§15. Полиномиальные идеалы

15.1. Нётеровость. Любое множество $M \subset A$ элементов произвольного коммутативного кольца A порождает в A идеал (M), состоящий из всевозможных конечных сумм

$$g_1 f_1 + g_2 f_2 + \cdots + g_m f_m \,,$$

в которых $g_\nu \in A$, а $f_\nu \in M$. Как A-модуль, идеал (M) представляет собою A-линейную оболочку элементов множества M.

Для произвольного идеала $I \subset A$ элементы $f_1, f_2, \ldots, f_m \in I$ называются *образующими* этого идеала, если они линейно порождают I как A-модуль, т. е. если $I = (f_1, f_2, \ldots, f_m)$.

Коммутативное кольцо A называется *нётеровым*, если каждый его идеал допускает конечное множество образующих. Условие нётеровости можно переформулировать несколькими равносильными способами:

Лемма 15.1
Следующие свойства коммутативного кольца A попарно эквивалентны:

(1) любое множество элементов $M \subset A$ содержит некоторое конечное подмножество, порождающее тот же идеал, что и M

(2) любой идеал в A 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). Для доказательства импликации (2) $\Rightarrow$ (3) заметим, что объединение $I = \bigcup\limits_\nu I_\nu$ всех идеалов возрастающей цепочки также является идеалом, и стало быть линейно порождается над A конечным числом элементов $f_1, f_2, \ldots, f_m \in I$. Все эти элементы содержатся в некотором идеале I_n из цепочки. Следовательно, $I_\nu = I_n = I \;\forall\, \nu \geqslant n$.

Чтобы вывести (1) из (3), рассмотрим цепочку идеалов $I_n = (f_1, f_2, \ldots, f_n)$, которая строится по индукции следующим образом: в качестве f_1 возьмём произвольный элемент множества M. При $i > 1$ в качестве f_i возьмём любой элемент из $(M) \smallsetminus (f_1, f_2, \ldots, f_{i-1})$, если только $(M) \neq (f_1, f_2, \ldots, f_{i-1})$. По построению, идеалы $I_{i-1} \subsetneq I_i$ строго возрастают, что не может продолжаться бесконечно силу (3). Поэтому на каком-то конечном шагу мы столкнёмся с равенством $(M) = (f_1, f_2, \ldots, f_i)$. □

Теорема 15.1
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 $\leqslant d$ из I, а через $L_\infty = \bigcup\limits_d L_d$ — множество старших коэффициентов вообще всех многочленов из I.

Упражнение 15.1. Убедитесь, что все L_d (включая L_∞) являются идеалами в A.

Поскольку кольцо A нётерово, все идеалы $L_d \subset A$ конечно порождены. Для каждого d (включая L_∞) обозначим через $f_1^{(d)}, f_2^{(d)}, \ldots, f_{m_d}^{(d)} \in A[x]$ многочлены, старшие коэффициенты которых порождают соответствующий идеал L_d в A, и пусть $D \in \mathbb{N}$ — это наибольшая из степеней многочленов $f_i^{(\infty)}$ (старшие коэффициенты которых порождают идеал $L_\infty \subset A$).

Покажем, что идеал I порождается многочленами $f_i^{(d)}$ с $0 \leqslant d < D$ и многочленами f_i^∞. Произвольный многочлен $g \in I$ сравним по модулю многочленов $f_1^{(\infty)}, f_2^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)}$ с многочленом, степень которого строго меньше D. В самом деле, старший коэффициент многочлена g лежит в идеале L_∞ и, значит, имеет вид $\sum \lambda_i a_i$, где $\lambda_i \in A$, а a_i — старшие коэффициенты многочленов $f_i^{(\infty)}$. Если $\deg g \geqslant D$, то все числа $m_i = \deg g - \deg f^{(\infty)}$ неотрицательны, и мы можем образовать многочлен $h = g - \sum \lambda_i \cdot f_i(x) \cdot x_i^{m_i}$, который сравним с g по модулю I и имеет $\deg h < \deg g$. Заменим g на h и повторим эту процедуру, пока не получим многочлен $h \equiv g \pmod{(f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{m_\infty}^{(\infty)})}$ степени $\deg h < D$. Теперь старший коэффициент многочлена h находится в идеале L_d с $d = \deg g_k < D$, и, вычитая из него подходящие A-линейные комбинации многочленов $f_i^{(d)}$, мы, тем же способом, что и выше, будем сокращать его старший член и строго уменьшать степень до тех пор, пока не получим нуль. □

Следствие 15.1
Если A нётерово, то $A[x_1, x_2, \dots, x_n]$ тоже нётерово.

Следствие 15.2
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 фактор алгебра A также нётерова, поскольку полный прообраз любого идеала $I \subset A$ при эпиморфизме $\Bbbk[x_1, x_2, \dots, x_n] \twoheadrightarrow A$ является конечно порождённым идеалом в $\Bbbk[x_1, x_2, \dots, x_n]$, и образы его образующих в A порождают I. □

15.2. Системы полиномиальных уравнений. 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 в $\Bbbk[x_1, x_2, \dots, x_n]$ идеал $J = (f_\nu)$, порождённый левыми частями исходных уравнений. В силу нётеровости кольца многочленов такая система, в свою очередь, эквивалентна конечной системе уравнений, левые части которых порождают идеал J.

Таким образом, любая (бесконечная) система полиномиальных уравнений, с одной стороны, равносильна некоторой своей конечной подсистеме, а с другой стороны, добавляя к уравнениям всевозможные их комбинации с произвольными полиномиальными коэффициентами, мы всегда можем считать, что уравнения образуют в кольце многочленов некоторый идеал J.

Множество всех решений такой системы уравнений образует в аффинном координатном пространстве $\mathbb{A}^n$ фигуру, которая обозначается

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

и называется *аффинным алгебраическим многообразием*. Отметим, что эта фигура может оказаться пустым множеством, как это происходит, например, когда идеал $I = (1) = \Bbbk[x_1, x_2, \dots, x_n]$ совпадает со всем кольцом (т. е. содержит уравнение $1 = 0$).

Для произвольной фигуры $\Phi \subset \mathbb{A}^n$ множество всех многочленов, тождественно зануляющихся на Φ, образует в кольце многочленов идеал, который обозначается

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

Множество нулей этого идеала $V(I(\Phi))$ представляет собою наименьшее аффинное алгебраическое многообразие, содержащее Φ.

Для любого идеала $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ имеется тавтологическое включение $J \subset I(V(J))$. Вообще говоря, это включение строгое. Например, для $J = (x^2) \in \mathbb{C}[x]$ имеем $V(J) = \{0\} \subset \mathbb{A}^1(\mathbb{C})$ и $I(V(J)) = (x) \supsetneq (x^2)$.

Теорема 15.2 (Nullstellensatz, или теорема Гильберта о нулях)
Над произвольным алгебраически замкнутым полем $\Bbbk$ для любого идеала $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ 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 первое утверждение, мы для каждого собственного[1] идеала $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ построим точку $p \in \mathbb{A}_n$, в которой зануляются все многочлены из J. Поскольку увеличение идеала J только усложняет задачу, мы без ограничения общности можем считать, что любой многочлен $g \notin J$ обратим по модулю J. Действительно, если найдётся необратимый по модулю J многочлен $g \notin J$, то уравнение $gh + f = 1$ будет неразрешимо относительно $h \in \Bbbk[x_1, x_2, \dots, x_n]$ и $f \in J$, а значит, идеал $J' = (J, g)$ не будет содержать 1, т. е. будет собственным, и мы можем расширить J до $J' \supsetneq J$. В силу нётеровости кольца многочленов после конечного числа таких расширений мы получим собственный идеал J, такой что $\Bbbk[x_1, x_2, \dots, x_n]/J$ является полем, что мы и будем далее предполагать.

Так как поле $\Bbbk[x_1, x_2, \dots, x_n]/J \supset \Bbbk$ конечно порождено как $\Bbbk$-алгебра, каждый элемент $\vartheta \in \Bbbk[x_1, x_2, \dots, x_n]/J$ алгебраичен над $\Bbbk$ по теор. 14.2, т. е. удовлетворяет уравнению $\mu(\vartheta) = 0$, где $\mu(t) \in \Bbbk[t]$ — неприводимый приведённый многочлен. Поскольку поле $\Bbbk$ алгебраически замкнуто, многочлен μ линеен, т. е. $\vartheta + c = 0$ для некоторого $c \in \Bbbk$, откуда $\vartheta = c \in \Bbbk$.

Таким образом, $\Bbbk[x_1, x_2, \dots, x_n]/J = \Bbbk$, т. е. любой многочлен $f \in \Bbbk[x_1, x_2, \dots, x_n]$ сравним по модулю идеала J с некоторой константой. Обозначим через $p = (p_1, p_2, \dots, p_n) \in \mathbb{A}^n$ точку, координаты которой суть константы $p_i \in \Bbbk$, с которыми сравнимы по модулю J линейные одночлены x_i. Так как редукция по модулю J

$$\Bbbk[x_1, x_2, \dots, x_n] \twoheadrightarrow \Bbbk = \Bbbk[x_1, x_2, \dots, x_n]/J \tag{15-1}$$

является гомоморфизмом, константа, с которой сравним по модулю J произвольно выбранный многочлен f равна значению этого многочлена в точке p:

$$[f(x_1, x_2, \dots, x_n)]_J = f([x_1]_J, \, [x_2]_J, \, \dots \, , \, [x_n]_J) = f(p_1, p_2, \dots, p_n)\,.$$

Иными словами, гомоморфизм (15-1) редукции по модулю J есть ни что иное, как гомоморфизм вычисления значений многочленов в точке p. Поэтому для любого $f \in J$ значение $f(p) = 0$, что и требовалось.

Докажем теперь второе утверждение. Поскольку при $J = \Bbbk[x_1, x_2, \dots, x_n]$ и $V(J) = \varnothing$ оно тривиально, мы будем считать, что $V(J) \neq \varnothing$ и $J \neq (1)$. Вложим $\mathbb{A}^n$ в большее пространство $\mathbb{A}^{n+1}$ с координатами $(t, \, x_1, x_2, \dots, x_n)$ в качестве гиперплоскости $t = 0$. Если многочлен

$$f \in \Bbbk[x_1, x_2, \dots, x_n] \subset \Bbbk[t, \, x_1, x_2, \dots, x_n]$$

тождественно обращается в нуль на $V(J)$, то идеал $J' \subset \Bbbk[t, \, x_1, x_2, \dots, x_n]$, 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 $V(J) \subset \mathbb{A}^{n+1}$. Тем самым, по слабой теореме о нулях, идеал J' содержит единицу, т. е. существуют $q_0, q_1, \dots, q_s \in \Bbbk[t, \, x_1, x_2, \dots, x_n]$ и $f_1, f_2, \dots, f_s \in J$, такие что

$$q_0(x, t) \cdot \bigl(1 - tf(x)\bigr) + q_1(t, x) \cdot f_1(x) + \dots + q_s(x, t) \cdot f_s(x) = 1\,.$$

Применим к этому равенству гомоморфизм $\Bbbk[t, \, x_1, x_2, \dots, x_n] \longrightarrow k(x_1, x_2, \dots, x_n)$, заданный правилами $t \mapsto 1/f(x)\,, \quad x_\nu \longmapsto x_\nu$. Получим равенство

$$q_1\bigl(1/f(x)\,,\, x\bigr) \cdot f_1(x) + \dots + q_s\bigl(1/f(x)\,,\, x\bigr) \cdot f_s(x) = 1$$

в поле рациональных функций $\Bbbk(x_1, x_2, \dots, x_n)$. Поскольку идеал J не содержит единицы, некоторые из $q_\nu\bigl(1/f(x), x\bigr)$ должны иметь ненулевой знаменатель, и в качестве общего знаменателя всех $q_\nu\bigl(1/f(x), x\bigr)$ можно взять некоторую степень f^m. Умножая обе части равенства на f^m получаем искомое выражение $\widetilde{q}_1(x) \cdot f_1(x) + \dots + \widetilde{q}_s(x) \cdot f_s(x) = f^m(x)$ с $\widetilde{q}_\nu \in \Bbbk[x_1, x_2, \dots, x_n]$. □

[1] т. е. отличного от всего кольца многочленов

15.3. Проективные гиперповерхности. Проективной гиперповерхностью степени d в $\mathbb{P}_n = \mathbb{P}(V)$ называется множество нулей $V(f) \subset \mathbb{P}(V)$ ненулевого однородного многочлена $f \in S^dV^*$ степени d на векторном пространстве V. Поскольку пропорциональные уравнения задают одну и ту же гиперповерхность, проективные гиперповерхности степени d в $\mathbb{P}(V)$ являются точками проективного пространства $\mathscr{S}_d = \mathbb{P}(S^dV^*)$, которое называется *пространством гиперповерхностей* степени d.

Упражнение 15.2. Какова размерность пространства $\mathscr{S}_d$?

Раскладывая произвольный многочлен $f \in S^dV^*$ на неприводимые множители

$$f = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k} ,$$

мы заключаем, что произвольная гиперповерхность $S \in \mathscr{S}_d$ является объединением гиперповерхностей $V(q_i^n) = V(q_i)$, уравнения которых суть степени неприводимых многочленов.

Гиперповерхность $V(q)$, задаваемая неприводимым многочленом q, называется *неприводимой*. Если основное поле $\Bbbk$ алгебраически замкнуто, то две неприводимые проективные гиперповерхности одинаковой степени совпадают тогда и только тогда, когда задающие их многочлены пропорциональны:

$$V(q_1) = V(q_2) \iff q_1 = \lambda \cdot q_2 , \quad \text{где } \lambda \in \Bbbk^* .$$

В самом деле, поскольку многочлен q_1 зануляется вдоль гиперповерхности $V(q_2)$, по теореме Гильберта о нулях некоторая степень q_1^m делится на q_2. В силу однозначности разложения на неприводимые множители в кольце многочленов, это возможно только если $q_1 = \lambda \cdot q_2$, где λ — обратимый элемент, т. е. константа.

Гиперповерхность $S = V(f^m)$ степени $d = mk$, уравнение которой является m-той степенью некоторого многочлена f степени k, называется *m-кратной* гиперповерхностью. Как подмножество в $\mathbb{P}_n$ гиперповерхность S совпадает с гиперповерхностью $V(f)$ степени $k = d/m$. При $d = km$ подмножество в $\mathscr{S}_d$, состоящее из всех m-кратных гиперповерхностей, представляет собою образ *вложения Веронезе*

$$\nu_{k,d} : \mathscr{S}_k = \mathbb{P}(S^kV^*) \xhookrightarrow{f \mapsto f^m} \mathscr{S}_d = \mathbb{P}(S^{km}V^*) \tag{15-2}$$

и является алгебраическим подмногообразием в $\mathscr{S}_d$.

Гиперповерхности, не содержащие кратных неприводимых компонент называются *приведёнными*, а содержащие кратные неприводимые компоненты — *неприведёнными*.

15.3.1. Пример: линейные системы гиперповерхностей. Проективные подпространства $\mathbb{P}(U) \subset \mathbb{P}(S^dV^*)$ называются *линейными системами* гиперповерхностей. Если векторное подпространство $U \subset S^dV^*$ линейно порождается уравнениями $f_1, f_2, \dots, f_m$, то гиперповерхности из линейной системы $\mathbb{P}(U)$, порождённой гиперповерхностями $V(f_1)$, $V(f_2)$, … , $V(f_m)$, задаются уравнениями вида

$$\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_m f_m = 0 ,$$

где $\lambda_1, \lambda_2, \dots, \lambda_m \in \Bbbk$ — некоторые константы. Любая такая гиперповерхность обязательно содержит пересечение $V(f_1) \cap V(f_2) \cap \ldots \cap V(f_m)$, точки которого называются *базисными точками* линейной системы.

Поскольку уравнение $f(p) = 0$ при фиксированном $p \in \mathbb{P}(V)$ является *линейным* уравнением на $f \in S^dV^*$, гиперповерхности степени d, проходящие через заданную точку p, образуют линейную систему коразмерности 1, т. е. проективную гиперплоскость в пространстве всех гиперповерхностей.

По старинной традиции, одномерные и двумерные линейные системы гиперповерхностей называются, соответственно, *пучками* и *связками* гиперповерхностей.

Упражнение 15.3. Докажите, что в любом пучке гиперповерхностей (над любым полем) всегда найдётся гиперповерхность, проходящая через любую наперёд заданную точку.

15.4. Результанты. Рассмотрим систему однородных полиномиальных уравнений

$$\begin{cases} f_1(x_0, x_1, \dots, x_n) = 0 \\ f_2(x_0, x_1, \dots, x_n) = 0 \\ \dots\dots\dots\dots \\ f_m(x_0, x_1, \dots, x_n) = 0 \end{cases} \tag{15-3}$$

где $f_1, f_2, \dots, f_m \in \Bbbk[x_0, x_1, \dots, x_n]$ — однородные многочлены заданных степеней $\deg f_i = d_i$. Ненулевые решения такой системы, рассматриваемые с точностью до пропорциональности, образуют в проективном пространстве $\mathbb{P}_n = \mathbb{P}(V)$ с однородными координатами $(x_0 : x_1 : \ \dots : x_n)$ фигуру $\Phi = V(f_1, f_2, \dots, f_m)$, являющуюся пересечением проективных гиперповерхностей $S_i = V(f_i)$. Такие фигуры называются *проективными алгебраическими многообразиями*.

При фиксированной размерности n, фиксированном числе уравнений m и фиксированных степенях $d_1, d_2, \dots, d_m$ этих уравнений, наборы гиперповерхностей

$$(S_1, S_2, \dots, S_m) \in \mathscr{S}_{d_1} \times \mathscr{S}_{d_2} \times \dots \times \mathscr{S}_{d_m}$$

с непустым пересечением $\bigcap\limits_i S_i = V(f_1, f_2, \dots, f_m) \neq \varnothing$, или — что то же самое — рассматриваемые с точностью до пропорциональности наборы многочленов

$$(f_1, f_2, \dots, f_m) \in S^{d_1}V^* \times S^{d_2}V^* \times \dots \times S^{d_m}V^*,$$

для которых система однородных уравнений (15-3) обладает ненулевым решением, образуют в пространстве наборов гиперповерхностей фигуру

$$\mathscr{R}(n;\, d_1, d_2, \dots, d_m) \subset \mathscr{S}_{d_1} \times \mathscr{S}_{d_2} \times \dots \times \mathscr{S}_{d_m}, \tag{15-4}$$

которая называется *результантным многообразием* системы m однородных полиномиальных уравнений степеней $d_1, d_2, \dots, d_m$ от $n+1$ переменных.

Например, если число уравнений равно числу переменных и все уравнения линейны, система (15-3) превращается в систему однородных линейных уравнений с квадратной матрицей

$$\begin{cases} a_{1,1}x_0 + a_{1,2}x_1 + \dots + a_{1,n}x_n = 0 \\ a_{2,1}x_0 + a_{2,2}x_1 + \dots + a_{2,n}x_n = 0 \\ a_{3,1}x_0 + a_{3,2}x_1 + \dots + a_{3,n1}x_n = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n+1,1}x_0 + a_{n+1,2}x_1 + \dots + a_{n+1,n}x_n = 0 \end{cases}$$

которая имеет ненулевое решение тогда и только тогда, когда $\det(a_{i,j}) = 0$. Таким образом, при $m = (n+1)$ и $d_1 = d_2 = \dots = d_{n+1} = 1$ результантное многообразие (15-4)

$$\mathscr{R}(n;\, 1,\, 1,\, \dots,\, 1) \subset \mathbb{P}_n^* \times \mathbb{P}_n^* \times \dots \times \mathbb{P}_n^*$$

представляет собою гиперповерхность, заданную одним неприводимым полиномиальным уравнением степени $(n+1)$ на коэффициенты $a_{i,j}$ многочленов $f_1, f_2, \dots, f_{n+1}$.

Покажем, что для произвольного числа уравнений произвольных степеней результантное многообразие (15-4) задаётся конечной системой полиномиальных уравнений на коэффициенты многочленов $(f_1, f_2, \dots, f_m) \in S^{d_1}V^* \times S^{d_1}V^* \times \dots \times S^{d_m}V^*$, однородных по каждому многочлену и зависящих только от n и $d_1, d_2, \dots, d_m$.

Для этого рассмотрим идеал $I \subset \Bbbk[x_0, x_1, \dots, x_n]$, порожденный многочленами f_ν. Отсутствие у системы (15-3) ненулевых решений означает, что аффинное алгебраическое многообразие $V(I) \subset \mathbb{A}(V)$ либо пусто, либо совпадает с началом координат. В обоих случаях каждая из координатных функций x_i тождественно зануляется на $V(I)$, и значит, существует m, такое что

$x_i^m \in I$ для всех i. Наоборот, если I содержит некоторую степень каждой из переменных, то система уравнений с левыми частями из идеала I содержит уравнения $x_0^m = x_1^m = \dots = x_n^m = 0$, имеющие только нулевое решение.

Таким образом, отсутствие ненулевых решений у системы (15-3) равносильно тому, что для некоторого m идеал I содержит все x_i^m. Последнее означает, что любой многочлен, степень которого больше $(n+1)(m-1)$, лежит в I, и тем самым, I содержит все S^dV^* с $d \gg 0$.

С другой стороны, пересечение $I \cap S^dV^*$ является образом линейного отображения

$$\mu_d \,:\, S^{d-d_1}V^* \oplus S^{d-d_2}V^* \oplus \dots \oplus S^{d-d_m}V^* \xrightarrow{(g_0,g_1,\dots,g_n)\mapsto\sum g_\nu\, f_\nu} S^d\,. \tag{15-5}$$

В стандартных базисах из мономов это отображение задаётся матрицей, элементы которой линейно зависят от коэффициентов многочленов f_ν, и при $d \gg 0$ размерность левой части (15-5), которая ведёт себя как $\sum\limits_{\nu=1}^{m}\binom{n+d-d_\nu}{n} \sim \frac{m}{n!}\,d^n$, становится больше, чем размерность правой части, которая ведёт себя как $\binom{n+d}{n} \sim \frac{1}{n!}\,d^n$. Поэтому при достаточно больших d неравенство $I \cap S^dV^* \neq S^dV^*$ (т. е. несюрьективность отображения (15-5)) описывается системой полиномиальных уравнений — обращением в нуль всех максимальных миноров матрицы μ_d, и выполнение этих полиномиальных уравнений для всех d, таких что размерность левой части (15-5) не меньше, чем размерность правой, равносильна тому, что система (15-3) имеет ненулевые решения. В силу нётеровости кольца многочленов, построенная таким образом бесконечная система полиномиальных уравнений, задающих результантное многообразие $\mathscr{R}$, эквивалентна некоторой конечной подсистеме. Эта конечная система детерминантных условий на матрицы (15-5) называется *системой результантов*.

Используя теоремы о размерностях алгебраических многообразий[1] можно показать, что для систем (15-3), в которых число уравнений равно числу неизвестных, результантное многообразие (15-4) является неприводимой гиперповерхностью, т. е. система результантов состоит в этом случае из одного неприводимого многочлена, который обобщает определитель системы линейных уравнений[2] и называется *результантом* набора из $n+1$ однородных многочленов $f_1, f_2, \dots, f_{n+1}$ от $(n+1)$ переменных. В этом курсе мы обсудим лишь простейший результант, возникающий при $n = 1$ — результант пары однородных многочленов от двух переменных.

15.4.1. Пример: результант двух бинарных форм. Однородный многочлен степени d

$$f(t_0,t_1) = a_0\, t_0^d + a_1\, t_0^{d-1}\, t_1 + a_2\, t_0^{d-2}\, t_1^2 + \;\cdots\; + a_{d-1}\, t_0\, t_1^{d-1} + a_d\, t_1^d\,,$$

который на проективной прямой $\mathbb{P}_1$ с однородными координатами $(t_0 : t_1)$ обращается в нуль в d точках $\alpha_1, \alpha_2, \dots, \alpha_d$, где $\alpha_\nu = (\alpha'_\nu : \alpha''_\nu)$, имеет (с точностью до постоянного множителя) вид

$$f(t_0,t_1) = \prod_{\nu=1}^{d} \det\begin{pmatrix} t_0 & \alpha'_\nu \\ t_1 & \alpha''_\nu\end{pmatrix} = \prod_{\nu=1}^{d}(\alpha''_\nu t_0 - \alpha'_\nu t_1)\,.$$

Таким образом, каждый коэффициент a_i многочлена f является однородным многочленом степени d от координат $(\alpha'_1, \alpha'_2, \dots, \alpha'_n, \alpha''_1, \alpha''_2, \dots, \alpha''_n)$ его корней, а именно

$$a_i = (-1)^i\sigma_i(\alpha',\alpha'')\;, \quad \text{где} \quad \sigma_i(\alpha',\alpha'') = \sum \alpha'_{\nu'_1}\alpha'_{\nu'_2}\cdots\alpha'_{\nu'_i}\alpha''_{\nu''_1}\alpha''_{\nu''_2}\cdots\alpha''_{\nu''_{d-i}}$$

(суммирование происходит по всем разбиениям множества $\{1,\,2,\,\dots\,,\,d\}$ на два непересекающихся подмножества $\{\nu'_1, \nu'_2, \dots, \nu'_i\}$ и $\{\nu''_1, \nu''_2, \dots, \nu''_{d-i}\}$, состоящих из i и $d-i$ элементов).

[1] см., например, лекцию 13 курса *A.L.Gorodentsev. Algebraic Geometry Start Up Course.* (`http://wwwth.itep.ru/ gorod/ps/stud/projgeom/lec-13.ps.gz`)

[2] явные формулы для результантов можно найти в статье *A.Morozov, Sh.Shakirov. Analogue of the identity Log Det = Trace Log for resultants.* (`http://ru.arxiv.org/abs/0712.2448`), а также в книге *I.M.Gelfand, M/M/Kapranov, A.V.Zelevinsky. Discriminants, Resultants, and Multidimensional Determinants.* Birkhäuser, 1994 (есть в «Колхозе»)

Зафиксируем степени $m, n \in \mathbb{N}$ и рассмотрим в кольце многочленов $\Bbbk[\alpha', \alpha'', \beta', \beta'', t]$ от пяти наборов переменных $\alpha' = (\alpha'_1, \alpha'_2, \dots, \alpha'_n)$, $\alpha'' = (\alpha''_1, \alpha''_2, \dots, \alpha''_n)$, $\beta' = (\beta'_1, \beta'_2, \dots, \beta'_m)$, $\beta'' = (\beta''_1, \beta''_2, \dots, \beta''_m)$ и $t = (t_0, t_1)$ произведения

$$\begin{aligned} f(t_0, t_1) &= \prod_{\nu=1}^{n} (\alpha''_\nu t_0 - \alpha'_\nu t_1) = \sum_{i=0}^{n} a_i \, t_0^i \, t_1^{n-i}, \quad \text{где } a_i = (-1)^i \sigma_i(\alpha', \alpha''), \\ g(t_0, t_1) &= \prod_{\mu=1}^{m} (\beta''_\mu t_0 - \beta'_\mu t_1) = \sum_{j=0}^{m} b_j \, t_0^j \, t_1^{m-j}, \quad \text{где } b_j = (-1)^j \sigma_j(\beta', \beta''), \end{aligned} \tag{15-6}$$

которые будем воспринимать как многочлены от (t_0, t_1) с коэффициентами в $\Bbbk[\alpha', \alpha'', \beta', \beta'']$. Придавая переменным α и β конкретные значения из поля $\Bbbk$, мы будем получать в формулах (15-6) пару однородных многочленов $f, g \in \Bbbk[t_0, t_1]$ степени $\deg f = n$ и $\deg g = m$, обращающихся в нуль в заданных наборах точек $\alpha_1, \alpha_2, \dots, \alpha_n$ и $\beta_1, \beta_2, \dots, \beta_m$ проективной прямой. Эти два набора точек имеют непустое пересечение тогда и только тогда, когда обращается в нуль произведение

$$R(f, g) = \prod_{\mu,\nu} \det \begin{pmatrix} \alpha'_\nu & \beta'_\mu \\ \alpha''_\nu & \beta''_\mu \end{pmatrix} = \prod_{\nu=1}^{n} g(\alpha_\nu) = (-1)^{mn} \prod_{\mu=1}^{m} f(\beta_\mu), \tag{15-7}$$

выражение которого через коэффициенты a_i и b_j многочленов f и g называется *результантом* бинарных форм f и g. Из (15-7) видно, что $R(f, g)$, рассматриваемый как элемент кольца $\Bbbk[\alpha, \beta]$ однороден степени mn как по переменным α, так и по переменным β. Явное выражение (15-7) через коэффициенты многочленов таково:

Лемма 15.2
В обозначениях (15-6)–(15-7) результант $R(f, g)$ равен *определителю Сильвестра*:

$$R(f, g) = \det \left.\begin{pmatrix} a_0 & & & & b_1 & & \\ a_1 & a_0 & & & b_2 & \ddots & \\ \vdots & a_1 & \ddots & & \vdots & \ddots & b_1 \\ a_n & \vdots & \ddots & a_0 & b_{m-1} & \ddots & b_2 \\ & a_n & \ddots & a_1 & b_m & \ddots & \vdots \\ & & \ddots & \vdots & & \ddots & b_{m-1} \\ & & & a_n & & & b_m \\ \multicolumn{4}{c}{\underbrace{\hphantom{a_0 \; a_0 \; \ddots \; a_0}}_{m}} & \multicolumn{3}{c}{\underbrace{\hphantom{b_1 \; \ddots \; b_1}}_{n}} \end{pmatrix}\right\} {\scriptstyle m+n} \tag{15-8}$$

(m коэффициентов a_0 и n коэффициентов b_m стоят на главной диагонали, на всех незаполненных местах стоят нули).

Доказательство. Рассмотрим векторное пространство U с базисом t_0, t_1 и линейное отображение (15-5) $M_{f,g} : S^{m-1}U \oplus S^{n-1}U \longrightarrow S^{m+n-1}U$, переводящее пару многочленов (h_1, h_2) в многочлен $fh_1 + gh_2$. Матрица в правой части формулы (15-8) есть матрица отображения $M_{f,g}$ в стандартном мономиальном базисе

$$\underbrace{(t_0^{m-1}, 0), \, (t_0^{m-2} t_1, 0), \, \dots, \, (t_0 t_1^{m-2}, 0), \, (t_1^{m-1}, 0)}_{m}, \; \underbrace{(0, t_0^{n-1}), \, (0, t_0^{n-2} t_1), \, \dots, \, (0, t_0 t_1^{n-2}), \, (0, t_1^{n-1})}_{n}$$

пространства $S^{m-1}U \oplus S^{n-1}U$ и стандартном мономиальном базисе

$$\underbrace{t_0^{m+n-1}, \, t_0^{m+n-2} t_1, \, \dots, \, t_0 t_1^{m+n-2}, \, t_1^{m+n-1}}_{m+n}$$

пространства $S^{m+n-1}U$.

Если точка (α,β) лежит на квадрике $\alpha_i'\beta_j''-\alpha_i''\beta_j'=0$, то с точностью до скалярного множителя $(\alpha_i''t_0-\alpha_i't_1)=(\beta_i''t_0-\beta_i't_1)$, и эта линейная форма от (t_0,t_1) является в кольце $\Bbbk[t_0,t_1]$ общим делителем многочленов $f(t_0,t_1)$ и $g(t_0,t_1)$, а значит, и всех многочленов из образа отображения $M_{f,g}$. Поэтому $\operatorname{im} M_{f,g}\neq S^{m+n-1}U$, и стало быть, матрица $M_{f,g}$ в этом случае вырождена.

Таким образом, определитель Сильвестра тождественно зануляется на каждой квадрике $\alpha_i'\beta_j''-\alpha_i''\beta_j'=0$. Следовательно, он делится в кольце $\Bbbk[\alpha,\beta]$ на каждую из квадратичных форм $\alpha_i'\beta_j''-\alpha_i''\beta_j'$. Поскольку все они неприводимы, определитель Сильвестра делится и на их произведение, равное результанту $R_{f,g}$. Так как и определитель Сильвестра, и результант являются биоднородными многочленами от (α,β) одинаковой бистепени (mn,mn), частное от этого деления — константа. А поскольку коэффициент при мономе

$$\left(\alpha_1''\alpha_2''\,\dots\,\alpha_n''\right)^m\left(\beta_1'\beta_2'\,\dots\,\beta_m'\right)^n=(-1)^{mn}a_0^mb_m^n$$

и в определителе (15-8) и в произведении (15-7) равен $(-1)^{mn}$, эта константа равна 1. □

15.4.2. Неоднородные многочлены и исключение переменных. Если в предыдущем примере потребовать, чтобы оба коэффициента a_0 и b_0 были отличны от нуля, и рассмотреть многочлены f и g в аффинной карте $t_1=1$ с аффинной координатой $t=t_0/t_1$, то всё сказанное в нём можно переговорить на языке неоднородных многочленов от переменной t. А именно, два многочлена

$$f(t)=a_0t^n+a_1t^{n-1}+\,\cdots\,+a_n=a_0\cdot\prod_{\nu=1}^{n}(t-\alpha_\nu)\in\Bbbk[x]$$
$$g(t)=b_0t^m+b_1t^{m-1}+\,\cdots\,+b_m=b_0\cdot\prod_{\mu=1}^{m}(t-\beta_\mu)\in\Bbbk[x]$$

тогда и только тогда не являются взаимно простыми (или, что то же самое, имеют общий корень в алгебраическом замыкании поля $\Bbbk$), когда обращается в нуль их результант

$$R(f,g)=a_0^mb_0^n\prod_{\mu,\nu}(\alpha_\nu-\beta_\mu)=\prod_{\nu=1}^{n}g(\alpha_\nu)=(-1)^{mn}\prod_{\mu=1}^{m}f(\beta_\mu)\,,$$

который явно выражается через коэффициенты a_i и b_j многочленов f и g по формуле Сильвестра (15-8). Потенциально, этим обстоятельством можно пользоваться для исключения переменных из систем полиномиальных уравнений.

Пусть, например, требуется решить систему уравнений $f(x,y)=g(x,y)=0$, где f и g произвольные многочлены из $\Bbbk[x,y]$. Рассмотрим их как многочлены от y с коэффициентами в кольце $\Bbbk[x]$ и вычислим их результант $r(x)=R(f,g)\in\Bbbk[x]$. Согласно сказанному выше, первая координата x_0 любого решения (x_0,y_0) является корнем многочлена $r(x)$ от одной переменной x, и наоборот, для любого $x_0\in\Bbbk$, такого что $r(x_0)=0$, многочлены $f(x_0,y),g(x_0,y)\in\Bbbk[y]$ будут иметь нетривиальный общий делитель в $\Bbbk[y]$, а значит, общий корень в алгебраическом замыкании поля $\Bbbk$. Таким образом, решение системы из двух полиномиальных уравнений от двух переменных (x,y) сводится к решению одного полиномиального результантного уравнения $r(x)=0$ на x. Практическая применимость такого способа отыскания решений[1] осложняется тем, что степень результантного уравнения равна произведению степеней многочленов f и g по исключаемой переменной y.

15.4.3. Пример: пересечение плоских кривых. Пусть поле $\Bbbk$ алгебраически замкнуто. Рассмотрим кривые $C_1,C_2\subset\mathbb{P}_2$ задаваемые в однородных координатах $x=(x_0:x_1:x_2)$ на $\mathbb{P}_2$ однородными уравнениями $f(x)=0$ и $g(x)=0$ степени $\deg f=n$ и $\deg g=m$. Воспринимая f, g как (неоднородные) многочлены от x_0 с коэффициентами в $\Bbbk[x_1,x_2]$, вычислим их результант

[1]замечательный пример подобного вычисления см. на стр. 114–116 книги
М. Рид. Алгебраическая геометрия для всех. (М., «Мир», 1991, есть в «Колхозе»)

$R(f,g) = r(x_1,x_2)$. Поскольку каждый коэффициент $a_i(x_1,x_2)$ многочлена f является однородным многочленом от (x_1,x_2) степени $n-i$, а каждый коэффициент $b_j(x_1,x_2)$ многочлена g — однородным многочленом от (x_1,x_2) степени $m-j$, из формулы Сильвестра вытекает, что $r(x_1,x_2)$ является однородным многочленом степени mn (не исключено, что нулевым).

Упражнение 15.4. Покажите, что если $r = 0$, то f и g имеют в $\Bbbk[x_0,x_1,x_2]$ нетривиальный общий делитель.

Таким образом, если $r = 0$, то кривые C_1 и C_2 имеют общую компоненту. Если же $r \neq 0$, то последние две координаты $(c_1 : c_2)$ каждой точки пересечения $c = (c_0 : c_1 : c_2) \in C_1 \cap C_2$ удовлетворяют однородному уравнению $r(x_1,x_2) = 0$ степени mn.

Отсюда вытекает, во-первых, что кривые без общих компонент могут пересекаться лишь по конечному числу точек, а во-вторых, что число этих точек пересечения не превышает произведения степеней кривых. Чтобы убедиться в последнем, достаточно выбрать систему координат так, чтобы точка $e_0 = (1:0:0)$ лежала вне конечного множества прямых, соединяющих всевозможные пары различных точек пересечения кривых C_1 и C_2. Тогда любая прямая, проходящая через e_0 будет содержать не более одной точки пересечения кривых C_1 и C_2, и тем самым, для каждого решения $(c_1 : c_2)$ результантного уравнения $r(x_1,x_2) = 0$ будет существовать ровно одна точка $c = (c_0 : c_1 : c_2) \in C_1 \cap C_2$.

Ответы и указания к некоторым упражнениям

<u>упр. 15.2</u>. $\binom{n+d}{d} - 1$.

<u>упр. 15.3</u>. Любая прямая в проективном пространстве имеет непустое пересечение с любой гиперплоскостью. Если $d = km$, то m-кратные

Оглавление

Раздел 1
Полилинейная алгебра . . . 2

§1. Тензорные произведения модулей . . . 2
1.1. Полилинейные отображения . . . 2
1.2. Универсальное полилинейное отображение . . . 3
1.3. Тензорное произведение модулей . . . 4
1.4. Изоморфизм $U^* \otimes V \simeq \mathrm{Hom}(U, V)$ и разложимые операторы . . . 6
1.5. Тензорные произведения абелевых групп . . . 7
1.6. Канонические изоморфизмы . . . 8
§2. Тензорная алгебра векторного пространства . . . 10
2.1. Свободная ассоциативная алгебра $\mathsf{T}(V)$ . . . 10
2.2. Двойственность . . . 10
2.3. Частичные свертки . . . 11
2.4. Линейный носитель тензора . . . 12
2.5. Условия (косо) симметричности . . . 12
2.6. Симметрическая алгебра пространства V . . . 13
2.7. Внешняя алгебра пространства V . . . 14
§3. Поляризация полиномов . . . 16
3.1. Симметрические и кососимметрические тензоры . . . 16
3.2. Поляризация коммутативных многочленов . . . 18
3.3. Частные производные в симметрической алгебре . . . 19
3.4. Поляризация грассмановых многочленов . . . 22
3.5. Частные производные в грассмановой алгебре . . . 22

Раздел 2
Формальные алгебраические функции . . . 25

§4. Исчисление формальных степенных рядов (напоминания) . . . 25
4.1. Алгебраические операции над рядами . . . 25
4.2. Дифференциальное исчисление . . . 26
4.3. Первообразные, логарифмы и экспоненты . . . 27
4.4. Бином Ньютона . . . 28
4.5. Действие $\mathbb{Q}[[d/dt]]$ на $\mathbb{Q}[t]$ . . . 31
4.6. Числа Бернулли . . . 33
§5. Симметрические функции . . . 34
5.1. Симметрические и кососимметрические многочлены . . . 34
5.2. Элементарные симметрические многочлены . . . 35
5.3. Полные симметрические многочлены. . . . 37
5.4. Степенные суммы Ньютона . . . 37
5.5. Детерминантные тождества . . . 39
5.6. Кольцо симметрических функций . . . 41
§6. Исчисление массивов, таблиц и диаграмм . . . 43
6.1. Массивы и элементарные операции над ними . . . 43
6.2. Уплотнение массивов . . . 45
6.3. Действие симметрической группы на DU-множествах . . . 49
6.4. Полиномы Шура . . . 51
6.5. Правило Литтлвуда – Ричардсона . . . 53

6.6. Скалярное произведение 56

Раздел 3
Элементы некоммутативной алгебры 57

§7. Группы в действии 57
7.1. Действие группы на множестве 57
7.2. Левое регулярное действие. 58
7.3. Присоединённое действие. 59
7.4. Длины орбит 59
7.5. Перечисление орбит 61
7.6. Орбиты p-групп. 62
7.7. Полупрямые произведения. 64
§8. Пространства с операторами 65
8.1. Приводимость и разложимость 65
8.2. Линейные представления группы 67
8.3. Полупростые модули над ассоциативной алгеброй 69
8.4. Полная приводимость представлений конечной группы. 71
§9. Линейные представления конечных групп 74
9.1. Разложение представлений на неприводимые. 74
9.2. Строение групповой алгебры. 76
9.3. Характеры. 80
§10. Категории и функторы 84
10.1. Категории 84
10.2. Функторы 86
10.3. Предпучки 86
10.4. Эквивалентные категории 90
10.5. Представимые функторы 92
10.6. Сопряжённые функторы 94
§11. Пределы 96
11.1. Пределы диаграмм. 96
11.2. Пределы предпучков. 101
§12. Категория G-модулей 104
12.1. Тензорное произведение модулей над алгеброй. 104
12.2. Индуцированные представления. 105
12.3. Кольцо представлений 107
§13. Представления симметрических групп 108
13.1. Действие S_n на заполненных диаграммах Юнга 108
13.2. Симметризаторы Юнга 109
13.3. Модуль таблоидов M^λ 112
13.4. Модуль Шпехта S^λ 113
13.5. Кольцо представлений симметрических групп 114

Раздел 4
Элементы коммутативной алгебры 120

§14. Целые расширения колец 120
14.1. Целые элементы 120
14.2. Алгебраические элементы. 124
14.3. Нормальные кольца 125
14.4. Базисы трансцендентности. 126
§15. Полиномиальные идеалы 128
15.1. Нётеровость 128

15.2. Системы полиномиальных уравнений 129
15.3. Проективные гиперповерхности 131
15.4. Результанты 132

Ответы и указания к некоторым упражнениям 137

Оглавление 138