Глава 6

# Въпрос 6: Алгоритъм за деление на полиноми на няколко променливи

Преди да изложим алгоритъма за деление на полиноми на няколко променливи, да напомним

Твърдение 6.1. (Алгоритъм за деление на полиноми на една променлива) *Нека $k$ е поле, а $g(x) \in k[x]$ е неконстантен полином. Тогава за всеки полином $f(x) \in k[x]$ съществуват еднозначно определени полиноми $q(x), r(x) \in k[x]$, така че*

$$f(x) = q(x)g(x) + r(x)$$

*и $\deg(r) < \deg(g)$ или $r(x) \equiv 0$ е тъждествено нулевият полином.*

**Доказателстово:** Псевдокод е език за описание на алгоритми. Ето алгоритъм за намиране на полиномите $q(x)$ и $r(x)$, записан в псевдокод:

Input: $g, f$
Output: $q, r$
$q := 0; r := f$
WHILE $r \neq 0$ AND $LT(g)$ DIVIDES $LT(r)$ DO

$$q := q + \frac{LT(z)}{LT(g)}$$

$$r := r - \frac{LT(r)}{LT(g)}g$$

Тук старшите членове $LT(g)$ и $LT(r)$ са пресметнати относно лексикографската наредба в $k[x]$.
Първо ще докажем, че изпълнението на посочения алгоритъм спира след краен брой стъпки. За целта да отбележим, че степента $\deg\left(r - \frac{LT(r)}{LT(g)}g\right) < \deg(r)$ намалява строго на всяка стъпка. Еквивалентно, твърдим, че

$$LT\left(r - \frac{LT(r)}{LT(g)}g\right) <_{\text{lex}} LT(r),$$

докато $LT(g) \leq_{\text{lex}} LT(r)$. Наистина, съгласно Лемата за старшия едночлен

$$LT\left(\frac{LT(r)}{LT(g)}g\right) = LT\left(\frac{LT(r)}{LT(g)}\right)LT(g) = \frac{LT(r)}{LT(g)}LT(g) = LT(r),$$

така че $LT(r)$ се унищожава в $r - \frac{LT(r)}{LT(g)}g$ и $LT\left(r - \frac{LT(r)}{LT(g)}g\right) < LT(r)$. След краен брой стъпки, намаляващи строго $\deg(r)$ се достига до $\deg(r) < \deg(g)$ и алгоритъмът спира.
Сега ще установим, че получените от алгоритъма полиноми $q(x)$ и $r(x)$ изпълняват обявените за тях свойства. Равенството $f = qg + r$ е изпълнено за началните стойности $q := 0$ и $r := f$. Освен това, ако на някоя стъпка от алгоритъма е изпълнено $f = qg + r$ и $LT(g)$ дели $LT(r)$, то на следващата стъпка

имаме

$$\left(q + \frac{LT(r)}{LT(g)}\right) g + \left(r - \frac{LT(r)}{LT(g)} g\right) = qg + r = f.$$

При това, алгоритъмът спира точно когато $r \equiv 0$ или $LT(g)$ не дели $LT(r)$. По този начин, полученият в края остатък $r(x) \in k[x]$ е или тъждествено нулевият полином или $\deg(r) < \deg(g)$. Следователно изходните полиноми $q(x), r(x) \in k[x]$ имат обявените за тях свойства.

Накрая ще проверим единствеността на $q$ и $r$. Наистина, нека $f = qg + r = q'g + r'$ за $q, r, q', r' \in k[x]$, $\deg(r) < \deg(g)$ или $r(x) = 0$, $\deg(r') < \deg(g)$ или $r'(x) = 0$. Ако предположим, че $r' - r \neq 0$ не е тъждествено нулевият полином, то от $(q-q')g = r'-r$ следва, че и $q-q' \neq 0$ не е тъждествено нулевият полином и съгласно Лема **??** получаваме, че

$$\deg(r' - r) = \deg(q - q') + \deg(g) \geq \deg(g).$$

От друга страна, $\deg(r) < \deg(g)$ и $\deg(r') < \deg(g)$ за $r' - r \neq 0$ дават $\deg(r' - r) < \deg(g)$, което е противоречие, доказващо $r'(x) = r(x)$. Сега от $(q-q')g = 0$ и $g \neq 0$ следва $q = q'$, Q.E.D.

Преди да изложим алгоритъма за деление на полиноми на няколко променливи да обърнем внимание на следната

Лема 6.2. *Ако $g(x) \in k[x]$ е неконстантен полином, а $r(x) \in k[x]$ е ненулев полином, то $\deg(r) < \deg(g)$ тогава и само тогава, когато нито един моном на $r(x)$ (с ненулев коефициент) не се дели на старшия член $LT(g)$ на $g$ относно лексикографската наредба.*

**Доказателство:** Мономът $x^p$, $p \in \mathbb{N} \cup \{0\}$ на една променлива $x$ дели монома $x^q$, $q \in \mathbb{N} \cup \{0\}$ на същата променлива $x$ точно когато $p \leq q$, така че частното $\frac{x^q}{x^p} = x^{q-p}$ е моном, изпълняващ равенството $x^q = x^p x^{q-p}$. С други думи, $x^p$ не дели $x^q$ при $p > q$. В случая, старшият член $LT(g) = a_n x^n$ на $g(x) = \sum_{i=0}^{n} a_i x^i$ не дели нито един моном $b_j x^j \not\equiv 0$ на $r(x) = \sum_{j=0}^{m} b_j x^j$ тогава и само тогава, когато $n > j$ за всички $0 \leq j \leq m$ с $b_j \neq 0$. Последното е еквивалентно на $\deg(g) = n > m = \deg(r)$, Q.E.D.

Пример 6.3. Ако искаме да разделим $f = xy^2 + 1$ на $f_1 = xy + 1$ и $f_2 = y + 1$, използвайки лексикографската наредба $>_{\text{lex}}$, започваме с деление на старшия член $LT(f) = xy^2$ със старшия член $LT(f_1) = xy$ на първия от изброените делители. Частното $a_1 = \frac{LT(f)}{LT(f_1)} = y$ се умножава с $f_1$ и заменяме $f$ с $f - yf_1 = 1 - y$. Този път $LT(f - yf_1) = -y$ не се дели на $LT(f_1) = xy$, но се дели на $LT(f_2) = y$ с частно $a_2 = \frac{LT(f-yf_1)}{LT(f_2)} = -1$. По-нататък, $LT(f - yf_1 + f_2) = LT(2) = 2$ не се дели нито на $LT(f_1) = xy$, нито на $LT(f_2) = y$. Следователно $r = f - yf_1 + f_2 = 2$ е остатък и

$$f = yf_1 - f_2 + 2 = a_1 f_1 + a_2 f_2 + r.$$

Пример 6.4. При деление на $f = x^2y + xy^2 + y^2$ с $f_1 = xy - 1$ и $f_2 = y^2 - 1$ относно лексикографската наредба, старшият член $LT(f) = x^2y$ се дели на $LT(f_1) = xy$ с частно $x$ и $f - xf_1 = xy^2 + x + y^2$. По-нататък, $LT(f - xf_1) = xy^2$ продължава да се дели на $LT(f_1) = xy$. Този път частното е $y$ и $f - xf_1 - yf_1 = x + y^2 + y$. Сега $LT(f - (x+y)f_1) = x$ не се дели нито на $LT(f_1) = xy$, нито на $LT(f_2) = y^2$, но $f - (x+y)f_1$ има моном $y^2$, който се дели на $LT(f_2)$ с частно 1. Това може да се случи само при деление на полиноми на повече от една променлива. Отделяме частичен остатък $r_1 = x$. Тогава $f - (x + y)f_1 - r_1 - f_2 = y + 1$ има мономи, делящи се на $LT(f_1) = xy$ или $LT(f_2) = y^2$. Затова $r = r_1 + y + 1 = x + y + 1$ е остатък при това деление и

$$f = (x + y)f_1 + f_2 + (x + y + 1) = a_1 f_1 + a_2 f_2 + r$$

за $a_1 = x + y$, $a_2 = 1$.

Теорема 1. (Деление на полиноми на няколко променливи) *Нека $k$ е поле, $>$ е мономна наредба в $k[x_1, \ldots, x_n]$, а $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ е наредена $s$-торка неконстантни полиноми. Тогава всеки полином $f \in k[x_1, \ldots, x_n]$ може да се запише във вида*

$$f = a_1 f_1 + \ldots + a_s f_s + r$$

*за подходящи полиноми $a_1, \ldots, a_s, r \in k[x_1, \ldots, x_n]$, където $r = 0$ е тъждествено нулевият полином или $r = \sum_{\alpha \in A} a_\alpha x^\alpha$ е $k$-линейна комбинация на мономи $x^\alpha$, които не се делят на нито един от мономите $LT(f_1), \ldots, LT(f_s)$. Полиномът $r$ се нарича остатък при деление на $f$ с $f_1, \ldots, f_s$.*

**Доказателство:** Ще установим, че следният алгоритъм предоставя обявеното представяне на $f$ :

Input:$f_1, \ldots, f_s, f$
Output:$a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
$i := 1$
divisionoccurred := false
WHILE $i \leq s$ AND divisionoccurred = false DO
IF $LT(f_i)$ divides $LT(p)$ THEN

$$a_i := a_i + \frac{LT(p)}{LT(f_i)}$$

$$p := p - \frac{LT(p)}{LT(f_i)} f_i$$

divisionoccurred := true
ELSE
$i := i + 1$
IF divisionoccurred = false THEN
$r := r + LT(p)$
$p := p - LT(p)$

Първо ще проверим верността на равенството $f = a_1 f_1 + \ldots + a_s f_s + p + r$ на всяка стъпка от алгоритъма. За началните данни тъждеството е очевидно. Ако допуснем верността му при някоя стъпка от алгоритъма и предположим, че някой старши член $LT(f_i)$ дели $LT(p)$, то при извършване на съответното деление заменяме $a_i$ с $a_i + \frac{LT(p)}{LT(f_i)}$ и $p$ с $p - \frac{LT(p)}{LT(f_i)} f_i$, така че

$$\left(a_i + \frac{LT(p)}{LT(f_i)}\right) f_i + \left(p - \frac{LT(p)}{LT(f_i)} f_i\right) = a_i f_i + p$$

не се променя. Делението с $f_i$ не променя $a_j$ за $j \neq i$ и остатъка $r$, така че верността на $f = a_1 f_1 + \ldots + a_s f_s + r$ се запазва. При отделяне на остатък $a_i$ не се променят, а сумата $p + r = (p - LT(p)) + (r + LT(p))$ се запазва. По този начин, $f = a_1 f_1 + \ldots + a_s f_s + p + r$ остава в сила след произволна стъпка от алгоритъма.

При $p = 0$ алгоритъмът спира, доколкото $f = a_1 f_1 + \ldots + a_s f_s + r$ и нито един от мономите на $r$ с ненулеви коефициенти не се дели на $LT(f_i)$ за всички $1 \leq i \leq s$.

Остава да проверим, че алгоритъмът спира след краен брой стъпки. За целта е достатъчно да установим, че всяка стъпка от алгоритъма намалява строго

старшия член $LT(p)$ на полинома $p$. Наистина, при деление с $f_i$ заменяме $p$ с $p - \frac{LT(p)}{LT(f_i)} f_i$. Съгласно $LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p)$, старшият член $LT(p)$ се унищожава от $p$ и $\frac{LT(p)}{LT(f_i)} f_i$, така че

$$LT(p) > LT\left(p - \frac{LT(p)}{LT(f_i)} f_i\right).$$

При отделяне на остатък отново имаме

$$LT(p) > LT(p - LT(p)).$$

По този начин, $LT(p)$ намалява строго при всяка стъпка и алгоритъмът прекъсва след краен брой стъпки, доколкото всяка мономна наредба $>$ е артинова. По този начин, алгоритъмът спира след краен брой стъпки с $p = 0$ или с $p \neq 0$ и минимален старши член $LT(p)$, Q.E.D.
Следващият пример показва, че частните $a_1, \dots a_s$ и остатъкът $r$ при деление на $f$ с $f_1, \dots, f_s$ не са единствени.

Пример 6.5. При деление на $f = x^2y + xy^2 + y^2$ с $g_1 = y^2 - 1$ и $g_2 = xy - 1$, използвайки лексикографската наредба, старшият член $LT(f) = x^2y$ не се дели на $LT(g_1) = y^2$, но се дели на $LT(g_2) = xy$ с частно $x$. Полагаме текущата стойност $a_2 = x$ и заменяме $p = f$ с $p = f - xg_2 = xy^2 + x + y^2$. Сега $LT(p) = xy^2$ се дели на $LT(g_1) = y^2$ с частно $x$. По този начин получаваме текущите стойности $a_1 = x$ и $p = f - xg_2 - xg_1 = 2x + y^2$. На третата стъпка, $LT(p) = 2x$ не се дели нито на $LT(g_1) = y^2$, нито на $LT(g_2) = xy$. Отделяме остатък $r = 2x$ и стигаме до $p = y^2$. Сега $LT(p) = y^2$ се дели на $LT(g_1) = y^2$ с частно 1. Затова заменяме $a_1 = x$ с $a_1 = x + 1$ и $p = y^2$ с $p = 1$. Накрая, заменяме $r = 2x$ с $r = 2x + 1$, а $p = 1$ с $p = 0$, за да получим

$$f = a_1g_1 + a_2g_2 + r = (x + 1)g_1 + xg_2 + (2x + 1).$$

Сравнявайки с Пример 6.4 се убеждаваме, че частните $a_i$ и остатъкът $r$ зависят от реда, в който са взети $f_1, \dots, f_s$. При фиксиран ред на полиномите $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ може да се докаже, че полиномите $a_1, \dots, a_s, r \in k[x_1, \dots, x_n]$ от Теорема 1 са единствени.

Пример 6.6. При деление на $f = xy^2 - x$ с $f_1 = xy + 1$ и $f_2 = y^2 - 1$, използвайки лексикографската наредба, се получава

$$f = yf_1 + 0.f_2 + (-x - y).$$

При деление на същия полином $f$ с $f_2$ и $f_1$ се стига до

$$f = xf_2 + 0.f_1.$$

По този начин, второто деление показва, че $f$ принадлежи на идеала $\langle f_1, f_2 \rangle$, породен от $f_1$ и $f_2$, докато първото деление не дава възможност да се стигне до същия извод.

### Задачи

Задача 6.7. *Нека $f_1 = xy^2 - x$ и $f_2 = x - y^3$ са полиноми на $x$ и $y$ с коефициенти от поле $k$. Да се раздели полинома $f = x^7y^2 + x^3y^2 - y + 1$ на полиномите*
*(а)* $(f_1, f_2)$;
*(б)* $(f_2, f_1)$; *използвайки*
*(i) лексикографската наредба* $>_{\text{lex}}$;
*(ii) градуирано лексикографската наредба* $>_{\text{grlex}}$ .

Задача 6.8. *Да разгледаме полиномите* $f = xy^2z^2 + xy - yz$, $f_1 = x - y^2$, $f_2 = y - z^3$, $f_3 = z^2 - 1$ *от* $k[x, y, z]$, *където* $k$ *е произволно поле. Да се раздели полинома* $f$ *на полиномите*
*(а)* $(f_1, f_2, f_3)$;
*(б)* $(f_2, f_3, f_{31})$;
*(в)* $(f_3, f_1, f_2)$; *използвайки лексикографската наредба.*

Задача 6.9. *Да разгледаме полиномите* $f = x^3 - x^2y - x^2z + x$, $f_1 = x^2y - z$, $f_2 = xy - 1$ *на* $x, y, z$ *с коефициенти от поле* $k$. *Относно градуирано лексикографската наредба* $>_{\text{grlex}}$ *да означим с* $r_1$ *остатъка на* $f$ *при деление с* $(f_1, f_2)$, *а с* $r_2$ *- остатъка на* $f$ *при деление с* $(f_2, f_1)$.
*(а) Да се докаже, че полиномът* $r = r_1 - r_2$ *принадлежи на идеала* $\langle f_1, f_2 \rangle$ *и да се намери в явен вид представяне* $r = Af_1 + Bf_2$.
*(б) Да се пресметне остатъка на* $r$ *при деление с* $(f_1, f_2)$.