§1. Коммутативные кольца и алгебры.

В этом семестре слово «кольцо» по умолчанию означает *коммутативное кольцо с единицей*, и гомоморфизмы колец по умолчанию преполагаются отображающими единицу в единицу.

1.1. Целые элементы и целые расширения. Рассмотрим коммутативное кольцо B и его подкольцо $A \subset B$. Элемент $b \in B$ называется *целым* над A, если он удовлетворяет условиям следующей леммы.

1.1.1. ЛЕММА. *Слюдующие свойства элемента $b \in B$ попарно эквивалентны:*

(1) $b^m = a_1 b^{m-1} + \cdots + a_{m-1} b + a_0$ *для некоторого* $m \in \mathbb{N}$ *и некоторых* $a_1, a_2, \dots, a_m \in A$;

(2) A*-модуль, натянутый на все неотрицательные степени* $\{b^i\}_{i \geqslant 0}$, *линейно порождается над* A *конечным числом элементов;*

(3) *существует конечно порожденный над* A *и* B*-точный*[1] A*-подмодуль* $M \subset B$, *такой что* $bM \subset M$.

Доказательство. Импликации (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) тривиальны. Чтобы вывести (1) из (3), допустим, что $\{e_1, e_2, \dots, e_m\}$ порождают M над A и что оператор умножения $M \xrightarrow{m \mapsto bm} M$ представляется матрицей Y, т. е. $(be_1, be_2, \dots, be_m) = (e_1, e_2, \dots, e_m) \cdot Y$. Заметим, что если линейное отображение $M \xrightarrow{\varkappa} M$ представляется матрицей X, т. е. переводит $(e_1, e_2, \dots, e_m) \longmapsto (e_1, e_2, \dots, e_m) \cdot X$, то $(\det X) \cdot M \subset \operatorname{im} \varkappa$ (это получается применением к $(e_1, e_2, \dots, e_m)$ обеих частей матричного тождества $\det X \cdot \mathrm{Id} = X \cdot \widehat{X}$, в котором $\widehat{X}$ — присоединённая к X матрица из алгебраических дополнений). В нашем случае нулевой оператор $M \xrightarrow{\varkappa} 0$ представляется матрицей $X = b \cdot \mathrm{Id} - Y$, а значит, умножение на $\det(b \cdot \mathrm{Id} - Y)$ аннулирует M. Из B-точности модуля M вытекает тогда, что $\det(b \cdot \mathrm{Id} - Y) = 0$. Это полиномиальное уравнение относительно b с коэффициентами из A и старшим членом b^m, как и требуется в (1). $\square$

1.1.2. Пример: целые алгебраические числа. Пусть $K \supset \mathbb{Q}$ — конечномерное[2] расширение полей. Элементы $z \in K$ называются *алгебраическими числами*. Алгебраическое число z является целым над $\mathbb{Z}$ тогда и только тогда, когда когда существует инвариантное относительно умножения на z подпространство $W \subset K$ и некоторый базис в нём, такой что умножение на z записывается в этом базисе целочисленной матрицей[3].

Упражнение 1.1. Докажите, что подходящее целочисленное кратное произвольного алгебраического числа является целым алгебраическим числом и что у поля K всегда можно выбрать базис над $\mathbb{Q}$, состоящий из целых алгебраических чисел.

Упражнение 1.2. Опишите все целые (над $\mathbb{Z}$) числа в полях $\mathbb{Q}$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$ и $\mathbb{Q}[\omega]$, где $\omega^2 + \omega + 1 = 0$.

1.1.3. Целое замыкание. Множество всех $b \in B$, целых над данным подкольцом $A \subset B$, называется *целым замыканием* A в B. Если оно не содержит ничего, кроме элементов самого A, то A называется *целозамкнутым* в B. Наоборот, если все $b \in B$ целы над A, то B называется *целым расширением* кольца A или *целой* A*-алгеброй*.

1.1.4. Пример: инварианты действия конечной группы. Пусть конечная группа $\mathfrak{G}$ действует на кольце B кольцевыми автоморфизмами $B \xrightarrow{g} B$ $(g \in \mathfrak{G})$. Тогда B цело над подкольцом $\mathfrak{G}$-инвариантов:

$$A = B^{\mathfrak{G}} \stackrel{\text{def}}{=} \{a \in B \mid ga = a \ \forall g \in \mathfrak{G}\} .$$

Действительно, если $b_1, b_2, \dots, b_s \in B$ образуют $\mathfrak{G}$-орбиту любого данного $b = b_1 \in B$, то многочлен $\beta(t) = \prod (t - b_i)$ имеет старший коэффициент 1, лежит в $A[t]$ и аннулирует b.

[1] A-модуль M называется B*-точным*, если для всякого $b \in B$ условие $bM = 0$ влечет равенство $b = 0$

[2] как векторное пространство над $\mathbb{Q}$

[3] исторически понятие целого элемента именно так и возникло

1.1.5. ЛЕММА. *Целое замыкание A является подкольцом*[4] *в B. Если $C \supset B$ — другое коммутативное кольцо и элемент $c \in C$ цел над целым замыканием A в B, то c цел и над A (в частности, если B — целая A-алгебра, то любая целая B-алгебра является также и целой A-алгеброй).*

Доказательство. Если $p^m = x_{m-1}\,p^{m-1} + \cdots + x_1\,p + x_0$, $\quad q^n = y_{n-1}\,q^{n-1} + \cdots + y_1\,q + y_0$ для $p, q \in B$, $x_\nu, y_\mu \in A$, то A-модуль, натянутый на $p^i q^j$ с $0 \leqslant i \leqslant (m-1)$, $0 \leqslant j \leqslant (n-1)$, является B-точным (ибо содержит 1) и переходит в себя при умножении и на $p+q$ и на pq. Аналогично, если $c^r = z_{r-1}\,c^{r-1} + \cdots + z_1\,c + z_0$ и все z_ν — целые над A, то умножение на c сохраняет B-точный A-модуль, натянутый на достаточное число произведений $c^i z_1^{j_1} z_2^{j_2} \cdots z_r^{j_r}$. □

1.1.6. СЛЕДСТВИЕ (ЛЕММА ГАУССА). *Пусть $A \subset B$ — произвольное расширение коммутативных колец, и многочлены $f, g \in B[x]$ оба имеют старший коэффициент 1. Все коэффициенты их произведения $h(x) = f(x)g(x)$ тогда и только тогда будут целыми над A, когда целы над A все коэффициенты и у $f(x)$ и у $g(x)$.*

Доказательство. Рассмотрим какое-либо расширение $C \supset B$, над которым f и g полностью разалагаются на линейные множители[5], т. е. $f(x) = \prod(t - \alpha_\nu)$, $g(x) = \prod(t - \beta_\mu)$ в $C[x]$ для некоторых $\alpha_\nu, \beta_\mu \in C$. По лемме из n° 1.1.5, все коэффициенты $h(x) = \prod(t - \alpha_\nu)\prod(t - \beta_\mu)$ являются целыми над $A \iff$ все α_ν, β_μ являются целыми над $A \iff$ все коэффициенты $f(x)$ и $g(x)$ являются целыми над A. □

1.1.7. ЛЕММА. *Пусть $B \supset A$ — целое над A. Если B — поле, то A также является полем. Наоборот, если A — поле, и в B нет делителей нуля, то B — поле.*

Доказательство. Если B — поле, целое над A, то обратный элемент $a^{-1} \in B$ к произвольному ненулевому $a \in A$ удовлетворяет уравнению $a^{-m} = \alpha_1\,a^{1-m} + \cdots + \alpha_{m-1}\,a^{-1} + \alpha_0$ с $\alpha_\nu \in A$. Умножая обе части на a^{m-1}, получаем $a^{-1} = \alpha_1 + \cdots + \alpha_{m-1}\,a^{m-2} + \alpha_0\,a^{m-1} \in A$. Обратно, если A — поле, и B — целая A-алгебра, то все неотрицательные целые степени b^i любого $b \in B$ порождают конечномерное векторное пространство V над A. Если $b \neq 0$, и в B нет делителей нуля, то линейный оператор $V \xrightarrow{x \mapsto bx} V$ не имеет ядра, а потому — биективен. Прообраз $1 \in V$ относительно этого оператора и есть b^{-1}. □

1.1.8. Пример: нормальные кольца. Коммутативное кольцо A без делителей нуля называется *нормальным*, если A целозамкнуто в своём поле частных Q_A. В частности, любое поле, по определению, нормально. Из упр. 1.2 вытекает, что кольцо $\mathbb{Z}$ нормально. Точно так же доказывается, что *любое факториальное кольцо A нормально*: многочлен $a_0 t^m + a_1 t^{m-1} + \cdots + a_{m-1} t + a_m \in A[t]$ аннулирует дробь $p/q \in Q_A$ с $\text{нод}(p, q) = 1$, только если $q | a_0$ и $p | a_m$, а стало быть, $a_0 = 1 \Rightarrow q = 1$.

Если кольцо A нормально, то из леммы Гаусса (см. n° 1.1.6) вытекает более традиционная её версия: если $f \in A[x]$ раскладывается $Q_A[x]$ на два множителя со старшими коэффициентами 1, то оба они автоматически лежат в $A[x]$.

1.2. Алгебраичность. Если кольцо $A = \Bbbk$ является полем, то целость над $\Bbbk$ элемента b какой-либо $\Bbbk$-алгебры $B \supset \Bbbk$ равносильна его *алгебраичности* над $\Bbbk$, т. е. тому, что b удовлетворяет *какому-нибудь* уравнению $f(b) = 0$ с ненулевым $f \in \Bbbk[x]$ или, что то же самое, тому что *гомоморфизм вычисления*

$$\mathrm{ev}_b \,:\, \Bbbk[x] \xrightarrow{f(x) \mapsto f(b)} B \tag{1-1}$$

имеет ненулевое ядро. Образ гомоморфизма (1-1) обозначается через $\Bbbk[b]$ и представляет собою наименьшую $\Bbbk$-подалгебру в B, содержащую 1 и b.

Если b не алгебраичен[6], то $\ker \mathrm{ev}_b = 0$ и гомоморфизм (1-1) отождествляет $\Bbbk[b]$ с кольцом многочленов (в частности, $\Bbbk[b]$ в этом случае бесконечномерно как векторное пространство над $\Bbbk$). Если b алгебраичен, то поскольку $\Bbbk[x]$ является областью главных идеалов, $\ker(\mathrm{ev}_b) = (\mu_b)$, где

[4] в частности, все A-кратные целых элементов — целые

[5] Для любого коммутативного кольца B и любого непостоянного $h(x) \in B[x]$ со старшим коэффициентом 1 существует коммутативное кольцо $C \supset B$ и $c_\nu \in C$, такие что $h(x) = \prod(x - c_\nu)$ в $C[x]$. Они строятся по индукции следующим образом. Фактор кольцо $F = B[x]/(f)$ содержит B как подкольцо классов вычетов констант, а элемент $\varkappa \stackrel{\text{def}}{=} x \pmod{h} \in F$ является корнем h. Это означает, что остаток от деления $h(x)$ на $(x - \varkappa)$ в $F[x]$ равен нулю, и в $F[x]$ мы имеем разложение $h(x) = (x - \varkappa) \cdot \widetilde{h}(x)$. Далее повторяем эту процедуру для $\widetilde{h}$ и F вместо h, B и т. д.

[6] элементы, не являющиеся алгебраическими (над $\Bbbk$), также называют *трансцендентными* (над $\Bbbk$)

$\mu_b \in \Bbbk[x]$ однозначно задаётся как многочлен наименьшей степени со старшим коэффициентом 1, аннулирующий b. Многочлен μ_b называется *минимальным многочленом* элемента b над $\Bbbk$. Если он неприводим (что равносильно отсутствию делителей нуля в $\Bbbk[b] = \Bbbk[x]/(\mu_b)$), то алгебра $\Bbbk[b]$ автоматически является полем (см. n° 1.1.7).

Упражнение 1.3. Свяжите размерность $\Bbbk[b]$ как векторного пространства над $\Bbbk$ с $\deg \mu_b$.

1.2.1. ЛЕММА. *Пусть поле $\Bbbk = Q_A$ является полем частных коммутативного кольца A без делителей нуля. Если элемент b какой-либо Q_A-алгебры B цел над A, то он алгебраичен над Q_A и все коэффициенты его минимального многочлена $\mu_b \in Q_A[x]$ целы над A.*

Доказательство. Поскольку b цел над A, он удовлетворяет уравнению $f(b) = 0$, в котором $f \in A[x]$ имеет старший коэффициент 1. Тем самым, $\ker \mathrm{ev}_b \neq 0$ и $f = \mu_b \cdot q$ в кольце $Q_A[x]$. По лемме Гаусса (см. n° 1.1.6), все коэффициенты и у μ_b, и у q должны быть целы над A. □

1.2.2. СЛЕДСТВИЕ. *Пусть A — нормальное кольцо (см. n° 1.1.8) с полем частных Q_A, и B — произвольная Q_A-алгебра. Если элемент $b \in B$ цел над A, то его минимальный многочлен над полем Q_A автоматически лежит в $A[x]$.* □

1.3. Конечно порожденные коммутативные $\Bbbk$-алгебры. Пусть $\Bbbk$ — произвольное поле. Коммутативная $\Bbbk$-алгебра B называется *конечно порожденной*, если она является фактор алгеброй кольца многочленов от конечного числа переменных с коэффициентами из $\Bbbk$, т. е. если существует эпиморфизм $\Bbbk$-алгебр

$$\Bbbk[x_1, x_2, \dots, x_m] \xrightarrow{\pi} B \,.$$

Образы $b_i = \pi(x_i) \in B$ называются *образующими алгебры* B, а $\ker \pi \subset \Bbbk[x_1, x_2, \dots, x_m]$ называется *идеалом соотношений* между ними.

1.3.1. ТЕОРЕМА. *Конечно порожденная $\Bbbk$-алгебра может быть полем только если все её элементы алгебраичны над $\Bbbk$.*

Доказательство. Пусть $\Bbbk$-алгебра B порождается элементами $\{b_1, b_2, \dots, b_m\}$ и является полем. Доказывать алгебраичность B будем индукцией по m. Случай $m = 1$, $B = \Bbbk[b]$ очевиден: если b трансцендентен, то гомоморфизм (1-1) отождествляет B с кольцом многочленов $\Bbbk[x]$, которое не является полем.

Пусть $m > 1$. Если b_m алгебраичен над $\Bbbk$, то $\Bbbk[b_m]$ — поле и B алгебраично над $\Bbbk[b_m]$ по предположению индукции. По лемме n° 1.1.5 B будет тогда алгебраично и над $\Bbbk$. Таким образом, достаточно показать, что b_m *должен* быть алгебраичен над $\Bbbk$.

Допустим, что b_m трансцендентен. Тогда гомоморфизм (1-1) продолжается до изоморфизма поля рациональных функций $\Bbbk(x)$ с наименьшим подполем $\Bbbk(b_m) \subset B$, содержащим b_m. По предположению индукции, B алгебраично над $\Bbbk(b_m)$, так что каждая из образующих $b_1, b_2, \dots, b_{m-1}$ удовлетворяет некоторому полиномиальному уравнению с коэффициентами из $\Bbbk(b_m)$. Умножая эти уравнения на подходящие многочлены от b_m, мы можем добиться того, чтобы все их коэффициенты лежали в $\Bbbk[b_m]$, а также сделать все их старшие коэффициенты равными одному и тому же многочлену, который мы обозначим через $p(b_m) \in \Bbbk[b_m]$. В результате поле B оказывается целым над подалгеброй $F = \Bbbk[b_m\,,\, 1/p(b_m)] \subset B$, порожденной над $\Bbbk$ элементами b_m и $1/p(b_m)$. По лемме n° 1.1.7 эта подалгебра F должна быть полем, что невозможно, поскольку, скажем, $1 + p(b_m)$ не обратим в F.

В самом деле, если существует многочлен $g \in \Bbbk[x_1, x_2]$, такой что $g\,(\,b_m\,,\, 1/p(b_m)\,) \cdot (1 + p(b_m)) = 1$, то, записывая рациональную функцию $g\,(\,x\,,\, 1/p(x)\,)$ в виде $h(x)/p^k(x)$, где $h \in \Bbbk[x]$ не делится на p, и умножая обе части предыдущего равенства на $p^k(b_m)$, мы получим на b_m полиномиальное уравнение $h(b_m) \cdot (p(b_m) + 1) = p^{k+1}(b_m)$, которое нетривиально, поскольку $h(x)(1 + p(x))$ не делится на $p(x)$. □

1.3.2. СЛЕДСТВИЕ. *Всякое поле $\mathbb{F}$, которое конечно порождено как алгебра над своим подполем $\Bbbk \subset \mathbb{F}$, конечномерно как векторное пространство над $\Bbbk$ (число $[\mathbb{F} : \Bbbk] \stackrel{\text{def}}{=} \dim_\Bbbk \mathbb{F}$ называется в этом случае степенью расширения $\Bbbk$ до $\mathbb{F}$).* □

1.3.3. Базисы трансцендентности. Предположим, что $\Bbbk$-алгебра A не имеет делителей нуля. Мы обозначаем через Q_A ее поле частных, а через $\Bbbk(a_1, a_2, \dots, a_m) \subset Q_A$ — наименьшее подполе,

содержащее заданные элементы $a_1, a_2, \ldots, a_m \in A$. Элементы $a_1, a_2, \ldots, a_m \in A$ называются *алгебраически независимыми* над $\Bbbk$, если между ними нет никаких полиномиальных соотношений вида
$$\varphi(a_1, a_2, \ldots, a_m) = 0 \quad \text{с } f \in A[x_1, x_2, \ldots, x_m]\ ,$$
т. е. если отображение вычисления $\mathrm{ev}_{(a_1,a_2,\ldots,a_m)} : \Bbbk[x_1, x_2, \ldots, x_m] \xrightarrow{x_i \mapsto a_i} A$ иньективно. Если $a_1, a_2, \ldots, a_m$ алгебраически независимы, то отображение вычисления продолжается до вложения полей
$$\Bbbk(x_1, x_2, \ldots, x_m) \xhookrightarrow{f(x_1,x_2,\ldots,x_m) \mapsto f(a_1,a_2,\ldots,a_m)} Q_A\ .$$
Алгебраически независимый набор элементов $a_1, a_2, \ldots, a_m \in A$ называется *базисом трансцендентности* для A, если любой $p \in A$ алгебраичен над $\Bbbk(a_1, a_2, \ldots, a_m)$. В этом случае, любой $q \in Q_A$ также алгебраичен над $\Bbbk(a_1, a_2, \ldots, a_m)$, ибо по лемме из n° 1.1.7 целое замыкание $\Bbbk(a_1, a_2, \ldots, a_m)$ в Q_A является полем, содержащим A, а значит, и Q_A.

1.3.4. ЛЕММА. *Любая конечно порожденная $\Bbbk$-алгебра A без делителей нуля либо алгебраична над $\Bbbk$, либо имеет базис трансцендентности, который можно строить, выкидывая лишние элементы из произвольного набора $a_1, a_2, \ldots, a_m \in A$, такого что A алгебраична над $\Bbbk(a_1, a_2, \ldots, a_m)$ (в частности, любая система образующих A как $\Bbbk$-алгебры содержит некоторый базис трансцендентности).*

Доказательство. Если имеется полиномиальное соотношение $\varphi(a_1, a_2, \ldots, a_m) = 0$, скажем, содержащее a_m, то мы удалим a_m. Если остающиеся $a_1, a_2, \ldots, a_{m-1}$ удовлетворяют полиномиальному соотношению, содержащему a_{m-1}, мы удалим a_{m-1} и т. д.. В конечном счете, мы получим либо алгебраически независимый набор элементов, скажем, $a_1, a_2, \ldots, a_s$, либо ровно один алгебраичный над $\Bbbk$ элемент, к примеру, a_1. Как бы то ни было, лемма из n° 1.1.5 показывает, что все прочие a_ν, а сними и всё A, алгебраичны либо над $\Bbbk(a_1, a_2, \ldots, a_s)$, либо даже над $\Bbbk$. □

1.3.5. ЛЕММА. *Если Q_A алгебраично над $\Bbbk(a_1, a_2, \ldots, a_r)$ для некоторых $a_1, a_2, \ldots, a_r \in A$, то в A не существует алгебраически независимой системы из $n > r$ элементов $b_1, b_2, \ldots, b_n \in A$.*

Доказательство. Удаляя часть a_ν, мы можем предположить, что $a_1, a_2, \ldots, a_s$ составляют базис трансцендентности для A. Пусть $b_1, b_2, \ldots, b_n \in A$ алгебраически независимы. Поскольку b_1 алгебраичен над $\Bbbk(a_1, a_2, \ldots, a_r)$, имеется полиномиальное соотношение $\varphi(b_1, a_1, a_2, \ldots, a_r) = 0$, в котором присутствует как b_1, так и какой-нибудь из a_ν, допустим, a_1. Тогда Q_A алгебраично над подалгеброй, натянутой на $\{b_1, a_2, a_3, \ldots, a_r\}$. В то же время, никаких полиномиальных соотношений вида $\varphi(b_1, a_2, a_3, \ldots, a_r)$ нет, поскольку иначе Q_A было бы алгебраично уже над $\Bbbk(a_2, \ldots, a_r)$. Таким образом, набор
$$\{b_1, a_2, a_3, \ldots, a_r\}$$
тоже является базисом трансцендентности для A. По тем же причинам и все наборы
$$\{b_1, \ldots, b_s, a_{s+1}, \ldots, a_r\}$$
(возможно, после некоторой перенумерации элементов a_ν и b_ν) являются базисами трансцендентности для A при всех $s = 2, 3, \ldots, r$. В частности, $b_{r+1}, \ldots, b_n$ будут алгебраичны над $\Bbbk(b_1, \ldots, b_r)$. □

1.3.6. СЛЕДСТВИЕ. *Все базисы трансцендентности имеют одинаковую мощность (она называется степенью трансцендентности алгебры A и обозначается* $\operatorname{tr}\deg A$*).* □

1.4. Нетеровость. Любой набор элементов $f_1, f_2, \ldots, f_n$ произвольного коммутативного кольца A порождает в A идеал $(f_1, f_2, \ldots, f_m) = \{g_1 f_1 + g_2 f_2 + \cdots + g_m f_m \mid g_\nu \in A\}$, который, как A-модуль, представляет собою A-линейную оболочку[7] элементов f_ν. Коммутативное кольцо A называется *нётеровым*, если оно удовлетворяет условиям леммы:

1.4.1. ЛЕММА. *Следующие свойства коммутативного кольца A попарно эквивалентны:*

[7]подчеркнём, что даже если набор элементов $\{f_\nu\}$ бесконечен, порождаемый ими идеал (т. е. минимальный по включению идеал, содержащий все эти элементы) по-прежнему состоит из *конечных* A-линейных комбинаций элементов f_ν

(1) *любое множество элементов f_ν содержит некоторое конечное подмножество, которое порождает тот же идеал, что и само множество;*

(2) *любой идеал допускает конечное множество образующих;*

(3) *для любой бесконечной цепочки вложенных идеалов $I_1 \subset I_2 \subset I_3 \subset \cdots$ существует $n \in \mathbb{N}$ такое, что $I_\nu = I_n \quad \forall \nu \geqslant n$.*

Доказательство. Ясно, что (1) $\Rightarrow$ (2). Чтобы из (2) вывести (3), возьмем конечное множество образующих для идеала $I = \bigcup I_\nu$, и т. к. все они принадлежат некоторому I_n, получим $I_\nu = I_n = I \ \forall \ \nu \geqslant n$. Наконец, (1) следует из (3), примененного к цепочке $I_n = (f_1, f_2, \dots, f_n)$, где f_i выбираются из $\{f_\nu\}$ так, чтобы $f_\nu \notin (f_1, f_2, \dots, f_{\nu-1})$. □

1.4.2. ТЕОРЕМА. *Если A нётерово, то кольцо многочленов $A[x]$ также нётерово.*

Доказательство. Рассмотрим произвольный идеал $I \subset A[x]$ и обозначим через $L_d \subset A$ множество старших коэффициентов всех многочленов степени d из I. Ясно, что и каждое отдельное L_d, и их объединение $L_\infty \stackrel{\text{def}}{=} \bigcup\limits_d L_d$ являются идеалами в A и, стало быть, конечно порождены. Строить конечный базис в I мы начнём с набора многочленов $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{s_\infty}^{(\infty)} \in I$, старшие коэффициенты которых порождают идеал $L_\infty \subset A$. Пусть $\max_\nu \left(\deg f_\nu^{(\infty)}\right) = m$.

Упражнение 1.4. Покажите, что по модулю многочленов $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{s_\infty}^{(\infty)}$ всякий $f \in I$ представляется многочленом степени строго меньшей, чем m.

Теперь для каждого $k = 1,\, 2,\, \dots,\, (m-1)$ обозначим через $f_1^{(k)}, f_2^{(k)}, \dots, f_{s_k}^{(k)}$ многочлены, старшие коэффициенты которых порождают идеал L_k. То же рассуждение, что и в упр. 1.4, показывает, что $s_0 + \dots + s_{m-1} + s_\infty$ многочленов $f_\nu^{(\mu)}$ с $\mu = 0,\, 1\, \dots,\, (m-1),\, \infty$ порождают идеал I. □

1.4.3. СЛЕДСТВИЕ. *Если A нётерово, то $A[x_1, x_2, \dots, x_n]$ тоже нётерово.* □

1.4.4. СЛЕДСТВИЕ. *Всякая конечно порожденная алгебра над полем нётерова.*

Доказательство. Полиномиальная алгебра $\Bbbk[x_1, x_2, \dots, x_n]$, где $\Bbbk$ — поле, нётерова по предыдущему следствию. Любая ее факторалгебра A также нётерова, поскольку полный прообраз любого идеала $I \subset A$ при эпиморфизме $\Bbbk[x_1, x_2, \dots, x_n] \twoheadrightarrow A$ является конечнопорождённым идеалом в $\Bbbk[x_1, x_2, \dots, x_n]$, и образы его образующих в A порождают I. □

1.5. Полиномиальные уравнения и идеалы. Любая (в том числе бесконечная) система полиномиальных уравнений $f_\nu(x_1, x_2, \dots, x_n) = 0$ с $f_\nu \in \Bbbk[x_1, x_2, \dots, x_n]$ эквивалентна системе, левые части которой образуют идеал, порождённый исходными уравнениями. В силу нётеровости кольца многочленов такая система, в свою очередь, эквивалентна конечной системе уравнений, левые части которых порождают тот же идеал, что и исходные уравнения. Множество всех решений системы полиномиальных уравнений, левые части которых составляют идеал $J \subset \Bbbk[x_1, x_2, \dots, x_n]$, изображается в аффинном пространстве $\mathbb{A}^n$ фигурой

$$V(J) \stackrel{\text{def}}{=} \{a \in \mathbb{A}_n \mid f(a) = 0 \quad \forall\, f \in J\}\,,$$

которая называется *аффинным алгебраическим многообразием* (и запросто может оказаться пустым множеством, как это происходит, к примеру, для несобственного идеала $I = (1)$).

С другой стороны, для любой фигуры $\varPhi \subset \mathbb{A}^n$ множество всех многочленов, тождественно зануляющихся на $\varPhi$, образует идеал

$$I(\varPhi) \stackrel{\text{def}}{=} \{\, f \in \Bbbk[x_1, x_2, \dots, x_n] \mid f(p) = 0 \quad \forall\, p \in \varPhi\,\}\,.$$

Множество нулей этого идеала $V(I(\varPhi))$ представляет собою наименьшее аффинное алгебраическое многообразие, содержащее $\varPhi$. Для любого идеала $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ имеется тавтологическое включение $J \subset I(V(J))$, которое, вообще говоря, является строгим — например, для $J = (x^2) \in \mathbb{C}[x]$ имеем $V(J) = \{0\} \subset \mathbb{A}^1(\mathbb{C})$ и $I(V(J)) = (x)$.

1.5.1. ТЕОРЕМА ГИЛЬБЕРТА О НУЛЯХ (NULLSTELLENSATZ). *Над произвольным алгебраически замкнутым полем $\Bbbk$ для любого идеала $J \subset \Bbbk[x_1, x_2, \ldots, x_n]$ справедливы следующие утверждения*

(1) *слабая теорема о нулях:* $V(J) = \varnothing \iff 1 \in J$;

(2) *сильная теорема о нулях:* $f \in I(V(J)) \iff f^m \in J$ *для некоторого* $m \in \mathbb{N}$.

Доказательство. Чтобы доказать (1), достаточно для каждого собственного идеала $J \subset \Bbbk[x_1, x_2, \ldots, x_n]$ найти точку $p \in \mathbb{A}_n$, в которой зануляются все многочлены из J. При этом без ограничения общности можно считать, что любой многочлен $g \notin J$ обратим по модулю J. Действительно, необратимость $g \notin J$ по модулю J означает неразрешимость уравнения $gh + f = 1$ относительно $h \in \Bbbk[x_1, x_2, \ldots, x_n]$ и $f \in J$, т.е. собственность идеала (g, J), порождённого g и J. Заменяя J на (g, J), мы лишь усложняем себе задачу, и после конечного числа таких замен мы получим максимальный собственный идеал J, для которого $\Bbbk[x_1, x_2, \ldots, x_n]/J$ является полем. Поскольку это поле конечно порождено как $\Bbbk$-алгебра, оно является алгебраическим расширением поля $\Bbbk$ конечной степени (см. n° 1.3.1 – n° 1.3.2), и поскольку $\Bbbk$ алгебраически замкнто, мы приходим к равенству $\Bbbk[x_1, x_2, \ldots, x_n]/J = \Bbbk$, которое означает, что любой многочлен $f \in \Bbbk[x_1, x_2, \ldots, x_n]$ сравним с константой по модулю J. Искомая точка $p = (p_1, p_2, \ldots, p_n)$ имеет в качестве координат константы $p_i \equiv x_i \pmod J$.

В (2) нетривиальна только импликация «$\Rightarrow$» для непустого многообразия $V(J) \subset \mathbb{A}^n$. Чтобы доказать ее, мы вложим $\mathbb{A}^n$ в большее пространство $\mathbb{A}^{n+1}$ с координатами $(t, x_1, x_2, \ldots, x_n)$ в качестве гиперплоскости $t = 0$. Если $f \in \Bbbk[x_1, x_2, \ldots, x_n] \subset \Bbbk[t, x_1, x_2, \ldots, x_n]$ тождественно обращается в нуль на $V(J)$, то идеал $J' \subset \Bbbk[t, x_1, x_2, \ldots, x_n]$, порожденный J и многочленом $g(t, x) = 1 - t\,f(x)$, имеет пустое множество нулей в $\mathbb{A}^{n+1}$, поскольку $g(x, t) \equiv 1$ вдоль цилиндра $V(J) \subset \mathbb{A}^{n+1}$. По слабой теореме о нулях, $1 \in J'$, т.е. существуют $q_0, q_1, \ldots, q_s \in \Bbbk[t, x_1, x_2, \ldots, x_n]$ и $f_1, f_2, \ldots, f_s \in J$, такие что

$$q_0(x,t)(1 - tf(x)) + q_1(t,x)f_1(x) + \cdots + q_s(x,t)f_s(x) = 1 \,.$$

Гомоморфизм $\Bbbk[t, x_1, x_2, \ldots, x_n] \longrightarrow k(x_1, x_2, \ldots, x_n)$, переводящий $t \longmapsto 1/f(x)$, $x_\nu \longmapsto x_\nu$, отображает это равенство в равенство $q_1(1/f(x)\,,\,x)\,f_1(x) + \cdots + q_s(1/f(x)\,,\,x)\,f_s(x) = 1$ в поле рациональных функций $\Bbbk(x_1, x_2, \ldots, x_n)$. Поскольку идеал J не содержит 1, некоторые из $q_\nu(1/f(x), x)$ должны иметь ненулевые знаменатели, каковые являются степенями f. Поэтому, умножение на подходящую степень f^m ведет к искомому выражению $\widetilde{q}_1(x)\,f_1(x) + \cdots + \widetilde{q}_s(x)\,f_s(x) = f^k(x)$ с $\widetilde{q}_\nu \in \Bbbk[x_1, x_2, \ldots, x_n]$. □

1.5.2. Пример: одноточечные множества. Аффинное алгебраическое многообразие $V(J) \subset \mathbb{A}(V)$ тогда и только тогда состоит из единственной точки — начала координат $\{O\} \in \mathbb{A}(V)$, когда $J \supset S^d V^*$ для всех $d \gg 0$ и $1 \notin I$, или (что то же самое) когда $0 < \dim \Bbbk[x_1, x_2, \ldots, x_n]/J < \infty$. Действительно, если J содержит некоторые степени $x_i^{m_i}$ всех координатных функций, то $V(J) = \{O\}$. Наоборот, если $V(J) = \{0\}$, то все x_i зануляются на $V(J)$ и по сильной теореме о нулях $x_i^{m_i} \in J$ для некоторых $m_i \in \mathbb{N}$. Тогда $S^d V^* \subset I$ для $d \geqslant 1 + \sum(m_\nu - 1)$.

Упражнение 1.5. Докажите, что идеал $I(\{O\})$ максимален и порождается $x_1, x_2, \ldots, x_n$.

1.5.3. Пример: системы результантов. Обозначим через $\mathscr{S}_d = \mathbb{P}(S^d V^*)$ пространство гиперповерхностей степени d в $\mathbb{P}_n = \mathbb{P}(V)$, зафиксируем некоторый набор из $m \geqslant 2$ степеней $d_1, d_2, \ldots, d_m$, и рассмотрим множество $\mathscr{R} \subset \mathscr{S}_{d_1} \times \mathscr{S}_{d_2} \times \cdots \times \mathscr{S}_{d_m}$, состоящее из всевозможных наборов m гиперповерхностей $S_1, S_2, \ldots, S_m \subset \mathbb{P}_n$ с непустым пересечением $\bigcap S_\nu \neq \varnothing$. Покажем, что $\mathscr{R}$ является алгебраическим многообразием, т. е. описывается конечной системой мультиоднородных полиномиальных уравнений на коэффициенты форм $(f_1, f_2, \ldots, f_m) \in S^{d_1}V^* \times S^{d_1}V^* \times \cdots \times S^{d_m}V^*$, задающих гиперповерхности $S_1, S_2, \ldots, S_m$.

Пусть $I \subset \Bbbk\langle x_1, x_2, \ldots, x_n\rangle$ — идеал, порожденный формами f_ν. Тогда $\bigcap S_\nu = \varnothing$ в $\mathbb{P}(V) \iff V(I) \subset \mathbb{A}(V)$ либо пусто, либо совпадает с началом координат $\iff S^d V^* \subset I \;\forall\, d \gg 0 \iff$ $\Bbbk$-линейное отображение:

$$\mu_d \;:\; S^{d-d_1}V^* \oplus S^{d-d_2}V^* \oplus \cdots \oplus S^{d-d_m}V^* \xrightarrow{(g_0, g_1, \ldots, g_n) \mapsto \sum g_\nu f_\nu} S^d \tag{1-2}$$

не сюрьективно $\forall\, d \gg 0$. В терминах стандартных мономиальных базисов, μ_d представляется матрицей, элементы которой — линейные формы с коэффициентами из f_ν. При $d \gg 0$ размерность левой части (1-2) (ведущая себя как $\sum\limits_{\nu=1}^{m} \binom{n+d-d_\nu}{n} \sim \frac{m}{n!}\,d^n$) становится больше, чем размерность правой (ведущей себя как $\binom{n+d}{n} \sim \frac{1}{n!}\,d^n$). Поэтому $\mathscr{R}$ задаётся бесконечной системой системой полиномиальных уравнений — обращением в нуль всех максимальных миноров всех матриц μ_d с $d \gg 0$. В силу нётеровости кольца многочленов, эта бесконечная система уравнений эквивалентна некоторой конечной подсистеме, которая называется *системой результантов* (и зависит от m, n и $d_1, d_2, \ldots, d_m$). Так, для $n = 1$, $m = 2$

значение d, для которого размерность левой части (1-2) становится равна размерности правой (а для больших d становится больше) — это $d = d_0 + d_1$. Для этого d отображение μ_d задаётся квадратной матрицей. Определитель этой матрицы называется *определителем Сильвестра* (или *результантом*) пары бинарных форм. Как мы видели в первом семестре, этот определитель порождает идеал результантных соотношений — две бинарные формы степеней d_0, d_1 тогда и только тогда имеют нетривиальный общий делитель (или, что то же самое, — общий нуль на $\mathbb{P}_1$), когда их результант $\det \mu_d = 0$. Таким образом, для $n = 1$, $m = 2$ результантное множество $\mathscr{R}$ является гиперповерхностью.

1.5.4. Как «практически» выяснить, лежит ли f в $(f_1, f_2, \ldots, f_m)$. Зафиксируем на множестве всех мономов[8] в $\Bbbk[x_1, x_2, \ldots, x_n]$ какое-нибудь линейное упорядочение, согласованное с умножением[9], и будем обозначать через f^L старший моном многочлена f относительно этого порядка. Старшие мономы всех многочленов из заданного идеала I порождают идеал I^L, который называется идеалом *главных частей* идеала I.

Упражнение 1.6. Убедитесь, что идеал I^L *мономиальный* (т. е. содержит вместе с каждым многочленом и все его мономы), а также что $(f_1, f_2, \ldots, f_s)^L \supset (f_1^L, f_2^L, \ldots, f_s^L)$ и приведите пример, в котором это включение строгое.

Система образующих $(f_1, f_2, \ldots, f_s)$ данного идеала I называется его *базисом Грёбнера*[10], если $I^L = (f_1^L, f_2^L, \ldots, f_s^L)$. Так, базис идеала $I \subset \Bbbk[x_1, x_2, \ldots, x_n]$, который получается индуктивным применением (неконструктивного) рассуждения из леммы n° 1.4.2, будет именно базисом Грёбнера. Если идеал I задан базисом Грёбнера, то вопрос о принадлежности данного многочлена h этому идеалу решается очень просто.

Упражнение 1.7. Пусть $(f_1, f_2, \ldots, f_s)^L = (f_1^L, f_2^L, \ldots, f_s^L)$. Докажите, что классы всех мономов по модулю мономов, лежащих в идеале[11] $(f_1^L, f_2^L, \ldots, f_s^L)$, составляют базис векторного пространства $\Bbbk[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_s)$ над полем $\Bbbk$.

С другой стороны, произвольную систему образующих можно *конструктивно* расширить до базиса Грёбнера. Для этого для каждой пары образующих многочленов f_i, f_j, таких что их старшие члены имеют вид $a_i m_i \cdot m$, $a_j m \cdot m_j$ для некоторых ненулевых констант $a_i, a_j \in \Bbbk$ и неединичных мономов m, m_i, m_j с $\text{НОД}(m_i, m_j) = 1$, надо добавить к конструируемому базису многочлен $S(f_i, f_j) = (a_i m_i) \cdot f_j - f_i \cdot (a_j m_j)$, называемый S-многочленом (а в некоммутативном случае — *скобкой Ширшова*) пары (f_i, f_j).

Упражнение 1.8. Убедитесь, что система образующих идеала тогда и только тогда, когда является базисом Грёбнера, когда вместе с каждой парой многочленов она содержит и их скобку Ширшова, и покажите, что произвольная система образующих данного идеала может быть дополнена до базиса Грёбнера присоединением конечного числа недостающих скобок Ширшова.

[8] его удобно представлять себе в виде точек первого координатного гипероктанта целочисленной решётки $\mathbb{Z}^n$, узлы которой суть показатели мономов

[9] т. е. удовлетворяющее условию $m_1 > m_2 \iff m_1 \cdot m > m_2 \cdot m$ для любых мономов m, m_1, m_2 (если мы используем «решёточное» представление для мономов, то удобнее использовать аддитивную запись)

[10] «базисы Грёбнера», равно как и вся описываемая здесь технология, были известны ещё в 50-е годы, причём сразу в контексте некоммутативных тензорных алгебр (см. например, работы Ширшова об идеалах в универсальных обёртывающих алгебрах свободных алгебр Ли); соответствующая коммутативная теория в те годы была не слишком интересна, с одной стороны, в силу своей тривиальности, с другой — в виду непосильной (для «ручной» работы) трудоёмкости практических вычислений; лишь спустя 10 – 15 лет, с внедрением компьютеров, эта техника приобрела широкую популярность (благодаря работам Бухбергера) и является ныне главным вычислительным средством «компьютерной алгебы»

[11] в «решёточной» интерпретации мономы, лежащие в идеале $(f_1^L, f_2^L, \ldots, f_s^L)$ — это неотрицательные целочисленные линейные комбинации мономов $f_1^L, f_2^L, \ldots, f_s^L$