Algebraiska strukturer, 25 februari

RINGAR

En mängd R med två binära operationer

$$(a,b) \mapsto a+b \text{ (addition)}$$
$$(a,b) \mapsto ab \text{ (multiplikation)}$$

är en **ring** om

- $(R,+)$ är en abelsk grupp,
- $a(bc) = (ab)c$, då a, b, $c \in R$ (multiplikation är associativ),
- $a(b+c) = ab+ac$ och $(b+c)a = ba+ca$ då a, b, $c \in R$ (multiplikation är distributiv m a p addition).

Anmärkning. Det neutrala elementet i gruppen $(R,+)$ brukar betecknas med 0. Vanligen säger man att R är en ring utan att använda beteckningen $(R,+,\cdot)$.

Exempel 1. (a) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ är ringar.
(b) $(\mathbb{Z}_n,\oplus,\odot)$ är en ring. Det enda egenskap som vi inte har visat är distributiviteten

$$\begin{aligned}[a]\odot([b]\oplus[c]) &= [a]\odot[b+c] = [a(b+c)] = [ab+ac] = \\ &= [ab]\oplus[ac] = [a]\odot[b]\oplus[a]\odot[c]\end{aligned}$$

för $[a]$, $[b]$, $[c] \in \mathbb{Z}_n$.
(c) Mängden, $M_n(\mathbb{R})$, av alla $n \times n$-reella matriser med matrisaddition och matrismultiplikation är en ring.
(d) Mängden, $\mathbb{Z}[\sqrt{2}]$, av alla tal av typen $a+b\sqrt{2}$ där a, $b \in \mathbb{Z}$. För att se detta räcker det att visa att mängden är sluten under vanlig addition och multiplikation:

$$(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2}) = (a_1+a_2)+(b_1+b_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}],$$
$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = (a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1))\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Låt $(R,+,\cdot)$ vara en ring.

- R är **kommutativ** om $ab = ba$ då a, $b \in R$.
- R har en **etta** om det finns ett neutralt element $1 \in R$ m a p multiplikation, dvs $1a = a1 = a$ då $a \in R$.

Exempel 2. (a) Alla ringar i Exempel 1 är kommutativa med undantag av $M_n(\mathbb{R})$ då $n \geq 2$.
(b) Alla ringar i Exempel 1 har en etta. Ett exempel på en ring utan etta är ringen av de jämna heltalen med vanlig addition och multiplikation.

Eftersom en ring R är en grupp m a p addition, så gäller följande:
(1) $a+b = a+c \Rightarrow b = c$, då a, b, $c \in R$,
(2) $a+x = b \Leftrightarrow x = b+(-a)$, då a, b, $x \in R$,

(3) $-(-a) = a$, $-(a+b) = (-a) + (-b)$, då $a, b \in R$,
(4) $(m+n)a = ma+na$, $m(a+b) = ma+mb$, $m(na) = (mn)a$ då $m, n \in \mathbb{Z}$ och $a, b \in R$.

Varning. $ab = ac \not\Rightarrow b = c$ och $ba = ca \not\Rightarrow b = c$ i allmänhet:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ och } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

Låt R vara en ring, $a, b \in R$. Då
(1) $0 \cdot a = a \cdot 0 = 0$,
(2) $a(-b) = (-a)b = -(ab)$,
(3) $(-a)(-b) = ab$.

INTEGRITETSOMRÅDE OCH KROPPAR

- Låt R vara en kommutativ ring. Vi säger att R saknar **nolldelare** om $ab = 0$ ger $a = 0$ eller $b = 0$ då $a, b \in R$ (om $ab = 0$ där $a \neq 0$ och $b \neq 0$ så kallas a och b **nolldelare**).
- En kommutativ ring R kallas en **kropp** om $(R \setminus \{0\}, \cdot)$ är en abelsk grupp.
- Man säger att en ring R är ett **intgritetsområde** om R är kommutativ, saknar nolldelare och har en etta $1 \neq 0$.

Exempel 3. (a) Alla ringar i exempel 1 (a) saknar nolldelare. Men det finns nolldelare i t ex $\mathbb{Z}_6$: $[2] \odot [3] = [0]$. Ringen $M_2(\mathbb{R})$ har nolldelare ty t ex

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(b) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ är exempel på kroppar. $\mathbb{Z}$ är inte kropp, eftersom $(\mathbb{Z} \setminus \{0\}, \cdot)$ inte är en grupp.
(c) Varje kropp K är ett integritetsområde ty $ab = 0$ och $a \neq 0$ ger att $a^{-1}(ab) = b = 0$, där $a, b \in K$ så att K saknar nolldelare. Klart att K har en etta $1 \neq 0$.

Proposition. $\mathbb{Z}_n$ är ett integritetsområde omm n är ett primtal.

Bevis. $\mathbb{Z}_n$ är en kommutativ ring med ettan $[1] \neq [0]$ då $n > 1$.

Om n inte är ett primtal dvs $n = n_1 n_2$ med $1 < n_1, n_2 < n$ så har $\mathbb{Z}_n$ nolldelare ty $[n_1] \odot [n_2] = [0]$ trots att $[n_1] \neq [0] \neq [n_2]$.

Om n är ett primtal så saknar $\mathbb{Z}_n$ nolldelare, ty $[s_1] \odot [s_2] = [0]$ med $0 \leq s_1, s_2 < n$ medför att $n | s_1 s_2$ varav $n | s_1$ eller $n | s_2$ vilket är möjligt omm $s_1 = 0$ eller $s_2 = 0$.

Kroppar $\subset$ Integritetsområde $\subset$ Kommutativa ringar $\subset$ Ringar

---

Exempel 4. $R = \mathbb{Z}$ är en kommutativ ring. R är ett integritetsområde. R är inte en kropp.

$\mathbb{Z}_6$ är en kommutativ ring men inte ett integritetsområde.

$M_2(\mathbb{R})$ är en icke-kommutativ ring.

Sats 25.1 (22.1) Låt D vara ett integritetsområde och a, b, $c \in D$, $a \neq 0$. Då gäller strykningarna: $ab = ac \Rightarrow b = c$.

Bevis. $ab = ac \Rightarrow a(b-c) = 0$. Eftersom D saknar nolldelare och $a \neq 0$ får vi att $b - c = 0$ och $b = c$.

Sats 26.1 (23.1) Varje ändligt integritetsområde är en kropp.

Bevis. Låt D vara ett integritetsområde. $D \setminus \{0\}$ är sluten under multiplikation, ty $ab = 0$ och $a, b \in D$ ger $a = 0$ eller $b = 0$. Multiplikationen är associativ på $D \setminus \{0\}$ ty den är associativ på hela D. D har en etta $1 \neq 0$. Vi måste visa bara att varje element $a \neq 0$ i D har en invers m a p multiplikation, dvs det finns b i D sådant att $ab = 1$. Vi fixar $a \neq 0$ i D och definierar en avbildning $\lambda_a : D \to D$ enligt

$$\lambda_a(x) = ax.$$

λ_a är injektiv, ty $ax = ay$ ger $x = y$ enligt Sats 25.1. Vi får då att $|\{\lambda_a(x) : x \in D\}| = |D|$. Eftersom D är ändlig och $\{\lambda_a(x) : x \in D\} \subseteq D$ har vi att

$$\{\lambda_a(x) : x \in D\} = D,$$

vilket ger att det finns $b \in D$ sådant att $\lambda_a(b) = 1$ dvs $ab = 1$. Alltså är $D \setminus \{0\}$ en grupp m a p multiplikation.

Följdsats. $\mathbb{Z}_n$ är en kropp omm n är ett primtal.

Bevis. Enligt Proposition 1 är $\mathbb{Z}_n$ ett integritetsområde omm n är ett primtal. Påståendet följer nu ur Sast 26.1.

DELRINGAR OCH DELKROPPAR

Man säger att S är en **delring** till en ring R om $S \subseteq R$ och elementen i S bildar en ring med avseende på operationerna i R.

Exempel. $(\mathbb{Z}, +, \cdot) \subset (\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot) \subset (\mathbb{C}, +, \cdot)$.

Sats. En delmängd S till en ring R är en delring omm S är icke-tom, S är sluten under operationerna i R och $-a \in S$ för varje $a \in S$.

Man säger att en delmängd F till en kropp K är en **delkropp** till K om F är en kropp m a p operationerna i K.

ENHETER

Ett element $r \in R$ kallar man för en **enhet** om r har en multiplikativ invers dvs det finns $r' \in R$ så att $rr' = r'r = 1$. Mängden av alla enheter betecknas med R^*.

Exempel. $\mathbb{Z}$ har enbart två enheter ± 1. Varje element $a \neq 0$ i en kropp K är en enhet, ty $(K \setminus \{0\}, \cdot)$ är en grupp.

Sats. Gruppen av alla enheter i $\mathbb{Z}_n$ är $Z_n^* = \{[k] \in \mathbb{Z}_n : SGD(k, n) = 1\}$.

Bevis. Om $SGD(k, n) = 1$ så finns det heltal m och l sådana att $km + nl = 1$, varav $[k] \odot [m] = [1 - nl] = [1]$. Alltså är $[m]$ en invers till $[k]$.

Antag att $[k] \in \mathbb{Z}_n$ har invers $[m] \in \mathbb{Z}_n$ dvs $[k] \odot [m] = [1]$. Alltså är $km = 1 + nq$ för något heltal q. Den sista likheten visar att k och n saknar gemensamma delare $\neq 1$ dvs $SGD(k, n) = 1$.

Sats. Alla enheter i en kommutativ ring R med etta bildar en en (abelsk) grupp med avseende på multiplikation.

Bevis.=Övning