Sølvkorn 2
Ringe etc.

Rasmus Sylvester Bryder

Jeg synes ikke, at bogen gør nok ud af at forklare om ringe og ringhomomorfier, så lad dette dokument (prøve at) klargøre, hvad der egentlig sker i ringkapitlet i Anders Thorups bog.

Nogle har tilsyneladende forstået dem fuldstændig.

Det er åbenbart ikke accepteret alle steder, at ringe har et multiplikativt neutralt element (altså, at vi om multiplikativiteten kun har, at den er associativ og brugt i den distributive lov). Så meget for global definition. På engelsk hedder disse ringe, der indeholder 1, "unit rings".

Det er ikke en selvfølge, at $\varphi(1) = 1$ er opfyldt for en afbildning på $R \to R'$, der opfylder (3.1.1). Betragt for eksempel $\mathbb{Z} \to \mathrm{Mat}_2(\mathbb{Z})$ givet ved, at $x \in \mathbb{Z}$ bliver ført over i 2×2-matricen med x i øverste venstre hjørne og 0 på de andre pladser. Da er de to første betingelser opfyldt, men billedet af 1 er tydeligvis ikke enhedsmatricen.

En grund til, at det kræves, skyldes nok observation 3.2: det er praktisk at have, at billedet af et element er invertibelt hvis elementet i originalmængden er det.

Vi har selvfølgelig, at $\varphi(0) = \varphi(0) + \varphi(0)$, hvorpå

$$\varphi(0) = (\varphi(0) + \varphi(0)) - \varphi(0) = 0.$$

Dette gælder for alle ringe og ringhomomorfier.

$\varphi(1) = 1$ er automatisk opfyldt, hvis $R \neq 0$ og R' er et integritetsområde. Vi har nemlig, at $\varphi(1) = \varphi(1)\varphi(1)$, hvorpå $\varphi(1)\varphi(1) - \varphi(1) = 0$, hvorpå altså $\varphi(1)(\varphi(1) - 1) = 0$. Idet $0 \neq 1$ er $0 \neq \varphi(1)$, så da R' er et integritetsområde, må $\varphi(1) = 1$. Det gælder selvfølgelig ikke generelt, så betingelsen er tilført for at bevare denne stabilitet.

Beviset for at en ringhomomorfi er injektiv hvis og kun hvis kernen er nulelementet, følger af at betragte ringenes additive grupper og benytte lemma GRP(5.4). Bogen kalder dette at "opfatte φ som en homomorfi af kommutative grupper".

Vi har, at $\varphi(-a) = -\varphi(a)$. Det følger af følgende udregning:

$$0 = \varphi(0) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a).$$

Altså er $\varphi(-a)$ den additive invers til $\varphi(a)$, nemlig $-\varphi(a)$.

Noget generelt om ringe, som lige kræver en afslutning: $\alpha - \mu = 0$ hvis og kun hvis $\alpha = \mu$.
"$\Leftarrow$": $\alpha = \alpha + 0 = \alpha + (-\mu + \mu) = (\alpha + (-\mu)) + \mu = 0 + \mu = \mu$.
"$\Rightarrow$": $\alpha - \mu = \alpha - \alpha = 0$.

Noget om idealer skal der også være plads til. Lad R være en ring.

Hvis $c \in (a)$, må $c = ra$ for et vist $r \in R$. Lad $s \in R$ være givet. Da har vi, at $sc \in (c)$. Da $sc = s(ra) = (sr)a \in (a)$, har vi, at $(c) \subseteq (a)$.

Vi har selvfølgelig, at $(c) = (a)$, hvis c og a er associerede.

Hvis u er en enhed, er $(u) = R$. Vi har nemlig, at $1 = uu^{-1} \in (u)$, idet $u^{-1} \in R$, da u er en enhed. Derpå er $r = r1 \in (u)$ for alle $r \in R$.

Den anden implikation gælder også. Lad u være givet, så $(u) = R$. Da er $1 \in (u)$; dvs. $1 = ru$ for et passende $r \in R$, men da ser vi, at u er invertibel med s som invers. u er en enhed.

Det var så 5.4(1).

Lad $p \in R$. Vi beviser lige sætning 5.4(6), altså at p er et primelement i R, hvis og kun hvis (p) er et primideal.

Antag, at p er primelement - da er p hverken 0 eller en enhed. Lad $a, b \in R$ være givet, så $ab \in (p)$. Da har vi, at $ab = pr$ for et $r \in R$, dvs. at $p \mid ab$. Men da p er et primelement, gælder enten at $p \mid a$ eller $p \mid b$. Da gælder enten, at $a = qp$ eller $b = sp$ for vist $q \in R$ eller $s \in R$, hvorpå $a \in (p)$ eller $b \in (p)$. Da er (p) et primideal, da $(p) \neq R$, idet p ikke var en enhed.

Vi husker, at (0) er et primideal, hvis R er et integritetsområde (2.10).

Antag, at (p) er et primideal og at $p \neq 0$. Da er (p) ægte, så p er ikke en enhed jf. 5.4(1). Lad $a, b \in R$ være givet, så $p|ab$. Da har vi, at $ab = rp$ for vist $r \in R$, derpå gælder, at $ab \in (p)$. Da (p) er et primideal, gælder, at $a \in (p)$ eller $b \in (p)$, dvs. enten $a = qp$ eller $b = sp$ for passende q, s, og dermed enten $p \mid a$ eller $p \mid b$. Da er p et primelement.