КОМБИНАТОРНА ТЕОРИЯ НА ПРЪСТЕНИТЕ

чл.-кор. Веселин Дренски

Институт по математика и информатика на БАН, каб. 566
email: drensky@math.bas.bg, тел: 9792820

Въведение

1. За какво е този курс?

Веднаж Айнщайн е казал: "You do not really understand something unless you can explain it to your grandmother."

Ако се опитаме да обясним елементарно, без дефиниции и формули, на нашите баби (предполагайки, че те не са професионални математички) или на приятели студенти – филолози какво се съдържа в курса по аналитична геометрия, който току що сме взели, навярно би се получило следното. (Моля колегите да ме извинят за наивното тълкуване на съдържанието на курса.)

Основните действия в курса се развиват в равнината и пространството. Изучаваме два типа обекти – точки и вектори. Векторите могат да се събират и умножават с число. Кои са важните множества от вектори? В равнината това са правите, а в пространството – правите и равнините. За да измерваме колко са векторите в едно от тези множества и в кое множество има повече вектори, въвеждаме понятието размерност – правите са едномерни, а равнините двумерни. Векторите имат дължина, а всеки два вектора сключват ъгъл помежду си. На базата на дължината и ъгъла между вектори дефинираме скаларно произведение. Когато говорим за точки, е удобно да въведем координатна система. Координатите на една точка са нещо като нашия домашен адрес. В равнината има две координати, "улицата" и "номера" на къщата или блока, в които живеем. В пространството имаме нужда от още една координата – "етажа", на който се намира нашето жилище. Интересните множества от точки са решения на уравнения или системи от уравнения (криви и повърхнини). Смяната на базиса има за цел да се намери най-удобното представяне на кривите и повърхнините.

Ако се опитаме накратко да обясним какво се съдържа в курса по линейна алгебра, ще трябва да отбележим, че най-напред там се изучават системи от линейни уравнения – начини за решаване, как да познаем дали една система е съвместима и колко решения има (от колко параметъра зависят решенията). По естсетвен начин

се стига до понятията вектори и матрици и операции с тях. Понататък се появяват линейните пространства над числови или произволни полета, като обобщения на множествата от векторите в равнината и пространството. Размерността на линейното пространство показва колко голямо е то (и от колко параметъра зависят неговите елементи). Необходимо е да се научим да сменяме базиса, за да подберем най-подходящия базис за задачата, която решаваме. След това се появяват линейните оператори и се търсят такива базиси, спрямо които операторите (и по-точнио техните матрици) имат възможно най-проста форма. Разглеждат се и линейни пространства с допълнителна структура – скаларно произведение и се изучават линейните оператори, които "се държат добре" спрямо скаларното произведение. Накрая се изучават билинейни и квадратични форми и се оказва, че тяхната теория е тясно свързана с теорията на матриците и на линейните оператори.

В курса по висша алгебра се изучават групи, пръстени и полета. Сред най-важните примери на пръстени са пръстените на полиномите и на квадратните матрици от даден ред. Броят на променливите в един полиномен пръстен може да се разглежда като мярка на това, колко са полиномите в пръстена и от колко параметъра зависят. Когато се разглеждат алгебрични уравнения и системи основните въпроси са как да решаваме уравненията и системите, имат ли те решения и колко са решенията. *Една от целите на настоящия курс е да дадем отговор на част от тези въпроси.*

Хомоморфизмите и изоморфизмите между групи и пръстени в курса по висша алгебра са аналог на линейните изображения от линейната алгебра. И докато общият вид на линейните изображения е ясен, а въпросът дали едно изображение между две крайномерни пространства се решава елементарно, то въпросът как изглеждат изоморфизмите между пръстените на полиномите е все още нерешена в общия случай задача. *В настоящия курс ще опишем изоморфизмите между пръстените на полиномите на две променливи. Ще покажем как да познаем дали един хомоморфизъм между два полиномни пръстена е изоморфизъм и ако това е така, как да намерим обратния изоморфизъм.*

"Комутатиивната" част от курса ще завърши с елементи от теория на инвариантите. Тази теория обобщава теорията на симетричните полиноми. Вместо "обикновените" симетрични полиноми, дефинирани чрез равенството

$$f(x_{\rho(1)}, \ldots, x_{\rho(n)}) = f(x_1, \ldots, x_n),$$

където ρ пробягва множеството на всички пермутации на числата $1, 2, \ldots, n$ в теория на инвариантите се разглеждат полиноми, които са "симетрични" относно произволна група от линейни оператори, действащи в n-мерното линейно пространство с базис $x_1, \ldots, x_n$.

Вторият раздел на курса съдържа елементи на теорията на некомутативните пръстени. Основният пример на некомутативен пръстен, с който сме се срещали в курсовете по алгебра е пръстенът на квадратниоте матрици от даден ред. Формулирана накратко, главната ни задача ще бъде да отговорим на въпроса: *Какво остава е вярно и какво е невярно в теория на пръстениет, ако се откажем от условието за комутативност?*

Накрая, в третия раздел, ще изучаваме пръстени, които "приличат" на комутативните и на матричните пръстени. Това са пръстените с полиномно тъждество. Това е област, която активно се развива по света през последните 60 години, а българската алгебрична група е една от активно работещите.

Основните обекти в курса са *алгебрите* над поле. Това са пръстени, които освен това имат структура на линейно пространство. Отново, типични примери са пръстените на полиномите с коефициенти от дадено поле и на квадратните матрици от даден ред, отново с елементи от дадено поле.

Защо *комбинаторна* теория на пръстените?

2. За кого е курсът?

Целта на курса е да запознае слушателя с основни резултати в комбинаторната теория на пръстените, с приложения в компютърната алгебра. Това ще му позволи да следи други курсове, които използват тази теория, както и да чете статии в съответните области. За следенето на курса ще бъдат достатъчни знанията от стандартните курсове по линейна и висша алгебра. Въпреки, че е изборен за бакалавърската програма, курсът ще бъде полезен и за студенти от магистърската програма и докторанти.

Предварителна програма

I. КОМУТАТИВНА АЛГЕБРА:

1. Компютърен подход към теория на идеалите в полиномни алгебри. Базиси на Грьобнер. Приложения: Работа във фактор-алгебри. Съвместимост на системи алгебрични уравнения.
2. Размерност на Гелфанд-Кирилов на крайно-породени комутативни алгебри.
3. Автоморфизми и дифереренцирания на полиномни алгебри. Алгоритъм за разпознаване на автоморфизмите и намиране на обратните им. Автоморфизми на полиномните алгебри на две променливи.
4. Теория на инвариантите на крайните групи. Теорема на Еми Ньотер за крайната породеност на алгебрата на инвариантите на крайна група. Формула на Молин за реда на Хилберт на алгебрата на инвариантите.

II. АСОЦИАТИВНИ АЛГЕБРИ:

5. Базиси на Грьобнер в свободната асоциативна алгебра.
6. Приложения на базисите на Грьобнер: Грасманова алгебра. Алгебри на Клифорд. Теорема на Поанкаре-Биркхоф-Вит за универсалните обвиващи на алгебрите на Ли и теорема на Вит за свободната алгебра на Ли.
7. Алгебри с междинен ръст.
8. Размерност на Гелфанд-Кирилов. Възможни стойности за размерността.
9. Проблеми на Бърнсайд и Курош. Контрапримери на Голод и Шафаревич.

III. АЛГЕБРИ С ПОЛИНОМНИ ТЪЖДЕСТВА (PI-АЛГЕБРИ)

10. Тъждества в грасмановата алгебра и алгебрата на горнотриъгълните матрици.
11. Тъждества в матричните алгебри. Теорема на Амицур-Левицки и централни полиноми.
12. Теорема на Нагата-Хигман за нилпотентност на нил-алгебрите от ограничен индекс.
13. Теореми на Регев за ръста на коразмерностите и за тензорното произведение на PI-алгебри.

14. Теорема на Ширшов за височината. Следствия: Положително решение на проблема на Курош за PI-алгебри. Теорема на Берел за крайната размерност на Гелфанд-Кирилов на крайно-породените PI-алгебри.

Литература

[AL] W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Math. 3, AMS, Providence, R.I., 1994.

[D] V. Drensky, Free Algebras and PI-Algebras, Springer, Singapore, 1999.

[H] I.N. Herstein, Noncommutative Rings, Carus Math. Monographs 15, Wiley and Sons, Inc., New York, 1968 (има руски превод).

[KL] G.R. Krause, T.H. Lenegan, Growth of Algebras and Gelfand-Kirillov Dimension, Pitman Publ., London, 1985 (Second edition by AMS).

[S] T.A. Springer, Invariant Theory, Lect. Notes in Math. 585, Springer-Verlag, 1977 (има руски превод).

[U] V.A. Ufnarovsky, Combinatorial and asymptotic methods in algebra, in A.I. Kostrikin, I.R. Shafarevich (Eds.), "Algebra VI", Encyclopaedia of Mathematical Sciences 57, Springer-Verlag, 1995, 1-196 (има руски оригинал).

1. Полиномни алгебри и техните идеали

1. Основни дефиниции

Ще фиксираме следните означения:
K е произволно поле, например полето на рационалните числа $\mathbb{Q}$, на реалните числа $\mathbb{R}$, на комплексните числа $\mathbb{C}$ или крайното поле $\mathbb{F}_q$ с q елемента, където $q = p^m$ за някое просто число p и естествено число m, и т.н. Елементите на K ще наричаме скалари или константи. Обикновено ще означаваме скаларите с малки гръцки букви. Всички линейни пространства са над фиксираното поле K.

Дефиниция 1. Линейното пространство R се нарича *асоциативна алгебра*, ако в R е дефинирана бинарна операция $\cdot$ (т.е. изображение $(R, R) \to R$), наречена *умножение* такава, че R е пръстен относно събирането и умножението, и за произволни два елемента $a, b \in R$ и произволна константа $\alpha \in K$

$$\alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b).$$

С други думи, понятието алгебра едновременно обобщава понятията линейно пространство и пръстен. Ако искаме изрично да отбележим, че R е алгебра над K, ще казваме, че R е K-алгебра. Алгебрата R е с 1 (или *унитарна*), ако R има единица като пръстен. Обикновено ще предполагаме, че алгебрите са с 1. Алгебрата е *комутативна*, ако удовлетворява условието

$$a \cdot b = b \cdot a$$

за всички $a, b \in R$. Често ще изпускаме знака за умножение $\cdot$ и ще означаваме $a \cdot b$ с ab.

Примери 2. (а) Полето K е комутативна алгебра относно обичайните операции. Всяко разширение L на полето K е също комутативна K-алгебра.

(б) Пръстенът на полиномите на една променлива $K[x]$ е алгебра. Друг пример е полето от рационални функции $K(x)$. По дефиниция, $K(x)$ се състои от всички дроби $f(x)/g(x)$ на два полинома $f(x)$ и $g(x)$, където $g(x) \neq 0$. Ще припомним, че обикновено в курса по алгебра не разглеждаме полиномите като функции и $g(x) \neq 0$ означава, че поне един от коефициентите на $g(x)$ не е равен на нула.

(в) Пръстенът на полиномите $K[x_1, \ldots, x_n]$ на n (фиксиран брой) променливи $x_1, \ldots, x_n$ също е алгебра. Когато работим с полиноми на малък брой променливи, обикновено ще означаваме променливите с x, y, z и т.н.

(г) Пръстенът на матриците от n-ти ред $M_n(K)$ с елементи от K е пример на некомутативна алгебра.

Дефиниция 3. Линейното подпространство S на алгебрата R се нарича *подалгебра*, ако е затворено относно умножението. (Когато разглеждаме алгебри с единица ще предполагаме, че единицата винаги се съдържа в подалгебрите. Разбира се, тогава алгебрите винаги съдържат полето K като подлагебра.) Подалгебрата S е породена от подмножеството от свои елементи $\{s_1, s_2, \ldots\}$ (наричани *пораждащи на* S), ако всеки елемент $s \in S$ може да се представи като крайна сума от вида

$$s = \sum \alpha_i s_{i_1} \cdots s_{i_k}, \quad \alpha_i \in K.$$

Понякога ще означаваме това с $S = K[s_1, s_2, \ldots]$ в комутативния и с $S = K\langle s_1, s_2, \ldots\rangle$ в некомутативния случай. Когато $S = K[s_1, s_2, \ldots]$, обикновено от контекста ще става ясно дали $s_1, s_2, \ldots$ са променливи (т.е. S е полиномна алгебра на много (дори безкрайно много) променливи, или $s_1, s_2, \ldots$ са просто пораждащите на S. Подалгебрата S е *крайно породена*, съответно *n-породена*, ако може да бъде породена от краен брой елементи, съответно от множество с n елемента. Линейното подпространство J на R се нарича *идеал*, ако за всеки $u \in J$ и всеки $a \in R$ произведенията ua и au принадлежат на J (означаваме това свойство с $RJ \subseteq J$ и $JR \subseteq J$). Идеалът J е породен от множеството $U = \{u_1, u_2, \ldots\}$, а съответното означение е $J = (U)$, ако всеки елемент $u \in J$ е от вида

$$u = \sum a_i u_i b_i, \quad a_i, b_i \in R.$$

Понятията крайна породеност и n-породеност на идеали са подобни на тези за подалгебри. В случая на комутативни алгебри идеалът J е *главен*, ако се поражда от един елемент, т.е. съществува елемент $u_0 \in J$ такъв, че $J = (u_0) = \{au_0 \mid a \in R\}$.

Понятието фактор-алгебра R/J на алгебрата R по модул идеала J е подобно на съответното понятие за пръстени. Основните теореми за идеали и фактор-пръстени са в сила и за алгебри. В частност, елементите на R/J са съседните класове $a + J = \{a + u \mid u \in J\}$, а операциите са дефинирани чрез

$$(a + J) + (b + J) = (a + b) + J,$$
$$\alpha(a + J) = (\alpha a) + J,$$
$$(a + J)(b + J) = ab + J.$$

Понятията хомоморфизъм и изоморфизъм са също подобни на тези за пръстени. (Ако $\varphi : R \to S$ е хомоморфизъм на алгебри, ще

предполагаме, че $\varphi(\alpha a) = \alpha\varphi(a)$ за всички $\alpha \in K$ и $a \in R$. За алгебри с единица ще искаме $\varphi(1_R) = 1_S$.) В частност, хомоморфизмите $R \to R$ се наричат *ендоморфизми*, а изоморфизмите $R \to R$ са *автоморфизми*.

В теория на множествата има т.н. *аксиома за избора*. Неформално формулирана, аксиомата за избора твърди, че ако имаме известно количество чекмеджета, всяко от които съдържа поне един предмет, то е възможно да изберем точно един предмет от всяко чекмедже, даже ако чекмеджетата са безкрайно много и няма "правило", по което да направим избора. Аксиомата за избора е формулирана за пръв път от Ернст Цермело през 1904 год. Известно е, че тя е независима от останалите обичайни аксиоми в теория на множествата и част от математиците не я използват в своите изследвания. Днес аксиомата за избора (и преди всичко нейните следствия) се използват от повечето математици. Може би главната причина за това е, че тя се използва съществено при доказателствата на множество известни теореми. Аксиомата на избора е еквивалентна на няколко други твърдения, едно от които е лемата на Макс Цорн. (Оригиналната статия на Цорн [Z] може да бъде изтеглена от Интернет.) По-долу ще направим едно приложение на Лемата на Цорн, което е в основата на много алгебрични разсъждения.

Дефиниция 4. Казваме, че в множеството A е зададена *частична наредба*, ако в A е дефинирана бинарна релация $<$, при която за някои двойки различни елементи a_1, a_2 на A казваме, че $a_1 < a_2$, при което са изпълнени условията:

(а) Не е възможно едновременно да се изпълняват $a_1 < a_2$ и $a_2 < a_1$.

(б) Ако $a_1 < a_2$ и $a_2 < a_3$, то $a_1 < a_3$ (транзитивност).

Лема 5. (Лема на Цорн) *Нека A е множество с частична наредба такава, че за всяка растяща редица $a_1 \leq a_2 \leq \cdots$ от елементи в A съществува елемент $a \in A$ със свойството, че $a_i \leq a$, $i = 1, 2, \ldots$ Тогава множеството A съдържа максимален елемент (който не е по-малък от никой елемент на A).*

Лема 6. *Ако R е пръстен с 1, то всеки идеал на R (който се съдържа строго в R) се съдържа в максимален идеал.*

Proof. Нека J е идеал на алгебрата R, който се съдържа строго в R и нека A е множеството на всички идеали, съдържащи J и различни от R. Нека $J_1 \subseteq J_2 \subseteq \cdots$ е растяща редица от идеали,

съдържащи J. Както в случая на пръстени се доказва, че обединението

$$J_\infty = \bigcup_{n\geq 1} J_n$$

е идеал на R. Тъй като единицата на R не принадлежи на никой идеал J_n (ако $1 \in J_n$, то $J_n = R$), то тя не принадлежи и на обединението J_∞. Следователно, $J_\infty \in A$. От лемата на Цорн следва, че в множеството A има максимален елемент, т.е. такъв идеал, който съдържа J и не се съдържа в по-голям собствен идеал на R. □

Упражнение 7. Да се докаже, че един идеал J на комутативната алгебра с единица R е максимален тогава и само тогава, когато фактор-алгебрата R/J е поле.

Дефиниция 8. Нека $f_i(X) = f_i(x_1, \ldots, x_n) \in K[X] = K[x_1, \ldots, x_n]$, $i \in I$, са полиноми на n променливи. Системата от алгебрични уравнения

$$f_i(X) = 0, \quad i \in I,$$

е *съвместима*, ако системата има решение в някакво разширение на основното поле.

Следното твърдение е известно като *Слаба форма на теоремата на Хилберт за нулите.*

Твърдение 9. *Системата*

$$f_i(X) = 0, \quad i \in I,$$

е съвместима тогава и само тогава, когато идеалът

$$J = (f_i(X) \mid i \in I),$$

породен от полиномите $f_i(X)$, не съвпада с цялата алгебра R.

Proof. Нека системата е съвместима и има решение $\Xi = (\xi_1, \ldots, \xi_n)$ в някакво разширение L на основното поле K. Да разгледаме хомоморфизма $\pi : K[X] \to L$ дефиниран чрез $\pi(x_j) = \xi_j$, $j = 1, \ldots, n$. Ядрото $\mathrm{Ker}(\pi)$ на π е идеал в $K[X]$, който се съдържа строго в R (защото $\pi(1) = 1 \neq 0$ и $1 \notin \mathrm{Ker}(\pi)$). Освен това, $\pi(f_i) = f_i(\Xi) = 0$ и $f_i \in \mathrm{Ker}(\pi)$. Следователно, идеалът J, породен от f_i-тата, се съдържа в $\mathrm{Ker}(\pi)$. Обратно, нека J се съдържа строго в $K[X]$. Тогава J се съдържа в максимален идеал M на $K[X]$. Да разгледаме естествения хомоморфизъм $\varphi : K[X] \to K[X]/M$ с ядро M. Тъй като ядрото е максимален идеал, то фактор-алгебрата $K[X]/M$ е изоморфна на поле L, което е разширение на K. Нека

$\zeta_j = \varphi(x_j) \in L$, $j = 1, \ldots, n$. Тогава $\varphi(f_i) = f_i(\zeta_1, \ldots, \zeta_n) = 0$ в L, т.е. системата е съвместима. $\square$

Забележка 10. Може да се докаже, че системата $f_i(X) = 0$, $i \in I$, има краен брой решения тогава и само тогава, когато идеалът $J = (f_i(X) \mid i \in I)$ е от крайна коразмерност в $K[X]$, т.е. факторалгебрата $K[X]/J$ е крайномерна (като линейно пространство над K).

Литература

[AL] W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Math. 3, AMS, Providence, R.I., 1994.

[AM] M.F. Atiyah, I.G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass. 1969. (Има руски превод.)

[BW] T. Becker, V. Weispfenning, Groebner Bases: A Computational Approach to Commutative Algebra, in cooperation with H. Kredel, Graduate Texts in Math. **141** Springer-Verlag, New York, 1993.

[L] S. Lang, Algebra, Third Edition, Addison-Wesley, Reading, Mass. 1993. (Има руски превод.)

[Z] M. Zorn, A remark on method in transfinite algebra, Bull. Amer. Math. Soc. **41** (1935), 667-670. (Може да бъде изтеглена от http://www.ams.org/bull/1935-41-10/S0002-9904-1935-06166-X/S0002-9904-1935-06166-X.pdf.)