Т. XX Записки научно-исследовательского института математики и механики ХГУ и Харьковского математического общества 1950

А. К. СУШКЕВИЧ (*Харьков*)

ОБ ОДНОЙ ЛИНЕЙНОЙ АЛГЕБРЕ БЕСКОНЕЧНОГО ПОРЯДКА

§ 1. Как объекты нашего исчисления мы рассматриваем бесконечные последовательности целых чисел

$$A=(a_0|a_1, a_2, a_3, \ldots, \text{in inf}),$$

обозначая их большими латинскими буквами и называя «агрегатами»; отдельные целые числа $a_0, a_1, a_2, \ldots$, из которых состоит агрегат, мы называем его «элементами», первый элемент a_0 мы отделяем от остальных вертикальной чёрточкой. Для вычисления с агрегатами мы ставим следующие три постулата:

I. Постулат равенства. *A и $B=(b_0|b_1, b_2, \ldots)$ равны тогда и только тогда, если они тождественны, т. е. если* $a_n=b_n$ ($n=0, 1, 2, \ldots$ in inf).

II. Постулат сложения. $A+B=(a_0+b_0|a_1+b_1, a_2+b_2, \ldots)$.

III. Постулат умножения. $AB=(a_0b_0|a_0b_1+a_1b_0, a_0b_2+a_1b_1+a_2b_0, \ldots)$, *вообще* $(n+1)$-*й элемент произведения*:

$$a_0b_n+a_1b_{n-1}+a_2b_{n-2}+\cdots+a_nb_0.$$

Совокупность всевозможных наших агрегатов обозначим через A. Из поставленных постулатов следует:

1. *Сложение агрегатов коммутативно и ассоциативно.* A—обычная абелева группа относительно сложения. Агрегат $(0|0, 0, 0, \ldots)=0$—«нулевой», мы его просто обозначаем через 0; $A+0=0+A=A$.

Агрегат $-A=(-a_0|-a_1, -a_2, \ldots)$—«противоположный» к агрегату $A=(a_0|a_1, a_2, \ldots)$; $A+(-A)=0$; $-(-A)=A$. Определение вычитания: $A-B=A+(-B)$.

2. *Умножение коммутативно, ассоциативно и дистрибутивно относительно сложения,* т. е. A—(коммутативное) кольцо.

Очевидно: $A\cdot 0=0$, $A(-B)=(-A)B=-(AB)$.

3. *В* A *нет нулевых делителей.*

Доказательство. Пусть $AB=(a_0b_0|a_0b_1+a_1b_0, \ldots)=0$; тогда по постулату I $a_0b_0=0$, $a_0b_1+a_1b_0=0, \ldots$, вообще $a_0b_n+a_1b_{n-1}+\ldots+a_nb_0=0$. Пусть, например, $b_0=b_1=\ldots=b_{n-1}=0\neq b_n$; тогда, следовательно, $a_0b_n=0$, $a_0b_{n+1}+a_1b_n=0$, $a_0b_{n+2}+a_1b_{n+1}+a_2b_n=0, \ldots$, откуда заключаем $a_0=a_1=a_2=\cdots=0$, т. е. $A=0$.

Следовательно, A есть область целости.

Назовём агрегат конечным, если все его элементы, начиная с некоторого $((m+1)$-го), равны нулю; будем обозначать

$$(a_0|a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots \text{in inf})=(a_0|a_1, a_2, \ldots, a_n).$$

Все конечные агрегаты, очевидно, составляют область целости.

Назовём агрегат скаляром, если все его элементы, начиная со 2-го, равны нулю. Будем обозначать

$$(a\,|\,0,\,0,\,0,\,\ldots\ \text{in inf}) = a.$$

Очевидно, что все скаляры составляют область целости, просто изоморфную области всех целых рациональных чисел.

Агрегат $(1\,|\,0,\,0,\,0,\,\ldots) = 1$ есть единица умножения для всех агрегатов, т. е. A есть область целости с единицей.

Обозначим $z = (0\,|\,1)$, тогда $z^2 = (0\,|\,0,\,1)$, $z^3 = (0\,|\,0,\,0,\,1)$ и т. д.; и можно формально написать:

$$A = (a_0\,|\,a_1,\,a_2,\,a_3,\,\ldots) = a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots \text{ in inf},$$

т. е. A — не что иное, как совокупность степенных рядов с целыми коэффициентами. Так как мы определили действия над нашими агрегатами чисто формально, то никакого вопроса о «сходимости» этих рядов не может быть: ведь наши агрегаты не числа, никаких численных значений мы им не приписываем; «степенной ряд» — только иное обозначение нашего агрегата. Можно сказать также, что A — линейная алгебра бесконечного порядка над абсолютной областью целости; «основными единицами» этой алгебры являются агрегаты

$$1,\ z,\ z^2,\ z^3,\ \ldots \text{ in inf}.$$

Заметим, что все те из наших степенных рядов, радиусы сходимости которых > 0, образуют субалгебру (только не инвариантную).

§ 2. Деление как действие, обратное умножению, возможно только в редких случаях, но если возможно, то однозначно. Отметим один частный случай, когда деление возможно: именно, если у делителя первый элемент есть ± 1; такой агрегат назовём «единицей» [алгебраической; в отличие обычную единицу (число 1) будем называть «единицей умножения»]: $\mathscr{E} = (\pm 1\,|\,a_1,\,a_2,\,a_3,\,\ldots)$.

Для «единицы» $\mathscr{E}$ всегда существует, и «обратный» агрегат $\frac{1}{\mathscr{E}} = \mathscr{E}^{-1}$ — тоже «единица»; $(\mathscr{E}^{-1})^{-1} = \mathscr{E}$. Легко видеть, что «обратные» агрегаты только и существуют у «единиц», т. е. «единицы» — делители обычной единицы (числа 1). Все «единицы» (включая и скаляры ± 1) составляют обычную абелеву группу относительно умножения.

Два агрегата, отличающихся друг от друга «единичным» множителем, назовём ассоциированными; они взаимно делятся друг на друга. Мы можем вообще говорить о «делимости» агрегатов; в вопросах делимости ассоциированные друг с другом агрегаты не считаются различными.

§ 3. Теорема. *Для всякого агрегата* $A = (a\,|\,a_1,\,a_2,\,a_3,\,\ldots)$ *при* $a \neq 0$ *существует единственно определённый ассоциированный с A агрегат* $\tilde{A} = (a\,|\,b_1,\,b_2,\,b_3,\,\ldots)$, *удовлетворяющий условиям*

$$0 \leqslant b_n < |\,a\,|$$
$$(n = 1,\ 2,\ 3,\ \ldots).$$

Доказательство. Дело сводится к нахождению такой «единицы» $X = (1\,|\,x_1,\,x_2,\,\ldots)$, что $AX = \tilde{A}$. Это даёт

$$ax_1 + a_1 = b_1,$$
$$ax_2 + a_1 x_1 + a_2 = b_2,$$
$$ax_3 + a_1 x_2 + a_2 x_1 + a_3 = b_3$$
и т. д.

Делим a_1 на a; неполное частное обозначаем через $-x_1$, остаток — через b_1; $0 \leqslant b_1 < |a|$. Далее, делим $a_2 + a_1 x_1$ на a и обозначим неполное частное через $-x_2$, остаток — через b_2; $0 \leqslant b_2 < |a|$, и т. д. Все x_n и b_n определяются однозначно.

Если в агрегате A первые m элементов равны нулю, но $(m+1)$-й элемент не равен нулю, то $A = z^m A'$, где $z = (0|1)$; в A' 1-й элемент (тот же, что в A $(m+1)$-й элемент) не равен нулю. Найдём для A' по указанному способу ассоциированный агрегат $\tilde{A}' = A'X$, где X — какая-то «единица»; тогда $AX = z^m A'X = z^m \tilde{A}'$. Обозначим $z^m \tilde{A}' = \tilde{A}$ и получим $AX = \tilde{A}$; в $\tilde{A}$, как и в A, первые m элементов равны нулю, $(m+1)$-й элемент тот же, что и в A (пусть он равен a), все последующие элементы больше или равны нулю и меньше $|a|$; этот агрегат $\tilde{A}$, ассоциированный с A, определяется однозначно при данном A. В обоих случаях мы будем говорить, что агрегат A приведён к нормальной форме; агрегат типа $\tilde{A}$ назовём нормальным.

Легко видеть, что в совокупности всех ассоциированных друг с другом агрегатов имеются всегда только два нормальных, первые элементы которых отличаются друг от друга знаком. Единственные нормальные «единицы» это — скаляры $+1$ и -1.

В вопросах делимости можно каждый агрегат брать в нормальной форме; два различных нормальных агрегата с одинаковыми первыми элементами не ассоциированы.

§ 4. Всякий агрегат делится на всякую «единицу» и на всякий ассоциированный с собою агрегат; если иных делителей данный агрегат не имеет, то назовём его «неразложимым».

Для того чтобы агрегат A делился на агрегат B, необходимо, чтобы первый элемент в A делился на первый элемент в B. Если у A и B первые элементы равны по абсолютной величине, и A делится на B, то в частном первый элемент равен ± 1, т. е. частное — «единица», а следовательно, A и B ассоциированы и B тоже делится на A.

Назовём агрегаты A и B взаимно простыми, если разрешимо уравнение

$$AX + BY = 1. \tag{1}$$

Теорема. *Агрегаты* $A = (a|a_1, a_2, \ldots)$ *и* $B(b|b_1, b_2, \ldots)$ *взаимно простые тогда и только тогда, если их первые элементы* a, b *взаимно простые.*

Доказательство. Пусть $X = (x|x_1, x_2, \ldots)$, $Y = (y|y_1, y_2, \ldots)$; (1) даёт ряд уравнений:

$$\begin{aligned} ax + by &= 1, \\ ax_1 + by_1 &= -a_1 x - b_1 y, \\ ax_2 + by_2 &= -a_1 x_1 - a_2 x - b_1 y_1 - b_2 y \end{aligned}$$

и т. д.

Все эти уравнения разрешимы в целых числах x, y; x_1, y_1; ... тогда и только тогда, если a и b взаимно простые.

§ 5. Теорема. *Если* $A = (ab|c_1, c_2, c_3, \ldots)$, *где* a *и* b *взаимно простые, то* $A = XY$, $X = (a|x_1, x_2, \ldots)$, $Y = (b|y_1, y_2, \ldots)$, *причём это разложение* A *однозначно (с точностью до ассоциированных агрегатов).*

Доказательство. Берём A в нормальной форме и будем искать, например, X тоже в нормальной форме. Из $A=XY$ следует:

$$ay_1+bx_1=c_1,$$
$$ay_2+bx_2=c_2-x_1y_1,$$
$$ay_3+bx_3=c_3-x_1y_2-x_2y_1,$$

вообще

$$ay_n+bx_n=c_n-x_1y_{n-1}-x_2y_{n-2}-\dots-x_{n-1}y_1;$$

все эти уравнения разрешимы в целых числах $y_1, x_1; y_2, x_2; \dots$

Пусть x_1', y_1'—какое-нибудь частное решение первого уравнения; общее его решение: $x_1=x_1'+at$, $y_1=y_1'-bt$, где t—любое целое число. Берём за $-t$ неполное частное, а следовательно, за x_1—остаток от деления x_1' на a $(0\leqslant x_1<|a|)$; этим x_1 определено однозначно. Если мы каким-нибудь способом нашли $ay_1'+bx_1'=c_1$ и $0\leqslant x_1'<|a|$, то $ay_1+bx_1=ay_1'+bx_1'$; $a(y_1-y_1')=b(x_1'-x_1)$; здесь правая часть делится на a, но a и b взаимно простые, следовательно, $x_1'-x_1$ делится на a; но $|x_1'-x_1|<|a|$, т. е. $x_1'=x_1$.

Подобно же однозначно определяются и все x_n при условии $0\leqslant x_n<|a|$ $(n=1, 2, \dots)$, т. е. X в нормальной форме определено однозначно. Если мы каким-нибудь способом нашли $A=X'Y'$, где у X' 1-й элемент равен a, то, приведя X' к нормальному виду, получим X, т. е. $X'=X\mathscr{E}$, где $\mathscr{E}$—«единица», т. е. $A=XY=X'Y'=X(\mathscr{E}Y')$, следовательно, $\mathscr{E}Y'=Y$; $Y'=\mathscr{E}^{-1}Y$ (закон однозначной обратимости умножения следует из отсутствия нулевых делителей).

Следствие. Если в агрегате A 1-й элемент $a=p^\alpha q^\beta r^\gamma\dots$ $(p, q, r$—различные простые числа), то A однозначно (с точностью до ассоциированных агрегатов) представляется в виде $A=PQR\dots$, где в P 1-й элемент равен p^α, в Q 1-й элемент равен q^β, в R 1-й элемент равен r^γ и т. д.

Агрегат вида $(p^\alpha|c_1, c_2, \dots)$ (p — простое) может быть разложимым или неразложимым. Например, легко видеть, что агрегат $P=(p^\alpha|1, 1, 1, \dots)$ неразложим.

§ 6. Теорема. *Если $A=(k|a_1, a_2, \dots)$, $B=(k|b_1, b_2, \dots)$—два агрегата с первым элементом k, отличным от нуля и от ±1, причём a_1-b_1 взаимно простое с k, а $C=(kl|c_1, c_2, \dots)$—любой агрегат с первым элементом, делящимся на k (причём может быть и $l=0$), то можно найти агрегаты $X=(x_0|x_1, x_2, \dots)$, $Y=(y_0|y_1, y_2, \dots)$ так, чтобы было*

$$AX+BY=C. \qquad (2)$$

Доказательство. Условие (2) даёт

$$k(x_0+y_0)=kl,$$

т. е.

$$x_0+y_0=l;$$

$$k(x_1+y_1)=c_1-a_1x_0-b_1y_0=c_1-a_1l+(a_1-b_1)y_0\equiv0 \pmod k;$$

отсюда определяем y_0, а затем и $x_0=l-y_0$; определяется также и значение $x_1+y_1=l_1$.

Далее,

$$k(x_2+y_2)=c_2-a_1x_1-a_2x_0-b_1y_1-b_2y_0=$$
$$=c_2-a_2x_0-b_2y_0-a_1l_1+(a_1-b_1)y_1\equiv0 \pmod k;$$

отсюда определяем y_1, затем $x_1=l_1-y_1$ и находим значение $x_2+y_2=l_2$; и т. д.

Таким образом, если (A, B)—идеал (или инвариантная субалгебра), порождённый агрегатами A и B, то $C\in(A, B)$. Иными словами:

Следствие 1. Все агрегаты с первыми элементами, делящимися на k ($k\neq 0$, $k\neq\pm 1$), составляют идеал (инвариантную субалгебру) N_k, порождаемый двумя подходящим образом выбранными агрегатами; за эти порождающие агрегаты (генераторы) можно взять k и $(k\,|-1)$:

$$\mathrm{N}_k=(k,\ (k\,|-1)).$$

Следствие 2. $\mathrm{N}_{k_1}\subset\mathrm{N}_k$ тогда и только тогда, если k_1 делится на k.

В частности, $\mathrm{N}_k\supset\mathrm{N}_{k^2}\supset\mathrm{N}_{k^3}\supset\ldots$

Пусть $m=p^\alpha q^\beta r^\gamma\ldots$—разложение числа m на простые множители; тогда $\mathrm{N}_m\subset\mathrm{N}_{p^\alpha}$, $\mathrm{N}_m\subset\mathrm{N}_{q^\beta}$, $\mathrm{N}_m\subset\mathrm{N}_{r^\gamma}$, ...

Теорема. N_m *есть пересечение* («*общее наименьшее кратное*») *идеалов* N_{p^α}, N_{q^β}, N_{r^γ}, ...

Доказательство. Достаточно показать, что всякий агрегат X, принадлежащий одновременно к N_{p^α}, к N_{q^β}, к N_{r^γ}, ..., принадлежит и к N_m. Но ведь тогда первый элемент в X делится на p^α, на q^β, на r^γ, ..., следовательно, он делится и на m, т. е. $X\in\mathrm{N}_m$.

Все агрегаты с первым элементом, равным нулю, очевидно, составляют идеал, порождаемый агрегатом $z=(0\,|\,1)$; этот идеал символически выражается в виде $z\mathrm{A}$; подобно же и $z^2\mathrm{A}$, $z^3\mathrm{A}$, ..., вообще, $z^m\mathrm{A}$, где m—натуральное число, являются идеалами; $A\supset z\mathrm{A}\supset z^2\mathrm{A}\supset\ldots$

Если N—любой идеал в A, то и zN—идеал, причём $z\mathrm{N}\subset z\mathrm{A}$.

Заметим, что если A—любой агрегат (только не «единица»), то $A\mathrm{A}=(A)$—идеал, главный идеал, порождаемый агрегатом A. В частности, и $z\mathrm{A}=(z)$—тоже главный идеал (порождаемый агрегатом z).

§ 7. Исследуем теперь так называемые «дополнительные» алгебры. Если N—данный идеал в A, то вся алгебра A распадается на классы агрегатов «по модулю N», один из этих классов—N, другие классы имеют вид $A+\mathrm{N}$, $B+\mathrm{N}$, $C+\mathrm{N}$, ..., где $A, B, C, \ldots$—агрегаты, подходящим образом выбранные из A. Эти классы и составляют «дополнительную алгебру» A/N (иногда её обозначают A—N) относительно тех же действий сложения и умножения, которые непосредственно переносятся на классы. По существу, дело сводится к тому, что мы в системе постулатов (§ 1) заменяем постулат равенства следующим постулатом:

$A=B$ тогда и только тогда, если $A-B\in\mathrm{N}$.

Иными словами, все агрегаты из N мы приравниваем нулю. От этого может случиться, что в алгебре A/N окажутся нулевые делители, тогда как в алгебре A их нет (§ 1); это случится тогда и только тогда, если окажется, что $AB\in\mathrm{N}$, тогда как ни A, ни B не принадлежат к N. Мы разберём некоторые частные случаи.

1. Пусть $\mathrm{N}=z\mathrm{A}=(z)$. В алгебре A/zA мы считаем $z=0$, т. е. и $Xz=0$ при любом агрегате X, т. е. мы принимаем равным *нулю всякий агрегат с первым элементом, равным нулю.* Этим всякий агрегат делается равным скаляру,—1-му элементу этого агрегата. Иначе, A/zA изоморфна абсолютной области целости; эта алгебра не имеет нулевых делителей (следовательно, zA—«простой» идеал).

2. Пусть $N = z^2A = (z^2)$. В алгебре A/z^2A мы считаем равным нулю все агрегаты, у которых первые два элемента равны нулю; эта алгебра изоморфна алгебре с двумя основными единицами: 1 и z, где $1 \cdot z = z \cdot 1 = z$, $z^2 = 0$. В этой алгебре все числа вида bz (b—обычное целое число)—нулевые делители.

3. Пусть $N = z^nA = (z^n)$ ($n \geqslant 3$). Алгебра A/z^nA есть система агрегатов вида $(a_0 | a_1, a_2, \ldots, a_{n-1}) = a_0 + a_1z + a_2z^2 + \cdots + a_{n-1}z^{n-1}$ при условии $z^n = 0$. Нулевыми делителями здесь являются агрегаты вида $(0 | a_1, \ldots, a_{n-1}) = z(a_1 + a_2z + \cdots + a_{n-1}z^{n-2})$.

4. Пусть $N = N_k$. В алгебре A/N_k считаются равным нулю все агрегаты с 1-м элементом, делящимся на k, в частности, и с первым элементом, равным нулю. Отсюда следует, что всякий агрегат $(a_0 | a_1, a_2, \ldots)$ в алгебре A/N_k равен одному из чисел $0, 1, 2, \ldots, k-1$, и алгебра A/N_k *изоморфна кольцу классов целых чисел по модулю* k. Если k—составное число, то нулевым делителем является всякий агрегат, у которого первый элемент не делится на k, но и не взаимно простой с k. Если же $k = p$—простое число, то A/N_p нулевых делителей не имеет и является телом; *идеал* N_p—*простой*.

5. Пусть теперь $N = zN_k$. Здесь в алгебре A/zN_k считаются равными нулю, во-первых, все агрегаты из z^2A, ибо $z^2A \subset zN_k$, т. е. всякий агрегат сводится к виду $(a | a_1)$; но, во-вторых, равны нулю и агрегаты вида $(0 | u)$, где u делится на k. Таким образом в алгебре A/zN_k всякий агрегат сводится к виду $(a | a_1)$, где $a_1 = 0, 1, 2, \ldots, k-1$. Нулевыми делителями являются здесь все агрегаты $(a | b)$, где a не взаимно простое с k. Пусть, например, $k = k_1k_2$, $a = k_1c$; тогда $(k_1c | x)(0 | k_2) = (0 | kc) = 0$.

В частности, агрегаты вида $(0 | b)$—тоже нулевые делители; они нильпотентны.

§ 8. Пусть $N = PA = (P)$, где $P = (p | p_1, p_2, \ldots)$ — некоторый агрегат с простым первым элементом p. В алгебре A/PA считаются равными нулю все агрегаты, имеющие вид PQ. Легко видеть, что всякий агрегат $A = (a_0 | a_1, a_2, \ldots)$ в алгебре A/PA может быть приведён к такому виду, что все a_n будут больше или равны нулю и меньше p, и такое представление однозначно. Докажем, что алгебра A/PA не имеет нулевых делителей. Пусть, именно, $AB = PQ$, причём и $A = (a_0 | a_1, a_2, \ldots)$, и $B = (b_0 | b_1, b_2, \ldots)$ взяты в указанной выше «приведённой» форме (т. е. $0 \leqslant a_n < p$, $0 \leqslant b_n < p$); пусть $P = (p | p_1, p_2, \ldots)$, $Q = (q | q_1, q_2, \ldots)$; тогда $a_0b_0 = pq$, т. е. a_0b_0 делится на p, но и $|a_0|$, и $|b_0| < p$, т. е., например, $b_0 = 0$; но тогда и $q = 0$. Далее, $a_0b_1 + a_1b_0 = pq_1 + p_1q$ или $a_0b_1 = pq_1$; если $a_0 \neq 0$, то b_1 делится на p, но $|b_1| < p$, т. е. $b_1 = 0$, следовательно, и $q_1 = 0$; и так докажем, что все $b_n = 0$, если только $a_0 \neq 0$. Доказательство несколько модифицируется, если $a_0 = 0$, но $A \neq 0$, т. е., например, $A = z^nA_1$, где в A_1 1-й элемент не равен нулю.

Докажем ещё, что в алгебре A/PA всякий агрегат $A = (a | a_1, a_2, \ldots)$, где $0 < a < p$ есть «единица». Для этого достаточно показать, что можно найти такие агрегаты X, Y, что

$$AX - PY = 1. \tag{3}$$

Пусть $X = (x | x_1, x_2, \ldots)$, $Y = (y | y_1, y_2, \ldots)$; тогда (3) даёт:

$$ax - py = 1,$$
$$ax_1 + a_1x - py_1 - p_1y = 0,$$
$$ax_2 + a_1x_1 + a_2x - py_2 - p_1y_1 - p_2y = 0$$

и т. д.

Это можно написать в виде сравнений:

$$ax \equiv 1 \pmod{p},$$
$$ax_1 \equiv p_1 y - a_1 x \pmod{p},$$
$$ax_2 \equiv p_1 y_1 + p_2 y - a_1 x_1 - a_2 x \pmod{p},$$

и т. д.

Первое сравнение однозначно (по модулю p) определит x, а далее, и y; второе сравнение однозначно (по модулю p) определит x_1, а далее, и y_1; третье сравнение определит x_2 и y_2, и т. д.

В частности, если взять $P = (p \mid -1)$, то алгебра A/PA будет не что иное, как система p-адических чисел Гензеля.

§ 9. 7. Пусть теперь $N = G_1 A = (G_1)$, где $G_1 = (g \mid g_1 g_2, \ldots)$ и $g = kl$, причём k и l взаимно простые. По теореме § 5 $G_1 = K_1 L_1$, где в K_1 1-й элемент равен k, а в L_1 1-й элемент равен l, причём это разложение однозначно с точностью до ассоциированных агрегатов. Отсюда следует, что в алгебре $A/G_1 A$ имеются нулевые делители. Легко убедиться (как и в § 8), что всякий агрегат с 1-м элементом, взаимно простым с kl, в алгебре $A/G_1 A$ является «единицей». Обозначим $K_1 + L_1 = E_1$; E_1 есть «единица», ибо 1-й элемент в E_1 есть $k + l$, но $k + l$ — взаимно простое с kl. Следовательно, существует E_1^{-1} — тоже «единица»; $K_1 E_1^{-1} + L_1 E_1^{-1} = 1$. Обозначим $K_1 E_1^{-1} = K$, $L_1 E_1^{-1} = L$; в алгебре $A/G_1 A$ K ассоциировано с K_1, L ассоциировано с L_1. Имеем $K + L = 1$. Пусть P — любой агрегат; тогда $P = PK + PL$. Обозначив $PK = P_1$, $PL = P_2$, имеем

$$P = P_1 + P_2;$$
$$P_1 P_2 = 0.$$

Докажем, что такое разложение P в сумму двух агрегатов, из которых один делится на K, а другой на L, — однозначно. Пусть $P = P_1 + P_2 = P_1' + P_2'$, где P_1 и P_1' делятся на K, а P_2 и P_2' делятся на L; тогда $P_1 - P_1' = P_2' - P_2$ делится и на K, и на L. Докажем, что тогда $P_1 - P_1'$ делится и на KL, т. е. (в алгебре $A/G_1 A$) и на G_1, т. е. $P_1 - P_1' = P_2' - P_2 = 0$, т. е. $P_1' = P_1$, $P_2' = P_2$ (всё это в алгебре $A/G_1 A$). Именно: $P_1 - P_1' = KL$; $K + L = 1$; $(P_1 - P_1') + LX = X$; левая часть здесь делится на L, а следовательно, и правая, т. е. X, делится на L, т. е. $P_1 - P_1'$ делится на KL.

Далее, если $P = P_1 + P_2$ и аналогично $P' = P_1' + P_2'$, то, очевидно, $P + P' = (P_1 + P_1') + (P_2 + P_2')$; $PP' = P_1 P_1' + P_2 P_2'$, ибо $P_1 P_2' = P_1' P_2 = 0$, как делящиеся на G_1. Очевидно, что все агрегаты P_1, P_1', ... составляют алгебру K, равно как и все агрегаты P_2, P_2', ..., — алгебру Λ. Мы видим, что $A/G_1 A = Z$ есть прямая сумма этих алгебр:

$$Z = K + \Lambda.$$

K есть совокупность агрегатов, делящихся на K, причём два таких агрегата мы считаем равными, если их разность делится на L, т. е. по существу K есть дополнительная алгебра к субалгебре LZ алгебры Z, т. е. $K = Z/LZ$. И подобно же $\Lambda = Z/KZ$.

Пусть $P = P_1 + P_2$ — «единица» в алгебре Z; тогда $P_1 = (r_1 k \mid \ldots)$, $P_2 = (r_2 l \mid \ldots)$, $P = (r_1 k + r_2 l \mid \ldots)$; $r_1 k + r_2 l$ — взаимно простое с kl, для чего необходимо и достаточно, чтобы r_1 было взаимно простое с l, а r_2 — взаимно простое с k. Но тогда P_1 — «единица» для K, а P_2 — «единица» для Λ. И обратно: если P_1 — «единица» для K, а P_2 — «единица» для Λ, то $P = P_1 + P_2$ — «единица» для Z.

Далее (в алгебре Z), $(P_1 + P_2)(K + L) = P_1 K + P_2 L = P_1 + P_2$, а так как такое представление однозначно. то $P_1 K = P_1$, $P_2 L = P_2$ для вся-

кого агрегата $P = P_1 + P_2$, т. е. K — единица умножения для K, а L — единица умножения для Λ. Если P — «единица» для Z, то имеем

$$P = (P_1 + L)(K + P_2) = P_1 + P_2;$$

такое представление P в виде произведения однозначно. Если P_1 пробегает «единицы» для K, а P_2 — единицы для Λ, то агрегаты $P_1 + L$, $K + P_2$ образуют группы $\mathfrak{K}$ и $\mathfrak{Z}$, изоморфные группам «единиц» из K и Λ. Группу «единиц» из Z обозначим через $\mathfrak{Z}$. Мы видим, что $\mathfrak{Z} = \mathfrak{K} \times \mathfrak{L}$ (прямое произведение).

Если взять $G_1 = (g\,|\,-1)$, то алгебра $A/G_1A = Z$ — не что иное, как система g-адических чисел Гензеля.