Независимый Московский Университет

Алгебра – II

Второй курс, осенний семестр 1999/2000 г.
Лекция 4

Конечные поля. Для любого кольца R существует канонический гомоморфизм $\mathbb{Z} \to R$ $(n \mapsto \overline{n})$, переводящий 1 в единицу кольца. Его образ — подкольцо кольца R, изоморфное либо $\mathbb{Z}$, либо $\mathbb{Z}/m\mathbb{Z}$ для некоторого $m \in \mathbb{Z}$.

Пусть $\mathbb{F}$ — конечное поле. Напомню, что характеристикой $\operatorname{char}\mathbb{F}$ поля $\mathbb{F}$ называется минимальное натуральное число p, для которого $\overline{p} = \overline{0}$ в поле $\mathbb{F}$. Поскольку поле конечно, то такое натуральное число существует. Из определения ясно, что канонический образ $\mathbb{Z}$ в $\mathbb{F}$ изоморфен $\mathbb{Z}/p\mathbb{Z}$. Число p — простое, поскольку в поле не может быть делителей нуля.

Упражнение 1. Пусть поле $\mathbb{F}$ конечно. Доказать, что если его подмножество $\mathbb{k}$ замкнуто относительно сложения и умножения, то $\mathbb{k}$ является подполем поля $\mathbb{F}$.

Как мы видели, любое конечное поле $\mathbb{F}$ является расширением поля, изоморфного $\mathbb{F}_p$ для некоторого простого числа p, то есть $\mathbb{F}$ изоморфно расширению $\mathbb{F}_p$. То же относится, очевидно, ко всем полям положительной характеристики: любое поле $\mathbb{F}$ характеристики p изоморфно расширению поля $\mathbb{F}_p$.

Упражнение 2. Доказать, что любое поле $\mathbb{F}$ характеристики 0 изоморфно расширению поля $\mathbb{Q}$.

Утверждение 1. *Пусть $\mathbb{F}$ — конечное поле характеристики p. Тогда число элементов поля $\mathbb{F}$ равно p^k, где k — некоторое натуральное число.*

Доказательство. Элементы вида $\overline{n} \in \mathbb{F}$ образуют подполе поля $\mathbb{F}$, изоморфное $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ для некоторого простого $p \in \mathbb{N}$. Рассмотрим аддитивную группу поля $\mathbb{F}$. Для любого $a \in \mathbb{F}$ мы имеем $pa = \overline{p}a = 0$. Следовательно, по теореме о строении конечных абелевых групп, аддитивная группа поля $\mathbb{F}$ изоморфна

$$\underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{k \text{ раз}}$$

для некоторого натурального числа k. Отсюда следует, что $|\mathbb{F}| = p^k$. $\square$

Теорема 2. *Всякая конечная подгруппа мультипликативной группы любого поля является циклической. В частности, мультипликативная группа любого конечного поля — циклическая.*

Доказательство. Пусть G — конечная подгруппа мультипликативной группы поля $\mathbb{F}$, и $|G| = n$. По теореме о строении конечных абелевых групп, группа G изоморфна $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m}$, где $n_1 \vdots n_2 \vdots \ldots \vdots n_m$ и $n_1 \cdots n_m = n$. Отсюда следует, что для любого $g \in G$ мы имеем $g^{n_1} = 1$. Однако многочлен $x^{n_1} - 1$

не может иметь более чем n_1 корней в поле $\mathbb{F}$, поэтому $n_1 = n$ и группа G является циклической. $\square$

Определение 1. *Элемент a поля $\mathbb{F}$ называется* примитивным корнем степени n из 1, *если $a^n = 1$ и $a^k \neq 1$ при $0 < k < n$.*

Мы видим, что каждый ненулевой элемент поля $\mathbb{F}_q$ является корнем степени $q-1$ из единицы, причем существует примитивный корень, то есть такой элемент $a \in \mathbb{F}_q$, что все ненулевые элементы поля $\mathbb{F}_q$ имеют вид a^k для некоторого $k \in \{1, \ldots, q-1\}$.

Упражнение 3. Доказать, что число примитивных корней из 1 степени n в поле комплексных чисел $\mathbb{C}$ равно $\varphi(n)$, где $\varphi(n)$ — функция Эйлера: количество натуральных чисел m таких, что $m \leqslant n$ и $(m, n) = 1$.

Теорема 3. *Для любого простого числа p и любого натурального числа k существует поле $\mathbb{F}_q$ из $q = p^k$ элементов. С точностью до изоморфизма, такое поле единственно.*

Доказательство. Если $k = 1$, то $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ является полем из $q = p$ элементов. Пусть $k > 1$. Рассмотрим поле $\mathbb{F}$ разложения многочлена $x^q - x$ над $\mathbb{F}_p$. Тогда многочлен $x^q - x$ раскладывается в $\mathbb{F}[x]$ на линейные множители, то есть

$$x^q - x = (x - a_1) \cdot (x - a_q)$$

для некоторых $a_1, \ldots, a_q \in \mathbb{F}$, причем $\mathbb{F} = \mathbb{F}_p[a_1, \ldots, a_q]$.

Лемма 3.1. *Все элементы $a_1, \ldots, a_q \in \mathbb{F}$ попарно различны.*

Доказательство. Если многочлен $x^q - x$ делится на $(x-b)^2$ для некоторого $b \in \mathbb{F}$, то производная многочлена $x^q - x$ делится на $x - b$, то есть b является одновременно корнем многочленов $x^q - x$ и $(x^q - x)' = qx^{q-1} - 1 = -1$ (поскольку $q = p \cdot p^{k-1} = 0$ в поле $\mathbb{F}_p$). Однако многочлен -1, очевидно, не имеет корней. Следовательно, многочлен $x^q - x$ не имеет кратных корней. $\square$

Лемма 3.2. *Элементы $\in \mathbb{F}$ образуют поле.*

Доказательство. Очевидно, достаточно проверить, что сумма и произведение корней многочлена $x^q - x$ снова является его корнем (см. упражнение 1).

Для произведения это очевидно: если $a^q = a$ и $b^q = b$, то $(ab)^q = a^q b^q = ab$. Чтобы доказать то же для суммы, проверим сначала равенство $(a+b)^p = a^p + b^p$, верное для любых элементов любого поля характеристики p.

По формуле бинома

$$(a+b)^p = \sum_{l=0}^{p} \binom{p}{l} a^l b^{p-l}.$$

При $0 < l < p$ биномиальный коэффициент $\binom{p}{l} = \frac{p!}{l!(p-l)!}$ делится на p, поэтому над полем характеристики p от формулы бинома остаются лишь два крайних члена: $(a+b)^p = a^p + b^p$.

С помощью индукции по k отсюда легко вывести, что при $q = p^k$ над полем характеристики p верно равенство $(a+b)^q = a^q + b^q$. В нашем случае, если $a^q = a$ и $b^q = b$, то $(a+b)^q = a^q + b^q = a + b$. $\square$

Так как $\mathbb{F} = \mathbb{F}_p[a_1, \ldots, a_q]$, то мы получаем $\mathbb{F} = \{a_1, \ldots, a_q\}$. Итак, $\mathbb{F}_q = \mathbb{F}$ является полем из q элементов. Как поле разложения многочлена $x^q - x$, оно единственно с точностью до изоморфизма. $\square$

В доказательстве теоремы 3 нам уже встретился следующий замечательный факт: если поле $\mathbb{F}$ имеет характеристику p, то для любых $a, b \in \mathbb{F}$ имеет место равенство $(a+b)^p = a^p + b^p$. Отсюда и из того, что $(ab)^p = a^p b^p$, легко следует, что отображение $F : \mathbb{F} \to \mathbb{F}$, заданное формулой $F(a) = a^p$, является гомоморфизмом. Ядро этого гомоморфизма не содержит 1, поэтому оно равно $\{0\}$ (поскольку в поле $\mathbb{F}$ лишь два идеала: $\mathbb{F}$ и $\{0\}$). Поэтому гомоморфизм F инъективен. В частности, если поле $\mathbb{F}$ конечно, то F обратим, то есть F является автоморфизмом. Он называется *автоморфизмом Фробениуса*.

Задача 1. Доказать, что группа автоморфизмов конечного поля $\mathbb{F}$ циклическая и порождена автоморфизмом Фробениуса.

Сепарабельные расширения.

Определение 2. Неприводимый многочлен $f(x) \in \Bbbk[x]$ называется *сепарабельным*, если у него нет кратных корней (в его поле разложения). Элемент алгебраического расширения поля $\Bbbk$ называется сепарабельным над $\Bbbk$, если его минимальный многочлен над $\Bbbk$ сепарабелен. Расширение $\mathbb{F}/\Bbbk$ называется сепарабельным, если все элементы поля $\mathbb{F}$ сепарабельны над $\Bbbk$.

Теорема 4. *Пусть $f(x) \in \Bbbk[x]$ — многочлен, не являющийся сепарабельным. Тогда $\operatorname{char} \Bbbk = p \neq 0$ и $f(x) = g(x^p)$ для некоторого многочлена $g(x) \in \Bbbk[x]$.*

Доказательство. Если многочлен $f(x)$ имеет кратный корень, то у него есть непостоянный общий делитель (над полем разложения) с многочленом $f'(x)$ (производной). Поскольку наибольший общий делитель можно искать с помощью алгоритма Евклида, а применение этого алгоритма к многочленам из $\Bbbk[x]$ дает многочлен из $\Bbbk[x]$, мы получаем, что многочлены $f(x)$ и $f'(x)$ имеют непостоянный общий делитель и над полем $\Bbbk$. Так как многочлен $f(x)$ неприводим, отсюда следует, что $f'(x)$ должен делиться на $f(x)$. Поскольку степень $f'(x)$ меньше степени $f(x)$, это возможно лишь при $f'(x) = 0$. Над полем характеристики нуль любой непостоянный многочлен имеет ненулевую производную, а постоянные многочлены, очевидно, сепарабельны. Поэтому $\operatorname{char} \Bbbk = p \neq 0$. При этом многочлен $f(x)$ может иметь ненулевые коэффициенты лишь при мономах вида x^{kp}, то есть $f(x) = \sum a_k x^{kp}$. Но тогда $f(x) = g(x^p)$, где $g(x) = \sum a_k x^k$. $\square$

Определение 3. Поле $\Bbbk$ характеристики $p > 0$ называется *совершенным*, если для любого $a \in \Bbbk$ найдется $b \in \Bbbk$ такой, что $b^p = a$. Любое поле нулевой характеристики тоже называется совершенным.

Теорема 5. *Любое алгебраическое расширение совершенного поля является сепарабельным.*

Доказательство. Для полей нулевой характеристики это следует из предыдущей теоремы. Пусть $\operatorname{char} \Bbbk = p > 0$ и $f(x)$ — минимальный многочлен несепарабельного над $\Bbbk$ элемента. Тогда $f(x) = \sum a_k x^{kp}$. Пусть $a_k = b_k^p$. Тогда $f(x) = h(x)^p$, где $h(x) = \sum b_k x^k$, в противоречии с неприводимостью многочлена $f(x)$. □

Теорема 6. *Пусть $\mathbb{F}/\Bbbk$ — расширение, и $\mathbb{L}$ — некоторое промежуточное поле. Тогда любой элемент $a \in \mathbb{F}$, сепарабельный над $\Bbbk$, сепарабелен также и над $\mathbb{L}$. В частности, если расширение $\mathbb{F}/\Bbbk$ сепарабельно, то расширение $\mathbb{F}/\mathbb{L}$ тоже сепарабельно.*

Доказательство. Пусть $g(x) \in \Bbbk[x]$ — минимальный многочлен элемента a над полем $\Bbbk$, а $f(x) \in \mathbb{L}[x]$ — минимальный многочлен элемента a над полем $\mathbb{L}$. Поскольку a сепарабелен над $\Bbbk$, многочлен $g(x)$ не имеет кратных корней. Многочлен $g(x)$ делится на $f(x)$ в $\mathbb{L}[x]$ и, следовательно, $f(x)$ тоже не имеет кратных корней. □

Определение 4. Пусть $\mathbb{F}/\Bbbk$ и $\mathbb{L}/\Bbbk$ — произвольные расширения. *Вложением* расширения $\mathbb{F}/\Bbbk$ в расширение $\mathbb{L}/\Bbbk$ называется гомоморфизм $\mathbb{F} \to \Bbbk$ (инъективный, ибо $\mathbb{F}$ — поле), оставляющий элементы поля $\Bbbk$ неподвижными.

Теорема 7. *Число вложений конечного расширения $\mathbb{F}/\Bbbk$ в расширение $\mathbb{L}/\Bbbk$ не превосходит $[\mathbb{F} : \Bbbk]$.*

Доказательство. Пусть $\mathbb{F} = \Bbbk(a_1, \ldots, a_n)$. Положим $\Bbbk_i = \Bbbk(a_1, \ldots, a_i)$ и обозначим через $f_i(x)$ минимальный многочлен элемента a_i над полем $\Bbbk_{i-1}$ (мы считаем $\Bbbk_0 = \Bbbk$). Ясно, что

$$[\mathbb{F} : \Bbbk] = \prod_{i=1}^{n} [\Bbbk_i : \Bbbk_{i-1}] = \prod_{i=1}^{n} \deg f_i.$$

С другой стороны, любое вложение σ поля $\Bbbk_{i-1}$ в $\mathbb{L}$ можно продолжить до вложения поля $\Bbbk_i$ не более чем $\deg f_i$ способами. Действительно, продолжение вложения σ целиком определяется образом элемента a_i, который, очевидно, может перейти лишь в корень многочлена f_i^σ (то есть многочлена, получающегося из f_i заменой каждого коэффициента на его образ при вложении σ). Поэтому число вложений $\mathbb{F}/\Bbbk$ в $\mathbb{L}/\Bbbk$ не превосходит $\prod \deg f_i$. □

Теорема 8. *Пусть $\mathbb{F} = \Bbbk(a_1, \ldots, a_n)$ — конечное расширение поля $\Bbbk$ и $\mathbb{L}/\Bbbk$ — некоторое расширение, в котором минимальный многочлен каждого из a_i над $\Bbbk$ разлагается на линейные множители. Число вложений конечного расширения $\mathbb{F}/\Bbbk$ в расширение $\mathbb{L}/\Bbbk$ равно $[\mathbb{F} : \Bbbk]$ тогда и только тогда, когда a_i сепарабелен над $\Bbbk(a_1, \ldots, a_{i-1})$ для любого $i = 1, \ldots, n$.*

Доказательство. Положим $\Bbbk_i = \Bbbk(a_1, \ldots, a_i)$ и обозначим через $f_i(x)$ минимальный многочлен элемента a_i над полем $\Bbbk_{i-1}$. Докажем, что любое вложение σ поля $\Bbbk_{i-1}$ в $\mathbb{L}$ можно продолжить до вложения поля $\Bbbk_i$ ровно столькими способами, сколько у многочлена $f_i(x)$ различных корней. Отсюда всё следует (см. доказательство предыдущей теоремы).

Пусть $g_i(x)$ — минимальный многочлен a_i над $\Bbbk$. Тогда для некоторого многочлена $h_i(x) \in \Bbbk_{i-1}[x]$ имеет место равенство $g_i(x) = f_i(x)h_i(x)$. Поскольку σ является гомоморфизмом, тождественным на $\Bbbk$, отсюда следует, что $g_i(x) = f_i^\sigma(x)h_i^\sigma(x)$. По условию $g_i(x)$ и, следовательно, как $f_i(x)$, так и $f_i^\sigma(x)$, раскладываются над полем $\mathbb{L}$ в произведение линейных множителей. Очевидно, что у многочлена $f_i^\sigma(x)$ столько же различных корней, сколько у $f_i(x)$. Остается воспользоваться тем, что a_i может переходить в любой из корней многочлена $f_i^\sigma(x)$ (по теореме о продолжении изоморфизма), и что выбором корня продолжение вложения σ определяется однозначно. □

Следствие 8.1. *Пусть $\mathbb{F} = \Bbbk(a_1, \ldots, a_n)$ — конечное расширение поля $\Bbbk$, причем a_i сепарабелен над $\Bbbk(a_1, \ldots, a_{i-1})$ для любого $i = 1, \ldots, n$. Тогда расширение $\mathbb{F}/\Bbbk$ сепарабельно.*

Доказательство. Пусть $\mathbb{L}$ — поле разложения произведения минимальных многочленов элементов $a_1, \ldots, a_n$. Согласно теореме 8 число вложений $\mathbb{F}/\Bbbk$ в $\mathbb{L}/\Bbbk$ равно $[\mathbb{F} : \Bbbk]$. Пусть $a \in \mathbb{F}$. Тогда $\mathbb{F} = \Bbbk(a, a_1, \ldots, a_n)$. По теореме 8 отсюда следует, что a сепарабелен над $\Bbbk$. □

Теорема 9 (О примитивном элементе). *Любое конечное сепарабельное расширение $\mathbb{F}/\Bbbk$ обладает элементом, порождающим $\mathbb{F}$ над $\Bbbk$ (примитивным элементом).*

Доказательство. Если поле $\Bbbk$ конечно, то и поле $\mathbb{F}$ конечно, но тогда мультипликативная группа поля $\mathbb{F}$ циклическая и её образующая порождает $\mathbb{F}$ над $\Bbbk$. Таким образом, можно считать, что поле $\Bbbk$ бесконечно.

С помощью индукции по числу образующих поля $\mathbb{F}$ над $\Bbbk$ всё сводится к случаю, когда $\mathbb{F} = \Bbbk(a, b)$. Пусть $\sigma_1, \ldots, \sigma_n$ — все различные вложения поля $\mathbb{F}$ в $\bar{\Bbbk}$ над $\Bbbk$. Рассмотрим многочлен

$$f(x) = \prod_{i<j} (\sigma_i(a) + \sigma_i(b)x - \sigma_j(a) - \sigma_j(b)x) \in \bar{\Bbbk}[x].$$

Очевидно, что это ненулевой многочлен, поэтому существует $c \in \Bbbk$, для которого $f(c) \neq 0$. Но тогда все элементы $\sigma_i(a + bc)$ различны, то есть поле $\Bbbk(a + bc)$ имеет по крайней мере n различных вложений в $\bar{\Bbbk}$ над $\Bbbk$, так что $[\Bbbk(a + bc) : \Bbbk] \geqslant n$ (по теореме 7). Но $n = [\mathbb{F} : \Bbbk]$ (по теореме 8), поэтому $\mathbb{F} = \Bbbk(a + bc)$. □

Норма и след. Пусть $\mathbb{F}/\Bbbk$ — произвольное конечное расширение. Рассмотрим $\mathbb{F}$ как линейное пространство над $\Bbbk$. Каждому элементу $a \in \mathbb{F}$ отвечает линейный оператор $L(a)$ в пространстве $\mathbb{F}$, состоящий в умножении на a. Заметим, что при $a \neq 0$ оператор $L(a)$ обратим.

Определение 5. *Нормой* $N(a)$ элемента a конечного расширения $\mathbb{F}/\Bbbk$ называется определитель оператора $L(a)$, а его *следом* $\mathrm{tr}(a)$ называется след этого оператора. *Характеристическим многочленом* элемента a называется характеристический многочлен оператора $L(a)$.

Теорема 10. *Пусть $\mathbb{F}/\Bbbk$ — произвольное конечное расширение, $n = [\mathbb{F} : \Bbbk]$, $a \in \mathbb{F}$, $f(x)$ — минимальный многочлен элемента a над $\Bbbk$ и $d = \deg f(x)$. Тогда характеристический многочлен элемента a равен $f(x)^{n/d}$.*

Доказательство. Ясно, что минимальный многочлен оператора $L(a)$ — то же самое, что и минимальный многочлен элемента a. Для расширения $\Bbbk(a)/\Bbbk$ минимальный многочлен, очевидно, совпадает с характеристическим. Пусть $(b_1, \ldots, b_m)$ — базис $\mathbb{F}$ как линейного пространства над $\Bbbk(a)$ (ясно, что $m = n/d$). Тогда элементы $a^k b_l$, где $0 \leqslant k < d$ и $1 \leqslant l \leqslant m$, составляют базис $\mathbb{F}$ над $\Bbbk$. В этом базисе матрица оператора $L(a)$ имеет блочно-диагональный вид с одинаковыми циклическими блоками по диагонали. Поэтому характеристический многочлен элемента a является степенью его минимального многочлена. □

Следствие 10.1. *Пусть $\mathbb{F}/\Bbbk$ — конечное сепарабельное расширение, а $\mathbb{L}/\Bbbk$ — такое расширение, над которым минимальный многочлен любого элемента из $\mathbb{F}$ разлагается на линейные множители. Обозначим через Φ множество всех вложений расширения $\mathbb{F}/\Bbbk$ в расширение $\mathbb{L}/\Bbbk$. Тогда для любого элемента $a \in \mathbb{F}$ его характеристический многочлен равен*

$$f_a(x) = \prod_{\varphi \in \Phi} (x - \varphi(a)).$$

В частности, $N(a) = \prod \varphi(a)$ и $\mathrm{tr}(a) = \sum \varphi(a)$.

Доказательство. Докажите сами. □

Теорема 11. *Пусть $\mathbb{F}/\Bbbk$ — конечное сепарабельное расширение степени n, $\mathbb{L}/\Bbbk$ — такое расширение, над которым минимальный многочлен любого элемента из $\mathbb{F}$ разлагается на линейные множители, $\varphi_1, \ldots, \varphi_n$ — все вложения расширения $\mathbb{F}/\Bbbk$ в расширение $\mathbb{L}/\Bbbk$. Рассмотрим гомоморфизм $\Bbbk$-алгебр $\psi : \mathbb{F} \to \mathbb{L}^n$, заданный формулой $\psi(a) = (\varphi_1(a), \ldots, \varphi_n(a))$ для любого $a \in \mathbb{F}$. Этот гомоморфизм можно продолжить до изоморфизма $\mathbb{L}$-алгебр $\mathbb{L} \otimes_{\Bbbk} \mathbb{F} \to \mathbb{L}^n$.*

Доказательство. Обозначим через A линейную оболочку над $\mathbb{L}$ образа гомоморфизма ψ. Ясно, что A является $\mathbb{L}$-подалгеброй алгебры $\mathbb{L}^n$.

Пространство $\mathbb{L}^n$ как A-модуль является суммой одномерных подмодулей $\langle e_i\rangle$, где $(e_1,\ldots,e_n)$ — стандартный базис пространства $\mathbb{L}^n$, поэтому $\mathbb{L}^n$ — полупростой A-модуль и, следовательно, A — тоже полупростой A-модуль (как подмодуль полупростого модуля). Таким образом, A — полупростая алгебра над $\mathbb{L}$. Простые A-модули $\langle e_i\rangle$ попарно неизоморфны, поскольку $\varphi_1,\ldots,\varphi_n$ — *различные* вложения поля $\mathbb{F}$ в поле $\mathbb{L}$. Число различных простых модулей над полупростой алгеброй не превосходит ее размерности, поэтому $A=\mathbb{L}^n$.

Гомоморфизм ψ продолжается с $\mathbb{F}$ на $\mathbb{L}\otimes_{\mathbb{k}}\mathbb{F}$ по $\mathbb{L}$-линейности. Из совпадения размерностей $\mathbb{L}\otimes_{\mathbb{k}}\mathbb{F}$ и A следует, что $\psi:\mathbb{L}\otimes_{\mathbb{k}}\mathbb{F}\to\mathbb{L}^n$ — изоморфизм. □

Выведем из доказанной нами теоремы следствие 10.1.

Пусть $(a_1,\ldots,a_n)$ — какой-нибудь базис $\mathbb{F}$ над $\mathbb{k}$. Положим $f_i=\psi(a_i)$. Векторы f_i порождают над полем $\mathbb{k}$ образ гомоморфизма ψ и, следовательно, они порождают над полем $\mathbb{L}$ алгебру A. Поскольку $A=\mathbb{L}^n$, отсюда следует, что эти векторы составляют базис пространства $\mathbb{L}^n$. Для любого элемента $a\in\mathbb{F}$ матрица оператора $L(a)$ в базисе (a_i) совпадает с матрицей оператора $L(\psi(a))$ в базисе (f_i). Однако в базисе (e_i) оператор $L(\psi(a))$ записывается диагональной матрицей с элементами $\varphi_1(a),\ldots,\varphi_n(a)$ по диагонали. Отсюда немедленно следует утверждение следствия 10.1.

Следствие 11.1. *Пусть $\mathbb{F}/\mathbb{k}$ — конечное сепарабельное расширение. Тогда $\mathbb{k}$-линейный функционал $\mathrm{tr}:\mathbb{F}\to\mathbb{k}$ ненулевой. Соответственно, $\mathbb{k}$-билинейная форма на $\mathbb{F}$, заданная формулой $(a,b)=\mathrm{tr}(ab)$ является невырожденной.*

Доказательство. $\mathbb{L}$-линейная функция $\xi:\mathbb{L}^n\to\mathbb{L}$, заданная формулой $\xi(c_1,\ldots,c_n)=c_1+\cdots+c_n$, является ненулевой. Поскольку $\psi:\mathbb{L}\otimes_{\mathbb{k}}\mathbb{F}\to\mathbb{L}^n$ — изоморфизм, то и $\mathbb{L}$-линейная функция $\xi\circ\psi:\mathbb{L}\otimes_{\mathbb{k}}\mathbb{F}\to\mathbb{L}$ ненулевая, значит и её ограничение на $\mathbb{F}$ — ненулевая $\mathbb{k}$-линейная функция. А это и есть след.

Утверждение о билинейной форме сразу следует из нетривиальности следа. Действительно, пусть $c\in\mathbb{F}$ — такой элемент, что $\mathrm{tr}(c)\neq 0$. Для любого ненулевого $a\in\mathbb{F}$ положим $b=ca^{-1}$. Тогда $(a,b)=\mathrm{tr}(c)\neq 0$. □

Целые расширения колец. Напомню, что под кольцом понимается коммутативное ассоциативное кольцо с единицей.

Определение 6. Кольцо A называется *расширением кольца* R, если $R\subseteq A$ и единица кольца R является также единицей кольца A. При этом кольцо A называется *конечным расширением* кольца R, если A является конечнопорождённым R-модулем.

Определение 7. Пусть кольцо A является расширением кольца R. Элемент $a\in A$ называется *целым* над R, если $f(a)=0$ для некоторого многочлена $f(x)\in R[x]$ со старшим коэффициентом единица.

Упражнение 4. Доказать, что если элемент $a\in A$ цел над R, то подкольцо $R[a]\subseteq A$ является конечным расширением кольца R.

Определение 8. Пусть R — произвольное кольцо. R-модуль V называется *точным*, если для любого ненулевого элемента $r \in R$ найдется такой элемент $v \in V$, что $rv \neq 0$.

Теорема 12. *Пусть A — расширение кольца R, и $a \in A$. Если существует точный $R[a]$-модуль V, конечнопорожденный как R-модуль, то элемент a цел над R.*

Доказательство. Пусть $v_1, \ldots, v_n$ порождают V как R-модуль. Определим матрицу $C = (c_{ij})$ из условий $av_j = \sum c_{ij} v_i$ для всех $j = 1, \ldots, n$. (Этими условиями матрица C определяется, вообще говоря, неоднозначно.)

Для любого многочлена $f(x) \in R[x]$ элемент $f(a) \in R[a]$ действует на образующие модуля V по формуле $f(a)v_j = \sum d_{ij} v_i$, где $D = (d_{ij}) = f(C)$. Пусть $f(x) = \det(xE - C)$ — характеристический многочлен матрицы C. По теореме Гамильтона–Кэли $f(C) = 0$. Поэтому $f(a)$ действует нулевым образом на каждую образующую модуля V и, следовательно, на любой элемент этого модуля. Поскольку $R[a]$-модуль V точен, отсюда следует, что $f(a) = 0$. Старший коэффициент многочлена $f(x)$ равен 1. Поэтому элемент a цел над R. $\square$

Следствие 12.1. *Для любого расширения A кольца R элементы A, целые над R, образуют подкольцо.*

Доказательство. Пусть $a, b \in A$ — элементы, целые над R, и $c \in R[a, b]$. Докажем, что c цел над R.

Согласно упражнению 4, кольцо $R[a]$ является конечнопорожденным R-модулем, а кольцо $R[a, b]$ — конечнопорожденным $R[a]$-модулем (поскольку элемент b, целый над R, является, тем самым, целым и над $R[a]$). Пусть $a_1, \ldots, a_k$ — образующие $R[a]$ как R-модуля, а $b_1, \ldots, b_m$ — образующие $R[a, b]$ как $R[a]$-модуля. Тогда элементы вида $a_i b_j$ порождают, очевидно, $R[a, b]$ как R-модуль. Ясно, что $R[a, b]$ является точным $R[c]$-модулем (напомню, что все рассматриваемые кольца — с единицей). По теореме 12, отсюда следует, что c цел над R.

В частности, если a, b — целые над R элементы кольца A, то $-a$, $a + b$ и ab — тоже целые над R. Поэтому целые элементы образуют подкольцо. $\square$

Определение 9. Пусть A — расширение кольца R. Подкольцо C кольца A, состоящее из всех элементов $a \in A$, целых над R, называется *целым замыканием* R в A. Если $C = R$, то R называется *целозамкнутым в* A. Если $C = A$, то A называется *целым над* R. Область целостности называется *целозамкнутой* (без указания, в каком кольце), если она целозамкнута в своем поле частных.

Упражнение 5. Доказать, что если R — факториальное кольцо, то оно целозамкнуто.