# Discrete Wiskunde
# Eerste semester

Tibo Fordeyn

# Inhoudsopgave

# Hoofdstuk 1

# Relaties en functies

## 1.1 Relaties en functies

Stel R is een relatie tussen A en B: $R \subset A \times B$, vaak genoteerd als $R : A \to B$, dan noemt men dit een binaire relatie. Dit hoofdstuk gaat uitsluitend over vormen van binaire relaties.
Het domein van een relatie omvat alle punten waaruit een pijl vertrekt. Het bereik omvat dus vanzelfsprekend alle plaatsen waar een pijl aankomt.

$$domR : \forall x \in A : \exists y \in B : (x, y) \in R.$$

$$codomR : \forall x \in A : \exists y \in B : (x, y) \in R.$$

We noemen zo'n relatie een **functie** wanneer **uit elk element a hoogstens één pijl vertrekt.**:

$$Functie \iff \forall a \in domR : \exists! b \in B : (a, b) \in R.$$

Relatie wordt een **afbeelding** genoemd indien **uit elk punt precies één pijl vertrekt**:

$$Afbeelding \iff \forall a \in A : \exists! b \in B : (a, b) \in R.$$

Relatie wordt een **bijectie** genoemd indien uit elk punt **precies één pijl vertrekt en aankomt**

$$Bijectie \iff \begin{cases} \forall a \in A : \exists! b \in B : (a, b) \in R \\ \forall b \in B : \exists! a \in A : (a, b) \in R \end{cases}.$$

Relatie wordt een **injectie** genoemd indien er **in geen enkel punt meer dan 1 pijl vertrekt of aankomt**

$$Injectie \iff \begin{cases} \forall a \in domR : \exists! b \in B : (a, b) \in R \\ \forall b \in codomR : \exists! a \in A : (a, b) \in R \end{cases}.$$

Relatie wordt een **surjectie** genoemd indien **uit elk punt één pijl vertrekt** en er **ten minste één aankomt**.

$$Surjectie \iff \begin{cases} \forall a \in A : \exists! b \in B : (a, b) \in R \\ \forall b \in B : \exists a \in A : (a, b) \in R \end{cases}.$$

## 1.2 Aftelbaarheid

Wanneer er een bijectie bestaat tussen A en B, zeggen we dat deze verzamelingen dezelfde cardinaliteit hebben. Op basis van cardinaliteit wordt er onderscheid gemaakt tussen aftelbare en niet-aftelbare verzamelingen.

- Voor een eindige verzameling A en B zeggen we dus dat ze eenzelfde cardinaliteit hebben als er een bijectie bestaat. Deze noeme we aftelbaar
- Voor een oneindige verzameling $V$, wordt deze aftelbbaar genoemd als er een bijectie bestaat van $\mathbb{N}$ op $V$, met ander woorden; als V dezelfde cardinaliteit heeft als $\mathbb{N}$

Zo bestaat er een bijectie van $\mathbb{N}$ naar $\mathbb{Z}$

$$b : \mathbb{N} \to \mathbb{Z} : n = \begin{cases} \frac{n}{2}, \text{ wanneer n even is} \\ -\frac{n+1}{2}, \text{ wanneer n oneven is} \end{cases} .$$

Indien zo'n bijectie niet bestaat voor de oneindige verzameling V, dan zegge we dat deze verzameling overaftelbaar is. En een eindige verzameling is dus altijd aftelbaar.

## 1.3 Functies, bijkomende definities voor functies

Een **identieke functie**:

$$I : V \to V : I(x) = x, x \in V \equiv I_V.$$

Merk op dat $\operatorname{dom} I = V$ niet altijd moet gelden.

Een **samenstelling**:

$$\text{brengt } f : A \to B, \text{ en } g : B \to C.$$

$$\text{samen tot } h : A \to C.$$

Dit onder de vanzelfsprekende voorwaarden:

- $\operatorname{dom} h = a : a \in \operatorname{dom} f, f(a) \in \operatorname{dom} g$
- $h = g(f(a)), \forall a \in A$

Een **inverse functie** van $f : A \to B$ is $G : B \to A$ als:

- $f \circ g = 1_{\operatorname{dom} f}$
- $g \circ f = 1_{\operatorname{codom} f}$

## 1.4 equivalentierelaties

1. reflexiviteit
$$\forall x \in V : (x, x) \in R.$$
2. symmetrie
$$\forall x, y \in V : (x, y) \in R \implies (y, x) \in R.$$
3. transitiviteit
$$\forall x, y, z \in V : (x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R.$$

De absolute waarde bijvoorbeeld is een equivalentieklasse.

Een **equivalentieklasse** bestaat wanneer $x \in V : (x, y) \in R$ deze elementen y vormen een deelverzameling, een equivalentieklasse. We noteren

$$[x]_R = \{y : y \in V \wedge (x, y) \in R\}.$$

twee willekeurige elementen $x$ en $y$ hun corresponderende equivalentieklassen zullen ofwel samenvallen, of disjunct zijn.

We sperken over een **partiële orderlatie** als:

- reflexiviteit:
$$\forall x \in V : (x, x) \in R.$$
- anti-symmetrie:
$$\forall x, y \in V : \{(x, y) \in R \wedge (y, x) \in R \implies x = y\}.$$
- Transitiviteit:
$$\forall x, y, z \in R : \{(x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R\}.$$

Een zeer duidelijk voorbeeld van een partiële orderelatie is $\subset$.

We spreken over een **totale orderelatie** wanneer ook

- $\forall x, y \in V : (x, y) \in R \vee (y, x) \in R$

Een duidelijk voorbeeld van een totale orderelatie is $\leq$, ga na dat dit zorgt voor totale ode, $<$ is een strikterer versie - zie straks.

Wanneer V geordend wordt door een totale orderelatie, dan zeggen we dat V een lineair geordende relatie of ketting is.

Het idee van equivalentieerlaties tegenover orderelaties is zeer intuïtief; equivalentierelatief zoals absolute waarde bekijken equivalente elementen, orderelaties zorgen voor een hiërarchische structuur, ze zorgen voor orde.

We spreken van een **strikte orderelatie** wanneer de orderelatie anti-reflexief is.

- $\forall x \in V : (x, x) \notin R$

**Besluit:-**

1.1 Speciale relaties:
functie $\Longrightarrow$ **uit elk punt in A vertrekt hoogstens één pijl.**
$afbeelding \Longrightarrow$ **uit elk punt precies één pijl.**
$bijectie \Longrightarrow$ **één naar één mapping.**
$injectie \Longrightarrow$ **ten hoogste één pijl vertrekt en komt aan.**
$surectie \Longrightarrow$ **precies één vertrekt en ten minste één pijl komt aan.**

1.2 aftelbaarheid:

# Hoofdstuk 2

# Modulorekenen

De modulo relatie is een equivalentierelatie.

## 2.1 Zeef van Eratosthenes

Om alle priemgetallen te vinden kleiner dan een getal $N \in \mathbb{N}$, beschouw een lijst 2 tot $N-1$ :

- Schrap alle veelvouden van 2
- schrap alle veelvouden van 3
- schrap alle veelvouden van 5
- ga zo verder tot $\sqrt{N}$, daarna mag je stoppen

**Elk getal $\geq 2$ kan als een vermenigvuldiging van priemgetallen geschreven worden, met de priemgetallen in stijgende volgorde.**

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 192.$$

Als een getal a deelbaar is door b, dan schrijven we $a|b$

$$\text{ggd}(a,b) \cdot \text{kgv}(a,b) = |a-b|.$$

nog een eigenschap die best logisch is:

$$\text{ggd}(a,b) = \text{ggd}(a-b,b) = \text{ggd}(a,b-a).$$

dit als het kleinste argument van het grootste wordt afgetrokken.

## 2.2 Modulorekenen basisprincipes

$$a \overset{m}{=} b.$$

betekent dat de mod m van a gelijk is aan de mod m van b.

$$\equiv m|a-b.$$

omdat

$$a \overset{m}{=} b \iff a - b \overset{m}{=} 0.$$

**Herinnering 2.2.1** Over equivalentieklassen

$[0]_m$, een goed voorbeeld voor een equivalentieklassen. Dit betekent dus alle getallen waarvan de modulo m, nul is.

**Definition 2.2.1: basiseigenschappen**

$$a \overset{m}{=} b \wedge c \overset{m}{=} d \implies a + c \overset{m}{=} b + d.$$

en

$$a \cdot c \overset{m}{=} b \cdot d.$$

Om modulus duidelijk te defini'eren:

$$a = mq + r, r < m, m \in \mathbb{N}_0, a, q, r \in \mathbb{N}.$$

m mag niet nul zijn, want je kunt natuurlijk niet delen door nul, q kan wel nul zijn want soms deel je door een getal en krijg je enkel rest, bv. $\frac{5}{6}$.

hieruit volgt:

$$q = a \text{ div } m.$$

$$r = a \text{ mod } m.$$

**Herinnering 2.2.2** equivalentieklassen

Nog eens de definitiie want ik vergeet deze altijd:

$$[x]_R = \{\forall y \in V \wedge (x, y) \in R\}.$$

Bemerk:

- optelling: $[a]_m +_m [b]_m = [a + b]_m$
- vermenigvuldiging: $[a]_m \times_m [b]_m = [a \cdot b]_m$

bijvoorbeeld:

$$[2]_3 +_3 [1]_3 = [3]_3 = 0.$$

$$[8]_3 \times_3 [14]_3 = [112]_3 = 1.$$

**Verduidelijking of addendum 2.2.1** de modulo optelling en vermenigvuldiging

dit betekent dat wanneer deze som of product groter zijn dan m, m er opnieuw van wordt afgetrokken.

## 2.3 Eenvoudige vergelijking

**Voorbeeld 2.3.1**

beschouw:

$$5 + x \overset{3}{=} -2.$$

dit is een eenvoudige vergelijking. Algemeen kunnen we oplossingen van de vorm:

$$x + a \overset{m}{=} b.$$

vinden door:

$$[x]_m = [b - a]_m.$$

echter is enkel de oplossing tussen 0 en m-1 kennen voldoende.

## 2.4 Lineaire congruenties

Beschouw de algemene vorm van een lineaire congruentie:

$$ax \overset{m}{=} b.$$

er zijn vele mogelijkheden voor oplossingen hiervan, soms kunnn ze niet opgelost worden. We overlopen.

**Voorbeeld 2.4.1**

Beschouw:

$$2x \overset{8}{=} 51.$$

zie als voorbeeld van standaardvorm

$$ax \overset{8}{=} b.$$

1. vind de grootste gemeenschappelijke deler van a en m.

   $$2.$$

2. kijk of de ggd b kan delen:

   $$\frac{51}{2} \notin \mathbb{Z}.$$

   nee, dit is niet het geval dus we moeten deze niet proberen oplossen want **er is geen oplossing**.

**Voorbeeld 2.4.2**

Beschouw:

$$4x \overset{7}{=} 26.$$

1. De ggd van a en m:

   $$\text{ggd}(4, 7) = 1.$$

   > **Verduidelijking of addendum 2.4.1** 7 is een priemgetal
   >
   > je ziet natuurlijk onmiddellijk dat dit één is en moet het snel opmerken in oefeningen, want 7 is een priemgetal. Als de modulo of a een priemgetal is, dan zal je één oplossing hebben.

2. als we zien dat deze ggd één is, moet je beseffen dat er **één enkele oplossing voor deze lineaire congruentie** zal zijn.

3. je past rekenreges toe om tot een makklijk antwoord te raken. Je mag altijd beide leden delen door een getal c, **als ze natuurlijk allebei perfect deelbaar zijn door dat getal**.

   $$\iff 2x \overset{7}{=} -1 \vee 2x \overset{7}{=} 6.$$

4. we vinden uiteindelijk het antwoord onmiddellijk door bij dat laatste te delen door twee.

   $$\implies x \overset{7}{=} 3.$$

**Voorbeeld 2.4.3**

Beschouw dit moeilijkere voorbeeld:

$$25x \overset{29}{=} 15.$$

1. We bemerken onmiddellijk dat de ggd één is aangezien 29 een priemgetal is.
2. natuurlijk is 15 deelbaar door één.
3. We kuisen de vergelijking op:

   $$5x \overset{29}{=} 3.$$

4. merk op dat 3 min twee keer 29 gelijk is aan min 55, we vinden:

   $$x \overset{29}{=} -11 \vee x \overset{29}{=} 18.$$

**Voorbeeld 2.4.4**

We kijken naar voorbeelden met meerdere antwoorden. Deze zijn een stukje lastiger en moeten herhaald worden voor het examen:

$$9x \overset{6}{=} 42.$$

1. ggd van a en m is drie

   **Verduidelijking of addendum 2.4.2** betekenis

   omdat de ggd van a en m 3 is, zullen er 3 oplossingen zijn! **ggd**$(a, m)$ = #**oplossingen**

2. 42 is deelbara door drie.

3. wanneer je in een situatie komt waar ALLE (ook a,b en m) bekenden deelbaar zijn door drie, **dan mag het**.

   $$3x \overset{2}{=} 14.$$

   we vinden

   $$x \overset{2}{=} 0.$$

   dit is de oplossing van de **gelijkwaardige congruentie**. Nu moeten we deze nog terugzetten naar de standaardvorm.

4. we doen dit door de nu gebruikte mod, vanaf de gevonden congruentiewaarde op te tellen in een congruentie met de originele mod:

   $$x \overset{6}{=} 0.$$
   $$x \overset{6}{=} 2.$$
   $$x \overset{6}{=} 4.$$

   Merk dus op dat we gewoon de 2, die de mod was van de gelijkwaardige congruentie, optellen bij de b van de gelijkwaardige congruentie.

**Verduidelijking of addendum 2.4.3** kort samengevat

$$ax \overset{m}{=} b.$$

1. check de ggd van a en m, deze is ook het aantal oplossingen (in het geval dat hij een deler van b is.)
2. kijk of deze gevonden ggd een deler is van b.
3. gebruik de verschillende technieken om de vergelijking te herleiden naar $a = 1$
4. indien dit een gelijkwaardige congruentie is; zet terug om naar de oorspronkelijke vergelijking. Doe dit door de mod terug te zetten, en als antwoorden de b van de gelijkwaardige congruentie opgeteld met de mod van de gelijkwaadige congruentie als antwoorden te beschouwen.

**Voorbeeldvraag 1**

Een vraag van op de powerpoint:

$$10x \overset{14}{=} 22.$$

1. de ggd is 2
2. 22 is deelbaar door 2, we zullen bijgevolg 2 antwoorden vinden.

3. we stellen een gelijkwaardige vergelijking op:

$$5x \overset{7}{=} 11.$$

$$x \overset{7}{=} 5.$$

4. we zetten de gelijkwaardige congruentie terug naar de oorspronkelijke gedaante.

$$x \overset{14}{=} 5.$$

$$x \overset{14}{=} 12.$$

dit is het antwoord. Te makkelijk.

## 2.5 stelsels van lineaire congruenties

for the record; ik haat stelsels en je zult hier zeker een paar oefeningen op moeten maken. voorbeeld van een stelsel:

$$\begin{cases} x \overset{m_1}{=} a_1 \\ x \overset{m_2}{=} a_2 \\ \dots \\ x \overset{m_n}{=} a_n \end{cases}.$$

hiervoor bestaat een unieke oplossing en alle andere oplossingen zijn congruent met deze oplossing.

**Voorbeeld 2.5.1**

Beschouw:

$$\begin{cases} x \overset{3}{=} 1 \\ x \overset{5}{=} 4 \\ x \overset{7}{=} 6 \end{cases}.$$

het idee is dat we x zullen uitwerken in drie delen. Eerst de mod 3, dan de mod 5, dan de mod 7.

1. zeg dat $x = \dots + \dots + \dots$, dit zijn de drie delen. Vermenigvuldig elk niet mod 3 deel met 3 zodat je er niet naar moet kijken voor het mod 3 deel, doe dan hetzelfde voor 5 en 7 en krijg:

$$x = 5 \cdot 7 + 3 \cdot 7 + 3 \cdot 5.$$

2. bekijk de termen van de vergelijking voor of ze al kloppen met het stelsel van congruenties, en zo niet vind je een geheel getal om het mee te vermenigvuldigen tot het wel klopt.

$$x = 2 \cdot 5 \cdot 7 + 3 \cdot 4 \cdot 7 + 90 = 244.$$

dit voldoet aan het stelsel, maar is niet het kleinste getal.

3. Als we nu alle mods vermenigvuldigen, dan kunnen we ons getal 244 eigenlijk daarmee aftrekken en het kleinst mogelijk antwoord bekomen.

$$3 \cdot 5 \cdot 7 = 105.$$

we krijgen dus als we ons gevonden getal 2 keer hiermee verminderen:

$$244 - 210 = 34.$$

als een equivalentieklasse:

$$[34]_{105}.$$

**Definition 2.5.1: Bewijs van de Chinese reststelling**

**dit bewijs heb ik niet super goed geleerd of diep bekeken, maar ik snap de oefeningen, dus je moet dit bewijs nog eens vanbuiten leren, maak er een anki kaartje van.** Het stelsel lineaire congruenties bezit een unieke oplossing modulo $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$

**Verduidelijking of addendum 2.5.1** bedoeling

Wat hiermee eigenlijk gezegd wordt is wat in bovenstaand voorbeeld gedemonstreerd wordt, namelijk dat het antwoord een rest is van een deling door M, M zijnde de vermenigvuldiging van de moduli.

1. We tonen aan dat er een oplossing $x \in [0, 1, 2, \ldots, M-1]$ bestaat.

$$\text{Stel } \frac{M}{m_i} = M_i.$$

er geldt:

$$\text{ggd}(M_i, m_i) = 1.$$

er bestaat een geheel getal waarvoor:

$$M_i y_i \overset{m_i}{=} 1.$$

**Voorbeeld 2.5.2**

Beschouw de algemene vorm:

$$\begin{cases} x \overset{m_1}{=} a_1 \\ x \overset{m_2}{=} a_2 \\ \ldots \\ x \overset{m_n}{=} a_n \end{cases}.$$

waar

$$M = \prod_{i=1}^{n} m_i.$$

$$M_i = \frac{M}{m_i}.$$

**Verduidelijking of addendum 2.5.2** ik had dit eerst niet door

in de cursus staat de redenering hierachter niet duidelijk, maar ik heb het net ingezien; het idee is gewoon dat je op deze manier scrijft dat je alle moduli vermenigvuldigd behalve die waar je in die term mee bezig bent!

1. Opschrijven van de termen, de moduli van vergelijkingen vermenigvuldigd :

$$x = \sum_{i=1}^{n} M_i.$$

2. Nu moet ervoor gezorgd worden dat per term de congruentie klopt.

$$x = \sum_{i=1}^{n} a_i M_i y_i.$$

voor de uiteindelijke oplossing nemen we de mod M hiervan (vanzelfsprekend):

$$x = \left[ \sum_{i=1}^{n} a_i y_i M_i \right] \mod M.$$

**De toepassingen en bewijzen heb ik niet heel uitgebreid bekeken, dus dat moet j edan no geens doen.**

# Hoofdstuk 3

# Algebraïsche structuren

in dit hoofdstukken worden groepen, ringen, velden en vectorruimten bekeken.

## 3.1 Binaire bewerkingen

De binaire bewerking is een bepaald type afbeelding.

Binaire bewerking:

$$V \times V \text{ op } V.$$

Bekijk nog eens wa een Cayley-tabel is.

**eigenschappen van bewerkingen**

we noemen de bewerking $\circ$ gewoon de voorbeeld bewerking.

1. Commutativiteit
$$\forall x, y \in V : x \circ y = y \circ x.$$
2. Associativiteit
$$\forall x, y, z \in V : (x \circ y) \circ z = x \circ (y \circ z).$$
3. Eenheidselement, een verzameling beschikt over een eenheidselement als
$$\forall x \in V : \exists e_0 \in V : e_\circ \circ x = x \circ e_\circ = x.$$
4. invers element, een verzameling beschikt over een invers element als
$$\forall x \in V : \exists x' : x \circ x' = x' \circ x = e_\circ.$$
zie $x'$ als de inverse van x. je kunt dus ook enkel een invers element hebben, als je ook een eenheidselement hebt.
5. Distributiviteit
$$(x \texttt{ bew } y) \circ z = (z \circ x) \texttt{ bew } (z \circ y).$$
en
$$(x \texttt{ bew } y) \circ z = (x \circ z) \texttt{ bew } (y \circ z).$$
waar 'bew' natuurlijk gewoon eender welke bewerking is.

## 3.2 Groepen

### 3.2.1 één binaire bewerking

**Semi-groep, groep, abelse groep**

Een groep wordt geschreven als een verzameling mt een daarin gedefinieerde bewerking: $(V, \circ)$.

1. **eigenschappn semi groep**
   - Associativiteit
2. **eigenschappen groep**
   - Associativiteit
   - Eenheidselment
   - Invers element
3. **eigenschappen abelse groep**
   - Associativiteit
   - Eenheidselement
   - Invers element
   - Commutativiteit

abelse groepen worden ook commutatieve groepen genoemd.
Orde: $\#V$
Orde van een element: kleinste $n \in \mathbb{N}_0$ waarvoor $a^n = e_{\circ,}$, hier moet $a^n$ gezien worden als $a \circ a \circ \ldots \circ a$

**Voorbeeld 3.2.1**

$$(\mathbb{Z}_2, +), \mathbb{Z}_2 = \{[0]_2, [1]_2\}.$$

zie dit als een subgroep van $\mathbb{Z}$ die enkel de elementen bevat die die $\mathbb{Z}_2$ is effectief Z modulo twee, maar ik kan deze vraag niet dus je moet het nog eens bekijken voor het examen. onthoud dat als de groep bestaat uit equivalentieklssen, optellingen ook tussen euivalentieklassen gebeuren.

**Verduidelijking of addendum 3.2.1** onthoud

SEMI-GROEP: A
GROEP: A,E,I
ABELSE GROEP: A,E,I,C
Orde: $\#V$
Orde van een element: kleinste $n \in \mathbb{N}_0$ waarvoor $a^n = e_{\circ,}$, hier moet $a^n$ gezien worden als $a \circ a \circ \ldots \circ a$

**eigenschappen**

We leiden uit de drie eigenschappen alreeds besproken enkele essentiële bijkomende eigenschappen af:

$$\text{linkse schrappingswet} \iff \forall x, y, a \in V : a \circ x = a \circ y \implies x = y.$$

$$\text{rechtse schrappingswet} \iff \forall x, y, a \in V : x \circ a = y \circ a \implies x = y.$$

Denk over de schrappingswetten als linkse en rechtse transiviteit.

**Definition 3.2.1: Bewijs linkse schrappingswet**

We beginnen bij het te bewijzen:

$$a \circ x = a \circ y.$$

steunt op het bestaan van inverse elementen:

$$\iff a^{-1} \circ (a \circ x) = a^{-1} \circ (a \circ y).$$

steunt op de associativiteit en de definitie van het eenheidselement:

$$e_\circ \circ x = e_\circ \circ y.$$

en dan volgt uit de definitie van het eenheidselement:

$$x = y.$$

rechtse schrappingswet is natuurlijk analoog.
2 kleine extra eigenschappen:

- $x \circ a = b \implies x = b \circ a^{-1}$
- $a \circ x = b \implies x = a^{-1} \circ b$
- $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$
  deze laatste geldt eigenlijk voor maakt niet uit hoeveel termen, veel termen tergelijk inverse nemen is de inverse van elk element en je wisselt de plaatsen om.

$$(a \circ b \circ \ldots \circ p \circ q)^{-1} = q^{-1} \circ p^{-1} \circ \ldots \circ b^{-1} \circ a^{-1}.$$

**deelgroepen of subgroepen**

we maken een onderscheid tussen echte en onechte deelgroepen. Onechte deelgroep:

$$(V, \circ), \texttt{ onechte deelgroep: } (\{e_\circ\}, \circ).$$

een echte deelgroep is elke andere deelgroep $(W, \circ)$

stelling van lagrange $\iff$ **Als $(W, \circ)$ een deelgroep is van $(V, \circ)$, dan is de orde van W een deelgroep van de orde van V.** dus stel nu de orde van v is 6, dan is die van W 3,2 of 1.

Als je wilt testen of die deelverzameling W met dezelfde bewerking ook een groep vormt moet je gewoon controleren of $a \circ b \in W$, en voor een oneindige groep controleer je ook of er zeker een invers element is.

**Definition 3.2.2: Bewijs test**

Bewijs dat

$$\forall a, b \in W : a \circ b \in V : a \in W : a^{-1} \in W.$$

Stel: $[x_1, x_2, \ldots, x_n], a \in W$

$$\begin{cases} a \circ x_1 & = y_1 \\ a \circ x_2 & = y_2 \\ \ldots & \\ a \circ x_n & = y_n \end{cases}.$$

dan $y_1, y_2, \ldots, y_n \in W$
deze zijn onderling niet gelijk dus

$$y_i = a \implies x = e_\circ \in W.$$

$$y_i = e_\circ \implies x = a^{-1} \in W.$$

dat laatste stuk snap ik niet helemaal dus dat moet je nog eens bekijken.

Wat eigenlijk werd bewezen is dat je niet moet checken of er een eenheidselement is voor een eindige deelgroep.

**morfismen**

via morfismen kunnen groepen in elkaar worden omgezet. Het deelt alle soorten groepen op.

1. een morfisme van V in W is een afbeelding $\theta$ van $(V, \circ)$ naar $(W, \blacksquare)$ waarbij:

$$\forall a, b \in V : \theta(a \circ b) = \theta(a) \blacksquare \theta(b).$$

2. is deze afbeelding bijectief dan spreken we over een **isomorfisme.**
3. Een isomorphisme van $(V, \circ)$ op $(V, \circ)$ is een **automorfisme**

en voor de duidelijkheid, theta is een functie.

> **Verduidelijking of addendum 3.2.2** bekijk nog
>
> cursus ging hier echt kort over dus wederom iets dat je nog eens dieper moet bekijken, eigenlijk gewoon een drietal oefeningen maken met de vtk oplossingensleutel en dan zul je het wel nappen.

**cyclische groepen**

We noemen een groep $(V, \circ)$ een cyclische groep als en slechts als er $a \in V$ zodat elk element van V geschreven kan worden onder de vorm $a^m, m \in \mathbb{Z}$. En a is hier een **voortbrengend element** van de groep $(V, \circ)$

1. $(V, \circ)$ is een cyclische groep $\implies$ het is een abelse groep. Commutativiteit is een vereiste.
   **bewijs dit later nog!**
2. de ggd van de orde van V en het voortbrengend element is één.

$$\text{ggd}(\#V, a).$$

3. elke deelgroep van een cyclische groep is zelf ook cyclisch.
4. groepen met als orde een priemgetal zijn altijd cyclisch. **(zie bewijs op slides!)**

en het idee is dus dat elk element geschreven kan worden als een product van het voortbrengend element met zichzelf.

> **Verduidelijking of addendum 3.2.3** hoe je dit moet interpreteren
>
> Bij een additieve groep staat $x^m$ gelijk aan $mx$, dus je moe teigenlijk dat tot de macht zien als een aantal keer dat je de operatie uitvoert op het element.

**verband tussen cyclische groepen en isomorfismen**

1. als een groep van oneindige orde cyclisch is, dan is deze isomorf met $(Z, +)$
2. als een groep een eindige orde heeft en cyclisch is, dan is deze isomorf met $Z_m, +$

**direct product van groepen**

> **Voorbeeld 3.2.2**
>
> Beschouw een groep $(V, \circ)$ en $(W, \blacksquare)$ We onderzoeken in de verzameling $V \times W$ de bewerking $\star$ die als volgt gedefinieerd wordt:
>
> $$(v_1, w_1) \star (v_2, w_2) = (v_1 \circ v_2, w_1 \blacksquare w_2).$$

we hebben nu een nieuwe groep:

$$(V \times W, \star).$$

**Voorbeeld 3.2.3**

We zoeken het direct product van

$$(Z_2, +) \text{ en } (Z_3, +).$$

- groep met 6 elementen
- $([1]_2, [1]_3)$ is het genererend element.
- hieruit volgt dat het isomorf is met $(Z_m, +)$
- dit is mod 6 rekening ontbonden in mod 2 en drie rekening

**Verduidelijking of addendum 3.2.4** bekijk filmpje

je gaat hier zeker een youtube filmpje over moeten zoeken.

**Verduidelijking of addendum 3.2.5** nut

dit is nuttig voor het ontbinden van grote groepen tot kleine bouwstenen of het combineren van kleine tot grote.

**Permutatiegroepen**

we bekijken dit thema beperkt tot eindige verzamelingen.
Voor een verzameling V met n elementen bestaan er n! verschillende elementen.

**Verduidelijking of addendum 3.2.6** Waarom zijn er n! elementen?

Het is eigenlijk enorm simpel en de cursus is wederom onduidelijk. Je mapt $A \to A$, dus eigenlijk het enige dat je doet is je schrijft de elemnten in een verschillende volgorde en noemt de nieuwe groep een permutatiegroep.

de manier waarop je de permutatiegroep schrijft is niet echt een matrix, cyclusnotaties wordt gehanteerd. Stel

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}.$$

Dan schrijf je de cycli op als volgt:

$$(134).$$

Dit is de cyclusnotatie. Omdat de 5 en de 2 naar zichzelf gaan schrijf ik die niet op. Je kan eigenlijk ook zeggen

$$(134)(2)(5).$$

### 3.2.2 twee binaire gewerkingen