Глава 8

Въпрос 8: Ньотерови пръстени. Теорема на Хилберт за базиса. Базиси на Грьобнер.

В настоящия въпрос ще докажем, че всеки идеал I в полиномиален пръстен $k[x_1, \ldots, x_n]$ е крайнопороден.

Определение 8.1. *Комутативният пръстен с единица R се нарича ньотеров, ако всеки идеал I в R е крайнопороден.*

За целта да започнем със следното

Определение 8.2. *Нека I е ненулев идеал в пръстена $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле k. Тогава мономният идеал $\langle LT(I) \rangle$, породен от множеството*

$$LT(I) := \{LT(f) \,|\, f \in I,\, f \neq 0 \in k[x_1, \ldots, x_n]\}$$

на старшите членове $LT(f)$ на ненулевите полиноми f от I се нарича идеал на старшите членове на I.

Ако идеалът $I = \langle f_1, \ldots, f_s \rangle$ в $k[x_1, \ldots, x_n]$ е породен от ненулевите полиноми $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, то $LT(f_i) \in LT(I) \subset \langle LT(I) \rangle$ за всяко $1 \leq i \leq s$, така че

$$\langle LT(f_1), \ldots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle.$$

Включването може да е строго, както се вижда от следния

Пример 8.3. Относно градуирано лексикографската наредба полиномите $f_1 = x^3 - 2xy$ и $f_2 = x^2y - 2y^2 + x$ имат старши членове $LT(f_1) = x^3$ и съответно $LT(f_2) = x^2y$. Следователно ненулевите полиноми в мономния идеал $\langle LT(f_1), LT(f_2) \rangle = \langle x^3, x^2y \rangle$ имат степен ≥ 3. Но, от друга страна,

$$x^2 = x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = xf_2 - yf_1 \in \langle f_1, f_2 \rangle = I$$

води до

$$x^2 = LT(x^2) \in LT(I) \subset \langle LT(I) \rangle,$$

така че

$$\langle LT(f_1), LT(f_2) \rangle \subsetneqq \langle LT(I) \rangle \quad \text{за} \quad I = \langle f_1, f_2 \rangle.$$

По определение, идеалът $\langle LT(I) \rangle$ на старшите членове на ненулев идеал I в полиномиален пръстен $k[x_1, \ldots, x_n]$ е мономен идеал. Следователно по Лемата на Диксон 2 съществуват краен брой ненулеви полиноми $g_1, \ldots, g_t \in I$, така че

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$$

се поражда от старшите им членове. Това ни дава възможност да докажем следната

Теорема 3. (Теорема на Хилберт за базиса) *Пръстенът $k[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле k е ньотеров.*

Доказателство: Ще установим, че за всеки идеал $I \triangleleft k[x_1, \dots, x_n]$ съществуват ненулеви полиноми $g_1, \dots, g_t \in I$, така че $I = \langle g_1, \dots, g_t \rangle$ се поражда от тях.
Ако $I = \{0\}$ е нулевият идеал, то $I = \langle 0 \rangle$ се поражда от тъждествено нулевия полином $0 \in k[x_1, \dots, x_n]$.
Ако идеалът $I \triangleleft k[x_1, \dots, x_n]$ е ненулев, да изберем ненулеви полиноми $g_1, \dots, g_t$ от I, чиито старши членове пораждат идеала $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ на старшите членове на I. Твърдим, че тези полиноми пораждат първоначалния идеал $I = \langle g_1, \dots, g_t \rangle$. Включването $\langle g_1, \dots, g_t \rangle \subseteq I$ е ясно. За обратното включване, нека $f \in I$ е произволен полином от I. При деление на f с $g_1, \dots, g_t$ получаваме представяне от вида

$$f = a_1 g_1 + \ldots + a_t g_t + r$$

за някакви полиноми $a_1, \dots, a_t, r \in k[x_1, \dots, x_n]$, така че $r = 0$ или нито един моном на r не се дели на $LT(g_1), \dots, LT(g_t)$. Трябва да докажем, че $r = 0$ за да получим, че $f \in \langle g_1, \dots, g_t \rangle$. По този начин установяваме включването $I \subseteq \langle g_1, \dots, g_t \rangle$, откъдето и съвпадението $I = \langle g_1, \dots, g_t \rangle$. Наистина, ако допуснем, че остатъкът r не е тъждествено нулев, то $r = f - a_1 g_1 - \ldots a_t g_t \in I$ има старши член $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1, \dots, LT(g_t) \rangle$. Съгласно Лема 7.2 съществува $1 \leq i \leq t$, така че $LT(g_i)$ дели $LT(r)$. Това противоречи на свойствата на остатъка r и установява тъждественото му анулиране $r = 0 \in k[x_1, \dots, x_n]$, Q.E.D.

Определение 8.4. (Базис на Грьобнер) *Нека I е ненулев идеал в $k[x_1, \dots, x_n]$. Ненулевите полиноми $g_1, \dots, g_t \in I$ образуват базис на Грьобнер на I относно фиксирана мономна наредба, ако старшите им членове $LT(g_1), \dots, LT(g_t)$ пораждат идеала $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ на старшите членове на I.*

От Лемата на Диксон 2 следва, че всеки ненулев идеал I в има базис на Грьобнер $g_1, \dots, g_t$ относно фиксирана мономна наредба. Още повече, по Теоремата на Хилберт за базиса 3, всеки базис на Грьобнер $g_1, \dots, g_t$ на I е пораждащо множество за този идеал, $I = \langle g_1, \dots, g_t \rangle$. Обратното не винаги е вярно. Съществуват пораждащи $g_1, \dots, g_t$ на идеал $I = \langle g_1, \dots, g_t \rangle$ в $k[x_1, \dots, x_n]$, чиито старши членове $LT(g_1), \dots, LT(g_t)$ не пораждат идеала на старшите членове $\langle LT(I) \rangle$, така че $g_1, \dots, g_t$ не образуват базис на Грьобнер на $I = \langle g_1, \dots, g_t \rangle$. В Пример 8.3 разгледахме полиномите $f_1 = x^3 - 2xy$ и $f_2 = x^2 y - 2y^2 + x$, които не образуват базис на Грьобнер на идеала $I = \langle f_1, f_2 \rangle$, породен от тях.

Пример 8.5. *Полиномите $x + z, y - z \in \mathbb{R}[x, y, z]$ образуват базис на Грьобнер на идеала $J = \langle x + z, y - z \rangle \triangleleft \mathbb{R}[x, y, z]$ относно лексикографската наредба.*

За да докажем твърдението, изказано в Пример 8.5 трябва да установим, че старшият член $LT(f)$ на произволен ненулев полином $f \in J$ принадлежи на идеала $\langle LT(x+z), LT(y-z) \rangle = \langle x, y \rangle$. Съгласно Лема 7.2, това е еквивалентно на делимост на $LT(f)$ с x или с y. При допускане на противното, $LT(f)$ а оттам и f се оказват полиноми на z. Но единственият полином $f(z) \in \langle x + z, y - z \rangle \subseteq IV(x + z, y - z) = I\left(\{(-z, z, z) \,|\, z \in \mathbb{R}\}\right)$ е тъждествено нулевият, така че $LT(f) \in \langle x, y \rangle$ за $\forall 0 \neq f \in J$ и $x + z, y - z$ е базис на Грьобнер на $J = \langle x + z, y - z \rangle$ относно лексикографската наредба.
Базисите на Грьобнер са въведени от Хиронака в средата на 60-те години. Той ги нарича стндартни базиси. Малко по-късно и независимо от него те са изучени в дисертацията на Бухбергер, който им дава името на своя научен ръководител Грьобнер.
Теоремата на Хилберт за базиса 3 дава непосредствено следната

ТЕОРЕМА 4. *Всяка ненамаляваща редица от идеали* $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ *в* $k[x_1,\dots,x_n]$ *се стабилизира след краен брой стъпки, т.е. съществува естествено число* N, *така че* $I_N = I_{N+1} = I_{N+2} = \dots$.

Доказателство: Обединението $I = \cup_{s=1}^{\infty} I_s$ на ненамаляваща редица от идеали $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ е идеал в $k[x_1,\dots,x_n]$. Наистина, ако $f, g \in I$, то съществуват естествени числа a, b, така че $f \in I_a$, $g \in I_b$. За $m = \max(a,b)$ имаме $f \in I_a \subseteq I_m$ и $g \in I_b \subseteq I_m$, откъдето $f - g \in I_m \subseteq I$, защото I_m е идеал в $k[x_1,\dots,x_n]$. За произволни $f \in I_a$ и $h \in k[x_1,\dots,x_n]$ получаваме, че $fh \in I_a \subseteq I$, доколкото I_a е идеал в $k[x_1,\dots,x_n]$. Това установява, че I е идеал в $k[x_1,\dots,x_n]$.
Съгласно Теоремата на Хилберт за базиса 3, съществуват полиноми $f_1,\dots,f_s \in I$, които пораждат $I = \langle f_1,\dots,f_s\rangle$. Ако $f_j \in I_{k_j}$ за $1 \leq j \leq s$ и положим $N = \max(k_1,k_2,\dots,k_s)$, то $f_1,\dots,f_s \in I_N$, съгласно $I_{k_j} \subseteq I_N$ за $k_j \leq N$. Следователно

$$I = \langle f_1,\dots,f_s\rangle \subseteq I_N \subseteq I_{N+1} \subseteq \dots \subseteq I,$$

откъдето $I = \langle f_1,\dots,f_s\rangle = I_N = I_{N+1} = I_{N+2} = \dots$, Q.E.D.

ОПРЕДЕЛЕНИЕ 8.6. *Многообразието* $V(I)$ *на идеал* I *в полиномиален пръстен* $k[x_1,\dots,x_n]$ *се определя като множеството от точки*

$$V(I) = \{(a_1,\dots,a_n) \in k^n \mid f(a_1,\dots,a_n) = 0 \ \text{ за } \forall f \in I\}.$$

ТВЪРДЕНИЕ 8.7. *Многообразието* $V(I)$ *на идеал* $I \triangleleft k[x_1,\dots,x_n]$ *е афинно многообразие.*
В частност, ако $I = \langle f_1,\dots,f_s\rangle$, *то* $V(I) = V(f_1,\dots,f_s)$.

Доказателство: Съгласно Теоремата на Хилберт за базиса 3, съществуват полиноми $f_1,\dots,f_s \in k[x_1,\dots,x_n]$, които пораждат $I = \langle f_1,\dots,f_s\rangle$. Твърдим, че $V(I) = V(f_1,\dots,f_s)$. От една страна, $f_i \in I$ гарантира, че $f_i(a_1,\dots,a_n) = 0$ във всяка точка $(a_1,\dots,a_n) \in V(I)$. Следователно $(a_1,\dots,a_n) \in V(f_1,\dots,f_s)$ или $V(I) \subseteq V(f_1,\dots,f_s)$. От друга страна, ако $(a_1,\dots,a_n) \in V(f_1,\dots,f_s)$ и $f \in I = \langle f_1,\dots,f_s\rangle$, то $f = \sum_{i=1}^{s} f_i h_i$ за някакви полиноми $h_1,\dots,h_s \in k[x_1,\dots,x_n]$. В резултат,

$$f(a_1,\dots,a_n) = \sum_{i=1}^{s} f_i(a_1,\dots,a_n) h_i(a_1,\dots,a_n) = \sum_{i=1}^{s} 0 h_i(a_1,\dots,a_s) = 0$$

и $(a_1,\dots,a_n) \in V(I)$, т.е. $V(f_1,\dots,f_s) \subseteq V(I)$. Това доказва $V(I) = V(f_1,\dots,f_s)$, Q.E.D.
Последното твърдение установява, че всяко афинно многообразие се определя от своя идеал.
Твърдение 8.7 дава непосредствено следното следствие, което вече използвахме при рационалната параметризация на афинни многообразие.

СЛЕДСТВИЕ 8.8. *Ако* $\{V_\alpha\}_{\alpha \in A}$ *е произволна (евентуално безкрайна) фамилия от афинни алгебрични многообразия* $V_\alpha = V(f_{\alpha,1},\dots,f_{\alpha,m_\alpha}) \subset k^n$, *то сечението* $\cap_{\alpha \in A} V_\alpha$ *е афинно алгебрично многообразие в* k^n.

Доказателство: Съгласно Задача 3.17, множеството

$$I\left(\cap_{\alpha \in A} V_\alpha\right) = \{f \in k[x_1,\dots,x_n] \mid f(a_1,\dots,a_n) = 0 \ \text{ за } \forall (a_1,\dots,a_n) \in \cap_{\alpha \in A} V_\alpha\}$$

е идеал в полиномиалния пръстен $k[x_1,\dots,x_n]$. По Теоремата на Хилберт за базиса 3, съществуват краен брой пораждащи $g_1 \dots, g_t \in k[x_1,\dots,x_n]$ на идеала $I\left(\cap_{\alpha \in A} V_\alpha\right) = \langle g_1,\dots,g_t\rangle$. Прилагайки Твърдение 8.7, оттук получаваме, че $VI\left(\cap_{\alpha \in A} V_\alpha\right) = V(g_1,\dots,g_t)$ е афинно алгебрично многообразие в k^n.
Остава да установим, че $\cap_{\alpha \in A} V_\alpha = VI\left(\cap_{\alpha \in A} V_\alpha\right)$. Наистина, нека $(a_1,\dots,a_n) \in VI\left(\cap_{\alpha \in A} V[\alpha\right)$. Ако допуснем, че $(a_1,\dots,a_n) \notin V_{\alpha_o} = V(f_{\alpha_o,1},\dots,f_{\alpha_o,m_{\alpha_o}})$ за

някое $\alpha_o \in A$, то съществува $1 \leq i \leq m_{\alpha_o}$, така че $f_{\alpha_o,i}(a_1,\dots,a_n) \neq 0$. Но съгласно $\cap_{\alpha\in A} V_\alpha \subseteq V_{\alpha_o}$ имаме $f_{\alpha_o,i} \in I(V_{\alpha_o}) \subseteq I\left(\cap_{\alpha\in A} V_\alpha\right)$, откъдето получаваме $f_{\alpha_o,i}(a_1,\dots,a_n) = 0$. Противоречието доказва, че $VI\left(\cap_{\alpha\in A} V_\alpha\right) \subseteq \cap_{\alpha\in A} V_\alpha$. Обратно, ако $(a_1,\dots,a_n) \in \cap_{\alpha\in A} V_\alpha$, то за произволен полином $f \in I\left(\cap_{\alpha\in A} V_\alpha\right)$ е изпълнено $f(a_1,\dots,a_n) = 0$. Следователно $(a_1,\dots,a_n) \in VI\left(\cap_{\alpha\in A} V_\alpha\right)$, откъдето $\cap_{\alpha\in A} V_\alpha \subseteq VI\left(\cap_{\alpha\in A} V_\alpha\right)$ и $\cap_{\alpha\in A} V_\alpha = VI\left(\cap_{\alpha\in A} V_\alpha\right)$, Q.E.D.

Задачи

Задача 8.9. *Нека $I = \langle g_1, g_2, g_3\rangle$ е идеалът в $\mathbb{R}[x,y,z]$, породен от полиномите $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$, $g_3 = x - yz^4$. Да се намери полином $g \in I$, така че $LT(g) \notin \langle LT(g_1), LT(g_2), LT(g_3)\rangle$ относно лексикографската наредба.*

Задача 8.10. *За идеалите $I = \langle f_1, f_2\rangle \lhd k[x,y]$ и $J = \langle g_1, g_2\rangle \lhd k[x,y]$, породени от полиномите $f_1 = x^2y - z$, $f_2 = xy - 1$, $g_1 = 2xy^2 - x$, $g_2 = 3x^2y - y - 1$, да се докаже, че идеалът на старшите членове $\langle LT(I)\rangle$ съдържа строго $\langle LT(f_1), LT(f_2)\rangle$ и идеалът на старшите членове $\langle LT(J)\rangle$ съдържа строго $\langle LT(g_1, LT(g_2)\rangle$ относно градуирано лексикографската наредба.*

Упътване: Намерете полином $f \in I = \langle f_1, f_2\rangle$, чийто старши член $LT(f)$ не се дели на $LT(f_1)$ и на $LT(f_2)$.

Задача 8.11. *Нека $I = \langle f_1, f_2, f_3\rangle$ е идеалът в $\mathbb{R}[x,y,z]$, породен от полиномите $f_1 = x^4y^2 - z$, $f_2 = x^3y^3 - 1$, $f_3 = x^2y^4 - 2z$. Да се докаже, че идеалът $\langle LT(I)\rangle$ на старшите членове съдържа строго $\langle LT(f_1), LT(f_3), LT(f_3)\rangle$ относно градуирано лексикографската наредба.*

Задача 8.12. *Да се докаже, че ако идеалът $\langle LT(I)\rangle$ на старшите членове на идеала $I = \langle f_1,\dots,f_s\rangle$ в полиномиалния пръстен $k[x_1,\dots,x_n]$ съдържа строго $\langle LT(f_1),\dots,LT(f_s)\rangle$, то съществува полином $f \in I$ с ненулев остатък при деление с $f_1,\dots,f_s$.*

Задача 8.13. *Да се докаже, че ако k е безкрайно поле, то полиномите $x - z^2, y - z^3 \in k[x,y,z]$ образуват базис на Грьобнер на идеала $I = \langle x - z^2, y - z^3\rangle$ в относно лексикографската наредба.*

Задача 8.14. *За произволни естествени $m \leq n$ нека $f_i = \sum_{j=i}^n a_{ij}x_j \in k[x_1,\dots,x_n]$ са линейни полиноми с $a_{ii} \neq 0$, $1 \leq i \leq m$. Да се докаже, че $f_1,\dots,f_m$ е базис на Грьобнер на идеала $I = \langle f_1,\dots,f_m\rangle$ относно лексикографската наредба.*

Задача 8.15. *Да се докаже, че следните две условия са еквивалентни в комутативния пръстен с единица R :*
(i) всеки идеал $I \lhd R$ е крайнопороден;
(ii) всяка ненамаляваща редица $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ от идеали в R се стабилизира след краен брой стъпки, т.е. $I_N = I_{N+1} = I_{N+2} = \dots$ за някое естествено N.

Задача 8.16. *Да се докаже, че всяка намаляваща редица $V_1 \supseteq V_2 \supseteq V_3 \supseteq \dots$ от афинни многообразия се стабилизира след краен брой стъпки, т.е. съществува естествено число N, така че $V_N = V_{N+1} = V_{N+2} = \dots$.*

Задача 8.17. *Нека V е афинно многообразие в k^n, $I(V)$ е идеалът на V в $k[x_1,\dots,x_n]$, а $V(I(V))$ е многообразието на идеала $I(V)$. Да се докаже, че $V(I(V)) = V$.*

Упътване: Проверете, че $V \subseteq V(I(V))$. Ако $V = V(f_1,\dots,f_s)$ и $I(V) = \langle g_1,\dots,g_t\rangle$, то от $\langle f_1,\dots,f_s\rangle \subseteq \langle g_1,\dots,g_t\rangle$ изведете включването $V \supseteq V(I(V))$.

Задача 8.18. *За произволни полиноми $f, g, h \in k[x_1,\dots,x_n]$ да се докаже, че*

$$V(f, gh) = V(f,g) \cup V(f,h).$$