Algebraiska strukturer, 27 februari

PRODUKT AV RINGAR

Låt R_1, R_2,..., R_k vara ringar. Mängden

$$R_1 \times R_2 \times \ldots \times R_k$$

är en ring med avseende på koordinatvis addition och multiplikation dvs

$$(r_1, r_2, \ldots, r_k) + (r_1', r_2', \ldots, r_k') = (r_1 + r_1', r_2 + r_2', \ldots, r_k + r_k'),$$
$$(r_1, r_2, \ldots, r_k)(r_1', r_2', \ldots, r_k') = (r_1 r_1', r_2 r_2', \ldots, r_k r_k').$$

ISOMORFI AV RINGAR

Precis som för grupper är det intressant att veta vad man skall mena med att två ringar egentligen är samma ring.

Två ringar R och S är **isomorfa** om det finns en bijektion $\Phi : R \to S$ som uppfyller

- $\Phi(a + b) = \Phi(a) + \Phi(b)$, för alla a, $b \in R$.
- $\Phi(ab) = \Phi(a)\Phi(b)$, för alla a, $b \in R$.

På vänstra ledet är $+$ och $\cdot$ operationerna i R och på det högra ledet är $+$ och $\cdot$ operationerna i S.

Avbildningen Φ kallas då en **isomorfi av ringar** (eller **ringisomorfi**) och vi skriver $R \approx S$.

Eftersom en ringisomorfi $\Phi : R \to S$ är en isomorfi av abelska grupperna $(R, +)$ och $(S, +)$ så gäller följande:

- $\Phi(0) = 0$, $\Phi(-a) = -\Phi(a)$, $\Phi(ma) = m\Phi(a)$ då $a \in R$ och $m \in \mathbb{Z}$.

Exempel. $\mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$.
Bevis. Betrakta $\Phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$, där $\Phi([a]_6) = ([a]_3, [a]_2)$.

- Definitionen av denna avbildning beror inte på heltalet a som definierar kongruensklassen (väldefinierad): Om $[a]_6 = [b]_6$ så är $[a]_3 = [b]_3$ och $[a]_2 = [b]_2$, ty $6|(a - b)$ implicerar att $3|(a - b)$ och $2|(a - b)$.
- Φ är injektiv, ty

$$\Phi([a]_6) = \Phi([b]_6) \Leftrightarrow ([a]_3, [a]_2) = ([b]_3, [b]_2) \Leftrightarrow$$
$$[a]_3 = [b]_3, [a]_2 = [b]_2 \Leftrightarrow 3|(a - b), 2|(a - b) \Rightarrow$$
$$6|(a - b) \Leftrightarrow [a]_6 = [b]_6$$

- Φ är surjektiv, ty Φ är injektiv och $|\mathbb{Z}_6| = |\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$.
- Φ bevarar operationer:

$$\Phi([a]_6 + [b]_6) = \Phi([a + b]_6) = ([a + b]_3, [a + b]_2) =$$
$$= ([a]_3, [a]_2) + ([b]_2, [b]_3) = \Phi([a]_6) + \Phi([b]_6),$$
$$\Phi([a]_6[b]_6) = \Phi([ab]_6) = ([ab]_3, [ab]_2) =$$
$$= ([a]_3, [a]_2)([b]_2, [b]_3) = \Phi([a]_6)\Phi([b]_6)$$

Detta visar att Φ är en isomorfi.

KARAKTERISTIK

Låt R vara en kommutativ ring med ettan e. Vi säger att R har **karakteristik** n om n är den additiva ordningen av ettan i R, dvs om n är det minsta positiva heltal så att

$$ne = \underbrace{e + e + \ldots + e}_{n} = 0.$$

Om sådant n inte existerar säger vi att R har karakteristik 0. Karakteristiken av R kommer att betecknas med $\mathrm{char}(R)$.

Övning. Låt $\mathrm{char}(R) = n$. Visa att $na = 0$ för varje $a \in R$.

Exempel. (a) Ringarna $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ har karakteristik 0, ty $n1 \neq 0$ då n är ett positivt heltal.

(b) $\mathbb{Z}_n$ har karakteristik n, ty den additiva ordningen av [1] är n.

Sats 27.1 (24.1) Karakteristiken av ett integritetsområde är ett primtal eller 0.

Bevis. Låt D vara integritetsområde och låt e beteckna ettan i D. Antag att karakteristiken n är sammansatt, $n = pq \neq 0$. Då gäller

$$0 = ne = \underbrace{e + e + \ldots + e}_{n} = \underbrace{(e + e + \ldots + e)}_{p}\underbrace{(e + e + \ldots + e)}_{q} = (pe)(qe)$$

men eftersom D saknar nolldelare måste en av faktorerna vara noll, vilket motsäger minimaliteten hos n.

Sats 27.2,3 (24.2,3) Om ett integritetsområde har karakteristik $p \neq 0$ (respektive $p = 0$) innehåller D en delring K isomorf med $\mathbb{Z}_p$ (respektive $\mathbb{Z}$).

Bevis. 1. Låt $\mathrm{char}(D) = p \neq 0$. Låt $K = \{ke, k \in \mathbb{Z}\}$. Eftersom den additiva ordningen av e är p har vi att $|K| = p$. K är en delring till D (Varför?). Vi kan definiera en avbildning $\Phi : \mathbb{Z}_p \to K$ genom $\Phi([k]) = ke$, för alla heltal $k \in \mathbb{Z}$. Denna är väldefinierad, eftersom $[n] = [m]$ ger att $p|(n-m)$ dvs $n - m = qp$ för något $q \in \mathbb{Z}$, vilket visar nu att $ne - me = (n-m)e = qpe = 0$, dvs $me = ne$. Φ uppfyller $\Phi([m] + [n]) = \Phi([m]) + \Phi([n])$ och $\Phi([m][n]) = \Phi([m])\Phi([n])$, då $m, n \in \mathbb{Z}$. Φ är injektiv ty $\Phi([m]) = \Phi([n]) \Leftrightarrow \Phi([m-n]) = 0 \Leftrightarrow (m-n)e = 0 \Leftrightarrow p|m-n \Leftrightarrow [m] = [n]$. $|\Phi(\mathbb{Z}_p)| = p = |K|$. Alltså är K isomorf med $\mathbb{Z}_p$.

2. Låt $\mathrm{char}(D) = 0$. Övning.

POLYNOM

Ett **polynom** med koefficienter i en ring R kan vi se som ett formelt uttryck

$$a_0 + a_1 x + \ldots + a_n x^n,$$

där $a_0, a_1, \ldots, a_n \in R$.

Vi kan addera och multiplicera två polynom:

$$(a_0 + a_1x + \ldots) + (b_0 + b_1x + \ldots) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$$
$$(a_0 + a_1x + \ldots + a_nx^n)(b_0 + b_1x + \ldots + b_mx^m) = c_0 + c_1x + \ldots + c_{n+m}x^{n+m},$$
$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

för $k = 0, 1, \ldots, m + n$. Mängden av polynom med koefficienter i R bildar en ring, $R[x]$-**polynomringen över** R. Om R är kommutativ blir $R[x]$ kommutativ.

Den **ledande termen** i $p(x) = a_0+a_1x+\ldots+a_nx^n$ är a_nx^n om $a_n \neq 0$. Då kallas a_n den **ledande koefficienten** och polynomets **grad** är n (grad $p(x)$). Vi antar att graden av nollpolynomet är -1.

Från och med nu förutsätter vi att K är en kropp.

Divisionsalgoritmen. Om $f(x)$ och $g(x)$ är polynom i $K[x]$, där K är en kropp, och $g(x) \neq 0$, finns det två entydigt bestämda polynom $q(x)$ och $r(x)$ i $K[x]$ så att

$$f(x) = q(x)g(x) + r(x)$$

och grad$r(x) <$ grad$g(x)$.

Bevis. Gör induktion över graden av $f(x)$ och eliminera den ledande termen i $f(x)$ med hjälp av $x^d g(x)$, där $d =$ grad$f(x) -$ grad$g(x)$.

Ett polynom med ledande koefficient 1 kallas **moniskt**.

Vi säger att $f(x)$ **delar** $g(x)$ i $K[x]$, eller $f(x)|g(x)$, om det finns ett polynom $h(x) \in K[x]$ så att $g(x) = f(x)h(x)$, dvs om resten vid division av $g(x)$ med $f(x)$ är noll.

Man säger att $a \in K$ är ett **nollställe** till $f(x) \in K[x]$ om $f(a) = 0$.

Faktorsatsen. Om $f(x) \in K[x]$ och K är en kropp, gäller att

$$(x - a)|f(x) \Leftrightarrow f(a) = 0$$

för alla $a \in K$.

Bevis. ($\Rightarrow$): Antag att $(x-a)|f(x)$. Då är $f(x) = (x-a)g(x)$ för något $g(x) \in K[x]$, och därmed $f(a) = (a - a)g(a) = 0$.

($\Leftarrow$): Antag att $f(a) = 0$. Använd divisionsalgoritmen för att skriva $f(x) = q(x)(x - a) + r(x)$, där grad$r(x) = 0$ eller $r(x) = 0$. Eftersom $f(a) = 0$ får vi $0 = q(a)(a - a) + r(a)$, och därmed $r(x) = 0$, eftersom $r(x)$ är ett konstant polynom.

Sats. Om $f(x)$ och $g(x)$ är polynom i $K[x]$, Kär en kropp, finns det ett unikt moniskt polynom $d(x)$ i $K[x]$ så att

(a) $d(x)|f(x)$ och $d(x)|g(x)$ och

(b) om $c(x)$ i $K[x]$ s.a. $c(x)|f(x)$ och $c(x)|g(x)$ så $c(x)|d(x)$.

Detta element kallas **största gemensamma delaren** till $f(x)$ och $g(x)$ ($SGD(f(x), g(x))$). Dessutom, finns det polynom $a(x)$ och $b(x)$ i $K[x]$ sådana att

$$SGD(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

Satsen visas genom att utföra Euklides algoritm (precis som för heltal)

$SGD(f, g)$ är maximalt element (av högsta grad) bland de moniska gemensamma delarna till $f(x)$ och $g(x)$.