5. Algebrou za lepší pochopení algebry

Ideály v okruzích

Definici ideálu (i s obrázkem!) viz na str. 40 skript a definici hlavního ideálu tamtéž v Tvrzení 7.4.

1. Určete $a, b \in \mathbb{N}$ takové, že $2\mathbb{Z} \cap 3\mathbb{Z} = a\mathbb{Z}$, resp. $2\mathbb{Z} + 3\mathbb{Z} = b\mathbb{Z}$. [$a = 6$, $b = 1$]

2. Najděte $a \in \mathbb{N}$ tak, aby ideál $a\mathbb{Z}$ byl roven:

   (a) $28\mathbb{Z} + 63\mathbb{Z}$ [7]

   (b) $15\mathbb{Z} + 18\mathbb{Z} + 40\mathbb{Z}$ [1]

   (c) $(-28)\mathbb{Z} \cap (-63)\mathbb{Z}$ [252]

3. Nechť $R = \mathbb{Z}[i]$. Najděte $a, b \in R$ taková, že $aR = (3+i)R + (4+2i)R$ a $bR = (3+i)R \cap (4+2i)R$.
   [s využitím 4.5(a): $a \parallel 1+i$, $b \parallel 10$]

4. Ať R je obor hlavních ideálů. Dokažte, že pro zadaná $a, b \in R$ je $aR \cap bR = cR$, kde $c =$NSN(a, b). (Nejdřív si tvrzení zkuste rozmyslet pro $R = \mathbb{Z}, \mathbb{Z}[i]$ a pak případně zobecněte pro libovolný OHI.)

5. Nechť $S = \mathbb{Z}[x]$ a uvažujme ideály $I = 2S + xS$ a $J = 3S + xS$. Ukažte, že:

   (a) I, J nejsou hlavní ideály. [kdyby byly, musely by být generovány dělitelem 2, resp. 3, který, protože jde o vlastní ideály, není invertibilní, tedy jde o ± 2 (resp. ± 3), čímž ale nenageneruji polynom x]

   (b) množina $\{ab \mid a \in I, b \in J\}$ netvoří ideál v okruhu S. *(Nápověda: přemýšlejte o polynomu $p(x) = x$.)* [polynom x nelze napsat jako součin ab ze zadání, na druhou stranu zde ale leží, protože $2x, 3x$ jsou daného tvaru součinu a ideál musí být uzavřený na sčítání]

(I)reducibilita polynomů v gaussovských oborech

6. Najděte všechny racionální kořeny daných polynomů z $\mathbb{Z}[x]$ (*především určete možné kandidáty, ideálně pomocí Tvrzení 8.1*):

   (a) $2x^3 - x^2 + 3$ [-1]

   (b) $4x^7 - 16x^6 + x^5 + 55x^4 - 35x^3 - 38x^2 + 12x + 8$. [$-\frac{1}{2}, 2$]

7. Rozmyslete si, proč je polynom $f(x) = 2x + 6$ ireducibilní v $\mathbb{Q}[x]$, ale je rozložitelný v $\mathbb{Z}[x]$. Najděte k němu v $\mathbb{Q}[x]$ asociovaný primitivní polynom. [2 je v $\mathbb{Q}$ invertibilní; $x + 3$]

8. Rozmyslete si, proč jsou následující polynomy v příslušných oborech ireducibilní (*může se hodit Eisensteinovo kritérium z Tvrzení 8.2*):

   (a) $x^3 + x^2 + x + 3$ v $\mathbb{Z}[x]$ [musel by mít kořen..]

   (b) $x^4 + x^3 - x + 1$ v $\mathbb{Z}[x]$ [upočítat možný rozklad na kvadratické]

   (c) $4x^3 - 15x^2 + 60x + 180$ v $\mathbb{Z}[x]$ [Eisenstein pro 5]

   (d) $x^5 - 36x^4 + 6x^3 + 30x^2 + 24$ v $\mathbb{Q}[x]$ [Eisenstein pro 3 + vztah ireducibility v $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$]

9. Spočtěte v oboru $\mathbb{Z}[x, y]$ NSD pro polynomy $6x^2y$ a $15xy^2 + 21x^3y$. (*Zaměřte se na zdůvodnění dle Věty 8.5 ze skript.*) [NSD $\parallel 3xy$]

10. Najděte v příslušných oborech ireducibilní rozklady daných polynomů:

	$x^2 - y + 2$	$x^2 - 2y^2$	$x^2 + y^2$	$x^2 + xy + y - 1$
$\mathbb{Q}[x, y]$	ireducibilní	ireducibilní	ireducibilní	$(x + 1)(x - 1 + y)$
$\mathbb{R}[x, y]$	ireducibilní	$(x+\sqrt{2}y)(x-\sqrt{2}y)$	ireducibilní	$(x + 1)(x - 1 + y)$
$\mathbb{C}[x, y]$	ireducibilní	$(x+\sqrt{2}y)(x-\sqrt{2}y)$	$(x + iy)(x - iy)$	$(x + 1)(x - 1 + y)$

A pro odvážné několik zábavných příkladů navíc:

11. Buď $R = \{f \in \mathbb{Q}[x];\ f(0) \in \mathbb{Z}\}$. Pak je R podokruh oboru $\mathbb{Q}[x]$. Dokažte, že pro libovolné $f, g \in R$ existuje NSD(f, g). Proč není přesto R Gaussovým oborem?

12. Rozložte polynom $2x^2 + 2x - 1$ nad eukleidovským oborem $\mathbb{Z}[\sqrt{3}]$ na ireducibilní prvky.
[$((\sqrt{3} - 1)x + 1)((\sqrt{3} + 1)x - 1)$]

13. (Další možná metoda, používá se obměněná implikace) Ukažte, že je-li primitivní polynom $f(x) \in \mathbb{Z}[x]$ reducibilní a prvočíslo p nedělí vedoucí koeficient $f(x)$, pak je reducibilní i polynom $\overline{f(x)} \in \mathbb{Z}_p[x]$ získaný vzetím koeficientů $f(x)$ modulo p.

14. S využitím předchozího tvrzení rozhodněte o (i)reducibilitě polynomu $x^5 + 4x^4 + 2x^3 + 3x^2 - x + 5$ v oboru $\mathbb{Z}[x]$. [ireducibilní; uvaž mod 3]

15. (Ještě jedna možná metoda:) Ukažte, že je-li R obor, pak polynom je $f(x) \in \mathbf{R}[x]$ reducibilní právě tehdy, je-li v $\mathbf{R}[x]$ reducibilní polynom $g(x)$ získaný z $f(x)$ lineární substitucí $x \mapsto ax + b$ pro $a, b \in \mathbf{R}$ a a invertibilní v R.

16. S využitím předchozího tvrzení rozhodněte o (i)reducibilitě následujících polynomů v $\mathbb{Z}[x]$
    (a) $x^4 + x^3 + x^2 + x + 1$ [ireducibilní, substituce $x \mapsto x + 1$]
    (b) $x^3 + 3x^2 + 5x + 5$ [ireducibilní, substituce $x \mapsto x - 1$]
    (c) $\frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i$ pro prvočíslo p [ireducibilní, substituce $x \mapsto x + 1$]

.

17. Rozložte v $\mathbb{Z}[x]$ polynom $x^{16} - 1$ na součin ireducibilních polynomů. [$(x^8+1)(x^4+1)(x^2+1)(x+1)(x-1)$; pro polynomy tvaru $x^{2^k} + 1$ využijme substituce $x \mapsto x + 1$ a Eisensteinovo kritérium.]

18. Rozmyslete si, proč je polynom $3x^3 + 2x^2 + (4 - 2i)x + (1 + i)$ v $(\mathbb{Z}[i])[x]$ ireducibilní.
[Eisenstein pro $1 + i$]