

Stelling 47 (Turán)**.** *Zij $\mathcal{G}$ een ongerichte simpele graaf met n toppen die geen deelgraaf K_r omvat voor een zekere $r \geqslant 2$. Dan is het aantal bogen in $\mathcal{G}$ ten hoogste $(r-2)n^2/(2r-2)$.*

Bewijs. Per inductie op r.
Voor $r = 2$ is $\mathcal{G}$ een graaf zonder bogen. De bovengrens $(r-2)n^2/(2r-2)$ is in dit geval ook gelijk aan nul.

Voor de inductiestap gaan we van r naar $r+1$. We nemen dus een graaf $\mathcal{G}$ die geen deelgraaf K_{r+1} bevat en n toppen heeft. Stel $\mathcal{H}$ gelijk aan de

grootste deelgraaf van $\mathcal{G}$ die geen deelgraaf K_r heeft. Noteer x voor het aantal toppen in $\mathcal{H}$.

Beschouw een top v van $\mathcal{G}$. Vermits $\mathcal{G}$ geen K_{r+1} omvat, kan er in de buurt $\mathcal{G}_v$ zeker geen K_r voorkomen (samen met v zouden we anders een K_{r+1} hebben). Vermits de grootste deelgraaf van $\mathcal{G}$ die geen K_r omvat x toppen heeft, weten we dat $\mathcal{G}_v$ niet meer toppen kan hebben dan x. Met andere woorden geldt voor elke top $\deg v \leqslant x$. We beschouwen nu de bogen die niet volledig in $\mathcal{H}$ liggen. Dit zijn dus bogen met minstens één top buiten $\mathcal{H}$. We zullen dit aantal bogen afschatten. Er zijn $n - x$ toppen buiten $\mathcal{H}$ en elk van die toppen heeft graad ten hoogste x. Dus kunnen er niet meer bogen zijn dan $(n - x)x$ buiten $\mathcal{H}$.

De inductiehypothese, toegepast op $\mathcal{H}$, geeft dat het aantal bogen binnen $\mathcal{H}$ niet meer is dan $(r - 2)x^2/(2r - 2)$. In totaal is het aantal bogen in $\mathcal{G}$ dus ten hoogste $((r - 2)x^2/(2r - 2)) + x(n - x)$.

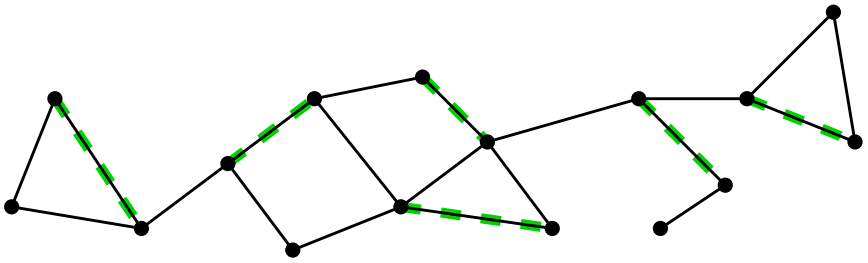
Vermits

$$\frac{r-2}{2r-2}x^2 + x(n-x) = \frac{r-1}{2r}n^2 - \frac{r}{2r-2}\left(x - \frac{(r-1)n}{r}\right)^2 \leqslant \frac{r-1}{2r}n^2$$

is de stelling bewezen. □

4.8 Koppelingen

Definitie 37. *Een **koppeling** (Engels: "matching") in een ongerichte (multi) graaf $\mathcal{G}$ is een verzameling van bogen van $\mathcal{G}$ waarin geen twee een top gemeenschappelijk hebben.*



In het algemeen kan je in een gegeven graaf vele verschillende koppelingen vinden. Eén enkele boog bijvoorbeeld vormt reeds een koppeling op zich.

Definitie 38. *Een koppeling heet **maximaal** indien we ze niet kunnen uitbreiden tot een koppeling met meer bogen. Een **maximumkoppeling** in een*

graaf $\mathcal{G}$ is een koppeling van maximale grootte. Dit wil zeggen dat er in $\mathcal{G}$ geen koppeling met meer bogen bestaat.

*Zij K een koppeling in $\mathcal{G}$. Een top van $\mathcal{G}$ heet K-**verzadigd** indien hij bevat is in een boog van K. Anders heet hij K-onverzadigd. Als het duidelijk is over welke koppeling K het gaat, spreken we gewoon van* verzadigd *en* onverzadigd*.*

*Een koppeling die alle toppen van een graaf verzadigt wordt een **volledige koppeling** genoemd.*

Een volledige koppeling is duidelijk een maximumkoppeling. Ook kan een graaf alleen maar een volledige koppeling hebben als zijn aantal toppen even is.

Hoe kunnen we nu koppelingen vinden met zoveel mogelijk bogen in een gegeven graaf?

Een strategie zou kunnen zijn om een willekeurige boog te nemen, dan een boog te nemen die daar geen top mee gemeenschappelijk heeft, enz. We krijgen zo zeker een koppeling en van zodra we geen nieuwe boog meer kunnen toevoegen, is de koppeling maximaal. Er is echter geen garantie dat de gevonden koppeling een maximumkoppeling is. We hebben dus een betere manier nodig.

Definitie 39. *Zij (V, E) een graaf met een koppeling K. Een K-**wisselpad** is een pad waarvan de opeenvolgende bogen afwisselend wel en niet tot K behoren. Een **vergrotend** K-**wisselpad** is een K-wisselpad waarvan de eerste en laatste top K-onverzadigd zijn.*

Elke boog vormt een wisselpad. Een boog waarvan beide toppen onverzadigd zijn vormt een vergrotend wisselpad.

Als we in een graaf een koppeling K hebben en een vergrotend K-wisselpad P, dan kunnen we in K de bogen die op P liggen vervangen door de bogen van P die niet in K zitten. Het resultaat is een koppeling K' die een boog meer heeft dan K. Vandaar de naam *vergrotend* wisselpad.

Willen we nu een maximumkoppeling vinden in een graaf $\mathcal{G}$, dan kunnen we als volgt te werk gaan.

Eerst maken we een maximale koppeling volgens de methode van hierboven. We maken nu uit deze koppeling een koppeling met meer bogen door een vergrotend wisselpad te zoeken en bogen uit te wisselen. Dit kunnen we herhalen tot er geen vergrotend wisselpad meer kan gevonden worden. Dat we op deze manier een koppeling van maximale grootte bekomen, wordt door volgende stelling van de Deen Petersen gegarandeerd. Hoewel Petersen zijn stelling reeds in 1891 bewees, geraakte ze in vergetelheid. In

1957 bewees de Fransman BERGE de stelling opnieuw. Daarom wordt deze stelling soms "de stelling van Berge" genoemd.

Stelling 48 (Petersen, 1891)**.** *Gegeven een ongerichte graaf $\mathcal{G}$. Een koppeling K in $\mathcal{G}$ is een maximumkoppeling* ***als en slechts als*** *er in $\mathcal{G}$ geen vergrotend K-wisselpad bestaat.*

Bewijs. $\boxed{\Rightarrow}$ Als K een maximumkoppeling is, kan er natuurlijk geen vergrotend K-wisselpad bestaan omdat de koppeling anders kan vergroot worden via de hierboven beschreven methode.

$\boxed{\Leftarrow}$ Veronderstel dat K een koppeling is die geen maximumkoppeling is. We moeten tonen dat er een vergrotend K-wisselpad bestaat. Omdat K geen maximumkoppeling is, moet er in $\mathcal{G}$ een koppeling K' bestaan die meer bogen heeft dan K. Stel nu $E' := K \setminus K' \cup K' \setminus K$, dit zijn de bogen die in K of K' zitten, maar niet in $K \cap K'$. Noteer $\mathcal{H}$ de deelgraaf van $\mathcal{G}$ met als bogenverzameling E' en als toppenverzameling de uiteinden van de bogen in E'. Omdat K en K' koppelingen zijn, moet elke samenhangscomponent van $\mathcal{H}$ een cyclus of pad zijn waarvan de bogen afwisselend in K en in K' zitten. Componenten met maar één boog kunnen ook voorkomen. Aangezien K' groter is dan K, moet er tenminste één component van $\mathcal{H}$ zijn die meer bogen van K' bevat dan van K. Deze component is dan een pad waarvan de eerste en laatste top K-onverzadigd zijn. Het is dus een vergrotend K-wisselpad. □

We hebben nu een manier om na te gaan of een koppeling een maximumkoppeling is en hebben ook gezien dat vergrotende wisselpaden helpen bij het vinden van een maximumkoppeling.

Kunnen we ook iets zeggen over de grootte van een maximumkoppeling in een gegeven graaf? Algemene uitspraken zijn hierover moeilijk te doen. Een cyclus van even lengte en een complete graaf met een even aantal toppen hebben beide een volledige koppeling.

Voor bipartiete grafen kunnen we echter meer zeggen.

4.9 Toewijzingen en het lessenroosterprobleem

Herinner dat de toppenverzameling V van een bipartiete graaf de disjuncte unie is van twee verzamelingen V_1 en V_2 waarbij elke boog een top in V_1 en een top in V_2 heeft.

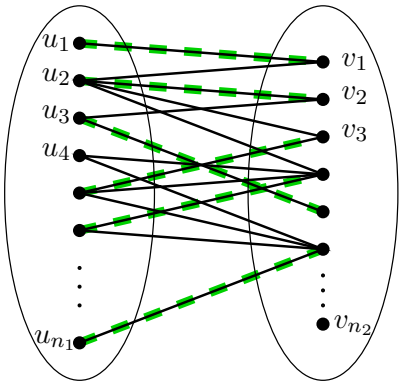
Definitie 40. *Zij $\mathcal{G} = (V_1 \cup V_2, E)$ een bipartiete ongerichte graaf. Indien elke top van V_1 adjacent is met elke top van V_2, spreekt men van een* ***com-***

***pleet bipartiete graaf**. Als $|V_1| = m$ en $|V_2| = n$ noteren we zulke graaf $K_{m,n}$.*

Opmerking. De ster S_n is eigenlijk $K_{1,n}$.

Zoals jullie weten is het niet eenvoudig om een lessenrooster op te stellen. Het aantal beschikbare lokalen bijvoorbeeld is een bovengrens op het aantal lessen dat tegelijkertijd kan gegeven worden. Er zijn ook lessen die enkel in een speciaal ingericht lokaal (bijvoorbeeld een labo of een lokaal met dataprojector) kunnen gegeven worden. Men wil meestal twee uur na elkaar doceren in eenzelfde lokaal. Sommige docenten hebben nog andere eigenaardige wensen die het probleem zeker niet vereenvoudigen.

Veronderstel dat we een universiteit hebben met n_1 docenten $u_1, u_2, \ldots, u_{n_1}$ en n_2 (disjuncte) studierichtingen die we $v_1, v_2, \ldots, v_{n_2}$ noteren. We kunnen een bipartiete graaf opstellen met als toppen de docenten en de studierichtingen. Twee toppen u_i en v_j zijn adjacent als en slechts als docent u_i lesgeeft in richting v_j. Indien we een lessenrooster willen opstellen zodanig dat zoveel mogelijk simultaan wordt lesgegeven, kunnen we het probleem formuleren met koppelingen in een bipartiete graaf. Elke koppeling komt overeen met een bepaald tijdslot waarin de docenten lesgeven aan een bepaalde groep studenten zodat het probleem herleid wordt tot het bepalen van een maximumkoppeling per tijdslot rekening houdend met de gestelde randvoorwaarden.



Wanneer elke docent alvast les zou willen geven in het tijdslot $10 - 12$, zouden we dus al zeker een koppeling moet vinden bestaande uit n_1 bogen. Het zal duidelijk zijn dat dergelijke voorwaarde niet altijd kan voldaan zijn.

Definitie 41. *Stel $\mathcal{G} = (V_1 \cup V_2, E)$ bipartiet ongericht en $W \subset V_1$.*
*Een **toewijzing** (Engels: "assignment") van W in V_2 is een koppeling K*

tussen toppen van W en V_2 die alle toppen van W verzadigt. Als W' de deelverzameling is van V_2 die door K verzadigd wordt, is K ook een toewijzing van W' in V_1.

*Een toewijzing is **maximaal** als de bijhorende koppeling maximaal is. We spreken van een **maximumtoewijzing** (respectievelijk **volledige toewijzing**) wanneer de bijhorende koppeling een maximumkoppeling (resp. volledige koppeling) is.*

Wij zijn vooral geïnteresseerd in toewijzingen van de volledige verzameling V_1 in V_2. We kunnen ons afvragen wanneer zulke toewijzing bestaat. Het antwoord wordt gegeven door een stelling van Philip Hall (1904–1982).

We zullen volgende notatie gebruiken: voor $W \subset V_1$ noteren we met $H(W)$ de **verzameling van buren van toppen** van W. Dit zijn dus toppen van V_2 die verbonden zijn met minstens één top in W.

Stelling 49 (P. Hall, 1935)**.** *Zij $\mathcal{G} = (V_1 \cup V_2, E)$ een bipartiete ongerichte graaf. Een toewijzing van V_1 in V_2 bestaat **als en slechts als** voor elke deelverzameling W van V_1 geldt dat $|H(W)| \geqslant |W|$.*

Bewijs. Het is duidelijk dat de voorwaarde nodig is. Inderdaad: elke deelverzameling van V_1 moet genoeg buren hebben, dit wil zeggen ten minste evenveel elementen als het aantal elementen in de verzameling zelf.

We bewijzen nu dat deze voorwaarde ook voldoende is. Neem dus aan dat de *voorwaarde van Hall* voldaan is (dus $\forall\ W \subset V_1 \colon |H(W)| \geqslant |W|$). We bewijzen per inductie op $|V_1|$ dat er een toewijzing van V_1 in V_2 bestaat. Als $|V_1| = 1$, dan is V_1 een singleton $\{u\}$. De voorwaarde van Hall geeft $|H(\{u\})| \geqslant 1$. De top u heeft dus ten minste één buur in V_2. Neem zo een buur en noem hem v. De boog $u \sim v$ vormt dan een toewijzing van V_1 in V_2.

We nemen nu aan dat de stelling waar is voor alle bipartiete grafen met $|V_1| \leqslant k$. We onderscheiden twee gevallen voor een bipartiete graaf $\mathcal{G} = (V_1 \cup V_2, E)$ met $|V_1| = k + 1$. Het eerste geval is dat elke echte deelverzameling van V_1 meer buren heeft dan de voorwaarde van Hall vereist. Dit is het zogenaamde "niet-kritisch geval".

Niet-kritisch geval We hebben dus

$$|H(W)| \geqslant |W| + 1$$

voor elke echte deelverzameling W van V_1. Voor een willekeurige top $u \in V_1$ hebben we dus minstens twee buren in V_2. Noem één van die buren v. We wijzen v alvast toe aan u en bekijken de bipartiete graaf $\mathcal{G}'$ die ontstaat

wanneer we $u \sim v$ uit $\mathcal{G}$ weglaten. Deze graaf heeft k toppen in V_1 en elke deelverzameling W van V_1 heeft tenminste $|W| + 1$ buren in V_2 en bijgevolg tenminste $|W|$ buren in $V_2 \setminus \{v\}$. Voor de graaf $\mathcal{G}'$ geldt dus de voorwaarde van Hall zodat we uit de inductiehypothese een toewijzing krijgen van $V_1 \setminus \{u\}$ in $V_2 \setminus \{v\}$. Samen met de boog $u \sim v$ vormt deze een toewijzing van V_1 in V_2.

Kritisch geval Nu is er minstens één echte deelverzameling W' van V_1 met $|H(W')| = |W'|$. Zulke W' heet een **kritische verzameling**. Voor de deelgraaf geïnduceerd op $W' \cup H(W')$ geldt uiteraard de voorwaarde van Hall. Omdat $|W'| \leqslant k$ kunnen we de inductiehypothese toepassen om een toewijzing van W' in $H(W')$ te vinden.

Voor de deelgraaf geïnduceerd op $V_1 \setminus W' \cup V_2 \setminus H(W')$ kunnen we de voorwaarde van Hall ook aantonen. Zij W een deelverzameling van $V_1 \setminus W'$. Dan heeft $W' \cup W$ ten minste $|W \cup W'|$ buren in V_2 (door de voorwaarde van Hall). Maar vermits precies $|W'|$ van die buren in $H(W')$ liggen, moeten minstens $|W|$ van hen in $V_2 \setminus H(W')$ liggen. Omdat $|V_1 \setminus W'| \leqslant k$ is ook hier de inductiehypothese van toepassing zodat we een toewijzing van $V_1 \setminus W'$ in $V_2 \setminus H(W')$ krijgen die samen met de toewijzing van W' in $H(W')$ uiteindelijk een toewijzing van V_1 in V_2 oplevert. □

We weten nu wanneer er een (maximum)toewijzing bestaat. Om zulke (maximum)toewijzing te vinden, is deze stelling echter nog niet voldoende. Er bestaan algoritmes om een maximumtoewijzing te vinden. We geven als voorbeeld de *Hongaarse methode* die ook bruikbaar is om een maximumkoppeling te vinden.

Algoritme voor een maximum toewijzing (Hongaarse methode). We vertrekken van een (eventueel lege) toewijzing K en proberen die uit te breiden door een vergrotend K-wisselpad te maken met volgend algoritme.

Neem een top w van V_1 die K-onverzadigd is. Bouw een gewortelde **wisselboom** $\mathcal{T}$ met wortel w (dit is een boom zodanig dat elk pad in $\mathcal{T}$ met beginpunt w een wisselpad is) door steeds bogen van $\mathcal{G}$ toe te voegen aan $\mathcal{T}$. Stop met bogen toe te voegen als één van volgende voorwaarden voldaan is:

1. de boom $\mathcal{T}$ heeft een onverzadigd blad $u \in V_2$;
2. alle bladeren van $\mathcal{T}$ zijn verzadigde toppen van V_1 en $\mathcal{T}$ kan niet verder uitgebreid worden.

Indien aan 2 is voldaan, herbegin je met een andere onverzadigde top. In het andere geval hebben we een vergrotend K-wisselpad P en wordt de

toewijzing K vervangen door $K \setminus P \cup P \setminus K$. We kunnen nu het algoritme opnieuw uitvoeren met deze nieuwe toewijzing. Uiteindelijk kunnen we geen wisselpaden meer vinden. We eindigen met een toewijzing K_H waarvan we kunnen bewijzen dat dit een maximumtoewijzing is. Dit zal je in de Oefening 36 doen.

We kunnen ons nu ook afvragen of we de grootte van een maximumtoewijzing kunnen bepalen zonder zo een toewijzing daadwerkelijk te construeren. De stelling van KÖNIG zegt dat dit inderdaad mogelijk is. We geven geen bewijs.

Stelling 50 (König)**.** *Zij $\mathcal{G} = (V_1 \cup V_2, E)$ een bipartiete ongerichte graaf en stel*

$$t := \max_{W \subset V_1} (|W| - |H(W)|)$$

Dan is het aantal bogen van een maximumtoewijzing van V_1 in V_2 gelijk aan $|V_1|$ indien $t \leqslant 0$ en aan $|V_1| - t$ anders.

Definitie 42. *Een **(toppen)overdekking** (Engels: "vertex cover") van een ongerichte graaf $\mathcal{G}$ is een deelverzameling U van toppen van $\mathcal{G}$ waarbij elke boog van $\mathcal{G}$ minstens één top van U bevat.*

*Een **minimale overdekking** is een overdekking die geen echte deelverzameling heeft welke ook een overdekking is. Een **minimumoverdekking** is een overdekking waarnaast geen overdekking bestaat met minder toppen.*

Merk op dat voor een bipartiete graaf $\mathcal{G} = (V_1 \cup V_2, E)$ zowel V_1 als V_2 overdekkingen zijn, welke minimaal zijn als $\mathcal{G}$ geen geïsoleerde top heeft. In het algemeen zullen de minimale overdekkingen dus deelverzamelingen hiervan zijn.

Onderstel nu dat we in een (niet noodzakelijk bipartiete) ongerichte graaf $\mathcal{G}$ een koppeling K en een overdekking U hebben. Dan moet elke boog van K ten minste één van zijn uiteinden in U hebben. Omdat de bogen van K geen toppen gemeenschappelijk hebben, moeten er tenminste zoveel toppen in U liggen als er bogen zijn in K. Dus geldt $|K| \leqslant |U|$ voor elke koppeling K en elke overdekking U.

We krijgen dus

$$\max |K| \leqslant \min |U|,$$

waarbij K de verzameling van alle koppelingen van $\mathcal{G}$ doorloopt en U de verzameling van alle overdekkingen.

De vraag is of de gelijkheid geldt. Het antwoord is duidelijk negatief. In een vijfhoek C_5 bijvoorbeeld zal een maximumkoppeling bestaan uit 2 bogen, terwijl een minimumoverdekking moet bestaan uit 3 toppen. Voor een bipartiete graaf geldt de gelijkheid daarentegen wel.

Stelling 51 (König–Egerváry, 1931)**.** *Voor een bipartiete ongerichte graaf* $\mathcal{G} = (V_1 \cup V_2, E)$ *geldt*

$$\max |K| = \min |U|$$

waarbij K *de verzameling van alle koppelingen van* $\mathcal{G}$ *doorloopt en* U *de verzameling van alle overdekkingen van* $\mathcal{G}$*.*

Bewijs. We weten al dat $\max |K| \leqslant \min |U|$. Het is dus voldoende om een koppeling K en een overdekking U te vinden met $|K| = |U|$. Voor K nemen we uiteraard een maximumkoppeling $K_{\max}$. Volgens de stelling van König hebben we ofwel

$$|K_{\max}| = |V_1|$$

ofwel

$$|K_{\max}| = |V_1| - \max_{W \subset V_1} (|W| - |H(W)|).$$

In het eerste geval kiezen we $U := V_1$. Dit is een overdekking.

In het andere geval nemen we W^* gelijk aan een deelverzameling van V_1 waarvoor het "maximum burentekort" van bovenstaande gelijkheid bereikt wordt. Dan volgt

$$|K_{\max}| = |V_1| - (|W^*| - |H(W^*)|) = |(V_1 \setminus W^*) \cup H(W^*))|.$$

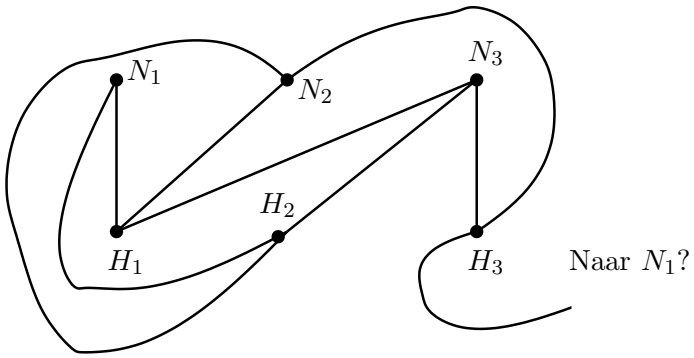
De verzameling

$$U := (V_1 \setminus W^*) \cup H(W^*))$$

heeft het gewenste aantal elementen en is een overdekking. Inderdaad: de verzameling $V_1 \setminus W^*$ overdekt alle bogen met een uiteinde in $V_1 \setminus W^*$ en $H(W^*)$ overdekt alle bogen met een uiteinde in W^*. □

4.10 Planaire grafen

Drie nieuwe huizen H_1, H_2 en H_3 moeten verbonden worden met de nutsvoorzieningen water N_1, elektriciteit N_2 en internet N_3. Is het mogelijk om leidingen te leggen op dezelfde hoogte tussen elk van de drie huizen en de drie voorzieningen zodanig dat ze mekaar niet moeten kruisen? We proberen op een tekening:



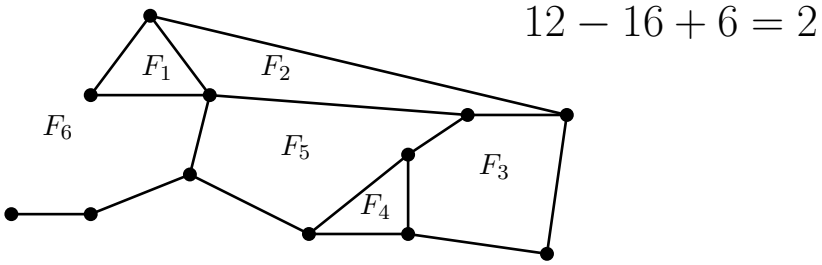
We zien geen mogelijkheid om $H3$ met $N1$ te verbinden. Misschien moeten we harder proberen? Misschien hangt het af van de ligging van de huizen en de voorzieningen?

Wiskundig stelt men zich de vraag of de compleet bipartiete graf $K_{3,3}$ in het vlak (of op een blad papier) kan getekend worden zodanig dat twee bogen elkaar nooit snijden.

Definitie 43. *Een multigraaf heet **planair** indien hij in een vlak kan getekend worden zonder dat twee bogen elkaar snijden.*

*Als we een planaire multigraaf in het vlak tekenen zodanig dat geen twee bogen snijden, wordt het vlak verdeeld in **gebieden** (Engels: "faces").*

Er bestaat een verband tussen het aantal toppen, bogen en gebieden van een planaire multigraaf. We noteren deze aantallen respectievelijk met v, e en f.



Stelling 52 (weeral van Euler)**.** *Voor een samenhangende planaire ongerichte multigraaf $\mathcal{G}$ geldt steeds*

$$v - e + f = 2.$$

Bewijs. We geven een bewijs per inductie op e, het aantal bogen in $\mathcal{G}$.

Als $e = 1$, dan is de graaf ofwel isomorf met het pad P_2 ofwel een lus. In het eerste geval hebben we $v = 2$ en $f = 1$ en in het tweede geldt $v = 1$ en $f = 2$. In beide gevallen is de formule van Euler voldaan.

Onderstel dat de stelling geldt voor alle planaire grafen met $e-1$ bogen. Er zijn twee gevallen.

1 We kunnen uit $\mathcal{G}$ een boog b weglaten zodat $\mathcal{G}' := \mathcal{G} - b$ nog steeds samenhangend is. Dan maakt b deel uit van een cyclus in $\mathcal{G}$. Daarom behoort b tot de rand van twee gebieden. De graf $\mathcal{G}'$ heeft dan $e-1$ bogen, $f-1$ gebieden en v toppen. De inductiehypothese geeft $v-(e-1)+(f-1) = 2$.

2 Er is geen boog die we kunnen weglaten zonder de samenhang te verliezen. Dan is $\mathcal{G}$ een boom. Bijgevolg geldt $f = 1$ en $v = e+1$. □

We komen nu terug naar het probleem van de drie huizen en voorzieningen. Is $K_{3,3}$ planair? Indien wel, moet $v - e + f = 2$. We weten dat $v = 6$ en $e = 9$. Dus moet $f = 5$. Maar doordat $K_{3,3}$ compleet bipartiet is, moeten de gebieden cyclussen zijn van lengte 4. Om 5 zulke cycli te maken hebben we in principe 20 bogen nodig, maar in een planaire graaf ligt elke boog op de grens van één of twee gebieden. De zuinigste manier om planair 5 vierhoeken te maken is dus met 10 bogen. Maar $K_{3,3}$ heeft er maar 9 en kan dus niet planair zijn. Het nutsvoorzieningsprobleem heeft bijgevolg geen oplossing en dus moeten we dieper graven.

Ook K_5 is niet planair. Veronderstel van wel. Dan moeten er 7 gebieden zijn vermits $v = 5$ en $e = \binom{5}{2} = 10$. In K_5 moeten de gebieden driehoeken zijn. Hiervoor zijn normaal $7 \cdot 3 = 21$ bogen nodig. Dit is onmogelijk met de 10 bogen die we ter beschikking hebben, ook al gebruiken we elke boog op de grens van twee gebieden.

We kunnen bovenstaande redeneringen veralgemenen.

Stelling 53. *Zij $\mathcal{G}$ een samenhangende planaire ongerichte simpele graaf met minstens twee bogen. Dan geldt $3f \leqslant 2e$ en $e \leqslant 3v - 6$.*

Bewijs. De stelling is duidelijk waar wanneer er maar één gebied is. Onderstel $f > 1$. Vermits de graaf simpel is, bestaat de rand van elk gebied uit minstens 3 bogen. Elke boog kan hoogstens twee keer optreden als rand van een gebied zodat

$$2e \geqslant 3f$$

Samen met $v - e + f = 2$ krijgen we $2 \leqslant v - e + \frac{2}{3}e = v - \frac{e}{3}$. □

Gevolg 13. *Elke samenhangende planaire ongerichte simpele graaf $\mathcal{G}$ heeft een top van graad $\leqslant 5$.*

Bewijs. We weten $e \leqslant 3v - 6$. Dus moet

$$\sum_{x \in V(\mathcal{G})} \deg(x) = 2e \leqslant 6v - 12.$$

Mocht elke top x graad $\geqslant 6$ hebben, zou $\sum_{x \in V(\mathcal{G})} \deg(x) \geqslant 6v$, tegenspraak. □

Uit het feit dat noch $K_{3,3}$ noch K_5 planair zijn, volgt gemakkelijk dat een graaf die een deelgraaf isomorf met $K_{3,3}$ of met K_5 bevat nooit planair kan zijn.

Als een graaf niet planair is, is het duidelijk dat als we een top van graad 2 weglaten en zijn 2 buren verbinden met een boog, de graf niet planair kan worden. Ook mogen we een boog $\{x, y\}$ gerust vervangen door een nieuwe top t en twee bogen $\{x, t\}$ en $\{t, y\}$, zonder de planariteit te veranderen.

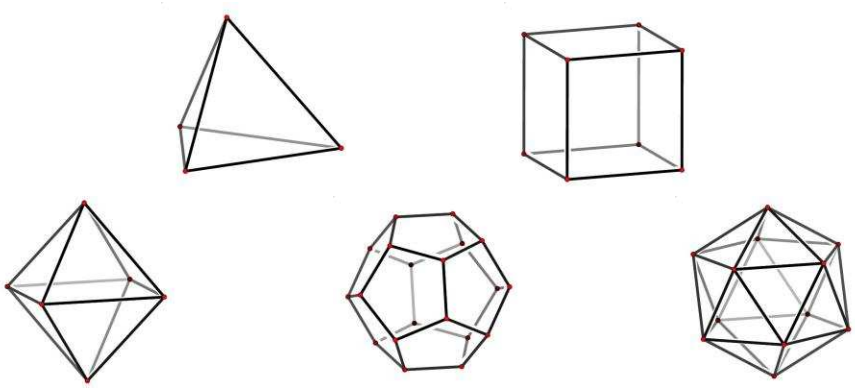
Definitie 44. *Een graaf $\mathcal{H}$ die ontstaat uit een graaf $\mathcal{G}$ door (eventueel meermaals) toepassen van bovenstaande operaties heet* ***boogequivalent*** *met $\mathcal{G}$.*

Volgende belangrijke stelling geven we zonder bewijs.

Stelling 54 (Kuratowski, 1930)**.** *Een multigraaf is planair* ***als en slechts als*** *hij geen deelgraaf bevat die boogequivalent is met $K_{3,3}$ of met K_5.*

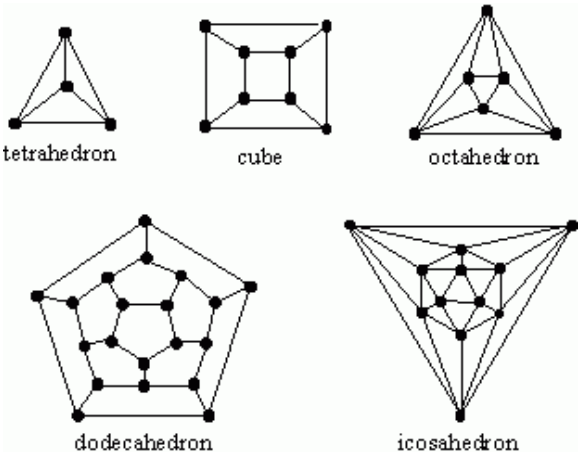
4.10.1 Platonische lichamen

We kennen allemaal de vijf regelmatige veelvlakken die soms ook "platonische lichamen" worden genoemd: de tetraëder, de kubus, de octaëder, de dodecaëder en de icosaëder. Waarom zijn er maar vijf zulke regelmatige veelvlakken?



Bij de platonische lichamen behoort elke ribbe tot juist twee zijvlakken en alle zijvlakken hebben evenveel ribben op hun rand. Bovendien liggen ook alle hoekpunten op eenzelfde aantal ribben.

Merk op dat de platonische lichamen aanleiding geven tot planaire grafen gevormd door de hoekpunten en ribben:



We bestuderen nu de planaire grafen waarin elke boog in de rand zit van twee gebieden, elke top graad n heeft en alle gebieden m bogen hebben in hun rand. Het is duidelijk dat we ook $n, m \geqslant 3$ moeten nemen.

Vermits elke boog op twee gebieden ligt, hebben we $2e = mf$. Vermits elke top graad n heeft en elke boog twee toppen verbindt, geldt ook $2e = nv$. De planariteit impliceert

$$0 < 2 = v - e + f = \frac{2e}{n} - e + \frac{2e}{m} = e\left(\frac{2m - nm + 2n}{nm}\right)$$

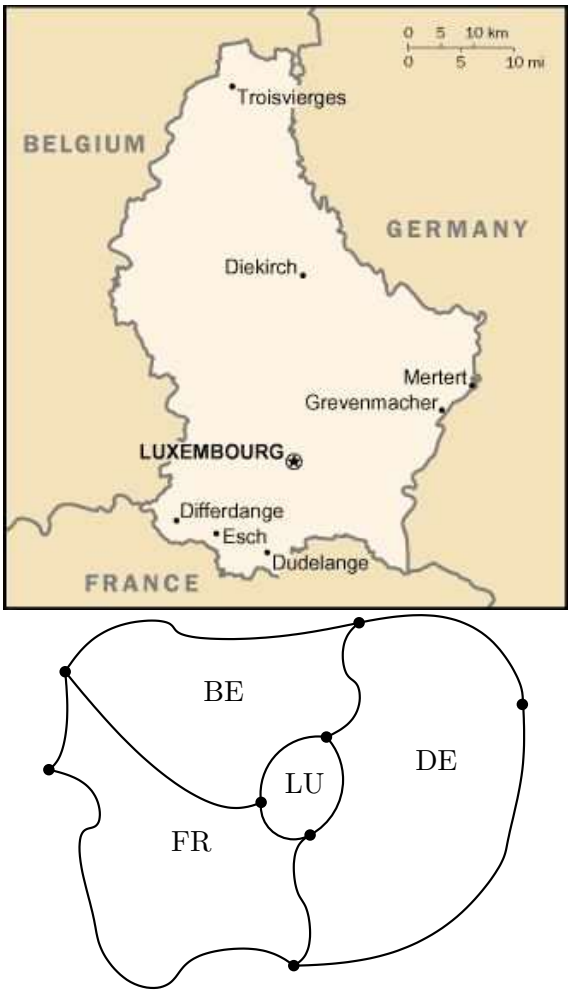
Vermits zowel e als m en n strikt positief zijn, moet $2m - nm + 2n > 0$ of $nm - 2n - 2m < 0$. Dit is equivalent met $nm - 2m - 2n + 4 < 4$ of $(n-2)(m-2) < 4$. Doordat $m, n \geqslant 3$, zijn zowel $n-2$ als $m-2$ positief. Er zijn maar vijf koppels (m, n) die voldoen aan alle voorwaarden. Deze geven aanleiding tot de vijf gekende platonische lichamen.

$m-2$	$n-2$	m	n	lichaam
1	1	3	3	tetraëder
2	1	4	3	kubus
1	2	3	4	octaëder
3	1	5	3	dodecaëder
1	3	3	5	icosaëder

4.10.2 Het kleuren van planaire grafen

In een atlas worden de landen meestal ingekleurd met verschillende kleuren zodat twee buurlanden nooit dezelfde kleur krijgen. Zo zie je duidelijk de grens tussen twee landen. Hoeveel kleuren heb je hiervoor minstens nodig?

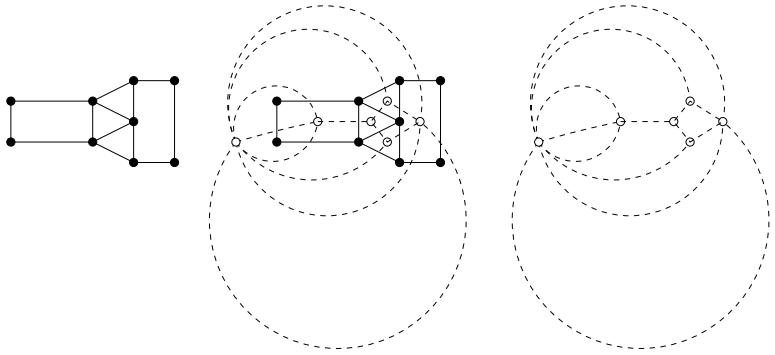
Luxemburg toont dat het antwoord minstens 4 is.



Een landkaart is natuurlijk een planaire graaf.

We moeten voor een planaire graaf dus bepalen hoeveel kleuren er minstens nodig zijn om de gebieden zó te kleuren dat aangrenzende gebieden nooit dezelfde kleur krijgen. Om dit probleem te vertalen naar een kleuring van toppen in een graf, voeren we het zeer belangrijke begrip *dualiteit* in.

Definitie 45. *Zij $\mathcal{G}$ een planaire ongerichte mulitgraaf. De* ***duale graf*** *$\mathcal{G}^*$ heeft als toppen de gebieden van $\mathcal{G}$ en twee toppen zijn adjacent als en slechts als de overeenkomstige gebieden een boog delen. De figuur hieronder toont een voorbeeld van een graaf en zijn duale (in streepjeslijn).*



Opmerking. De duale van een planaire graaf is opnieuw een planaire graaf.

Het probleem wordt nu: wat is het minimaal aantal kleuren nodig om de toppen van een planaire graaf te kleuren zodanig dat adjacente toppen nooit dezelfde kleur hebben?

Stelling 55. *Elke samenhangende planaire ongerichte simpele graaf $\mathcal{G}$ kan met* 6 *kleuren gekleurd worden.*

Bewijs. We doen dit bij inductie op v, het aantal toppen van de planaire graaf $\mathcal{G}$.

Voor $v = 1$ is het duidelijk in orde.

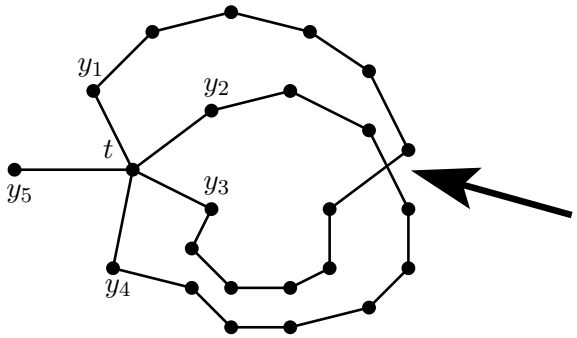
Onderstel nu dat de stelling geldt voor alle planaire grafen met $v - 1$ toppen. Uit Gevolg 13 weten we dat $\mathcal{G}$ een top t heeft met $\deg(t) \leqslant 5$. Als we t weglaten, krijgen we een graaf $\mathcal{G}'$ met $v - 1$ toppen. Deze kan dus gekleurd worden met 6 kleuren. Vermits t hoogstens 5 buren heeft (die in $\mathcal{G}'$ elk een kleur krijgen), is er zeker een kleur over voor t. □

We kunnen dit resultaat nog een beetje verfijnen.

Stelling 56. *Elke samenhangende planaire ongerichte simpele graaf $\mathcal{G}$ kan met 5 kleuren gekleurd worden.*

Bewijs. Ook per inductie op v, zoals in het vorige bewijs. Dat bewijs kan trouwens alleen maar mis gaan voor vijf kleuren als t echt 5 buren heeft, elk van een andere kleur in de kleuring van $\mathcal{G}'$. We bekijken dit geval van nabij.

Noteer de 5 buren van t met y_1, y_2, y_3, y_4 en y_5, genummerd in wijzerzin (zie tekening). Zij $\mathcal{G}'$ de graaf die uit $\mathcal{G}$ ontstaat als je t weglaat, alsook de 5 bogen op t. Als $\mathcal{G}'$ kan gekleurd worden met 5 kleuren waarbij y_1 en y_3 dezelfde kleur hebben, is er een kleur over voor t. Anders moet elke kleuring van $\mathcal{G}'$ met 5 kleuren een pad van y_1 tot y_3 hebben dat alternerend de kleuren van y_1 en y_3 gebruikt.



Op dezelfde manier is er een pad van y_2 naar y_4 dat alleen de kleuren van y_2 en y_4 gebruikt (die verschillend zijn van die van y_1 en y_3). Dus kunnen de twee gevonden paden geen top gemeenschappelijk hebben. Maar door de ligging van y_2 tussen y_1 en y_3, moeten de twee paden kruisen. Dit spreekt de planariteit tegen. □

Lang heeft men als conjectuur gehad dat 4 kleuren voldoende moeten zijn. In 1976 bewezen Appel en Haken met een computer (door eerst "met de hand" het probleem te herleiden tot 1800 gevallen en die dan door de computer te laten oplossen) dat 4 kleuren inderdaad volstaan. Momenteel is hiervoor nog steeds geen bewijs gekend dat niet steunt op computerberekeningen. Sommige wiskundigen zijn hierdoor van mening dat de "4-kleurenstelling" nog niet bewezen is en blijven ze een conjectuur of vermoeden noemen.

4.11 Oefeningen

1. ○ Professor McBrain en zijn echtgenote April geven een feestje waar nog vier andere koppels op uitgenodigd zijn. Sommige mensen schudden elkaar de hand, maar uiteraard niet hun eigen partner. Op het eind van het feestje vraagt McBrain aan alle gasten en aan zijn vrouw aan hoeveel mensen ze een hand hebben gegeven, en hij krijgt negen verschillende antwoorden. Hoeveel mensen hebben een hand gegeven aan April?

2. ○ Drie huizen A, B en C moeten elk aangesloten worden aan gas, elektriciteit en water: G, E, W. Geef de incidentiematrix van de graaf die dit probleem voorstelt. Teken de graaf. Is het mogelijk hem zo te tekenen dat er geen kruisende bogen zijn (m.a.w. is de graaf *planair*)?

3. ○ De wielgraaf W_n is de graaf met $V(W_n) = \{0, 1, \ldots, n\}$ en met bogen $E(W_n) = \{\{0,1\},\{0,2\},\ldots,\{0,n\}\} \cup \{\{1,2\},\{2,3\},\ldots,\{n-1,n\},\{n,1\}\}$. Beschrijf een Hamiltoncyclus in W_n.

4. ○ Hoeveel bogen heeft de complete graaf K_n? Voor welke waarden van n kan je de graaf K_n tekenen zodat de bogen elkaar niet kruisen?

5. ○ Maak een samenhangende simpele graaf met vijf toppen en zes bogen die geen 3-cycli bevat.

6. ◐ Zij $V(\mathcal{G})$ de verzameling van alle woorden van lengte 3 in het alfabet $\{0,1\}$ en $E(\mathcal{G})$ bevat koppels woorden die in precies één letter van elkaar verschillen. Toon aan dat $\mathcal{G}$ isomorf is met de hoekpunten en ribben van een gewone kubus.

7. ○ Zeg van de volgende lijsten van getallen of het de graden kunnen zijn van de toppen van een graaf. Zo ja, teken een graaf die eraan voldoet.

   (a) 2, 2, 2, 3
   (b) 2, 2, 4, 4, 4
   (c) 1, 2, 2, 3, 4
   (d) 1, 2, 3, 4

8. ○ Als $(V(\mathcal{G}), E(\mathcal{G}))$ een graaf is, dan is het complement $\bar{\mathcal{G}}$ van $\mathcal{G}$ de graaf met dezelfde toppen en alle mogelijke bogen die niet in $\mathcal{G}$ zitten. Als de graden van de toppen van $\mathcal{G}$ gegeven worden door $x_1, x_2, \ldots, x_n$, wat zijn dan de graden van de toppen van $\bar{\mathcal{G}}$?

9. ○ Bewijs dat het complement (zie oefening 8) van een niet-samenhangende simpele graaf steeds samenhangend is. Geldt het omgekeerde ook?

10. ◐ Zoek zoveel mogelijk niet-isomorfe reguliere grafen van graad 4 met 7 toppen.

11. ◐ Toon aan: als $\mathcal{G}$ een simpele graaf is met minstens 2 toppen, dan heeft $\mathcal{G}$ 2 toppen van dezelfde graad. [Vergelijk met oefening 2 van hoofdstuk 2.]

12. ○ Zoek een hamilton-cyclus in de graaf bestaande uit de hoekpunten en de ribben van een kubus.

13. ◐ Een muis heeft het plan opgevat om een $3 \times 3 \times 3$-kubus kaas op te eten. Nu is de muis nogal systematisch aangelegd, en ze begint dus aan een hoek en eet daar eerst het volledige $1 \times 1 \times 1$-kubusje op. Daarna neemt ze een van de buur-$(1 \times 1 \times 1)$-kubusjes enz. Kan de muis eindigen in het midden van de grote kubus?

14. ◐ Zij $\mathcal{G}$ een ongerichte graaf zonder lussen. Toon aan dat je de bogen van $\mathcal{G}$ zo kunt richten dat er geen enkele gerichte cyclus ontstaat.

15. ◐ Waar of onwaar?

    (a) Als een graaf een Eulercyclus heeft dan heeft hij een even aantal bogen.

    (b) Zij $\mathcal{G}$ een simpele graaf met 9 toppen en veronderstel dat de som van alle graden minstens 27 is. Dan heeft $\mathcal{G}$ een top met graad minstens 4.

    (c) Het aantal mensen dat een oneven aantal broers en zussen heeft is even.

    (d) Als een simpele graaf een Eulercyclus heeft, dan heeft hij ook een Hamiltoncyclus.

    (e) Als een simpele graaf een Hamiltoncyclus heeft, dan heeft hij ook een Eulercyclus.

    (f) In een reguliere graaf heeft elke top niet alleen hetzelfde aantal buren maar ook hetzelfde aantal toppen op afstand 2.

16. ○ Voor welke waarden van m en n is de compleet bipartiete graf $K_{m,n}$ een Eulergraf?

17. ○ Toon aan dat een Eulergraaf met een even aantal toppen die regulier is steeds een even aantal bogen heeft.

18. ◐ Zij $\mathcal{G}$ een simpele graaf met 10 toppen en 28 bogen. Toon aan dat $\mathcal{G}$ een cyclus van lengte vier bevat.

19. ◐ Zij $\mathcal{G}$ een simpele graaf met 10 toppen en 38 bogen. Bewijs dat $\mathcal{G}$ K_4 bevat als deelgraaf.

20. ○ Zij $\mathcal{G}$ een graaf waarin elke top graad 4 heeft. Toon aan dat je de bogen met 2 kleuren zodanig kan kleuren dat elke top op 2 bogen van de ene en 2 bogen van de andere kleur ligt.

21. ○ Hoeveel verschillende grafen met n genummerde toppen zijn er?

22. ● Hoeveel automorfismen zijn er van de volgende grafen?

    (a) K_n

    (b) C_n, de cyclus met n toppen

    (c) P_n, het pad langs n toppen

    (d) S_n, de ster met n toppen

    (e) de kubus in 3 dimensies

23. ◐ Toon aan dat er meer dan 6600 niet-isomorfe grafen zijn met 8 toppen.

24. ○ Hoeveel toppen kan een samenhangende reguliere simpele graaf met 22 bogen hebben?

25. ◐ Toon aan dat de Petersengraaf geen Hamiltoncyclus, maar wel een Hamiltonpad heeft. Toon aan dat, als je 1 top en de incidente bogen verwijdert uit de graf, er wel een Hamiltoncyclus is.

26. ◐ Zij $n \geq 2$ een geheel getal, en $a_1 \geq a_2 \geq \cdots \geq a_n$ een n-tal strikt positieve gehele getallen zodat $a_1 + a_2 + \cdots + a_n = 2n - 2$. Toon aan dat er een boom bestaat met n toppen en met als geordende gradenrij $a_1, a_2, \ldots, a_n$.

27. ◐ Een complete k-boom is een gewortelde boom waarin elke top ofwel k ofwel 0 kinderen heeft. Als T zo'n boom is met m toppen die geen blad zijn, hoeveel bladen heeft T dan?

28. ● Er zijn n parkeerplaatsen $1, 2, \ldots, n$ in een eenrichtingsstraat. De auto's $1, 2, \ldots, n$ komen in die volgorde in de straat. Elke auto i heeft een favoriet plaatsje $f(i)$. Als een auto de straat inrijdt, gaat hij eerst

naar z'n favoriete parkeerplaats. Als die niet vrij is, dan gaat hij naar de volgende plaats en daarna terug de volgende, tot hij een lege plaats vindt. Als de auto de straat uitrijdt zonder een parkeerplaats te vinden, dan geeft hij het op en is het parkeerplan mislukt. Als op het einde alle auto's geparkeerd zijn, dan noemen we f een *parkeerfunctie* op $[n]$. Toon aan dat het aantal parkeerfuncties op $[n]$ gelijk is aan $(n+1)^{n-1}$. Hoeveel parkeerfuncties zijn er op $[n]$ waarbij voor geen enkele i geldt dat $f(i) = f(i+1)$?

29. ○ Teken alle niet-isomorfe bomen met zes toppen.

30. ● Hoeveel verschillende Hamiltoncycli heeft de complete graf K_n? Hoeveel verschillende Hamiltoncycli zonder gemeenschappelijke bogen zijn er in K_{21}?

31. ● Stel $n \in \mathbb{Z}$, $n \geq 2$. Toon aan dat het aantal Hamiltoncycli in $K_{n,n}$ gelijk is aan $(n-1)!n!/2$. Hoeveel Hamiltonpaden zijn er in $K_{n,n}$?

32. ○ Zijn $\mathcal{T}_1$ en $\mathcal{T}_2$ twee bomen met $|E(\mathcal{T}_1)| = 17$ en $|V(\mathcal{T}_2)| = 2|V(\mathcal{T}_1)|$. Bepaal $|V(\mathcal{T}_1)|$, $|V(\mathcal{T}_2)|$ en $|E(\mathcal{T}_2)|$.

33. ○ Zij $\mathcal{F}_1$ een bos met zeven bomen, en met $|E(\mathcal{F}_1)| = 40$. Wat is $|V(\mathcal{F}_1)|$?

34. ◐ Zoek 2 niet-isomorfe opspannende bomen voor de complete bipartiete graaf $K_{2,3}$. Hoeveel niet-isomorfe opspannende bomen heeft deze graf?

35. ◐ Zoek alle maximale koppelingen van de Petersengraaf. Hoe groot is een maximumkoppeling van deze graf?

36. ● Bewijs dat de Hongaarse methode altijd een maximumtoewijzing oplevert.

37. ● Aan een toernooi doen $2n$ ploegen mee. Er zijn al twee ronden gespeeld. Toon aan dat we de ploegen nog altijd in twee groepen van n ploegen kunnen verdelen, zodat ploegen van eenzelfde groep nog niet tegen elkaar gespeeld hebben.

38. ◐ Zij $(X \cup Y, \sim)$ een bipartiete graaf waarin de graad van elke top in X minstens zo groot is als de graad van elke top in Y. Toon aan dat er een volledige toewijzing bestaat van X in Y.

39. ● Zij $\mathcal{G}$ een bipartiete graaf. Toon aan dat $\mathcal{G}$ een volledige toewijzing heeft asa voor elke deelverzameling X van $V(\mathcal{G})$ geldt dat $|X| \leq$

$|N(X)|$ (met $N(X)$ bedoelen we de verzameling van de buren van punten van X).

40. ◐ Zij $\mathcal{G}$ een reguliere bipartiete graaf. Toon aan dat $\mathcal{G}$ een volledige toewijzing heeft.

41. ● Er zijn n kinderen en n speelgoedjes in de kleuterklas. Elk kind wil met r specifieke speelgoedjes spelen, en voor elk speelgoedje zijn er precies r kinderen die ermee willen spelen. Toon aan dat we r speelrondes kunnen organiseren, zodanig dat elk kind juist een keer met elk van zijn r voorkeurspeelgoedjes heeft gespeeld.

42. ● Een graaf $\mathcal{G}$ noemen we *factor critical* als $\mathcal{G} - v$ een volledige koppeling heeft, voor elke top v van $\mathcal{G}$. Toon aan dat een bipartiete graaf nooit factor critical is.

43. ○ In Rydell High School is het laatste jaar in zes studentencomités vertegenwoordigd door Annemarie (A), Gary (G), Jill (J), Kenneth (K), Michael (M), Norma (N), Paul (P) en Rosemary (R). De laatstejaars in deze comités zijn {A,G,J,P}, {G,J,K,R}, {A,M,N,P}, {A,G,M,N,P}, {A,G,K,N,R} en {G,K,N,R}.

    (a) De studentenraad roept een vergadering bijeen, waarin minstens een laatstejaars uit elk comité moet zitten. Zoek een selectie zodanig dat het aantal deelnemers minimaal is.

    (b) Voor de vergadering moeten de financiën van elk comité onderzocht worden door een laatstejaarsvertegenwoordiger die niet in dat comité zit. Kan dit? Zo ja, hoe?

44. ◐ Zij $\mathcal{G} = (X \cup Y, \sim)$ een bipartiete graaf met $X = \{x_1, x_2, \ldots, x_m\}$ en $Y = \{y_1, y_2, \ldots, y_n\}$. Hoeveel volledige toewijzingen van X in Y bestaan er als

    (a) $m = 2$, $n = 4$ en $\mathcal{G} = K_{2,4}$?

    (b) $m = 4$, $n = 4$ en $\mathcal{G} = K_{4,4}$?

    (c) $m = 5$, $n = 9$ en $\mathcal{G} = K_{5,9}$?

    (d) $m \leq n$ en $\mathcal{G} = K_{m,n}$?

45. ○ Fritz moet jobs toewijzen aan jobstudenten. Hij heeft 25 kandidaten en 25 jobs die moeten ingevuld worden. Elke student is voor minstens 4 jobs geschikt, maar elke job kan door ten hoogste 4 studenten uitgevoerd worden. Kan Fritz elke student een job geven waarvoor hij geschikt is? Leg uit.

Figuur 4.3: Een beroemde fullereen met 60 toppen.

46. ○ Bepaal voor elk van de volgende collecties van verzamelingen indien mogelijk een systeem van verschillende representanten. Indien onmogelijk, leg uit waarom.

    (a) $A_1 = \{2,3,4\}$, $A_2 = \{3,4\}$, $A_3 = \{1\}$, $A_4 = \{2,3\}$

    (b) $A_1 = A_2 = A_3 = \{2,4,5\}$, $A_4 = A_5 = \{1,2,3,4,5\}$

    (c) $A_1 = \{1,2\}$, $A_2 = \{2,3,4\}$, $A_3 = \{2,3\}$, $A_4 = \{1,3\}$, $A_5 = \{2,4\}$

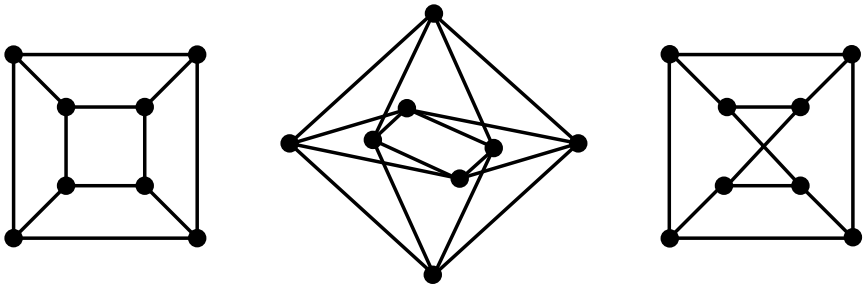
47. ◐ Een **fullereen** is een convexe polyeder van graad 3 met als zijvlakken enkel vijf- en zeshoeken.

    (a) Bewijs dat elke fullereen juist 12 vijfhoekige zijvlakken heeft.

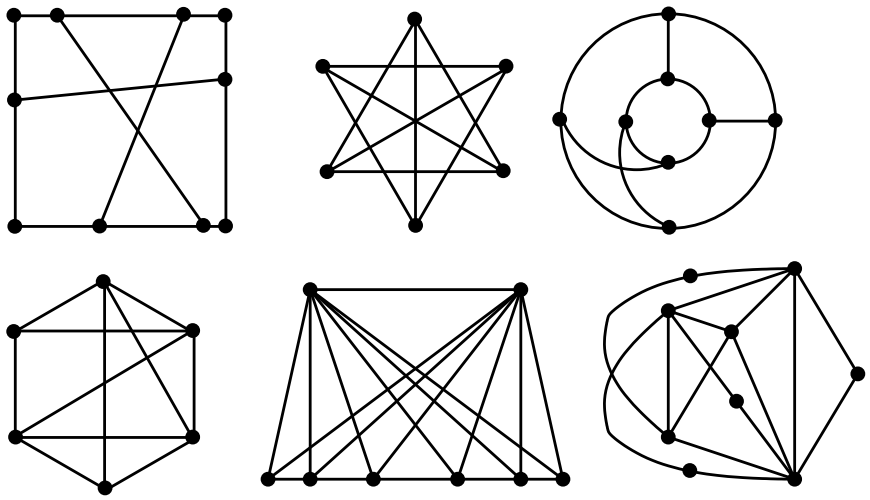
    (b) Bewijs dat het aantal toppen van een fullereen steeds even is.

48. ◐ Toon aan dat je een planaire graaf krijgt als je een willekeurige boog van K_5 verwijdert. Is hetzelfde waar voor $K_{3,3}$?

49. ○ Bepaal voor volgende grafen of ze bipartiet zijn.



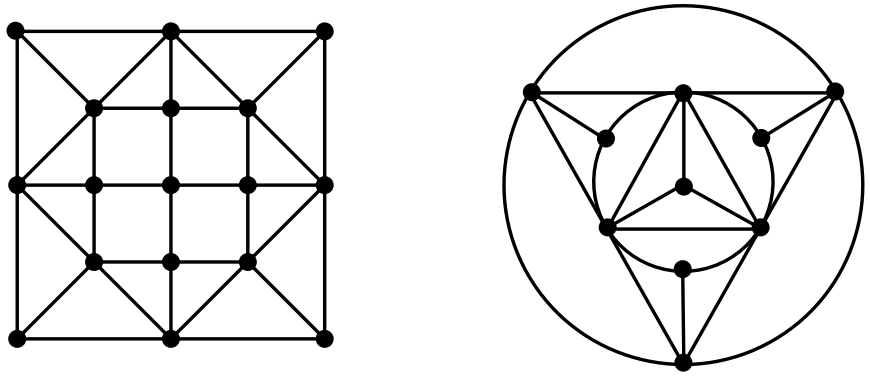
50. ◐ Bepaal welke van de volgende grafen planair is. Teken de planaire grafen zonder dat de bogen snijden. Zoek in de grafen die niet planair zijn een deelgraaf die boogequivalent is met K_5 of $K_{3,3}$.



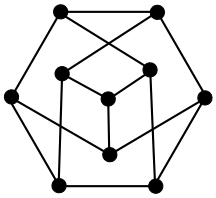
51. ◐ Zij $m, n \in \mathbb{Z}$ met $m \geq n \geq 2$. Hoeveel cycli van lengte 4 zitten in $K_{m,n}$? Hoeveel paden van lengte 2? Hoeveel paden van lengte 3?

52. ◐ Zij $X = \{1, 2, 3, 4, 5\}$. Construeer de lusvrije ongerichte graaf $\mathcal{G}$ als volgt. Elke 2-deelverzameling van X stelt een top van $\mathcal{G}$ voor. Twee toppen zijn met elkaar verbonden als ze corresponderen met disjuncte 2-deelverzamelingen van X. Met welke graaf is $\mathcal{G}$ isomorf?

53. ○ Check de stelling van Euler op volgende grafen.



54. ○ Toon aan dat volgende graaf isomorf is met de Petersengraaf.



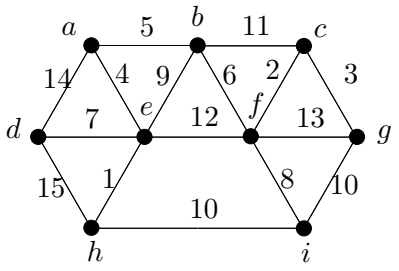
55. ● Gegeven een feestje kunnen we een graaf maken door voor elke deelnemer een top te voorzien en een boog te maken tussen twee mensen die elkaar kennen. Een **volle driehoek** is een deelgraaf van drie toppen die twee per twee verbonden zijn. Hij komt dus overeen met drie mensen waar elk van hen de twee andere kent. Een **lege driehoek** daarentegen is een drietal mensen die elkaar helemaal niet kennen.

    Bewijs volgende stelling.

    > Zij E en F respectievelijk het aantal lege en volle driehoeken in een graaf met N toppen. Dan geldt
    >
    > $$E + F \geqslant \binom{N}{3} - \left\lceil \frac{N}{2} \left\lceil \left(\frac{N-1}{2} \right)^2 \right\rceil \right\rceil$$

    Toon ook aan dat deze grens scherp is voor alle $N \in \mathbb{N}_0$

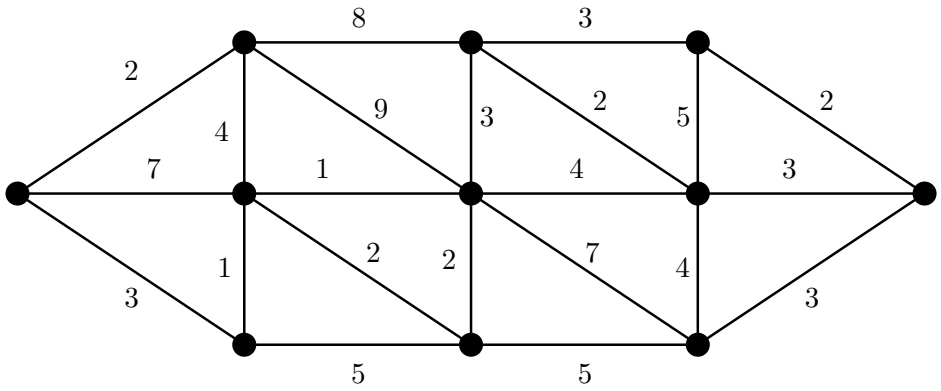
56. ◐ Bepaal een opspannende boom van minimaal gewicht voor onderstaande graaf. Hoeveel opspannende bomen heeft deze graf?



    [examen januari 2005]

57. ◐ Bewijs dat elk gesloten circuit in de graaf van oefening 54 minstens lengte 5 heeft. Gebruik dit samen met de stelling van Euler om aan te tonen dat deze graaf niet planair is.

58. ◐ Vind een opspannende boom met minimaal gewicht in volgende graaf. Geef ook zijn gewicht en de volgorde in dewelke je de bogen vindt.

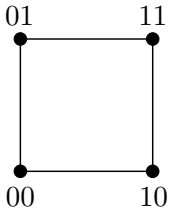


[examen augustus 2005]

59. ◐ Zij $d \in \mathbb{N}_0$ en stel

$$V_d = \{\text{alle woorden van lengte } d \text{ gevormd met de tekens 0 en 1}\}$$

De graaf Q_d heeft toppenverzameling V_d en bogen tussen toppen die juist in één letter verschillen. Hiernaast zien we bijvoorbeeld Q_2



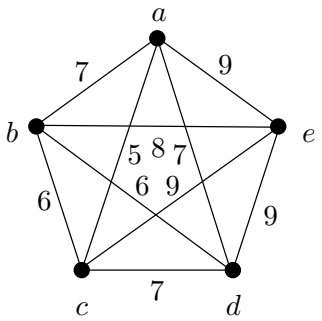
(a) Teken Q_1 en Q_3.

(b) Toon aan dat Q_d steeds bipartiet is.

(c) Heeft Q_d voor alle waarden van d een koppeling die alle toppen bevat? Staaf uw antwoord.

[examen augustus 2005]

60. ◐ Bepaal een opspannende boom van minimaal gewicht in nevenstaande graaf. Geef ook zijn gewicht.



[examen augustus 2006]

61. ◐ Zij $\mathcal{G}$ een planaire graaf. Bewijs dat $\mathcal{G}$ bipartiet is als en slechts als $\mathcal{G}^*$ Euleriaans is. [examen augustus 2006]

62. ◐ Beschouw nevenstaande graaf en noteer hem $\mathcal{G}$.

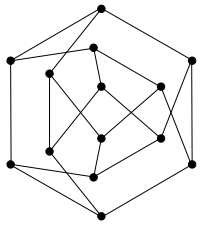
    (a) Is dit een Eulergraf? Verklaar.

    (b) Toon aan dat $\mathcal{G}$ bipartiet is door hem over te tekenen op je antwoordblad en de toppen zó te nummeren dat toppen enkel kunnen adjacent zijn als hun nummers niet allebei even of oneven zijn.

    (c) Vind een maximumkoppeling in $\mathcal{G}$. Is dit een volledige koppeling?

    (d) Wat is de lengte van de kortste cycli in $\mathcal{G}$?

    (e) Is deze graaf planair? Geef een bewijs.



[examen januari 2006]

Hoofdstuk 5

Genererende functies

In dit hoofdstuk nemen we de methode van inclusie en exclusie (zie paragraaf 2.5) nog eens onder de loupe.

5.1 Voorbeelden en definitie

Eerste voorbeeld

Een moeder koopt 12 snoepjes en wil die verdelen onder haar drie kinderen: Piet, Andres en Jan. Wèl zó dat Piet er minstens 4 krijgt, Andres en Jan minstens 2 en Jan hoogstens 5.

Noteren we c_P, c_A en c_J voor het aantal snoepjes dat Piet, Andres en Jan respectievelijk krijgen, hebben we $c_P + c_A + c_J = 12$ en $c_P \geqslant 4$, $c_A \geqslant 2$ en $5 \geqslant c_J \geqslant 2$.

We kunnen alle oplossingen opschrijven:

c_P	4	4	4	4	5	5	5	5	6	6	6	7	7	8
c_A	3	4	5	6	2	3	4	5	2	3	4	2	3	2
c_J	5	4	3	2	5	4	3	2	4	3	2	3	2	2

We hebben dus 12 op alle mogelijke manieren geschreven als som van drie natuurlijke getallen die voldoen aan de voorwaarden. Dit doen we eigenlijk ook als we de distributiviteit toepassen bij het uitwerken van volgend product van veeltermen :

$$(x^4 + x^5 + x^6 + x^7 + x^8)(x^2 + x^3 + x^4 + x^5 + x^6)(x^2 + x^3 + x^4 + x^5) \quad (5.1)$$

De eerste factor komt overeen met het feit dat de toegelaten waarden voor c_P enkel 4, 5, 6, 7 en 8 zijn. De tweede factor ontstaat uit de opmerking dat een oplossing steeds een c_A zal hebben in $\{2, 3, 4, 5, 6\}$.

In het product (5.1) komt de coëfficiënt van x^{12} overeen met alle mogelijke manieren om x^{12} te bekomen door een term te nemen in elk van de drie factoren. Dus is de oplossing van het vraagstuk ook de coëfficiënt van x^{12} in het product (5.1) van veeltermen.

Tweede voorbeeld

We hebben grote hoeveelheden knikkers van vier kleuren : rood, groen, wit en zwart. Op hoeveel manieren kan je 24 knikkers kiezen zó dat er een even aantal witte is en minstens 6 zwarte.

We maken een veelterm die een factor heeft voor elke kleur. Op de rode of groene knikkers is er geen beperking : er kunnen geen, 1, 2, ..., 17 of 18 (niet meer want minstens 6 knikkers zijn zwart) knikkers zijn van die kleur. Dit geeft voor beide kleuren een factor $(1+x+x^2+\cdots+x^{18})$. De factor van de witte knikkers bevat enkel even machten : $(1+x^2+x^4+\cdots+x^{18})$. Aangezien er minstens 6 zwarte knikkers zijn, krijgen we een factor $(x^6+x^7+\cdots+x^{24})$.

Het antwoord op de vraag is dus gelijk aan de coëfficiënt van x^{24} in het product

$$\left(1+x+x^2+\cdots+x^{18}\right)^2\left(1+x^2+x^4+\cdots+x^{18}\right)\left(x^6+x^7+\cdots+x^{24}\right).$$

Het is tijd voor een definitie.

Definitie 46. *Zij $a_0, a_1, a_2, \ldots$ een rij van reële getallen. De* ***genererende functie*** *voor die rij is per definitie*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum_{i=0}^{\infty} a_ix^i$$

Voorbeeld. De genererende functie van de rij $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}, 0, 0, \ldots$ is $\sum_{i=0}^{n}\binom{n}{i}x^i = (1+x)^n$.

Voorbeeld. We weten zeer goed dat $(1-x)(1+x+x^2+\cdots+x^n) = 1-x^{n+1}$, waaruit volgt

$$\frac{1-x^{n+1}}{1-x} = 1+x+x^2+\cdots+x^n.$$

Bijgevolg is $\frac{1-x^{n+1}}{1-x}$ een genererende functie voor de rij $\underbrace{1, 1, 1, \ldots, 1}_{n+1 \text{ keer}}, 0, 0, \ldots$.

Voorbeeld. Ook de rij $1, 1, 1, \ldots$ kunnen we genereren omdat $(1-x)(1+x+x^2+\cdots) = 1$ (voor $\mid x \mid < 1$) zodat

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots \tag{5.2}$$

Als we beide leden afleiden krijgen we

$$\frac{1}{(1-x)^2} = 0 + 1 + 2x + 3x^2 + \cdots \tag{5.3}$$

zodat $1/(1-x)^2$ een genererende functie is voor de rij $1, 2, 3, \ldots$

Als we nu beide leden van (5.3) vermenigvuldigen met x, krijgen we

$$\frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + \cdots \tag{5.4}$$

zodat $x/(1-x)^2$ een genererende functie is voor de rij $0, 1, 2, 3, \ldots$.

Nog eens beide leden van (5.4) afleiden geeft

$$\frac{1+x}{(1-x)^3} = 1 + 2^2x + 3^2x^2 + \cdots$$

zodat deze functie de rij $1^2, 2^2, 3^2, \ldots$ genereert.

We zien nu ook gemakkelijk dat

$$x(1+x)/(1-x)^3 \tag{5.5}$$

de rij $0^2, 1^2, 2^2, \ldots$ genereert.

Voorbeeld. Willen we nu de rij $1, 1, 0, 1, 1, 1, \ldots$ genereren, starten we met (5.2) en trekken we gewoon x^2 af. We hebben inderdaad

$$\frac{1}{1-x} - x^2 = 1 + x + x^3 + x^4 + \cdots$$

Analoog genereert $1/(1-x) + 2x^3$ de rij $1, 1, 1, 3, 1, 1, \ldots$

5.2 Veralgemeende binomiaalcoëfficiënten

Wat is het volgende getal in de rij $0, 2, 6, 12, 20, 30, 42, ?$

Merk op dat

$$\begin{aligned} a_0 &= 0 + 0^2 \\ a_1 &= 1 + 1^2 \\ a_2 &= 2 + 2^2 \\ a_3 &= 3 + 3^2 \\ &\vdots \end{aligned}$$

De genererende functie van die rij kunnen we nu gemakkelijk opstellen door (5.4) en (5.5) te combineren:

$$\frac{x(1+x)}{(1-x)^3} + \frac{x}{(1-x)^2} = \frac{2x}{(1-x)^3}$$

Het antwoord is dus de coëfficiënt van x^7 in $2x/(1-x)^3$. Hoe bepalen we die coëfficiënt?

We breiden het begrip binomiaalcoëfficiënt uit.

We weten dat voor $n, r \in \mathbb{N}_0$ geldt

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}$$

Definitie 47. *We stellen nu per definitie voor alle niet-nulle natuurlijke getallen n en r*

$$\binom{-n}{r} := \frac{(-n)(-n-1)(-n-2)\cdots(-n-r+1)}{r!}.$$

Dan geldt

$$\begin{aligned}\binom{-n}{r} &= (-1)^r \frac{n(n+1)(n+2)\cdots(n+r-1)}{r!} \\ &= (-1)^r \frac{(n+r-1)!}{r!(n-1)!} \\ &= (-1)^r \binom{n+r-1}{r}\end{aligned}$$

We stellen ook $\forall n \in \mathbb{Z}$: $\binom{n}{0} := 1$.

Uit de analyse weet je dat de McLaurin-reeks voor $(1+x)^{-n}$ gelijk is aan

$$1 + (-n)x + \frac{(-n)(-n-1)}{2!}x^2 + \frac{(-n)(-n-1)(-n-2)}{3!}x^3 + \cdots$$

zodat

$$(1+x)^{-n} = \sum_{r=0}^{\infty} \binom{-n}{r} x^r.$$

Dit is een veralgemening van het binomium van Newton. Nog anders gezegd : $(1+x)^{-n}$ is een genererende functie voor $\binom{-n}{0}, \binom{-n}{1}, \binom{-n}{2}, \ldots$.

We passen dit nieuw begrip toe.

Voorbeeld. Bepaal de coëfficiënt van x^5 in $(1-2x)^{-7}$?

Pas het veralgemeend binomium van Newton toe :

$$(1+(-2x))^{-7} = \sum_{r=0}^{\infty} \binom{-7}{r} (-2x)^r$$

Dus is de coëfficiënt die we zoeken gelijk aan

$$\binom{-7}{5}(-2)^5 = (-32)(-1)^5\binom{11}{5} = 14784.$$

Voorbeeld. Op hoeveel manieren kunnen we 24 snoepjes verdelen onder 4 kinderen zodat iedereen minstens 3 snoepjes krijgt en hoogstens 8?

De genererende functie is

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

en we zoeken de coëfficiënt van x^{24}. We hebben

$$f(x) = x^{12}(1+x+x^2+x^3+x^4+x^5)^4 = x^{12}\left(\frac{1-x^6}{1-x}\right)^4$$

zodat we eigenlijk de coëfficiënt van x^{12} in $\left(\frac{1-x^6}{1-x}\right)^4$ nodig hebben. Dit is niet moeilijk :

$$\begin{aligned}\left(\frac{1-x^6}{1-x}\right)^4 &= (1-x^6)^4(1-x)^{-4} \\ &= \left[1-\binom{4}{1}x^6+\binom{4}{2}x^{12}-\binom{4}{3}x^{18}+\binom{4}{4}x^{24}\right]\left[\binom{-4}{0}+\binom{-4}{1}(-x)+\binom{-4}{2}(-x)^2+\cdots\right]\end{aligned}$$

zodat de coëfficiënt van x^{12} gelijk is aan

$$\binom{15}{12} - \binom{4}{1}\binom{9}{6} + \binom{4}{2}\cdot 1 = 125$$

Voorbeeld. Op hoeveel manieren kan je een deelverzameling van [15] met 4 elementen kiezen zodanig dat er geen twee opeenvolgende getallen inzitten?

Zulk een verzameling is bijvoorbeeld $\{1,3,7,10\}$. We merken op dat de verschillen

$$\begin{aligned}1-1 = 0 &=: c_1 \\ 3-1 = 2 &=: c_2 \\ 7-3 = 4 &=: c_3 \\ 10-7 = 3 &=: c_4 \\ 15-10 = 5 &=: c_5\end{aligned}$$

als som 14 hebben. Dit blijkt algemeen zo te zijn zodat de vraag kan geformuleerd worden als "vind alle getallen $c_1, c_2, c_3, c_4, c_5 \in [15]$ met $c_1+c_2+c_3+c_4+c_5 = 14$ en $0 \leqslant c_1, c_5$ en $2 \leqslant c_2, c_3, c_4$." Het volstaat dus om de coëfficiënt van x^{14} te bepalen in

$$\begin{aligned} f(x) &= (1 + x + x^2 + x^3 + \cdots)^2(x^2 + x^3 + x^4 + \cdots)^3 \\ &= x^6(1 - x)^{-5} \end{aligned}$$

De coëfficiënt van x^8 in $(1 - x)^{-5}$ is $\binom{-5}{8}(-1)^8$. Het antwoord is dus 495.

5.3 Partities van natuurlijke getallen

Een bekende waspoederfabrikant wil reclame maken via de televisie. Hij kan bij een bepaalde zender reclamespots kopen van 15, 30 en 60 seconden. Op hoeveel manieren kan hij zendtijd kopen als hij in totaal n minuten reclame wil maken?

Laat ons 15 seconden als tijdseenheid beschouwen. Dan is het antwoord het aantal mogelijke combinaties van natuurlijke getallen a, b en c zodanig dat $a + 2b + 4c = 4n$. De genererende functie die hiermee overeen komt is

$$\begin{aligned} f(x) :=& (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^4 + x^8 + \cdots) \\ =& \frac{1}{1 - x} \cdot \frac{1}{1 - x^2} \cdot \frac{1}{1 - x^4} \end{aligned}$$

Het antwoord vinden we terug als de coëfficiënt van x^{4n} in $f(x)$. We merken ook op dat dit antwoord het aantal manieren is om het natuurlijk getal $4n$ te schrijven als som van enen, tweeën en vieren.

Definitie 48. *Een **partitie** van een niet-nul natuurlijk getal n is een schrijfwijze van n als som van niet-nulle natuurlijke getallen.*

Voorbeeld. $11 = 4 + 3 + 3 + 1$

Opmerking. Een partitie (zie Definitie 14 op blz. 57) van een eindige verzameling V geeft aanleiding tot een partitie van het natuurlijk getal $|V|$.

Voorbeeld. Op hoeveel manieren kunnen we 6 schrijven als som van niet-nulle natuurlijke getallen?

Dit komt neer op het tellen van de partities van het getal 6. We schrijven ze eens alle neer.

1+1+1+1+1+1	2+2+2
1+1+1+1+2	1+5
1+1+1+3	2+4
1+1+2+2	3+3
1+1+4	6
1+2+3	

Er zijn in totaal dus 11 manieren.

Notatie. We noteren het aantal partities van een natuurlijk getal n met $p(n)$.
Ga zelf na dat $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$ en $p(5) = 7$.
Kunnen we voor $p(n)$ een genererende functie vinden? Het antwoord is JA!

We kunnen bijvoorbeeld $p(10)$ vinden als de coëfficiënt van x^{10} in het product

$$\underbrace{(1 + x + x^2 + \cdots)}_{\text{voor de enen}}\underbrace{(1 + x^2 + x^4 + \cdots)}_{\text{voor de tweeën}} \cdots \underbrace{(1 + x^{10} + x^{20} + \cdots)}_{\text{voor de tienen}}$$
$$= \frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdot \cdots \cdot \frac{1}{1-x^{10}}$$
$$= \prod_{i=1}^{10} (1 - x^i)^{-1}$$

Hoeveel partities van 6 hebben alle termen verschillend?
Uit het voorbeeld hoger halen we dat dit aantal 4 is. We schrijven $p_{\neq}(6) = 4$.
In het algemeen hebben we een genererende functie

$$P_{\neq}(x) = (1 + x)(1 + x^2) \cdots = \prod_{i=1}^{\infty} (1 + x^i)$$

Hoeveel partities van 6 gebruiken enkel oneven termen?
We zien weer uit ons voorbeeld dat dit aantal 4 is. We schrijven $p_o(6) = 4$.
Dit is juist evenveel als $p_{\neq}(6)$. Is dit toeval?

Stelling 57. *Voor elk niet-nul natuurlijk getal n geldt $p_{\neq}(n) = p_o(n)$.*

Bewijs. De genererende functie voor $p_o(n)$ is

$$\begin{aligned} P_o(x) &= (1 + x + x^2 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots \\ &= \frac{1}{1-x} \cdot \frac{1}{1-x^3} \cdot \cdots \end{aligned}$$

Merk op dat

$$1 + x = \frac{1-x^2}{1-x}, 1 + x^2 = \frac{1-x^4}{1-x^2}, \ldots$$

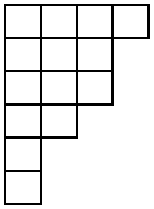
zodat

$$\begin{aligned} P_{\neq}(x) &= (1 + x)(1 + x^2)(1 + x^3)\cdots \\ &= \frac{\cancel{1-x^2}}{1-x} \cdot \frac{\cancel{1-x^4}}{\cancel{1-x^2}} \cdot \frac{1-x^6}{1-x^3} \cdot \frac{1-x^8}{\cancel{1-x^4}} \cdot \cdots \\ &= P_o(x) \end{aligned}$$

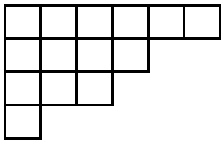
Vermits de genererende functies gelijk zijn, zijn ook de gegenereerde rijen gelijk. □

Een **Young tableau** is een grafische voorstelling van een partitie. Je schrijft vierkantjes op rijen om de verschillende termen van de partitie in dalende grootte op te geven:

14 = 4 + 3 + 3 + 2 + 1 + 1



Als je dit "transponeert", krijg je



14 = 6 + 4 + 3 + 1

Deze methode bewijst dat het aantal partities van n met m termen gelijk is aan het aantal partities van n waarbij de grootste term m is.

5.4 Beroemde genererende functies

We beëindigen dit hoofdstuk met een lijst van nuttige genererende functies.

Voor elke $n, m \in \mathbb{N}$ en elke $a \in \mathbb{R}$ geldt

- $(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = \sum_{i=0}^{n}\binom{n}{i}x^i$;
- $\frac{1-x^{n+1}}{1-x} = 1 + x + x^2 + \cdots + x^n = \sum_{i=0}^{n} x^i$;
- $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i$;
- $$\begin{aligned}\frac{1}{(1+x)^n} &= \binom{-n}{0} + \binom{-n}{1}x + \binom{-n}{2}x^2 + \cdots \\ &= \sum_{i=0}^{\infty}\binom{-n}{i}x^i \\ &= 1 + (-1)\binom{n+1-1}{1}x + (-1)^2\binom{n+2-1}{2}x^2 + \cdots \\ &= \sum_{i=0}^{\infty}(-1)^i\binom{n+i-1}{i}x^i\end{aligned}$$
- $$\begin{aligned}\frac{1}{(1-x)^n} &= \binom{-n}{0} + \binom{-n}{1}(-x) + \binom{-n}{2}(-x)^2 + \cdots \\ &= \sum_{i=0}^{\infty}\binom{-n}{i}(-x)^i \\ &= 1 + (-1)\binom{n+1-1}{1}(-x) + (-1)^2\binom{n+2-1}{2}(-x)^2 + \cdots \\ &= \sum_{i=0}^{\infty}\binom{n+i-1}{i}x^i\end{aligned}$$

5.5 Oefeningen

1. ◐ Bepaal het aantal oplossingen met gehele getallen voor $c_1 + c_2 + c_3 + c_4 + c_5 = 30$ met $2 \leqslant c_1 \leqslant 4$ en $3 \leqslant c_i \leqslant 8$ voor $i \in \{2, 3, 4, 5\}$.

2. ◐ Bepaal de genererende functie voor het aantal manieren om € 35 te verdelen onder 5 kinderen

   (a) als er geen restricties zijn;

   (b) als elk kind minstens € 1 krijgt;

   (c) als elk kind minstens € 2 krijgt;

   (d) als het oudste kind minstens € 10 krijgt;

   (e) als de jongste twee kinderen elk minstens € 10 krijgen.

3. ◐

   (a) Zoek de genererende functie voor het aantal manieren om 10 chocoladerepen te kiezen uit (een grote hoeveelheid van) 6 soorten.

   (b) Zoek de genererende functie voor het aantal manieren om r voorwerpen te kiezen uit n verschillende voorwerpen (waarbij je verschillende keren hetzelfde voorwerp kan kiezen).

4. ○ Zoek de genererende functie voor het aantal manieren om n eurocent te hebben in 'koperen' muntjes (1, 2 en 5 eurocent).

5. ◐ Gebruik genererende functies om het aantal manieren te tellen om 100€ te wisselen in

   (a) biljetten van 10, 20 en 50€ ;

   (b) biljetten van 5, 10, 20 en 50€ ;

   (c) biljetten van 5, 10 en 20 € , waarbij je elke soort minstens één en hoogstens 4 keer gebruikt.

6. ○ Zoek genererende functies voor de volgende rijen getallen

   (a) $\binom{8}{0}, \binom{8}{1}, \ldots, \binom{8}{8}$

   (b) $\binom{8}{1}, 2\binom{8}{2}, \ldots, 8\binom{8}{8}$

   (c) $1, -1, 1, -1, \ldots$

   (d) $0, 0, 0, 6, -6, 6, -6, \ldots$

   (e) $1, 0, 1, 0, 1, 0, \ldots$

   (f) $0,\ 0,\ 1,\ a,\ a^2,\ a^3,\ \ldots$ (met $a \neq 0$)

7. ○ Bepaal de rij die gegenereerd wordt door volgende functies

   (a) $f(x) = (2x-3)^3$
   (b) $f(x) = x^3/(1-x^2)$
   (c) $f(x) = 1/(3-x)$
   (d) $f(x) = 1/(1-x) + 3x^7 - 11$
   (e) $f(x) = x^4/(1-x)$
   (f) $f(x) = 1/(1+3x)$

8. ○ Stel dat f en g de genererende functies zijn van $a_0, a_1, \ldots$ en $b_0, b_1, b_2, \ldots$ respectievelijk. Druk g uit in termen van f als

   (a) $b_3 = 3$ en $b_i = a_i$ voor $i \in \mathbb{N} \setminus \{3\}$
   (b) $b_3 = 3$, $b_7 = 7$ en $b_i = a_i$ voor $i \in \mathbb{N} \setminus \{3, 7\}$
   (c) $b_1 = 1$, $b_3 = 3$ en $b_i = 2a_i$ voor $i \in \mathbb{N} \setminus \{1, 3\}$
   (d) $b_1 = 1$, $b_3 = 3$, $b_7 = 7$ en $b_i = 2a_i + 5$ voor $i \in \mathbb{N} \setminus \{1, 3, 7\}$

9. ○ Zoek de coëfficiënt van x^7 in

   (a) $(1 + x + x^2 + \cdots)^{15}$
   (b) $(1+x+x^2+\cdots)^n$, voor $n \in \mathbb{N}$

10. ○ Zoek de coëfficiënt x^{53} in $(x^7 + x^8 + \cdots)^6$.

11. ○ Zoek de coëfficiënt van x^{12} in $(x^2 + x^3 + x^4 + x^5 + x^6)^5$.

12. ◐ Bepaal de coëfficiënt van x^n in $\frac{1}{1-10x+21x^2}$.

13. ○ Twee bakken frisdrank, 24 flesjes Cola en 24 flesjes limo, worden verdeeld onder 5 testpersonen die een smaaktest ondergaan. Op hoeveel manieren kan dat gebeuren als

    (a) elke testpersoon minstens 2 flesjes van elk moet krijgen;
    (b) elke testpersoon minstens 2 flesjes Cola en 3 flesjes limo moet krijgen?

14. ◐ Als je een dobbelsteen 12 maal werpt, wat is dan de kans dat de som van de uitkomsten 30 is?

15. ○ Zoek de genererende functie voor het aantal manieren waarop een verkoper van een tv-station n minuten zendtijd kan verkopen als er verkocht wordt in blokken van 30, 60 of 120 seconden.

16. ○ Zoek alle partities van 7.

17. ◐ Wat is de genererende functie voor het aantal partities van $n \in \mathbb{N}$ als

(a) elk getal niet meer dan 5 keer mag voorkomen;

(b) elk getal niet groter mag zijn dan 12 en niet meer dan 5 keer mag voorkomen.

18. ◐ Gebruik genererende functies om het aantal oplossingen met gehele getallen te bepalen voor

$$c_1 + c_2 + c_3 + c_4 + c_5 + c_6 = 33,$$

waarbij $0 \leq c_1, c_2 \leq 10$, $c_3, c_4, c_5, c_6 > 3$. [examen augustus 2005]

19. ◐ In de Vrije Universiteit van Buenos Aires gaat professor Mendoza als volgt te werk bij het verbeteren van de examens in de 2de zittijd. Hij wil aan de 15 studenten die herexamen doen in totaal precies 150 punten geven. Als een student minder dan 4 op 20 heeft gaat die naar de ombudsman, en daar wil Mendoza niets mee te maken hebben. Maar zelf vindt hij dat geen van de studenten meer dan 14 op 20 verdient. Op hoeveel manieren kan hij de studenten punten geven binnen deze beperkingen? NB. Mendoza geeft enkel gehele punten en raadt u aan genererende functies te gebruiken. [examen augustus 2006]

Hoofdstuk 6

Recurrentievergelijkingen

In dit hoofdstuk gaan we verder met de studie van rijen. In het voorgaande hoofdstuk hebben we met rijen formele machtreeksen geassocieerd die zeer handig bleken bij het oplossen van telproblemen. Deze genererende functies werden voor het eerst ingevoerd door Abraham De Moivre in 1718 toen hij een exacte formule in functie van $n \in \mathbb{N}$ (zoals $a_n = 3n + 2$ of $b_n = (n + 1)(n + 2)(n + 3)$) wou voor de $n$de (of *algemene*) term van een rij die gegeven wordt door een zogenaamde **recurrentie relatie**. Hierbij wordt de rij gegeven door enkele begintermen en dan een **recursieve definitie** die a_n uitdrukt als functie van voorgaande termen, dus

$$a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k}), \quad n \geq k. \tag{6.1}$$

Voorbeeld. $a_0 = 1, a_1 = 1$ en $a_n = a_{n-2} + a_{n-1}$ voor de rij $1, 1, 2, 3, 5, 8, 13, \ldots$

We zullen nu onderzoeken wanneer zulke recursieve definitie kan 'vertaald' worden in een formule voor de algemene term a_n die enkel afhangt van n.

6.1 Homogene eerste orde lineaire recurrentievergelijkingen

Indien we aannemen dat elk jaar de wereldbevolking met 3% toeneemt dan voldoet de omvang van de wereldbevolking aan de recurrente betrekking

$$a_n = 1.03 \cdot a_{n-1}, \quad n \geq 1.$$

Deze is van de vorm

$$a_n = r a_{n-1} \tag{6.2}$$

Eerste orde betekent dat a_n enkel afhangt van a_{n-1} en niet van de voorgaande termen in de rij;
lineair wil zeggen dat enkel de eerste macht van a_{n-1} voorkomt, niet a_{n-1}^5 of zo;
homogeen betekent dat a_n naast a_{n-1} niet afhangt van iets anders. Dus niet $a_n = ra_{n-1} + \sin n$ of zo.

Ook hangt r niet af van n. We zeggen dat het hier gaat om een recurrentievergelijking **met constante coëfficiënten**.

Die eerste orde homogene lineaire recurrentierelaties geven eigenlijk *meetkundige rijen*, die we reeds kennen vanuit het secundair onderwijs.

Voorbeeld. Los de vergelijking $a_{n+1} = 3a_n$ op met als **randvoorwaarde** $a_0 = 5$.
We rekenen enkele elementen van de rij uit :

$$\begin{aligned} a_0 &= 5 \\ a_1 &= 3 \cdot 5 = 15 \\ a_2 &= 3 \cdot 15 = 3^2 \cdot 5 \\ a_3 &= 3 \cdot a_2 = 3^3 \cdot 5 \\ &\vdots \end{aligned}$$

We zien dat

$$a_n = 3^n \cdot 5.$$

Stelling 58. *Zij $r \in \mathbb{C}$ en $a_0 \in \mathbb{C}$. De oplossing van de recurrentievergelijking $a_{n+1} = ra_n$ is steeds van de vorm $a_n = r^n a_0$.*

Bewijs. Eenvoudige oefening. □

Voorbeeld. Los de vergelijking $a_n = 7a_{n-1}$ op als je weet dat $a_2 = 98$.
We weten dat $a_n = 7^n a_0$ zodat $a_2 = 7^2 a_0$. Hieruit volgt $a_0 = 2$ en dus $a_n = 7^n \cdot 2$.

Voorbeeld. De vergelijking $a_{n+1}^2 = 5a_n^2$ lijkt op het eerste gezicht niet lineair te zijn. Maar als je de *substitutie* $b_n := a_n^2$ uitvoert, krijg je dat b_n voldoet aan $b_{n+1} = 5b_n$. Als we de beginvoorwaarde $a_0 = 2$ meegeven, vinden we dat $b_n = 5^n b_0$ met $b_0 = 4$. Dus geldt $b_n = 5^n \cdot 4$ zodat de uiteindelijke oplossing $a_n = \left(\sqrt{5}\right)^n \cdot 2$ is.

Voorbeeld. We komen terug op het raadsel van vorig hoofdstuk: vul de rij 0, 2, 6, 12, 20, 30, 42, ... aan.

Neem de verschillen

$$\begin{aligned} a_1 - a_0 &= 2 \\ a_2 - a_1 &= 4 \\ a_3 - a_2 &= 6 \\ a_4 - a_3 &= 8 \\ &\vdots \end{aligned}$$

We zien dus dat $a_n - a_{n-1} = 2n$. Dit is een niet-homogene lineaire eerste orde recurrentievergelijking die we later zullen leren oplossen in het algemeen. Toch kunnen we hier reeds een oplossing bedenken:

$$\begin{aligned} &(a_n - a_{n-1}) + (a_{n-1} - a_{n-2}) + \cdots + (a_2 - a_1) + (a_1 - a_0) \\ = \quad &2n + 2(n-1) + \cdots + 2 \cdot 2 + 2 \cdot 1 \end{aligned}$$

zodat

$$a_n - a_0 = 2(1 + 2 + 3 + \cdots + n),$$

waaruit we vinden dat

$$a_n - 0 = 2 \cdot \frac{n(n+1)}{2}$$

of

$$a_n = n^2 + n.$$

Voorbeeld. Ook met niet-constante coëfficiënten kan gezond verstand tot een oplossing leiden.

$$a_n = n a_{n-1} \qquad \text{met } a_0 = 1$$

geeft onmiddellijk $a_n = n!$.

6.2 Homogene tweede orde lineaire recurrentievergelijkingen

Definitie 49. *Zij $k \in \mathbb{N}_0$ en $0 \neq c_0, c_1, \ldots, c_k \neq 0$ reële getallen en $f : \mathbb{N} \longrightarrow \mathbb{R}$ een functie. Een* ***lineaire recurrentievergelijking van orde*** *k* ***met constante coëfficiënten*** *is een uitdrukking*

$$c_0 a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = f(n).$$

Om een eenduidige oplossing te hebben voor a_n, zijn ***beginvoorwaarden*** *$a_0, a_1, \ldots, a_{k-1}$ nodig. Als $\forall n \in \mathbb{N}$ geldt dat $f(n) = 0$, heet de vergelijking* ***homogeen****.*

Wij concentreren ons op homogene van orde 2:

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0. \tag{6.3}$$

Geïnspireerd door het geval van orde 1 proberen we een oplossing te vinden van de vorm $a_n = cr^n$ voor constanten $c \neq 0$ en $r \neq 0$. We substitueren dit in (6.3) en bekomen

$$c_0 cr^n + c_1 cr^{n-1} + c_2 cr^{n-2} = 0. \tag{6.4}$$

We delen dit alles door $cr^{n-2} \neq 0$ en krijgen

$$c_0 r^2 + c_1 r + c_2 = 0. \tag{6.5}$$

Dit is een kwadratische vergelijking die we de **karakteristieke vergelijking** van de gegeven recurrentievergelijking noemen. De algemene methode voor het oplossen van kwadratische vergelijkingen leert ons dat er drie soorten oplossingen mogelijk zijn, naargelang de discriminant, $c_1^2 - 4c_0c_2$, positief, nul of negatief is. Er zijn dan respectievelijk twee reële oplossingen, één reële wortel met multipliciteit twee of twee complex toegevoegde oplossingen.

We bekijken voorbeelden in elk van deze gevallen om de oplossingsmethode te schetsen.

6.2.1 Twee reële wortels

Voorbeeld. Los volgende recurrentievergelijking op als je weet dat $a_0 = 1$ en $a_1 = 2$.

$$a_n + a_{n-1} - 6a_{n-2} = 0$$

De karakteristieke vergelijking is

$$r^2 + r - 6 = 0 \qquad \Longleftrightarrow \qquad (r-2)(r+3) = 0.$$

De wortels zijn dus 2 en -3. Bijgevolg zijn $a_n = 2^n$ en $a_n = (-3)^n$ oplossingen van de recurrentievergelijking, maar ook alle combinaties

$$a_n = c_1 2^n + c_2 (-3)^n$$

van deze twee zijn oplossingen. De beginvoorwaarden laten ons toe de constanten c_1 en c_2 te expliciteren. We krijgen een stelsel

$$\begin{cases} 1 = a_0 = c_1 \cdot 1 + c_2 \cdot 1 \\ 2 = a_1 = c_1 \cdot 2 + c_2 \cdot (-3) \end{cases}$$

We lossen dit stelsel op:

$$\left\{\begin{array}{rl} c_2 &= 1-c_1 \\ 2 &= 2c_1-3c_2 \end{array}\right. \iff \left\{\begin{array}{rl} c_2 &= 1-c_1 \\ 5c_1 &= 5 \end{array}\right. \iff \left\{\begin{array}{rl} c_2 &= 0 \\ c_1 &= 1 \end{array}\right.$$

Bijgevolg is een oplossing van de recurrentievergelijking, met beginvoorwaarden,

$$a_n = 2^n.$$

Voorbeeld. We stellen nu een formule op voor de beroemde rij van Fibonacci[1]: 0, 1, 1, 2, 3, 5, 8, ... die voldoet aan

$$F_{n+2} = F_{n+1} + F_n \quad \text{met } F_0 = 0 \text{ en } F_1 = 1.$$

De karakteristieke vergelijking is

$$r^2 - r - 1 = 0.$$

De discriminant is 5 zodat we als oplossingen

$$r_+ = \frac{1+\sqrt{5}}{2} \text{ en}$$
$$r_- = \frac{1-\sqrt{5}}{2}$$

vinden. Een algemene oplossing is dus

$$a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

De beginvoorwaarden geven

$$\left\{\begin{array}{rrl} 0 = & F_0 &= c_1 + c_2 \\ 1 = & F_1 &= c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) \end{array}\right. \iff \left\{\begin{array}{rl} c_2 &= -c_1 \\ 1 &= c_1\sqrt{5} \end{array}\right. \iff \left\{\begin{array}{rl} c_1 &= \frac{1}{\sqrt{5}} \\ c_2 &= -\frac{1}{\sqrt{5}} \end{array}\right.$$

zodat

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right). \tag{6.6}$$

[1]Deze getallenrij heet in India de Hemachandrarij, vernoemd naar de twaalfde-eeuwse Indische geleerde Hemachandra (1089–1173). Hij ontdekte deze rij ongeveer een halve eeuw voor Fibonacci (1170–1250) bij de studie van patronen in Indische muziek en Sanskrietgedichten (zie Oefening 8). We merken op dat de rij van Fibonacci ook nog voor Hemachandra gekend was in India: Gopala bestudeerde ze in 1135 en reeds in de 7de eeuw vindt men rijen terug met een Fibonacci-achtig voorschrift ($a_n = a_{n-1} + a_{n-2}$ maar met andere beginwaarden).

Opmerking. Dit is de zogenaamde "Formule van Binet", dezelfde Binet als in de stelling van Cauchy–Binet (zie Appendix A).

Opmerking. Het is verbazend dat Formule (6.6) voor elke waarde van n een geheel getal geeft. Dat ligt aan de zeer speciale eigenschappen van het getal $(1+\sqrt{5})/2$. Dit getal komt nog voor op andere plaatsen in de Wiskunde en in de natuur. Het is de zogenaamde *Gulden snede'* (Engels: "Golden ratio").

Voorbeeld. Voor $n \in \mathbb{N}$ stellen we a_n gelijk aan het aantal deelverzamelingen van $[n]$ die geen opeenvolgende getallen bevatten. De toegelaten deelverzamelingen van $[3]$ zijn bijvoorbeeld $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$ en $\{1,3\}$. Je kan zelf nagaan dat $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $a_3 = 5$ en $a_4 = 8$. We bepalen een recurrentievergelijking voor de rij $(a_n)_n$.

Een toegelaten deelverzameling A van $[n]$ valt in één van volgende gevallen:

1. $n \in A$: dan moet $n-1 \notin A$ en is $A \setminus \{n\}$ een toegelaten deelverzameling voor $[n-2]$. Het aantal deelverzamelingen A in deze situatie is dus a_{n-2};
2. $n \notin A$: dan is A een toegelaten deelverzameling van $[n-1]$. Zo zijn er juist a_{n-1}.

We krijgen dus de recurrentievergelijking

$$a_n = a_{n-1} + a_{n-2}, \qquad \text{met } a_0 = 1 \text{ en } a_1 = 2.$$

Dit lijkt op de Fibonacci-rij F_n uit vorig voorbeeld. We hebben $\forall n \in \mathbb{N}$: $a_n = F_{n+2}$ zodat

$$a_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right]$$

We tonen even dat de methode met de karakteristieke vergelijking ook werkt voor recurrentievergelijkingen van hogere orde.

Voorbeeld. Los op :

$$2a_{n+3} = a_{n+2} + 2a_{n+1} - a_n \qquad \text{met } a_0 = 0, a_1 = 1 \text{ en } a_2 = 2.$$

De karakteristieke vergelijking is

$$2r^3 - r^2 - 2r + 1 = 0.$$

Gelukkig kunnen we deze veelterm op zicht ontbinden tot $(2r-1)(r-1)(r+1)$. De wortels zijn nu duidelijk $\frac{1}{2}$, 1 en -1. Bijgevolg is de oplossing van de vorm

$$a_n = c_1(1)^n + c_2(-1)^n + c_3 \left(\frac{1}{2} \right)^n.$$

Met de beginvoorwaarden vinden we

$$a_n = \frac{5}{2} + \frac{1}{6}(-1)^n - \frac{8}{3}\left(\frac{1}{2}\right)^n.$$

6.2.2 Twee complex toegevoegde wortels

Voor een opfrissing over complexe getallen verwijzen we naar Appendix B.

Aan de hand van de goniometrische vorm van een complex getal kunnen we gemakkelijk machten berekenen, want de stelling van De Moivre zegt

$$\Big(r(\cos\theta + i\sin\theta)\Big)^n = r^n(\cos n\theta + i\sin n\theta)$$

Voorbeeld. Bepaal $(1+\sqrt{3}i)^{10}$.
We bepalen eerst de goniometrische vorm van $1+\sqrt{3}i$. Dat is $2(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3})$. Hieruit volgt

$$\begin{aligned}(1+\sqrt{3}i)^{10} &= 2^{10}(\cos\frac{10}{3}\pi + i\sin\frac{10}{3}\pi)\\ &= 2^{10}(\cos\frac{4}{3}\pi + i\sin\frac{4}{3}\pi)\\ &= 2^{10}(-\frac{1}{2} + \left(-\frac{\sqrt{3}}{2}\right)i)\\ &= -2^9(1+\sqrt{3}i)\end{aligned}$$

Voorbeeld. Los op:

$$a_n = 2(a_{n-1} - a_{n-2}) \qquad \text{met } a_0 = 1 \text{ en } a_1 = 2.$$

De karakteristieke vergelijking is

$$r^2 - 2r + 2 = 0.$$

De discriminant is $4 - 8 = -4 = (2i)^2$ zodat de twee oplossingen $r_+ = 1+i$ en $r_- = 1-i$ zijn. We krijgen dus

$$a_n = c_1(1+i)^n + c_2(1-i)^n$$

als algemene oplossing.

We gaan over naar de goniometrische vorm :

$$\begin{aligned} 1+i &= \sqrt{2}(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}) \\ 1-i &= \sqrt{2}(\cos\frac{\pi}{4}-i\sin\frac{\pi}{4}) \end{aligned}$$

en krijgen

$$\begin{aligned} a_n &= c_1(\sqrt{2})^n(\cos\frac{n\pi}{4}+i\sin\frac{n\pi}{4})+c_2(\sqrt{2})^n(\cos\frac{n\pi}{4}-i\sin\frac{n\pi}{4}) \\ &= (\sqrt{2})^n\left(k_1\cos\frac{n\pi}{4}+k_2\sin\frac{n\pi}{4}\right) \end{aligned}$$

met $k_1 = c_1 + c_2$ en $k_2 = i(c_1 - c_2)$.

De beginvoorwaarden geven

$$\left\{\begin{array}{lll} 1= & a_0 & = k_1 \\ 2= & a_1 & = (\sqrt{2})(k_1\cos\frac{\pi}{4}+k_2\sin\frac{\pi}{4}) \end{array}\right. \iff \left\{\begin{array}{ll} k_1 & = 1 \\ 2 & = 1+k_2 \end{array}\right. \iff \left\{\begin{array}{ll} k_1 & = 1 \\ k_2 & = 1 \end{array}\right.$$

zodat de oplossing $a_n = (\sqrt{2})^n\left(\cos\frac{n\pi}{4}+\sin\frac{n\pi}{4}\right)$ is.

Opmerking. Ook hier is het opmerkelijk dat een formule met vierkantswortels, sinussen en cosinussen steeds leidt tot gehele getallen.

6.2.3 Eén reële wortel met multipliciteit twee

Voorbeeld. Los op:

$$a_{n+2} = 4a_{n+1} - 4a_n \qquad \text{met } a_0 = 1 \text{ en } a_1 = 3.$$

De karakteristieke vergelijking is

$$r^2 - 4r + 4 = 0 \iff (r-2)^2 = 0$$

zodat we als enige oplossing $r = 2$ krijgen. Dus is $a_n = c_1 2^n$ een oplossing. We merken op dat $a_n = n2^n$ ook een oplossing is omdat

$$\begin{aligned} & (n+2)2^{n+2} = 4(n+1)2^{n+1} - 4n2^n \\ \Leftrightarrow\ & 4(n+2) = 8(n+1) - 4n \\ \Leftrightarrow\ & 4n + 8 = 8n + 8 - 4n. \end{aligned}$$

We nemen nu als algemene oplossing

$$a_n = c_1 2^n + nc_2 2^n$$

en bepalen de constanten aan de hand van de beginvoorwaarden :

$$\left\{\begin{array}{lll} 1= & a_0 & = c_1 \\ 3= & a_1 & = 2c_1 + 2c_2 \end{array}\right. \iff \left\{\begin{array}{ll} c_1 & = 1 \\ 3 & = 2 + 2c_2 \end{array}\right. \iff \left\{\begin{array}{ll} c_1 & = 1 \\ c_2 & = \frac{1}{2} \end{array}\right.$$

zodat de oplossing $a_n = 2^n + \frac{1}{2}n2^n = 2^{n-1}(2+n)$ is.

Algemeen

kunnen we zeggen dat we in het geval van een meervoudige wortel r van multipliciteit m voor de karakteristieke veelterm als stuk met r in de algemene oplossing moeten nemen

$$c_0 r^n + c_1 n r^n + c_2 n^2 r^n + \cdots + c_{m-1} n^{m-1} r^n$$

6.3 Niet-homogene recurrentievergelijkingen

We bekijken enkel de gevallen

$$a_n + c a_{n-1} = f(n) \qquad \text{en} \qquad a_n + b a_{n-1} + c a_{n-2} = f(n).$$

De methode bestaat erin om eerst de vergelijking homogeen te maken door nul te schrijven in plaats van $f(n)$. Als $a_n^{(h)}$ de algemene oplossing is voor de **gehomogeniseerde** recurrentievergelijking en $a_n^{(p)}$ is een willekeurige oplossing van de oorspronkelijke recurrentievergelijking die we de **particuliere** oplossing noemen, dan is $a_n^{(h)} + a_n^{(p)}$ de algemene oplossing van de oorspronkelijke recurrentievergelijking.

De methodes die hoger beschreven werden, laten ons toe om $a_n^{(h)}$ te vinden. Voor $a_n^{(p)}$ laten we ons inspireren door de functie $f(n)$ in het rechterlid. We illustreren de methode op twee voorbeelden.

Voorbeeld. Los op:

$$a_n - 3a_{n-1} = 5 \cdot 7^n \qquad \text{met } a_0 = 2.$$

De homogene vergelijking is $a_n = 3a_{n-1}$ zodat $a_n^{(h)} = c \cdot 3^n$. Voor de particuliere oplossing proberen we $a_n^{(p)} := A \cdot 7^n$. Substitutie in de vergelijking geeft

$$\begin{aligned} & A \cdot 7^n - 3A \cdot 7^{n-1} = 5 \cdot 7^n \\ \Leftrightarrow \quad & 7A - 3A = 5 \cdot 7 \text{ zodat } A = \frac{35}{4} \end{aligned}$$

Dus hebben we als algemene oplossing $a_n = c \cdot 3^n + \frac{35}{4} \cdot 7^n$.

We bepalen c met de beginvoorwaarden : $2 = a_0 = c + \frac{35}{4}$ dus $c = -\frac{27}{4}$. De uiteindelijke oplossing is

$$a_n = -\frac{27}{4} \cdot 3^n + \frac{35}{4} \cdot 7^n.$$

Voorbeeld. We krijgen ook een niet-homogene eerste orde recurrentievergelijking voor het beroemde probleem van de torens van Hanoi voor n schijven.

De vergelijking is $a_{n+1} = 2a_n + 1$ met $a_0 = 0$ en we zien direct dat $a_n^{(h)} = c \cdot 2^n$. Als particuliere oplossing proberen we $a_n^{(p)} = A \cdot 1^n$. Substitutie geeft $A = 2A + 1$ zodat $A = -1$ en dus $a_n = c \cdot 2^n - 1$.
De beginvoorwaarde geeft $0 = c - 1$ zodat $c = 1$ en de oplossing wordt dus

$$a_n = 2^n - 1.$$

Voor tweede orde niet-homogene recurrentievergelijkingen verwijzen we naar de oefeningen.

6.4 Beroemde particuliere oplossingen

$f(n)$	$a_n^{(p)}$
c	A
n	$A_1 n + A_0$
n^2	$A_2 n^2 + A_1 n + A_0$
$n^t, t \in \mathbb{N}$	$A_t n^t + A_{t-1} n^{t-1} + \cdots + A_1 n + A_0$
$r^n, r \in \mathbb{R}$	$A r^n$
$n^t r^n$	$r^n (A_t n^t + A_{t-1} n^{t-1} + \cdots + A_1 n + A_0)$

6.5 Een methode met genererende functies

We geven enkel een voorbeeld om de methode te illustreren:

$$a_n - 3a_{n-1} = n, \qquad \text{voor } n \geqslant 1 \text{ en met } a_0 = 1.$$

Deze recurrentievergelijking stelt eigenlijk een oneindig aantal vergelijkingen voor als we alle waarden van n invullen:

$$\begin{aligned} &\text{voor } n = 1 && a_1 - 3a_0 = 1 \\ &\text{voor } n = 2 && a_2 - 3a_1 = 2 \\ &\text{voor } n = 3 && a_3 - 3a_2 = 3 \\ &\vdots && \vdots \end{aligned}$$

We vermenigvuldigen nu de n-de vergelijking met x^n en krijgen

$$\begin{aligned} &\text{voor } n = 1 && a_1 x^1 - 3a_0 x^1 = 1x^1 \\ &\text{voor } n = 2 && a_2 x^2 - 3a_1 x^2 = 2x^2 \\ &\text{voor } n = 3 && a_3 x^3 - 3a_2 x^3 = 3x^3 \\ &\vdots && \vdots \end{aligned}$$

Als we alle vergelijkingen optellen vinden we

$$\sum_{n=1}^{\infty} a_n x^n - 3\sum_{n=1}^{\infty} a_{n-1}x^n = \sum_{n=1}^{\infty} nx^n. \tag{6.7}$$

We stellen $f(x) := \sum_{n=0}^{\infty} a_n x^n$, de genererende functie van $a_0, a_1, a_2, \ldots$ Dan kan vergelijking (6.7) herschreven worden als

$$(f(x) - a_0) - 3x\sum_{n=1}^{\infty} a_{n-1}x^{n-1} = \sum_{n=1}^{\infty} nx^n$$

of

$$f(x) - 1 - 3xf(x) = \sum_{n=0}^{\infty} nx^n.$$

We herinneren ons van het voorbeeld op blz. 127 dat de genererende functie van de rij $0, 1, 2, 3, \ldots$ gelijk is aan $x/(1-x)^2$ zodat

$$f(x) - 3xf(x) = 1 + \frac{x}{(1-x)^2} \qquad \text{of} \qquad f(x) = \frac{1}{1-3x} + \frac{x}{(1-x)^2(1-3x)}$$

We ontbinden de laatste term van $f(x)$ in partieelbreuken :

$$\frac{x}{(1-x)^2(1-3x)} = \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1-3x}$$
$$\Updownarrow$$
$$x = A(1-x)(1-3x) + B(1-3x) + C(1-x)^2$$

zodat we (door $x = 1$, $x = 1/3$ en $x = 0$ te stellen bijvoorbeeld) krijgen

$$f(x) = \frac{-1/4}{1-x} + \frac{-1/2}{(1-x)^2} + \frac{7/4}{1-3x}$$

Nu kunnen we a_n vinden als de coëfficiënt van x^n in $f(x)$. Dit is de som van de coëfficiënten van x^n in de drie termen van $f(x)$.

1. $\frac{-1/4}{1-x} = -\frac{1}{4}(1 + x + x^2 + \cdots)$ zodat de coëfficiënt van x^n hier $-\frac{1}{4}$ is.
2. $\frac{-1/2}{(1-x)^2} = \frac{1}{2}(1-x)^{-2} = -\frac{1}{2}\left(\binom{-2}{0} + \binom{-2}{1}(-x) + \binom{-2}{2}(-x)^2 + \cdots\right)$ zodat de coëfficiënt van x^n hier $-\frac{1}{2}\binom{-2}{n}(-1)^n = -\frac{1}{2}\binom{2+n-1}{n} = -\frac{1}{2}(n+1)$ is.
3. $\frac{7/4}{1-3x} = \frac{7}{4}(1 + (3x) + (3x)^2 + \cdots)$ zodat de coëfficiënt van x^n hier $\frac{7}{4}3^n$ is.

Bijgevolg hebben we als algemene formule voor $a_n = \frac{7}{4}3^n - \frac{1}{2}n - \frac{3}{4}$.

6.6 Oefeningen

1. ○ Als $(a_n)_n$ een oplossing is van de recurrentierelatie $a_{n+1} - da_n = 0$ met $a_3 = 153/49$ en $a_5 = 1377/2401$, wat is dan d?

2. ● Voor $n > 1$ noemen we een permutatie $p_1, p_2, \ldots, p_n$ van de getallen 1, 2, …, n **ordelijk** als er voor elke $i \in \{1, 2, \ldots, n-1\}$ een $j > i$ bestaat met $|p_j - p_i| = 1$.

   (a) Geef alle ordelijke permutaties van 1, 2;

   (b) idem voor 1, 2, 3 en 1, 2, 3, 4;

   (c) als p_1, p_2, p_3, p_4 en p_5 een ordelijke permutatie is van 1, 2, 3, 4, 5, welke waarden kan p_1 dan hebben?

   (d) Als $n > 1$, dan stellen we met a_n het aantal ordelijke permutaties van 1, 2, …, n voor. Vind een recurrentierelatie voor a_n en los ze op.

3. ◐ Los op : $a_n + 2a_{n-1} + 2a_{n-2} = 0$ voor $n \geqslant 2$, $a_0 = 1$ en $a_1 = 3$.

4. ◐ Zoek een recurrentievergelijking voor het aantal manieren om motors en auto's te parkeren in een rij van n parkeerplaatsen als elke motor 1 plaats en elke auto 2 plaatsen nodig heeft.

5. ◐ Als $a_0 = 0$, $a_1 = 1$, $a_2 = 4$ en $a_3 = 37$ aan de vergelijking $a_{n+2} + ba_{n+1} + ca_n = 0$ voldoen, met $n \geqslant 0$ en b, c constant, zoek dan b en c en los de recurrentievergelijking op.

6. ● Een alfabet Σ bevat 4 cijfers $1, 2, 3, 4$ en 7 letters a, b, c, d, e, f, g. Zoek een recurrentierelatie voor het aantal woorden van lengte n zonder opeenvolgende letters. Los ze op.

7. ● Toon aan dat twee opeenvolgende Fibonacci getallen relatief priem zijn.

8. ◐ In de 12de eeuw bestudeerde de Indische geleerde Hemachandra het volgende probleem. Een muziekinstrument kan lange en korte tonen produceren. Een lange toon duurt twee tijdeenheden en een korte één. Vind een recurrentievergelijking voor het aantal manieren waarop je n tijdeenheden kunt opvullen met korte en/of lange tonen. [Hint: voorbeeld op pagina 142.]

9. ● Gebruik een recurrentierelatie om de formule voor $\sum_{i=0}^{n} i^2$ af te leiden.

10. ◐ Gegeven is een rij $(a_n)_{n\in\mathbb{N}}$ met $a_0 = 1$ en

$$a_{n+1} = \begin{cases} 2a_n & \text{indien } n \text{ even is} \\ 2a_n + 1 & \text{indien } n \text{ oneven is} \end{cases}$$

Vind een algemene formule voor a_n. [HINT: probeer een formule op te stellen voor a_{n+2}.]

11. ◐ Gegeven is de recurrentie

$$a_{n+1} = 1 + \sum_{i=0}^{n-1} a_i \text{ met } a_0 = 1.$$

Welke bekende rij is $(a_n)_{n\in\mathbb{N}}$?

12. ◐ Los op : $a_{n+2} - 6a_{n+1} + 9a_n = 3(2^n) + (3^n)$, $n \geqslant 0$, $a_0 = 1$, $a_1 = 4$.

13. ◐ Los op : $a_n = 7a_{n-1} - 10a_{n-2}$ met $a_0 = 2$ en $a_1 = 1$.

14. ◐ Los op : $a_n = a_{n-2}$ met $a_0 = 5$ en $a_1 = -1$.

15. ● Los op : $a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 3 + 5n$, $n \geqslant 0$.

16. ● Los de vorige twee oefeningen op met behulp van genererende functies.

17. ◐ Los volgende recurrentievergelijking op:

$$a_n + 2a_{n-1} + 2a_{n-2} = 0 \qquad \text{met } a_0 = 0 \text{ en } a_1 = 3$$

[examen januari 2005]

18. ◐

    (a) Geef alle oplossingen van $a_n = -5a_{n-1} - 6a_{n-2} + 42 \cdot 4^n$.
    (b) Geef de unieke oplossing van deze vergelijking waarvoor geldt $a_1 = 56$ en $a_2 = 278$.

    [examen augustus 2005]

19. ◐ De Lucasgetallen worden bepaald door de vergelijkingen $L_0 = 2$, $L_1 = 1$ en $L_{n+2} = L_{n+1} + L_n$ voor $n \geqslant 0$.

    (a) Geef een formule voor L_n die niet afhangt van Lucasgetallen van andere orde.
    (b) Toon aan: als $n \geqslant 1$ dan geldt $L_n^2 - L_{n-1}L_{n+1} = 5(-1)^n$.

    [examen januari 2006]

Bijlage A

De stelling van Cauchy–Binet

Deze stelling geeft een formule voor het berekenen van de determinant van het product van twee matrices die niet noodzakelijk vierkant zijn.

A.1 Herhaling en notatie voor determinanten

Zij A een matrix. De i-de kolom van A noteren we A_i en het element op rij i en kolom j in als a_{ij}. Bijgevolg hebben we voor elke kolom van A

$$A_i = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{pmatrix}$$

Indien A vierkant is, kunnen we de determinant beschouwen. We herhalen dat de *determinant* van een $(n \times n)$-matrix A gedefinieerd is als de som van alle mogelijke producten (samen met een gepast teken) van n elementen van A zodanig gekozen dat er juist één element is van elke rij en juist één van elke kolom. Met permutaties kunnen we dit kort schrijven als

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\ a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}$$

Hierbij is $\operatorname{sgn}(\sigma)$ het *teken* van de permutatie σ. Dit teken is $+1$ indien σ een even aantal cycli heeft van even lengte en -1 in het andere geval.

Equivalent kunnen we ook zeggen dat $\operatorname{sgn}(\sigma) = +1$ als en slechts als σ kan geschreven worden als de samenstelling van een even aantal verwisselingen.

De determinant kan beschouwd worden als functie van de kolommen:

$$\det\colon ({}^n\mathbb{K})^n \longrightarrow \mathbb{K}\colon (A_1, A_2, \ldots, A_n) \longmapsto \det(A_1, A_2, \ldots, A_n)$$

Eigenschap 17. *De afbeelding* det *is* multilineair *: als een kolom A_i van A kan geschreven worden als lineaire combinatie van zekere kolommen B_1, B_2 tot en met B_k, is* $\det A$ *gelijk aan dezelfde lineaire combinatie van de determinanten van de matrices $(A_1, A_2, \ldots, B_j, \ldots, A_n)$. We hebben dus*

$$\det(A_1, A_2, \ldots, \sum_{j=1}^{k} \beta_j B_j, \ldots, A_n) = \sum_{j=1}^{k} \beta_j \det(A_1, A_2, \ldots, B_j, \ldots, A_n)$$

Eigenschap 18. *De afbeelding* det *is* alternerend *: als twee kolommen van A gelijk zijn, is* $\det A$ *gelijk aan* 0*. Een gevolg is dat het verwisselen van twee kolommen in A het teken van de determinant verandert :*

$$\det(A_1, A_2, \ldots, A_j, \ldots, A_i, \ldots, A_n) = -\det(A_1, A_2, \ldots, A_i, \ldots, A_j, \ldots, A_n)$$

Uit Eigenschap 18 kunnen we nu ook afleiden dat de determinant, bij permutatie van de kolommen volgens σ, verandert van teken zoals $\operatorname{sgn}(\sigma)$. We hebben

$$\det(A_{\sigma(1)}, A_{\sigma(2)}, \ldots, A_{\sigma(n)}) = \operatorname{sgn}(\sigma) \det(A_1, A_2, \ldots, A_n)$$

We noteren de getransponeerde van de matrix A door $A^\top$. Er geldt $\det A^\top = \det A$.

A.2 De stelling

Zij A een $(n \times m)$-matrix en B een $(m \times n)$-matrix. Dan is AB een $(n \times n)$-matrix waarvan we de determinant kunnen berekenen.

Stelling 59 (Cauchy–Binet)**.** *Zij A een $(n \times m)$-matrix en B een $(m \times n)$-matrix met $m \geqslant n$. Er geldt*

$$\det AB = \sum_{1 \leqslant k_1 < k_2 < \cdots < k_n \leqslant m} \det(A_{k_1}, A_{k_2}, \ldots, A_{k_n}) \cdot \det(B_{k_1}^\top, B_{k_2}^\top, \ldots, B_{k_n}^\top)$$

We nemen dus de som over alle mogelijke keuzes van n kolommen uit A en de overeenkomstige rijen van B.

Bewijs. Het element in rij i en kolom j van het product AB wordt gegeven door $\sum_{k=1}^{m} a_{ik}b_{kj}$. De j-de kolom van AB is dus gelijk aan AB_j, het product van A met de j-de kolom van B. Dit product kan ook nog herschreven worden als een lineaire combinatie van de kolommen van A, namelijk $AB_j = \sum_{k=1}^{m} A_k b_{kj}$. Het linkerlid wordt dus

$$\begin{aligned}\det AB &= \det(AB_1, AB_2, \ldots, AB_n)\\ &= \det(\sum_{k_1=1}^{m} A_{k_1} b_{k_1 1}, \sum_{k_2=1}^{m} A_{k_2} b_{k_2 2}, \ldots, \sum_{k_n=1}^{m} A_{k_n} b_{k_n n})\end{aligned}$$

We passen de multilineariteit van de determinant n keer toe.

$$\begin{aligned}\det AB &= \sum_{k_1=1}^{m} b_{k_1 1} \det(A_{k_1}, \sum_{k_2=1}^{m} A_{k_2} b_{k_2 2}, \ldots, \sum_{k_n=1}^{m} A_{k_n} b_{k_n n})\\ &= \sum_{k_1=1}^{m}\sum_{k_2=1}^{m} b_{k_1 1} b_{k_2 2} \det(A_{k_1}, A_{k_2}, \ldots, \sum_{k_n=1}^{m} A_{k_n} b_{k_n n})\\ &\quad\vdots\\ &= \sum_{k_1=1}^{m}\sum_{k_2=1}^{m}\cdots\sum_{k_n=1}^{m} b_{k_1 1} b_{k_2 2}\cdots b_{k_n n} \det(A_{k_1}, A_{k_2}, \ldots, A_{k_n})\end{aligned}$$

Natuurlijk is $\det(A_{k_1}, A_{k_2}, \ldots, A_{k_n}) = 0$ zodra $k_i = k_j$ voor zekere $i \neq j$. Bijgevolg blijven er niet veel niet-nulle termen over in bovenstaande som : enkel de termen waarvoor alle k_i twee aan twee verschillend zijn van mekaar. Zo een term met $k_1, k_2, \ldots, k_n$ allemaal verschillend komt neer op een keuze van n getallen in $[m]$, waarbij de volgorde belang heeft. Bovendien wordt er gesommeerd over alle mogelijke keuzes. We kunnen al deze keuzes bekomen door eerst n getallen $k_1, k_2, \ldots, k_n$ te kiezen met $k_1 < k_2 < \cdots < k_n$ en dan deze te permuteren. We kunnen dus schrijven

$$\begin{aligned}\det AB &= \sum_{1\leqslant k_1<k_2<\cdots<k_n\leqslant m}\ \sum_{\sigma\in S_n} b_{k_{\sigma(1)}1} b_{k_{\sigma(2)}2}\cdots b_{k_{\sigma(n)}n} \det(A_{k_{\sigma(1)}}, A_{k_{\sigma(2)}}, \ldots, A_{k_{\sigma(n)}})\\ &= \sum_{1\leqslant k_1<k_2<\cdots<k_n\leqslant m}\ \sum_{\sigma\in S_n} b_{k_{\sigma(1)}1} b_{k_{\sigma(2)}2}\cdots b_{k_{\sigma(n)}n} \operatorname{sgn}(\sigma) \det(A_{k_1}, A_{k_2}, \ldots, A_{k_n})\\ &= \sum_{1\leqslant k_1<k_2<\cdots<k_n\leqslant m} \det(A_{k_1}, A_{k_2}, \ldots, A_{k_n}) \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{k_{\sigma(1)}1} b_{k_{\sigma(2)}2}\cdots b_{k_{\sigma(n)}n}\end{aligned}$$

Met de definitie van de determinant kunnen we nu verifiëren dat de som $\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{k_{\sigma(1)}1} b_{k_{\sigma(2)}2}\cdots b_{k_{\sigma(n)}n}$ gelijk is aan de determinant van de matrix die bestaat uit de k_1-ste, de k_2-de, ..., de k_{n-1}-de en de k_n-de rij van

B. Deze rijen komen juist overeen met kolommen in de getransponeerde matrix $B^\top$ zodat we uiteindelijk zien dat

$$\det AB = \sum_{1 \leqslant k_1 < k_2 < \cdots < k_n \leqslant m} \det(A_{k_1}, A_{k_2}, \ldots, A_{k_n}) \cdot \det(B_{k_1}^\top, B_{k_2}^\top, \ldots, B_{k_n}^\top)$$

□

Wij pasten in het bewijs van Stelling 40 deze stelling toe in het speciale geval dat $B = A^\top$.

Gevolg 14. *Zij A een $(n \times m)$-matrix met $m \geqslant n$. Er geldt*

$$\det AA^\top = \sum_{1 \leqslant k_1 < k_2 < \cdots < k_n \leqslant m} \det(A_{k_1}, A_{k_2}, \ldots, A_{k_n})^2$$

We nemen dus de som over alle mogelijke keuzes van n kolommen uit A.

Augustin Louis
Cauchy
(1789–1857)

Jacques Philippe
Marie Binet
(1786–1856)

Bijlage B

De complexe getallen

We geven hier een korte herhaling over complexe getallen. Deze worden in de cursus gebruikt bij het oplossen van recurrentievergelijkingen.

B.1 Definities

In de verzameling der reële getallen heeft geen enkel negatief getal een vierkantswortel. Het kwadraat van een reëel getal is namelijk steeds positief.

Men kan $\mathbb{R}$ uitbreiden tot een grotere verzameling waarin elk getal een vierkantswortel heeft. Dit gebeurt als volgt: neem het Cartesisch product $\mathbb{R}^2$, en definieer hierop een optelling en een vermenigvuldiging als volgt:

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

Hieruit volgt in het bijzonder dat

$$(a, 0)(c, 0) = (ac, 0)$$

zodat de elementen van de vorm $(a, 0)$ optellen en vermenigvuldigen als reële getallen. Daarom voeren we de volgende identificatie uit:

$$(a, 0) = a \in \mathbb{R}.$$

Verder zien we dat

$$(0, 1)(0, 1) = (-1, 0) = -1.$$

Het element $(0, 1)$ is dus een vierkantswortel uit -1.

We voeren de volgende notatie in:

$$i = (0, 1)$$

zodat

$$i^2 = -1.$$

We kunnen dus schrijven

$$(a, b) = (a, 0) + b(0, 1) = a + bi$$

en de definitie van de vermenigvuldiging wordt dan

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

Merk ook op dat

$$a + bi = c + di \iff a = c \text{ en } b = d.$$

We noemen $a + bi$ een **complex getal**. a wordt het **reëel gedeelte** van $a + bi$ genoemd. Het getal b heet het **imaginair gedeelte**. Men noteert:

$$\begin{aligned} a &= \mathrm{Re}(a + bi) \\ b &= \mathrm{Im}(a + bi). \end{aligned}$$

De verzameling van de complexe getallen noteert men

$$\mathbb{C} = \{z = a + bi \mid a, b \in \mathbb{R}\}.$$

Merk op dat

$$(a + bi)(a - bi) = a^2 + b^2.$$

$a - bi$ wordt het **complex toegevoegde** van $z = a + bi$ genoemd. Notatie:

$$a - bi = \overline{a + bi} = \overline{z}.$$

Eigenschap 19. $\mathbb{C}$ *is een commutatief lichaam.*

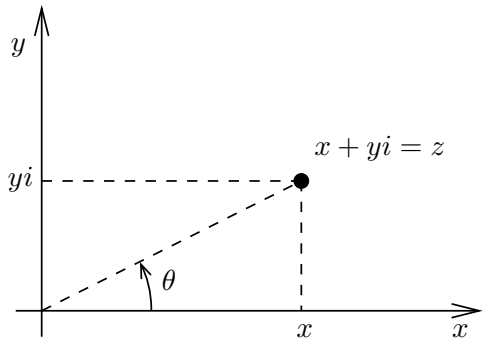
Bewijs. We laten het bewijs over aan de lezer. We merken op dat het inverse voor de vermenigvuldiging gegeven wordt door de formule:

$$(a + bi)^{-1} = \frac{a - bi}{a^2 + b^2}.$$

□

B.2 Meetkundige interpretatie

De verzameling $\mathbb{C}$ van complexe getallen is gelijk aan $\mathbb{R}^2$. We kunnen dus de complexe getallen identificeren met de punten van het vlak. We spreken dan van het *complexe vlak*. Neem een complex getal $z = a + bi$ en bekijk de volgende reële getallen: r, de afstand in het vlak tussen de oorsprong en het punt z, en θ, de hoek tussen de x-as en de rechte door de oorsprong en z (Figuur B.1). Uit de figuur leiden we gemakkelijk af dat



Figuur B.1: Meetkundige voorstelling van een complex getal

$$\begin{cases} x &= r\cos\theta \\ y &= r\sin\theta \end{cases}$$

en

$$r^2 = x^2 + y^2.$$

We kunnen dus schrijven

$$z = r(\cos\theta + i\sin\theta).$$

Men noemt dit de **goniometrische vorm** van het complex getal z. Het getal r heet de **modulus** van z en θ is het **argument**. We noteren de modulus soms ook $|z|$. De getallen r en θ samen noemt men de **poolcoördinaten** van het punt (x, y).

Het grote voordeel van de goniometrische vorm is dat men complexe getallen in goniometrische vorm gemakkelijk kan vermenigvuldigen.

Abraham de Moivre (1667–1754)

Als $z = r(\cos\theta + i\sin\theta)$ en $z' = r'(\cos\theta' + i\sin\theta')$, dan hebben we

$$\begin{aligned} zz' &= rr'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') \\ &= rr'(\cos\theta\cos\theta' - \sin\theta\sin\theta' + i(\cos\theta\sin\theta' + \cos\theta'\sin\theta)) \\ &= rr'(\cos(\theta+\theta') + i\sin(\theta+\theta')) \end{aligned}$$

Gevolg 15 (Stelling van De Moivre)**.** *Voor elk complex getal z geldt*

$$z^n = (r(\cos\theta + i\sin\theta))^n = r^n(\cos n\theta + i\sin n\theta).$$

B.3 De complexe exponentiële functie

Voor $z = x + yi \in \mathbb{C}$ definiëren we

$$e^{x+yi} = \exp(x+yi) = e^x(\cos(y) + i\sin(y)).$$

Dit is het complex getal met poolcoördinaten e^x en y, zodat we onmiddellijk de volgende eigenschap, karakteristiek voor de exponentiële functie, hebben.

Eigenschap 20. *Voor elke z,z' in $\mathbb{C}$ geldt:*

$$e^{z+z'} = e^z e^{z'}$$

en

$$e^{-z} = \frac{1}{e^z}.$$

Opmerking. Uit de definitie van de exponentiële functie volgt de beroemde formule

$$e^{i\pi} = -1.$$

Eigenschap 21. *De complexe exponentiële functie* $\exp : \mathbb{C} \longrightarrow \mathbb{C}_0$ *is surjectief. Verder geldt*

$$e^z = e^{z'} \Longleftrightarrow \exists k \in \mathbb{N} \ : \ z - z' = 2k\pi i.$$

Bewijs. De eerste bewering volgt onmiddellijk uit het voorgaande: neem een complex getal $z = x + yi \neq 0$ en neem de poolcoördinaten r en θ. Dan is

$$z = r(\cos(\theta) + i\sin(\theta)) = e^{\ln(r)+i\theta}.$$

Voor de tweede bewering redeneren we als volgt. Onderstel dat $e^z = e^{z'}$, dan is $e^{z-z'} = 1$. Stel $z - z' = a + bi$, dan is $e^{a+bi} = e^a(\cos(b) + i\sin(b)) = 1$ zodat

$$\begin{cases} e^a\cos(b) & = 1 \\ e^a\sin(b) & = 0. \end{cases}$$

Uit de tweede vergelijking volgt dat $\sin(b) = 0$, waaruit $b = n\pi$ voor een geheel getal n. Substitueren we dit in de eerste vergelijking, dan krijgen we

$$e^a\cos(b) = e^a(-1)^n = 1.$$

Aangezien $e^a \geq 0$ volgt dat n noodzakelijk even is, stel $n = 2k$. Echter, dan is $e^a = 1$, zodat $a = 0$. Bijgevolg is $z - z' = a + bi = 2k\pi i$. □

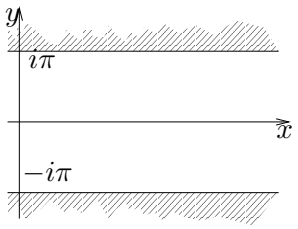
B.4 De logaritmische functie

De exponentiële functie wordt bijectief als we het domein beperken tot een horizontale strip met breedte 2π, zo is bijvoorbeeld

$$\exp : \{z \in \mathbb{C} \mid -\pi < \mathrm{Im}(z) \leq \pi\} \longrightarrow \mathbb{C}_0$$

bijectief. De inverse functie noemt men de **complexe logaritme**

$$\ln : \mathbb{C}_0 \longrightarrow \{z \in \mathbb{C} \mid -\pi < \mathrm{Im}(z) \leq \pi\}.$$



Figuur B.2: Beeld van de complexe logaritme

B.5 De complexe trigonometrische functies

Herneem de definitie van exponentiële functie

$$\begin{cases} e^{ix} & = \cos(x) + i\sin(x) \\ e^{-ix} & = \cos(x) - i\sin(x) \end{cases}$$

Hieruit volgt onmiddellijk dat

$$\begin{cases} \cos(x) & = \frac{e^{ix}+e^{-ix}}{2} \\ \sin(x) & = \frac{e^{ix}-e^{-ix}}{2i} \end{cases}$$

We gebruiken deze formules om de complexe sinus en cosinus te definiëren.

Definitie 50. *Voor elke $z \in \mathbb{C}$ stellen we*

$$\begin{cases} \cos(z) & = \frac{e^{iz}+e^{-iz}}{2} \\ \sin(z) & = \frac{e^{iz}-e^{-iz}}{2i} \end{cases}$$

Op dezelfde manier definiëren we de complexe hyperbolische functies.

Definitie 51. *Voor elke $z \in \mathbb{C}$ stellen we*

$$\begin{cases} \cosh(z) & = \frac{e^{z}+e^{-z}}{2} \\ \sinh(z) & = \frac{e^{z}-e^{-z}}{2} \end{cases}$$

Uit voorgaande definities volgen nu onmiddellijk de volgende betrekkingen:

$$\cosh(iz) = \cos(z) \qquad \sinh(iz) = i\sin(z)$$
$$\cos(iz) = \cosh(z) \qquad \sin(iz) = i\sinh(z)$$

B.6 De complexe n-demachtswortel

Gebruik makende van het voorgaande kunnen we makkelijk volgende eigenschap bewijzen.

Eigenschap 22. *Elk van nul verschillend complex getal c heeft precies n n-demachtswortels in $\mathbb{C}$.*

Bewijs. We zoeken naar complexe getallen z zodat

$$z^n = c$$

Schrijf $c = se^{i\varphi}$ en $z = re^{i\theta}$. Dan wordt de voorgaande betrekking

$$r^n e^{in\theta} = se^{i\varphi}$$

of

$$\begin{cases} r^n & = s \\ n\theta & = \varphi + 2k\pi \end{cases}$$

dus

$$z = \sqrt[n]{s} e^{\frac{\varphi+2k\pi}{n} i}$$

Omdat $e^{2i\pi} = 1$, hoeven we hierin k slechts de waarden $0, 1, 2, \ldots, n-1$ te laten aannemen om alle oplossingen te krijgen. Dit bewijst onze eigenschap. □

B.7 Complexe veeltermen

Een complexe veelterm $P(Z)$ is een uitdrukking van de vorm

$$P(Z) = a_n Z^n + a_{n-1} Z^{n-1} + \cdots a_1 Z + a_0 = \sum_{i=0}^{n} a_i Z^i$$

waarbij de coëfficiënten $a_0, a_1, \ldots, a_n$ complexe getallen zijn. Het symbool Z wordt de **veranderlijke** genoemd. Met elke complexe veelterm $P(Z)$ kunnen we een functie

$$P: \ \mathbb{C} \longrightarrow \mathbb{C}: \ z \mapsto P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

associëren. Deze functie wordt een **complexe veeltermfunctie** genoemd. De graad van een veelterm is de hoogste macht van Z die in deze veelterm voorkomt. Indien $a_n \neq 0$,

$$\mathrm{gr}(\sum_{i=0}^{n} a_i Z^i) = n.$$

De verzameling van alle complexe veeltermen in de veranderlijke Z wordt $\mathbb{C}[Z]$ genoteerd. Net zoals reële veeltermen kan men complexe veeltermen bij elkaar optellen en met mekaar vermenigvuldigen. Dit gebeurt op de voor de hand liggende manier. Deling van veeltermen is niet altijd mogelijk, maar we hebben wel de quotiëntstelling die analoog is aan Stelling 12 die we bewezen voor gehele getallen.

Stelling 60 (quotiëntstelling voor complexe veeltermen)**.** *Beschouw twee complexe veeltermen $M(Z)$ en $N(Z)$, en onderstel dat $N(Z) \neq 0$. Er bestaan twee unieke veelterm $Q(Z)$ en $R(Z)$ die voldoen aan de volgende twee voorwaarden:*

- $M(Z) = Q(Z)N(Z) + R(Z)$;
- $\deg(R) < \deg(N)$.

*Q en R worden respectievelijk het **quotiënt** en de **rest** bij deling van de veelterm M door de veelterm N genoemd.*

Bewijs. We bewijzen eerst de existentie. Dit gebeurt per inductie op de graad van M. Onderstel $\deg(N) = n$. Voor $\deg(M) = 0, 1, \ldots, n-1$ is de stelling waar: het volstaat om $Q = 0$ en $M = R$ te nemen.
Onderstel nu dat de stelling waar is voor $\deg(M) < m$, met m een gegeven getal dat we minstens gelijk aan n mogen onderstellen. We zullen aantonen dat de stelling ook geldt voor $\deg(M) = m$. Stel

$$M(Z) = a_m Z^m + M_1(Z)$$

met $\deg(M_1) < m$. Vanwege de inductiehypothese hebben we dat

$$M_1(Z) = Q_1(Z)N(Z) + R_1(Z)$$

met $\deg(R_1) < n$. Schrijf nu

$$N(Z) = b_n Z^n + N_1(Z)$$

met $\deg(N_1) < n$. Dan is

$$a_m Z^m = \frac{a_m}{b_n} Z^{m-n} N(z) - \frac{a_m}{b_n} Z^{m-n} N_1(z)$$

Merk op dat

$$\deg\left(\frac{a_m}{b_n} Z^{m-n} N_1(z)\right) \leq m - n + n - 1 = m - 1$$

Vanwege de inductiehypothese vinden we dus veeltermen $Q_2(Z)$ en $R_2(Z)$ met $\deg(R_2) < n$ zodat

$$-\frac{a_m}{b_n} Z^{m-n} N_1(z) = Q_2(Z)N(Z) + R_2(Z)$$

Als we de bovenstaande formules met elkaar combineren, vinden we

$$M(Z) = \left(\frac{a_m}{b_n} Z^{m-n} + Q_1(Z) + Q_2(Z)\right) N(Z) + R_1(Z) + R_2(Z)$$

en dit bewijst de existentie.
Voor de uniciteit gaan we als volgt te werk: onderstel dat

$$M(Z) = Q(Z)N(Z) + R(Z) = \widetilde{Q}(Z)N(Z) + \widetilde{R}(Z)$$

met de graden van $R(Z)$ en $\widetilde{R}(Z)$ allebei kleiner dan de graad van $N(Z)$. Dan volgt dat

$$\widetilde{R}(Z) - R(Z) = (Q(Z) - \widetilde{Q}(Z))N(Z)$$

Als $Q(Z) \neq \widetilde{Q}(Z)$, dan is de graad van het rechterlid tenminste gelijk aan de graad van N. De graad van het linkerlid is echter strikt kleiner dan de graad van N, en dit is een contradictie. Het is dus onmogelijk dat $Q(Z) \neq \widetilde{Q}(Z)$, en dus moet $Q(Z) = \widetilde{Q}(Z)$. Maar dan is ook $R(Z) = \widetilde{R}(Z)$, en dit impliceert de uniciteit. □

Ten slotte formuleren we nog, zonder bewijs, de volgende stelling:

Stelling 61 (Grondstelling van de algebra)**.** *Elke complexe veelterm* $P(Z) = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$ *kan ontbonden worden in lineaire factoren:*

$$P(Z) = a_n(Z - z_0)(Z - z_1)(Z - z_2)\cdots(Z - z_n)$$

voor zekere $z_i \in \mathbb{C}$*.*

De stelling vertelt ons echter niet hoe de z_i berekend kunnen worden!

Definitie 52. *Zij* $P(Z)$ *een (complexe) veelterm. Een waarde* $z_0 \in \mathbb{C}$ *heet een* ***wortel*** *van* $P(Z)$ *indien de veeltermfunctie* $P(z)$ *nul wordt in* z_0*. Dit betekent dat* $P(z_0) = 0$ *en ook dat* $P(Z)$ *een factor* $(Z - z_0)$ *heeft.*

Gevolg 16. *Een complexe veelterm van graad* n *heeft steeds* n *wortels. Anders gezegd: een complexe veeltermfunctie van graad* n *heeft steeds* n *nulpunten.*

We merken op dat eenzelfde factor $(Z - z_0)$ meerdere keren kan voorkomen in de ontbinding van een complexe veelterm $P(Z)$. Dus moet men vorig gevolg niet interpreteren alsof er steeds n *verschillende* wortels zijn. We moeten rekening houden met de *multipliciteit* die we nu definiëren. Indien $P(Z) = (Z - z_0)^k Q(Z)$, met z_0 geen wortel van $Q(Z)$, noemen we z_0 een wortel met **multipliciteit** k.

Bibliografie

[1] Norman Biggs. *Discrete Mathematics*. Clarendon Press, Oxford, revised edition, 1989.

[2] Miklós Bóna. *A walk through combinatorics*. World Scientific Publishing Co. Inc., River Edge, NJ, 2002.

[3] Ralph P. Grimaldi. *Discrete and Combinatorial Mathematics, an Applied Introduction*. Addison-Wesley, New York, second edition, 1989.

[4] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill, New York, 5th edition, 2003.

Index