



Samenvatting

Algebra 1 - Collegejaar 2011-2012

Dictaat algebra 1

Disclaimer

De informatie in dit document is afkomstig van derden. W.I.S.V. 'Christiaan Huygens' betracht de grootst mogelijke zorgvuldigheid in de samenstelling van de informatie in dit document, maar garandeert niet dat de informatie in dit document compleet en/of accuraat is, noch aanvaardt W.I.S.V. 'Christiaan Huygens' enige aansprakelijkheid voor directe of indirecte schade welke is ontstaan door gebruikmaking van de informatie in dit document.

De informatie in dit document wordt slechts voor algemene informatie in dit documentdoeleinden aan bezoekers beschikbaar gesteld. Elk besluit om gebruik te maken van de informatie in dit document is een zelfstandig besluit van de lezer en behoort uitsluitend tot zijn eigen verantwoordelijkheid.

Samenvatting Algebra I

1. H1

$a \equiv b \pmod n$ als $(a - b)$ deelbaar is door n

$I_2(\mathbb{R})$ = de groep isometrieën van $\mathbb{R}^2$
 $= \{f : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \mid f \text{ is bijectief en voor alle } x, y \in \mathbb{R}^2 \mid f(x) - f(y) = |x - y|\}$

$I_2(\mathbb{R})$ is een ondergroep van $S(\mathbb{R}^2)$ en $I_2(\mathbb{R})$ werkt op $\mathbb{R}^2$

Voor $F \in \mathbb{R}^2$:

$Sym(F) = \{f \in I_2(\mathbb{R}) \mid f[F] = F\}$ = de stabilisator van F in $I_2(\mathbb{R})$

$I_2(\mathbb{R})$ werkt op F

Voorbeelden van symmetriegroepen

ruit(V_4), vierkant(D_4), regelmatige n -hoek met $n \geq 3$ (D_n), tetraëder(S_4) en kubus/octaëder

Neem r een rotatie en s_x een spiegeling in D_n . Dan geldt dat $r^i \circ s_x = s_x \circ r^{-i}$.
Het bewijs volgt uit dat $r^i \circ s_x$ een spiegeling is en dus orde 2 heeft.

2. H2

Definitie groep:

Een verzameling G voorzien van een bewerking $\circ$ die voldoet aan:

(G1) G bevat een eenheidselement e voor de bewerking $\circ$

(G2) voor alle $a, b, c \in G$ geldt $a \circ (b \circ c) = (a \circ b) \circ c$

(G3) voor elke $a \in G$ bestaat er een $a^{-1} \in G$ met $a \circ a^{-1} = e = a^{-1} \circ a$

De orde $\#G$ van een groep G is het aantal elementen in G

De orde van een element $g \in G$ is het kleinste positieve getal n zodat $g^n = e$.

Bestaat zo'n n niet dan is de orde oneindig

De linksvermenigvuldiging met een element is bijectief.

$S(X)$ is de permutatiegroep van elementen uit X

Een $x \in X$ is een dekpunt van $\sigma \in G$ als $\sigma(x) = x$

S_n is de permutatiegroep van $\{1, 2, \dots, n\}$

Alle permutaties zijn te schrijven als product van disjuncte cyclen.

$(123)(345) = (12345)$

Als $\sigma = (123)$ dan $\sigma(1) = 2$ en $\sigma(4) = 4$

Als $\rho \in S(X)$ dan is de cykelnotatie van ρ te vinden door te kijken naar de banen van de groep voortgebracht door σ

Voorbeeld 1:

$$\sigma = (12)(56)(35467)(3649) \in S_9$$

Dan

$$\sigma(1) = 2$$

$$\sigma(2) = 1$$

$$\sigma(3) = 7$$

$$\sigma(7) = 3$$

$$\sigma(4) = 9$$

$$\sigma(9) = 6$$

$$\sigma(6) = 5$$

$$\sigma(5) = 4$$

$$\sigma(8) = 8$$

$$\text{Dus } \sigma = (12)(37)(4965)(8)$$

Voorbeeld 2:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 1 & 11 & 10 & 3 & 4 & 7 & 2 & 12 & 6 & 8 & 9 \end{pmatrix} = (1 \ 5 \ 3 \ 11 \ 8 \ 2)(4 \ 10 \ 6)(9 \ 12)$$

$$\tau\sigma\tau^{-1} = (\tau(x_1) \ \tau(x_2) \dots \tau(x_k)) \text{ (Zie bewijzen)}$$

Elementen uit een conjugatieklasse hebben hetzelfde cykeltype.

Definitie ondergroep:

Een verzameling $H \subset G$ heet een ondergroep van G als:

(H1) H bevat het eenheidselement $e \in G$

(H2) voor alle $a, b \in H$ geldt $a \circ b \in H$

(H3) voor elke $a \in H$ geldt $a^{-1} \in H$

De ondergroep H van G voortgebracht door een deelverzameling $V = \{g_1, g_2, \dots\}$ van G is de groep van alle elementen die te schrijven zijn als product van elementen uit V . V heet de verzameling voortbrengers van H . Notatie $\langle V \rangle = H$

Een cyclische groep is een groep voortgebracht door 1 element.

De tekenafbeelding $\varepsilon : S_n \rightarrow \{-1, 1\}$ is een homomorfisme met A_n de groep van even permutaties als kern.

$$\varepsilon((ab)) = -1 \text{ met } a \neq b$$

2 elementen $x, y \in G$ heten geconjugeerd als $y = gxg^{-1}$ voor een zekere $g \in G$

3. H3

Een isometrie is een bijectieve functie f waarvoor geldt dat voor alle $x, y \in \mathbb{R}^n$
 $|f(x) - f(y)| = |x - y|$

Iedere isometrie is op een unieke manier te schrijven als een product van een translatie en een orthogonale afbeelding.

Een orthogonale afbeelding is of een rotatie om de oorsprong of een spiegeling door een lijn door de oorsprong.

4. H4

Een homomorfisme van een groep G naar een groep G' is een afbeelding $f : G \rightarrow G'$ waar voor geldt dat voor alle $x, y \in G$ $f(xy) = f(x)f(y)$.

Een isomorfisme is een bijectief homomorfisme. Als er een isomorfisme tussen G en G' bestaat dan zijn G en G' isomorf.

Een homomorfisme van groep G naar groep G is een endomorfisme.

De conjugatie-afbeelding $\sigma_g : x \rightarrow gxg^{-1}$ is een endomorfisme en als G abels is het triviale endomorfisme.

Een bijectief endomorfisme is een automorfisme.

Een (linker)nevenklasse van G $gN = \{gn \in G | n \in N\}$
 $G/H = \{gH | g \in G\}$

Een rechternevenklasse van G $Ng = \{ng \in G | n \in N\}$
 $G \backslash H = \{Hg | g \in G\}$

De stelling van Lagrange: $\#G = [G : H] \cdot \#H$

Gevolg: De orde van $x \in G$ deelt de orde van G

Isomorfiestelling:

Zij $f : G \rightarrow G'$ een homomorfisme met kern N , en definieer een bewerking op G/N door $g_1Ng_2N = g_1g_2N$. Dan wordt G/N hiermee een groep en de afbeelding $\bar{f} : G/N \rightarrow f[G]$ gegeven door $gN \rightarrow f(g)$ een groepsisomorfisme.

Een ondergroep $H \subset G$ is een normaaldeler als $gH = Hg$ voor alle $g \in G$

5. H5

Een werking of actie van een groep G op een verzameling X is een homomorfisme van G naar $S(X)$.

stabilisator: $G_x = \{g \in G | gx = x\}$

baan: $Gx = \{gx | g \in G\}$

Er is een bijectie tussen G/G_x en Gx en daarmee geldt dat:

$$\#Gx = [G : G_x]$$

$\#Gx \times \#G_x = \#G$ als G eindig is.

Banenformule:

$$\chi(g) = \#\{x \in X \mid gx = x\}$$

$$\#(G/X) = \frac{1}{\#G} \sum_{g \in G} \chi(g)$$

De reguliere werking van G op G/H wordt gegeven door $g \circ xH = gxH$. Dan is deze werking een homomorfisme met als kern $\bigcap_{x \in G} xHx^{-1}$

Neem β een verzameling representantensysteem voor de G -banen van X dan

$$\#X = \#X^G + \sum_{x \in \beta \setminus X^G} [G : G_x]$$

6. H6

De niet negatieve voortbrenger van $a\mathbb{Z} + b\mathbb{Z}$ (de groep getallen die te schrijven zijn als $c_1a + c_2b$ met $c_1, c_2 \in \mathbb{Z}$) heet de grootste gemene deler van a en b .

De niet negatieve voortbrenger van $a\mathbb{Z} \cap b\mathbb{Z}$ (de groep getallen die te schrijven zijn als c_1a en c_2b met $c_1, c_2 \in \mathbb{Z}$) heet het kleinste gemene veelvoud van a en b .

Er bestaan oneindig veel priemgetallen en elk geheel getal is uniek te schrijven als product van priemgetallen.

Neem $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ en $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$.

Dan $\text{ggd}(a, b) = p_1^{c_1} p_2^{c_2} \dots p_n^{c_n}$ met $c_k = \min(a_k, b_k)$

En ook $\text{kgv}(a, b) = p_1^{d_1} p_2^{d_2} \dots p_n^{d_n}$ met $d_k = \max(a_k, b_k)$

Hieruit volgt direct dat $\text{ggd}(a, b) \cdot \text{kgv}(a, b) = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$ met $e_k = c_k + d_k = a_k + b_k$

Dus $\text{ggd}(a, b) \cdot \text{kgv}(a, b) = a \cdot b$

Definitie ring:

Een ring is een additief geschreven abelse groep A voorzien van een multiplicatief geschreven bewerking $\times$ die aan de volgende voorwaarde voldoet:

(R1) A bevat een eenheidselement voor $\times$

(R2) Er geldt $a(bc) = (ab)c$ voor alle $a, b, c \in A$

(R3) Er geldt $a(b+c) = ab+ac$ en $(a+b)c = ac+bc$ voor alle $a, b, c \in A$

Een belangrijk voorbeeld van een ring is $\mathbb{Z}/n\mathbb{Z}$

De eenhedengroep van A geschreven als $A^* = \{a \in A \mid \text{er bestaat een } a^\dagger \in A \text{ met } a \times a^\dagger = a^\dagger \times a = 1\}$

Een homomorfisme tussen ringen wordt een ringhomomorfisme genoemd als:

$f(1) = 1'$ (let op 1 het multiplicatieve eenheidselement, maar 1 is niet altijd e)

$f(x \times y) = f(x) \times f(y)$

Een bijectief ringhomomorfisme heet een ringisomorfisme.

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggd}(a, n) = 1\}$$

De φ -functie van Euler: $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

Zie bladzijde 77-78 voor het euclidisch algoritme.

De Chinese rest stelling: Voor n en m onderling ondeelbare getallen zijn $\mathbb{Z}/nm\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ringisomorf.

Kleine stelling van Fermat:

$a^p \equiv a \pmod{p}$ als p een priemgetal is en $a \in \mathbb{Z}$

7. H8

De ondergroepen van de quotiëntgroep $\overline{G} = G/N$ zijn van de vorm $\overline{H} = H/N$ met H een ondergroep van G die N bevat.

Voor zulke H is $f : G/H \rightarrow \overline{G}/\overline{H}$ een bijectie. Verder is H alleen normaal in G als $\overline{H}$ normaal is in $\overline{G}$ en in dat geval is f een isomorfisme.

Zij N een normaal deler van G en H een ondergroep, dan is er een natuurlijk isomorfisme $H/(H \cap N) \xrightarrow{\sim} HN/N$

Zij $f : G \rightarrow G'$ een homomorfisme en N een normaal deler van G die in $\ker(f)$ bevat is. Dan bestaat er een uniek homomorfisme $\bar{f} : G/N \rightarrow G'$ zodat f de samenstelling is van de quotiëntafbeelding $\pi : G \rightarrow G/N$ en $\bar{f}$

Rekenregels

$$r^i \circ s_x = s_x \circ r^{-i} \quad ax = b \Leftrightarrow x = a^{-1}b$$

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

$$\tau\sigma\tau^{-1} = (\tau(x_1) \ \tau(x_2) \dots \tau(x_k)) \text{ (Zie bewijzen)}$$

$$g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$$

$$\#Gx \times \#Gx = \#G \text{ als } G \text{ eindig is.}$$

$$\varphi(p_1^ap_2^b \dots p_n^z) = (p_1 - 1)p_1^{a-1}(p_2 - 1)p_2^{b-1} \dots (p_n - 1)p_n^{z-1}$$

$$G_{gx} = (g^{-1}Gg)_x$$

Symbolen

$I_n(\mathbb{R}) = \{f : \mathbb{R}^n \rightarrow \mathbb{R}^n \mid f \text{ is een isometrie}\}$

$O_n(\mathbb{R}) = \{f : \mathbb{R}^n \rightarrow \mathbb{R}^n \mid f \text{ is orthogonale afbeelding}\}$

$GL_n(\mathbb{R}) = \{f : \mathbb{R}^n \rightarrow \mathbb{R}^n \mid f \text{ is lineaire afbeelding}\}$

$Sym(F) = \{f \in I_2(\mathbb{R}) \mid f[F] = F\}$

$V_4 = \{e, a, b, c \mid e^2 = a^2 = b^2 = c^2 = e\}$

$D_n = \{\sigma^a \rho^b \mid a \in \{0, 1\} \text{ en } b \in \{0, 1, \dots, n-1\}\}$ met σ een spiegeling en ρ een rotatie van orde n .

$S(X)$ is de groep van permutaties van X

$S_n = S(\{1, 2, \dots, n\})$

$\langle \{g_1, g_2, \dots\} \rangle$ is de groep voortgebracht door $\{g_1, g_2, \dots\}$

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

$A_n = \{g \in S_n \mid \varepsilon(g) = 1\}$

$Aut(G)$: isomorfisme van G naar G

$gN = \{gn \in G \mid n \in N\}$

$G/H = \{gH \mid g \in G\}$

$Inn(G)$: de groep van conjugatie-afbeeldingen

$Z(G) = \{g \in G \mid gx = xg \text{ voor alle } x \in G\}$ $End(G)$: groep van homomorfisme van G naar G .

A^{tor} : de torsie-ondergroep van A

$Out(G) = Aut(G)/Inn(G)$

$G_x = \{g \in G \mid gx = x\}$

$Gx = \{gx \mid g \in G\}$

$G \setminus X = \{Gx \mid x \in X\}$

$X^G = \{x \in X \mid Gx = \{x\}\}$

$\chi_X(g) = \#\{x \in X \mid gx = x\}$

$\#(G/X) = \frac{1}{\#G} \sum_{g \in G} \chi(g)$

$\#X = \#X^G + \sum_{x \in \beta \setminus X^G} [G : G_x]$

$[G : H] = \#(G/H)$

$N_x = Aut(G)_x = \{g \in G \mid gxg^{-1} = x\}$

$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$

$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

$F_p = \mathbb{Z}/p\mathbb{Z}$

$[x, y] = xyx^{-1}y^{-1}$

$[G, G] = \langle \{[x, y] \mid x, y \in G\} \rangle$

$G_{ab} = G/[G, G]$

Begrippen

abelse groep: een groep waarvan alle elementen commuteren.

actie/werking

Een werking of actie van een groep G op een verzameling X is een homomorfisme van G naar $S(X)$.

anti-homomorfisme

Een afbeelding $f : G \rightarrow G'$ heet een anti-homomorfisme als voor alle $x, y \in G$ geldt

$$f(xy) = f(y)f(x)$$

f is een homomorfisme $\Leftrightarrow g(x) = f(x^{-1})$ is een anti-homomorfisme.

automorfisme:

Een bijjectief endomorfisme is een automorfisme.

baan: $Gx = \{gx | g \in G\}$

centrum: $Z(G) = \{g \in G | gx = xg \text{ voor alle } x \in G\}$

congruentie: gelijkheid in modulo rekenen

conjugatie-afbeelding

De conjugatie-afbeelding $\sigma_g : x \rightarrow gxg^{-1}$ is een endomorfisme en als G abels is het triviale endomorfisme.

commutator:

De commutator van $a, b \in G$ is het element $[a, b] = aba^{-1}b^{-1}$

commuteren:

Neem G een groep met bewerking $\circ$. $a, b \in G$ commuteren als $a \circ b = b \circ a$

cyclische groep:

Een cyclische groep is een groep voortgebracht door 1 element.

dekpunt: een $x \in X$ is een dekpunt van $\sigma \in G$ als $\sigma(x) = x$.

eenhedengroep

De eenhedengroep van een ring A geschreven als $A^* = \{a \in A | \text{er bestaat een } a^\dagger \in A \text{ met } a \times a^\dagger = a^\dagger \times a = 1\}$

endomorfisme:

Een isomorfisme van groep G naar groep G is een endomorfisme.

conjugatie-afbeelding:

De conjugatie-afbeelding $\sigma_g : x \rightarrow gxg^{-1}$ is een endomorfisme en als G abels is het triviale endomorfisme.

copriem

2 getallen $a, b \in \mathbb{Z}$ zijn copriem als $\text{ggd}(a, b) = 1$

geconjugueerd

2 elementen $x, y \in G$ heten geconjugueerd als $y = gxg^{-1}$ voor een zekere $g \in G$

gelijkvormigheid:

Een gelijkvormigheid is een niet-constante afbeelding $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ die voldoet aan de volgende eigenschap:

$$\frac{|\phi(a) - \phi(b)|}{|a - b|} = \frac{|\phi(c) - \phi(d)|}{|c - d|} \text{ voor alle } a, b, c, d \in \mathbb{R}^2 \text{ met } a \neq b \text{ en } c \neq d$$

groep:(blz. 17)

Een verzameling G voorzien van een bewerking $\circ$ die voldoet aan:

(G1) G bevat een eenheidselement e voor de bewerking $\circ$

(G2) voor alle $a, b, c \in G$ geldt $a \circ (b \circ c) = (a \circ b) \circ c$

(G3) voor elke $a \in G$ bestaat er een $a^{-1} \in G$ met $a \circ a^{-1} = e = a^{-1} \circ a$

G-verzameling

X is een G-verzameling als G op X werkt.

homomorfisme:

Een homomorfisme van een groep G naar een groep G' is een afbeelding $f : G \rightarrow G'$ waarvoor geldt dat voor alle $x, y \in G$ $f(xy) = f(x)f(y)$.

inbedding

Laat $\lambda_g \in S(G)$ de linksvermenigvuldiging met $g \in G$ zijn. Dan is $f : G \rightarrow S(G)$ met $f(g) = \lambda_g$ een inbedding.

index: $[G : H] = \#(G/H)$

inwendig automorfisme: een conjugatie-afbeelding

isometrie: een bijectieve functie f waarvoor geldt dat voor alle $x, y \in \mathbb{R}^n$ $|f(x) - f(y)| = |x - y|$

isomorf:

Als er een isomorfisme tussen G en G' bestaat dan zijn G en G' isomorf.

isomorfisme :

Een isomorfisme is een bijectief homomorfisme.

kanonieke of natuurlijke afbeelding: de afbeelding $G \rightarrow G/H$

karakteristieke ondergroep:

Een ondergroep $H \subset G$ heet karakteristiek als $\sigma[H] = H$ voor alle $\sigma \in \text{Aut}(G)$

lengte van een baan: orde van de baan

machtsverzameling

De machtsverzameling $P(X)$ is de verzameling van deelverzamelingen van X

natuurlijke of kanonieke afbeelding: de afbeelding $G \rightarrow G/H$

nevenklasse

Een linkernevenklasse van G $gN = \{gn \in G | n \in N\}$

Een rechternevenklasse van G $Ng = \{ng \in G | n \in N\}$

normaaldeler:

Een ondergroep $H \subset G$ is een normaaldeler als $gH = Hg$ voor alle $g \in G$

ondergroep

Een verzameling $H \subset G$ heet een ondergroep van G als:

(H1) H bevat het eenheidselement $e \in G$

(H2) voor alle $a, b \in H$ geldt $a \circ b \in H$

(H3) voor elke $a \in H$ geldt $a^{-1} \in H$

orde

De orde $\#G$ van een groep G is het aantal elementen in G

De orde van een element $g \in G$ is het kleinste positieve getal n zodat $g^n = e$.

Bestaat zo'n n niet dan is de orde oneindig

stabilisator: $G_x = \{g \in G | gx = x\}$

symmetrisch verschil:

Het symmetrisch verschil van de verzamelingen A en B $A \triangle B = (A \cup B) \setminus (A \cap B)$

ring:

Een ring is een additief geschreven abelse groep A voorzien van een multiplicatief geschreven bewerking $\times$ die aan de volgende voorwaarde voldoet:

(R1) A bevat een eenheidselement voor $\times$

(R2) Er geldt $a(bc) = (ab)c$ voor alle $a, b, c \in A$

(R3) Er geldt $a(b+c) = ab+ac$ en $(a+b)c = ac+bc$ voor alle $a, b, c \in A$

ringhomomorfisme

Een homomorfisme tussen ringen wordt een ringhomomorfisme genoemd als:

$f(1) = 1'$ (let op 1 het multiplicatieve eenheidselement, maar 1 is niet altijd e)

$f(x \times y) = f(x) \times f(y)$

ringisomorfisme: Een bijectief ringhomomorfisme heet een ringisomorfisme.

torsie-element: een element van eindige orde.

torsie-ondergroep:

Zij A een abelse groep. De torsie-ondergroep A^{tor} van A is de verzameling van

elementen van eindige orde uit A .

transitieve werking:

Een werking is transitief als er een $x \in X$ bestaat zodat $Gx = X$

trouwe werking: een injectieve werking.

uitwendig automorfisme: niet inwendige automorfisme

viergroep van Klein: $V_4 = \{e, a, b, c | e^2 = a^2 = b^2 = c^2 = e\}$

voortgebracht:

De ondergroep H van G voortgebracht door $\{g_1, g_2, \dots\}$ is de groep van alle elementen die te schrijven zijn als product van elementen uit $\{g_1, g_2, \dots\}$. $\{g_1, g_2, \dots\}$ heet de verzameling voortbrengers van H . Notatie $\langle \{g_1, g_2, \dots\} \rangle = H$

werking/actie

Een werking of actie van een groep G op een verzameling X is een homomorfisme van G naar $S(X)$.

Bewijzen**2.16**

Neem $a, b \in G$. Dan geldt voor $[a, b] = aba^{-1}b^{-1}$
 $[a, b] = aba^{-1}b^{-1} \Leftrightarrow [a, b]b = aba^{-1} \Leftrightarrow [a, b]ba = ab$
 $[a, b] = e \Leftrightarrow aba^{-1}b^{-1} = e \Leftrightarrow ab = ba$

2.23

Neem G een groep met orde 4. En stel G is niet cyclisch. Neem $g \in G$ met $g \neq e$.
 Dan heeft g dus niet orde 1 en g kan geen orde 4 hebben, want G is niet cyclisch.
 Dus de orde van g is 2, want de orde van g deelt de orde van G .
 Dus $G = V_4$

2.28

Stel $H_1 \not\subset H_2$ en $H_2 \not\subset H_1$
 Dan $H_1 \setminus H_2 \neq \emptyset$ en $H_2 \setminus H_1 \neq \emptyset$
 Neem $e_1 \in H_1 \setminus H_2$ en $e_2 \in H_2 \setminus H_1$
 Dan $e_2 \notin H_1$ dus $e_1e_2 \notin H_1$, want $e_1^{-1} \in H_1$ en als $e_1e_2 \in H_1$ dan $e_1^{-1}e_1e_2 = e_2 \in H_1$
 En ook $e_1 \notin H_2$ dus $e_1e_2 \notin H_2$, want $e_2^{-1} \in H_2$ en als $e_1e_2 \in H_2$ dan $e_1e_2e_2^{-1} = e_1 \in H_2$
 Dus $e_1, e_2 \in H_1 \cup H_2$, maar $e_1e_2 \notin H_1 \cup H_2$
 Dus als $H_1 \not\subset H_2$ en $H_2 \not\subset H_1$ dan is $H_1 \cup H_2$ geen ondergroep van G
 Dus als $H_1 \cup H_2$ een ondergroep is van G dan $H_1 \subset H_2$ of $H_2 \subset H_1$

Stel $H_1 \subset H_2$ of $H_2 \subset H_1$, dan $H_1 \cup H_2 = H_1$ of $H_1 \cup H_2 = H_2$
 Aangezien H_1 en H_2 beide ondergroepen van G zijn is dus ook $H_1 \cup H_2$ een ondergroep van G .

2.46

Voor x_i met $i \in \{1, 2, \dots, k-1\}$
 $\tau\sigma\tau^{-1}(\tau(x_i)) = \tau\sigma(x_i) = \tau(x_{i+1})$

Voor x_k
 $\tau\sigma\tau^{-1}(\tau(x_k)) = \tau\sigma(x_k) = \tau(x_1)$

Voor andere elementen x uit $\{1, 2, \dots, n\}$
 $\tau\sigma\tau^{-1}(\tau(x)) = \tau\sigma(x) = \tau(x)$

Alle elementen uit $\{1, 2, \dots, n\}$ zijn te schrijven als $\tau(x)$ met $x \in \{1, 2, \dots, n\}$
 Dus nu weten we wat $\tau\sigma\tau^{-1}$ doet met alle elementen uit $\{1, 2, \dots, n\}$ en $\tau\sigma\tau^{-1} = (\tau(x_1) \tau(x_2) \dots \tau(x_k))$
 Neem $\sigma \in S_n$ dan $\sigma = (x_1 x_2 \dots x_a)(x_{a+1} \dots x_b) \dots (x_{n-(c-1)} \dots x_n)$
 $\tau\sigma\tau^{-1} = \tau(x_1 x_2 \dots x_a)\tau^{-1}\tau(x_{a+1} \dots x_b)\tau^{-1} \dots \tau(x_{n-(c-1)} \dots x_n)\tau^{-1}$
 $\tau\sigma\tau^{-1} = (\tau(x_1) \tau(x_2) \dots \tau(x_a))(\tau(x_{a+1}) \dots \tau(x_b)) \dots (\tau(x_{n-(c-1)}) \dots \tau(x_n))$
 σ en $\tau\sigma\tau^{-1}$ hebben dus hetzelfde cykeltype, namelijk a (b-a) ... c

Zie blz. 46-47 voor bewijzen over de kern en het beeld van homomorfisme.

5.2

Neem $f : G \rightarrow S(X)$ een actie.

$e \circ x = f(e)(x) = x$, want f is een homomorfisme dus $f(e) = e' \in S(X)$ en de eenheid in $S(X)$ is de eenheidsfunctie.

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

Neem $f : G \rightarrow S(X)$ een functie met $f(g)(x) = g \circ x$.

Dan $f(gh)(x) = gh \circ x = g \circ (h \circ x) = f(g)(f(h)(x)) = (f(g) \circ f(h))(x)$

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

Dus f is een homomorfisme en daarmee een actie.

8. TENTAMENSOMMEN

Vind σ^n $\sigma^n \equiv \sigma^{n \bmod r}$ met r de orde van σ **Vind $a^b \bmod n$** $a^b \equiv (a \bmod n)^b \bmod n$ (bijvoorbeeld $2003^{2003} \equiv 3^{2003} \bmod 1000$)Bepaal de $\gcd(a, n)$ Als $\gcd(a, n) \neq 1$ ontstaat er vaak een patroon in $\overline{a^1}, \overline{a^2}, \overline{a^3}, \overline{a^4} \dots \overline{a^b}$ **Voorbeeld:**Bepaal $5^{248691} \bmod 50$ $\gcd(5, 50) = 5 \neq 1$

$$\overline{5^1} = \overline{5}$$

$$\overline{5^2} = \overline{25}$$

$$\overline{5^3} = \overline{5^2} * \overline{5} = \overline{25} * \overline{5} = \overline{125} = \overline{25}$$

$$\overline{5^4} = \overline{5^3} * \overline{5} = \overline{25} * \overline{5} = \overline{125} = \overline{25}$$

$$\dots$$
$$\overline{5^{248691}} = \overline{5^{248691-1}} * \overline{5} = \overline{25} * \overline{5} = \overline{125} = \overline{25}$$

Als $\gcd(a, n) = 1$ dan $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$

Nu zijn er 2 mogelijkheden:

- 1) Bepaal de orde van $\overline{a}$ (Vaak moeilijk te vinden)
- 2) Gebruik Gevolg 4.8 de orde van $\overline{a}$ deelt $\#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$

Noem de orde of anders $\varphi(n)$ r Dan $a^r \equiv 1 \bmod n$ Dus $a^b \equiv a^{b \bmod r} \bmod n$ **Voorbeeld:**Bepaal $2003^{2003} \bmod 100$

$$2003^{2003} \equiv 3^{2003} \bmod 100$$

$$\gcd(3, 100) = 1$$

$$r = \#(\mathbb{Z}/100\mathbb{Z})^* = \varphi(100) = \varphi(2^2)\varphi(5^2) = 2 \cdot (4 \cdot 5) = 40$$

$$2003 \equiv 3 \bmod 40$$

$$\text{Dus } 3^{2003} \equiv 3^3 \bmod 100$$

$$\text{Dus } 2003^{2003} \equiv 3^3 \bmod 100$$

$$\#(\mathbb{Z}/(p_1^a p_2^b \dots p_n^z)\mathbb{Z})^* = \varphi(p_1^a p_2^b \dots p_n^z) = (p_1 - 1)p_1^{a-1}(p_2 - 1)p_2^{b-1} \dots (p_n - 1)p_n^{z-1}$$

Bestaat er een geheel getal x met $x \equiv a \pmod{m}$ en $x \equiv b \pmod{n}$?

Als $a = b$ dan ja, namelijk $x = a + nm$

Als $a \neq b$ en $\text{ggd}(m, n) = 1$ dan bepaal r en s zodat $rm + sn = 1$
 Dan $x = asn + brm$ (blz. 79)

Als $a \neq b$ en $\text{ggd}(m, n) \neq 1$ nee, want $x \equiv a \pmod{\text{ggd}(m, n)}$ en $x \equiv b \pmod{\text{ggd}(m, n)}$
 dus $a = b$

Bestaat er een geheel getal x met $x \equiv a \pmod{m}$ en $x \equiv b \pmod{n}$ en $x \equiv c \pmod{p}$?

Bepaal eerst een getal y met $y \equiv a \pmod{m}$ en $y \equiv b \pmod{n}$

Bepaal dan x met $x \equiv y \pmod{\text{kgv}(m, n)}$ en $x \equiv c \pmod{p}$

Kleuringen

Bereken het aantal echt verschillende kleuringen van een vorm V als de zijdes/vlakken gekleurd kunnen worden met n kleuren.

Neem X de verzameling van gekleurde V en G de groep van de symmetrieën van V . Dan werkt G op X en zijn 2 gekleurde V gelijk als en slechts als ze in de zelfde baan van X onder G zitten. Dus is het aantal banen van X onder G $\#(G \backslash X)$ ook het aantal echt verschillende kleuringen. Met de banenformule vinden we dan dat

$$\#(G \backslash X) = \frac{1}{\#G} \sum_{g \in G} \#\{x \in X | gx = x\}$$

Verder geldt dat $gx = x$ betekent dat als je een bepaalde kleuring x neemt die hieraan voldoet en je kijkt naar de kleur van een bepaalde zijde/vlak dat alle zijdes/vlakken in dezelfde baan als die zijde/vlak dezelfde kleuren heeft. Dus $\#\{x \in X | gx = x\}$ is n^k met k het aantal banen van de verzameling van alle zijdes/vlakken onder g .

Neem bijvoorbeeld de kleuring van een regelmatige 6-hoek met n kleuren. Dan is het aantal echt verschillende kleuringen $\#(D_6 \backslash X) = \frac{1}{\#D_6} \sum_{g \in D_6} \#\{x \in X | gx = x\}$

We weten dat $\#D_6 = 12$. Nu moeten we het aantal banen van de zijdes van D_6 onder g berekenen voor alle $g \in D_6$

Bij $e \in D_6$ blijven alle zijdes op dezelfde plaats dus 6 banen

Bij een rotatie van orde 6 heb je maar 1 baan
Er zijn in D_6 2 van zulke rotaties.

Bij een rotatie van orde 3 heb je maar 2 baan
Er zijn in D_6 2 van zulke rotaties.

Bij een rotatie van orde 2 heb je maar 3 baan
Er is in D_6 maar 1 zo'n rotatie.

Bij een spiegeling waarbij de spiegellijn door de middens van 2 zijdes gaat heb je 3 banen. Er zijn in D_6 3 van zulke spiegelingen.

Bij een spiegeling waarbij de spiegellijn door 2 snijpunten gaat heb je 4 banen. Er zijn in D_6 3 van zulke spiegelingen.

Dus het antwoord is hier $\frac{1}{12}(n^6 + 2n + 2n^2 + n^3 + 3n^3 + 3n^4)$

D_{2n}

Heeft hetzelfde aantal typen rotaties als het aantal delers van $2n$. (Dus 2 als $n = 1$)

Voor een rotatie van orde g zijn er van $\frac{2n}{g}$ vrijheidsgraden.

Dus bij a kleuren heb je $a^{\left(\frac{2n}{g}\right)}$ kleuringen die op zijn plek blijven.

Verder heb je 2 soorten spiegelingen waarvan er elk n zijn.

De spiegelingen door de zijdes hebben n vrijheidsgraden.

Dus bij a kleuren heb je a^n kleuringen die op zijn plek blijven.

De spiegelingen door de hoekpunten hebben $n + 1$ vrijheidsgraden.

Dus bij a kleuren heb je a^{n+1} kleuringen die op zijn plek blijven.

D_{2n+1}

Heeft hetzelfde aantal typen rotaties als het aantal delers van $2n + 1$. (Dus 2 als $2n + 1$ een priemgetal is)

Voor een rotatie van orde g zijn er van $\frac{2n+1}{g}$ vrijheidsgraden.

Dus bij a kleuren heb je $a^{\left(\frac{2n+1}{g}\right)}$ kleuringen die op zijn plek blijven.

Verder heb je 1 soort spiegelingen waarvan er $2n + 1$ zijn.

De spiegelingen door de zijdes hebben $n + 1$ vrijheidsgraden.

Dus bij a kleuren heb je a^{n+1} kleuringen die op zijn plek blijven.

hoekpunten/vlakken viervlak

De symmetriegroep is S_4 dus kijk per cykeltype naar het aantal elementen van dat type en het aantal disjuncte cycli.

vlakken kubus/hoekpunten achthoek

blz. 61-62

hoekpunten kubus/vlakken achthoek

blz. 61-62 voor de symmetrieën zoek het aantal banen.

Voor vlakken twintigvlak.

De eenheid heeft 20 vrijheidsgraden.

24 hoekpunt tot hoekpunt rotaties, namelijk 6 paren punten met 4 verschillende hoeken waarover je kan draaien, met 4 vrijheidsgraden.

15 rotaties om lijnen van middens van zijdes met 10 vrijheidsgraden.

20 rotaties van lijnen door middens van vlakken, namelijk 10 paren vlakken en 2 hoeken per paar met 8 vrijheidsgraden.

Voor hoekpunten twaalfvlak.

De eenheid heeft 20 vrijheidsgraden.

24 rotaties van lijnen door middens van vlakken, namelijk 6 paren vlakken met 4 verschillende hoeken waarover je kan draaien, met 4 vrijheidsgraden.

15 rotaties om lijnen van middens van zijdes met 10 vrijheidsgraden.

20 rotaties van hoekpunten, namelijk 10 paren vlakken en 2 hoeken per paar met 8 vrijheidsgraden.

Voor hoekpunten twintigvlak.

De eenheid heeft 12 vrijheidsgraden.

24 punt tot punt rotaties, namelijk 6 paren punten met 4 verschillende hoeken waarover je kan draaien, met 4 vrijheidsgraden.

15 rotaties om lijnen van middens van zijdes met 6 vrijheidsgraden.

20 rotaties van lijnen door middens van vlakken, namelijk 10 paren vlakken en 2 hoeken per paar met 4 vrijheidsgraden.

Voor vlakken twaalfvlak.

De eenheid heeft 12 vrijheidsgraden.

24 rotaties van lijnen door middens van vlakken, namelijk 6 paren vlakken met 4 verschillende hoeken waarover je kan draaien, met 4 vrijheidsgraden.

15 rotaties om lijnen van middens van zijdes met 6 vrijheidsgraden.

20 rotaties van lijnen tussen hoekpunten, namelijk 10 paren hoekpunten en 2 hoeken per paar met 4 vrijheidsgraden.

Homomorfismen tellen

Bepaal $\#Hom(G, G')$.

Als G' abels is dan $\#Hom(G, G') = \#Hom(G_{ab}, G')$.

(Voorbeeld $\#Hom(S_n, \mathbb{C}) = \#Hom(\{\pm 1\}, \mathbb{C})$)

Omdat elk element te schrijven is als een product van de voortbrengers ligt een homomorfisme vast als je weet wat de voortbrengers doen. Dus je moet opzoek naar het aantal combinatie van beelden van de voortbrengers.

Het aantal combinaties wordt altijd beperkt door een aantal vergelijkingen:

$$f(e) = e'$$

$$f(xy) = f(x)f(y)$$

$$f(g)^n = e \text{ voor } n \text{ de orde van } g$$

$$\text{Als } G = D_n \text{ dan } f(\rho)^{-1}f(\sigma) = f(\sigma)f(\rho)$$

$$\text{Als } G = S_n \text{ dan } f(\tau)f((x_1 \ x_2 \ \dots \ x_a))f(\tau)^{-1} = f((\tau(x_1) \ \tau(x_2) \ \dots \ \tau(x_a)))$$

Voorbeeld

Bepaal $\#Hom(S_n, \mathbb{C})$

$(\mathbb{C}, +)$ is abels dus $\#Hom(S_n, \mathbb{C}) = \#Hom((S_n)_{ab}, \mathbb{C}) = \#Hom(\{\pm 1\}, \mathbb{C})$

Voor een homomorfisme $f : \{\pm 1\} \rightarrow \mathbb{C}$ geldt dat:

$$f(1) = 0$$

$$f((-1)^2) = f(-1) + f(-1) = 0 \Rightarrow f(-1) = 0$$

$$\text{Dus } \#Hom(S_n, \mathbb{C}) = \#Hom(\{\pm 1\}, \mathbb{C}) = 1$$

Voorbeeld

Bepaal $\#Hom(C_7, S_{15})$

Een homomorfisme $f : C_7 \rightarrow S_{15}$ wordt volledig bepaald door het beeld van de voortbrenger ρ van C_7 . Er moet gelden dat $f(\rho)^7 = (1)$ dus de orde van $f(\rho)$ is een deler van 7. Dus $f(\rho) = (1)$ of $f(\rho)$ is een product van 7-cykels.

Het aantal verschillende 7-cykels is $\frac{15 * 14 * 13 * 12 * 11 * 10 * 9}{7}$, want voor het eerst getal heb je 15 mogelijkheden enzovoort, maar je hebt dat elke 7-cykel 7 keer gehad, omdat je dezelfde 7-cykel op 7 manieren kan schrijven.

Het aantal verschillende producten van 7-cykels is $\frac{15!}{7 \cdot 7 \cdot 2}$, want je heb 15! verschillende volgorde van 15 getallen. Neem steeds de eerst 7 getallen in die volgorde de eerste 7-cykel en de volgende 7 de tweede. Dan heb je hetzelfde element als je de cykels verwisseld, als je de eerste cykel anders schrijft en als je de tweede cykels anders schrijft. Dus je deelt door $7 \cdot 7 \cdot 2$.

$$\text{Dus } \#Hom(C_7, S_{15}) = 1 + \frac{15 * 14 * 13 * 12 * 11 * 10 * 9}{7} + \frac{15!}{7 \cdot 7 \cdot 2}$$

Bewijs: $a^{k_1} \equiv a^{k_2} \pmod n$ voor alle $a \in \mathbb{Z}$

- Controleer dat het geldt voor alle priemdelers van n
- Alle priemgetallen tussen 1 en n zijn priemdelers van n of zitten in $(\mathbb{Z}/n\mathbb{Z})^*$
Dus bewijs (met chinese reststelling of orde van de groep dat voor alle $a \in (\mathbb{Z}/n\mathbb{Z})^*$ geldt $a^{k_1-k_2} \equiv 1 \pmod n$
- Dan geldt het dus voor alle priemgetallen tussen 1 en n .
Het is genoeg dat $a^{k_1} \equiv a^{k_2} \pmod n$ voor alle a tussen 1 en n .
Neem a tussen 1 en n . Dan $a = p_1 p_2 \dots p_g$ een product van priemgetallen tussen 1 en n . $a^{k_1} \equiv p_1^{k_1} p_2^{k_1} \dots p_g^{k_1} \pmod n$ en $p_i^{k_1} \equiv p_i^{k_2} \pmod n$.
Dus $p_1^{k_1} p_2^{k_1} \dots p_g^{k_1} \equiv p_1^{k_2} p_2^{k_2} \dots p_g^{k_2} \pmod n$ en $p_1^{k_2} p_2^{k_2} \dots p_g^{k_2} = a^{k_2}$
Dus $a^{k_1} \equiv a^{k_2} \pmod n$

Voorbeeld:

Bewijs: $a^6 \equiv a^2 \pmod{60}$ voor alle $a \in \mathbb{Z}$

$$2^6 = 64 \equiv 4 = 2^2 \pmod{60}$$

$$3^6 = 729 \equiv 9 = 3^2 \pmod{60}$$

$$5^6 = 15625 \equiv 25 = 5^2 \pmod{60}$$

$(\mathbb{Z}/60\mathbb{Z})^*$ is isomorf met $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$

$(\mathbb{Z}/3\mathbb{Z})^*$ en $(\mathbb{Z}/4\mathbb{Z})^*$ hebben orde 2 en $(\mathbb{Z}/5\mathbb{Z})^*$ heeft orde 4

Dus elk element uit $(\mathbb{Z}/60\mathbb{Z})^*$ heeft orde die 4 deelt.

Dus $p^4 \equiv 1 \pmod{60} \Rightarrow p^6 \equiv p^2 \pmod{60}$ voor alle priemgetallen in $(\mathbb{Z}/60\mathbb{Z})^*$

Dus voor elk priemgetal tussen 1 en 60 geldt $p^6 \equiv p^2 \pmod{60}$

Neem a tussen 1 en 60. Dan $a = p_1 p_2 \dots p_g$ een product van priemgetallen tussen 1 en 60.

$$a^6 \equiv p_1^6 p_2^6 \dots p_g^6 \pmod{60} \text{ en } p_i^6 \equiv p_i^2 \pmod{60}.$$

$$\text{Dus } p_1^6 p_2^6 \dots p_g^6 \equiv p_1^2 p_2^2 \dots p_g^2 \pmod{60} \text{ en } p_1^2 p_2^2 \dots p_g^2 = a^2$$

$$\text{Dus } a^6 \equiv a^2 \pmod{60}$$

Bewijs: Als $a^{k_1} \equiv a^{k_2} \pmod d$ voor alle $a \in \mathbb{Z}$ dan is d een deler van n

Zoek een a zodat $a^{k_1} - a^{k_2} = n$ (priemdelers van n)

9. OVERZICHT GROEPEN

$$1 = \{e\}$$

De triviale groep.

$$\{\pm 1\}$$

De enige groep van orde 2. Deze groep is abels, cyclisch en wordt voortgebracht door -1 met als bewerking de vermenigvuldiging.

$$C_n \ (n \geq 3)$$

De cyclische groep van orde n . Deze groep wordt dus voortgebracht door een element ρ met orde n . De groep is abels. De groep kan worden opgevat als de rotaties van een regelmatige n -hoek, als ondergroep van S_n met ρ een n -cykel, als ondergroep van D_n en als $(\mathbb{Z}/n\mathbb{Z}, +)$.

$$V_4$$

De viergroep van Klein. De groep heeft orde 4 en is abels. De groep is $\{e, a, b, c\}$ met e het eenheidselement en voor $x, y, z \in V_4$ allen ongelijk aan elkaar en e geldt $xy = yx = z$ en $x^2 = e$

$$D_n \ (n \geq 3)$$

Een niet abelse groep van orde $2n$. De groep wordt voortgebracht door σ een element van orde 2 en ρ een element van orde n met een bewerking die voldoet aan $\rho^{-1}\sigma = \sigma\rho$

De normaaldelers van D_n zijn 1, $\langle \rho^g \rangle$ waarbij g een deler van n is.

$$[D_n, D_n] = \langle \rho^2 \rangle$$

$$(D_n)_{ab} = \begin{cases} \{\pm 1\} & \text{als } n \text{ oneven is} \\ V_4 & \text{als } n \text{ even is} \end{cases}$$

$$Q$$

De quaternionengroep (de groep van 4D complexe getallen) van orde 8. De groep is $\{\pm 1, \pm i, \pm j, \pm k\}$ met $i^2 = j^2 = k^2 = ijk = -1$ en $(-1)^2 = 1$.

Zie bladzijde 99.

$$S_n = S(\{1, 2, 3, \dots, n\}) \ (n \geq 4)$$

De groep van permutaties van $\{1, 2, 3, \dots, n\}$ met orde $n!$. De groep is niet abels, want $(12)(23) \neq (32)(21)$ en wordt voortgebracht door $\{(12), (12\dots n)\}$

De normaaldelers zijn 1, A_n en als $n = 4$ ook V_4 .

$$[S_n, S_n] = A_n$$

$$(S_n)_{ab} = \{\pm 1\}$$

A_n

De groep van even permutaties van n elementen. dat wil zeggen dat A_n de ondergroep van S_n is van alle elementen die als product van een even aantal 2-cykels te schrijven zijn. De orde is $\frac{1}{2}n!$ en de groep is niet abels. De groep wordt voortgebracht door $\{(12i)|i = 3, \dots, n\}$

$$(A_n)_{ab} = \begin{cases} A_2 & \text{als } n = 2 \\ A_3 & \text{als } n = 3 \\ C_3 & \text{als } n = 4 \\ 1 & \text{als } n \geq 5 \end{cases}$$

$G \times G'$

De groep $\{(g, g')|g \in G, g' \in G'\}$ waarbij $(x_1, x_2) \circ (y_1, y_2) = (x_1y_1, x_2y_2)$

$G \times 1$ is een ondergroep van $G \times G'$ die isomorf is met G en hetzelfde geldt voor $1 \times G'$ en G'