Ringer

Definisjon: En ring $(R,+,\cdot)$ består av en ikke-tom mengde R og to binære operasjoner $+$ og $\cdot$ på R slik at

(i) $+$ er assosiativ
(ii) $+$ er kommutativ
(iii) Det finnes et nøytralt element 0 for addisjon $(a+0=a)$
(iv) Ethvert element $a\in R$ har en additiv invers $-a$ $(a+(-a)=0)$

} $(R,+)$ er en abelsk gruppe

(v) $\cdot$ er assosiativ
(vi) Det finnes et nøytralt element 1 for multiplikasjon $(1\cdot a=a\cdot 1=a)$
(vii) $\cdot$ er distributiv med $+$ $(a(b+c)=ab+ac,\ (b+c)a=ba+ca)$

Setning: (i) $a\cdot 0=0\cdot a=0$ for alle $a\in R$.
(ii) $(-a)b=-(ab)$ og $a(-b)=-(ab)$ for alle $a,b\in R$
(iii) $(-a)(-b)=ab$ for alle $a,b\in R$.

Bevis: (i) $0+a\cdot 0 \overset{\text{def av } 0}{=} a\cdot 0 \overset{\text{def } 0}{=} a(0+0) \overset{\text{distr.}}{=} a\cdot 0+a\cdot 0$, dvs

$$0+a\cdot 0 = a\cdot 0 + a\cdot 0$$

Kan forkorte siden $(R,+)$ er en gruppe

Samt gir $0=a\cdot 0$. (kan nå si at $0\cdot a=0$ på samme måte)

(ii) Husk at $-c$ er det entydig bestemte element slik at $c+(-c)=0$

Vi må altså vise at $ab+(-a)b=0$. Men

$ab+(-a)b=(a+(-a))b=0\cdot b=0$, samt viser at $(-a)b=-(ab)$

Viser $a(-b)=-(ab)$ på samme måte.

(iii) Fra (ii): $(-a)(-b) \overset{(ii)}{=} -(a(-b)) = -(-ab) = ab$

$-(ab)$

Fordi inverser til inverser er elementet selv.

Definisjon (i) Vi sier at $a \in R$ oppfyller forkortningsregelen dersom hver gang $ab = ac$, så $b = c$.

(ii) Vi sier at $a \neq 0$ er en nulldivisor dersom det finnes en $b \neq 0$ slik at $ab = 0$

Setning: Et ikke-null element $a \in R$ oppfyller forkortningsregelen hvis og bare hvis den ikke er en nulldivisor.

Bevis: Anta først at a oppfyller forkortningsregelen. Vi må vise at hvis $ac = 0$, så er $c = 0$. Observer at $ac = 0$, betyr at

$$ac = a \cdot 0$$

Siden forkortningsregelen gjelder, gir dette $c = 0$.

Anta så at a ikke oppfyller forkortningsregelen; vi må vise a er en nulldivisor. Vi vet at det finnes elementer b, c slik at $ab = ac$, men $b \neq c$. Derved er

$$ab + a(-c) = 0 \Rightarrow a(\underbrace{b + (-c)}_{\neq 0}) = 0$$

som viser at a er en nulldivisor.

Notasjon: Vi skriver gjerne $a - b$ for $a + (-b)$.

Definisjon: Anta at $(R, +, \cdot)$ og $(S, +, \cdot)$ er to ringer. En funksjon fra $\varphi : R \to S$ kalles en (ring)-homomorfi dersom

(i) $\varphi(x+y) = \varphi(x) + \varphi(y)$ for alle $x, y \in R$

(ii) $\varphi(xy) = \varphi(x)\varphi(y)$ — " —

(iii) $\varphi(1_R) = 1_S$

En homomorfi som er bijektiv kalles en isomorfi.

Setning: $\varphi(0_R) = 0_S$.

Idealer

Definisjon: En delmengde I av en ring kalles et ideal dersom

(i) $0 \in I$

(ii) Hvis $x, y \in I$, så $x + y \in I$

(iii) Hvis $x \in I$, så er $-x \in I$

$\Big\}$ $(I, +)$ er en undergruppe av $(R, +)$

(iv) Hvis $x \in I$ og $r \in R$, så $rx, xr \in I$.

Eksempel: (i) $R = \mathbb{Z}$: $(t) = \{nt : n \in \mathbb{Z}\}$ er et ideal.

(ii) Anta $r_1, r_2, \ldots, r_n \in R$. Da er

$$I = \{s_1 r_1 + s_2 r_2 + \cdots + s_n r_n : s_1, s_2, \ldots, s_n \in R\}$$

et ideal (idealet generert av $r_1, r_2, \ldots, r_n$)

(iii) R = alle funksjoner $f : X \to R$

Hvis $a \in X$, så er

$$I_a = \{f \in R : f(a) = 0\}$$ et ideal.

(iv) R = alle polynomer $p(x)$

Velg et polynom $q(x)$ i R.

$I = \{p(x) : p(x)$ er delelig med $q(x)\}$ "polynomdivisjonen $p(x) : q(x)$ går opp"

Kvotientringer

Anta at R er en ring og at I er et ideal i R.

Definer en relasjon på R ved

$$x \sim y \iff y - x \in I$$

Grupper: $x^{-1}y \in I$

Setning: $\sim$ er en ekvivalensrelasjon

Bevis: (i) **Refleksiv** (dvs $x \sim x$): $x - x = 0 \in I$, da $x \sim x$

$x + (-x)$

(ii) **Symmetrisk** (dvs $x \sim y \Rightarrow y \sim x$). Anta at $x \sim y$, dvs $y - x \in I$. Dermed

$(-1)(y-x) \in I$, dvs $x - y \in I$ altså $y \sim x$.

(iii) **Transitiv** (dvs $x \sim y$ og $y \sim z$, da $x \sim z$) Anta at $x \sim y$ og $y \sim z$, dvs

$y - x \in I$ og $z - y \in I$. Vi må vise at $x \sim z$, dvs at $z - x \in I$.

Siden $z - x = (z-y) + (y-x) \in I$, så $x \sim z$.

$\Uparrow I$ $\quad \Uparrow I$

Setning: Hvis $x \sim x'$ og $y \sim y'$, da $x + y \sim x' + y'$ og $xy \sim x'y'$

Bevis: At $x \sim x'$ og $y \sim y'$, betyr at $x' - x \in I$ og $y' - y \in I$

$i \in I$ $\quad j \in I$

Dermed $x' = x + i$, $y' = y + j$. Vi får

$$(x'+y') - (x+y) = x + i + y + j - x - y = i + j \in I$$

$\Uparrow I$ $\quad \Uparrow I$

Dvs vist at $x + y \sim x' + y'$.

Tilsvarende for multiplikasjon:

$$x'y' - xy = (x+i)(y+j) - xy = xy + xj + iy + ij - xy$$

$$= xj + iy + ij \in I$$

$\Uparrow I$ $\quad \Uparrow I$ $\quad \Uparrow I$

La $R/\sim$ være mengden av alle ekvivalensklassene til $\sim$.

Vi skal innføre operasjoner på $R/\sim$ slik at $R/\sim$ blir en ring.

Idé: $[x][y] = [xy]$

$[x] + [y] = [x+y]$

Veldefinert.

Potensielt problem: Hva hvis $[x] = [x']$, $[y] = [y']$ men $[xy] \neq [x'y']$

Dette problemet oppstår ikke her pga av setningen ovenfor.

Teorem: $(R/\sim, +, \cdot)$ er en ring med nullelement $[0]$ og enhetselement $[1]$.

Bevis: Vi må sjekke alle sju aksiomene for en ring. Tar bare noen.

Sjekker at $[0]$ er et nullelement: $[a] + [0] = [a+0] = [a]$

0 er nullelement i den opprinnelige ringen.

Sjekker distributiv lov: $[a]([b]+[c]) = [a][b] + [a][c]$

Regner ut venstresiden $[a]([b]+[c]) = [a][b+c] = [a(b+c)] = [ab+ac]$

feil

Regner ut høyresiden $[a][b] + [a][c] = [ab] + [ac]$

$= [ab+ac]$

Distributiv lov i den opprinnelige ringen.

Så $[a]([b]+[c]) = [a][b] + [a][c]$

Eksempel: R ringen av reelle polynomer.

$I = \{p(x) : p(x) \text{ er delelig med } x^2+1\}$

Hva $R/\sim$ = isomorf til de komplekse tall

Kvopper

Definisjon: En kvopp er en kommutativ ring der alle ikke-null elementer har en multiplikativ invers (dvs at hvis $a \neq 0$ så finnes det et element a^{-1} slik at $aa^{-1} = 1$)

Eksempler: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(p)$ p primtall.

Slavisk utdypning:

Definisjon: En kvopp $(K, +, \cdot)$ består av en ikke tom mengde K med binære operasjoner $+$ og $\cdot$ slik at

(i) $+$ og $\cdot$ er assosiative $(a+b)+c = a+(b+c)$, $(ab)c = a(bc)$

(ii) —"— kommutative $a+b = b+a$ $ab = ba$.

(iii) Vi har et nøytralt element 0 for addisjon og et nøytralt element 1 for multiplikasjon ($a+0=a$, $a \cdot 1 = a$)

(iv) Ethvert element $a \in K$ har en additiv invers $-a$ $(a+(-a)=0)$

(v) Ethvert element $a \neq 0$ har en multiplikativ invers a^{-1} $(aa^{-1}=1)$

(vi) $\cdot$ er distributiv over $+$: $a(b+c) = ab + ac$.

Definisjon: Anta at $(K, +, \cdot)$ og $(F, +, \cdot)$ er to kropper. En funksjon $\varphi: K \to F$ kalles en (kropp-) homomorfi dersom

(i) $\varphi(x+y) = \varphi(x) + \varphi(y)$

(ii) $\varphi(xy) = \varphi(x)\varphi(y)$

En bijektiv homomorfi kalles en isomorfi.