KTH Teknikvetenskap

# SF2703 ALGEBRA GRUNDKURS
# ANTECKNINGAR
# 2009-02-20

## 1. Introduktion till ringar

I många fall har vi både en addition och en multiplikation.

**Definition 1.1 (ring).** Vi säger att $R$ är en *ring* om det finns två operationer, $+$ och $\cdot$, som uppfyller

- $R$ är en abelsk grupp under $+$. (addition)
- Multiplikationen, $\cdot$, är *associativ*, dvs $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, för alla $a, b, c$ i $R$.
- Multiplikation och addition är *distributiv*, dvs

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{och} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

  för alla $a, b, c$ i $R$.

Det neutrala element under addition kallas *nolla* och skrivs $0$. Om det finns ett neutralt element under multiplikation kallar vi det för *etta* och betecknar det $1$.

Vi säger att $R$ är en kommutativ ring om multiplikationen är kommutativ, dvs om $a \cdot b = b \cdot a$, för alla $a, b$ i $R$.

Om det finns en etta och alla nollskilda element är inverterbara under multiplikation har vi en *skevkropp* och om dessutom multiplikationen är kommutativ är det en *kropp*.

**Exempel 1.1.** Vi har sedan tidigare sett att heltalen, de rationella talen, de reella talen och de komplexa talen bildar ringar. Heltalen, $\mathbb{Z}$, är en kommutativ ring med etta, medan de rationella talen, $\mathbb{Q}$, de reella talen, $\mathbb{R}$ och de komplexa talen, $\mathbb{C}$, alla är kroppar. Kvaternionerna bildar en skevkropp.

De hela talen modulo ett heltal $n$, dvs $\mathbb{Z}_n$, bildar en kommutativ ring med etta, som inte är en kropp om inte $n$ är ett primtal.

I analysen stöter vi på en mängd ringar som består av funktioner av olika slag. exempelvis bildar mängden av alla funktioner från $\mathbb{R}$ till $\mathbb{R}$ en ring under punktvis addition och multiplikation. På samma sätt får vi mindre ringar genom att restricera oss till kontinuerliga, deriverbara eller differentierbara funktioner. I komplex analys stöter vi på ringen av holomorfa funktioner.

**Definition 1.2 (nolldelare, integritetsområde).** Ett element $a \neq 0$ där det finns ett $b \neq 0$ så att $a \cdot b = 0$ eller $b \cdot a = 0$ kallas en *nolldelare*. Om ringen är kommutativ med etta och saknar nolldelare är det ett *integritetsområde*.

**Exempel 1.2.** Om ringen inte är kommutativ behöver inte $a \cdot b = 0$ innebära att $b \cdot a = 0$. Exempelvis har vi i $\mathrm{Gl}_2(\mathbb{R})$ att

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0 \quad \text{men} \quad \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ -2 & -2 \end{pmatrix} \neq 0.$$

**Exempel 1.3.** Heltalen, $\mathbb{Z}$, är ett integritetsområde, medan $\mathbb{Z}_n$ inte är ett integritetsområde om $n$ är sammansatt.

**Sats 1.1.** *Ett ändligt integritetsområde är en kropp.*

*Bevis.* Varje nollskilt element $a$ ger en injektiv funktion $R \longrightarrow R$ genom multiplikation med $a$. Eftersom $R$ är ändlig är den också surjektiv finns ett element $b$ så att $ab = 1$. Alltså är alla nollskilda element inverterbara. □

**Definition 1.3 (delring).** En delring i $R$ är en additiv delgrupp $Q \subseteq R$ som är sluten under multiplikation.

**Exempel 1.4.** Heltalen är en delring av de rationella talen och de reella talen är en delring i de komplexa talen.

## 2. Polynomringar, matrisringar och gruppringar

Om $R$ är en ring kan vi bilda en polynomring i en variabel $x$ över $R$ genom att se på polynom med koefficienter i $R$. Det är ganska lätt att förstå vad som menas genom att se på formella uttryck

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \tag{1}$$

där koefficienterna är element i ringen $R$. Multiplikationen ges då av att

$$\begin{aligned}(a_0 \quad &+a_1x + a_2x^2 + \cdots + a_mx^m) \cdot (b_0 + b_1x + b_2x^2 + \cdots + b_nx^n) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (\textstyle\sum_{i+j=m+n} a_ib_j)x^{m+n}\end{aligned}$$

För att slippa fundera över vad formella uttryck är för något kan vi i stället se det som oändliga sekvenser $(a_0, a_1, \dots)$, sådana att $a_i = 0$ för alla utom ändligt många heltal $i$. Produkten definieras då genom att

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$$

där

$$c_k = \sum_{\substack{i,j \in \mathbb{N} \\ i+j=k}} a_ib_j.$$

Detta fungerar i och med att $c_i$ blir noll för alla $i > m + n$ om $a_i = 0$ för alla $i > m$ och $b_i = 0$ för alla $i > n$.

Man kan kontrollera att denna multiplikation är associativ och att de distributiva lagarna håller. Vi kan nu använda symbolerna $a, ax, ax^2, \dots$ för sekvenserna

$$a = (a, 0, \dots), \quad ax = (0, a, 0, \dots), \quad ax^2 = (0, 0, a, 0, \dots)$$

och så vidare. På så sätt kan vi skapa mening hos uttryck som (1).

**Definition 2.1 (Polynomring i en variabel).** Om $R$ är en ring skriver vi $R[x]$ för ringen av polynom i en variabel $x$ med koefficenter i $R$.

Vi kan definiera *graden* hos ett polynom som den högsta potens av $x$ som ingår i polynomet. För att graden ska bete sig som vi är vana vid, dvs att

$$\mathrm{grad} f(x)g(x) = \mathrm{grad} f(x) + \mathrm{grad} g(x)$$

behövs att koefficientringen saknar nolldelare.

För en ring $R$ kan vi också betrakta kvadratiska matriser med koefficienter i $R$. Matrismultiplikationen är associativ och de distributiva lagarna gäller, så vi får en ring av matriser av storlek $n \times n$ med koefficienter i $R$.

**Definition 2.2.** Om $R$ är en ring och $n$ är ett positivt heltal skriver vi $M_n(R)$ för ringen av $n \times n$-matriser med koefficienter i $R$.

**Exempel 2.1.** Det vanligaste är att vi har matriser med koefficienter i en kropp, $k$, och vi har då möjlighet att använda de flesta resultat från linjär algebra. Exempelvis $M_n(\mathbb{C})$, $M_n(\mathbb{R})$.

För en grupp $G$ och en kommutativ ring $R$ med etta kan vi bilda en *gruppring*, $RG$, eller $R[G]$, genom att låta

$$RG = \{f : G \longrightarrow R | f(g) = 0, \text{utom för ändligt många } g\}$$

Additionen sker punktvis, men multiplikationen sker genom

$$f_1 \cdot f_2(g) = \sum_{\substack{g', g'' \in G \\ g'g'' = g}} f_1(g') f_2(g'').$$

**Exempel 2.2.** Om $R$ är en kropp ges gruppringen för en cyklisk grupp av ordning $n$ av sekvenser $(a_1, a_2, \ldots, a_m)$ med komponenentvis addition och multiplikation

$$(a_0, a_1, \ldots, a_{n-1}) \cdot (b_0, b_1, \ldots, b_{n-1}) = (c_0, c_1, \ldots, c_{n-1})$$

där $c_k = \sum_{i=0}^{n} a_i b_{k-i}$, där indexen räknas modulo $n$.

## 3. Homomorfier och kvotringar

Precis som för grupper är det speciellt intressant att se på funktioner mellan ringar som bevarar ringstrukturen. I det här fallet finns det två operationer och vi säger att $\Phi : R \longrightarrow S$ är en *ringhomomorfi*, eller *homomorfi* av ringar, om

$$\Phi(a + b) = \Phi(a) + \Phi(b) \qquad \text{och} \qquad \Phi(a \cdot b) = \Phi(a) \cdot \Phi(b),$$

för alla $a$ och $b$ i $R$. Det betyder att $\Phi$ är en homomorfi av abelska grupper som dessutom bevarar multiplikationen. En bijektiv ringhomomorfi kallas för *ringisomorfi*, eller *isomorfi av ringar*.

Vi låter *kärnan* av en ringhomomorfi vara kärnan som abelska grupper, dvs

$$\ker \Phi = \{a \in R | \Phi(a) = 0\} = \Phi^{-1}(0).$$

**Definition 3.1.** Ett *ideal* i en ring $R$ är en delring, $I$, som uppfyller

$$aI \subseteq I \qquad \text{och} \qquad Ia \subseteq I$$

för alla element $a$ i $R$.

Om bara $aI \subseteq I$ säger vi att $I$ är ett *vänsterideal* och om bara $Ia \subseteq I$ är $I$ ett *högerideal*. Ibland säger vi *tvåsidigt ideal* istället för *ideal* för att understryka att det inte bara är ett vänsterideal eller ett högerideal.

**Sats 3.1.** *Kärnan till en ringhomomorfi $\Phi : R \longrightarrow S$ är ett ideal i $R$.*

*Bevis.* Det är klart att det är en delgrupp om vi ser på $R$ under addition. Alltså räcker det att visa att $a \ker \Phi \subseteq \ker \Phi$ och $(\ker \Phi)a \subseteq I$. Tag $b \in \ker \Phi$ och $a \in R$. Då har vi att

$$\Phi(ab) = \Phi(a)\Phi(b) = \Phi(a) \cdot 0 = 0 = 0 \cdot \Phi(a) = \Phi(b) \cdot \Phi(a) = \Phi(ba)$$

vilket visar att både $ab$ och $ba$ ligger i $\ker \Phi$. □

Eftersom alla delgrupper av en abelsk grupp är normala kan vi definiera $R/I$ som en abelsk grupp om $I$ är en abelsk delgrupp. Om $I$ dessutom är ett ideal kan vi definiera en multiplikation på $R/I$ som gör den till en ring. Vi multiplicerar sidoklasser till $I$ genom

$$(a + I) \cdot (b + I) = ab + I.$$

Detta är väldefinierat eftersom ifall $a' = a + i$ och $b' = b + j$, där $i, j \in I$, så får vi att

$$a'b' = (a + i)(b + j) = ab + ib + aj + ij = ab + i'$$

där $i' = ib + aj + ij \in I$.

Vi kan sedan konstatera att multiplikationen måste vara associativ eftersom multiplikationen i $R$ är associativ. Likaså följer de distributiva lagarna direkt från de distributiva lagarna i $R$.

**Sats 3.2 (Första isomorfisatsen för ringar).** *Om $\Phi : R \longrightarrow S$ är en ringhomomorfi gäller att*

$$R/\ker \Phi \cong \mathrm{im}\Phi.$$

*Bevis.* Vi vet redan att satsen är sann om vi ser $R$ och $S$ som abelska grupper. Det återstår att se att isomorfin bevarar multiplikationen och därmed är en ringisomorfi. Om $a+\ker \Phi$ och $b+\ker \Phi$ är två sidoklasser i $R/\ker \Phi$ så avbildas de genom $\Psi : R/\ker \Phi \longrightarrow S$ på $\Phi(a)$ och $\Phi(b)$, medan produkten avbildas på $\Phi(ab) = \Phi(a)\Phi(b)$. Därmed har vi att

$$\Psi((a + \ker \Phi) \cdot (b + \ker \Phi)) = \Psi(a + \ker \Phi) \cdot \Psi(b + \ker \Phi)$$

och $\Psi$ är en ringhomomorfi. □

**Exempel 3.1.** Om $R = \mathbb{Z}$ och $n > 0$ är ett heltal får vi $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$ som en kvot av $\mathbb{Z}$ med idealet $n\mathbb{Z}$.

För ett polynom, $f(x)$, med reella koefficienter kan vi bilda idealet $(f(x))$ som genereras av $f(x)$, dvs

$$(f(x)) = \{f(x)g(x) | g(x) \in \mathbb{R}[x]\}.$$

Kvoten $\mathbb{R}[x]/f(x)$ bildar en ring som är ett ändligdimensionellt vektorrum över $\mathbb{R}$ med dimension lika med graden av $f(x)$.

Om $f(x) = x^2 + 1$ får vi ett två-dimensionellt vektorrum och om vi betecknar sidoklassen $\bar{x} = x + (x^2 + 1)$ med $i$ ser vi att denna ring är isomorf mer de komplexa talen, $\mathbb{C}$.

---

## REKOMMENDERADE UPPGIFTER

**7.1 Grundläggande definitioner och exempel.** 1, 2, 3, 4, 7, 11, 12, 13, 14, 15

**7.2 Exempel: polynomringar, matrisringar och gruppringar.** 1, 2, 3, 4, 6, 9, 10

**7.3 Ringhomomorfier och kvotringar.** 1, 2, 3, 4, 5, 6, 13, 14, 27, 29