

ВВЕДЕНИЕ

Кольцо многочленов $F[x]$ над полем F от одной переменной x обладает рядом хороших свойств. В нём есть алгоритм деления с остатком и алгоритм Евклида. Все идеалы в этом кольце главные. В этом смысле оно очень похоже на кольцо целых чисел $\mathbb{Z}$. Задача принадлежности многочлена f идеалу I в таком кольце решается тривиально с помощью деления с остатком на образующий элемент идеала I . Вычисления в факторкольце приводят к арифметике остатков по модулю образующего многочлена. Если переменных становится хотя бы две, то таких хороших свойств уже нет. Например, непонятно, что значит «разделить x на y с остатком». Идеалы в кольце $F[x, y]$ уже не обязательно главные. Системы полиномиальных уравнений от двух и более переменных, вообще говоря, уже не эквивалентны одному уравнению. Наша ближайшая цель — научиться исследовать системы нелинейных полиномиальных уравнений над полем. В частности, мы хотим научиться отвечать на следующие вопросы:

- всякая ли система может быть задана конечным набором уравнений?
- как проверить, совместна ли система?
- как узнать, конечно ли множество решений системы (над $\bar{F}$)?
- как проверить принадлежность многочлена f идеалу I ?
- как проводить вычисления в факторалгебре $F[x_1, \dots, x_n]/I$?
- как исключить заданные неизвестные из системы?

Заметим, что для линейных систем ответы на эти вопросы легко получить с помощью приведения системы к ступенчатому виду методом Гаусса.

1. СВОЙСТВА КОНЕЧНОСТИ ПОЛУГРУППЫ $\mathbb{Z}_{\geq 0}^n$

Мы будем работать в кольце многочленов $F[x_1, \dots, x_n]$. Договоримся называть *моном* выражение $x_1^{a_1} \dots x_n^{a_n}$, где a_i — неотрицательные целые числа. *Термом* будем называть одночлен, то есть, моном с коэффициентом. Моноид мономов изоморфен моноиду $\mathbb{Z}_{\geq 0}^n$. Иногда нам будет удобнее говорить о мономах в аддитивном смысле именно как об элементах $\mathbb{Z}_{\geq 0}^n$. Следуя книге [1], рассмотрим «свойство конечности» этой полугруппы.

Определение 1.1. *Идеалом* полугруппы $\mathbb{Z}_{\geq 0}^n$ называется всякое ее подмножество, содержащее вместе с каждой точкой α и точку $\alpha + \gamma \ \forall \gamma \in \mathbb{Z}_{\geq 0}^n$.

Определение 1.2. *Октантом* $O(\alpha)$ с центром в точке α называется множество $\{\alpha + \gamma \mid \gamma \in \mathbb{Z}_{\geq 0}^n\}$.

Ясно, что октант является идеалом, и что идеал вместе с каждой своей точкой содержит весь октант с центром в ней.

Теорема 1.3 (Свойство конечности полугруппы $\mathbb{Z}_{\geq 0}^n$). *Всякий идеал в $\mathbb{Z}_{\geq 0}^n$ является объединением конечного числа октантов.*

Доказательство. □

Определение 1.4. Подмножество $\mathbb{Z}_{\geq 0}^n$ называется *коидеалом*, если его дополнение — идеал.

Следствие 1.5. *Всякий мономиальный идеал в $F[x_1, \dots, x_n]$ конечно порожден.*

Следствие 1.6 (Лемма Диксона). *Пусть $M_1, \dots, M_s, \dots$ — бесконечная последовательность мономов. Тогда обязательно найдутся два монома M_i и M_j , такие, что $M_i \mid M_j$.*

Предложение 1.7. *Моном M принадлежит мономиальному идеалу $(M_1, \dots, M_s)$ тогда и только тогда, когда $M_i \mid M$ для некоторого i .*

Далее нам понадобится понятие допустимого упорядочения на мономах, чтобы можно было выбирать «старший моном» в многочленах.

Определение 1.8. (Допустимым) мономиальным упорядочением $\prec$ на $\mathbb{M}_n$ называется линейный порядок, удовлетворяющий свойствам:

- (1) $M \prec N \implies MP \prec NP \ \forall M, N, P \in \mathbb{M}_n$;
- (2) $1 \prec M \ \forall M \in \mathbb{M}_n$.

Определение 1.9. Пусть $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{R}^n$. Вектор a *лексикографически младше* вектора b ($a \prec_{\text{lex}} b$), если существует такое $k, 0 \leq k < n$, что $a_i = b_i$ для всех натуральных $i \leq k$, но $a_{k+1} < b_{k+1}$. Аналогично будем сравнивать векторы-столбцы.

Примеры. Зафиксируем порядок на переменных (положив, например, $x_1 \prec x_2 \prec \dots \prec x_n$). Пусть $M = x_1^{a_1} \dots x_n^{a_n}$ и $N = x_1^{b_1} \dots x_n^{b_n}$ — произвольные мономы из $\mathbb{M}_n$. Следующие бинарные отношения на $\mathbb{M}_n$ являются мономиальными упорядочениями:

- (1) *Лексикографическое упорядочение (lex):*

$$M \prec_{\text{lex}} N \iff (a_1, \dots, a_n) \prec_{\text{lex}} (b_1, \dots, b_n).$$

- (2) *Сначала по степени, затем лексикографическое упорядочение (deglex):*

$$M \prec_{\text{deglex}} N \iff (\deg M, a_1, \dots, a_n) \prec_{\text{lex}} (\deg N, b_1, \dots, b_n).$$

- (3) *Сначала по степени, затем обратное лексикографическое упорядочение (degrevlex):*

$$M \prec_{\text{degrevlex}} N \iff (\deg M, b_n, \dots, b_1) \prec_{\text{lex}} (\deg N, a_n, \dots, a_1).$$

Предложение 1.10. *Любое мономиальное упорядочение вполне упорядочивает множество $\mathbb{M}_n$ (то есть, любая убывающая цепочка мономов обрывается).*

Зафиксируем некоторое упорядочение на мономах. Будем обозначать через $\text{LM } f$ старший моном ненулевого многочлена f , а через $\text{LM } I$ множество старших мономов ненулевых элементов из I .

Теорема 1.11. Пусть I — идеал в $F[x_1, \dots, x_n]$. Рассмотрим его как векторное пространство над F . Пусть подпространство L порождено всеми мономами, не принадлежащими $\text{LM } I$. Тогда справедливо разложение векторных пространств

$$F[x_1, \dots, x_n] = I \oplus L.$$

Доказательство. □

Определение 1.12. Система образующих G идеала I называется его *базисом Грёбнера*, если $(\text{LM } G) = (\text{LM } I)$.

Следствие 1.5 показывает, что у каждого идеала существует конечный базис Грёбнера. Действительно, достаточно взять многочлены $g_1, \dots, g_s \in I$, такие, что $\text{LM } g_1, \dots, \text{LM } g_s$ порождают мономиальный идеал $(\text{LM } I)$.

Следствие 1.13 (Теорема Гильберта о базисе). *Кольцо многочленов $F[x_1, \dots, x_n]$ нётерово, то есть, всякий идеал в нем конечно порожден.*

Задача 1.1. Для всякого подмножества $I \subset \{1, \dots, n\}$ можно рассмотреть подполугруппу

$$\mathbb{Z}_{\geq 0}^n(I) := \{(a_1, \dots, a_n) \in \mathbb{Z}_{\geq 0}^n \mid a_i = 0 \forall i \in I\}.$$

Сдвинутой координатной подполугруппой называется множество вида $\alpha + \mathbb{Z}_{\geq 0}^n(I)$, где $\alpha \in \mathbb{Z}_{\geq 0}^n$. Докажите, что всякий коидеал в $\mathbb{Z}_{\geq 0}^n$ является объединением конечного числа сдвинутых координатных подполугрупп.

Задача 1.2. Докажите, что из любой бесконечной последовательности мономов можно выбрать подпоследовательность, в которой каждый следующий моном делится на предыдущий.

Задача 1.3. Покажите, что в $F[x, y]$ упорядочения deglex и degrevlex совпадают.

Задача 1.4. Покажите, что на множестве мономов из $F[x, y]$ существует континуум различных упорядочений.

Задача 1.5. Зафиксируем лексикографический порядок с $x \succ y \succ z$. Верно ли, что множество $\{x - z^2, y - z^3\}$ является базисом Грёбнера идеала, порожденного этими двумя многочленами?

Задача 1.6. Приведите пример ассоциативного коммутативного кольца с единицей, не являющегося нётеровым.

СПИСОК ЛИТЕРАТУРЫ

- [1] А. Г. Хованский, С. П. Чулков. Геометрия полугруппы $\mathbb{Z}_{\geq 0}^n$: приложения к комбинаторике, алгебре и дифференциальным уравнениям. М., МЦНМО, 2006.
- [2] Cox D., Little J., O'Shea D., *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, New York, NY: Springer, 1998. [Имеется перевод: Кокс Д., Литтл Дж., О'Ши Д., *Идеалы, многообразия и алгоритмы*, М., Мир, 2000.]
- [3] Hong H. and Weispfenning V., *Algorithmic Theory of Admissible Term Orders*, preprint, 1999.
- [4] Robbiano L., *Term Orderings on the Polynomial Ring*, in Proceedings of EUROCAL 85, Springer Lecture Notes in Computer Science 204, 513-517, 1985.
- [5] Robbiano L., *On the Theory of Graded Structures*, The Journal of Symbolic Computation, 2, 139-170, 1986.
- [6] Trevisan G., *Classificazione dei semplici ordinamenti di un gruppo libero commutativo con N generatori*, Rend. Sem. Mat. Padova, 22, 143-156, 1953.