Polynomringar

Ett polynom är ett uttryck

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

Vi ska titta på polynom med koefficienter i en kommutativ ring R. Mängden av polynom med koefficienter i R betecknas $R[X]$.

Om vi har två polynom

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

$$q(x) = b_0 + b_1 x + \ldots + b_m x^m$$

så kan vi bilda

$$(p+q)(x) = (a_0+b_0) + (a_1+b_1)x + \ldots + (a_m+b_m)x^m +$$

$$+ a_{m+1}x^{m+1} \ldots + a_n x^n \quad (n \geq m)$$

Vi kan addera element i R så $(p+q)(x) \in R[x]$.

$$p\cdot q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \dots$$
$$\dots + a_n b_m x^{n+m}$$

som vanligt. Produkten av två element i R ligger i R så $p\cdot q(x) \in R[x]$. Med dessa operationer blir $R[x]$ en ring.

Övn: verifiera det!!

Ex: $\mathbb{Z}_3[x]$ $\quad (\overset{a_2}{1}\cdot x^2 + \overset{a_1}{2}x + \overset{a_0}{1})(\overset{b_1}{1}\cdot x + \overset{b_0}{2}) =$

$$= x^3 + 2x^2 + x + 2x^2 + 2\cdot 2x + 2 =$$
$$= x^3 + x^2 + 2x + 2$$

(Ex: Eftersom $\mathbb{Z}_3[x]$ är en ring, kan vi bilda $(\mathbb{Z}_3[x])[y]$

$$1 + xy + x^2y = 1 + (x+x^2)y$$)

Polynomdivision

Om n inte är ett primtal kan det hända att graden inte adderas vid multiplikation.

$R[x]$

Ex: $\mathbb{Z}_{15}[x]$ $\quad (3x^4+2x+1)(5x^2+3x) =$

$$= \cancel{15x^6} + 9x^5 + 10x^3 + 6x^2 + 5x^2 + 3x =$$

$$= 9x^5 + 10x^3 + 11x^2 + 3x$$

Vi får så

$$9x^5+10x^3+11x^2+3x=(3x^4+2x+1)(3x^2+3x)$$

men också $=(3x^4+2x+1)3x+(10x^3+5x^2)$

I det första fallet har vi att $9x^5+10x^3+11x^2+3x$ ger rest 0 vid division med $(3x^4+2x+1)$ men i det andra fallet får vi en rest $10x^3+5x^2$.

Om vi däremot antar att vi har koefficienter i en kropp så går det bra för vi har sett att i en kropp gäller att $x, y \neq 0 \Rightarrow xy \neq 0$.

Det ger $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

graden hos polynomet

för $f(x), g(x) \in F[x]$

Sats: Om $a(x), b(x) \in F[x]$ så finns ett unikt par $q(x), r(x)$ så att $$a(x) = b(x)q(x) + r(x)$$ $$\deg r(x) < \deg b(x).$$

bevis: Vi antar $\deg a(x) \geq \deg b(x) \Rightarrow$ $a_n b_m^{-1} x^{n-m} b(x) - a(x)$ har lägre grad än $a(x)$. Vi kan sedan göra induktion över graden. q, r unika för antas $a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x)$.
$\Rightarrow b(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$

men $\deg(r_2(x) - r_1(x)) < \deg b(x)$ och

$\deg b(x)(q_1(x) - q_2(x)) \geq \deg b(x)$ om

$q_1(x) - q_2(x) \neq 0 \Rightarrow q_1(x) = q_2(x)$

och därmed även $r_2(x) = r_1(x)$.

Ex: i $\mathbb{Z}_5[x]$, dela $x^3 + x + 1$ med

$x^2 + 2x + 2$. Vi multiplicerar

$x^2 + 2x + 2$ med x och tar sedan

$$(x^3 + x + 1) - (x^2 + 2x + 2)x =$$

$$= \cancel{x^3} + x + 1 - \cancel{x^3} - 2x^2 - 2x = 3x^2 + 4x + 1$$

$$3x^2 + 4x + 1 - (x^2 + 2x + 2) \cdot 3 = 3x$$

$$\underset{a_3}{x^3} + x + 1 = (\underset{b_2}{x^2} + 2x + 2)(x+3) + 3x$$

$$
\begin{array}{rl}
 & x + 3 \\
x^2+2x+2 \,\big) & x^3 + 0x^2 + x + 1 \\
- & (x^3 + 2x^2 + 2x) \\
\hline
 & 3x^2 + 4x + 1 \\
- & (3x^2 + x + 1) \\
\hline
 & 3x
\end{array}
$$

Så Svar: ?

$$x^{n-m} a_n b_m^{-1} b_m x^m = a_n x^n$$

Vi kan nu definiera delare (resten = 0) och SGD av polynom i $F[x]$. Euklides algoritm fungerar på samma sätt som i $\mathbb{Z}$.

Ex: Bestäm $SGD(2x^3+2x+1, x^2+3x+4)$ i $\mathbb{Z}_5[x]$.

$$
\begin{array}{r|l}
 & \quad 2x+4 \\
\hline
x^2+3x+4 & 2x^3+0x^2+2x+1 \\
- & (2x^3+x^2+3x) \\
\hline
 & \qquad 4x^2+4x+1 \\
- & \qquad (4x^2+2x+1) \\
\hline
 & \qquad\qquad 2x
\end{array}
$$

$$2x^3+2x+1 = (x^2+3x+4)(2x+4)+2x$$

$$x^2+3x+4 = 2x(3x+4)+4$$

$$\mathrm{SGD}(2x^3+2x+1,\ x^2+3x+4) = 4$$

$$
\begin{array}{r|l}
 & \phantom{x^2+{}}3x+4 \\
\hline
2x & x^2+3x+4 \\
- & x^2 \\
\hline
 & \phantom{x^2+{}}3x+4 \\
- & \phantom{x^2+{}}3x \\
\hline
 & \phantom{x^2+3x+{}}4
\end{array}
$$

Genom att gå baklänges kan vi skriva 4 som

$$4 = (x^2+3x+4) - 2x(3x+4)$$

$$= (x^2+3x+4) - \big((2x^3+2x+1) - (x^2+3x+4)(2x+4)\big)(3x+4)$$

$$= (x^2+3x+4)\big(1+(2x+4)(3x+4)\big) - (2x^3+2x+1)(3x+4)$$

$$= (x^2+3x+4)(x^2+2) - (2x^3+2x+1)(3x+4)$$

Vi kan också skriva

$$1 = 4^{-1}(x^2+3x+4)(x^2+2) - 4^{-1}(2x^3+2x+1)(3x+4)$$

$$= (x^2+3x+4)(4x^2+3) + (2x^3+2x+1)(3x+4)$$

Faktorisering av polynom

Varje heltal $\neq -1, 0, 1$ har en unik (upp till ordning och tecken) faktorisering i primfaktorer (med tecken). Motsvarande gäller polynom. Motsvarigheten till primtalen är irreducibla polynom, vilka är polynom som inte går att skriva som en produkt av polynom av lägre grad.

Tex: i $\mathbb{R}[x]$ är x^2+1 irreducibelt.

För polynom i $F[x]$ gäller att de kan faktoriseras på ett unikt (upp till ordning och multiplikation med konstanter) sätt. Beviset följer som för heltalen via induktion.

Ex: Faktorisera polynomet x^4+3x+3 i $\mathbb{Z}_7[x]$. Vi har att $1+3+3=0$ så $x-1=x+6$ är en faktor.

$$
\begin{array}{r|l}
 & x^3 + x^2 + x + 4 \\
\hline
x+6 & x^4 + 0x^3 + 0x^2 + 3x + 3 \\
- & (x^4 + 6x^3) \\
\hline
 & x^3 + 0x^2 \\
- & (x^3 + 6x^2) \\
\hline
 & x^2 + 3x \\
- & (x^2 + 6x) \\
\hline
 & 4x + 3 \\
- & 4x + 3 \\
\hline
 & 0
\end{array}
$$

Vi har att $1+1+1+4=0$ så $(x+6)$ är en faktor även i x^3+x^2+x+4.

$$
\begin{array}{r|l}
 & x^2 + 2x + 3 \\
\hline
x+6 & x^3 + x^2 + x + 4 \\
- & (x^3 + 6x^2) \\
\hline
 & 2x^2 + x \\
- & (2x^2 + 5x) \\
\hline
 & 3x + 4 \\
- & 3x + 4 \\
\hline
 & 0
\end{array}
$$

Svar: $x^4 + 3x + 3 = (x+6)^2\,(x^2 + 2x + 3)$

x	x^2+2x+3
0	3
1	6
2	4
3	4
4	6
5	3
6	2

$\Leftarrow$ x^2+2x+3 är irreducibelt