ПОЛИНОМЫ ЛОРАНА*

В. Н. Малозёмов — malv@math.spbu.ru

Н. А. Соловьёва — vinyo@mail.ru

24 октября 2009 г.

В докладе использованы материалы из обзорной статьи [1].

1°. *Полиномом Лорана* называется выражение вида

$$h(z) = \sum_{k=m}^{n} h_k\, z^{-k}, \tag{1}$$

где m, n — целые числа, $m \leqslant n$, и h_k — вещественные коэффициенты. Если h_m и h_n отличны от нуля, то число $|h| := n - m$ называется *степенью* полинома Лорана $h(z)$. Будем писать $h = 0$, если все коэффициенты полинома Лорана $h(z)$ равны нулю. Считаем, что $|h| = -\infty$, когда $h = 0$.

Полином Лорана нулевой степени имеет вид Cz^{-p}, где $C \neq 0$.

2°. Множество полиномов Лорана (при всех $m, n \in \mathbb{Z}$, $m \leqslant n$) обычно обозначают через $\mathbb{R}[z, z^{-1}]$. На $\mathbb{R}[z, z^{-1}]$ естественным образом вводятся операции сложения и умножения. Пусть

$$h(z) = \sum_{k=m_1}^{n_1} h_k\, z^{-k}, \qquad g(z) = \sum_{k=m_2}^{n_2} g_k\, z^{-k}. \tag{2}$$

Обозначим $m = \min\{m_1, m_2\}$, $n = \max\{n_1, n_2\}$ и положим

$$h_k = 0 \ \text{ при } \ k \in m : n \setminus m_1 : n_1\,,$$
$$g_k = 0 \ \text{ при } \ k \in m : n \setminus m_2 : n_2\,.$$

Тогда формулы (2) можно переписать в виде

$$h(z) = \sum_{k=m}^{n} h_k\, z^{-k}, \qquad g(z) = \sum_{k=m}^{n} g_k\, z^{-k}.$$

*Семинар по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD»: `http://www.dha.spb.ru/`

По определению

$$\big(h+g\big)(z) = h(z) + g(z) = \sum_{k=m}^{n} \big(h_k + g_k\big)\, z^{-k}.$$

Далее положим

$$c_p \;=\; \sum_{\substack{k+s=p,\\ k\in m_1:n_1,\\ s\in m_2:n_2}} h_k\, g_s\,, \qquad p\in m_1+m_2 : n_1+n_2\,.$$

В частности,

$$c_{m_1+m_2} = h_{m_1}\, g_{m_2}\,, \qquad c_{n_1+n_2} = h_{n_1}\, g_{n_2}\,. \tag{3}$$

По определению

$$\big(h\, g\big)(z) = h(z)\, g(z) = \sum_{p=m_1+m_2}^{n_1+n_2} c_p\, z^{-p}.$$

Отметим, что в силу (2) и (3)

$$\big|h\, g\big| = \big|h\big| + \big|g\big|. \tag{4}$$

Действительно,

$$\big|h\, g\big| = (n_1+n_2) - (m_1+m_2) = (n_1-m_1) + (n_2-m_2) = \big|h\big| + \big|g\big|.$$

Множество $\mathbb{R}[z, z^{-1}]$ с введёнными операциями сложения и умножения становится кольцом с единицей. Единицей является полином $h(z)\equiv 1$.

Элемент $h \in \mathbb{R}[z, z^{-1}]$ называется обратимым, если существует элемент $g\in\mathbb{R}[z, z^{-1}]$, такой, что $h(z)\, g(z) \equiv 1$. Согласно (4) обратимым может быть полином Лорана только нулевой степени. Вместе с тем, любой полином Лорана нулевой степени обратим, поскольку

$$C\, z^{-p}\big(\tfrac{1}{C}\, z^p\big) \equiv 1.$$

3°. Говорят, что полином Лорана $a(z)$ делится на полином Лорана $b(z)$, если существует полином Лорана $q(z)$, такой, что

$$a(z) = b(z)\, q(z).$$

Деление можно выполнять «в столбик».

ПРИМЕР 1. Пусть $a(z) = z + 2 + z^{-1}$, $b(z) = z + 1$. Имеем

$$
\begin{array}{r|l}
-\;z + 2 + z^{-1} & z + 1 \\
\cline{2-2}
z + 1\phantom{+z^{-1}} & 1 + z^{-1}. \\
\cline{1-1}
-\;1 + z^{-1} & \\
1 + z^{-1} & \\
\cline{1-1}
0 &
\end{array}
$$

Значит, $a(z) = b(z)\,q(z)$, где $q(z) = 1 + z^{-1}$.

В общем случае полином Лорана делится на любой полином Лорана нулевой степени. Действительно,

$$
\sum_{k=m}^{n} a_k\, z^{-k} = C\, z^{-p} \left(\frac{1}{C} \sum_{k=m}^{n} a_k\, z^{-k+p} \right) =
$$

$$
= C\, z^{-p} \left(\frac{1}{C} \sum_{k=m-p}^{n-p} a_{k+p}\, z^{-k} \right).
$$

4°. В кольце $\mathbb{R}[z, z^{-1}]$ точное деление возможно не всегда, но всегда возможно деление с остатком. Последнее означает, что для любых полиномов $a(z)$, $b(z)$ из $\mathbb{R}[z, z^{-1}]$ с $|a| \geqslant |b| \geqslant 1$ существуют полиномы $q(z)$, $r(z)$ из $\mathbb{R}[z, z^{-1}]$ с $|q| \leqslant |a| - |b|$ и $|r| < |b|$, такие, что

$$
a(z) = b(z)\,q(z) + r(z).
$$

Деление с остатком можно выполнять «в столбик».

ПРИМЕР 2. Пусть $a(z) = z + 3 + z^{-1}$, $b(z) = z + 1$. Имеем

$$
\begin{array}{r|l}
-\;z + 3 + z^{-1} & z + 1 \\
\cline{2-2}
z + 1\phantom{+z^{-1}} & 1 + 2z^{-1}. \\
\cline{1-1}
-\;2 + z^{-1} & \\
2 + 2z^{-1} & \\
\cline{1-1}
-z^{-1} &
\end{array}
$$

Значит, $z+3+z^{-1} = (z+1)(1+2z^{-1}) - z^{-1}$, то есть $q(z) = 1+2z^{-1}$, $r(z) = -z^{-1}$.

Отметим, что деление с остатком полиномов Лорана, вообще говоря, не единственно. В рассматриваемом примере

$$
z + 3 + z^{-1} = (z + 1)(1 + z^{-1}) + 1,
$$

то есть $q(z) = 1 + z^{-1}$, $r(z) \equiv 1$. И ещё один вариант:

$$z + 3 + z^{-1} = (z+1)(2 + z^{-1}) - z,$$

то есть $q(z) = 2 + z^{-1}$, $r(z) = -z$.

Во всех трёх случаях степень неполного частного $q(z)$ равна единице ($|q| = |a| - |b|$), а степень остатка $r(z)$ равна нулю.

Приведём пример, в котором $|q| < |a| - |b|$.

ПРИМЕР 3. Пусть $a(z) = z + 1 + z^{-1}$, $b(z) = z + 1$. При $q(z) \equiv 1$, $r(z) = z^{-1}$ имеем $a(z) = b(z)\, q(z) + r(z)$ и

$$\big|q\big| = 0 < 1 = \big|a\big| - \big|b\big|.$$

Однако и здесь возможен варинт деления с остатком, когда $|q| = |a| - |b|$. Действительно,

$$z + 1 + z^{-1} = (z+1)(1 + z^{-1}) - 1.$$

5°. Рассмотрим вопрос о нахождении наибольшего общего делителя (НОД) двух полиномов Лорана.

Напомним, что наибольшим общим делителем двух ненулевых полиномов $a(z)$, $b(z)$ из $\mathbb{R}[z, z^{-1}]$ называется такой полином $c(z) = \text{НОД}(a(z), b(z))$ из $\mathbb{R}[z, z^{-1}]$, что он делит $a(z)$ и $b(z)$ и делится на любой их общий множитель.

Для нахождения наибольшего общего делителя обычно используется метод последовательного деления с остатком (алгоритм Евклида). Опишем его.

Пусть даны два ненулевых полинома $a(z)$, $b(z)$ из $\mathbb{R}[z, z^{-1}]$. Можно считать, что $|a| \geqslant |b|$. Обозначим $a_0(z) = a(z)$, $a_1(z) = b(z)$ и выполним последовательное деление с остатком по правилу:

$$\begin{aligned}
&a_0(z) = a_1(z)\, q_1(z) + a_2(z), \quad |a_2| < |a_1|;\\
&a_1(z) = a_2(z)\, q_2(z) + a_3(z), \quad |a_3| < |a_2|;\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&a_{n-2}(z) = a_{n-1}(z)\, q_{n-1}(z) + a_n(z), \quad |a_n| < |a_{n-1}|;\\
&a_{n-1}(z) = a_n(z)\, q_n(z).
\end{aligned} \tag{5}$$

Последнее деление будет наверняка точным, если $|a_n| = 0$. Но точное деление может произойти и ранее.

Просмотрев цепочку равенств (5) снизу вверх, видим, что $a_n(z)$ делит все полиномы $a_{n-1}(z), a_{n-2}(z), \dots, a_1(z), a_0(z)$. Следовательно, $a_n(z)$ является общим делителем $a(z)$ и $b(z)$.

Просмотрев цепочку равенств сверху вниз, заключаем, что остатки $a_2(z)$, $\ldots, a_n(z)$ делятся на любой общий множитель полиномов $a(z)$ и $b(z)$. В частности, $a_n(z)$ делится на любой общий множитель полиномов $a(z)$ и $b(z)$. По определению

$$a_n(z) = \text{НОД}(a(z), b(z)).$$

Равенствам (5) можно придать другую форму:

$$\begin{bmatrix} a_1(z) \\ a_2(z) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_1(z) \end{bmatrix} \begin{bmatrix} a_0(z) \\ a_1(z) \end{bmatrix};$$

$$\begin{bmatrix} a_2(z) \\ a_3(z) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_2(z) \end{bmatrix} \begin{bmatrix} a_1(z) \\ a_2(z) \end{bmatrix};$$

$$\vdots$$

$$\begin{bmatrix} a_{n-1}(z) \\ a_n(z) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_{n-1}(z) \end{bmatrix} \begin{bmatrix} a_{n-2}(z) \\ a_{n-1}(z) \end{bmatrix};$$

$$\begin{bmatrix} a_n(z) \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_n(z) \end{bmatrix} \begin{bmatrix} a_{n-1}(z) \\ a_n(z) \end{bmatrix}.$$

Отсюда следует, что

$$\begin{bmatrix} a_n(z) \\ 0 \end{bmatrix} = \prod_{k=n}^{1} \begin{bmatrix} 0 & 1 \\ 1 & -q_k(z) \end{bmatrix} \begin{bmatrix} a(z) \\ b(z) \end{bmatrix}.$$

Учитывая, что

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_k(z) \end{bmatrix}^{-1} = \begin{bmatrix} q_k(z) & 1 \\ 1 & 0 \end{bmatrix},$$

приходим к представлению

$$\begin{bmatrix} a(z) \\ b(z) \end{bmatrix} = \prod_{k=1}^{n} \begin{bmatrix} q_k(z) & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_n(z) \\ 0 \end{bmatrix}. \tag{6}$$

6°. Приведём пример на нахождение наибольшего общего делителя.

ПРИМЕР 4. Пусть $a(z) = z + 3 + z^{-1}$, $b(z) = z + 1$. Имеем (см. пример 2)

$$z + 3 + z^{-1} = (z+1)(1 + 2z^{-1}) - z^{-1},$$
$$z + 1 = -z^{-1}(-z^2 - z).$$

Значит, НОД$(z+3+z^{-1}, z+1) = -z^{-1}$.

Формула (6) принимает вид

$$\begin{bmatrix} z+3+z^{-1} \\ z+1 \end{bmatrix} = \begin{bmatrix} 1+2z^{-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -z^2-z & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -z^{-1} \\ 0 \end{bmatrix}.$$

Отметим, что наибольший общий делитель двух полиномов Лорана, вообще говоря, не единствен. В рассматриваемом примере, так же, как и в примере 2, возможно другое развитие событий:

$$z+3+z^{-1} = (z+1)(1+z^{-1}) + 1,$$
$$z+1 = 1 \cdot (z+1).$$

Значит, НОД$(z+3+z^{-1}, z+1) = 1$ и

$$\begin{bmatrix} z+3+z^{-1} \\ z+1 \end{bmatrix} = \begin{bmatrix} 1+z^{-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} z+1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Ещё один вариант:

$$z+3+z^{-1} = (z+1)(2+z^{-1}) - z,$$
$$z+1 = -z(-1-z^{-1}).$$

Значит, НОД$(z+3+z^{-1}, z+1) = -z$ и

$$\begin{bmatrix} z+3+z^{-1} \\ z+1 \end{bmatrix} = \begin{bmatrix} 2+z^{-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1-z^{-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -z \\ 0 \end{bmatrix}.$$

7°. В примере 4 все три наибольших общих делителя имеют одинаковую степень. Это не случайно.

ПРЕДЛОЖЕНИЕ. *Все наибольшие общие делители полиномов Лорана $a(z)$ и $b(z)$ имеют одинаковую степень.*

Доказательство. Возьмём два наибольших общих делителя $c(z)$ и $d(z)$. По определению найдутся полиномы Лорана $p(z)$ и $q(z)$, такие, что

$$c(z) = d(z)\, p(z), \qquad d(z) = c(z)\, q(z).$$

Согласно (4), $|c| = |d| + |p|$, $|d| = |c| + |q|$, откуда следует, что $|p| = |q| = 0$. Значит, $|c| = |d|$. □

ЛИТЕРАТУРА

1. Daubechies I., Sweldens W. *Factoring wavelets transforms into lifting steps* // J. Fourier Anal. Appl. 1998. Vol. 4. No. 3. P. 247–269.