II. Lichamentheorie

H8 priemlichamen, charact, lin. algebra in lichamen toegepast

Def zij K lichaam. $K' \subset K$ heet een deellichaam als geldt

(a) $1 \in K'$

(b) $a,b \in K' \Rightarrow K' \ni a-b$

(c) $a,b \in K',\ b \neq 0 \Rightarrow ab^{-1} \in K'$

Vgl met deelring $R' \subset R$:

(D1) $1 \in R'$

(D2) $(R',+)$ is o.g. van $(R,+)$

(D3) $a,b \in R' \Rightarrow ab \in R$

we zien dat deellichamen deelringen zijn:
(a) $\Leftrightarrow$ (D1), (a),(b) $\Rightarrow$ (D2) want $0 = 1-1 \in K'$ en $a-b \in K'$
en (a),(c) $\Rightarrow$ als $a,b \in K'$ dan $a,\ 1b^{-1} \in K'$ dus $K' \ni a(b^{-1})^{-1} = ab \Rightarrow$ (D3)

de omkering is echter niet waar: als een deelring geen lichaam is bijvoorbeeld, zoals $\mathbb{Z}[i] \subset \mathbb{C}$, dan kan het ook geen deellichaam zijn, want

St/Prop $K' \subset K$ deellichaam is met $+|_{K'}, \cdot|_{K'}$ en $0, 1$ uit K (die ook in K' liggen) zelf een lichaam.

Bew we weten al dat een deelring $R' \subset R$ voor willekeurige ring R zelf een ring is. K' is deelring dus voldoet hiermee al aan (R1) t/m (R4). Resteert aan te tonen:

wegens (R5) in K.

(R5): simpel, want $a,b \in K'$, dan $a \cdot|_{K'} b = a \cdot b = b \cdot a$
$= b \cdot|_{K'} a$

(R6): in feite zijn (R1) t/m (R5) te bewijzen uit (D1) t/m (D3) en het feit dat K comm. ring is.
nu pas gebruiken we (c): als $a,b \in K'$, $b \neq 0$ dan $ab^{-1} \in K$.
Dat levert namelijk op: $1, b \in K'$ voor $b \in K'$, dus $1b^{-1} \in K'$ voor $b \in K$, als $b \neq 0$. Dus elke $b \in K'$ heeft een inverse en wel dezelfde als in K. Dus is K' delingsring, comm. dus lichaam. $\square$

Doorsneden van deellichamen zijn zelf weer deellichamen.

Def (Priemlichaam) Zij $\mathcal{C}$ de collectie van alle deellichamen van K. Dan is het priemlichaam van K, K_0, gedefinieerd als

$$K_0 = \bigcap_{K' \in \mathcal{C}} K'$$

— Dit is het "kleinste" deellichaam van K mbt. inclusie-ordening op $\mathcal{C}$. Immers als $K' \in \mathcal{C}$ dan $K_0 \subset K'$. We zien ook dat vanwege (a) en (b) volgt $0,1 \in K'$, $\forall K' \in \mathcal{C}$ dus $0,1 \in K_0$.

St. 8.2 Zij K lichaam. Dan is K_0 ofwel isomorf met $\mathbb{Q}$ ofwel met een $\mathbb{F}_p$ voor een zeker priemgetal p.

Bew Definieer $\kappa : \mathbb{Z} \to K$ door $\kappa(n) = 1+1+\dots+1 = n1 \in K_0$

$\kappa(-n) = -(1+1+\dots+1) = \underbrace{-(n1)}_{=(-n)1} \in K_0$ $\quad \kappa(0) = 0 \in K_0$

voor $n \in \mathbb{Z}_{\geq 0}$, dit dekt alle gevallen. Merk op dat wegens $0,1 \in K_0$ en (a),(b),(c) die van toepassing zijn op K_0, geldt $1+1+\dots+1 \in K_0$ en ook $-(1+\dots+1) \in K_0$ en $0 \in K_0$.

Hierdoor is $\kappa(\mathbb{Z}) \subset K_0$.

Bovendien volgt $\kappa(n+m) = (n+m)1 = n1 + m1 = \kappa(n) + \kappa(m)$

en $\kappa(1) = (1)1 = 1$ en $\kappa(nm) = (nm)1 = (n1)(m1) = \kappa(n)\kappa(m)$

dus κ is een ringhomomorfisme $\kappa : \mathbb{Z} \to K_0$.

Nu hangt de rest af van wat $\operatorname{Ker}(\kappa)$ wordt.

— Maar eerst: het beeld van een ringhomomorfisme is een deelring van K_0 (zie H2). Omdat K_0 een lichaam is, heeft het geen nuldelers (eenheden zijn geen nuldelers en 0 ook niet) en $1,0 \in K_0$ en $1 \neq 0$ in K dus $1 \neq 0$ in K_0. Bovendien $1,0 \in \kappa(\mathbb{Z})$. Dus $\kappa(\mathbb{Z})$ is een domein en omdat $\mathbb{Z}/\operatorname{Ker}(\kappa) \cong \kappa(\mathbb{Z})$ volgt wegens st. 4.5 dat $\operatorname{Ker}(\kappa)$ een priemideaal in $\mathbb{Z}$ is, dus $\operatorname{Ker}(\kappa) = \{0\}$ of (p) met p priemgetal.

(nu wordt duidelijk waar we naartoe gaan!)

(i) als $\operatorname{Ker}(\kappa) = \{0\}$, dan is κ injectief. Nu gaan we een nieuwe functie definiëren:

$$\kappa_1 : \mathbb{Q} \to K_0 \quad \text{door} \quad \kappa_1\left(\frac{a}{b}\right) = \overbrace{\kappa(a)\,\kappa(b)^{-1}}^{\in K_0 \text{ wegens (c) en } \kappa(\mathbb{Z}) \subset K_0}$$

voor $a, b \in \mathbb{Z}$, $b \neq 0$, dus $\frac{a}{b} \in \mathbb{Q} = Q(\mathbb{Z})$

is dit welgedefinieerd? dwz als $\frac{a}{b} = \frac{a'}{b'}$ ($a'b = b'a$) is dan moet volgen $\kappa(a)\kappa(b)^{-1} = \kappa(a')\kappa(b')^{-1}$

neem dus $b \neq 0 \neq b'$, $a'b = b'a$ in $\mathbb{Z}$. Dan

$\kappa(a)\kappa(b') = \kappa(a')\kappa(b)$ want $\kappa(a)\kappa(b') = \kappa(ab') = \kappa(a'b) = \kappa(a')\kappa(b)$

en dus ($\uparrow$ neem inv. κ, neem inv) $\kappa(a)\kappa(b')\kappa(b')^{-1}\kappa(b)^{-1} = \kappa(a')\kappa(b)\kappa(b')^{-1}\kappa(b)^{-1}$

en dit geeft $\kappa(a)\kappa(b)^{-1} = \kappa(a')\kappa(b')^{-1} \Rightarrow \kappa_1\left(\frac{a}{b}\right) = \kappa_1\left(\frac{a'}{b'}\right)$

welgedefinieerd

bovendien voor $n \in \mathbb{Z}$ geldt in $\mathbb{Q}$ $n \leftrightarrow \frac{n}{1}$ dus

$\kappa_1(n) = \kappa_1\left(\frac{n}{1}\right) = \kappa(n)\kappa(1)^{-1} = \kappa(n)$, dus $\kappa_1\big|_{\mathbb{Z}(\subset \mathbb{Q})} = \kappa$.

Het is dus een welgedefinieerde voortzetting van κ op $\mathbb{Q}$.

Bovendien is het een homom, want

- $\kappa_1\left(\frac{a}{b}\cdot\frac{c}{d}\right) = \kappa(ac)\,\kappa(bd)^{-1} = \kappa(a)\kappa(c)\kappa(b)^{-1}\kappa(d)^{-1}$
$= \kappa(a)\kappa(b)^{-1}\cdot\kappa(c)\kappa(d)^{-1} = \kappa_1\left(\frac{a}{b}\right)\kappa_1\left(\frac{c}{d}\right)$
- $\kappa_1\left(\frac{a}{b} + \frac{c}{d}\right) = \kappa_1\left(\frac{ad+bc}{bd}\right) = \kappa(ad+bc)\,\kappa(bd)^{-1}$
$= (\kappa(a)\kappa(d) + \kappa(b)\kappa(c))\,\kappa(b)^{-1}\kappa(d)^{-1}$
$= \kappa(a)\kappa(b)^{-1} + \kappa(c)\kappa(d)^{-1} = \kappa_1\left(\frac{a}{b}\right) + \kappa_1\left(\frac{c}{d}\right)$
- en $\kappa_1(1) = \kappa(1) = 1$

Dus is $\kappa_1 : \mathbb{Q} \to K_0$ een lichaamshomomorfisme waarvan we weten (H2) dat het dus injectief is, en dus bovendien is $\kappa_1(\mathbb{Q}) \cong \mathbb{Q}$. Maar dan is $\kappa_1(\mathbb{Q})$ lichaam dat een deellichaam is van K, dus $K_0 \subset \kappa_1(\mathbb{Q})$. omdat het beeld $\kappa_1(\mathbb{Q}) \subset K_0$, volgt $\mathbb{Q} \cong K_0$.

(ii) Stel $\operatorname{Ker}(\kappa) = (p)$. Dan is $\kappa(\mathbb{Z}) \cong \mathbb{Z}/(p)$ en $\mathbb{Z}/(p) =: \mathbb{F}_p$ is een lichaam, dus $\kappa(\mathbb{Z})$ is deellichaam van K_0 van K, maar K_0 is het kleinste deellichaam van K dus $K_0 \subset \kappa(\mathbb{Z})$, $\kappa(\mathbb{Z}) \subset K_0 \Rightarrow K_0 = \kappa(\mathbb{Z}) \cong \mathbb{F}_p$.

$\square$

Karakteristiek

Def voor K lichaam met priemlichaam K_0 definiëren we het <u>karakteristiek</u> van K, $\mathrm{char}(K)$, als volgt: $\mathrm{char}(K) = 0$ als $K_0 \cong \mathbb{Q}$
$\mathrm{char}(K) = p$ als $K_0 \cong \mathbb{F}_p$. □

Opm We zien dus dat $\big(\mathrm{char}(K)\big) = \mathrm{Ker}(\kappa)$

Opm 2 ! We kunnen $\mathrm{char}(R)$ definiëren voor willekeurige ringen op deze manier met $\kappa : \mathbb{Z} \to R$.

Als echter R geen domein is, kan het voorkomen dat $\kappa(\mathbb{Z}) \subset R$ dat niet is in welk geval $\mathrm{char}(R)$ niet 0 of priem hoeft te zijn.

Anders is $\kappa(\mathbb{Z})$ wél een domein, zodat uit $\mathbb{Z}/\mathrm{Ker}(\kappa) \cong \kappa(\mathbb{Z})$ volgt dat $\mathrm{Ker}(\kappa)$ wel door 0 of p wordt voortgebracht.

Opm 3 ! κ is tevens voor R een commutatieve ring het <u>unieke</u> homomorfisme $\mathbb{Z} \to R$. Immers volgt met dezelfde stappen uit het bewijs dat κ een homomorfisme is, en uniciteit volgt omdat, als $\phi : \mathbb{Z} \to R$ homomorfisme is, dan voor $n \in \mathbb{Z}_{>0}$ volgt $n = \underbrace{1+1+\dots+1}_{n \text{ termen}} \in \mathbb{Z}$, dus $\phi(n) = \phi(\underbrace{1+1+\dots+1}_{n \text{ termen}}) = \underbrace{\phi(1)+\dots+\phi(1)}_{n \text{ termen}}$ wegens additiviteit van ϕ en dit is (daar $\phi(1) = 1$), $1+1+\dots+1 \in R$. Hetzelfde volgt voor $-n \in \mathbb{Z}_{\leq 0}$ en 0 dus $\phi = \kappa$ volgt.

— (**Gevolg**) R domein met $\mathrm{char}(R) = p$ priem >0 (priem is als $p>0$ nogal wiedes want $\mathbb{Z}/p\mathbb{Z} \cong \kappa(\mathbb{Z}) \subset R$, een domein) dan geldt voor alle $a, b \in K$ dat

$(a+b)^p = a^p + b^p$ en gevolg hiervan is dat

$F : R \to R$ door $x \mapsto x^p$ een endomorfisme (homom $R \to R$) en als R een lichaam is, is F injectief

— Bewijs: gebruik het binomium van newton voor commutatieve ringen: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ waar $\binom{n}{k} = \underbrace{1+1+\cdots+1}_{\binom{n}{k} \text{ keer}}$. Dan volgt dat voor p geldt: $\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{(p-k)(p-k-1)\cdots 1}$ als $p > k > 0$, dan

- de noemer heeft alleen factoren kleiner dan p en de teller heeft een factor p. Omdat p priem is, kan er geen factor p in de noemer zitten want dan zouden kleinere factoren samen p kunnen vormen dus is p niet irred. contradictie, of blijkbaar is er dan geen unieke priemontb van de noemer omdat deze zowel in irred factoren zonder als met p ontb. kan worden. Dat klopt ook niet, $\mathbb{Z}$ is PID. dus omdat er toch een geheel getal **uitkomt**, volgt dan $\binom{p}{k}$ door p deelbaar is $\Longrightarrow (a+b)^p = a^p + b^p + \sum_{k=1}^{n-1} \binom{p}{k} a^k b^{n-k}$
$= a^p + b^p + pc = a^p + b^p$.

omdat R commutatief is, volgt $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$ en $F(1) = 1^p = 1$ en $F(x+y) = (x+y)^p = x^p + y^p = F(x) + F(y)$ dus $F: R \to R$ is inderdaad homom. Als R een lichaam is moet $\ker(F) = \{0\}$ zijn (2.10) dus is F injectief $\square$

Def we noemen een lichaam perfect als $F: K \to K$ ook surjectief is: dan bestaat dus voor $p = \mathrm{char}(K)$ priem >0 de unieke p-de machtswortel van $x \in K$ voor alle $x \in K$. ($\sqrt[p]{x}$)

ook lichamen K met $\mathrm{char}(K) = 0$ heten perfect

Def F heet ook wel het Frobenius-homomorfisme.

— vectorruimten en lineaire algebra: een K-vectorruimte voor een lichaam K is een abelse (additief geschreven) groep $(V, +, 0)$ die behalve aan G1 t/m G4 ook voldoet aan : er is een afb; $\cdot : K \times V \to V$ met

(V1)	$\lambda(v+w) = (\lambda v)+(\lambda w)$	$\forall \lambda \in K$	$v, w \in V$
(V2)	$(\lambda+\mu)v = (\lambda v)+(\mu v)$	$\forall \lambda, \mu \in K$	$v \in V$
(V3)	$\lambda(\mu v) = (\lambda\mu)v$	$\forall \lambda, \mu \in K$	$v \in V$
(V4)	$1v = v$	$\forall v \in V$	

— als $K \subset L$ lichaamsuitbreiding is (we zeggen dat L K uitbreidt precies als K een deellichaam van L is) dan is L i.h.b. een K-vr. als we als bewerking $\cdot : K \times V$ gewoon vermenigvuldiging in L nemen beperkt tot $K \times L$: wegens de twee distributieve wetten volgen (V1) & (V2), wegens $1 \in K \subseteq L$ de identiteit volgt (V4) en wegens associativiteit van $\cdot$ volgt (V3).

Def De graad van de uitbreiding is dan gedefinieerd als $[L:K] :=$
$\dim_K(L) = |B|$ waar B een K-basis voor L is, dus een verzameling $B \subset V$ zodat voor elke $v \in V$ er een unieke eindig aantal $v_1, \ldots v_n \in V$ $(n \in \mathbb{N}_1)$ zijn en evenveel $\lambda_1, \ldots \lambda_n \in K$ met
$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$$

(dit kan een kardinaliteitsgetal zijn, vaak zeggen wij dan simpelweg "$\dim_K(L) = \infty$")

— als $W \subset V$ ondergroep is, dan is het een normaaldeler want V is abels en we hebben dan quotiëntgroep $V/W = \{v+W : v \in V\}$ welke weer een K-vectorruimte kan worden door $(\lambda, v+W) \mapsto (\lambda v)+W$ oftewel $(\lambda, \bar{v}) \mapsto \overline{\lambda v}$ als scalairverm. te kiezen.