Нётеровость, конечность, целостность

§1. О нетеровости колец

Коммутативное ассоциативное кольцо A называется *нетеровым*, если выполнено одно из перечисленных ниже эквивалентных условий:

1) любой идеал $I \subset A$ является конечным A-модулем, то есть существует такая конечная коллекция элементов $\{i_1, \ldots, i_t\}$ из идеала I, что любой элемент $i \in I$ записывается в виде $i = a_1 i_1 + \cdots + a_t i_t$, $a_i \in A$;

2) любая возрастающая последовательность идеалов из A стабилизируется, т.е. если $I_1 \subseteq I_2 \subseteq \ldots$, то начиная с некоторого n $\quad I_n = I_{n+1} = \ldots$.

Контрольный вопрос. Как бы вы определили нетеров модуль?

Образцом использования понятия нетеровости и по сей день служит гильбертово доказательство следующей теоремы.

> *Теорема Гильберта о базисе.* Если кольцо A нетерово, то и кольцо многочленов $A[T]$ нетерово.
>
> *Следствие.* Если кольцо A нетерово, то и кольцо многочленов от n переменных $A[T_1, T_2, \ldots, T_n]$ нетерово.

Докажем, следуя идее Гильберта, нетеровость кольца формальных степенных рядов $A[\,[T]\,]$ над нетеровым кольцом A.

Доказательство. Напомним, что формальным степенным рядом называется выражение вида $\sum\limits_{m=0}^{\infty} a_m T^m$, где коэффициенты a принадлежат кольцу A. Два формальных ряда $\sum a_m T^m$ и $\sum b_m T^m$ можно сложить: $\sum a_m T^m + \sum b_m T^m = \sum (a_m + b_m) T^m$ и можно перемножить по "правилу свертки":

$$\left(\sum a_m T^m\right) \times \left(\sum b_m T^m\right) = \sum c_k T^k, \quad \text{где } c_k = \sum_{\substack{n,m \\ n+m=k}} a_m b_n$$

Первый не равный нулю коэффициент формального ряда называется его *началом.*

Пусть I — идеал в кольце $A[\,[T]\,]$. Рассмотрим коллекцию $J_k = \{a \in A \mid a$ – начало с номером k некоторого ряда из $I\}$. J_k — не просто подмножество в A, а абелева группа и, более того, идеал кольца A (почему?). Ясно также, что $J_0 \subset J_1 \subset J_2 \subset \ldots$ (почему?). Возрастающая цепочка идеалов J_k стабилизируется по причине нетеровости кольца A. Следовательно, все начала лежат в некотором идеале $J_n \in A$.

Пусть $a_{1n}, a_{2n}, \ldots, a_{\ell n}$ — конечная система образующих идеала J_n над A. Рассмотрим формальные ряды вида $\tau_i(T) = a_{in} T^n + \ldots$ из идеала J_n. Покажем, что любой формальный ряд τ, начинающийся со степени $N \geqslant n$, записывается в виде линейной комбинации рядов τ_i с коэффициентами из кольца $A[\,[T]\,]$.

В самом деле, пусть a_N — начало τ. Тогда

$$a_N = q_{10}a_{1n} + \cdots + q_{\ell 0}a_{\ell n}, \quad q_j \in A$$

Рассмотрим ряд $\tau - q_{10}T^{(N-n)}\tau_1 - q_{20}T^{(N-n)}\tau_2 - \cdots - q_{\ell 0}T^{(N-n)}\tau_\ell = \tilde{\tau}_1$. Он начинается со степени $\tilde{a}_{N+1}T^{N+1} + \cdots$. Снова имеем $\tilde{a}_{N+1} = q_{11}a_{1n} + \cdots + q_{\ell 1}a_{\ell n}$, и снова рассмотрим ряд

$$\tilde{\tau}_1 - T^{(N-n+1)}q_{11}\tau_1 - T^{(N-n+1)}q_{21}\tau_2 - \cdots - T^{(N-n+1)}q_{\ell 1}\tau_\ell = \tilde{\tau}_2,$$

который начинается со степени T^{N+2}, и так далее.
В итоге, шаг за шагом, мы получим искомое представление ряда τ в виде

$$\tau = T^{N-n}(q_{10} + q_{11}T + q_{12}T^2 + \cdots)\tilde{\tau}_1 + T^{N-n}(q_{20} + q_{21}T + \cdots)\tilde{\tau}_2 + \cdots + T^{N-n}(q_{\ell 0} + q_{\ell 1}T + \cdots)\tilde{\tau}_\ell$$

Остается понять, что делать с формальными рядами, которые начинаются со степеней, меньших n. Выберем конечную систему образующих $\{a_{1i}, \ldots, a_{?i}\}$ идеала J_i, $0 \leqslant i < n$. Пусть τ_{qi} — формальный ряд с началом $a_{qi}T^i$. Несложно проверить, что если к коллекции $\{\tau_1, \ldots, \tau_\ell\}$ добавить конечное число рядов τ_{qi}, $i = 0, \ldots, n-1$, то получится система образующих идеала I над кольцом $A[\,[T]\,]$ (убедитесь в этом сами). □

Контрольный вопрос. Как доказать теорему Гильберта для кольца $A[T]$?

Подкольцо нетерова кольца не обязано быть нетеровым (пример?).

Докажем, что факторкольцо нетерова кольца по идеалу J нетерово. В самом деле, рассмотрим фактор-кольцо $\overline{A} = A/J$, и пусть $a \mapsto \overline{a}$ — канонический гомоморфизм $A \longrightarrow \overline{A} = A/J$. Если $\overline{I}$ — идеал в $\overline{A}$, то его полный прообраз I является идеалом в кольце A (почему?). Поскольку A нетерово, $I = Ai_1 + \cdots + Ai_s$. Но тогда $\overline{I} = \overline{A}\,\overline{i}_1 + \cdots + \overline{A}\,\overline{i}_s$, ч.т.д.

Заметим, что любое конечно порожденное надкольцо кольца A (т.е. кольцо $B = A[\alpha_1, \ldots, \alpha_m]$, $\alpha_i \in B$) является фактор-кольцом кольца многочленов $A[T_1, \ldots, T_m]$ (почему?). Отсюда следует (как?), что конечно порожденное расширение нетерова кольца — нетерово.

Две "конечности"

Пусть A — коммутативное ассоциативное кольцо с единицей и без делителей нуля.

Если $B \supset A$ — надкольцо кольца A, то B можно рассматривать как A-модуль. В связи с этим напомним, что A-модуль M называется *конечным A-модулем*, если каждый элемент M записывается как линейная комбинация фиксированной коллекции элементов $\{y_1, \ldots, y_t\} \in M$ с коэффициентами из A. Коллекцию $\{y_1, \ldots, y_t\}$ будем называть *образующими модуля M над кольцом A*.

$$m = \sum a_i y_i, \quad a_i \in A,\ m \in M$$

Определение. Говорят, что надкольцо B *конечно над* A, если B — конечный модуль над A.

С другой стороны, надкольцо B называется конечно порожденным над A, если $B = A[x_1, \ldots, x_s]$, $x_i \in B$, т.е. любой элемент B записывается как многочлен от фиксированной коллекции $\{x_1, \ldots, x_s\}$ элементов B с коэффициентами из A.

Таким образом, в алгебре естественно возникают два понятия "конечности". Во-первых, их не следует путать.

> *Пример 1.* Кольцо p-дробей $\mathbb{Z}[\frac{1}{p}]$, p – простое, конечно порождено над $\mathbb{Z}$, но не конечно над $\mathbb{Z}$. (Почему?)

Во-вторых, интересно исследовать взаимосвязь этих понятий.

§2. Простое расширение конечно, если оно цело

Начнем с простого расширения $B = A[z]$.

> *Теорема 1 (О простом расширении).* Простое расширение $A[z]$ конечно тогда и только тогда, когда есть такой набор $a_i \in A$, что $z^N + a_{N-1}z^{N-1} + \cdots + a_0 = 0$.
>
> *Определение.* Если элемент z из некоторого надкольца кольца A удовлетворяет уравнению $z^N + a_{N-1}z^{N-1} + \cdots + a_0 = 0$ с некоторыми $a_i \in A$, то говорят, что z *цел над* A.

Доказательство. Пусть простое расширение $B = A[z]$ конечно.
Выберем конечную систему образующих $\{y_1, \ldots, y_s\}$ B над A. Тогда

$$zy_i = \sum_{j=1}^{s} v_{ij} y_j, \quad i = 1, \ldots, s, \quad v_{ij} \in A \tag{$*$}$$

или в матричном виде

$$(zE - V) \begin{pmatrix} y_1 \\ \vdots \\ y_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \text{где } V = (v_{ij}). \tag{$**$}$$

Воспользуемся теперь хорошо известным фактом из теории матриц:
пусть P — квадратная матрица, а $\hat{P}$ — матрица, полученная из P заменой каждого матричного элемента p_{ij} его алгебраическим дополнением $\hat{p}_{ij}$. Тогда из теоремы о разложении определителя по строке следует, что

$$\hat{P}^T P = P \hat{P}^T = (\det P)E$$

При этом, если P — матрица с элементами из кольца W, то и $\hat{P}$ — матрица с элементами из W.

Возвращаясь к системе ($**$) и умножая обе ее части на матрицу $\widehat{zE - V}^T$, получаем

$$\det(zE - V) \begin{pmatrix} y_1 \\ \vdots \\ y_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

т.е. элемент $\det(zE - V)$ кольца B аннулирует каждую из образующих y_i. Но тогда он аннулирует и все элементы B. В частности, он аннулирует 1, а значит $\det(zE - V) = 0$. Но это означает, что z удовлетворяет уравнению $f_V(T) = 0$, где $f_V(T) = \det(TE - V)$ — характеристический многочлен матрицы V.
Тем самым, мы показали, что z цел над A.

Важное замечание. Только что мы доказали очень полезное утверждение:

> *Теорема 2 ("Конечен будешь – цел будешь").* Если надкольцо B конечно над A, то любой элемент $z \in B$ цел над A.

Продолжим доказательство теоремы 1. Осталось показать, что если z цел над A, то простое расширение конечно. Пусть $z^N + a_{N-1}z^{N-1} + \cdots + a_0 = 0$. Тогда A-модуль $B = A[z]$ порождается над A элементами $1,\ z,\ z^2, \ldots, z^{N-1}$. (Проверьте это.) $\square$

Закончим параграф таким определением:

> *Определение.* Надкольцо B *цело над кольцом* A, если любой элемент B цел над A. (Также говорят о *целом расширении* колец $B > A$.)

> *Пример 2.* Кольцо $k[X]$ цело над кольцом $k[X^2]$. (Почему?)

§3. Конечные и целые расширения

Утверждение. Если имеется башня расширений колец $A < B < C$, причем B конечно (цело) над A, а C конечно (цело) над B, то надкольцо C конечно (цело) над A.

Утверждение о башне конечных расширений колец доказывается так же, как и соответствующее утверждение о конечной башне полей (советую вспомнить это простое рассуждение). Докажем наше утверждение для башни целых расширений.

Рассмотрим элемент $z \in C$. Поскольку он цел над B, то

$$z^N + b_{N-1}z^{N-1} + \cdots + b_0 = 0, \text{ где } b_i \in B.$$

Рассмотрим расширение $A[z,\ b_{N-1},\ b_{N-2}, \ldots, b_0]$ кольца A, полученное присоединением к A элементов z, b_{N-1}, b_{N-2}, $\ldots$, b_0. Это можно сделать, построив башню простых расширений

$$A[z,\ b_{N-1},\ b_{N-2}, \ldots, b_0] > A[b_{N-1},\ b_{N-2}, \ldots, b_0] > A[b_{N-2}, \ldots, b_0] > \cdots A[b_0] > A.$$

Так как элементы $b_i \in B$ целы над A, а элемент z цел над $A[b_{N-1}, \ldots, b_0]$, то все расширения в построенной башне целы (почему?), а так как они просты, то, по теореме 1, они конечны. В итоге мы построили башню конечных расширений. Следовательно, надкольцо $A[z,\ b_{N-1},\ b_{N-2}, \ldots, b_0]$ конечно над A. Тогда, по теореме 2, элемент $z \in C$ цел над A, что и требовалось доказать. $\square$

§4. Вариация на тему Галуа

Пусть G — конечная группа автоморфизмов кольца B.

Пример 3.

1) Группа $\mathbb{Z}_2 = \langle 1, \sigma \rangle$ действует в кольце многочленов $k[T]$ над полем или кольцом k по формуле $(T)^\sigma = -T$, $x^\sigma = x$, $x \in k$.

2) Конечная матричная группа $G \in GL_n(k)$ действует линейными заменами переменных $T_i \longrightarrow \sum g_{ij} T_j$ в кольце многочленов $k[T_1, \ldots, T_n]$ (при этом G тождественно действует на k).

Рассмотрим кольцо неподвижных элементов B^G (почему это кольцо?).
Возникают два важных (в теории инвариантов) вопроса:

а) Пусть $B > B^G > A$ и B конечно над A. Верно ли, что B^G конечно над A?

б) В той же ситуации, пусть B конечно порождено над A. Верно ли, что кольцо инвариантов B^G конечно порождено над A?

Попробуем ответить на эти вопросы. Но сначала отметим следующий факт:

Теорема 3. Кольцо B цело над кольцом инвариантов B^G.

Доказательство. Пусть $z \in B$, $\sigma \in G$. Рассмотрим G-орбиту $\{z^\sigma\}$ элемента z и построим многочлен

$$F(T) = \prod_{\{z^\sigma\}} (T - z^\sigma)$$

Коэффициенты этого многочлена лежат в кольце B^G (почему?), и его коэффициент при старшей степени равен 1. Кроме того, z — корень многочлена $F(T)$. Все это означает, что элемент $z \in B$ цел над кольцом инвариантов B^G. $\Box$

Теперь частичный ответ "да" на вопрос б) дает следующее общее утверждение:

Теорема 4. Пусть $B > C > A$ — башня колец. Предположим, что кольцо A нетерово, B конечно порождено над A, и B цело над C. Тогда C конечно порождено над A.

Доказательство. По условию, $B = A[x_1, \ldots, x_n]$. Каждый элемент x_i цел над C, т.е. является корнем многочлена $f_i(T) \subset C[T]$. Присоединим к кольцу A коэффициенты всех многочленов $f_i(T)$, $i = 1, \ldots, n$. Получим конечно порожденное расширение $A' = A[c_1, \ldots, c_\ell]$ кольца A. Так как кольцо A нетерово, то и A' нетерово (почему?). Кольцо A' содержит A и содержится в C. Кольцо B цело над кольцом A' и конечно порождено над ним (почему?). По теореме 2, кольцо B конечно над A'. A'-подмодуль $C < B$ также конечен над A', т.к. A' нетерово (задача из листка №3). Обозначим через $\{w_1, \ldots, w_q\}$ образующие C над A'. Тогда $C = A[c_1, \ldots, c_\ell, w_1, \ldots, w_q]$. $\Box$

Если кольцо A нетерово, то положительный ответ на вопрос а) очевиден: кольцо инвариантов B^G конечно над A как A-подмодуль конечного A-модуля B над нетеровым кольцом.

Замечание. В классической теории инвариантов в качестве A чаще всего выступает поле, а оно нетерово. А как обстоят дела, если не требовать от A нетеровости?

§5. Целое замыкание. Кольцо целых алгебраических чисел (первое знакомство)

Пусть B — надкольцо A. Рассмотрим в B подмножество, состоящее из всех элементов, целых над A. Покажем, что это подмножество является кольцом (оно очевидным образом содержит кольцо A). Для этого достаточно проверить, что для любых z_1 и z_2 из B, целых над A, их сумма z_1+z_2 и произведение z_1z_2 целы над A. С этой целью рассмотрим конечно порожденное надкольцо $A[z_1,z_2]$, которое конечно над A (почему?). Но z_1+z_2 и z_1z_2 лежат в кольце $A[z_1,z_2]$, которое конечно, а потому цело над A.

Определение. Кольцо всех элементов B, целых над A, называется *целым замыканием кольца A в B*. Обозначим его $O_{A,B}$ или просто O_B, если ясно, о каком кольце A идет речь.

Пример 4.

а) целое замыкание $\mathbb{Z}$ в $\mathbb{Z}[\frac{1}{3}]$ равно $\mathbb{Z}$ (почему?)

б) целое замыкание $\mathbb{Z}$ в $\mathbb{Q}$ равно $\mathbb{Z}$ (почему?)

в) целое замыкание $\mathbb{Z}$ в $\mathbb{Q}(\sqrt{2})$ состоит из чисел вида $a+b\sqrt{2}$, $a,b\in\mathbb{Z}$ (хорошее упражнение на делимость целых чисел).

Упражнение. Как устроено целое замыкание кольца многочленов $\mathbb{Z}[x,y]$ в его поле частных $\mathbb{Z}(x,y)$?

Рассмотрим детальнее целое замыкание кольца $\mathbb{Z}$ в поле алгебраических чисел.

Определения.
Конечное расширение K поля $\mathbb{Q}$ называется *полем алгебраических чисел.*
Целое замыкание $\mathbb{Z}$ в K называется *кольцом целых поля K* и обозначается O_K.

Теорема 5. Кольцо O_K конечно над $\mathbb{Z}$.

Доказательство. Нам пригодится следующая техническая лемма.
Техническая лемма. Если $z\in K$, то $mz\in O_K$ для некоторого $m\in Z$.

Доказательство. Действительно, поскольку расширение K конечно над $\mathbb{Q}$, то оно алгебраично над $\mathbb{Q}$, а потому

$$a_Nz^N+a_{N-1}z^{N-1}+\cdots+a_0=0,\ \text{где все}\ a_i\in\mathbb{Z}$$

Умножив обе части равенства на a_N^{N-1}, получим

$$(a_Nz)^N+a_{N-1}(a_Nz)^{N-1}+a_{N-2}a_{N-1}(a_Nz)^{N-2}+\cdots+a_0a_N^{N-1}=0$$

По определению (a_Nz) является целым алгебраическим числом. □

Переходим к доказательству теоремы.
Конечность O_K над $\mathbb{Z}$ есть следствие дискретности абелевой группы O_K в группе K. Мы воспользуемся одним из проявлений дискретности: существованием невырожденной билинейной формы $\mathrm{tr}_{K/Q}(xy)$, принимающей на O_K целые значения (см. Дополнение 1).

Выберем базис $\alpha_1, \ldots, \alpha_n$ поля K над $\mathbb{Q}$. Можно считать (техническая лемма!), что все $\alpha_i \in O_K$. Через $\alpha_1^*, \ldots, \alpha_n^*$ обозначим двойственный базис K в смысле невырожденной билинейной формы $\mathrm{tr}_{K/Q}$ (напомним: это означает, что $\mathrm{tr}_{K/Q}(\alpha_i\alpha_j^*) = \delta_{ij}$). Пусть γ — произвольный элемент кольца O_K. Тогда

$$\gamma = \sum \gamma_i \alpha_i^*, \ \ \gamma_i \in \mathbb{Q}$$

Умножив обе части этого равенства на α_i и взяв от обеих частей след, получим

$$\mathrm{tr}_{K/Q}(\gamma\alpha_j) = \gamma_j \ \ \text{(почему?)}$$

Но слева стоит целое число (γ и α_j лежат в O_K!). Следовательно, абелева группа O_K лежит в конечно порожденной абелевой группе $\mathbb{Z}\alpha_1^* + \mathbb{Z}\alpha_2^* + \cdots + \mathbb{Z}\alpha_n^*$, а потому сама конечно порождена. $\square$

Итак, мы показали, что O_K - конечно порожденная абелева группа. Кроме того, в ней по очевидным причинам нет элементов конечного порядка. Следовательно, O_K — свободная абелева группа конечного ранга (решетка над $\mathbb{Z}$). А техническая лемма прямо указывает на то, что $\mathrm{rk}_{\mathbb{Z}}\, O_K = [K : \mathbb{Q}] = n$.

Насколько хороши кольца целых?
Пример кольца $O_{\mathbb{Q}(\sqrt{-5})}$, где $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ подсказывает, что вообще говоря, кольцо O_K не является факториальным, т.е. в нем отсутствует однозначность разложения на неразложимые множители. Отсутствие факториальности автоматически влечет присутствие в таком кольце неглавных идеалов, т.е. идеалов, которые (как O_K-модули) можно породить конечно, но нельзя породить одним элементом. (Вопрос: а двумя можно?)

К какому же естественному классу колец относятся кольца целых алгебраических чисел O_K? Вот ответ на этот вопрос.

> *Определение.* Нетерово кольцо без делителей нуля, целозамкнутое в своем поле частных, называется *дедекиндовым* (*арифметическим*), если все его ненулевые простые идеалы максимальны.

Упражнения.

1) $\mathbb{Z}$ — дедекиндово кольцо.
2) Не всякое факториальное кольцо дедекиндово (пример?).
3) Всякое ли кольцо главных идеалов дедекиндово?

§6. Кольцо целых алгебраических чисел дедекиндово

Пусть K — поле алгебраических чисел, O_K — кольцо целых поля K. Кольцо O_K — нетерово. В самом деле, O_K — конечный модуль над нетеровым кольцом $\mathbb{Z}$. Кольцо O_K целозамкнуто в своем поле частных $R(O_K) = K$ (здесь два "почему?"). Так как отсутствие делителей нуля в кольце O_K очевидно, то остается доказать, что любой ненулевой простой идеал $P \subset O_K$ максимален.

Доказательство. Сначала покажем, что $\mathbb{Z}$-модуль P представляет из себя подрешетку полного ранга в решетке O_K. Пусть $\gamma \in P$. Так как сдвиг γO_K решетки полного ранга является решеткой полного ранга, то идеал P (рассматриваемый как $\mathbb{Z}$-модуль) содержит подрешетку полного ранга γO_K. Следовательно, P — подрешетка полного ранга в O_K*. Но в таком случае фактор-кольцо O_K/P конечно (почему?). С другой стороны, фактор-кольцо O_K/P не содержит делителей нуля, так как идеал P прост. Остается заметить, что конечное коммутативное кольцо без делителей нуля есть поле (почему?). □

Мы еще раз вернемся к дедекиндовым кольцам, чтобы доказать их фундаментальное свойство: ненулевые идеалы дедекиндова кольца образуют полугруппу (по умножению) с однозначным разложением на простые множители.

Дополнения

Дополнение 1. Докажем невырожденность формы $\mathrm{tr}_{K/Q}$ в поле алгебраических чисел K. Предположим, что эта форма вырождена, т.е. существует такой ненулевой элемент ω из K, что $\mathrm{tr}_{K/Q}(\omega K) = 0$. В частности, $\mathrm{tr}_{K/Q}(\omega \frac{1}{\omega}) = 0$. С другой стороны, $\mathrm{tr}_{K/Q}(1) = n$. Противоречие.

Дополнение 2. Рассмотрим фундаментальный параллелепипед Π решетки O_K в вещественном векторном пространстве $K \otimes \mathbb{R}$. Его объем $\mathrm{Vol}\,\Pi$ является важным инвариантом поля K. Квадрат объема $(\mathrm{Vol}\,\Pi)^2$ называется дискриминантом поля K. Разумеется, $(\mathrm{Vol}\,\Pi)^2$ равен определителю матрицы Грама формы $\mathrm{tr}_{K/Q}$ в любом базисе решетки O_K.

Дополнение 3. Есть еще одно, эквивалентное двум уже имеющимся, определение нетеровости: кольцо A называется нетеровым, если любой непустой набор S собственных идеалов кольца A содержит максимальный элемент (т.е. такой идеал из S, который не содержится в виде собственного подмножества ни в каком другом идеале из S).

Новый лик нетеровости открывает путь *нетеровой индукции.*
Этот полезный прием состоит в следующем. Предположим, вы хотите доказать, что все идеалы нетерова кольца A обладают свойством (Ω). При этом вы умеете делать две вещи: а) проверять, что (Ω) верно для всего кольца A (база индукции), б) доказывать, что из того, что (Ω) верно для всех идеалов J, строго содержащих идеал I, следует, что оно верно и для самого I (шаг индукции). Тогда свойством (Ω) обладают все идеалы кольца A.

В самом деле, рассмотрим множество идеалов S, для которых свойство (Ω) не выполняется. Покажем, что S пусто. Действительно, если S не пусто, то рассмотрим его максимальный элемент. Он не может быть всем кольцом, а потому любой идеал, его строго содержащий, уже обладает свойством (Ω). Следовательно, он сам обладает свойством (Ω). С другой стороны, он лежит в S. Противоречие.

Литература

Э.Б.Винберг. *Курс алгебры.* Москва, Факториал, 2004
Ван дер Варден. *Алгебра.* Москва, Наука, 1976
С. Ленг. *Алгебра.* Москва, Мир, 1968

*Это изящное рассуждение сообщил мне Роман Гайдук