Глава 9

Въпрос 9: Характеризация на базисите на Грьобнер. S-полиноми.

Във въпрос 8 доказахме, че всеки ненулев идеал $I \lhd k[x_1, \ldots, x_n]$ има базис на Грьобнер относно фиксирана мономна наредба, който поражда I като идеал. Сега ще разгледаме критерий за това кога една крайна система пораждащи $g_1, \ldots, g_t$ на ненулев идеал $I \lhd k[x_1, \ldots, x_n]$ е базис на Грьобнер на I. За тази цел започваме с изучаване на свойствата на делението с базис на Грьобнер.

Твърдение 9.1. *Ако $g_1, \ldots, g_t$ е базис на Грьобнер на ненулев идеал I в полиномиалния пръстен $k[x_1, \ldots, x_n]$, то за всеки полином $f \in k[x_1, \ldots, x_n]$ съществува единствен полином $r \in k[x_1, \ldots, x_n]$, чиито мономи не се делят на нито един от старшите членове $LT(g_1), \ldots, LT(g_t)$ и разликата $f - r \in I$.*

Доказателство: Чрез деление на f с $g_1, \ldots, g_t$ получаваме представяне $f = g_1h_1 + \ldots + g_th_t + r$ чрез някакви полиноми $h_1, \ldots, h_t, r \in k[x_1, \ldots, x_n]$, така че нито един моном на r не се дели на $LT(g_1), \ldots, LT(g_t)$ и $f - r = g_1h_1 + \ldots + g_th_t \in I$. Това доказва съществуването на полинома $r \in k[x_1, \ldots, x_n]$ с необходимите свойства.
Да предположим, че $f = f_1 + r_1 = f_2 + r_2$ за $f_1, f_2 \in I$ и $r_1, r_2 \in k[x_1, \ldots, x_n]$ без мономи, делящи се на някое $LT(g_i)$, $1 \leq i \leq t$. Ако полиномът $r_2 - r_1 = f_1 - f_2 \in I$ е ненулев, то $LT(r_2 - r_1) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ и съгласно Лема 7.2, старшият моном $LT(r_2 - r_1)$ се дели на някое $LT(g_i)$. Това противоречи на избора на r_1 и r_2 без мономи, делящи се на $LT(g_1), \ldots, LT(g_t)$ и доказва тъждественото съвпадение $r_2 = r_1$ като полиноми, Q.E.D.
Съгласно горното твърдение, остатъкът при делението на полином f с базис на Грьобнер $g_1, \ldots, g_t$ на идеал не зависи от реда на елементите на този базис. При пермутация на $g_1, \ldots, g_t$ частните $a_1, \ldots, a_t$ от представянето $f = a_1g_1 + \ldots + a_tg_t + r$ могат да се променят.
Непосредствено получаваме следното:

Следствие 9.2. *Нека $f \in k[x_1, \ldots, x_n]$ е полином, а $g_1, \ldots, g_t$ е базис на Грьобнер на идеал $I \lhd k[x_1, \ldots, x_n]$. В такъв случай, полиномът $f \in I$ тогава и само тогава, когато f има нулев остатък при деление с $g_1, \ldots, g_t$.*

Определение 9.3. *Ако $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ са полиноми на $x_1, \ldots, x_n$ с коефициенти от поле k, то остатъкът на f при деление с наредената s-торка $F = (f_1, \ldots, f_s)$ ще бележим с*

$$\overline{f}^F.$$

Съгласно Твърдение 9.1, ако F е базис на Грьобнер на идеала $\langle F \rangle$, то наредбата на елементите на F не е от значение при пресмятане на $\overline{f}^F$.

Пример 9.4. *Ако $F = (x^2y - y^2, x^4y^2 - y^2) \subset k[x, y]$, то относно лексикографската наредба*

$$\overline{x^5y}^F = xy^3,$$

защото при деление на x^5y *с* F *получаваме*

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0(x^4y^2 - y^2) + xy^3.$$

ОПРЕДЕЛЕНИЕ 9.5. *Най-малкото общо кратно на мономи* $x^\alpha, x^\beta \in k[x_1, \ldots, x_n]$ *е мономът* $LCM(x^\alpha, x^\beta) = x^\gamma$ *с* $\gamma_i := \max(\alpha_i, \beta_i)$ *за всички* $1 \leq i \leq n$.

Непосредствено се вижда, че мономите x^α, x^β делят $LCM(x^\alpha, x^\beta) = x^\gamma$ и ако x^δ се дели както на x^α, така и на x^β, то x^δ се дели на x^γ. За да проверим гореспоменатото свойство на най-малкото общо кратно на мономи, което е аналогично на определението за най-малко общо кратно на цели числа, да отбележим, че мономът $x^\lambda = x_1^{\lambda_1} \ldots x_n^{\lambda_n}$ дели монома $x^\mu = x_1^{\mu_1} \ldots x_n^{\mu_n}$ тогава и само тогава, когато $\mu_i \geq \lambda_i$ за $\forall 1 \leq i \leq n$, така че частното $\frac{x^\mu}{x^\lambda}$ е моном на $x_1, \ldots, x_n$. По този начин, от $\alpha_i \leq \max(\alpha_i, \beta_i) = \gamma_i$ и $\beta_i \leq \max(\alpha_i, \beta_i) = \gamma_i$ за всички $1 \leq i \leq n$ получаваме, че x^α и x^β делят x^γ. Ако x^α и x^β делят x^δ, то $\delta_i \geq \alpha_i$ и $\delta_i \geq \beta_i$ за всички $1 \leq i \leq n$, така че $\delta_i \geq \max(\alpha_i, \beta_i) = \gamma_i$ и x^γ дели x^δ.

ОПРЕДЕЛЕНИЕ 9.6. *Нека* f *и* g *са ненулеви полиноми от* $k[x_1, \ldots, x_n]$, *а* $x^\gamma = LCM(LM(f), LM(g))$. *Тогава*

$$S(f, g) := \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g$$

се нарича S*-полином на* f *и* g.

Старшите членове $LT(f) = LC(f)LM(f)$ и $LT(g) = LC(g)LM(g)$ делят $x^\gamma = LCM(LM(f), LM(g))$, така че $S(f, g) \in k[x_1, \ldots, x_n]$ е полином на $x_1, \ldots, x_n$. Например, за $f = x^3y^2 - x^2y^3 + x, g = 3x^4y + y^2 \in \mathbb{R}[x, y]$ и градуирано лексикографската наредба имаме

$$LCM(LM(f), LM(g)) = LCM(x^3y^2, x^4y) = x^4y^2,$$

$$S(f, g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = xf - \frac{1}{3}yg = -x^3y^3 + x^2 - \frac{1}{3}y^2,$$

За произволни ненулеви полиноми $f, g \in k[x_1, \ldots, x_n]$ с $LCM(LM(f), LM(g)) = x^\gamma$ да отбележим, че старшите членове

$$LT\left(\frac{x^\gamma}{LT(f)} f\right) = LT\left(\frac{x^\gamma}{LT(f)}\right) LT(f) = LC(f)^{-1} \frac{x^\gamma}{LM(f)} LC(f)LM(f) = x^\gamma$$

и

$$LT\left(\frac{x^\gamma}{LT(g)} g\right) = LT\left(\frac{x^\gamma}{LT(g)}\right) LT(g) = LC(g)^{-1} \frac{x^\gamma}{LM(g)} LC(g)LM(g) = x^\gamma$$

съвпадат с най-малкото общо кратно на съответните старши мономи. Тези старши членове се унищожават в $S(f, g)$ и $LM(S(f, g)) < x^\gamma$. Следващата лема установява, че всяко унищожаване на старши членове на полиноми с един и същи старши моном възниква по този начин.

ЛЕМА 9.7. *Да разгледаме полинома* $g = \sum_{i=1}^t c_i x^{\alpha(i)} g_i$, *където* $c_1, \ldots, c_t$ *са от полето* k, $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ *и* $LM(x^\alpha(i)g_i) = x^\delta$ *за всички* $1 \leq i \leq t$ *с* $c_i \neq 0$. *Ако* $LM(g) < x^\delta$, *то съществуват* $a_1, \ldots, a_{t-1} \in k$, *така че*

$$g = \sum_{i=1}^{t-1} a_i x^{\delta - \gamma(i,i+1)} S(g_i, g_{i+1}),$$

където $x^{\gamma(i,i+1)} = LCM(LM(g_i), LM(g_{i+1}))$ *и* $LM(x^{\delta-\gamma(i,i+1)} S(g_i, g_{i+1})) < x^\delta$.

Доказателство: Нека $LM(g_i) = x^{\beta(i)}$, $LC(g_i) = d_i \in k$, така че $LT(g_i) = d_i x^{\beta(i)}$ за всички $1 \leq i \leq t$. По предположение, $x^{\alpha(i)+\beta(i)} = x^\delta$, така че $x^{\beta(i)}$ дели x^δ. За всяко $1 \leq j \leq n$ степенният показател $\gamma(i,i+1)_j = \max(\beta(i)_j, \beta(i+1)_j)$ на x_j в $x^{\gamma(i,i+1)} = LCM(LM(g_i), LM(g_{i+1})) = LCM(x^{\beta(i)}, x^{\beta(i+1)})$ не надминава степенния показател δ_j на x_j в x^δ, така че $x^{\gamma(i,i+1)}$ дели x^δ. Следователно $x^{\delta-\gamma(i,i+1)}$ са мономи на $x_1, \ldots, x_n$ и

$$x^{\delta-\gamma(i,i+1)} S(g_i, g_{i+1}) = x^{\delta-\gamma(i,i+1)} \left(\frac{x^{\gamma(i,i+1)}}{LT(g_i)} g_i - \frac{x^{\gamma(i,i+1)}}{LT(g_{i+1})} g_{i+1} \right) =$$

$$\frac{x^\delta}{d_i x^{\beta(i)}} g_i - \frac{x^\delta}{d_{i+1} x^{\beta(i+1)}} g_{i+1} = \frac{x^{\alpha(i)} g_i}{d_i} - \frac{x^{\alpha(i+1)} g_{i+1}}{d_{i+1}}.$$

Полиномите

$$p_i := \frac{x^{\alpha(i)} g_i}{d_i} \in k[x_1, \ldots, x_n]$$

имат старши моном $LM(p_i) = x^\delta$ със старши коефициент $LC(p_i) = 1$ спрямо фиксираната мономна наредба. Оттук, $x^{\delta-\gamma(i,i+1)} S(g_i, g_{i+1}) = p_i - p_{i+1}$ е полином на $x_1, \ldots, x_n$ с коефициенти от полето k и $LM\left(x^{\delta-\gamma(i,i+1)} S(g_i, g_{i+1})\right) = LM(p_i - p_{i+1}) < x^\delta$. Непосредствено се вижда, че $g = \sum_{i=1}^t c_i x^{\alpha(i)} g_i = \sum_{i=1}^t c_i d_i p_i$ е k-линейна комбинация на $p_1, \ldots, p_t$ с коефициенти $c_1 d_1, \ldots, c_t d_t$. Трябва да установим съществуването на $a_1, \ldots, a_{t-1} \in k$, така че

$$\sum_{i=1}^{t-1} a_i (p_i - p_{i+1}) = \sum_{i=1}^{t-1} a_i p_i - \sum_{i=1}^{t-1} a_i p_{i+1} = \sum_{i=1}^{t-1} a_i p_i - \sum_{j=2}^{t} a_{j-1} p_j =$$

$$a_1 p_1 + \sum_{i=2}^{t-1} (a_i - a_{i-1}) p_i - a_{t-1} p_t = \sum_{i=1}^{t} c_i d_i p_i = g.$$

Полагаме $a_1 := c_1 d_1$ и $a_i := a_{i-1} + c_i d_i$ за всички $2 \leq i \leq t-1$. Достатъчно е да проверим, че $-a_{t-1} = c_t d_t$ при този избор. С индукция по $2 \leq i \leq t-1$ доказваме, че $a_i = \sum_{j=1}^i c_j d_j$. От друга страна, старшите членове $LT c_i x^{\alpha(i)} g_i) = c_i d_i x^{\alpha(i)+\beta(i)} = c_i d_i x^\delta$ се унищожават в съгласно предположението $LT(g) = LT\left(\sum_{i=1}^t c_i x^{\alpha(i)} g_i\right) < x^\delta$. С други думи, $\sum_{i=1}^t c_i d_i = 0$ или $a_t = a_{t-1} + c_t d_t = 0$. Това дава $-a_{t-1} = c_t d_t$ и гарантира верността на равенството $\sum_{i=1}^{t-1} a_i (p_i - p_{i+1}) = g$ за избраните коефициенти $a_1, \ldots, a_{t-1}, a_t = 0$ от полето k, Q.E.D.

Теорема 5. *Системата пораждащи $g_1, \ldots, g_t$ на идеала $I = \langle g_1, \ldots, g_t \rangle$ в полиномиалния пръстен $k[x_1, \ldots, x_n]$ е базис на Грьобнер на I тогава и само тогава, когато за произволни $1 \leq i \neq j \leq t$ остатъкът при деление на $S(g_i, g_j)$ с $g_1, \ldots, g_t$, е нулев.*

Доказателство: Ако $g_1, \ldots, g_t$ е базис на Грьобнер на $I = \langle g_1, \ldots, g_t \rangle$, то $S(g_i, g_j) \in \langle g_i, g_j \rangle \subseteq \langle g_1, \ldots, g_t \rangle = I$. Съгласно Следствие 9.2 това е достатъчно за анулиране на остатъка на $S(g_i, g_j)$ при деление с $g_1, \ldots, g_t$.

Обратно, нека $\overline{S(g_i, g_j)}^G = 0$ за $\forall 1 \leq i < j \leq t$ и $G = \{g_1, \ldots, g_t\}$. Трябва да докажем, че всеки ненулев полином $0 \neq f \in I = \langle g_1, \ldots, g_t \rangle$ има старши член $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$. С други думи, $LT(f)$ се дели на някой от мономите $LT(g_i)$. По определение, $f \in I$ означава съществуване на полиноми $h_1, \ldots, h_t \in k[x_1, \ldots, x_n]$, така че $f = \sum_{i=1}^t h_i g_i$. Старшият член на сума може да се оцени отгоре с максимума на старшите членове на събираемите,

$$LT(f) \leq \max(LT(h_1 g_1), \ldots, LT(h_t g_t)).$$

За всички представяния на фиксирания полином $0 \neq f \in I = \langle g_1, \ldots, g_t \rangle$ във вида $f = \sum_{i=1}^{t} h_i g_i$ разглеждаме множеството на мономите

$$\max(LT(h_1 g_1), \ldots, LT(h_t g_t)).$$

Благодарение на артиновостта на фиксираната мономна наредба, това множество има минимален елемент $x^\delta = \max(LM(h_1 g_1), \ldots, LM(h_t g_t))$, отговарящ на представяне $f = \sum_{i=1}^{t} h_i g_i \in \langle g_1, \ldots, g_t \rangle = I$. Ако $LM(f) = x^\delta$, то съществува $1 \leq i \leq t$, така че $LM(f) = x^\delta = LM(h_i g_i) = LM(h_i) LM(g_i)$ и $LT(g_i)$ дели $LT(f)$, което доказва теоремата. Да предположим, че

$$LM(f) < x^\delta = \max(LM(h_1 g_1), \ldots, LM(h_t g_t))$$

и да представим

$$f = \sum_{LM(h_i g_i) = x^\delta} h_i g_i + \sum_{LM(h_i g_i) < x^\delta} h_i g_i =$$

$$\sum_{LM(h_i g_i) = x^\delta} LT(h_i) g_i + \sum_{LM(h_i g_i) = x^\delta} (h_i - LT(h_i)) g_i + \sum_{LM(h_i g_i) < x^\delta} h_i g_i.$$

Всеки моном на

$$f_1 := \sum_{LM(h_i g_i) = x^\delta} (h_i - LT(h_i)) g_i + \sum_{LM(h_i g_i) < x^\delta} h_i g_i$$

е по-малък от x^δ, така че $LM(f) < x^\delta$ изисква унищожаване на мономите, подобни на x^δ в

$$f_0 := \sum_{LM(h_i g_i) = x^\delta} LT(h_i) g_i.$$

По-точно, ако $LT(h_i) = a_i x^{\alpha(i)}$, то $LM(x^{\alpha(i)} g_i) = LM(h_i g_i) = x^\delta$ и $LM(f_0) < x^\delta$ позволява прилагането на Лема 9.7. По този начин получаваме представяне

$$f_0 = \sum_{i,j} c_{ij} x^{\delta - \gamma(i,j)} S(g_i, g_j),$$

където $c_{ij} \in k$, $x^{\gamma(i,j)} = LCM(LM(g_i), LM(g_j))$ и $LM(x^{\delta - \gamma(i,j)} S(g_i, g_j)) < x^\delta$. По предположение, $\overline{S(g_i, g_j)}^{\{g_1, \ldots, g_t\}} = 0$, така че при деление на $S(g_i, g_j)$ с $g_1, \ldots, g_t$ съществуват частни $f_{ijm} \in k[x_1, \ldots, x_n]$, за които

$$S(g_i, g_j) = \sum_{m=1}^{t} f_{ijm} g_m.$$

Съгласно алгоритъма за деление на полиноми на няколко променливи,

$$LM(S(g_i, g_j) \geq LM(f_{ijm} g_m).$$

Следователно $F_{ijm} := x^{\delta - \gamma(i,j)} f_{ijm}$ имат

$$LM(F_{ijm} g_m) \leq LM(x^{\delta - \gamma(i,j)} S(g_i, g_j)) < x^\delta.$$

По този начин

$$f_0 = \sum_{m=1}^{t} \left(\sum_{i,j} c_{ij} F_{ijm} \right) g_m = \sum_{m=1}^{t} h'_m g_m$$

за $h'_m := \sum_{i,j} c_{ij} F_{ijm}$ с $LM(h'_m g_m) < x^\delta$. Вземайки предвид, че и

$$f_1 = \sum_{l=1}^{t} h''_l g_l$$

за $h_l'' \in k[x_1, \ldots, x_n]$ с $LM(h_l'' g_l) < x^\delta$, получаваме представяне

$$f = \sum_{i=1}^{t} (h_i' + h_i'') g_i = \sum_{i=1}^{t} \widetilde{h_i} g_i,$$

където $\widetilde{h_i} := h_i' + h_i''$ имат $LM(\widetilde{h_i} g_i) < x^\delta$. В резултат,

$$\max(LM(\widetilde{h_1} g_1), \ldots, \widetilde{h_t} g_t)) < x^\delta,$$

което противоречи на минималността на x^δ и доказва теоремата, Q.E.D.
Теорема 5 предоставя алгоритъм за установяване на това дали дадена крайна система пораждащи на полиномиален идеал е негов базис на Грьобнер. Например, полиномите $y - x^2, z - x^3 \in \mathbb{R}[x, y, z]$ образуват базис на Грьобнер на идеала $I = \langle y - x^2, z - x^3 \rangle$ на усуканата кубика в $\mathbb{R}^3$ относно лексикографската наредба с $y > z > x$. За целта е достатъчно да пресметнем, че

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3$$

и при деление на $-zx^2 + yx^3$ с $y - x^2, z - x^3$ се получава нулев остатък

$$-zx^2 + yx^3 = x^3(y - x^2) + (-x^2)(z - x^3) + 0.$$

Задачи

Задача 9.8. *Да се докаже, че полиномите $x + z, y - z \in \mathbb{R}[x, y, z]$ образуват базис на Грьобнер на идеала $I = \langle x + z, y - z \rangle$ относно лексикографската наредба. Да се раздели xy на $x + z, y - z$ и на $y - z, x + z$, за да се илюстрира единствеността на остатъка и неединствеността на частните при деление с пермутация на базис на Грьобнер.*

Задача 9.9. *НекаI е идеал в пръстена на полиномите $k[x_1, \ldots, x_n]$, $a >$ е мономна наредба в $k[x_1, \ldots, x_n]$. Да се докаже, че всеки полином $f \in k[x_1, \ldots, x_n]$ може да се представи във вида $f = g + r$, където $g \in I$ и нито един моном на r не се дели на елемент от $LT(I)$. При това, за всеки две представяния $f = g + r = g' + r'$ е в сила $r = r'$.*

Задача 9.10. *Нека $f_1, \ldots, f_s$ и $g_1, \ldots, g_t$ са два базиса на Грьобнер на един и същи ненулев идеал $I \lhd k[x_1, \ldots, x_n]$ относно една и съща мономна наредба. Да се докаже, че f има един и същи остатък при деление с $f_1, \ldots, f_s$ и $g_1, \ldots, g_t$.*

Задача 9.11. *Нека $I \lhd k[x_1, \ldots, x_n]$ е ненулев полиномиален идеал с базис на Грьобнер $G = \{g_1, \ldots, g_t\}$ относно някаква мономна наредба. За произволни полиноми $f, g \in k[x_1, \ldots, x_n]$ да се докаже, че:*
(i) $\overline{f}^G = \overline{g}^G$ *тогава и само тогава, когато* $f - g \in I$;
(ii) $\overline{f + g}^G = \overline{f}^G + \overline{g}^G$;
(iii) $\overline{fg}^G = \overline{\overline{f}^G \overline{g}^G}^G$.

Задача 9.12. *Да се пресметне $S(f, g)$ относно лексикографската наредба за полиномите:*
(i) $f = 4x^2z - 7y^2, \quad g = xyz^2 + 3xz^4$;
(ii) $f = x^4y - z^2, \quad g = 3xz^2 - y$;
(iii) $f = x^7y^2z + 2ixyz, \quad g = 2x^7y^2z + 4$;
(iv) $f = xy + z^3, \quad g = z^2 - 3z$.

Задача 9.13. *Да се докаже, че $y - x^2, z - x^3$ не е базис на Грьобнер на идеала $I = \langle y - x^2, z - x^3 \rangle$ на усуканата кубика в $\mathbb{R}^3$ относно лексикографската наредба с $x > y > z$.*

Задача 9.14. *Използвайки Теорема 5 определете дали следните множества G са базиси на Грьобнер на идеала, който пораждат:*
(i) $G = \{x^2 - y, x^3 - z\}$ *относно градуирано лексикографската наредба* $>_{\text{grlex}}$;
(ii) $G = \{xy^2 - xz + y, xy - z^2, x - yz^4\}$ *относно лексикографската наредба* $>_{\text{lex}}$.

Задача 9.15. *За произволни полиноми* $f, g \in k[x_1, \ldots, x_n]$ *и мономи* x^α, x^β *на* $x_1, \ldots, x_n$ *да се докаже, че*

$$S(x^\alpha f, x^\beta g) = \frac{LCM(x^\alpha LM(f), x^\beta LM(g))}{LCM(LM(f), LM(g))} S(f, g).$$