ALGEBRAÏSCHE VOORKENNIS

(Dit wordt niet op het college behandeld)

Groepen.

Een groep is een verzameling G met daarop een binaire operatie $\cdot$ zodat

1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ voor alle $a, b, c \in G$ (associatieve eigenschap)
2) er is een element $e \in G$ (neutraal element) zodat $a \cdot e = e \cdot a = a$ voor alle $a \in G$.
3) bij elke $a \in G$ hoort een element a^{-1} (inverse) zodat $a \cdot a^{-1} = a^{-1} \cdot a = e$

Het neutrale element en de inverse zijn door deze regels eenduidig bepaald
Een groep heet abels of commutatief als bovendien
4) $a \cdot b = b \cdot a$ voor alle $a, b \in G$.

In dit college hebben we voornamelijk met abelse groepen te maken.

Een ondergroep van een groep G met operatie $\cdot$ is een deelverzameling H van G die met dezelfde operatie $\cdot$ van G een groep vormt. Notatie $H \leq G$.

Stelling 1. H ondergroep van $G \iff H \subset G$ en $ab^{-1} \in H$ voor alle $a, b \in H$.

H heet een normaaldeler van G, notatie $H \trianglelefteq G$, als H een ondergroep is van G en als

A2

$aHa^{-1} = H$ voor alle $a \in G$, d.w.z.
$axa^{-1} \in H$ voor alle $x \in H$, $a \in G$.

Als G abels is, is elke ondergroep een normaaldeler.

- Uit een groep G en een normaaldeler H van G kunnen we als volgt de factorgroep G/H vormen:

de elementen van G/H zijn de nevenklassen
$aH = \{a.x : x \in H\}$;
de groepsoperatie is $(aH).(bH) = abH$.

De orde van een groep G met operatie $\cdot$ is het aantal elementen van G, notatie $|G|$.

Stelling 2. (Lagrange). Als G een eindige groep is en H is een ondergroep van G, dan is $|H|$ een deler van $|G|$.

Een groepshomomorfisme $f: G_1 \to G_2$ van een groep G_1 naar een groep G_2 is een afbeelding zodat

$$f(a.b) = f(a).f(b) \quad \text{voor } a, b \in G_1.$$

Een groepsisomorfisme is een groepshomomorfisme dat inverteerbaar is. Twee groepen heten isomorf, notatie $G_1 \cong G_2$, als er een isomorfisme $f: G_1 \to G_2$ bestaat.

We definiëren e_{G_2} eenheidselt van G_2.

$\ker f = \{x \in G_1 : f(x) = e_{G_2}\}$ (de kern van f)
$\operatorname{im} f = \{f(x) : x \in G_1\}$ (het beeld van f)

A3

Stelling 3 (Homomorfiestelling) Ker f is een normaaldeler van G_1 en $G_1/\ker f \cong \text{im}(f)$.

Een groep G heet cyclisch als er een element $a \in G$ bestaat zodat

$$G = \{a^n : n \in \mathbb{Z}\}.$$

(a^n is $n\times$ a met zichzelf vermenigvuldigd als $n > 0$, $a^n = (a^{-1})^m$ als $n = -m < 0$, $a^0 = e$)
We geven bovenstaande groep wel aan met $\langle a \rangle$. en we noemen a een voortbrenger van G.

Stelling 4 (i). Een ondergroep van een cyclische groep is weer cyclisch.
(ii) Een oneindige cyclische groep is isomorf met $\mathbb{Z}$ (additieve groep)
(iii) Zij $G = \langle a \rangle$ een eindige cyclische groep van orde zeg m. Dan is $G = \{e, a, a^2, \ldots, a^{m-1}\}$ (als verzameling) ~~Verder a^k~~ en $a^m = e$.
Verder is a^k een voortbrenger van $G \iff \text{ggd}(k,m) = 1$.

Zij G een willekeurige groep. De orde van $a \in G$, notatie ord(a), is het kleinste positieve gehele getal m zodat $a^m = e$; wanneer zo'n m niet bestaat zeggen we dat $\text{ord}(a) = \infty$.

Stelling 4. Zij G een groep, $a \in G$, $\text{ord}(a) = m$.

(i) $a^k = e \iff k \equiv 0 \pmod m$
(ii) $a^{k_1} = a^{k_2} \iff k_1 \equiv k_2 \pmod m$
(iii) $e, a, a^2, \ldots, a^{m-1}$ zijn verschillend.
(iv) de cyclische groep $\langle a \rangle$ heeft orde m
(v) als G eindig is dan is m een deler van $|G|$: dus $a^{|G|} = e$.

Gevolg. Als $\text{ord}(a) = m$ dan is $\text{ord}(a^k) = \frac{m}{\text{ggd}(k,m)}$ voor $k \in \mathbb{Z}$

Bewijs. Zij r de orde van a^k. Dan geldt:

$$(a^k)^{\frac{m}{\text{ggd}(k,m)}} = a^{\frac{km}{\text{ggd}(k,m)}} = (a^m)^{\frac{k}{\text{ggd}(k,m)}} = e. \quad \text{Dus } r \mid \frac{m}{\text{ggd}(k,m)}.$$

Anderzijds is $a^{kr} = e$. Dus $kr \equiv 0 \pmod m$
We vinden zo:

$$k \mid kr,\ m \mid kr \Rightarrow \text{kgv}(k,m) = \frac{km}{\text{ggd}(k,m)} \mid kr \Rightarrow \frac{m}{\text{ggd}(k,m)} \mid r.$$

□

Ringen.

Een ring is een verzameling R, met daarop twee binaire operaties $+$ (optelling) en $\cdot$ (vermenigvuldiging) zo dat

(1) R met $+$ is een abelse groep; (neutraal element 0; de inverse van a t.a.v. $+$ geven we aan met $-a$);

(2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ voor alle $a, b, c \in R$;
(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ voor alle $a, b, c \in R$;
(4) $(a + b) \cdot c = a \cdot c + b \cdot c$ voor alle $a, b, c \in R$.

In dit college beschouwen we alleen <u>commutatieve</u> ringen met 1. Zulke ringen voldoen nog aan de volgende eisen:

(5) $a \cdot b = b \cdot a$ voor alle $a, b \in R$;
(6) er is een element $1 \in R$, zodat $1 \neq 0$ en zodat $a \cdot 1 = 1 \cdot a = a$ voor alle $a \in R$.

Dus wanneer we over een ring spreken nemen we impliciet aan dat die aan (5) en (6) voldoet.

Een element $a \in R$ heet een <u>eenheid</u> als er een $b \in R$ is met $a \cdot b = 1$.
De eenheden van R vormen een groep, de <u>eenhedengroep</u> van R, die we met R^* aangeven.

<u>Voorbeeld.</u> $\mathbb{Z}^* = \{1, -1\}$

A5)

We zeggen dat een element a van een ring R een element $b \in R$ deelt, notatie $a \mid b$, als er een $c \in R$ bestaat met $a \cdot c = b$.

Er geldt: $a \mid b$ en $b \mid a \iff$ er is een eenheid $\varepsilon \in R^*$ met $b = a \cdot \varepsilon$.

(zulke a en b heten <u>geassocieerd</u>.)

Een <u>ideaal</u> van een ring R is een deelverzameling $I \subset R$ zodat

(1) voor alle $a, b \in I$ geldt: $x - y = x + (-y) \in I$;
(2) voor alle $a \in I$, $r \in R$ is $r \cdot a \in I$.

Het ideaal voortgebracht door een element a van R, notatie (a) of aR is het kleinste ideaal van R dat a bevat. Er geldt:

$$(a) = \{r \cdot a : r \in R\}$$

Zo'n ideaal heet een <u>hoofdideaal</u>. Een <u>hoofdidealring</u> is een ring waarvan elk ideaal een hoofdideaal is.

Uit een ring R en een ideaal $I \subset R$ kunnen als volgt de <u>restklassenring</u> R/I worden gevormd:

de elementen zijn $a + I = \{a + x : x \in I\}$ (de restklassen)
de optelling is $(a + I) + (b + I) = (a + b) + I$;
de vermenigvuldiging is $(a + I) \cdot (b + I) = a \cdot b + I$.

Voorbeeld. $\mathbb{Z}/(n)$ $(n>0)$ ook wel genoteerd als $\mathbb{Z}_n$ of $\mathbb{Z}/n\mathbb{Z}$,

De elementen van $\mathbb{Z}/(n)$ zijn $\bar{a} = a+(n) = \{x \in \mathbb{Z} : x \equiv a \pmod n\}$
met $a \in \{0, 1, \ldots, n-1\}$
$\mathbb{Z}/(n)$ met $+$ is een cyclische groep van orde n
(op isomorfie na de enige)

De eenhedengroep van $\mathbb{Z}/(n)$ is

$$(\mathbb{Z}/(n))^* = \{\bar{a} \in \mathbb{Z}/(n) : \exists\, \bar{b} \in \mathbb{Z}/(n) \text{ met } \bar{a}\cdot\bar{b} = \bar{1}\}$$

$$= \{\bar{a} \in \mathbb{Z}/(n) : \gcd(a,n) = 1\}.$$

Zij $n = p_1^{k_1} \cdots p_t^{k_t}$ met $p_1, \ldots, p_t$ verschillende priemgetallen, $k_1 > 0, \ldots, k_t > 0$. Definieer $\varphi(n) := p_1^{k_1-1}(p_1-1)\cdots p_t^{k_t-1}(p_t-1)$.
Dan geldt:

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

Uit Stelling 4.1(v) volgt nu: $\bar{a} \in (\mathbb{Z}/(n))^* \Rightarrow \bar{a}^{\varphi(n)} = \bar{1}$ m.a.w.

Stelling 5 (Fermat-Euler). $\gcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$

In het bijzonder als $n = p$ is een priemgetal, dan volgt:
$p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$

Een ringhomomorfisme is een afbeelding $f : R_1 \to R_2$ van een ring R_1 naar een ring R_2 zodat
(1) $f(a+b) = f(a) + f(b)$ voor alle $a, b \in R$;
(2) $f(a\cdot b) = f(a)\cdot f(b)$ voor alle $a, b \in R$.

Een inverteerbaar ringhomomorfisme heet een ringisomorfisme.
Voor een ringhomomorfisme $f: R_1 \to R_2$ definiëren we:

$\ker f = \{a \in R_1 : f(a) = 0\}$ (de kern van f)
$\operatorname{im} f = \{f(a) : a \in R_1\}$ (het beeld van f)

Stelling 6. (homomorfiestelling voor ringen)
$\ker f$ is een ideaal en

$$R_1/\ker f \cong \operatorname{im} f.$$

Lichamen

Een lichaam is een verzameling K met twee operaties $+$ (optelling) en $\cdot$ (vermenigvuldiging) zodat

1) K is met $+$ en $\cdot$ een commutatieve ring met eenheidselement $1 \neq 0$;
2) voor elke $a \in K$ met $a \neq 0$ is er een inverse a^{-1} zodat $a \cdot a^{-1} = a^{-1} \cdot a = 1$
(m.a.w. $K^* = K \setminus \{0\}$ is met $\cdot$ een groep)

Voorbeelden: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...

Stelling 7. $\mathbb{Z}/(n)$ is een lichaam $\Leftrightarrow$ n is een priemgetal

We geven het eindige lichaam van p-priemgetal elementen wel aan als $\mathbb{F}_p$. In de literatuur komt ook $GF(p)$ voor.

Vectorruimten

Op de colleges lineaire algebra worden vectorruimten over $\mathbb{R}$ en over $\mathbb{C}$ behandeld. Op precies dezelfde manier kunnen vectorruimten met scalairen uit een willekeurig lichaam worden gedefinieerd.

Een vectorruimte over een lichaam K of K-vectorruimte is een verzameling V met twee operaties $+$ (vectoroptelling) en $\cdot$ (scalaire vermenigvuldiging) zodat

1) V met $+$ is een abelse groep (neutraal element 0; de inverse van a t.o.v. $+$ geven we aan met $-a$);

2) voor alle $a \in V, \lambda \in K$ is $\lambda \cdot a \in V$
3) $\lambda(a+b) = \lambda a + \lambda b$ voor $a, b \in V, \lambda \in K$,
4) $(\lambda+\mu)a = \lambda a + \mu b$ voor $a \in V, \lambda, \mu \in K$,
5) $\lambda(\mu a) = (\lambda\mu)a$ voor $a \in V, \lambda, \mu \in K$,
6) $1 \cdot a = a$ voor $a \in V$.

Een <u>lineaire deelruimte</u> van V is een deelverzameling W van V die met de optelling $+$ en scalaire vermenigvuldiging $\cdot$ van V weer een K-vectorruimte is.

<u>Stelling 8</u> W is een lineaire deelruimte van V
$\Leftrightarrow W \subset V$ en $\lambda a + \mu b \in W$ voor alle $a, b \in W$, $\lambda, \mu \in K$

A.2

Voorbeeld. Zij $\mathbb{F}_2 = \{0,1\}$ het lichaam van 2 elementen. We definiëren de $\mathbb{F}_2$-vectorruimte

$$\mathbb{F}_2^n = \{ (a_1, \dots, a_n) : a_1, \dots, a_n \in \mathbb{F}_2 \}$$

met

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) := (a_1 + b_1, \dots, a_n + b_n)$$
$$\lambda (a_1, \dots, a_n) := (\lambda a_1, \dots, \lambda a_n) \quad \text{voor } \lambda \in \mathbb{F}_2.$$

Zij $W = \{ (a_1, \dots, a_n) \in \mathbb{F}_2^n : a_1 + \dots + a_n = 0 \}$

Dan is W een lineaire deelruimte van V.

Zij V een K-vectorruimte. Een stel vectoren $\{\underline{a}_1, \dots, \underline{a}_n\} \subset V$ heet <u>lineair onafhankelijk</u> als uit $\lambda_1 \underline{a}_1 + \dots + \lambda_n \underline{a}_n = \underline{0}$ $(\lambda_1, \dots, \lambda_n \in K)$ volgt dat $\lambda_1 = 0, \dots, \lambda_n = 0$

Anders heet $\{\underline{a}_1, \dots, \underline{a}_n\}$ lineair afhankelijk.

We zeggen dat V wordt <u>voortgebracht</u> door een stel vectoren $\{\underline{a}_1, \dots, \underline{a}_n\}$ als
$V = \{ \lambda_1 \underline{a}_1 + \dots + \lambda_n \underline{a}_n : \lambda_1, \dots, \lambda_n \in K \}$.

Een stel vectoren $\{\underline{a}_1, \dots, \underline{a}_n\}$ heet een <u>basis</u> van V als
1) V wordt voortgebracht door $\{\underline{a}_1, \dots, \underline{a}_n\}$;
2) $\{\underline{a}_1, \dots, \underline{a}_n\}$ lineair onafhankelijk is.

Een vectorruimte hoeft geen basis te hebben. Als een vectorruimte wel een basis heeft dan geldt:

Stelling 9 Zij V een K-vectorruimte met een basis. Dan is het aantal elementen in een basis van V onafhankelijk van de keuze van die basis.

Het aantal elementen in een basis van V heet de dimensie van V. We zeggen dat V oneindige dimensie heeft als V geen basis heeft.

Een vectorruimte-homomorfisme of lineaire afbeelding is een afbeelding $f: V_1 \to V_2$ van K-vectorruimten zodat

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y) \quad \text{voor } x, y \in V_1, \ \lambda, \mu \in K.$$

Een inverteerbaar vectorruimte-homomorfisme heet wel een vectorruimte-isomorfisme.