Polynomy

Polynom je možno definovat dvěma způsoby:

- jako reálnou nebo komplexní funkci, jejichž hodnoty jsou dány jistým vzorcem,
- jako ten vzorec samotný.

a) polynomy, 1, b) P. Olšák, FEL ČVUT, c) P. Olšák 2010, d) BI-LIN, e) L, f) 2009/2010, g) . Viz p. d. 4/2010

První způsob zavedení polynomu

Definice 1: *Polynom* je komplexní funkce $p : \mathbf{C} \to \mathbf{C}$, pro kterou existují komplexní čísla $a_0, a_1, \ldots, a_n$ taková, že

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

pro všechna $x \in \mathbf{C}$.

Čísla $a_0, a_1, \ldots, a_n$ nazýváme *koeficienty polynomu*.

Dále zavádíme pojmy:

Rovnost polynomů jako rovnost funkcí:
$p = q$, když $p(x) = q(x)$ pro všechna $x \in \mathbf{C}$.

Součet polynomů, násobek polynomu jako součet a násobek funkcí:
$p+q$ je funkce, pro kterou $(p+q)(x) = p(x)+q(x)$ pro všechna $x \in \mathbf{C}$,

αp je funkce, pro kterou $(\alpha p)(x) = \alpha \cdot p(x)$ pro všechna $x \in \mathbf{C}$.

Druhý způsob zavedení polynomu

Definice 2: *Polynom* je vzorec tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

kde $a_0, a_1, \ldots, a_n$ jsou komplexní čísla a x je formální proměnná.

Čísla $a_0, a_1, \ldots, a_n$ nazýváme *koeficienty polynomu*.

Hodnota polynomu $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ v bodě $\alpha \in \mathbf{C}$ je komplexní číslo, které dostaneme dosazením čísla α za proměnou x do uvedeného vzorce.

Dále zavádíme pojmy:

Rovnost polynomů: Dva polynomy se rovnají, pokud současně platí

- koeficienty se stejnými indexy se rovnají,
- má-li jeden polynom koeficient, který druhý polynom nemá, pak tento koeficient je nulový.

Součet polynomů, násobek polynomu: jako součet příslušných vzorců a násobek vzorce konstantou. Přesněji:

Má-li polynom p koeficienty $a_0, a_1, \ldots, a_m$ a má-li polynom q koeficienty $b_0, b_1, \ldots, b_n$ a je $m \le n$, pak polynom $p+q$ má koeficienty

$$a_0 + b_0, a_1 + b_1, \ldots, a_m + b_m, b_{m+1}, \ldots b_n.$$

Dále polynom αp má koeficienty $\alpha a_0, \alpha a_1, \ldots, \alpha a_m$.

Výsledky operací jsou tedy popsány pomocí svých koeficientů *algoritmicky*. Na vstupu do algoritmu jsou koeficienty polynomů, které sčítáme resp. násobíme. S proměnnou x algoritmy nepracují.

Součin polynomů

Součin dvou polynomů p a q, které mají koeficienty $a_0, a_1, \dots, a_m$ a $b_0, b_1, \dots, b_n$, je polynom, který má koeficienty $c_0, c_1, \dots, c_{m+n}$ takové, že

$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0,$$

přičemž v tomto vzorci klademe $a_i = 0$ pro $i > m$ a $b_i = 0$ pro $i > n$.

Jak jsme na to přišli?

$$\begin{aligned}
&(a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m) \cdot (b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n) = \\
&= (a_0 b_0) + (a_0 b_1 + a_1 b_0)\, x + \\
&\quad + (a_0 b_2 + a_1 b_1 + a_2 b_0)\, x^2 + \cdots + \\
&\quad + (a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_m b_n + \cdots + a_{m+n} b_0)\, x^{m+n}.
\end{aligned}$$

Vztah mezi funkcí a koeficienty

Jaký je vztah mezi prvním a druhým způsobem pojetí polynomu?

Tj. mezi polynomem jako *funkcí* a polynomem jako *vzorcem* charakterizovaným svými *koeficienty*?

Tvrzení:

- Polynom daný koeficienty jednoznačně určuje funkci podle definice 1.
- Polynom jako funkce má své koeficienty určeny jednoznačně (až na „přebývající“ nulové koeficienty).

První část tvrzení je zřejmá. Vzorec určuje funkci.

Druhá část tvrzení není zcela zřejmá. K jejímu důkazu použijeme pomocnou větu:

Věta: nulová funkce je polynom, který musí mít všechny koeficienty nulové.

Důkaz: Nechť $p(x) = a_n x^n + \cdots + a_1 x + a_0 = 0$ pro všechna $x \in \mathbf{C}$, Koeficient a_0 musí být nulový (stačí dostadit $x = 0$). Takže platí $p(x) = x\,(a_n x^{n-1} + \cdots + a_1) = x\,q(x) = 0$. Polynom q je nulový pro všechna $x \in \mathbf{C} \setminus \{0\}$. Protože q je funkce spojitá, je také $q(0) = 0$. Dosazením $x = 0$ dostáváme $a_1 = 0$ a postup můžeme opakovat. Dostaneme $a_2 = 0, \dots, a_n = 0$.

Vraťme se k tvrzení: Polynom jako funkce má své koeficienty určeny jednoznačně.

Důkaz: Ať polynom p (jako funkce) má koeficienty $a_0, a_1, \dots, a_n$ a také ať má koeficienty $b_0, b_1, \dots, b_n$ (koeficienty doplníme nulami, kdyby původně měl být počet koeficientů různý). Funkce $p - p$ je nulová a má zřejmě koeficienty $a_0 - b_0, a_1 - b_1, \dots, a_n - b_n$. Podle předchozí věty musejí být tyto koeficienty nulové, takže musí být $a_i = b_i$ pro všechna i. Nemůže se tedy stát, aby měl jeden polynom (jako funkce) dvě sady různých koeficientů.

Stupeň polynomu

Definice: polynom se všemi koeficienty nulovými se nazývá *nulový polynom*.

Stupeň polynomu p s koeficienty $a_0, a_1, \ldots, a_n$ je největší index i takový, že $a_i \neq 0$. Stupeň nulového polynomu definujeme hodnotou -1.

Stupeň polynomu p značíme $\mathrm{St}\,p$

Pozorování: Pro nenulové polynomy p a q platí:

$$\mathrm{St}(p+q) \le \max(\mathrm{St}\,p,\ \mathrm{St}\,q), \qquad \mathrm{St}(p \cdot q) = \mathrm{St}\,p + \mathrm{St}\,q$$

Dělení polynomu polynomem se zbytkem

Věta: Pro polynomy p a q (polynom q nenulový) existují polynomy r a z takové, že

- $p = r \cdot q + z$, (neboli $p/q = r + z/q$),
- $\mathrm{St}\,z < \mathrm{St}\,q$.

Polynomu r říkáme *částečný podíl* a polynomu z říkáme *zbytek* při dělení polynomu p polynomem q.

Platnost věty je zaručena existencí algoritmu, který pro každé p, q vytvoří r a z uvedených vlastností.

Algoritmus (příklad):

$$\begin{array}{l}
(2x^5 - 3x^4 + 3x^3 - x^2 - 6x + 8) : (x^2 - 2x + 4) = 2x^3 + x^2 - 3x - 11 \\
\underline{-(2x^5 - 4x^4 + 8x^3)} \\
\quad x^4 - 5x^3 - x^2 - 6x + 8 \\
\quad \underline{-(x^4 - 2x^3 + 4x^2)} \\
\qquad -3x^3 - 5x^2 - 6x + 8 \\
\qquad \underline{-(-3x^3 + 6x^2 - 12x)} \\
\qquad\quad -11x^2 + 6x + 8 \\
\qquad\quad \underline{-(-11x^2 + 22x - 44)} \\
\qquad\qquad -16x + 52
\end{array}$$

Algoritmus (náčrt):

$$\begin{array}{l}
p \qquad\qquad : \ q \ = \ c_k x^k + c_{k-1} x^{k-1} + \ldots + c_0 \\
\underline{-c_k x^k \cdot q} \\
p - c_k x^k \cdot q \\
\underline{-c_{k-1} x^{k-1} \cdot q} \\
p - c_k x^k \cdot q - c_{k-1} x^{k-1} \cdot q \\
\underline{\qquad \ldots} \\
p - (c_k x^k + c_{k-1} x^{k-1} + \ldots + c_0) \cdot q = p - r\,q = z
\end{array}$$

Algoritmus:

- vždy skončí po konečně mnoha krocích,
- vyprodukuje polynomy r a z, které mají vlastnosti podle věty.

(rozmyslete si, proč)

Jednoznačnost částečného podílu a zbytku

Polynomy r a z s vlastnomstmi podle předchozí věty jsou určeny výchozími polynomy p a q jednoznačně.

Důkaz: Ať kromě r a z ještě polynomy r_1 a z_1 mají uvedené vlastnosti, tj.

$$p = r \cdot q + z = r_1 \cdot q + z_1, \qquad \mathrm{St}\, z < \mathrm{St}\, q, \quad \mathrm{St}\, z_1 < \mathrm{St}\, q.$$

Po odečtení první rovnosti je $(r - r_1)\, q = z_1 - z$. Stupeň na pravé straně je menší než q, takže na levé straně musí být q násobeno nulou. Tj. $r = r_1$. Z toho také plyne, že $z = z_1$.

Hornerovo schéma =

= algoritmus na efektivní vyhodnocení polynomu v daném bodě.

$$\begin{aligned} p(\alpha) &= a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_2\alpha^2 + a_1\alpha + a_0 = \\ &= ((\cdots((a_n\alpha + a_{n-1})\,\alpha + a_{n-2})\,\alpha + \cdots + a_2)\,\alpha + a_1)\,\alpha + a_0. \end{aligned}$$

Mezivýpočty (závorky) mohou zůstávat v registru procesoru.

Odhadněte počet násobení a sčítání při vyhodnocení polynomu stupně n v bodě

a) přímo pomocí vzorce z definice polynomu

b) podle Hornerova schématu

Tři řádky Hornerova schématu

Při psaní mezivýpočtů na papír můžeme použít třířádkové schéma:

$$\begin{array}{r|ccccccc} & a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\ \alpha: & & \alpha b_{n-1} & \alpha b_{n-2} & \dots & \alpha b_2 & \alpha b_1 & \alpha b_0 \\ \hline & b_{n-1} & b_{n-2} & b_{n-3} & \dots & b_1 & b_0 & p(\alpha) \end{array}$$

kde $b_{n-1} = a_n$, $b_{k-1} = a_k + \alpha b_k$ pro $k = n-1, n-2, \dots, 3, 2, 1$.

Vyplatí se to, protože platí následující tvrzení ...

Tvrzení: třetí řádek Hornerova schématu obsahuje koeficienty b_i, což jsou koeficienty polynomu r, pro který platí:

$$p(x) = r(x)\,(x - \alpha) + p(\alpha)$$

tedy: r je částečný podíl polynomu p polynomem $(x - \alpha)$.

Důkaz: je třeba využít rekurentních vztahů

$$b_{n-1} = a_n, \quad b_{k-1} = a_k + \alpha b_k$$

a propočítat výraz $r(x)\,(x - \alpha) + p(\alpha)$.

K čemu to je: nemusíme pro výpočet částečného podílu polynomu polynomem stupně prvního používat algoritmus ze slídu [12].

Kořen polynomu

Definice: *Kořen polynomu p* je takové číslo $\alpha \in \mathbf{C}$, pro které je $p(\alpha) = 0$.

Jinými slovy: kořen je číslo, ve kterém má polynom nulovou hodnotu.

Definice: *Kořenový činitel polynomu p* je polynom tvaru $x - \alpha$, kde α je kořen polynomu p.

Pozorování: Polynom je dělitelný svým kořenovým činitelem.

Důkaz: Částečný podíl polynomu p kořenovým činitelem $(x - \alpha)$ musí mít stupeň zbytku menší než 1, takže zbytek je konstanta z. Takže

$$p(x) = r(x) \cdot (x - \alpha) + z.$$

Po dosazení $x = \alpha$ dostáváme $0 = p(\alpha) = r(\alpha) \cdot 0 + z$, takže $z = 0$.

Základní věta algebry

Věta: Každý polynom stupně aspoň prvního má v $\mathbf{C}$ kořen.

Poznámka: Polynom stupně nula je nenulová konstanta, tj. nemá kořen.

Pozorování: Třebaže má polynom stupně aspoň prvního reálné koeficienty, nemusí mít žádný reálný kořen. Například polynom $x^2 + 1$. Základní věta algebry praví, že polynom má *komplexní*, kořen.

Důkaz základní věty algebry: neuvádíme.

Rozklad polynomu na kořenové činitele

Nechť p je polynom stupně aspoň prvního. Pak má kořen α_1 a je dělitelný kořenovým činitelem $x - \alpha_1$, tedy $p = (x - \alpha_1) \cdot p_1(x)$. Polynom p_1 má stupeň o jeden menší, než stupeň p.

Nechť p_1 je polynom stupně aspoň prvního. Pak má kořen α_2 a je dělitelný činitelem $x-\alpha_2$, tedy $p = (x-\alpha_1)\cdot p_1(x) = (x-\alpha_1)(x-\alpha_2)\cdot p_2(x)$. Polynom p_2 má stupeň o dva menší, než stupeň p.

Opakovaným postupem této úvahy dostáváme

$$p = (x - \alpha_1) \cdot p_1(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n) \cdot K,$$

kde $K = p_n$ je polynom stupně nultého (nenulová konstanta).

Tomuto vzorci se říká *rozklad polynomu p na kořenové činitele*.

Násobnost kořene

Pozorování: Všechna čísla α_i v předchozím vzorci (v rozkladu na kořenové činitele) jsou kořeny polynomu p.

Pozorování: Počet kořenových činitelů v předchozím vzorci je roven stupni polynomu.

Definice: *Násobnost* kořene α je počet výskytů čísla α v kořenových činitelích v rozkladu na kořenové činitele.

Pozorování: Každý polynom má tolik kořenů, kolik je jeho stupeň. Každý kořen ovšem započítáme tolikrát, kolik činí jeho násobnost.

Pozorování: Konstanta K v rozkladu na kořenové činitele je rovna koeficientu a_n.

Nalézt rozklad na kořenové činitele

není algebraicky pro obecný polynom p možné.

Při hledání rozkladu je totiž potřeba najít všechny kořeny polynomu p na základě znalosti jeho koeficientů. Vzorce existují pro polynomy stupně 1, 2, 3, 4 a dále pro některé speciální polynomy.

Příklad: Pro polynom stupně 2 vzorce pro kořeny jistě znáte:

$$\alpha_1 = \frac{-a_1 + \sqrt{a_1^2 - 4a_2a_0}}{2a_2}, \qquad \alpha_2 = \frac{-a_1 - \sqrt{a_1^2 - 4a_2a_0}}{2a_2}$$

Pro polynomy stupně pátého a vyššího algebraické vzorce *neexistují*. Pomocí teorie grup Niels Abel a Évartiste Galois dokázali, že tyto vzorce skutečně neexistují (tj. je dokázáno, že vzorce ani v budoucnu nikdo objeví).

To není ve sporu se základní větou algebry, která říká, že kořen existuje (zdůvodněte proč).

Speciální případ: kořeny jsou celá čísla

Jsou-li koeficienty polynomu celočíselné, pak je možno vyzkoušet, zda nepůjde nalézt kořen mezi děliteli koeficientu a_0. Těch je konečně mnoho. Pokud mezi nimi kořen nenalezneme, nemáme sice rozklad, ale máme aspoň jistotu, že polynom nemá další celočíselné kořeny. Platí totiž:

Věta: Je-li α celočíselný kořen polynomu p s celočíselnými koeficienty, pak α dělí koeficient a_0.

Důkaz: V rovnosti $0 = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ (která plyne z toho, že α je kořen) odečteme z obou stran a_0 a ze zbytku vytkneme α. Dostáváme $a_0 = -\alpha \cdot (a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) = \alpha \cdot c$, kde c je celé číslo. Takže α dělí a_0.

Příklad

Rozložíme $p(x) = x^5 - 12x^4 + 48x^3 - 62x^2 - 33x + 90$. Má-li být kořenem celé číslo, může to být jedině dělitel devadesátky, tedy čísla $1, 2, 3, 5, 6, \ldots, 90, -1, -2, -3, \ldots, -90$. Těchto konečně mnoho čísel můžeme zkusit dosadit do polynomu. Vychází např. $p(2) = 0$, takže 2 je kořen. Další kořeny stačí hledat v polynomu $p_1(x) = p(x)/(x-2)$. Koeficienty tohoto polynomu najdeme ve třetím řádku Hornerova schématu. Je $p_1(x) = x^4 - 10x^3 + 28x^2 - 6x - 45$. Tento polynom má kořen 3 a $p_2(x) = p(x)/((x-2)(x-3)) = x^3 - 7x^2 + 7x + 15$. Trojka je znovu kořen polynomu p_2 a $p_3(x) = p(x)/((x-2)(x-3)^2) = x^2 - 4x - 5$. Tento kvadratický polynom má kořeny 5 a -1. Rozklad daného polynomu je: $p(x) = (x-2)(x-3)^2(x-5)(x+1)$.

Jiný příklad: rozklad polynomu $x^5 - 12x^4 + 48x^3 - 62x^2 - 33x + 91$ nelze algebraicky nalézt. Dělitele 91 jsou $1, 7, 13, 91, -1, -7, -13, -91$. Můžeme zjistit, že žádné z těchto čísel není kořen, takže polynom nemá celočíselné kořeny.

Komplexně sdružené kořeny

Polynomy s reálnými koeficienty ne vždy mají jen reálné kořeny. Komplexní kořeny se ovšem v takovém případě vyskytují v párech:

Tvrzení: Je-li $\alpha \in \mathbf{C}$ kořen polynomu p s reálnými koeficienty, pak $\overline{\alpha}$ (komplexně sdružené číslo k číslu α) je také kořen polynomu p, dokonce stejné násobnosti.

Proč je $\overline{\alpha}$ kořen? Platí

$$\begin{aligned} p(\overline{\alpha}) &= a_0 + a_1\overline{\alpha} + a_2\overline{\alpha}^2 + \cdots + a_n\overline{\alpha}^n = \\ &= \overline{a_0} + \overline{a_1}\ \overline{\alpha} + \overline{a_2}\ \overline{\alpha^2} + \cdots + \overline{a_n}\ \overline{\alpha^n} = \\ &= \overline{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n} = \overline{p(\alpha)} = \overline{0} = 0. \end{aligned}$$

Proč mají α a $\overline{\alpha}$ stejnou násobnost? Součin $(x-\alpha)\cdot(x-\overline{\alpha})$ je polynom s reálnými koeficienty (propočítejte si to).

Reálný rozklad

Dvojici kořenových činitelů $(x-\alpha)$ a $(x-\overline{\alpha})$ můžeme roznásobit a dostáváme kvadratický polynom s reálnými koeficienty

$$(x-\alpha)\cdot(x-\overline{\alpha}) = x^2+\beta x+\gamma.$$

Nahradíme-li všechny takové páry kořenových činitelů jejich součiny, dostáváme v případě polynomu s reálnými koeficienty:

- součin kořenových činitelů s reálnými kořeny násobený
- součinem kvadratických polynomů, které nemají reálné kořeny.

Reálný rozklad má obecně tvar

$$p(x) = c\cdot(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)(x^2+\beta_1 x+\gamma_1)\cdots(x^2+\beta_m x+\gamma_m)$$

Reálný rozklad s násobnostmi

Zapíšeme-li v reálném rozkladu vícenásobné kořenové činitele pomocí mocnin a stejně tak opakované kvadratické polynomy pomocí mocnin, dostáváme rozklad:

$$p(x) = c\,(x-\alpha_1)^{u_1}\cdots(x-\alpha_k)^{u_k}\cdot(x^2+\beta_1 x+\gamma_1)^{v_1}\cdots(x^2+\beta_m x+\gamma_m)^{v_m}$$

Takový rozklad se často používá,

- aby se výpočet obešel bez použití komplexních čísel a
- aby explicitně počítal s možností výskytu vícenásobných kořenů

(např. integrál racionální lomené funkce).

Parciální zlomky

Věta: Nechť $\mathrm{St}\,p < \mathrm{St}\,q$ a α je k násobným kořenem polynomu q. Označme $q = (x-\alpha)^k\cdot q_1$. Pak existuje $a\in\mathbf{C}$ a polynom p_1 takový, že $\mathrm{St}\,p_1 < \mathrm{St}\,q - 1$ a

$$\frac{p(x)}{q(x)} = \frac{a}{(x-\alpha)^k} + \frac{p_1(x)}{(x-\alpha)^{k-1}q_1(x)} \quad \forall\, x\in\mathbf{C} \text{ takové, že } q(x)\neq 0$$

Důkaz: Protože α je k-násobným kořenem q, platí $q_1(\alpha)\neq 0$. Dokazovaná rovnost je ekvivalentní s $p(x) = a\cdot q_1(x) + p_1(x)\cdot(x-\alpha)$. Po dosazení $\alpha\to x$ je $p(\alpha) = a\cdot q_1(\alpha)$, tj. $a = p(\alpha)/q_1(\alpha)$. Polynom $p(x) - a\cdot q_1(x)$ má stupeň nejvýše roven $\max(\mathrm{St}\,p, \mathrm{St}\,q_1)$ a má kořen α. Dělení jeho kořenovým činitelem vychází tedy beze zbytku a výsledkem dělení je polynom p_1. Jeho stupeň je tedy aspoň o jedničku menší než $\max(\mathrm{St}\,p, \mathrm{St}\,q_1)$ a je tedy menší než $\mathrm{St}\,q - 1$.

Rozklad na parciální zlomky

je důsledek předchozí věty:

$$\frac{p(x)}{q(x)} = \frac{a_k}{(x-\alpha)^k} + \frac{a_{k-1}}{(x-\alpha)^{k-1}} + \cdots + \frac{a_1}{(x-\alpha)} + \frac{p_2(x)}{q_1(x)} =$$
$$= \sum_{i=1}^{k_1}\frac{a_{i,k_1}}{(x-\alpha_1)^i} + \sum_{i=1}^{k_2}\frac{a_{i,k_2}}{(x-\alpha_2)^i} + \cdots + \sum_{i=1}^{k_u}\frac{a_{i,k_u}}{(x-\alpha_r)^i}$$

Reálný rozklad na parciální zlomky:

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{k_1}\frac{a_{i,k_1}}{(x-\alpha_1)^i} + \sum_{i=1}^{k_2}\frac{a_{i,k_2}}{(x-\alpha_2)^i} + \cdots + \sum_{i=1}^{k_u}\frac{a_{i,k_u}}{(x-\alpha_r)^i} +$$
$$+ \sum_{i=1}^{m_1}\frac{b_{i,m_1}x + c_{i,m_1}}{(x^2+\beta_1 x+\gamma_1)^i} + \sum_{i=1}^{m_2}\frac{b_{i,m_2}x + c_{i,m_2}}{(x^2+\beta_2 x+\gamma_2)^i} + \cdots + \sum_{i=1}^{m_v}\frac{b_{i,m_v}x + c_{i,m_v}}{(x^2+\beta_s x+\gamma_s)^i}$$

Polynom nad tělesem

Číselné obory **Q**, **R** a **C** jsou příklady takzvaných *těles* (o tom promluvíme podrobněji později). Těleso zde značím písmenem T.

Pokud polynom má koeficienty jen z T a definiční obor je také z T (tj. za formální proměnnou x dosazujeme jen čísla z T), pak hovoříme o *polynomu nad tělesem T*.

Definice: Polynom p nad tělesem T je *ireducibilní v T*, pokud jej není možné rozložit na součin polynomů r, s nad T stupně aspoň prvního. Takže nemůže platit $p = r \cdot s$.

Pokud je možné polynom výše zmíněným způsobem rozložit, říkáme mu *reducibilní v T*.

Příklad: Polynom $x^2 + 1$ je ireducibilní v **R**.

Příklad: Polynom $x^2 + 1$ je reducibilní v **C**, protože

$$x^2 + 1 = (x + i) \cdot (x - i).$$

Příklad: V **C** jsou ireducibilní pouze polynomy stupně nejvýše prvního. To zaručuje základní věta algebry.

Příklad: Polynom $x^2 - 2$ je ireducibilní v **Q**, ale je reducibilní v **R** i **C**, protože $x^2 - 2 = (x - \sqrt{2}) \cdot (x + \sqrt{2})$ a to jsou polynomy stupně aspoň prvního nad **R** i nad **C**, ale ne nad **Q**.

Příklad: Rozklad na kořenové činitele je rozklad na součin ireducibilních polynomů v **C**.

Příklad: Reálný rozklad je rozklad na součin ireducibilních polynomů v **R**.