Листок по алгебре (полугруппы в решётках, выпуклые множества и целые точки в многогранниках) для матем. кружка, осень 2018
автор: Дмитрий Анатольевич Степанов, доцент каф. ФН-12 МГТУ им. Баумана
email: dstepanov@bmstu.ru

---

1 Полугруппы в целочисленных решётках

Полугруппа — это алгебраическая структура с одной ассоциативной бинарной операцией. Пример: $(\mathbf{N},+)$. **Моноид** — это полугруппа, обладающая нейтральным элементом. Пример: $(\mathbf{Z}_{\geqslant 0}=\{0\}\cup\mathbf{N},+)$. Все полугруппы и моноиды, рассматриваемые в этом листке, будут коммутативными.

Задача 1.1. Пусть известно, что подполугруппа S полугруппы $(\mathbf{N},+)$ содержит числа 3 и 7. Какие ещё числа обязана содержать полугруппа S?

Задача 1.2. Пусть S — произвольная полугруппа $S\subseteq\mathbf{N}$, и d — наибольший общий делитель всех чисел, входящих в S. Доказать, что существует такое натуральное число c, что S состоит из всех чисел вида dn, $n\geqslant c$, и, возможно, ещё нескольких чисел, меньших dc. Наименьшее натуральное c с таким свойством называется **кондуктором** полугруппы S. Например, для полугруппы из задачи 1.1 $d=1$ и кондуктор $c=12$.

Полугруппа (или моноид) S называется **конечно порождённой**, если существуют такие $s_1,\dots,s_k\in S$, что для любого $s\in S$ найдутся такие $n_1,\dots,n_k\in\mathbf{Z}_{\geqslant 0}$, что

$$s=n_1s_1+\dots+n_ks_k;$$

здесь n_is_i обозначает $\underbrace{s_i+\dots+s_i}_{n_i\text{ раз}}$, $i=1,\dots,k$. Набор таких элементов $s_1,\dots,s_k\in S$, что любой $s\in S$ представляется в виде линейной комбинации элементов $s_1,\dots,s_k$ с неотрицательными коэффициентами, называется **системой порождающих** полугруппы (моноида) S.

Задача 1.3. Доказать, что любая полугруппа $S\subseteq\mathbf{N}$ конечно порождена.

Задача 1.4. Пусть полугруппа $S\subseteq\mathbf{N}$ порождена двумя взаимно простыми числами $a,b\in\mathbf{N}$. Доказать, что кондуктор $c(S)$ полугруппы S равен $(a-1)(b-1)$.

Задача 1.5. Множество $\mathbf{Z}^2_{\geqslant 0}=\{(a,b)\,|\,a,b\in\mathbf{Z}_{\geqslant 0}\}$ всех целочисленных векторов с неотрицательными координатами является коммутативным моноидом относительно операции сложения векторов. Привести пример подмоноида $S\subset\mathbf{Z}^2_{\geqslant 0}$, который не будет конечно порождён.

Задача 1.6. Пусть $k_1,k_2\in\mathbf{R}$, $0<k_1<k_2$. Убедиться, что множество $S(k_1,k_2)$ всех целочисленных неотрицательных векторов, лежащих не ниже прямой $y=k_1x$ и не выше прямой $y=k_2x$, является моноидом. При каком условии на k_1 и k_2 такой моноид будет конечно порождён?

Подмножество I полугруппы S называется **идеалом**, если $\forall x\in I$ и $\forall y\in S$ $x+y\in I$, т. е. I "поглощает" при сложении все остальные элементы полугруппы S. Например, в моноиде $\mathbf{Z}^2_{\geqslant 0}$ идеалом будет множество

$$I=\{(a,b)\in\mathbf{Z}^2_{\geqslant 0}\,|\,a\geqslant 1,b\geqslant 1\}.$$

Задача 1.7. Доказать, что любой идеал I моноида $\mathbf{Z}^2_{\geqslant 0}$ конечно порождён в следующем смысле: существуют такие элементы $(a_i, b_i) \in I$, $i = 1 \ldots, k$, что I является объединением сдвинутых на (a_i, b_i) моноидов $\mathbf{Z}^2_{\geqslant 0}$:

$$I = \bigcup_{i=1}^{k} \big((a_i, b_i) + \mathbf{Z}^2_{\geqslant 0}\big).$$

Обобщить доказательство на идеалы в моноиде $\mathbf{Z}^n_{\geqslant 0}$, $n > 2$.

Подмножество $\sigma \subset \mathbf{R}^n$ называется **рациональным полиэдральным конусом**, если σ может быть представлено как множество решений системы линейных неравенств

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \geqslant 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \geqslant 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \geqslant 0 \end{cases} \tag{1}$$

с *целыми* коэффициентами a_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n$. Рациональный полиэдральный конус называется **строго выпуклым**, если система линейных однородных *уравнений* с теми же левыми частями, что у системы (1), имеет только тривиальное решение.

Задача 1.8. (Лемма Гордана) Пусть $\sigma \subseteq \mathbf{R}^n$ — рациональный полиэдральный конус, и $S = \sigma \cap \mathbf{Z}^n_{\geqslant 0}$ — моноид, состоящий из всех неотрицательных целочисленных векторов, содержащихся в σ. Доказать, что S конечно порождён (для начала можно ограничиться случаем строго выпуклого конуса σ).

2 Выпуклые множества

Подмножество A плоскости, пространства или аффинного пространства $\mathbf{R}^n$ называется **выпуклым**, если вместе с любыми двумя своими точками $x, y \in A$ оно содержит и весь отрезок, соединяющий x и y: $[x, y] \subseteq A$.

Задача 2.1. Пусть A — замкнутое выпуклое множество плоскости, а y — точка, не принадлежащая A. Доказать, что существует прямая L, разделяющая точку y и множество A, т. е. такая прямая, что y лежит по одну, а A целиком по другую сторону от L. Обобщить это утверждение на замкнутые выпуклые множества в $\mathbf{R}^n$, $n > 2$.

Непустое пересечение любого семейства выпуклых множеств выпукло. Пусть A — произвольное подмножество в $\mathbf{R}^n$, $n \geqslant 1$. Его **выпуклой оболочкой** $\operatorname{conv}(A)$ называется пересечение всех выпуклых множеств, содержащих A.

Задача 2.2. Пусть $A = \{P_1, \ldots, P_k\}$ — конечное множество точек плоскости. Доказать, что множество $\operatorname{conv}(A)$ можно представить как пересечение конечного числа полуплоскостей. Обобщить доказательство на конечные подмножества пространства $\mathbf{R}^n$ для произвольного n.

Задача 2.3. Пусть $A = \{P_1, \ldots, P_k\}$ — конечное множество точек пространства $\mathbf{R}^n$, $n \geqslant 2$, причём точки $P_1, \ldots, P_k$ порождают $\mathbf{R}^n$ (при $n = 2$ это означает, что

$P-1, \dots, P_k$ не лежат на одной прямой, при $n = 3$ — не лежат на одной плоскости и т. д.). Доказать, что среди всех семейств полупространств (полуплоскостей при $n = 2$), пересечение которых даёт $\mathrm{conv}(A)$ (см. задачу 2.2), есть минимальное. Граничные гиперплоскости (прямые при $n = 2$, плоскости при $n = 3$) полупространств этого семейства называются **опорными гиперплоскостями** (прямыми, плоскостями) множества $\mathrm{conv}(A)$.

Суммой Минковского подмножеств $A, B \subseteq \mathbf{R}^n$ называется множество

$$A + B = \{a + b \,|\, a \in A, b \in B\}.$$

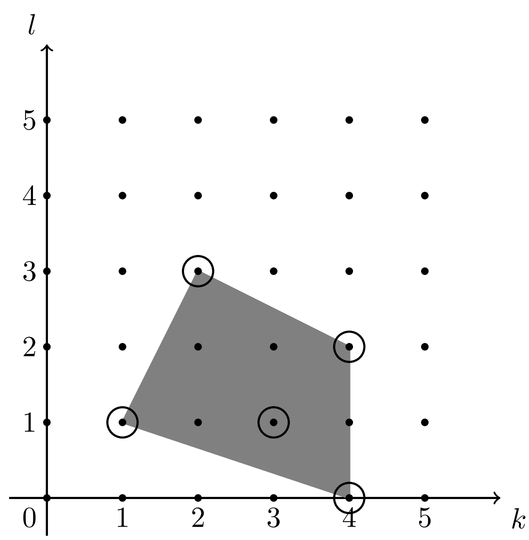
Задача 2.4. Взяв в качестве множеств A и B какие-либо отрезки, треугольники, прямоугольники или иные фигуры на плоскости, построить несколько примеров суммы Минковского.

Задача 2.5. Доказать, что если A и B — выпуклые множества, то и $A+B$ — выпуклое множество.

Задача 2.6. Пусть $A = \mathrm{conv}(P_1, \dots, P_k)$, $B = \mathrm{conv}(Q_1, \dots, Q_l)$. Доказать, что

$$A + B = \mathrm{conv}(\{P_i + Q_j \,|\, i = 1, \dots, k,\ j = 1, \dots, l\}).$$

Пусть $f(x, y) = \sum\limits_{k+l \leq n} a_{k,l} x^k y^l$ — многочлен от двух переменных степени не выше n. **Многоугольником Ньютона** многочлена f называется выпуклая оболочка $N(f)$ тех точек $(k, l) \in \mathbf{Z}^2_{\geqslant} \subset \mathbf{R}^2$, для которых $a_{k,l} \neq 0$. Например, если $f(x, y) = x^4y^2 - 2x^2y^3 + 3x^3y - x^4 + xy$, то многоугольник Ньютона $N(f)$ — четырёхугольник, изображённый на рисунке ниже. Эта конструкция очевидным образом обобщается на многочлены от трёх и большего числа переменных и даёт понятие **многогранника Ньютона**.



Задача 2.7. Доказать, что $N(fg) = N(f) + N(g)$ для любых ненулевых многочленов f и g.

Разбиением многоугольника C называется такое множество выпуклых многоугольников C_i, $i = 1, \ldots, k$, что а) $C = \cup_{i=1}^{k} C_i$ и б) Любые два многоугольника C_i, C_j, $i \neq j$, либо не пересекаются, либо пересекаются по общей стороне либо общей вершине. Многоугольники C_i, $i = 1, \ldots, k$, называются также **клетками** данного разбиения. Пусть $C = A + B$ — сумма Минковского выпуклых многоугольников A и B. Разбиение $C = \cup_i C_i$ называется **смешанным**, если каждый из многоугольников C_i, в свою очередь, представляет собой сумму Минковского вершины одного из многоугольников A или B и второго многоугольника или сумму Минковского стороны многоугольника A и стороны многоугольника B.

Задача 2.8. Построить пример какого-нибудь смешанного разбиения.

Задача 2.9. Доказать, что если $C = A + B$ — сумма Минковского выпуклых многоугольников A и B, то смешанное разбиение многоугольника C всегда существует.

Задача 2.10. Показать, что смешанное разбиение суммы Минковского двух многоугольников, вообще говоря, не единственно.

Клетка C_i некоторого смешанного разбиения $C = \cup_i C_i$ многоугольника $C = A + B$ называется **смешанной**, если она является суммой стороны многоугольника A и стороны многоугольника B.

Задача 2.11. Выделить смешанные клетки в разбиениях, построенных в задачах 2.8 и 2.10.

Сумма площадей всех смешанных клеток некоторого смешанного разбиения суммы $C = A + B$ выпуклых многоугольников A и B называется **смешанной площадью** этой суммы и обозначается $\mathrm{MVol}(A, B)$ (в старших размерностях этому понятию соответствует понятие **смешанного объёма** (англ. *mixed volume*)). Можно показать, что смешанная площадь $\mathrm{MVol}(A, B)$ не зависит от выбора смешанного разбиения суммы $A + B$.

Задача 2.12. Найти смешанные площади в примерах, построенных в задаче 2.10, и убедиться, что они не зависят от разбиения.

3 Целые точки в многогранниках

Задача 3.1. Пусть P — многоугольник на плоскости, т. е. фигура, ограниченная замкнутой ломаной без самопересечений, вершины которого имеют целые координаты. Пусть i — количество целых точек внутри многоугольника, b — количество целых точек на его границе. Доказать следующую *формулу Пика* для площади многоугольника P:

$$S(P) = i + \frac{b}{2} - 1.$$

Задача 3.2. Найти обобщение формулы Пика на многоугольники, содержащие дыры.

Задача 3.3. Привести пример, показывающий, что объём трёхмерного многогранника с целыми вершинами не может быть выражен через количество его внутренних целых точек и количество целых точек на его границе.

Если $n \in \mathbf{N}$ и P — выпуклый многоугольник, обозначим через nP многоугольник, полученный из P гомотетией с коэффициентом n и центром в начале координат. Через $|P \cap \mathbf{Z}^2|$ обозначим количество целых точек в многоугольнике nP.

Задача 3.4. Доказать, что $\lim\limits_{n\to\infty} \frac{|nP\cap\mathbf{Z}^2|}{n^2} = S(P)$.

Теория, основы которой намечены в данном листке, имеет ряд интересных приложений. Например, следующая теорема даёт оценку числа решений алгебраической системы уравнений.

Теорема (Бернштейн, 1975). *Пусть $f_1, \ldots, f_n$ — полиномы от n переменных, причём система*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots\ldots\ldots\ldots \\ f_n(x_1, \ldots, x_n) = 0 \end{cases}$$

имеет конечное множество ненулевых комплексных решений (т. е. таких решений $(z_1, \ldots, z_n) \in \mathbf{C}^n$, что $z_i \neq 0$ для всех $i = 1, \ldots, n$). Пусть $P_i = N(f_i)$ — многогранник Ньютона полинома f_i, $i = 1, \ldots, n$. Тогда количество ненулевых комплексных решений этой системы не превосходит числа $\mathrm{MVol}(P_1, \ldots, P_n)$*. Более того, для достаточно общего выбора коэффициентов многочленов $f_1, \ldots, f_n$ число решений системы в точности равно* $\mathrm{MVol}(P_1, \ldots, P_n)$.

Также были предложены различные подходы к обобщению формулы Пика в высшие размерности. Например, доказано, что если P — выпуклый многогранник в $\mathbf{R}^n$ с целыми вершинами, то величина $|(\lambda P \cap \mathbf{Z}^n)|$ как функция от λ является многочленом степени n с рациональными коэффициентами. Это т. н. **многочлен Экхарта** многогранника P. Найден алгоритм (*алгоритм Барвинка*), за полиномиальное (по исходным данным) время вычисляющий количество целых точек внутри данного рационального многогранника фиксированной размерности. Отметим, однако, что формулы, выражающие количество целых точек внутри многогранника размерности $\geqslant 3$ с целыми вершинами, известны только в частных случаях и оказываются чрезвычайно сложны. Например, количество целых точек в тетраэдре с вершинами $(0,0,0)$, $(a,0,0)$, $(0,b,0)$, $(0,0,c)$, где a, b, c — натуральные попарно взаимно простые числа, равно (Морделл, 1951):

$$\frac{abc}{6} + \frac{ab+bc+ca}{4} + \frac{1}{12}\left(\frac{bc}{a} + \frac{ac}{b} + \frac{ab}{c} + \frac{1}{abc}\right) + \frac{a+b+c}{4} - \\ - s(ab,c) - s(bc,a) - s(ca,b) + 2,$$

где $s(x,y)$ — т. н. **Дедекиндова сумма**. Она вычисляется с помощью “пилообразной” функции

$$((x)) = \begin{cases} \{x\} - 1/2, \ x \in \mathbf{R} \setminus \mathbf{Z} \\ 0, \quad x \in \mathbf{Z} \end{cases}.$$

Тогда $s(x,y) = \sum\limits_{n=1}^{y-1} \left(\left(\frac{n}{y}\right)\right)\left(\left(\frac{xn}{y}\right)\right)$.

Список литературы

[1] Хованский А. Г. Малочлены. М.: Фазис, 1996.

[2] Хованский А. Г., Чулков С. П. Геометрия полугруппы $\mathbf{Z}^n_{\geqslant 0}$. Приложения к комбинаторике, алгебре и дифференциальным уравнениям. М.: МЦНМО, 2006.

[3] Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры: пер. с англ. — М.: Мир, 2000.

[4] Cox, D. A., Little, J. O'Shea, D. Using Algebraic Geometry (Second Edition). Springer, 2005.