Sølvkorn 7
Legemer og karakteristik

Rasmus Sylvester Bryder

Vi minder om, at enhver ringhomomorfi φ opfylder, at $\varphi(x+y) = \varphi(x) + \varphi(y)$, $\varphi(xy) = \varphi(x)\varphi(y)$ og $\varphi(1) = 1$ for alle x, y.

Sætning 1. *Enhver legemshomomorfi er injektiv.*

Bevis. Lad $\varphi : H \to L$ være en legemshomomorfi. Antag, at $x \in H$ er forskellig fra 0. Da er $1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, hvilket viser, at $\varphi(x) \neq 0$ for alle $x \neq 0$. □

Vi definerer for $n \in \mathbb{Z}$ og $h \in H$, hvor H er en ring:

$$nh = \begin{cases} \underbrace{h + \cdots + h}_{n} & \text{for } n > 0 \\ 0 & \text{for } n = 0 \\ (-n)(-h) = \underbrace{-h - \cdots - h}_{-n} & \text{for } n < 0 \end{cases}$$

Af denne definition følger regnereglerne

$$(n_1 + n_2)h = n_1h + n_2h \tag{1}$$
$$n(h_1 + h_2) = nh_1 + nh_2 \tag{2}$$
$$(n_1h_1)(n_2h_2) = (n_1n_2)(h_1h_2) \tag{3}$$

for $n, n_1, n_2 \in \mathbb{Z}$ og $h, h_1, h_2 \in H$. Disse bevises ikke her, men er lette at bevise ud fra definitionen (gør det!).

Vi definerer *karakteristikken* af en ring R som det mindste naturlige tal n, for hvilket gælder, at $n1_R = \sum_{i=1}^{n} 1_R = 0$. Hvis $\sum_{i=1}^{n} 1_R \neq 0$ for alle $n \in \mathbb{N}$, siger vi, at ringen har karakteristik 0.

Det er let at vise, at et legeme enten har primtalskarakteristik eller karakteristik 0: antag, at karakteristikken er sammensat $n = pq$, hvor $p, q < n$. Da vil $(pq)1 = 0$, men $p1 \neq 0$ og $q1 \neq 0$, thi n er det mindste tal, så $n1 \neq 0$. Det følger af (3) ovenfor, at $(pq)1 = (p1)(q1)$. Men dette strider imod, at nulreglen gælder i legemet.

En bemærkning, der er værd at knytte til alt dette, er at den cykliske undergruppe af den additive gruppe frembragt af 1-elementet, $\{n1 \mid n \in \mathbb{Z}\}$, er en delring af enhver betragtet ring, hvilket følger af ovenstående regneregler, og dette er den mindste delring forskellig fra nulringen i enhver ring – *primringen* kaldes den – thi enhver delring er nødt til at indeholde 1-elementet og må være stabil under addition.

Sætning 2. *Følgende tre betingelser er ækvivalente for en ring R og $m \in \mathbb{N}$:*

(1) R har karakteristik m.

(2) Homomorfien $\phi : \mathbb{Z} \to H$ givet ved $\phi(n) = n1$ har kerne $m\mathbb{Z}$.

(3) Primringen består af m elementer.

Bevis. (1) $\Rightarrow$ (2): Antag, at ringen R har karakteristik $m > 0$. Vi har pr. definition, at m er det mindste positive tal, så $\phi(m) = 0$; alle multiplum af m har altså billedet 0, hvorpå $m\mathbb{Z} \subseteq \ker \phi$. Hvis $n = am + r$, $0 < r < m$, $a \in \mathbb{Z}$, har vi desuden, at $\phi(n) = \phi(r) = r1 \neq 0$, thi m var det mindste positive tal n, så $n1 = 0$. Altså er $\ker \phi = m\mathbb{Z}$.

(2) $\Rightarrow$ (3): Vi har pr. isomorfisætningen, at $\mathbb{Z}/m$ er isomorf med $\phi(\mathbb{Z})$. Billedet af $\mathbb{Z}$ er netop alle elementer i R på formen $n1$, hvor $n \in \mathbb{Z}$; altså $\{n1 \mid n \in \mathbb{Z}\}$, eller primringen, som altså har m elementer.

(3) $\Rightarrow$ (1): $\{n1 \mid n \in \mathbb{Z}\}$ er den cykliske undergruppe $\langle 1 \rangle$ i $(R, +)$. Altså har 1 orden m i $(R, +)$. Da må R have karakteristik m. □

Hvis R har karakteristik 0, vil ϕ defineret som ovenfor ikke give billedet 0 for noget element i $\mathbb{Z}$ ud over 0, hvorpå $\ker \phi = 0\mathbb{Z}$.

Hvis $\ker \phi = 0\mathbb{Z}$, vil $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$ være indeholdt i R. $\mathbb{Z}$ er dermed isomorf med primringen, som dermed har uendelig mange elementer.

Hvis primringen har uendelig mange elementer, vil $n1 \neq 0$ for alle $n \in \mathbb{N}$, hvorpå R har karakteristik 0. Dette giver følgende sætning:

Sætning 3. *Følgende tre betingelser er ækvivalente for en ring R:*

(1) R har karakteristik 0.

(2) Homomorfien $\phi : \mathbb{Z} \to H$ givet ved $\phi(n) = n1$ er injektiv.

(3) Primringen består af uendelig mange elementer.

Vi tager nu skridtet videre og lader H være et legeme. Vi husker, at $\mathbb{Q}$ er et legeme og at $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ er et legeme for ethvert primtal p.

Sætning 4. *Legemet $\mathbb{F}_p$, hvor p er et primtal, er indeholdt i ethvert legeme H af karakteristik p, og er det mindste legeme af karakteristik p.*

Bevis. Hvis $\mathbb{F}_p$ er indeholdt i ethvert legeme af karakteristik p, må det følgelig være det mindste af slagsen. Homomorfien $\phi : \mathbb{Z} \to H$ givet ved $\phi(n) = n1$ har kerne $p\mathbb{Z}$. Altså vil $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ være isomorf med delringen $\phi(\mathbb{Z})$ af H, således at der findes en isomorfi $\eta : \mathbb{F}_p \to \phi(\mathbb{Z})$. Inklusionsafbildningen $\iota : \phi(\mathbb{Z}) \hookrightarrow H$ giver en injektiv afbildning $\iota \circ \eta : \mathbb{F}_p \hookrightarrow H$, hvorpå $\mathbb{F}_p$ er indeholdt i H. □

Hvis H har karakteristik p, er primringen i H isomorf med $\mathbb{F}_p$. Man kan også danne homomorfien $\varphi : \mathbb{F}_p \to H$ givet ved $\varphi(a) = a1$, som er veldefineret: hvis $m = n$ i $\mathbb{F}_p$, vil $p|m - n$, så $(m - n)1 = 0$ og $m1 = n1$. Sætning 1 giver da det ønskede.

Sætning 5. *Legemet $\mathbb{Q}$ er indeholdt i ethvert legeme H af karakteristik 0, og er det mindste legeme af karakteristik 0.*

Bevis. Hvis $\mathbb{Q}$ er indeholdt i ethvert legeme af karakteristik 0, må det følgelig være det mindste af slagsen. Betragt afbildningen $\varphi : \mathbb{Q} \to H$ givet ved $\varphi(z) = (a1)(b1)^{-1}$, hvor $z = \frac{a}{b}$, $a, b \in \mathbb{Z}$. Denne er veldefineret, thi hvis $\frac{a}{b} = \frac{c}{d}$ i $\mathbb{Q}$, findes $u, u' \neq 0$, så $ua = u'c$ og $ub = u'd$, hvorpå

$$\frac{a1}{b1} = \frac{(u1)(a1)}{(u1)(b1)} = \frac{(ua)1}{(ub)1} = \frac{(u'c)1}{(u'd)1} = \frac{(u'1)(c1)}{(u'1)(d1)} = \frac{c1}{d1}.$$

φ ses let at være en homomorfi med regneregler for legemer ($(ab)^{-1} = a^{-1}b^{-1}$) og ovenstående regneregler; det er let at se, at $\varphi(1) = 1$. Det ønskede følger nu af sætning 1. □

Dette kan også indses hurtigt således: hvis H er af karakteristik 0, må $\mathbb{Z}$ være indeholdt i H. Da indeholder H også inverser til alle heltal forskellige fra 0, og da indeholder H alle brøker.