10. Okruhy polynomů

1. Zjistěte, zda je prvek $1+x$ invertibilní v $\mathbb{Z}[[x]]$.

2. Buď R obor integrity a ať $a \in R[[x]]$ má invertibilní prvek, řekněme b. Dokažte, že pak $b' = -b^2 a'$.

3. V $R[[x]]$ můžeme definovat i derivace vyšších řádů. Klademe $a^{(0)} = a$ a $a^{(i+1)} = (a^{(i)})'$. Dokažte Leibnizovu formuli

$$(ab)^{(n)} = \sum_{0 \le i \le n} \binom{n}{i} a^{(i)} b^{(n-i)}$$

pro libovolná $a, b \in R[[x]]$ a $n \ge 0$. Dokažte, že je-li $a = \sum a_i x^i$, tak $a^{(n)} = \sum (i+1)\dots(i+n) a_{i+n} x^i$.

4. Dokažte, že v $T[[x]]$, kde T je těleso, je $a = \sum a_i x^i$ invertibilní prvek právě když $a_0 \ne 0$. Zobecněte toto tvrzení pro libovolný okruh.

5. Máme-li vypočítat hodnotu polynomu $a = \sum a_i x^i \in R[x]$ v bodě $\alpha \in R$, lze s výhodou použít tzv. Hornerova schématu. Ať $n = \operatorname{st} a$. Definujme $b_{n-1} = a_n$ a $b_j = a_{j+1} + \alpha b_{j+1}$ pro $-1 \le j < n-1$. Hornerovým schématem se míní takový zápis, že do prvé řádky se umístí $a_n \ a_{n-1} \ \dots \ a_0$, do druhé $0 \ \alpha b_{n-1} \ \dots \ \alpha b_0$ a do třetí $b_{n-1} \ b_{n-2} \ \dots \ b_{-1}$. Protože třetí řádek je součtem prvého a druhého, lze zjevně Hornerovo schéma vyplňovat zleva doprava po sloupcích. Nakonec se získá hodnota b_{-1}, a ta je (viz následující cvičení) rovna $a(\alpha)$. Vypočtěte pomocí Hornerova schématu hodnotu polynomu $x^6 + 2x^5 - 3x^4 + x^3 - 5x^2 + 3x - 1 \in \mathbb{Z}[x]$ v bodě 3.

6. (Pokračování.) Položte $b = \sum_{0 \le i < n} b_i x^i$ a dokažte, že $a = (x - \alpha) b + b_{-1}$, a tím i $a(\alpha) = b_{-1}$.

7. (Pokračování.) Představme si, že Hornerovo schéma vytvoříme znovu, opět v bodě α, ale vstupním polynomem nebude a, nýbrž b. Dalším opakováním tak dostaneme řadu polynomů, označme je například $a^{[i]}$, takovou, že $a^{[0]} = a$ a $a^{[i]} = a^{[i+1]}(x - r) + a^{[i]}(r)$. Dokažte, že $a^{(k)}(\alpha) = (k!) a^{[k]}(\alpha)$ ($a^{(k)}$ je k–tá derivace polynomu a). Spočítejte uvedeným způsobem prvou až šestou derivaci polynomu $x^6 + 2x^5 - 3x^4 + x^3 - 5x^2 + 3x - 1 \in \mathbb{Z}[x]$ v bodě 3.

8*. Uvažme podokruhy $\mathbb{Z}[\sqrt{2}]$ a $\mathbb{Z}[\sqrt{3}]$ tělesa $\mathbb{R}$. Ukažte, že se jedná o eukleidovské obory integrity, kde eukleidovskými funkcemi jsou (po řadě) zobrazení $a + b\sqrt{2} \to |a^2 - 2b^2|$ a $a + b\sqrt{3} \to |a^2 - 3b^2|$. (Srovnej s cvičením 18.)

9. Spočítejte největší společný násobek polynomů $2x^3 + 1$ a $x^4 - x^3 + 2x^2 - x - 1$, a to jednak v $\mathbb{Q}[x]$, jednak v $\mathbb{Z}_3[x]$.

10. Buď $c = NSD(a, b)$, kde $a, b, c \in \mathbb{Q}[x]$. Dokažte, že c je největší společný dělitel a a b také v $\mathbb{R}[x]$ a $\mathbb{C}[x]$.

11. Uvažte (nekomutativní) těleso kvaterniónů $\mathbb{H}$ (viz cvičení 14 kapitoly 5) a ukažte, že v $\mathbb{H}[x]$ existuje polynom stupně 2, který má více než dva kořeny.

12. Kolik různých kořenů, a jaké násobnosti, má polynom $x^3 - 1$ v $\mathbb{C}[x]$, v $\mathbb{R}[x]$ a $\mathbb{Z}_3[x]$?

13. Je-li R okruh a A množina, tak R^A označme množinu všech zobrazení $f : A \to R$. Na R^A lze definovat binární operace sčítání 'po složkách', tj. pro $f, g \in R^A$ budou $f+g$ a $f \cdot g$ definovány tak, že $(f+g)(a) = f(a)+g(a)$ a $(fg)(a) = f(a)g(a)$ pro všechna $a \in A$. Definujte na R^A unární operaci a nulární operace tak, aby R^A byl okruh.

14. (Pokračování) Definujte zobrazení $\tau : R[x] \to R^R$ tak, že $(\tau(a))(\alpha) = a(\alpha)$ pro všechna $a \in R[x]$ a $\alpha \in A$. Dokažte, že $\tau : R[x] \to R^R$ je homomorfismus. Předpokládejte navíc, že R je obor integrity. Ukažte, že pak je τ prosté právě když R je nekonečná množina.

15. (Pokračování) Buď T nekonečné komutativní těleso. Ukázali jsme, že v takovém případě každému prvku a oboru integrity $T[x]$ odpovídá právě jedna polynomiální funkce $\alpha \to a(\alpha)$. Jaké funkce odpovídají prvkům podílového tělesa $T[x]$? Dokažte!

16. Najděte nějaký generátor (tzv. primitivní prvek) grupy $\mathbb{Z}_{23}^*$. Kolik má grupa $\mathbb{Z}_{23}^*$ generátorů?

17. Číslo $p = 2^{31} - 1$ je prvočíslo a 7 je primitivní prvek (generátor) grupy $\mathbb{Z}_p^*$. Dokažte, že potom je i číslo 16807 primitivní prvek $\mathbb{Z}_p$.

18*. Dokažte, že okruh $\mathbb{Z}[\sqrt{5}]$ není Gaussův. (Návod: Ukažte, že prvek 2 je ireducibilní, ale není prvočíslo. Využijte toho, že 2 dělí $4 = (\sqrt{5}+1)(\sqrt{5}-1)$. Jako první krok ověřte, že $u = a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ je invertibilní právě když $N(u) = a^2 - 5b^2$ je rovno ± 1. Potom ukažte, že pro $u, v \in \mathbb{Z}[\sqrt{5}]$, $u|v$, platí $N(u)|N(v)$, přičemž u je vlastním dělitelem v právě když $N(u)$ je vlastním dělitelem $N(v)$. Ověřte, že $N(u)$ je různé od ± 2 pro každé $u \in \mathbb{Z}[\sqrt{5}]$, a z předchozího kroku odvoďte, že u je ireducibilní, kdykoliv platí $N(u) = \pm 4$.)

Řešení

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

2. $ab = 1$, takže $(ab)' = a'b + ab' = 0$, odkud $a'b^2 + (ab)b' = 0 = a'b^2 + b'$.

3. $(ab)^{(n+1)} = \left(\sum \binom{n}{i} a^{(i)} b^{(n-i)}\right)' = \sum \binom{n}{i} a^{(i+1)} b^{(n-i)} + \sum \binom{n}{i} a^{(i)} b^{(n+1-i)} = a^{(n+1)} + b^{(n+1)} + \sum_{1 \le i \le n} \left(\binom{n}{i} + \binom{n}{i+1}\right) a^{(i)} b^{(n+1-i)} = \sum_{0 \le i \le n+1} \binom{n+1}{i} a^{(i)} b^{(n+1-i)}$. Dále $a^{(n+1)} = (a^{(n)})' = (\sum (i+1)\dots(i+n) a_{i+n} x^i)' = \sum (i+1)(i+2)\dots(i+n+1) a_{i+n+1} x^i$.

4. Definujme b_j, $j \ge 0$, indukcí tak, aby $(\sum_{0 \le i \le j} a_i x^i) \cdot (\sum_{0 \le i \le j} b_i x^i)$ byl polynom rovný $1 + \sum c_i x^i$, kde $c_i = 0$ pro $0 \le i \le j$. Pro $j = 0$ stačí položit $b_0 = a_0^{-1}$. Dále $(\sum_{0 \le i \le j+1} a_i x^i) \cdot (\sum_{0 \le i \le j+1} b_i x^i) = 1 + c_{j+1} x^{j+1} + a_{j+1} b_0 x^{j+1} + a_0 b_{j+1} x^{j+1} + \sum_{i \ge j+1} d_i x^i$, takže za b_{j+1} lze zvolit $-a_0^{-1}(a_{j+1} b_0 + c_{j+1})$. V obecném případě je zjevně možné použít pro $a_0 \in R$ invertibilní tutéž konstrukci.

5.

1	2	−3	1	−5	3	−1
0	3	15	36	111	318	963
1	5	12	37	106	321	962

6. $(x-r)b+b_{-1}=\sum(b_{i-1}-rb_i)x^i=\sum a_i x^i=a$.

7. Indukcí podle k, případ $k=0$ je zřejmý. Je $a=(x-r)b+a(r)$. Z Leibnizovy formule plyne $a^{(k+1)}=(x-r)b^{(k+1)}+(k+1)b^{(k)}$. Přitom $b^{(k)}(r)=k!b^{[k]}(r)=k!a^{[k+1]}(r)$ podle indukčního předpokladu, takže $a^{(k+1)}(r)=(k+1)!a^{[k+1]}(r)$.

Hornerovo schéma z cvičení 5 pokračuje takto:

1	5	12	37	106	321
0	3	24	108	435	1623
1	8	36	145	541	1944
0	3	33	207	1056	
1	11	69	352	1597	
0	3	42	333		
1	14	111	685		
0	3	51			
1	17	162			
0	3				
1	20				
0					
1					

Derivace tedy po řadě jsou 1944, $1597\cdot 2=3194$, $685\cdot 6=4110$, $162\cdot 24=3888$, $20\cdot 120=2400$, $1\cdot 720=720$.

8. Funkci $\mu:\mathbb{Z}[\sqrt{2}]\to\mathbb{N}_0$, $\mu(a+b\sqrt{2})=a^2-2b^2$ můžeme rozšířit i na okruh $\mathbb{Q}[\sqrt{2}]$. Snadno ověříme, že pro libovolná $u,v\in\mathbb{Q}[\sqrt{2}]$ platí $\mu(u\cdot v)=\mu(u)\cdot\mu(v)$. Naším úkolem je pro daná nenulová $a+b\sqrt{2}, c+d\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ nalézt $p+q\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ tak, aby platilo $\mu((a+b\sqrt{2})-(c+d\sqrt{2})(p+q\sqrt{2}))<\mu(c+d\sqrt{2})$. Tuto nerovnost lze ovšem díky multiplikativitě μ zapsat jako $\mu(\frac{a+b\sqrt{2}}{c+d\sqrt{2}}-(p+q\sqrt{2}))<1$. Výraz v závorce upravíme na $(\frac{ac-2bd}{c^2-2d^2}-p)+(\frac{bc-ad}{c^2-2d^2}-q)\sqrt{2}$. Zvolíme celá čísla p a q tak, aby hodnoty obou rozdílů byly $\leq\frac{1}{2}$ (p a q jsou tedy nejlepší možné celočíselné aproximace daných zlomků). Snadno nyní nahlédneme, že μ nabývá v uvažovaném případě nanejvýš hodnoty $\frac{1}{2}$.

V okruhu $\mathbb{Z}[\sqrt{3}]$ lze postupovat zcela stejně, hodnota μ je při analogickém postupu omezena $\frac{3}{4}$.

Všimněte, si (viz též cvičení 18), že již pro $\mathbb{Z}[\sqrt{5}]$ tentýž postup nevede k cíli, neboť závěrečné omezení dá hodnotu $\frac{5}{4}$, což je více než 1.

9. V $\mathbb{Q}[x]$ jsou oba polynomy nesoudělné, v $\mathbb{Z}_3[x]$ je jejich NSD roven $x-1$.

10. Eukleidův algoritmus proběhne ve všech třech zmíněných okruzích stejně, (tj. členy příslušné posloupnosti všechny leží v $\mathbb{Q}[x]$).

11. $x^2 + 1$ má kořeny i, j, k, $-i$, $-j$ a $-k$.

12. V $\mathbb{C}[x]$ 3 kořeny, v $\mathbb{R}[x]$ 1 kořen, v obou případech násobnosti 1. V $\mathbb{Z}_3[x]$ 1 kořen, násobnosti 3.

13. $-f$ definujeme tak, že $(-f)a = -(f(a))$ pro každé $a \in A$. Roli neutrálního prvku (nuly) má konstatní zobrazení $a \to 0$.

14. $\operatorname{Ker} \tau$ obsahuje nenulový polynom $\Leftrightarrow$ existuje polynom takový, že všechny prvky R jsou jeho kořeny.

15. Racionální funkce $\alpha \to \frac{a(\alpha)}{b(\alpha)}$.

16. Nejmenší primitivní prvek je 5, dohromady jich je $\varphi(22) = 10$.

17. $i \mapsto 7^i \bmod p$ je izomorfismus $\mathbb{Z}_{p-1}(+)$ a $\mathbb{Z}_p^*(\cdot)$. Přitom $16807 = 7^5$, 5 je nesoudělné s $2^{31} - 2$, a tedy generátor $\mathbb{Z}_{p-1}(+)$.