Оглавление

Предисловие

Этот курс является расширенным вариантом записок лекций, прочитанных студентам пятого курса математического факультета Московского Педагогического Государственного Университета осенью 1998 года и вышедших отдельными брошюрами в издательствах "Диалог-МГУ" (1999 год) и "МАКС Пресс" (2002 год). Излагаемый материал также послужил основой для четырех занятий, проведенных автором в рамках летней школы для старших школьников и студентов младших курсов "Современная математика" (Дубна, 16-28 июля 2002 года).

Для освоения курса достаточно иметь самые начальные знания по алгебре. Предполагается, что читатель знаком с понятиями кольца, поля и владеет теорией систем линейных уравнений. Даже излагаемые на втором курсе сведения об идеалах колец здесь в основном напоминаются.

Теорема Абеля о неразрешимости в радикалах алгебраических уравнений степени пять и выше на первый взгляд лишает нас всякого оптимизма относительно возможности решения произвольного уравнения или системы уравнений. Однако рассматриваемые здесь результаты, объединенные с численными методами решения уравнений, позволяют эффективно решать многие системы алгебраических уравнений.

У этого курса две цели. Первая – продемонстрировать, что такие абстрактные теоремы как теорема Гильберта о базисе или теорема Гильберта о нулях имеют простую и весьма полезную интерпретацию в теории систем алгебраических уравнений. В случае теоремы Гильберта о нулях существенно, чтобы система рассматривалась не над вещественными, а над комплексными числами. Это может послужить еще одной мотивировкой для введения комплексных чисел, естественность которых нередко вызывает сомнения у студентов–младшекурсников. Вторая цель – ввести понятие базиса Гребнера идеала и показать, насколько сильные алгоритмические методы это понятие предоставляет для решения общих систем алгебраических уравнений. В последние десятилетия базис Гребнера идеала стал играть важную роль во многих исследованиях по абстрактной алгебре, компьютерной алгебре, алгебраической геометрии, теории выпуклых многогранников, дискретной геометрии и других областях математики, и поэтому изложение первоначальных сведений по этому вопросу в рамках университетского курса представляется вполне уместным. Мы не останавливаемся здесь на вычислительных аспектах теории, но изложенного материала вполне достаточно, например, для того, чтобы подготовленный студент написал программу, которая для произвольной системы алгебраических уравнений отвечала на вопрос конечно или бесконечно число ее (комплексных) решений.

В основной части текста (главы 1-5) мы доказываем лишь простые утверждения. Все трудные результаты приводятся на уровне формулировок и иллюстраций. Это сделано для того, чтобы не утруждать читателя излишними подробностями и быстрее перейти к решению конкретных систем. По нашему мнению, алгоритм Бухбергера и его применение к решению систем, изложенные в виде рецептов, доступны школьнику старших классов. Удивительно, что понятие базиса Гребнера возникло в математике сравнительно недавно. Оно было введено Бруно Бухбергером в его диссертации 1965 г., написанной под руководством Вольфганга Гребнера. Аналогичные идеи были высказаны также Х. Хиронакой и А. И. Ширшовым.

Для полноты изложения в главе 6 собраны доказательства всех использованных утверждений. Глава 7 содержит материал, касающийся современных исследований по базисам Гребнера. Лекции снабжены большим количеством задач, решение которых весьма полезно для овладения изложенным материалом.

После появления первого издания настоящего курса в нашей стране вышло в свет несколько замечательных книг, в которых обсуждаются базисы Гребнера. В первую очередь отметим монографию Д. Кокса, Дж. Литтла и Д. О'Ши "Идеалы, многообразия и алгоритмы" (Москва: Мир, 2000.). Единственное, чем можно мотивировать перепечатку наших лекций после появления книги Д. Кокса и др. – это небольшим объемом первых. К тому же книга Д. Кокса, Дж. Литтла и Д. О'Ши уже исчезла из московских книжных магазинов. Также мы рекомендуем читателю, желающему быстро освоить основные факты о базисах Гребнера, главу 6 книги В. В. Прасолова "Многочлены" (Москва: МЦНМО, 2000). В этих лекциях мы активно использовали материал как из упомянутых книг, так и из других источников, перечисленных в конце текста, поэтому курс нисколько не претендует на оригинальность.

Автор познакомился с понятием базиса Гребнера на лекциях профессора В. Н. Латышева, которые, будучи студентом, прослушал в Московском Государственном Университете им. М. В. Ломоносова в 1994 году. Я благодарен Виктору Николаевичу за его лекции, а также за последующие полезные обсуждения. Особая благодарность слушателям курса в летней школе "Современная математика" – их интерес к теме, многочисленные вопросы и замечания побудили автора существенно дополнить изначальный текст. Также я благодарен Московскому Центру Непрерывного Математического Образования за предоставленную возможность издать этот курс, и моей жене Л. А. Аржанцевой за помощь в компьютерных вычислениях и в работе над текстом.

Глава 1.

Основные понятия и результаты теории систем алгебраических уравнений

1.1. Введение

Фиксируем натуральное число n и некоторое поле $\mathbb{K}$ (можно считать, что $\mathbb{K}$ есть поле рациональных чисел $\mathbb{Q}$, поле действительных чисел $\mathbb{R}$ или поле комплексных чисел $\mathbb{C}$). Пусть $x_1, \ldots, x_n$ — переменные, а $P_1(x_1, \ldots, x_n)$, $P_2(x_1, \ldots, x_n)$, $\ldots$ — набор (возможно, бесконечный) многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами в поле $\mathbb{K}$.

Определение 1.1. *Системой алгебраических уравнений* (САУ) называется система вида

$$\begin{cases} P_1(x_1, \ldots, x_n) = 0; \\ P_2(x_1, \ldots, x_n) = 0; \\ \quad \ldots\ldots\ldots \end{cases} \tag{1}$$

Определение 1.2. САУ называется *конечной*, если в нее входит лишь конечное число уравнений.

Определение 1.3. Набор чисел $(a_1, a_2, \ldots, a_n)$ из поля $\mathbb{K}$ называется *решением* системы (1), если

$$P_1(a_1, a_2, \ldots, a_n) = 0,\ P_2(a_1, a_2, \ldots, a_n) = 0,\ \ldots .$$

Определение 1.4. Две САУ называются *эквивалентными*, если множества их решений совпадают.

Пример 1.5. Над полем $\mathbb{R}$ системы

$$\left\{ x^2 + y^2 = -1 \right. \quad \text{и} \quad \left\{ \begin{array}{l} x + y = 2; \\ x^2 + 2xy + y^2 = 3. \end{array} \right.$$

эквивалентны, так как множества их решений пусты.

Над полем $\mathbb{C}$ системы неэквивалентны, т.к. $x = i$, $y = 0$ удовлетворяет первой системе, но не удовлетворяет второй.

Решить систему значит описать множество всех ее решений или доказать, что решений нет.

Задача 1.6. Решить первую и вторую систему над $\mathbb{C}$.

Основная задача. Научиться решать САУ.

В такой общей постановке задача вряд ли может быть решена. Исторически алгебра формировалась как наука о решении САУ (заметим, что одно алгебраическое уравнение можно рассматривать как частный случай САУ). Было накоплено огромное количество результатов, в том числе и негативного характера. Наиболее яркий из таких результатов — это теорема Абеля о неразрешимости в радикалах общего алгебраического уравнения степени ≥ 5.

В этом курсе мы рассмотрим несколько методов, позволяющих эффективно решать САУ. Эти методы были развиты сравнительно недавно и тесно примыкают к весьма абстрактным разделам коммутативной алгебры.

Интересно также качественное исследование множества решений САУ. Например, хотелось бы знать:

1) Имеет ли система хотя бы одно решение?

2) Эквивалентны ли две данные системы?

3) Конечно или бесконечно множество решений системы?

4) Как устроено множество решений с геометрической точки зрения?

Развиваемые здесь методы оказываются полезными при исследовании подобных вопросов.

1.2. Системы линейных уравнений

Простейший пример САУ — это система линейных уравнений. Здесь имеется вполне завершенная теория, которая как правило излагается в ВУЗе на первом курсе.

Напомним основные определения и результаты.

Рассмотрим систему

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{2}$$

Определение 1.7. Система (2) называется *совместной*, если она имеет хотя бы одно решение.

Определение 1.8. Система (2) называется *определенной*, если она имеет ровно одно решение.

Определение 1.9. Матрица

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$

называется *матрицей коэффициентов* системы (2), а матрица

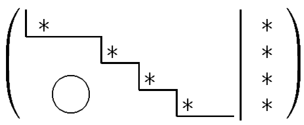
$$\widetilde{A} = \left(\begin{array}{ccc|c} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{array}\right)$$

– *расширенной матрицей* системы.

Универсальный метод решения систем линейных уравнений (т.е. метод, применимый к произвольной системе) — это метод Гаусса, или метод последовательного исключения неизвестных. Он состоит в следующем.

Шаг 1. Элементарными преобразованиями строк приводим расширенную матрицу системы к ступенчатому виду

$$\left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{array}\right) \rightsquigarrow$$

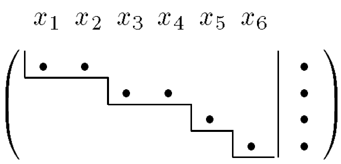


Теорема Кронекера - Капелли. *Система (2) совместна тогда и только тогда, когда ранг* $\operatorname{rk} A$ *матрицы коэффициентов равен рангу* $\operatorname{rk} \widetilde{A}$ *расширенной матрицы.*

После приведения к ступенчатому виду равенство рангов означает, что число ненулевых строк у матриц A и $\widetilde{A}$ одинаково.

Далее предполагаем, что система совместна.

Шаг 2. Переменные, которые соответствуют "ступенькам" в ступенчатом виде, назовем *главными*, а прочие неизвестные — *свободными*.



Так на схеме слева переменные x_1, x_3, x_5, x_6 — главные, а x_2, x_4 — свободные.

Выбор главных и свободных переменных неоднозначен. В то же время число главных и число свободных неизвестных определено однозначно.

Задача 1.10. Привести пример системы линейных уравнений, у которой нет нулевых коэффициентов, число решений бесконечно, но переменная x_1 не может быть свободной.

Задача 1.11. Сколько есть способов выбрать множество свободных неизвестных в системе

$$\begin{cases} x_1 + 2x_2 + x_3 + x_4 - x_5 = 0 \\ 2x_1 + 3x_2 + 2x_3 + 2x_4 - 2x_5 = 1 \end{cases} \quad ?$$

Теорема 1.12. *Число свободных неизвестных равно* $n - rkA$. *В частности, система (2) определена* $\iff rkA = rk\widetilde{A} = n$.

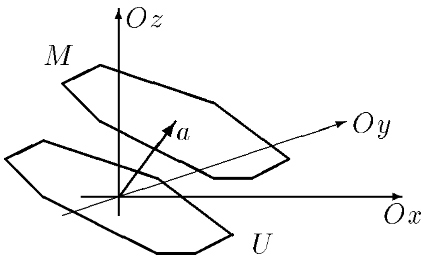
Шаг 3. Выражаем в обратном порядке главные неизвестные через свободные. Свободные неизвестные могут независимо принимать произвольные значения из поля $\mathbb{K}$.

Замечание. Если система над бесконечным полем ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...) имеет более одного решения, то она имеет бесконечно много решений (есть свободная неизвестная). В частности, множество из двух точек в $\mathbb{R}^n$ не может быть задано системой линейных уравнений.

Помимо метода Гаусса есть и другие методы решения системы (2). Например, метод Крамера использует определители. Этот метод не универсален, он применим только к квадратным определенным системам.

Геометрически множество решений системы линейных уравнений над $\mathbb{R}$ есть некоторое подмножество пространства $\mathbb{R}^n$. Эти множества описывает следующая теорема.

Теорема 1.13. *1) Множество решений системы (2) либо пусто, либо есть линейное многообразие* M, *т.е. результат параллельного переноса подпространства* $U \subseteq \mathbb{R}^n$ *на некоторый вектор* $a \in \mathbb{R}^n$.



2) Обратно, всякое линейное многообразие может быть задано системой линейных уравнений.

Задача* 1.14. Доказать теорему 1.13.

Пример 1.15. В $\mathbb{R}^3$ есть четыре типа подпространств: 1) начало координат; 2) прямая, проходящая через 0; 3) плоскость, проходящая через 0; 4) все пространство $\mathbb{R}^3$.

Поэтому в качестве множества решений системы линейных уравнений от трех неизвестных может выступать пустое множество, произвольная точка, произвольная прямая, произвольная плоскость или все пространство $\mathbb{R}^3$.

Задача 1.16. Привести примеры конкретных систем от 3-х неизвестных, реализующие каждую из указанных возможностей.

Итак, указан явный алгоритм решения системы (2), а также получены ответы на качественные вопросы. В этой теории встают алгоритмические проблемы наиболее эффективного способа приведения матрицы к ступенчатому виду, вычисления определителя матрицы за наименьшее число операций и т.п. Здесь мы не будем касаться подобных задач.

Резюмируя вышесказанное, отметим, что

1) теория систем линейных уравнений не зависит от того, над каким полем рассматривается система (в теории нелинейных систем это уже не так, см. пример 1.5);

2) свободные переменные могут независимо принимать **произвольные** значения из основного поля, а главные переменные **однозначно** через них выражаются.

Проблема. Какие результаты из теории систем линейных уравнений можно перенести на произвольные САУ? В частности, можно ли там определить понятие свободной переменной?

1.3. Некоторые сведения о многочленах

Пусть $\mathbb{K}[x_1, \ldots, x_n]$ – множество всех многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами в поле $\mathbb{K}$ (или, как говорят, над полем $\mathbb{K}$). На этом множестве определены операции сложения и умножения. Множества с такими операциями в алгебре называют кольцами.

Для многочленов от одной неизвестной будем обозначать $deg\ f(x)$ степень многочлена $f(x)$.

Теорема о делении с остатком для многочленов от

одной переменной. *Для любых многочленов* $f(x)$, $g(x) \in \mathbb{K}[x]$, $g(x) \neq 0$ *существуют и единственны многочлены* $q(x)$, $r(x) \in \mathbb{K}[x]$ *такие, что* $f(x) = g(x)q(x) + r(x)$ *и* $deg\ r(x) < deg\ g(x)$.

Многочлен $q(x)$ называется неполным частным, а многочлен $r(x)$ – остатком при делении $f(x)$ на $g(x)$. Доказательство этой теоремы несложно получить рассуждая по индукции по степени многочлена $f(x)$ (деление многочленов "в столбик").

Задача 1.17. Разделить $x^2 - x + 1$ на $x^3 + 2x$ с остатком.

Задача 1.18. Верна ли теорема о делении с остатком в кольце $\mathbb{Z}[x]$?

Теорема Безу. *Число* $\alpha \in \mathbb{K}$ *является корнем многочлена* $f(x) \in \mathbb{K}[x]$ *тогда и только тогда, когда* $f(x)$ *делится на* $(x - \alpha)$ *(без остатка).*

Доказательство этой теоремы следует из теоремы о делении с остатком (степень остатка при делении $f(x)$ на $(x - \alpha)$ равна нулю, т.е. это константа).

Определение 1.19. Многочлен $p(x_1, \ldots, x_n)$ называется *неприводимым*, если он отличен от константы и равенство $p = p_1 p_2$ влечет за собой равенство константе одного из многочленов p_1 или p_2.

Определение 1.20. Два многочлена называются *ассоциированными*, если они отличаются ненулевым числовым множителем.

Неприводимые многочлены являются аналогом простых чисел. Для многочленов также имеет место теорема об однозначном разложении на простые множители.

Теорема о факториальности кольца многочленов. *Каждый многочлен из кольца* $\mathbb{K}[x_1, \ldots, x_n]$*, отличный от константы, разлагается в произведение неприводимых многочленов, причем это разложение единственно с точностью до порядка множителей и ассоциированности.*

В случае кольца многочленов от одной переменной доказательство этой теоремы полностью аналогично доказательству соответствующей теоремы для целых чисел (последнюю называют основной теоремой арифметики). Здесь используется алгоритм Евклида, из которого выводят

Лемма о линейном представлении наибольшего общего делителя (НОД). *Пусть $f(x)$, $g(x) \in \mathbb{K}[x]$ и $d(x) =$ НОД$(f(x), g(x))$. Тогда существуют многочлены $u(x)$ и $v(x)$, такие что $f(x)u(x) + g(x)v(x) = d(x)$.*

а затем

Основная лемма. *Если $f(x)g(x)$ делится на неприводимый многочлен $p(x)$, то либо $f(x)$ делится на $p(x)$, либо $g(x)$ делится на $p(x)$.*

Детали доказательства мы оставляем читателю. Для многочленов от многих переменных доказательство факториальности сложнее. Оно приведено в Главе 6.

1.4. Системы уравнений над вещественными и комплексными числами

Между нелинейными системами над $\mathbb{R}$ и над $\mathbb{C}$ имеются принципиальные различия. Это связано с тем, что поле $\mathbb{C}$ алгебраически замкнуто.

Определение 1.21. Поле $\mathbb{K}$ называется *алгебраически замкнутым*, если всякий непостоянный многочлен с коэффициентами из поля $\mathbb{K}$ имеет корень в поле $\mathbb{K}$.

В противном случае говорят, что поле *алгебраически незамкнуто.*

Задача 1.22. Доказать, что если поле $\mathbb{K}$ алгебраически замкнуто, то каждый многочлен степени N с коэффициентами из $\mathbb{K}$ имеет в $\mathbb{K}$ ровно N корней (с учетом кратностей).

Поле $\mathbb{R}$ алгебраически незамкнуто, так как многочлен $x^2 + 1$ не имеет вещественных корней.

Основная теорема алгебры. *Каждый непостоянный многочлен с комплексными коэффициентами имеет комплексный корень.*

Следовательно, поле $\mathbb{C}$ алгебраически замкнуто.

Задача* 1.23. Являются ли алгебраически замкнутыми следующие поля: 1) $\mathbb{Q}$; 2) $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ — поле вычетов по простому модулю p; 3) $\mathbb{C}(t) = \{\frac{f}{g} \mid f, g \in \mathbb{C}[t],\ g \not\equiv 0\}$ — поле рациональных дробей над $\mathbb{C}$?

Предложение 1.24. *Всякая конечная система уравнений над $\mathbb{R}$ эквивалентна системе из одного уравнения.*

Доказательство. Система

$$\begin{cases} P_1(x_1, \ldots, x_n) = 0, \\ P_2(x_1, \ldots, x_n) = 0, \\ \quad \cdots\cdots\cdots \\ P_m(x_1, \ldots, x_n) = 0 \end{cases}$$

эквивалентна уравнению

$$P_1^2(x_1, \ldots, x_n) + P_2^2(x_1, \ldots, x_n) + \ldots + P_m^2(x_1, \ldots, x_n) = 0 \quad \blacksquare$$

Задача 1.25.** Доказать данное предложение для произвольного алгебраически незамкнутого поля.

На практике данное предложение не очень полезно, так как решить полученное уравнение, как правило, труднее, чем решить систему. Однако предложение 1.24 представляет определенный теоретический интерес.

Покажем, что над полем $\mathbb{C}$ предложение 1.24 неверно.

Лемма 1.26. *Над полем $\mathbb{C}$ система*

$$\begin{cases} x = 0 \\ y = 0 \end{cases}$$

не эквивалентна никакому уравнению.

Доказательство. Пусть уравнение $P(x, y) = 0$ имеет решение $x = 0$, $y = 0$. Покажем, что тогда оно имеет и другие решения. Пусть

$$P(x, y) = b_0(y) + b_1(y)x + \ldots + b_m(y)x^m,$$

где $b_i(y)$ — многочлены от y и $b_m(y) \not\equiv 0$. Тогда существует такое $y_0 \neq 0$, что $b_m(y_0) \neq 0$. По основной теореме алгебры уравнение

$$b_m(y_0)x^m + \ldots + b_1(y_0)x + b_0(y_0) = 0$$

от одной переменной x имеет некоторый корень x_0. Значит, уравнение $P(x, y) = 0$ имеет ненулевое решение (x_0, y_0). Лемма доказана. ∎

Задача 1.27. а) Привести пример многочлена от одной неизвестной с целыми коэффициентами, который не имеет рациональных корней и имеет ровно три действительных корня.

б) Привести пример системы уравнений с целыми коэффициентами от двух неизвестных, которая несовместна над $\mathbb{Q}$, имеет ровно три решения над $\mathbb{R}$ и бесконечно много решений над $\mathbb{C}$.

Глава 2.

Системы уравнений и идеалы в кольцах многочленов

2.1. Понятие идеала

В этом параграфе мы напомним некоторые сведения из теории колец. Пусть R — коммутативное ассоциативное кольцо с единицей 1.

Определение 2.1. Непустое подмножество I кольца R называется *идеалом* в R (записывается $I \lhd R$), если

1) $\forall a, b \in I \quad a - b \in I$;

2) $\forall a \in I,\ \forall c \in R \quad ac \in I$.

Пример 2.2. В кольце целых чисел $\mathbb{Z}$ множество $n\mathbb{Z}$ целых чисел, которые делятся на фиксированное целое число n, составляет идеал. При $n = 2$ имеем идеал четных чисел, при $n = 1$ — все кольцо $\mathbb{Z}$, а при $n = 0$ — один элемент 0.

Предложение 2.3. *В кольце $\mathbb{Z}$ всякий идеал имеет вид $n\mathbb{Z}$, $n = 0, 1, 2, \ldots$.*

Доказательство. Пусть I — ненулевой идеал в $\mathbb{Z}$ и $a \in I$ — наименьшее натуральное число в I (объясните, почему такое существует). Из определения идеала следует $a\mathbb{Z} \subseteq I$ (проверьте). Пусть $b \in I$, но $b \notin a\mathbb{Z}$. По теореме о делении с остатком существуют такие q и r, что $b = aq + r$ и $0 < r < a$. Но $r = b - aq \in I$ — противоречие с минимальностью a. Итак, $I = a\mathbb{Z}$. Предложение доказано. ■

Задача 2.4. Пусть $I \triangleleft R$. Доказать, что $I = R \Longleftrightarrow 1 \in I$.

Задача 2.5. (Основная теорема сельского хозяйства) Доказать, что в поле нет нетривиальных идеалов.

Задача 2.6. Проверьте, что множество $(a) = \{ar \mid r \in R\}$ есть идеал кольца R для всякого фиксированного $a \in R$.

Определение 2.7. Идеал I кольца R называется *главным*, если существует такой элемент $a \in I$, что $I = (a)$. Элемент a называется *порождающим* (или *образующим*) для идеала I.

Например, идеал $n\mathbb{Z} \triangleleft \mathbb{Z}$ – главный и $n\mathbb{Z} = (n) = (-n)$.

Пример 2.8. В кольце многочленов от двух неизвестных $\mathbb{K}[x, y]$ множество многочленов, свободный член которых равен нулю, образует идеал I_0, и этот идеал не является главным. Действительно, если $I_0 = (f)$, $f \in \mathbb{K}[x, y]$, то, поскольку $x \in I_0$, f есть либо ненулевая константа (и тогда $I_0 = \mathbb{K}[x, y]$ — противоречие), либо $f = \alpha x$, $\alpha \in \mathbb{K}$, $\alpha \neq 0$. Но $y \in I_0$, и потому f делит y — противоречие.

Определение 2.9. Кольцо R называется *кольцом главных идеалов*, если каждый идеал в R является главным.

Кольцо $\mathbb{Z}$ является кольцом главных идеалов (предложение 2.3), а кольцо $\mathbb{K}[x, y]$ — нет (пример 2.8).

Понятие главного идеала можно обобщить следующим образом. Пусть $a_1, a_2, \ldots, a_k$ — произвольные элементы кольца R.

Задача 2.10. Доказать, что множество

$$(a_1, a_2, \ldots, a_k) = \{a_1r_1 + a_2r_2 + \ldots + a_kr_k \mid r_1, r_2, \ldots, r_k \in R\} \subseteq R$$

есть идеал кольца R.

Определение 2.11. Элементы $a_1, \ldots, a_k$ составляют *базис* идеала $I = (a_1, a_2, \ldots, a_k)$. Говорят, что идеал $I \lhd R$ *допускает конечный базис*, если в нем найдутся такие элементы $a_1, a_2, \ldots, a_k$, что $I = (a_1, a_2, \ldots, a_k)$.

Заметим, что в определении базиса идеала (в отличие от определения базиса векторного пространства) нет требования минимальности на число элементов базиса. Например, добавляя к базису произвольный элемент идеала, мы вновь получаем базис того же идеала.

Задача 2.12. Доказать, что $(a_1, a_2, \ldots, a_k, a) = (a_1, a_2, \ldots, a_k)$ для любого $a \in (a_1, a_2, \ldots, a_k)$.

Задача 2.13. Доказать, что в кольце $\mathbb{Z}$ идеал (5,13) совпадает со всем кольцом $\mathbb{Z}$. Более общо, $(a_1, a_2, \ldots, a_k) = ($НОД$(a_1, a_2, \ldots, a_k))$.

Задача 2.14. Доказать, что в кольце $\mathbb{K}[x, y]$ идеал I_0 (см. пример 2.8) совпадает с идеалом (x, y).

Задача 2.15. Доказать, что $(f_1) = (f_2)$ тогда и только тогда, когда многочлены f_1 и f_2 отличаются на ненулевую константу.

2.2. Идеалы в кольцах многочленов Теорема Гильберта о базисе

В этом параграфе мы более подробно рассмотрим идеалы и их базисы в кольце многочленов.

Предложение 2.16. *Кольцо $\mathbb{K}[x]$ есть кольцо главных идеалов для любого поля $\mathbb{K}$.*

Доказательство по сути повторяет доказательство предложения 2.3 (воспользоваться теоремой о делении с остатком для многочленов).

Задача 2.17. Найти образующую идеала в $\mathbb{R}[x]$, состоящего из всех многочленов, обращающихся в ноль в точках $x = 0$, $x = 1$ и $x = 2$.

Задача* 2.18. Доказать, что кольцо $\mathbb{Z}[x]$ не является кольцом главных идеалов.

Как уже указывалось, кольца многочленов от многих переменных не являются кольцами главных идеалов. Тем не менее для них справедлива следующая фундаментальная теорема, доказанная Давидом Гильбертом на рубеже XIX и XX веков:

Теорема Гильберта о базисе. *Каждый идеал $I \lhd \mathbb{K}[x_1, \ldots, x_n]$ допускает конечный базис, т.е. найдутся такие $f_1(x_1, \ldots, x_n)$, ..., $f_k(x_1, \ldots, x_n) \in I$, что*

$$I = \{f_1 r_1 + \ldots + f_k r_k \mid r_1, \ldots, r_k \in \mathbb{K}[x_1, \ldots, x_n]\}.$$

Доказательство приведено в Главе 6.

Задача* 2.19. Рассмотрим в кольце $\mathbb{K}[x, y]$ идеалы:

1) $I_1 = \{\sum_{i,j} a_{ij} x^i y^j \mid a_{ij} \in \mathbb{R},\ i + j \geq 17\}$;
2) $I_2 = (y, x^2, yx^3, y^2x^4, y^3x^5, \ldots)$ (самостоятельно определите идеал, порожденный бесконечным множеством элементов!)

Найти конечные базисы в этих идеалах.

Задача* 2.20. Найти конечный базис в идеале

$$I_3 = \{f(x, y, z, t) \in \mathbb{R}[x, y, z, t] \mid f(a, a, a, a) = 0\ \forall a \in \mathbb{K}\},$$

где $\mathbb{K}$ – произвольное бесконечное поле.

Задача 2.21. Найти четыре различных базиса в идеале

$$(x, y, z) \lhd \mathbb{K}[x, y, z].$$

Задача 2.22. Доказать, что для любого множества M многочленов от n переменных в нем найдется конечное подмножество $m_1, \ldots, m_k$ такое, что каждый многочлен $m \in M$ может быть представлен в виде $m = m_1 r_1 + \ldots + m_k r_k$, где r_i – некоторые многочлены.

Задача 2.23. Привести пример кольца R и идеала $I \lhd R$, таких что I не обладает конечным базисом.

2.3. Идеал системы

Со всякой САУ

$$\begin{cases} P_1(x_1,\ldots,x_n)=0,\\ P_2(x_1,\ldots,x_n)=0,\\ \quad\cdots\cdots\cdots \end{cases}$$

мы можем связать идеал I, порожденный многочленами, отвечающими уравнениям системы :

$$I=(P_1(x_1,\ldots,x_n),P_2(x_1,\ldots,x_n),\ldots).$$

Если систему (1) обозначить для краткости буквой S, то соответствующий идеал будет обозначаться $I(S)$.

Лемма 2.24. *Если $F\in I(S)$, то $F(x_1^0,\ldots,x_n^0)=0$ для всякого решения $(x_1^0,\ldots,x_n^0)$ системы S.*

Доказательство. $F\in I(S)\iff F=r_1P_1+\ldots+r_mP_m$, откуда

$$\begin{aligned} &F(x_1^0,\ldots,x_n^0)=r_1(x_1^0,\ldots,x_n^0)P_1(x_1^0,\ldots,x_n^0)+\ldots\\ &+r_m(x_1^0,\ldots,x_n^0)P_m(x_1^0,\ldots,x_n^0)=r_1(x_1^0,\ldots,x_n^0)\cdot 0+\ldots\\ &+r_m(x_1^0,\ldots,x_n^0)\cdot 0=0.\ \blacksquare \end{aligned}$$

Предложение 2.25. *Пусть $\{P_1,\ldots,P_m\}$ и $\{\overline{P}_1,\ldots,\overline{P}_k\}$ — два базиса одного идеала I. Тогда системы*

$$\begin{cases} P_1(x_1,\ldots,x_n)=0,\\ \quad\cdots\cdots\cdots\\ P_m(x_1,\ldots,x_n)=0 \end{cases}\quad(*)\qquad \text{и}\qquad \begin{cases} \overline{P}_1(x_1,\ldots,x_n)=0,\\ \quad\cdots\cdots\cdots\\ \overline{P}_k(x_1,\ldots,x_n)=0 \end{cases}\quad(**)$$

эквивалентны.

Доказательство. Пусть $(x_1^0,\ldots,x_n^0)$ — решение системы (*). Покажем, что оно является решением системы (**). Поскольку $\overline{P}_i\in(P_1,\ldots,P_m)$ по условию, из леммы 2.24 следует, что $\overline{P}_i(x_1^0,\ldots,x_n^0)=0$. Аналогично, каждое решение (**) является решением (*). ■

Вывод. Множество решений системы однозначно определяется идеалом системы. Различные базисы одного идеала отвечают эквивалентным системам.

Следствие 2.26. *Каждая система алгебраических уравнений эквивалентна конечной системе.*

Доказательство. Из теоремы Гильберта о базисе следует, что во всяком идеале $I \lhd \mathbb{K}[x_1, \ldots, x_n]$ можно выбрать конечный базис. ■

На самом деле, анализируя доказательство теоремы Гильберта о базисе, можно доказать, что всякая бесконечная система

$$\begin{cases} P_1(x_1, \ldots, x_n) = 0, \\ P_2(x_1, \ldots, x_n) = 0, \\ \quad \cdots\cdots\cdots \end{cases}$$

эквивалентна системе

$$\begin{cases} P_1(x_1, \ldots, x_n) = 0, \\ P_2(x_1, \ldots, x_n) = 0, \\ \quad \cdots\cdots\cdots \\ P_N(x_1, \ldots, x_n) = 0, \end{cases}$$

а уравнения $P_{N+1}(x_1, \ldots, x_n) = 0$, $P_{N+2}(x_1, \ldots, x_n) = 0$, ... на множество решений системы не влияют.

Следствие 2.26 позволяет нам в дальнейшем рассматривать только конечные системы.

Следствие 2.27. *Всякая САУ от одного неизвестного эквивалентна системе из одного уравнения.*

Доказательство. Следует из предложения 2.16. ■

Задача 2.28. а) Доказать следствие 2.27 непосредственно, используя понятие наибольшего общего делителя многочленов;

б) Какому уравнению эквивалентна система:

$$\begin{cases} x^4 + x^3 - x - 1 = 0, \\ x^3 + 2x^2 + 2x + 1 = 0, \\ x^6 + x^5 + x^2 + 2x + 1 = 0 \end{cases} \qquad ?$$

Может показаться, что если системы S_1 и S_2 эквивалентны, то $I(S_1) = I(S_2)$. Эту гипотезу легко опровергнуть.

Пример 2.29. Уравнения $x = 0$ и $x^2 = 0$ эквивалентны, тогда как идеалы (x^2) и (x) не совпадают.

Задача 2.30. Привести пример эквивалентных систем S_1 и S_2 таких, что $I(S_1) \not\subset I(S_2)$ и $I(S_2) \not\subset I(S_1)$.

Можно ли, имея лишь идеалы $I(S_1)$ и $I(S_2)$, выяснить, эквивалентны ли системы S_1 и S_2 (разумеется, не решая самих систем)? Например, над полем $\mathbb{R}$ уравнения $x^2+y^2-2xy+1=0$ и $x^4+y^4+2=0$ эквивалентны (не имеют решений), но связи между идеалами $(x^2+y^2-2xy+1)$ и (x^4+y^4+2) не видно.

Для алгебраически замкнутых полей Гильберт получил очень красивый ответ на интересующий нас вопрос. Формулировке (но не доказательству) этого ответа мы посвятим следующую главу.

Глава 3.

Понятие аффинного алгебраического многообразия и формулировка теоремы Гильберта о нулях

3.1. Определение и примеры аффинных алгебраических многообразий

Неформально говоря, аффинные алгебраические многообразия — это множества решений систем алгебраических уравнений. Несмотря на кажущуюся простоту определения, объект это весьма сложный. Для его изучения за последние два века в математике сформировалась специальная дисциплина — алгебраическая геометрия — одна из самых высоконаучных, самых разработанных и самых трудных дисциплин. В нашем курсе мы лишь коснемся этого предмета.

На самом деле определение алгебраического многообразия весьма технично, но мы ограничимся следующей наивной точкой зрения.

Пусть $\mathbb{A}^n$ — это n-мерное пространство над полем $\mathbb{K}$.

Определение 3.1. Подмножество X в $\mathbb{A}^n$ называется *аффинным алгебраическим многообразием*, если найдется такая система S:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \quad \cdots\cdots\cdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases}$$

что $\overline{x} \in X \iff \overline{x}$ — решение системы S.

Множество решений системы S обозначим через $X(S)$. Для идеала $I \lhd \mathbb{K}[x_1, \ldots, x_n]$ определим подмножество $X(I)$ в $\mathbb{A}^n$ как множество точек, в которых все многочлены из идеала I равны нулю.

Ясно, что две системы S_1 и S_2 эквивалентны $\iff X(S_1) = X(S_2)$. Поэтому эквивалентные системы определяют одно и то же многообразие, а неэквивалентные системы — различные многообразия.

Ясно также, что $X(S) = X(I(S))$.

Задача 3.2. Задать уравнениями в $\mathbb{C}^3$ множество, состоящее из трех точек $(1, 2, 3)$, $(4, 5, 6)$ и $(7, 8, 9)$.

Задача 3.3. Доказать, что аффинными многообразиями **являются:**

а) произвольный конечный набор точек на прямой $\mathbb{A}^1$;

б) произвольный конечный набор точек в $\mathbb{A}^n$;

в) произвольное подпространство в $\mathbb{A}^n$;

г) произвольный конечный набор подпространств в $\mathbb{A}^n$;

д) всякая парабола на плоскости;

не являются:

е) подмножество целых чисел на прямой $\mathbb{R}^1$;

ж) множество $\{(x, y) \mid y = \sin x\} \subseteq \mathbb{R}^2$.

Задача 3.4. Доказать, что а) пересечение; б) объединение двух аффинных многообразий в $\mathbb{A}^n$ является аффинным многообразием.

Пример 3.5. Множество точек $\{(t, t^2, t^3) \mid t \in \mathbb{K}\} \subseteq \mathbb{A}^3$ является аффинным многообразием, его задает система

$$\begin{cases} y = x^2 \\ z = x^3. \end{cases}$$

Соответствующий идеал $I = (x^2 - y, x^3 - z) \triangleleft \mathbb{K}[x, y, z]$.

Как уже указывалось, совсем несхожие идеалы могут задавать совпадающие многообразия. В то же время для всякого многообразия X есть наибольший идеал $J(X)$, задающий это многообразие и содержащий все остальные задающие его идеалы. А именно,

$$J(X) = \{P \in \mathbb{K}[x_1, \ldots, x_n] \mid P(\overline{x}) = 0 \quad \forall \overline{x} \in X\}.$$

Задача 3.6. Проверить, что $J(X)$ — идеал.

Например, для точки ноль в $\mathbb{A}^2$ идеал J есть (x, y), а для оси Ox в $\mathbb{A}^2$ идеал J есть (y).

Идеал $J(X(S))$ может не совпадать с идеалом системы, но обязательно его содержит. Так множество нулей идеала $(x^2) \triangleleft \mathbb{K}[x]$ есть одна точка $\{0\}$, $J(\{0\}) = (x)$ и $(x^2) \subset (x)$.

Задача 3.7. Найти $J(X)$, где $X =$

а) $\{2, 3, 4, 5\} \subseteq \mathbb{A}^1$;

б) $\{x = y = z\} \subseteq \mathbb{A}^3$;

в) $\{(x, y) \mid x^4 = y^2\} \subseteq \mathbb{A}^2$;

г) $\{(x, y) \mid x^2 - 2xy + y^2 = 0\} \subseteq \mathbb{A}^2$.

Задача 3.8.** а) Рассмотрим кривую X в $\mathbb{C}^3$, заданную параметрически $x = t^3, \quad y = t^4, \quad z = t^5, \quad t \in \mathbb{C}$. Доказать, что идеал $J(X)$ не может быть порожден двумя элементами.

б) Задать указанную кривую системой из трех уравнений.

Предложение 3.9. *Системы S_1 и S_2 эквивалентны тогда и только тогда, когда $J(X(S_1)) = J(X(S_2))$.*

Доказательство. Системы S_1 и S_2 эквивалентны $\iff$ $X(S_1) = X(S_2) \iff J(X(S_1)) = J(X(S_2))$. ■

Задача 3.10. Доказать эти эквивалентности.

Предложение 3.9 пока представляется бесполезным с практической точки зрения, так как неясно, как находить идеал $J(X(S))$.

Над полем $\mathbb{C}$ идеал $J(X(S))$ можно описать более конструктивно. В этом и состоит теорема Гильберта о нулях.

3.2. Радикал идеала

Пусть $I \triangleleft \mathbb{K}[x_1, x_2, \ldots, x_n]$ — произвольный идеал.

Определение 3.11. *Радикалом* идеала I называется множество

$$r(I) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \exists s \in \mathbb{N}: \ f^s \in I\}.$$

Предложение 3.12.

1) $I \subseteq r(I)$;

2) $r(I)$ — идеал в $\mathbb{K}[x_1, \ldots, x_n]$;

3) $X(I) = X(r(I))$.

Доказательство. 1) Для всякого $f \in I$ возьмем $s = 1$.

2) Нужно проверить два свойства из определения идеала:

(1) $f_1, f_2 \in r(I) \Longrightarrow f_1 - f_2 \in r(I)$. Нам известно, что $\exists s_1, s_2 \in \mathbb{N}$: $f_1^{s_1} \in I$ и $f_2^{s_2} \in I$. Тогда

$$(f_1 - f_2)^{s_1+s_2} = \sum_{k=0}^{s_1+s_2} C_{s_1+s_2}^k (-1)^{s_1+s_2-k} f_1^k f_2^{s_1+s_2-k}$$

(формула бинома Ньютона). При $k \geq s_1$ $f_1^k = f_1^{s_1} \cdot f_1^{k-s_1} \in I \Longrightarrow f_1^k \cdot C_{s_1+s_2}^k (-1)^k f_2^{s_1+s_2-k} \in I$. При $k < s_1$ имеем $s_1 + s_2 - k > s_2$ $\Longrightarrow f_2^{s_1+s_2-k} \in I \Longrightarrow f_2^{s_1+s_2-k} \cdot C_{s_1+s_2}^k (-1)^{s_1+s_2-k} f_1^k \in I$. Итак, все слагаемые лежат в $I \Longrightarrow (f_1 - f_2)^{s_1+s_2} \in I \Longrightarrow f_1 - f_2 \in r(I)$;

(2) $f_1 \in r(I)$, $f_2 \in \mathbb{K}[x_1, \ldots, x_n] \Longrightarrow f_1 f_2 \in r(I)$. Мы знаем, что $\exists s: \ f_1^s \in I$. Но тогда $(f_1 f_2)^s = f_1^s f_2^s \in I \Longrightarrow f_1 f_2 \in r(I)$.

3) Из того, что $I \subseteq r(I)$ следует, что $X(r(I)) \subseteq X(I)$. Обратно, пусть $\overline{x} \in X(I)$ и пусть $f(\overline{x}) \neq 0$ для некоторого

$f \in r(I)$. Тогда $f^s(\overline{x}) = (f(\overline{x}))^s \neq 0\ \forall s$ — противоречие, т.к. $\exists s:\ f^s \in I$. ■

Задача 3.13. Найти $r(I)$ для следующих идеалов I:
а) $I = (x^2) \triangleleft \mathbb{K}[x]$; в) $I = (x^2, y^3) \triangleleft \mathbb{K}[x, y]$;
б) $I = (x, y) \triangleleft \mathbb{K}[x, y]$; г) $I = (x^2 + y^2 + z^2) \triangleleft \mathbb{K}[x, y, z]$.

Задача 3.14. Доказать, что в кольце многочленов радикал главного идеала является главным идеалом.

3.3. Теорема Гильберта о нулях

Теорема Гильберта о нулях. Над полем комплексных чисел для каждой системы алгебраических уравнений S имеем

$$\boxed{\mathrm{J(X(S))=r(I(S))}}$$

После переформулировки на язык систем уравнений утверждение становится более понятным: для системы

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \quad \cdots\cdots\cdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

алгебраических уравнений многочлен $F(x_1, \ldots, x_n)$ обращается в нуль на всех решениях данной системы тогда и только тогда, когда найдутся $r_1(x_1, \ldots, x_n), \ldots, r_m(x_1, \ldots, x_n)$ и $s \in \mathbb{N}$ такие, что $\boxed{F^s = r_1 f_1 + \ldots + r_m f_m}$.

(Объясните эквивалентность этих формулировок!)

Например, к системе

$$\begin{cases} f_1 = x + 2y + 4yz^2 = 0, \\ f_2 = 4xz^2 - y = 0 \end{cases}$$

можно добавить уравнение $x + y = 0$ и множество решений не изменится, поскольку $(x + y)^2 = f_1 x - f_2 y$. Теорема Гильберта о нулях утверждает, что множество решений системы не изменяет только добавление уравнений, полученных подобным способом.

Задача 3.15. 1) Показать на примере, что над полем $\mathbb{R}$ теорема Гильберта неверна.

2) Доказать, что если коэффициенты многочленов $f, f_1, \ldots, f_m$ вещественые и при этом f обращается в нуль на множестве общих нулей многочленов $f_1, \ldots, f_m$ над $\mathbb{C}$, то существуют такие многочлены $r_1, \ldots, r_m$ с вещественными коэффициентами, что $f^s = r_1 f_1 + \ldots + r_m f_m$ для некоторого $s \in \mathbb{N}$.

3.4. Применения в теории систем алгебраических уравнений над $\mathbb{C}$

Следствие 3.16. *Системы S_1 и S_2 эквивалентны тогда и только тогда, когда $r(I(S_1)) = r(I(S_2))$.*

Это следствие можно применять в конкретных задачах уже достаточно эффективно. Оно позволяет доказывать эквивалентность двух систем, не находя множества их решений.

Определение 3.17. Идеал I называется *радикальным*, если $I = r(I)$.

Следствие 3.16 показывает, что имеется естественная биекция между радикальными идеалами кольца многочленов и классами эквивалентности систем (т.е. аффинными алгебраическими многообразиями).

Задача 3.18. Доказать, что радикал произвольного идеала является радикальным идеалом.

Предложение 3.19. *Пусть $f_1(x_1, \ldots, x_n)$ и $f_2(x_1, \ldots, x_n)$ — два неприводимых многочлена. Уравнения $f_1 = 0$ и $f_2 = 0$ эквивалентны тогда и только тогда, когда многочлены f_1 и f_2 пропорциональны.*

Доказательство. Из неприводимости f_1 и теоремы о факториальности кольца многочленов следует, что если какая-то степень многочлена f делится на f_1, то и сам f делится на f_1. Поэтому $r((f_1)) = (f_1)$.

Уравнения эквивалентны тогда и только тогда, когда

$r((f_1)) = r((f_2)) \iff (f_1) = (f_2)$. Последнее равносильно пропорциональности многочленов (см. задачу 2.15). ■

Задача 3.20. На примере показать, что предложение 3.19 не может быть доказано над $\mathbb{R}$.

Задача 3.21. Доказать, что над $\mathbb{C}$ система эквивалентна одному уравнению тогда и только тогда, когда радикал идеала этой системы является главным идеалом. Верно ли, что в этой ситуации идеал системы является главным ?

Задача 3.22. Объяснить, почему утверждения леммы 1.26 и примера 2.8 эквивалентны.

Следствие 3.23. *Система S несовместна $\iff 1 \in I(S)$.*

Доказательство. $\Longleftarrow$ Если $1 \in I(S)$, то к системе можно добавить уравнение $1 = 0$, которое не имеет решений.

$\Longrightarrow$ Если S несовместна, то $X(S) = \emptyset$. В соответствии между аффинными многообразиями и радикальными идеалами пустому множеству отвечает идеал, совпадающий со всем кольцом многочленов (почему ?), откуда $J(X(S)) = r(I(S)) = \mathbb{C}[x_1, \ldots, x_n]$. Поэтому $1 \in r(I(S))$, т.е. $\exists s: \ 1^s \in I(S) \Longrightarrow 1 \in I(S)$. ■

Заметим, что в условиях следствия 3.23 $I(S) = \mathbb{C}[x_1, \ldots, x_n]$.

Пример 3.24. Система

$$\begin{cases} x^2 + xy - y + 1 = 0, \\ x^3 - x^2 + x + y^3 = 0, \\ y^4 + x^3 + yx^3 + x - 1 = 0 \end{cases}$$

несовместна.

Действительно, если обозначить уравнения $f_1 = 0$, $f_2 = 0$ и $f_3 = 0$ соответственно, то $xf_1 + yf_2 - f_3 = 1 = 0$ — противоречие. ■

Следствие 3.23 показывает, что уравнение "1=0" как следствие системы является единственной причиной несовместности системы над $\mathbb{C}$. Над полем $\mathbb{R}$ это не так.

При изучении на 1-ом курсе поля комплексных чисел студентам достаточно трудно объяснить, зачем такое поле рассматривать и почему надо полагать именно $i^2 = -1$. Хочется надеяться, что после изучения основной теоремы алгебры и теоремы Гильберта о нулях те достоинства, которыми обладают комплексные числа по сравнению с действительными, станут более понятными.

С другой стороны, системы с действительными коэффициентами очень важны в приложениях. Исследованию специфики систем алгебраических уравнений с действительными коэффициентами посвящено много работ, см. например обзор в разделе 3.2 книги [3].

В следующей главе мы вернемся к многочленам над произвольным полем. В идеале системы $I(S)$ будет построен некоторый замечательный базис — базис Гребнера. В главе 5 мы укажем ряд алгоритмов, позволяющих решать многие (но не все !) системы алгебраических уравнений. При этом теоретические результаты настоящей главы окажутся весьма полезными.

Глава 4.

Базис Гребнера идеала

4.1. Лексикографический порядок на множестве одночленов

Для нахождения базиса Гребнера идеала $I \lhd \mathbb{K}[x_1, \ldots, x_n]$ нам потребуется определить для многочлена $P(x_1, \ldots, x_n)$ понятие старшего члена.

Ясно, что старший член многочлена $3x^5 - x + 2$ есть одночлен $3x^5$. А как выделить старший член у многочлена от многих переменных, например у $x^2y + y^2x + z^5$? Имеется несколько способов однозначного определения старшего члена многочлена. Здесь мы рассмотрим только один такой способ, называемый *лексикографическим.*

Определение 4.1. Многочлен, состоящий из одного члена $P = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$, $a \in \mathbb{K}$, называют *одночленом* или *мономом.*

Старшим членом многочлена $P = \sum a_{i_1\ldots i_n}x_1^{i_1}\ldots x_n^{i_n}$ будет один из его одночленов $a_{i_1\ldots i_n}x_1^{i_1}\ldots x_n^{i_n}$. Каждому такому одночлену можно сопоставить набор $(i_1, \ldots, i_n)$ целых неотрицательных чисел, который называют *набором степеней.*

Например, при $n = 5$ одночлену $\sqrt{2}x_2^3x_4$ отвечает набор (0,3,0,1,0), а одночлену $3x_1^5x_4x_5^3$ — набор (5,0,0,1,3),

Определение 4.2. Будем говорить, что набор $(i_1, \ldots, i_n)$ *больше* набора $(j_1, \ldots, j_n)$, если $\exists k \le n$ такое, что $i_1 = j_1$,

$i_2 = j_2, \ldots, i_{k-1} = j_{k-1}, i_k > j_k$.

Например, при $n = 4$

$$(2,3,0,7) < (4,0,0,0) \ (k=1) \quad \text{и} \quad (3,1,5,2) > (3,1,5,1) \ (k=4).$$

Ясно, что указанным способом можно сравнить любые два различных набора одной длины.

Задача 4.3. а) Конечно ли число наборов, меньших данного набора $(i_1, i_2, \ldots, i_n)$?

б)* Пусть A_1, A_2, …— наборы целых неотрицательных чисел длины n. Доказать, что не существует бесконечной цепочки $A_1 > A_2 > \ldots$.

Замечание. Этот способ упорядочения наборов называют еще *чисто лексикографическим*. Рассматривают также *однородный лексикографический* порядок: у двух наборов $(i_1, \ldots, i_n)$ и $(j_1, \ldots, j_n)$ вначале сравнивают степени $\sum_{t=1}^n i_t$ и $\sum_{t=1}^n j_t$ и только в случае их совпадения наборы сравнивают лексикографически. При таком упорядочении решение задачи 4.3 сильно упрощается. Однако достоинства чисто лексикографического порядка мы увидим в главе 5. В главах 4-5 упорядочение всюду считается чисто лексикографическим.

Определение 4.4. *Старшим членом* многочлена

$$P(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$$

называется ненулевой одночлен $a_{i_1^0 \ldots i_n^0} x_1^{i_1^0} \ldots x_n^{i_n^0}$, такой что набор $(i_1^0, \ldots, i_n^0)$ больше всякого другого набора степеней, встречающегося в $P(x_1, \ldots, x_n)$.

Например, старший член многочлена $3x_1 + x_2^2 x_3^4 + x_4^7$ есть $3x_1$ (это может показаться странным!), а старший член многочлена $x^2y + y^2x + z^5$ есть x^2y (здесь мы нумеруем $x_1 = x$, $x_2 = y$, $x_3 = z$).

Лемма о старшем члене. Старший член произведения многочленов $P_1 \cdot P_2$ есть произведение старших членов P_1 и P_2.

Доказательство немедленно следует из того факта, что если $(i_1, \ldots, i_n) < (l_1, \ldots, l_n)$ и $(j_1, \ldots, j_n) \leq (k_1, \ldots, k_n)$, то $(i_1 + j_1, \ldots, i_n + j_n) < (l_1 + k_1, \ldots, l_n + k_n)$.

Творческая задача. Предложить несколько других способов упорядочения одночленов, для которых справедлива лемма о старшем члене. (Мы приведем примеры таких упорядочений в главе 7.)

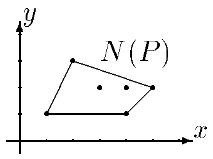
4.2. Многогранник Ньютона многочлена

Со времен Ньютона в математике известна следующая замечательная геометрическая интерпретация наборов степеней многочлена от многих переменных.

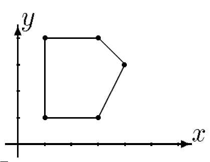
Рассмотрим многочлен

$$P(x,y) = 3xy + x^2y^3 - 5x^3y^2 - x^4y + 2x^4y^2 - x^5y^2$$

и отметим на плоскости $\mathbb{R}^2$ наборы степеней его одночленов: (1,1); (2,3); (3,2); (4,1); (4,2); (5,2). Получен конечный набор точек с целыми координатами. Их выпуклая оболочка есть выпуклый многоугольник (см. рисунок).



Его обозначают $N(P)$ и называют *многогранником (многоугольником) Ньютона* многочлена P (если P есть многочлен от n переменных, $N(P)$ есть выпуклый многогранник в пространстве $\mathbb{R}^n$). Оказывается, многие свойства многочлена P можно узнать только по многограннику $N(P)$ (попробуйте указать примеры таких свойств).



Задача 4.5. а) Найти набор степеней старшего члена многочлена, многоугольник Ньютона которого указан на рисунке.

б) Что представляет собой многогранник Ньютона для многочлена от одной переменной?

в) Найти число вершин, число ребер и число граней многогранника Ньютона многочлена

$$x^4 + 2y^4 + 3z^4 - xyz + 2x^3y^3 - xz + y^2z^2 - 5.$$

Определение 4.6. *Суммой Минковского* двух подмножеств P_1 и P_2 арифметического пространства называется подмножество

$$P_1 + P_2 = \{p_1 + p_2 \mid p_1 \in P_1, p_2 \in P_2\}.$$

Предложение 4.7. *Для любых многочленов f, $g \in \mathbb{K}[x_1, \ldots, x_n]$ имеет место равенство $N(fg) = N(f) + N(g)$.*

Замечание. Указанное свойство аналогично свойству степени многочлена из леммы о старшем члене. Можно сказать, что многогранник Ньютона является "обобщенной степенью" многочлена.

Доказательство. Пусть w – произвольная линейная функция на пространстве $\mathbb{R}^n$. Для произвольного выпуклого многогранника P будем называть подмножество

$$P^w = \{p \in P \mid w(p) \leq w(p') \;\; \forall \;\; p' \in P\}$$

гранью многогранника P, отвечающей функции w. (Легко видеть, что это определение соответствует нашему интуитивному пониманию того, что такое грань.)

Задача 4.8. Доказать, что сумма Минковского двух выпуклых многогранников является выпуклым многогранниiком. Доказать, что $(P_1 + P_2)^w = P_1^w + P_2^w$ для любых выпуклых многогранников P_1 и P_2. В частности, для любой вершины v многогранника $P_1 + P_2$ однозначно определены вершины v_1 и v_2 многогранников P_1 и P_2 соответственно, для которых $v = v_1 + v_2$. Показать на примере, что сумма двух вершин не всегда является вершиной.

Многогранник $N(fg)$ – это выпуклая оболочка точек v_1+v_2, где v_1 пробегает наборы степеней f, а v_2 – наборы степеней g (почему ?). Но все эти точки лежат в $N(f)+N(g)$, причем среди них есть все вершины многогранника $N(f)+N(g)$. ■

Ряд интересных свойств многогранников Ньютона, а также обобщение этого понятия с одного многочлена на полиномиальный идеал можно найти в книге Б. Штурмфельса [8].

4.3. Задача вхождения

Вернемся к идеалам в кольцах многочленов. Как выяснить, принадлежит ли многочлен $h(x)$ главному идеалу $(f(x))$? Да очень просто, нужно делить многочлен $h(x)$ на $f(x)$ "в столбик" и если разделится без остатка, то $h(x) \in (f(x))$, иначе $h(x) \notin (f(x))$.

Задача 4.9. Принадлежит ли x^2+2 идеалу (x^3+x+1)?

Аналогичная задача часто возникает и для многочленов от нескольких переменных, но здесь ее решение существенно сложнее.

Задача вхождения. Пусть идеал $I \triangleleft \mathbb{K}[x_1,\ldots,x_n]$ задан своим базисом $I=(f_1,\ldots,f_m)$. Требуется найти алгоритм, позволяющий за конечное число шагов выяснить, принадлежит ли данный многочлен $h(x_1,\ldots,x_n)$ идеалу I, т.е. существуют ли такие многочлены $r_1(x_1,\ldots,x_n),\ldots,r_m(x_1,\ldots,x_n)$, что $h = f_1r_1+\ldots+f_mr_m$.

Пример 4.10. Принадлежит ли многочлен $h = x_2x_3^2x_4 - x_1x_3x_4^2$ идеалу $(x_1+x_2, x_3+x_4) \triangleleft \mathbb{K}[x_1,x_2,x_3,x_4]$?

Ответ. Да, $h=(x_1+x_2)x_3^2x_4-(x_3+x_4)x_1x_3x_4$.

Здесь мы использовали подбор. Этот метод не поможет при более громоздких выражениях для h и f_i.

Задача 4.11. Доказать, что $x+y^2x+3xy^3 \notin (x^2,y) \triangleleft \mathbb{K}[x,y]$.

4.4. Определение базиса Гребнера и решение задачи вхождения

После некоторых раздумий можно найти следующий метод упрощения выражения для h в задаче вхождения.

Зафиксируем обозначения. Для всякого многочлена P имеем $P = P_C + P_M$, где P_C — старший член P, а P_M — сумма остальных членов. Например, для $P = 2x^2 + xy^3 - 4z^2$ $P_C = 2x^2$, $P_M = xy^3 - 4z^2$.

Операция редукции. Предположим, что старший член многочлена h делится на старший член некоторого из многочленов f_i, т.е. $h_C = f_{iC}Q$, где Q — одночлен. Тогда положим $h_1 = h - Qf_i = Q(-f_{iM}) + h_M$. При этом старший член h_1 меньше старшего члена h.

Лемма 4.12. $h \in (f_1, \ldots, f_m) \Longleftrightarrow h_1 \in (f_1, \ldots, f_m)$.

Доказательство. Достаточно проверить, что разность $h-h_1$ принадлежит $(f_1, \ldots, f_m)$. Имеем $h - h_1 = Qf_i \in (f_1, \ldots, f_m)$. ■

Итак, задачу вхождения теперь можно решать не для h, а для h_1 и здесь вновь можно применять редукцию (возможно, с другим f_i). Если за конечное число редукций многочлен h сведется (редуцируется) к нулю, то $h \in (f_1, \ldots, f_m)$, т.к. нуль принадлежит любому идеалу.

Пример 4.13. $h = x_2x_3^2x_4 - x_1x_3x_4^2$, $f_1 = x_1 + x_2$, $f_2 = x_3 + x_4$. Моном $h_C = -x_1x_3x_4^2$ делится на $f_{1C} = x_1$ $(Q = -x_3x_4^2)$

Редукция 1. $h \to x_2x_3^2x_4 + x_2x_3x_4^2 = h_1$. Здесь $h_{1C} = x_2x_3^2x_4$ делится на $f_{2C} = x_3$ $(Q = x_2x_3x_4)$.

Редукция 2. $h_1 \to x_2x_4^3 + x_2x_3x_4^2 = h_2$ (редукция произведена дважды). Здесь $h_{2C} = x_2x_3x_4^2$ делится на $f_{2C} = x_3$ $(Q = x_2x_4^2)$.

Редукция 3. $h_2 \to x_2x_4^3 - x_2x_4^3 = 0$.

Итак, $h \in (f_1, f_2)$.

А как быть, если h не редуцируется к нулю, т.е. на некотором этапе возникает многочлен, старший член которого не делится ни на один из одночленов f_{1C}, f_{2C}, …, f_{mC}? Можно ли утверждать, что h не принадлежит идеалу ?

Как это часто бывает в математике, если мы не можем сказать ничего конкретного, мы фиксируем желаемое в определении.

Определение 4.14. Базис $f_1, \ldots, f_m$ идеала $I = (f_1, \ldots, f_m)$ называется *базисом Гребнера* этого идеала, если всякий многочлен $h \in I$ редуцируется к нулю при помощи $f_1, \ldots, f_m$,

или

Определение 4.14.1 Набор многочленов $f_1, \ldots, f_m$ — *базис Гребнера* в $I = (f_1, \ldots, f_m)$, если для любого $h \in I$ одночлен h_C делится на один из одночленов $f_{1C}, f_{2C}, \ldots, f_{mC}$.

Задача 4.15. а) Доказать эквивалентность этих определений.

б) Пусть $f_1, \ldots, f_m$ — базис Гребнера идеала I. Доказать, что если $h \in I$, то h редуцируется к нулю произвольной применимой к нему последовательностью редукций.

Задача 4.16. Пусть $f_1, \ldots, f_m$ – набор многочленов из идеала I, для которых старший член h_C любого элемента $h \in I$ делится на один из старших членов f_{iC}. Доказать, что в этом случае многочлены $f_1, \ldots, f_m$ являются базисом идеала I и тем самым являются базисом Гребнера в I.

Пример 4.17. Покажем, что $f_1 = x$, $f_2 = y$ есть базис Гребнера в идеале $(x, y) \triangleleft \mathbb{K}[x, y]$. Пусть $h(x, y)$ — произвольный многочлен. Если старший член h делится на x, то редукция с помощью f_1 есть замена x на 0 (обнуление старшего члена). Если старший член делится на y, редукция с помощью f_2 также обнуляет старший член. Поэтому всякий многочлен редуцируется к своему свободному члену. Остается заметить, что многочлен принадлежит идеалу (x, y) тогда и только тогда, когда его свободный член равен нулю.

Пример 4.18. Рассмотрим идеал $I = (x^2 - y, x^2 - z) \triangleleft \mathbb{K}[x, y, z]$, $f_1 = x^2 - y$, $f_2 = x^2 - z$. Многочлен $z - y \in I$, так как $z - y =$

$f_1 - f_2$. С другой стороны, старший член $z - y$ не делится на старшие члены f_1 и f_2 (они равны x^2). Поэтому f_1 и f_2 не образуют базис Гребнера идеала I. Ниже мы докажем, что f_1, f_2 и $f_3 = z - y$ — базис Гребнера в I.

Решение задачи вхождения. Предположим, что нам известен базис Гребнера идеала I. Пусть дан многочлен h. Будем производить всевозможные редукции h с помощью элементов базиса (любая из цепочек возможных редукций конечна). Многочлен h лежит в I тогда и только тогда, когда в результате редукций получаем нуль.

Это решение представляет собой алгоритм, который несложно реализовать на ЭВМ и применять к задачам со сколь угодно сложными выражениями для f_i и h.

Заметим, что из задачи 4.16 и теоремы Гильберта о базисе вытекает существование базиса Гребнера в любом идеале. В самом деле, рассмотрим идеал, порожденный старшими членами элементов идеала и выберем в нем конечный базис из числа образующих. Тогда элементы исходного идеала, старшие члены которых образуют базис идеала старших членов, составляют конечный базис Гребнера исходного идеала. Однако это доказательство существования не дает алгоритма построения базиса Гребнера идеала по некоторому его исходному базису. Такой алгоритм будет предъявлен в следующем параграфе.

4.5. Алгоритм Бухбергера Бриллиантовая лемма

Пусть $I \triangleleft \mathbb{K}[x_1, \ldots, x_n]$ — идеал и $f_1, \ldots, f_m$ — его базис.

Определение 4.19. Говорят, что многочлены f_i и f_j имеют *зацепление*, если их старшие члены f_{iC} и f_{jC} делятся одновременно на некоторый одночлен w, отличный от константы.

Если f_i и f_j имеют зацепление, т.е. $f_{iC} = wq_1$, $f_{jC} = wq_2$, где w – наибольший общий делитель f_{iC} и f_{jC}, то рассмотрим многочлен $F_{i,j} = f_i q_2 - f_j q_1 \in I$. (Его принято называть S-многочленом пары f_i, f_j и обозначать $S(f_i, f_j)$ или $S(i, j)$.) Редуцируем многочлен $F_{i,j}$ с помощью базиса $f_1, \ldots, f_m$ до тех пор, пока это возможно. В результате получим нередуцируемый многочлен $\widetilde{F}_{i,j}$. Если $\widetilde{F}_{i,j} \equiv 0$, то будем говорить, что зацепление *разрешимо.* Иначе добавим $\widetilde{F}_{i,j}$ к базису идеала I: $f_{m+1} = \widetilde{F}_{i,j}$.

В новом базисе $f_1, \ldots, f_m, f_{m+1}$ будем вновь искать возможные зацепления и редуцировать соответствующие многочлены $F_{i,j}$.

Задача 4.20. В базисе $f_1, \ldots, f_m, f_{m+1}$ зацепление (i, j) разрешимо.

Пример 4.21. Рассмотрим идеал $I = (x^2 - y, x^2 - z)$ (Пример 4.18). Здесь $f_1 = x^2 - y$, $f_2 = x^2 - z$. Имеется зацепление $f_{1C} \,\vdots\, x^2$, $f_{2C} \,\vdots\, x^2$, $\Longrightarrow F_{1,2} = -y + z$. Положим $f_3 = y - z$. Других зацеплений нет.

Пример 4.22. Пусть $I = (f_1 = x^2 + y^2 + z^2, f_2 = x + y - z, f_3 = y + z^2)$. Зацепление имеют только f_1 и f_2:

$$F_{1,2} = f_1 - xf_2 = y^2 + z^2 - xy + xz = -xy + xz + y^2 + z^2.$$

Редуцируем с помощью f_2:

$$-xy + xz + y^2 + z^2 \rightsquigarrow (y - z)y - (y - z)z + y^2 + z^2 = 2y^2 + 2z^2 - 2yz.$$

Редуцируем с помощью f_3:

$$2y^2 + 2z^2 - 2yz \rightsquigarrow 2z^4 + 2z^3 + 2z^2.$$

Дальше редуцировать нельзя $\Longrightarrow f_4 = 2z^4 + 2z^3 + 2z^2$. На константу можно сократить и считать, что $f_4 = z^4 + z^3 + z^2$. Других зацеплений нет.

Оказывается, что и в общем случае возможно лишь конечное число неразрешимых зацеплений.

Теорема 4.23. *Для каждого набора многочленов $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ после редуцирования конечного числа зацеплений мы получим набор $f_1, \ldots, f_m, f_{m+1}, \ldots, f_M$, в котором каждое зацепление разрешимо.*

Теорема 4.24. *(Diamond Lemma). Базис $f_1, \ldots, f_m$ идеала I является базисом Гребнера тогда и только тогда, когда в нем нет зацеплений или каждое зацепление разрешимо.*

Доказательства этих теорем приведены в Главе 6.

Теоремы 4.23 и 4.24 обосновывают существование эффективного алгоритма для построения базиса Гребнера идеала. Этот алгоритм называется *алгоритмом Бухбергера.* Повторим еще раз его этапы. Пусть $f_1, \ldots, f_m$ – набор многочленов, являющийся базисом идеала I.

1) Проверим, есть ли в наборе зацепления. Если зацеплений нет, то набор является базисом Гребнера идеала I, иначе переходим к пункту 2.

2) По найденному зацеплению (i, j) многочленов f_i и f_j положим $f_{iC} = wq_1$, $f_{jC} = wq_2$, и составим многочлен $F_{i,j} = f_i q_2 - f_j q_1$. Редуцируем многочлен $F_{i,j}$ с помощью набора $\{f_i\}$ до тех пор, пока это возможно. Если многочлен $F_{i,j}$ редуцировался к ненулевому многочлену f, то переходим к пункту 3, иначе к пункту 4. (Отметим, что редуцируемость многочлена $F_{i,j}$ к нулю и вид многочлена f вообще говоря зависят от выбранной нами последовательности применяемых редукций (покажите это на примере !). В алгоритме мы используем любую применимую последовательность редукций и, получив нередуцируемый многочлен f, переходим к пункту 3, более никогда зацепление (i, j) не рассматривая.)

3) Добавляем многочлен f к набору $f_1, f_2, \ldots, f_k$ в качестве f_{k+1} и переходим к пункту 4.

4) В построенном к настоящему моменту множестве многочленов $\{f_i\}$ рассматриваем зацепление, которое не было рассмотрено ранее, и переходим к пункту 2. Если все имеющиеся зацепления ранее рассматривались, алгоритм завершен.

За конечное число шагов мы получим набор $f_1, \dots, f_m, f_{m+1}, \dots, f_M$, где каждое зацепление разрешимо. Это и есть базис Гребнера идеала $I = (f_1, \dots, f_m)$ (см. примеры 4.21, 4.22).

Задача 4.25. Когда набор многочленов $f_1(x), \dots, f_m(x)$ является базисом Гребнера порожденного ими идеала в $\mathbb{K}[x]$?

4.6. Минимальный редуцированный базис Гребнера

Итак, базис Гребнера идеала $I \triangleleft \mathbb{K}[x_1, \dots, x_n]$ построен. Можно ли его упростить?

Упрощение первое. Пусть f_1 и f_2 — элементы базиса Гребнера такие, что f_{1C} делится на f_{2C}. Тогда удалим элемент f_1 из базиса.

Задача 4.26. Элементы $f_2, \dots, f_m$ по-прежнему составляют базис Гребнера идеала I.

Определение 4.27. Базис Гребнера $\{f_1, \dots, f_m\}$ называется *минимальным*, если f_{iC} не делится на f_{jC} при $i \neq j$.

Каждый базис Гребнера можно свести к минимальному, отбрасывая "лишние" члены. Отметим, что минимизацию можно применять к базису идеала только если известно что этот базис является базисом Гребнера, иначе может измениться сам идеал I (рассмотрите идеал $(x, x+y)$!).

Упрощение второе касается нестарших членов многочленов $f_1, \dots, f_m$. Предположим, что некоторый член q многочлена f_i делится на старший член многочлена f_j. Тогда редуцируем q с помощью f_j и результат редукции запишем в f_i на место q. При этой операции базис Гребнера идеала остается базисом Гребнера, число элементов базиса не изменяется, но понижаются степени членов многочленов $f_1, \dots, f_m$.

Определение 4.28. Базис Гребнера $\{f_1, \dots, f_m\}$ называется *редуцированным*, если ни один член многочлена f_i не делится на старший член многочлена f_j для всех $i, j = 1, \dots, m$, $i \neq j$.

Каждый базис Гребнера конечной последовательностью редукций можно свести к редуцированному базису Гребнера. Оказывается, больше никаких упрощений произвести нельзя. Более того, имеет место

Теорема 4.29. *Минимальный редуцированный базис Гребнера идеала $I \triangleleft \mathbb{K}[x_1, \ldots, x_n]$ определен однозначно*[1]*, т.е. не зависит от выбора исходного базиса идеала I и от последовательности проводимых операций (но зависит от упорядочения переменных $x_1, \ldots, x_n$).*

(Доказательство см. в Главе 6.)

Пример 4.30. Рассмотрим базис Гребнера $f_1 = x^2 + y^2 + z^2$; $f_2 = x + y - z$; $f_3 = y + z^2$; $f_4 = z^4 + z^3 + z^2$ из примера 4.22.

1) *Минимизация:* старший член f_1 делится на старший член $f_2 \Longrightarrow f_1$ можно отбросить.

   Минимальный базис: $\{f_2, f_3, f_4\}$.

2) *Редукция:* заменяем y в f_2 на $-z^2$. Имеем: $f_2 \rightsquigarrow x - z^2 - z$. Больше редукций делать не с чем. Итак, минимальный редуцированный базис есть $\{x - z^2 - z; y + z^2; z^4 + z^3 + z^2\}$.

Задача 4.31. Выберите какой-либо другой базис в идеале из примера 4.30 и убедитесь, что построенный с помощью этого базиса минимальный редуцированный базис Гребнера совпадает с уже построенным.

Задача 4.32. Укажите алгоритм, определяющий, совпадают ли идеалы $(f_1, \ldots, f_k)$ и $(g_1, \ldots, g_s)$ в кольце $\mathbb{K}[x_1, \ldots, x_n]$.

С точки зрения теории систем алгебраических уравнений построение минимального редуцированного базиса Гребнера идеала системы состоит из двух этапов. На первом этапе, редуцируя всевозможные зацепления, мы добавляем новые (нередуцируемые к нулю) уравнения к исходной системе не изменяя множества ее решений (поскольку добавленные уравнения

[1] Мы дополнительно предполагаем, что числовой коэффициент при старшем члене каждого элемента нашего базиса равен единице.

принадлежат идеалу системы). На втором этапе мы отбрасываем (минимизация) или "упрощаем" (редуцирование) некоторые уравнения системы. При этом часто оказывается, что именно исходные уравнения системы либо отброшены, либо существенно упрощены и полученная система (а она эквивалентна исходной) легко решается. Однако базис Гребнера не всегда допускает упрощения, и в этом случае мы просто увеличиваем число уравнений системы. Но и эта процедура полезна при решении системы и, как показывают результаты следующей главы, успех (возможно при помощи компьютерных вычислений) во многих случаях гарантирован.

Задача 4.33. Показать, что для систем линейных уравнений алгоритм Бухбергера плюс минимизация есть метод Гаусса приведения системы к ступенчатому виду, а переход к редуцированному базису Гребнера равносилен обратному ходу в методе Гаусса (выражение главных неизвестных через свободные).

Задача 4.34. Показать, что алгоритм Бухбергера плюс минимизация в случае многочленов от одной переменной доставляют алгоритм нахождения НОДа конечного набора многочленов.

В этом курсе мы не станем обсуждать проблему оценки сложности алгоритма Бухбергера. Перечислим лишь чем такая сложность измеряется. Пусть дан идеал I кольца $\mathbb{K}[x_1, \ldots, x_n]$, порожденный k многочленами, степени которых не превосходят числа d. При фиксированных значениях n, k и d нужно оценить:

1) максимально возможную степень многочлена, возникающего в минимальном редуцированном базисе Гребнера;

2) число элементов минимального редуцированного базиса Гребнера;

3) степени и коэффициенты многочленов, возникающих в промежуточных вычислениях;

4) число операций, которые необходимо произвести.

Эти характеристики будут зависить от того, какой порядок на множестве одночленов мы выберем (общее понятие порядка будет обсуждаться в главе 7), а также какую из модификаций алгоритма Бухбергера будем использовать. Информацию на этот счет можно найти в книгах, указанных в конце текста, а также в цитируемых там журнальных статьях. Следует отметить, что в этом направлении остается еще много нерешенных задач и, видимо, еще преждевременно говорить о том, что удовлетворительная теория здесь построена.

4.7. Вычисление базисов Гребнера

Мы предлагаем читателю использовать изложенные выше сведения в конкретных вычислениях. Постройте минимальный редуцированный базис Гребнера для идеалов (во всех задачах считаем $x > y > z$ и вычисляем базис Гребнера для чисто лексикографического порядка):

1) $(x^2 - 1,\ (x-1)y,\ (x+1)z)$;

2) $(x^2 - 1,\ (x-1)y,\ (x-1)z)$;

3) $(x^3yz - xz^2,\ xy^2z - xyz,\ x^2y^2 - z)$;

4) $(x^2y + xz + y^2z,\ xz^2 - zy,\ xyz - y^2)$;

5) $(xy^2 - z - z^2,\ x^2y - y,\ y^2 - z^2)$;

6) $(xy + x^2z,\ xz + yz^3,\ yz - y^2z^3)$.

Глава 5.

Применение базисов Гребнера для решения систем алгебраических уравнений

5.1. Критерий несовместности

В этом параграфе будет указан эффективный критерий несовместности для системы алгебраических уравнений. Основное поле предполагается полем $\mathbb{C}$.

Теорема 5.1. *Система S несовместна тогда и только тогда, когда базис Гребнера идеала $I(S)$ содержит ненулевую константу.*

Доказательство. Если ненулевая константа принадлежит $I(S)$, то система несовместна. Наоборот, если S несовместна, то по следствию 3.23 $1 \in I(S)$. Поэтому старший член некоторого элемента базиса Гребнера делит 1 и потому есть константа. ∎

Задача 5.2. Выпишите некоторую (не совсем простую) несовместную систему S и вычислите базис Гребнера идеала $I(S)$.

Отметим, что в математике имеются и другие способы выяснения совместна ли данная САУ или нет. Так широко известная в математической логике теорема Тарского-Зайденберга об элиминации кванторов позволяет в частности распознавать совместность систем над вещественными и комплексными числами. Доказательство этой теоремы, основанное на "методе интервалов" (см. раздел 3.8 книги Н. К. Верещагин, А. Шень, Языки и исчисления, М.: МЦНМО, 2000, 286 стр.), предлагает достаточно простой (но трудоемкий !) алгоритм для такого распознавания.

5.2. Критерий эквивалентности систем

Поиск алгоритма для выяснения эквивалентности двух систем над комплексными числами естественно приводит нас к алгоритмическому исследованию радикала идеала. Начнем с алгоритма, определяющего, принадлежит ли многочлен радикалу данного идеала.

Задача* 5.3. Пусть $\mathbb{K}$ – произвольное поле. Рассмотрим идеал $I = (f_1, \ldots, f_m)$ кольца $\mathbb{K}[x_1, \ldots, x_n]$.

1) Доказать, что многочлен $f \in \mathbb{K}[x_1, \ldots, x_n]$ тогда и только тогда лежит в радикале идеала I, когда в кольце $\mathbb{K}[x_1, \ldots, x_n, y]$ (здесь y - дополнительная переменная) идеал $(f_1, \ldots, f_m, 1-yf)$ совпадает со всем кольцом;

2) Указать алгоритм, определяющий, принадлежит ли многочлен f радикалу идеала $(f_1, \ldots, f_m)$.

Следствие 3.16 показывает, что две системы S_1 и S_2 эквивалентны тогда и только тогда, когда $I(S_1) \subseteq r(I(S_2))$ и $I(S_2) \subseteq r(I(S_1))$. Отсюда непосредственно следует

Теорема 5.4. *Две системы над полем комплексных чисел*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \quad \cdots\cdots\cdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \qquad \text{и} \qquad \begin{cases} g_1(x_1, \ldots, x_n) = 0, \\ \quad \cdots\cdots\cdots \\ g_k(x_1, \ldots, x_n) = 0 \end{cases}$$

эквивалентны тогда и только тогда, когда $f_i \in r((g_1, \ldots, g_k))$

$i = 1, \ldots, m$ *и* $g_j \in r((f_1, \ldots, f_m)), j = 1, \ldots, k$ [1].

Задача 5.5. Пусть $I = (f_1, \ldots, f_m)$ и $l = a_1x_1 + \ldots + a_nx_n$, $a_i \in \mathbb{K}$. Указать алгоритм, определяющий минимальное число s, для которого $l^s \in I$, или показывающий, что l не лежит в радикале идеала I.

Далее естественно рассмотреть задачу об алгоритмическом построении образующих радикала данного идеала. Эта задача решена, однако ее решение слишком сложное для того, чтобы обсуждать его в этом курсе. Подготовленному читателю мы рекомендуем обратиться к статьям (Gianni P., Trager B., Zacharias G, Gröbner bases and primary decomposition of polynomial ideals, in: Computational Aspects of Commutative Algebra, ed. by Robbiano L., Academic Press, New York, 1988, 15-33) и (Eisenbud D., Huneke C., Vasconcelos W., Direct methods for primary decomposition, Invent. Math., 110 (1992), 207-235). Было бы очень интересно отыскать простое решение указанной задачи.

5.3. Критерий конечности числа решений системы

Предположим, что система S от неизвестных $x_1, x_2, \ldots, x_n$ имеет конечное число решений. Тогда неизвестная x_1 может принимать на множестве решений только конечное число значений. Обозначим их $\alpha_1, \alpha_2, \ldots, \alpha_{N_1}$. Многочлен $f(x_1) = (x_1 - \alpha_1)(x_1 - \alpha_2) \ldots (x_1 - \alpha_{N_1})$ обращается в ноль на множестве решений системы S. По теореме Гильберта о нулях $\exists k_1 \in \mathbb{N} : f^{k_1} \in I(S)$. Старший член многочлена f^{k_1} есть $x_1^{N_1k_1}$. По определению базиса Гребнера имеется такой элемент f_i в этом базисе, что старший член f_i делит старший член f^{k_1}. Поэтому старший член f_i есть степень переменной x_1. Аналогично, для остальных переменных $x_2, \ldots, x_n$ должны найтись элементы

[1] Автор благодарен А. Гайфуллину, обратившему его внимание на этот результат.

базиса Гребнера, старшие члены которых являются степенями этих переменных.

Обратно, пусть $f_1, \ldots, f_n$ — элементы базиса Гребнера идеала $I(S)$ такие, что старший член f_{iC} равен $x_i^{N_i}$. В силу лексикографического упорядочения одночленов (вот где существенно, что порядок чисто лексикографический !) многочлен f_n не содержит переменных $x_1, x_2, \ldots, x_{n-1}$, т.е.

$$f_n = a_{N_n} x_n^{N_n} + a_{N_n-1} x_n^{N_n-1} + \ldots + a_1 x_n + a_0$$

и $a_{N_n} \neq 0$. Отсюда, переменная x_n как корень многочлена от одной неизвестной может принимать лишь конечное число значений. Аналогично, многочлен f_{n-1} зависит лишь от x_n и x_{n-1} и старший член его не равен нулю ни при каких значениях x_n. Но x_n принимает лишь конечное число значений, и потому значения x_{n-1} принадлежат множеству корней конечного числа многочленов, то есть конечному множеству. Рассуждая аналогично, мы показываем, что переменные $x_{n-2}, x_{n-3}, \ldots, x_1$ могут принимать лишь конечное число значений. Тем самым доказана

Теорема 5.6. *Число решений системы S конечно тогда и только тогда, когда базис Гребнера идеала $I(S)$ содержит элементы $f_1, f_2, \ldots, f_n$, старшие члены которых являются степенями переменных $x_1, x_2, \ldots, x_n$ соответственно.*

Заметим, что в данном критерии не требуется, чтобы старшие члены всех элементов базиса Гребнера являлись степенями переменных.

Итак, применяя алгоритм Бухбергера к произвольной системе S, мы получаем базис Гребнера и, глядя на него, можно сразу сказать, конечно или бесконечно число решений системы.

Если мы выяснили, что система S имеет решения и их конечное число, то наш алгоритм сводит решение системы к последовательному решению конечного числа алгебраических уравнений от одной неизвестной. Хотя точной формулы здесь вообще говоря нет (теорема Абеля), известно много достаточно точных численных методов решения и потому можно использовать компьютер.

Задача 5.7. Показать, что для систем линейных уравнений указанный критерий конечности числа решений эквивалентен критерию определенности системы из главы 1 (см. теорему 1.12).

Пример 5.8. Решить систему:

$$\begin{cases} ab = c^2 + c, \\ a^2 = a + bc, \\ ac = b^2 + b. \end{cases}$$

Будем считать $a > b > c$. Занумеруем уравнения f_1, f_2 и f_3. Зацепления f_1 и f_2 дают

$$f_1 \cdot a - f_2 \cdot b = (-c^2 - c)a + (a + bc)b = ab - ac + b^2c - ac^2 = f_4.$$

Редукция с помощью f_1: $f_4 \rightsquigarrow -ac^2 - ac + b^2c + c^2 + c = \overline{f_4}$.

Редукция с помощью f_3: $\overline{f_4} \rightsquigarrow -b^2 - b - bc + c^2 + c = \overline{\overline{f_4}}$.

Зацепление f_2 и f_3: $f_2c - f_3a = ab + ab^2 - ac - bc^2 = f_5$.

Редукция с помощью f_1: $f_5 \rightsquigarrow -ac + cb + c^2 + c = \overline{f_5}$.

Редукция с помощью f_3: $\overline{f_5} \rightsquigarrow -b^2 - b + cb + c^2 + c = \overline{\overline{f_5}}$.

Редукция с помощью $\overline{\overline{f_4}}$: $\overline{\overline{f_5}} \rightsquigarrow 2bc = \overline{\overline{\overline{f_5}}}$

Зацепление f_1 и f_3: $f_1c - f_3b = b^3 + b^2 - c^3 - c^2 = f_6$.

Редукция с помощью $\overline{\overline{f_4}}$: $f_6 \rightsquigarrow -b^2c + bc + bc^2 - c^3 - c^2 = \overline{f_6}$

Редукция с помощью $\overline{\overline{f_4}}$: $\overline{f_6} \rightsquigarrow 2bc + 2bc^2 - 2c^3 - 2c^2 = \overline{\overline{f_6}}$

Редуцируем $\overline{\overline{f_6}}$ с помощью $\overline{\overline{\overline{f_5}}}$. Получим $-2c^3 - 2c^2 = \overline{\overline{\overline{f_6}}}$. Мы видим, что в базисе Гребнера лежат элементы $a^2 - a - bc$, $-b^2 - b - bc + c^2 + c$, $-2c^3 - 2c^2$. Отсюда следует конечность числа решений. Найдем эти решения. Из $-2c^3 - 2c^2 = 0 \Longrightarrow c = 0$ или $c = -1$.

1) $c = -1$. Из $2bc = 0 \Longrightarrow b = 0$. Имеем $a^2 - a - bc = 0 \Longrightarrow a^2 = a \Longrightarrow a = 0$ или $a = 1$. Наборы: $(1, 0, -1)$ — не годится, $(0, 0, -1)$ — годится.

2) $c = 0 \Longrightarrow a^2 = a \Longrightarrow a = 0$ или $a = 1$, $b^2 + b = 0 \Longrightarrow b = 0$ или $b = -1$. Наборы: $(0, 0, 0)$ — годится, $(0, -1, 0)$ — годится, $(1, 0, 0)$ — годится, $(1, -1, 0)$ — не годится.

Ответ. $\{(0, 0, 0);\ (1, 0, 0);\ (0, -1, 0);\ (0, 0, -1)\}$.

Пример 5.9. Решить систему:

$$\begin{cases} ab = c^2 + c, \\ a^2 + a = bc, \\ ac = b^2 + b. \end{cases}$$

Зацепление f_1 и f_2: $f_1 \cdot a - f_2 \cdot b = -ab - ac + b^2c - ac^2 = f_4$.

Редукция с помощью f_1: $f_4 \rightsquigarrow -ac^2 - ac + b^2c - c^2 - c = \overline{f_4}$

Редукция с помощью f_3: $\overline{f_4} \rightsquigarrow -b^2 - b - bc - c^2 - c = \overline{\overline{f_4}}$.

Дальнейшие вычисления показывают, что все прочие зацепления редуцируются к нулю.

Значит, базис Гребнера состоит из 4-х элементов

$$\{f_1, f_2, f_3, \overline{\overline{f_4}}\}.$$

Отсюда следует, что переменная c может принимать бесконечно много значений.

5.4. Свободные неизвестные Размерность множества решений

Обратимся теперь к системам, имеющим бесконечное множество решений. Что значит здесь решить систему? Ведь перечислить явно бесконечно много решений невозможно. Выход подсказывает понятие свободной неизвестной из теории линейных систем (параграф 1.2): для описания множества решений все переменные разделяются на два множества — свободные и главные. Свободным неизвестным можно придавать любые значения, а главные выражаются через них. Однако в нелинейном случае на этом пути встает ряд трудностей. Проиллюстрируем их на примере.

Пример 5.10. Рассмотрим уравнение $x^3y^2 = 1$. Ясно, что оно имеет бесконечно много решений. В то же время ни x ни y не может принимать все значения, т.к. $x \neq 0$, $y \neq 0$. Если все-таки считать x свободной, $x \in \mathbb{C} \setminus \{0\}$, то $y = \sqrt{1/x^3}$. Но функция $\sqrt{\ }$ над полем $\mathbb{C}$ определена неоднозначно — каждому значению x отвечают два значения y.

Попытаемся определить понятие свободной неизвестной для произвольной системы с учетом указанных трудностей.

Определение 5.11. Множество $H_F \subset \mathbb{C}^n$ решений ненулевого уравнения $F(x_1, \ldots, x_n) = 0$ называется *гиперповерхностью*[2].

Определение 5.12. Подмножество $U \subset \mathbb{C}^n$ называется *алгебраически плотным* (далее просто *плотным*), если его дополнение содержится в некоторой гиперповерхности H_F.

Задача 5.13. 1) Какие подмножества плотны в $\mathbb{C}$?

2) Привести несколько примеров плотных подмножеств в $\mathbb{C}^2$.

Теорема 5.14. *Пусть S — система уравнений от неизвестных $x_1, x_2, \ldots, x_n$; $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ — некоторый набор из этих неизвестных и $Ox_{i_1} \ldots x_{i_k}$ — соответствующее координатное подпространство в $\mathbb{C}^n$. Координатная проекция $\mathbb{C}^n \to$*

[2]Как показывает задача 1.25, над алгебраически незамкнутым полем любое аффинное многообразие является гиперповерхностью.

$Ox_{i_1}\dots x_{i_k}$ определяет отображение множества решений $X(S)$ системы S на подпространство $Ox_{i_1}\dots x_{i_k}$, и образ этого отображения либо плотен в $Ox_{i_1}\dots x_{i_k}\cong\mathbb{C}^k$, либо лежит в некоторой гиперповерхности H_F в $\mathbb{C}^k$.

(Доказательство см. в Главе 6.)

В первом случае набор переменных $x_{i_1},\dots,x_{i_k}$ называют *свободным* (ведь эти переменные могут принимать почти любые наборы значений на множестве решений $X(S)$), а во втором случае — *зависимым* (поскольку значения переменных $x_{i_1},\dots,x_{i_k}$ на множестве решений лежат на гиперповерхности $F(x_{i_1},\dots,x_{i_k})=0$).

Определение 5.15. *Размерностью* $dim\ X(S)$ множества решений $X(S)$ системы S называется максимальное число переменных по всем свободным наборам переменных. Свободный набор переменных, в котором число переменных равно $dim\ X(S)$, будем называть *максимальным свободным набором переменных.* Если свободных переменных нет, будем говорить, что множество решений *нульмерно.*

Задача* 5.16. Пусть $F(x_1,\dots,x_n)$ — ненулевой многочлен. Доказать, что размерность множества решений уравнения $F=0$ равна $n-1$.

Задача 5.17. Доказать, что набор из одной переменной $\{x_i\}$ является свободным для системы S тогда и только тогда, когда x_i принимает бесконечно много значений на множестве решений $X(S)$.

Задача 5.18. Доказать, что подмножество свободного набора переменных вновь является свободным набором переменных.

Задача* 5.19. Привести пример системы и свободного набора переменных для этой системы, который не может быть включен в максимальный свободный набор переменных.

Как для данной системы эффективно находить максимальные свободные наборы переменных и размерность множества решений?

Здесь нам вновь помогут базисы Гребнера.

Алгоритм поиска максимального свободного набора переменных:

1) Рассмотрим лексикографический порядок:

   $x_1 > x_2 > \ldots > \widehat{x_i} > \ldots > x_n > x_i$ (переменная x_i переставлена в конец) и построим для него базис Гребнера идеала $I(S)$. Если в нем есть элемент, зависящий только от x_i, то x_i — зависимая переменная, иначе — свободная.

   Таким образом, найдем хотя бы одну свободную переменную (если таковой нет, то множество решений нульмерно).

2) Перенумеровав переменные, считаем, что x_n — свободная. Переставляя на предпоследнее место переменные $x_1, \ldots, x_{n-1}$, строим базисы Гребнера для лексикографических порядков $x_1 > x_2 > \ldots > \widehat{x_i} > \ldots > x_i > x_n$. Если такой базис содержит элемент, зависящий лишь от x_i и x_n, то набор $\{x_i, x_n\}$ зависим, иначе свободен.

3) Подставляя в качестве x_n последовательно все свободные переменные и действуя как в пункте 2), находим все свободные пары переменных. Продолжая в том же духе, мы найдем все свободные тройки, четверки и т.д. до максимальных наборов.

Обоснование этого алгоритма, а также возможные его оптимизации мы оставляем читателю.

Задача 5.20. Доказать, что множество решений конечно $\Longleftrightarrow$ множество решений нульмерно.

Пример 5.21. Вернемся к системе из примера 5.9.

$$\begin{cases} ab = c^2 + c, \\ a^2 + a = bc, \\ ac = b^2 + b. \end{cases}$$

Для порядка $a > b > c$ мы построили базис Гребнера

$$\{f_1 = ab-c^2-c, f_2 = a^2+a-bc, f_3 = ac-b^2-b, f_4 = b^2+b+bc+c^2+c\}.$$

Отсюда следует, что переменная c свободна, а набор $\{b, c\}$ зависим. Положим $b > a > c$. Имеем $f_1 = ab-c^2-c$, $f_2 = bc-a^2-a$, $f_3 = b^2 + b - ac$.

Зацепление f_1 и f_2: $f_1c - f_2a = -c^3 - c^2 + a^3 + a^2 = f_4$.

Получена зависимость между a и $c \Longrightarrow$ набор $\{a, c\}$ не свободен.

Наконец, положим $c > a > b$. Тогда из зацепления второго и третьего уравнений системы получаем многочлен $-a^3 - a^2 + b^3 + b^2$. Следовательно, набор $\{a, b\}$ не свободен.

Вывод. Множество решений имеет размерность 1.

5.5. Геометрическая структура множества решений системы

Пусть максимальный свободный набор переменных для системы S получен. Перенумеровав переменные, можно считать, что этот набор есть $\{x_1, x_2, \ldots, x_k\}$. Имеется проекция $\phi: X(S) \to Ox_1 \ldots x_k$, образ которой мы обозначим U. Множество U плотно в $Ox_1 \ldots x_k \cong \mathbb{C}^k$.

Пусть $u_0 = (x_1^0, \ldots, x_k^0) \in U$. Рассмотрим прообраз $\phi^{-1}(u_0)$. Множество точек в этом прообразе – это множество решений нашей системы при фиксированных значениях свободных переменных $x_1 = x_1^0, \ldots, x_k = x_k^0$.

Хотелось бы думать, что прообраз $\phi^{-1}(u_0)$ конечен. Однако это не всегда так.

Пример 5.22. Рассмотрим уравнение $xyz = 0$. Набор $\{x, y\}$ является максимальным свободным набором переменных. При $x \neq 0$, $y \neq 0$ переменная z находится однозначно: $z = 0$. Однако если $x = 0$ или $y = 0$, то z может принимать любые значения. Поэтому прообраз каждой точки из координатного креста плоскости Oxy есть аффинная прямая.

Задача 5.23. Найти множество U в примере 5.22.

Тем не менее, имеет место следующая теорема.

Теорема 5.24. *Во множестве U найдется такое плотное подмножество U_1, что $\phi^{-1}(u)$ конечно для всякого $u \in U_1$.*

(см. доказательство в Главе 6.)

Так, в примере 5.22 $U_1 = U \setminus \{Ox \cup Oy\}$.

Если значения свободных переменных принадлежат множеству U_1, то значения остальных переменных находятся "почти однозначно". На явные формулы для выражения $x_{k+1}, \ldots, x_n$ через $x_1, \ldots, x_k$ рассчитывать не приходится, но при фиксированных значениях $x_1, \ldots, x_k$ из U_1 значения $x_{k+1}, \ldots, x_n$ можно найти, решая конечное число алгебраических уравнений от одной неизвестной.

Если же значения $(x_1, \ldots, x_k) \in U \setminus U_1$, то происходят вырождения. Здесь следует подставить значения $x_1, \ldots, x_k$ в систему и вновь начать решать полученную систему от неизвестных $x_{k+1}, \ldots, x_n$ рассмотренными методами.

В заключение получим точное решение системы из примера 5.9. Построенный базис Гребнера

$$\{f_1 = ab - c^2 - c, f_2 = a^2 + a - bc, f_3 = ac - b^2 - b,$$

$$f_4 = b^2 + b + bc + c^2 + c\}$$

является минимальным, но не редуцированным. Минимальным редуцированным базисом в этом случае является базис

$$\{f_1 = ab - c^2 - c, f_2 = a^2 + a - bc, f_3 = ac + bc + c^2 + c,$$

$$f_4 = b^2 + b + bc + c^2 + c\}.$$

Поэтому исходная система

$$\begin{cases} ab = c^2 + c, \\ a^2 + a = bc, \\ ac = b^2 + b \end{cases}$$

эквивалентна системе

$$\begin{cases} ab = c^2 + c, \\ a^2 + a = bc, \\ ac = -bc - c^2 - c, \\ b^2 + b + bc + c^2 + c = 0. \end{cases}$$

При $c = 0$ имеем решения $(0, 0, 0)$, $(0, -1, 0)$ и $(-1, 0, 0)$. При $c \neq 0$ из третьего уравнения получаем $a = -b - c - 1$. После подстановки этого выражения в первое и второе уравнения получаем уравнения, эквивалентные четвертому. Переменная c является свободной, переменная b выражается из четвертого уравнения

$$b = \frac{-c - 1 \pm \sqrt{-3c^2 - 2c + 1}}{2},$$

а для переменной a имеем

$$a = \frac{-c - 1 \mp \sqrt{-3c^2 - 2c + 1}}{2}.$$

Окончательно получаем ответ:

1) c – любое комплексное число, $b = \frac{-c-1\pm\sqrt{-3c^2-2c+1}}{2}$ и $a = \frac{-c-1\mp\sqrt{-3c^2-2c+1}}{2}$;

2) $a = b = c = 0$.

Отсюда следует, что $U = U_1 = O_c$, то есть свободная переменная может принимать любые значения, при фиксированном значении $c \neq 0$ система имеет два решения, а при $c = 0$ система имеет три решения.

Замечание. Множество решений уравнения $xyz = 0$ есть объединение трех плоскостей. Ряд приведенных в этой главе примеров был основан именно на том, что множество решений системы есть объединение конечного числа подобных "частей", каждая из которых является решением системы, полученной из исходной добавлением дополнительных уравнений. В алгебраической геометрии эти "части" называют *неприводимыми компонентами* множества решений и предпочитают изучать каждую из компонент отдельно. Подробное изучение понятия неприводимой компоненты выходит за рамки настоящего курса. Заинтересованному читателю следует обратиться к учебникам по алгебраической геометрии, см. например И. Р. Шафаревич, Основы алгебраической геометрии, том 1, М.: Наука, 1988.

5.6. Решение систем

Решите следующие системы (это можно сделать, не применяя понятие базиса Гребнера, однако мы рекомендуем именно этот путь в качестве тренировки). В каждом из случаев продемонстрируйте применение критериев совместности, конечности числа решений и понятие свободной переменной, найдите размерность множества решений.

1)
$$\begin{cases} x^2 = 1, \\ (x-1)y = 0, \\ (x+1)z = 0. \end{cases}$$

2)
$$\begin{cases} x^2 + y^2 + z^2 = 0, \\ x + y - z = 0, \\ y + z^2 = 0. \end{cases}$$

3)
$$\begin{cases} xz - 2y + 1 = 0, \\ yz - 1 + z = 0, \\ yz + xyz + z = 0. \end{cases}$$

4)
$$\begin{cases} x^3yz - xz^2 = 0, \\ xy^2z - xyz = 0, \\ x^2y^2 - z = 0. \end{cases}$$

5)
$$\begin{cases} xy^2 - z - z^2 = 0, \\ x^2y - y = 0, \\ y^2 - z^2 = 0. \end{cases}$$

6)
$$\begin{cases} xy + z - 1 = 0, \\ x - y - z^2 = 0, \\ x^2 - 2y + 1 = 0. \end{cases}$$

7)
$$\begin{cases} zx - y - x + xy = 0, \\ yz - z + x^2 + yx^2 = 0, \\ x - x^2 + y = 0. \end{cases}$$

8)
$$\begin{cases} xy - xz + y^2 = 0, \\ yz - x^2 + x^2y = 0, \\ x - xy + y = 0. \end{cases}$$

9)
$$\begin{cases} yz + x^2 + z = 0, \\ xyz + xz - y^3 = 0, \\ xz + y^2 = 0. \end{cases}$$

10)
$$\begin{cases} x^2 + z^2y + yz = 0, \\ y^2 - zx + x = 0, \\ xy + z^2 - 1 = 0. \end{cases}$$

Глава 6.

Доказательства

6.1. К главе 1

Доказательство теоремы о факториальности кольца многочленов от многих переменных.

Проведем индукцию по числу переменных. Для кольца многочленов от одной переменной факториальность доказана выше. Считаем, что кольцо $\mathbb{K}[x_1, \ldots, x_{n-1}]$ факториально. Рассмотрим многочлен $f(x_1, \ldots, x_n)$ как многочлен от переменной x_n с коэффициентами в кольце $\mathbb{K}[x_1, \ldots, x_{n-1}]$, т.е.

$$f(x_n) = f_0(x_1, \ldots, x_{n-1}) + f_1(x_1, \ldots, x_{n-1})x_n + \ldots$$

$$+f_m(x_1, \ldots, x_{n-1})x_n^m.$$

Определение 6.1. *Содержанием* многочлена f называется многочлен $Cont(f) = \text{НОД}(f_0(x_1, \ldots, x_{n-1}), \ldots, f_m(x_0, \ldots, x_{n-1}))$.

Лемма Гаусса. $Cont(fg) = Cont(f)Cont(g)$.

Доказательство. Ясно, что $Cont(fg)$ делится на $Cont(f)Cont(g)$. Сократив на общий множитель, будем считать, что $Cont(f) = Cont(g) = 1$. Пусть p – неприводимый делитель $Cont(fg)$. Допустим, что p делит $f_0, \ldots, f_s$ и $g_0, \ldots, g_r$, но не делит f_{s+1} и g_{r+1}. Тогда в fg коэффициент при x_n^{s+r+2}

делится на p, все входящие в него члены делятся на p, и потому $f_{s+1}g_{r+1}$ делится на p. В силу неприводимости p один из сомножителей делится на p. Противоречие. ■

Рассмотрим поле рациональных дробей

$$D = \{\frac{f(x_1, \ldots, x_{n-1})}{g(x_1, \ldots, x_{n-1})} \mid g \neq 0\}.$$

Многочлен f можно рассматривать как многочлен от x_n над полем D. Утверждается, что если f неприводим в $\mathbb{K}[x_1, \ldots, x_n]$, то он неприводим и в $D[x_n]$. Действительно, если $f = gh$ – разложение в $D[x_n]$, то, приведя к общему знаменателю коэффициенты, получим $qf = g'h'$, где g', h' – многочлены из $\mathbb{K}[x_1, \ldots, x_n]$ тех же степеней по x_n, что и g, h. Сократив на $Cont(g')Cont(h')$, получим $r'f' = g''h''$. По лемме Гаусса r' есть константа. Поэтому f', а следовательно и f, приводимы в $\mathbb{K}[x_1, \ldots, x_n]$.

Проведенное рассуждение показывет, что разложение на неприводимые множители в $D[x_n]$ определяет разложение на неприводимые множители в $\mathbb{K}[x_1, \ldots, x_n]$. Однозначность разложения вытекает из однозначности разложения в $D[x_n]$ и в $\mathbb{K}[x_1, \ldots, x_{n-1}]$. ■

6.2. К главе 2

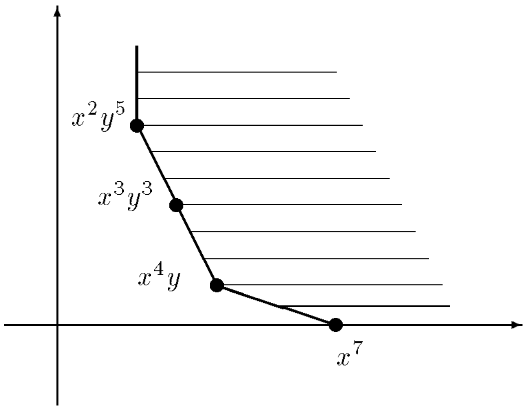
Доказательство теоремы Гильберта о базисе.

Рассмотренное ниже доказательство принадлежит Гордану (1900). Оно было получено почти сразу после оригинального доказательства Гильберта. Для нас оно интересно тем, что в нем (впервые ?) возникло понятие идеала старших членов и идеи, близкие к понятию базиса Гребнера.

Этап 1. Пусть $I \triangleleft \mathbb{K}[x_1, \ldots, x_n]$ – идеал, порожденный (бесконечным) множеством одночленов $m_1, m_2, \ldots$.

Лемма Диксона. *В идеале I можно выбрать базис из конечного числа одночленов $m_1, m_2, \ldots, m_k$. Другими словами,* *любое множество одночленов содержит конечное число минимальных элементов относительно отношения делимости. Эти элементы составляют наименьший мономиальный базис идеала I.*

Доказательство. Будем использовать индукцию по числу переменных. В случае, когда $n = 1$, базис состоит из одного одночлена наименьшей степени. В случае n переменных подставим во все одночлены $x_n = 1$ и в полученной совокупности одночленов от $n - 1$ переменной выберем минимальный базис $m'_1, \ldots, m'_s$. Рассмотрим одночлены $m_1, \ldots, m_s$, отвечающие m'_i, с наименьшими показателями при x_n. Пусть l есть наибольший показатель при x_n в одночленах $m_1, \ldots, m_s$. Рассмотрим все одночлены из I степени p относительно x_n, $p = 0, 1, \ldots, l - 1$. Подставим в них $x_n = 1$ и в полученном множестве выберем вновь минимальные одночлены $m_1^{(p)}, \ldots, m_{s_p}^{(p)}$. В конечном множестве одночленов $m_1, \ldots, m_s, \ldots, m_i^{(p)} x_n^p \ldots$ остается выбрать минимальные элементы относительно отношения делимости. ■



Эта лемма допускает следующую геометрическую интерпретацию. Будем сопоставлять одночлену точку решетки $\mathbb{Z}^n$ – набор степеней одночлена. Тогда одночлены из наименьшего мономиального базиса отвечают точкам, попавшим на конечную часть ломанной – границы выпуклой оболочки всех одночленов идеала.

Этап 2. Общий случай. Рассмотрим лексикографический порядок на множестве одночленов. Пусть J – идеал, порожденный старшими членами f_C элементов f идеала I. Выберем конечный базис $m_1, \ldots, m_k$ в идеале J. Пусть f_i – многочлены из идеала I, старшие члены которых равны m_i. Покажем, что f_i образуют базис в I. Для произвольного элемента $f \in I$ его старший член $f_C = m_i r$ для некоторого номера i и одночлена r. Тогда старший член $f - f_i r$ строго меньше старшего члена f. За конечное число мы получим $f \in (f_1, \ldots, f_k)$. ■

Другое доказательство этой теоремы основано на рассмотрении кольца $\mathbb{K}[x_1, \ldots, x_n]$ как кольца многочленов от x_n с коэфициентами в $\mathbb{K}[x_1, \ldots, x_{n-1}]$. Можно показать, что старшие члены многочленов из идеала I образуют идеал P в $\mathbb{K}[x_1, \ldots, x_{n-1}]$. По предположению индукции P имеет конечный базис. Это позволяет построить конечный базис в I. Детали мы оставляем читателю.

6.3. К главе 3

Доказательство теоремы Гильберта о нулях.

Удачное доказательство этой теоремы содержится в книге В. В. Прасолова "Многочлены". Для полноты изложения мы приведем здесь это доказательство. Помимо собственно доказательства в процессе рассуждений читатель познакомится с такими полезными в алгебре фактами как лемма Нетер о нормализации, характеристическое свойство максимальных идеалов и прочее.

Сначала мы докажем частный случай теоремы о нулях, из которого затем выведем общую теорему. Далее кольцо $\mathbb{C}[x_1, \ldots, x_n]$ будем обозначать буквой K.

Предложение 1. *Пусть многочлены $f_1, \ldots, f_m \in K$ не имеют общих нулей. Тогда существуют такие многочлены $g_1, \ldots, g_m \in K$, что*

$$g_1 f_1 + \ldots + g_m f_m = 1.$$

Доказательство. Предположим, что таких многочленов не существует. Это в точности означает что идеал $(f_1, \ldots, f_m)$ не совпадает со всем кольцом K.

ШАГ 1. Пусть J - максимальный (собственный) идеал кольца K, содержащий $(f_1, \ldots, f_m)$. Тогда кольцо $A = K/J$ является полем.

В самом деле, достаточно проверить, что в кольце K/J любой ненулевой элемент обратим. Если $f \notin J$, то $J + (f)$ – идеал, строго содержащий J, поэтому $J + (f) = K$. Это показывает, что найдутся такие многочлены $a \in J$ и $b \in K$, что $a + bf = 1$. В таком случае класс $\overline{b} \in A$ является обратным для класса $\overline{f} \in A$.

Пусть α_i – образ элемента x_i при канонической проекции

$$p: \ \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]/J = A.$$

Таким образом, $A = \mathbb{C}[\alpha_1, \ldots, \alpha_n]$ – конечно порожденная алгебра над $\mathbb{C}$, являющаяся в то же время полем.

ШАГ 2. Если конечно порожденная алгебра над $\mathbb{C}$ является полем, то она совпадает с $\mathbb{C}$.

Для доказательства этого утверждения нам понадобится[1]

Лемма Нетер о нормализации. *В алгебре $A = \mathbb{C}[\alpha_1, \ldots, \alpha_n]$ можно выбрать алгебраически независимые*

[1]В доказательстве можно было бы обойтись и без леммы Нетер (см. например В. Доценко, Об одном доказательстве теоремы Гильберта о нулях, Мат. Просвещение, третья серия, вып. **6** (2002), 116-118), но мы решили познакомить читателя с этим результатом.

над $\mathbb{C}$ элементы $y_1, \ldots, y_k$ так, что любой элемент $a \in A$ будет целым над $\mathbb{C}[y_1, \ldots, y_k]$, т.е. будет удовлетворять нормированному алгебраическому уравнению над $\mathbb{C}[y_1, \ldots, y_k]$:

$$a^l + b_1 a^{l-1} + \ldots + b_l = 0, \quad \textit{где} \quad b_1, \ldots, b_l \in \mathbb{C}[y_1, \ldots, y_k].$$

Доказательство. Применим индукцию по n. Если элементы $\alpha_1, \ldots, \alpha_n$ алгебраически независимы, то утверждение очевидно. Пусть $f(\alpha_1, \ldots, \alpha_n) = 0$ – алгебраическое соотношение между ними. Если f – многочлен степени m, у которого коэффициент при x_n^m не равен нулю, то

$$\alpha_n^m + b_1 \alpha_n^{m-1} + \ldots + b_m = 0, \qquad b_1, \ldots, b_m \in \mathbb{C}[\alpha_1, \ldots, \alpha_{n-1}].$$

Это показывает, что α_n цел над $\mathbb{C}[\alpha_1, \ldots, \alpha_{n-1}]$. По предположению индукции мы можем выбрать искомые элементы $y_1, \ldots, y_k$ для кольца $\mathbb{C}[\alpha_1, \ldots, \alpha_{n-1}]$. Теперь тот факт, что всякий элемент из $\mathbb{C}[\alpha_1, \ldots, \alpha_n]$ цел над $\mathbb{C}[y_1, \ldots, y_k]$ вытекает из следующих стандартных свойств целых элементов, проверку которых мы оставляем читателю:

(I) если элемент $a \in \mathbb{C}[\alpha_1, \ldots, \alpha_n]$ цел над $\mathbb{C}[\alpha_1, \ldots, \alpha_{n-1}]$, то a цел и над $\mathbb{C}[y_1, \ldots, y_k]$;

(II) если $a_1, a_2 \in \mathbb{C}[\alpha_1, \ldots, \alpha_n]$ целы над $\mathbb{C}[\alpha_1, \ldots, \alpha_{n-1}]$, то элементы $a_1 + a_2$ и $a_1 a_2$ также целы над $\mathbb{C}[\alpha_1, \ldots, \alpha_{n-1}]$.

Если же коэффициент при x_n^m в многочлене f равен нулю, то сделаем замену $x_n = \xi_n$, $x_i = \xi_i + a_i \xi_n$, $i = 1, \ldots, n-1$. Попробуем подобрать числа $a_i \in \mathbb{C}$ так, чтобы у многочлена

$$g(\xi_1, \ldots, \xi_{n-1}, \xi_n) = f(x_1, \ldots, x_n) =$$

$$= f(\xi_1 + a_1 \xi_n, \ldots, \xi_{n-1} + a_{n-1} \xi_n, \xi_n)$$

был ненулевой коэффициент при ξ_n^m. Этот коэффициент равен

$$g_m(0, \ldots, 0, 1) = f_m(a_1, \ldots, a_{n-1}, 1),$$

где f_m и g_m – однородные составляющие старшей степени многочленов f и g. Ясно, что ненулевой однородный многочлен $f_m(x_1, \ldots, x_n)$ не может быть тождественно равен нулю при $x_n = 1$. ■

Вернемся к доказательству того, что поле A совпадает с $\mathbb{C}$. Выберем элементы $y_1, \ldots, y_k$, о которых идет речь в лемме Нетер. Покажем, что в таком случае в алгебре $B = \mathbb{C}[y_1, \ldots, y_k]$ любой ненулевой элемент x обратим. По условию A – поле, поэтому x обратим в A. Кроме того, согласно лемме Нетер элемент x^{-1} удовлетворяет уравнению

$$(x^{-1})^l + b_1(x^{-1})^{l-1} + \ldots + b_l = 0, \quad b_1, \ldots, b_l \in B.$$

Умножив обе части этого уравнения на x^{l-1}, получим

$$x^{-1} = -b_1 - b_2 x - \ldots - b_l x^{l-1} \in B.$$

Но B есть кольцо многочленов над полем $\mathbb{C}$. Обратимыми элементами в нем являются только константы. Поэтому $B = \mathbb{C}$. Любой элемент из A является корнем нормированного многочлена с коэффициентами в B. Следовательно, $A = \mathbb{C}$.

ШАГ 3. Многочлены $f_1, \ldots, f_m$ обращаются в нуль в точке

$$(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n.$$

В самом деле, при канонической проекции

$$p: \ \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]/J = A = \mathbb{C}$$

элементы x_i переходят в α_i, а многочлены $f_1, \ldots, f_m$, принадлежащие идеалу J, переходят в нуль.

Итак, предположив, что $(f_1, \ldots, f_m) \neq \mathbb{C}[x_1, \ldots, x_n]$, мы показали, что у многочленов $f_1, \ldots, f_m$ есть общий корень. Предложение 1 доказано. ■

Докажем теперь теорему Гильберта о нулях: если многочлен $F(x_1, \ldots, x_n)$ обращается в нуль на всех общих решениях уравнений $f_1 = 0, \ldots f_m = 0$, то найдется $s \in \mathbb{N}$, для которого $F^s \in (f_1, \ldots, f_m)$. Для $F = 0$ утверждение очевидно, поэтому будем считать, что $F \neq 0$. Добавим к переменным $x_1, \ldots, x_n$ новую переменную $x_{n+1} = z$ и рассмотрим многочлены $f_1, \ldots, f_m, 1 - zF$. У них нет общих нулей, поэтому

$$1 = h_1 f_1 + \ldots + h_m f_m + h(1 - zF),$$

где $h_1, \ldots, h_m, h$ – некоторые многочлены от переменных $x_1, \ldots, x_n, z$. Положим $z = 1/F$. После приведения к общему знаменателю получим

$$F^s = r_1 f_1 + \ldots + r_m f_m,$$

где $r_1, \ldots, r_m$ – многочлены от $x_1, \ldots, x_n$. Это соотношение имеет требуемый вид. ■

6.4. К главе 4

Доказательство теоремы 4.23.

Будем рассуждать от противного. Пусть при редуцировании многочленов $F_{i,j}$ возникает бесконечно много нередуцируемых многочленов. Рассмотрим идеал, порожденный их старшими членами. По теореме Гильберта о базисе в нем можно выбрать конечный базис из числа образующих. Тогда у любого последующего многочлена старший член делится на старший член одного из "базисных" многочленов и, следовательно, этот многочлен можно редуцировать. Полученной противоречие завершает доказательство. ■

Доказательство теоремы 4.24.

Если $\{f_1, \ldots, f_m\}$ является базисом Гребнера, то каждый многочлен $F_{i,j}$ редуцируется к нулю, поскольку по определению он лежит в идеале I. Следовательно, любое зацепление разрешимо.

Для доказательства обратной импликации уточним используемые обозначения. Пусть $f = ax^\alpha + \ldots$ и $g = bx^\beta + \ldots$, где $ax^\alpha = ax_1^{\alpha_1} \ldots x_n^{\alpha_n}$ есть старший член многочлена f и $bx^\beta =$

$bx_1^{\beta_1}\dots x_n^{\beta_n}$ есть старший член многочлена g. Обозначим через x^γ наименьшее общее кратное одночленов x^α и x^β. Напомним, что $S(f,g)=\frac{x^\gamma}{ax^\alpha}f-\frac{x^\gamma}{bx^\beta}g$ (эти обозначения здесь удобнее чем индексные обозначения $F_{i,j}$). Доказательство будет использовать следующую лемму.

Лемма 1. *Пусть $f_1,\dots,f_s$ – многочлены с одним и тем же старшим членом x^α. Тогда если старший член многочлена $f=\sum\lambda_i f_i$ строго меньше чем x^α, то $f=\sum_{i<j}\nu_{i,j}S(f_i,f_j)$ (здесь λ_i и $\nu_{i,j}$ – числа).*

Доказательство. По условию $f_i=a_ix^\alpha+\dots$ и $f_j=a_jx^\alpha+\dots$, поэтому $S(f_i,f_j)=\frac{f_i}{a_i}-\frac{f_j}{a_j}$. Ясно также, что

$$f=\sum\lambda_i f_i=\lambda_1a_1\left(\frac{f_1}{a_1}-\frac{f_2}{a_2}\right)+(\lambda_1a_1+\lambda_2a_2)\left(\frac{f_2}{a_2}-\frac{f_3}{a_3}\right)+\dots$$

$$\dots+(\lambda_1a_1+\dots+\lambda_{s-1}a_{s-1})\left(\frac{f_{s-1}}{a_{s-1}}-\frac{f_s}{a_s}\right)+(\lambda_1a_1+\dots+\lambda_sa_s)\frac{f_s}{a_s}.$$

Однако по условию $\lambda_1a_1+\dots+\lambda_sa_s=0$. ■

Вернемся к доказательству теоремы. Нам достаточно показать, что любой многочлен $f\in I$ представим в виде $f=\sum h_if_i$, где старший член f совпадает с наибольшим из старших членов многочленов h_if_i. Будем рассуждать от противного. Пусть $f=\sum h_if_i$ – запись f, для которой наибольший из старших членов многочленов h_if_i является наименьшим возможным, однако этот старший член все равно больше старшего члена многочлена f. Перепишем данное представление как $f=\sum_{i=1}^t(h_{iC}f_i+h_{iM}f_i)+\sum_{i=t+1}^m h_if_i$, где многочлены $h_{iC}f_i$, $i=1,\dots,t$ – это в точности члены представления, старший член которых является наибольшим. По предположению старшие члены в сумме $F=\sum_{i=1}^t h_{iC}f_i$ взаимно уничтожаются. По лемме 1 имеем представление $F=\sum_{i<j}\nu_{i,j}S(h_{iC}f_i,h_{jC}f_j)$. Однако h_{iC} – одночлены, поэтому $S(h_{iC}f_i,h_{jC}f_j)$ делится на $S(f_i,f_j)$. Редуцируемость к нулю многочленов $S(f_i,f_j)$ с помощью набора $\{f_i\}$ обеспечивает нам представление каждого из $S(f_i,f_j)$ в виде комбинации $\sum g_lf_l$, для которых старший член

многочлена $S(f_i, f_j)$ совпадает с наибольшим из старших членов многочленов $g_l f_l$. Подставляя полученные комбинации в выражения для F и f, получим представление f в виде комбинации $\sum d_s f_s$, у которой наибольший из старших членов многочленов $d_s f_s$ меньше, чем у исходной комбинации. Требуемое противоречие получено.

Остается объяснить, почему не нужно рассматривать S-многочлены для тех пар f_i, f_j, которые не имеют зацепления. Мы докажем, что если старшие члены многочленов f и g взаимно просты, то $S(f, g)$ редуцируется к нулю при помощи многочленов f и g. Для этого достаточно доказать, что f и g образуют базис Гребнера идеала (f, g), или что старший член любого многочлена вида $fu+gv$ делится либо на старший член f_C, либо на старший член g_C. Предположим противное в последнем утверждении. Пусть $F = fu + gv$ – многочлен, старший член которого не делится ни на f_C, ни на g_C. Можно считать, что в этой записи старший член многочлена u минимален по всем таким представлениям многочлена F. По предположению старшие члены многочленов fu и gv сокращаются, откуда $u_C = wg_C$, а $v_C = -wf_C$ для некоторого одночлена w. Но тогда $F = f(gw + u_1) + g(-wf + v_1) = fu_1 + gv_1$, и старший член u_1 меньше старшего члена u. Противоречие. ∎

Доказательство теоремы 4.29.

ШАГ 1. Пусть $f_1, \ldots, f_s$ и $g_1, \ldots, g_t$ – два минимальных базиса Гребнера идеала I. Мы покажем, что $s = t$ и (возможно после перестановки многочленов) старшие члены f_i и g_i совпадают для всех i (мы предполагаем, что все многочлены нормированы, т.е. имеют коэффициент 1 при старшем члене). По определению базиса Гребнера, старший член многочлена f_1 делится на старший член некоторого из g_i (можно считать, что на старший член многочлена g_1). С другой стороны, старший член g_1 делится на старший член некоторого f_j. В силу минимальности базиса $f_1, \ldots, f_s$ получаем $j = 1$. Отсюда следует, что старшие члены f_1 и g_1 совпадают. Далее, старший член f_2 делится на старший член g_k, причем $k \neq 1$, т.к. иначе старший член f_2 делился бы на старший член f_1, что противоречило бы минимальности базиса $f_1, \ldots, f_s$. Можно считать, что $k = 2$ и мы получаем как и выше, что старшие члены f_2 и g_2 совпадают. Продолжая этот процесс, несложно заметить, что многочлены f_i и g_j должны исчерпаться одновременно, откуда $s = t$.

ШАГ 2. Пусть базисы $f_1, \ldots, f_s$ и $g_1, \ldots, g_s$ дополнительно являются редуцированными. Предположим, что $f_i - g_i \neq 0$ для некоторого i. Тогда старший член многочлена $f_i - g_i \in I$ делится на старший член одного из g_j. С другой стороны, старший член $f_i - g_i$ является нестаршим членом одного из многочленов f_i или g_i. Заметим, что старшие члены g_j и f_j совпадают. Получено противоречие с редуцированностью базисов. ■

6.5. К главе 5

Доказательство теоремы 5.14.

После перенумерации можно обозначить переменные $x_{i_1}, \ldots, x_{i_k}$ просто $x_1, \ldots, x_k$. Рассмотрим естественную проекцию π подалгебры $A = \mathbb{C}[x_1, \ldots, x_k]$ алгебры $\mathbb{C}[x_1, \ldots, x_n]$ на факторалгебру $B = \mathbb{C}[x_1, \ldots, x_n]/I(S)$. Если отображение π не является инъективным, то найдется многочлен $F(x_1, \ldots, x_k)$, лежащий в идеале системы. Это означает, что образ координатной проекции лежит в гиперповерхности H_F.

Предположим, что отображение π является вложением и докажем, что образ координатной проекции в этом случае плотен. Мы будем отождествлять алгебру A с ее образом $\pi(A)$ и рассматривать A как подалгебру в B. Нам потребуется следующее утверждение, заимствованное из книги Э. Б. Винберга и А. Л. Онищика "Семинар по группам Ли и алгебраическим группам", М. Наука, 1988, стр. 72.

Предложение 1. *Пусть B – алгебра без делителей нуля, конечно порожденная над своей подалгеброй A. Тогда для любого элемента $b \in B$, $b \neq 0$ найдется такой элемент*

$a \in A$, $a \neq 0$, что всякий гомоморфизм $\phi : A \to \mathbb{C}$, не аннулирующий a, продолжается до гомоморфизма $\psi : B \to \mathbb{C}$, не аннулирующего b.

Доказательство. ШАГ 1. Пусть $B = A[u]$, где элемент u не удовлетворяет никакому уравнению над A (т.е. является трансцендентным над A). Для любого многочлена $f \in A[x]$ обозначим через f^ϕ многочлен из $\mathbb{C}[x]$, полученный из f применением гомоморфизма ϕ ко всем коэффициентам. Пусть $b = g(u)$. Возьмем в качестве a любой ненулевой коэффициент многочлена g. Тогда $g^\phi \neq 0$. Пусть $\alpha \in \mathbb{C}$ – любое число, не являющееся корнем многочлена g^ϕ. Определим гомоморфизм ψ формулой $\psi(f(u)) = f^\phi(\alpha)$. Тогда $\psi(b) \neq 0$.

ШАГ 2. Предположим, что $B = A[u]$ и элемент u является алгебраическим над A. Пусть $p \in A[x]$ – минимальный многочлен элемента u и a_1 – старший коэффициент этого многочлена. Если $q \in A[x]$ – такой многочлен, что $q(u) = 0$, то существует такое k, что $a_1^k q$ делится на p в $A[x]$. Поэтому, если $\phi(a_1) \neq 0$ и $\alpha \in \mathbb{C}$ – любой корень многочлена p^ϕ, то формула $\psi(f(u)) = f^\phi(\alpha)$ корректно определяет гомоморфизм $\psi : B \to \mathbb{C}$, совпадающий с ϕ на A.

Любой элемент $b \in B$ алгебраичен над A. Пусть $h \in A[x]$ – такой ненулевой многочлен, что $h(b) = 0$. Можно считать, что свободный член a_2 многочлена h отличен от нуля. Если $\psi(b) = \beta$, то $h^\phi(\beta) = 0$. Пусть $\phi(a_2) \neq 0$. Тогда и $\beta \neq 0$. Остается положить $a = a_1 a_2$.

ШАГ 3. Индукция по числу образующих алгебры B над A сводит доказательство к последовательному применению шагов 1 и 2. ■

Вернемся к доказательству теоремы 5.14. Точки на множестве решений $X(S)$ определяются значениями переменных x_i, для которых обнуляются все многочлены из идеала системы. Это позволяет установить биекцию между точками из $X(S)$ и гомоморфизмами алгебры $B = \mathbb{C}[x_1, \ldots, x_n]/I(S)$ в поле $\mathbb{C}$ (значения переменных отвечают образам этих переменных при соответствующем гомоморфизме).

Предположим, что алгебра B не имеет делителей нуля. По только что доказанному найдется такой элемент a алгебры $A = \pi(\mathbb{C}[x_1, \ldots, x_k])$, что каждый гомоморфизм $A \to \mathbb{C}$, не обнуляющий a, продолжится до гомоморфизма $B \to \mathbb{C}$ (здесь мы положили $b = 1$). Это означает, что каждая точка на координатном подпространстве $Ox_1 \ldots x_k$, в которой не обращается в нуль многочлен a, является образом некоторой точки из $X(S)$ при координатной проекции.

Рассмотрим случай, когда алгебра B имеет делители нуля. Мы покажем, что этот случай сводится к предыдущему. Пусть $b_1 \neq 0$, $b_2 \neq 0$, но $b_1 b_2 = 0$. Тогда хотя бы одно из отображений $\pi_i : A \to B/(b_i)$, $i = 1, 2$ инъективно. В самом деле, если $\pi_i(c_i) = 0$, то $\pi(c_1 c_2) = 0$, что противоречит инъективности π, поскольку в A делителей нуля нет. Далее мы можем рассматривать в качестве B соответствующую B_i и доказывать, что для отвечающего ей множества решений образ координатной проекции плотен в $Ox_1 \ldots x_k$ (тем более будет плотен образ $X(S)$). Если в B_i есть делители нуля b_3 и b_4, поступаем аналогично и т. д. В результате мы получим идеал в B, порожденный элементами $b_i, b_j, \ldots$. По теореме Гильберта о базисе такой идеал порождается конечным числом своих базисных элементов. Следовательно, за конечное число шагов мы получим алгебру B', в которую вкладывается A и которая не содержит делителей нуля. ■

Доказательство теоремы 5.24.

В силу максимальности свободного набора $\{x_1, \ldots, x_k\}$ для любого $j > k$ значения переменных $\{x_1, \ldots, x_k, x_j\}$ на множестве решений связаны соотношением $F_j(x_1, \ldots, x_k, x_j) = 0$. Пусть $h_j(x_1, \ldots, x_k)$ – коэффициент при старшем члене по переменной x_j. Если при значениях $x_1 = x_1^0, \ldots, x_k = x_k^0$ значение $h_j(x_1^0, \ldots, x_k^0)$ отлично от нуля, то переменная x_j может принимать лишь конечное число значений на соответствующем прообразе $\phi^{-1}(u_0)$. Поэтому для всех точек множества U, в которых многочлен $h_{k+1}(x_1, \ldots, x_k) h_{k+2}(x_1, \ldots, x_k) \ldots h_n(x_1, \ldots, x_k)$ отличен от нуля, прообраз $\phi^{-1}(u_0)$ конечен. ■

Глава 7.

Добавление. Универсальный базис Гребнера

В этом курсе мы практически не рассматривали вопрос о различных упорядочениях на множестве одночленов, остановившись для простоты на лексикографическом порядке. В этой главе мы немного поговорим о понятии порядка на множестве одночленов в полной общности, а также посмотрим, какие изменения такое обобщение вносит в теорию базисов Гребнера.

Рассмотрим произвольное поле $\mathbb{K}$ и кольцо многочленов $\mathbb{K}[x_1, \ldots, x_n]$. Предположим, что на множестве одночленов $\{x^a = x_1^{a_1} \ldots x_n^{a_n}\}$ введен полный порядок $\prec$, для которого выполнены свойства:

1) единица $1 = x^0$ есть (единственный) минимальный элемент этого порядка;

2) если $x^a \prec x^b$, то для любого x^c имеем $x^a x^c \prec x^b x^c$.

Всюду далее слово "порядок" будет означать полный порядок на множестве одночленов со свойствами 1),2). Порядок позволяет корректно определить старший член у любого многочлена.

Задача 7.1. Доказать в этой ситуации справедливость леммы о старшем члене.

Пример 7.2. Пусть $\omega_1, \ldots, \omega_n$ – набор положительных действительных чисел, линейно независимых над полем рациональных чисел. Будем считать, что одночлен $x^a = x_1^{a_1} \ldots x_n^{a_n}$ больше одночлена $x^b = x_1^{b_1} \ldots x_n^{b_n}$ если $a_1\omega_1 + \ldots + a_n\omega_n > b_1\omega_1 + \ldots + b_n\omega_n$. Нетрудно проверить, что тем самым определен порядок (зачем нужны положительность и линейная независимость чисел ω_i ?). Мы получили достаточно богатый запас порядков. В то же время, лексикографический порядок нельзя определить подобным способом (почему ?).

Задача 7.3. 1) Описать все возможные порядки на множестве одночленов от одной переменной;

2) Доказать, что при $n > 1$ число различных порядков бесконечно.

Задача* 7.4. Доказать, что для любого порядка $\prec$ не существует бесконечной цепочки одночленов $x^{a_1} \succ x^{a_2} \succ x^{a_3} \succ \ldots$.

После того, как старший член определен, определение базиса Гребнера дословно переносится на порядок $\prec$. Заметим, что базис Гребнера, построенный по некоему порядку $\prec$, может очень сильно отличаться от базиса Гребнера, построенного по лексикографическому порядку. Проблема выбора для данного идеала того порядка, для которого базис Гребнера будет иметь максимально простой и удобный вид, активно исследуется в настоящее время. Читателю, желающему попробовать здесь свои силы, рекомендуем ознакомиться с литературой по базисам Гребнера, приведенной в конце курса. Сейчас же мы, следуя книге [8], докажем весьма неожиданный результат – для любого идеала $I \lhd \mathbb{K}[x_1, \ldots, x_n]$ найдется конечный универсальный базис Гребнера, т.е. базис, который подходит для всех возможных порядков.

Определение 7.5. Базис $f_1, \ldots, f_M$ идеала I называется *универсальным* базисом Гребнера, если он является базисом Гребнера идеала I для любого возможного порядка $\prec$ на множестве одночленов.

Теорема 7.6. *Любой идеал $I \lhd \mathbb{K}[x_1, \ldots, x_n]$ обладает конечным универсальным базисом Гребнера.*

Доказательство. С каждым порядком $\prec$ мы свяжем (мономиальный) идеал $I(\prec)$ – это идеал, порожденный старшими членами многочленов из идеала I относительно порядка $\prec$. Заметим, что базис Гребнера идеала I относительно порядка $\prec$ однозначно определяется идеалом $I(\prec)$ – достаточно найти базис идеала $I(\prec)$ из одночленов и в качестве базиса Гребнера в I взять многочлены из I, старшие члены которых образуют упомянутый базис в $I(\prec)$. (С другой стороны, для различных порядков $\prec_1$ и $\prec_2$ идеалы $I(\prec_1)$ и $I(\prec_2)$ могут совпадать – приведите пример !) Если мы докажем, что среди идеалов $I(\prec)$ по всем порядкам $\prec$ имеется лишь конечное число различных, то для получения (конечного) универсального базиса Гребнера нам будет достаточно объединить базисы Гребнера, отвечающие этому конечному набору мономиальных идеалов.

Будем рассуждать от противного. Пусть число идеалов вида $I(\prec)$ бесконечно. Рассмотрим многочлен $f_1 \in I$. Число членов в нем конечно, поэтому найдется такой член m_1 этого многочлена, который содержится в бесконечном множестве A_1 различных идеалов типа $I(\prec)$.

Лемма 7.7. *Найдется многочлен $f_2 \in I$, ни один член которого не делится на m_1.*

Доказательство. Поскольку m_1 лежит в бесконечном числе идеалов вида $I(\prec)$, мы можем выбрать из них идеал $I(\prec_1)$, который не совпадает с (m_1). Будем называть одночлены, не попавшие в идеал $I(\prec_1)$, *нормальными* одночленами относительно порядка $\prec_1$. Докажем, что любой многочлен $F \in \mathbb{K}[x_1, \ldots, x_n]$ допускает ровно одну запись вида $F = F_1 + F_2$, где F_1 – линейная комбинация нормальных одночленов, а многочлен F_2 лежит в I. В самом деле, если среди членов многочлена F есть принадлежащие к идеалу $I(\prec_1)$, к таким членам можно применить редукцию. Задача 7.4 показывает, что после конечного числа редукций многочлен F можно будет заменить линейной комбинацией нормальных одночленов. Это показывает, что нужная запись существует. Для доказательства единственности достаточно рассмотреть случай $F_1 + F_2 = 0$, или $F_1 = -F_2$, что означает, что $F_1 \in I$. В этом случае старший член многочлена F_1 относительно порядка $\prec_1$ лежит в идеале $I(\prec_1)$, что приводит к противоречию с нормальностью всех членов F_1.

Пусть r – одночлен, лежащий в $I(\prec_1)$ и не делящийся на m_1. Рассмотрим для него полученную запись $r = F_1 + F_2$. Остается положить $f_2 = r - F_1$ (все члены F_1 нормальны и потому не делятся на m_1). ■

Пусть f_2 – многочлен, построенный в предыдущей лемме. Тогда мы вновь замечаем, что любой идеал вида $I(\prec)$ содержит один из его членов и потому найдется бесконечное множество идеалов A_2 из числа идеалов из A_1, которые содержат некоторый член m_2 многочлена f_2. Пусть $I(\prec_2)$ – один из этих идеалов, не совпадающий с (m_1, m_2). Повторяя рассуждения из доказательства леммы 7.7, мы найдем многочлен $f_3 \in I$, ни один из членов которого не лежит в идеале (m_1, m_2). В этом многочлене мы опять находим член m_3, который лежит в бесконечно многих идеалах типа $I(\prec)$ из множества A_2 и т.д. Окончательно мы получим бесконечную цепочку попарно различных идеалов

$$(m_1) \subset (m_1, m_2) \subset (m_1, m_2, m_3) \subset \ldots$$

Это противоречит теореме Гильберта о базисе. ■

Задача 7.8. Пусть $f \in \mathbb{K}[x_1, \ldots, x_n]$. Найти универсальный базис Гребнера главного идеала (f).

Несколько интересных примеров вычислений универсального базиса Гребнера, а также общий алгоритм его нахождения можно найти в главах 1 и 3 книги [8].

Глава 8.

Указания и ответы к задачам

8.1. К главе 1

1.6. Первая система: $x = \pm i\sqrt{1+y^2},\ y \in \mathbb{C}$ (бесконечно много решений). Вторая система несовместна.

1.10.

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ 2x_1 + x_2 + x_3 = 2 \end{cases}$$

1.11. $(x_3, x_4, x_5),\ (x_1, x_4, x_5),\ (x_1, x_3, x_5),\ (x_1, x_3, x_4)$ – 4 способа.

1.14. 1) Проверьте, что множество U решений однородной системы

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0, \\ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{cases} \tag{1}$$

является подпространством в $\mathbb{R}^n$.

2) Докажите, что каждое решение системы

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases} \tag{2}$$

есть сумма некоторого фиксированного решения a этой системы и решения $u \in U$ соответствующей однородной системы. Тем самым множество решений есть линейное мноообразие.

3) Обратно, по каждому подпространству U построим однородную систему, множеством решений которой является U. Коэффициенты уравнений этой системы суть базисные вектора ортогонального дополнения к U в $\mathbb{R}^n$. Подставим в эту однородную систему вектор a и найдем столбец свободных членов искомой системы.

1.17. $q(x) = 0,\ r(x) = x^2 - x + 1.$

1.18. Нет. Нельзя разделить с остатком x на $2x$.

1.22. Воспользоваться теоремой Безу и индукцией по степени многочлена.

1.23. Нет. Следующие многочлены не имеют корней:
1) $x^2 + 1$ над $\mathbb{Q}$;
2) $x^p - x + \overline{1}$ над $\mathbb{Z}_p$ (малая теорема Ферма);
3) $x^2 - t$ над $\mathbb{C}(t)$ (каковы степени числителя и знаменателя у возможного корня ?).

1.25. Пусть $\mathbb{K}$ алгебраически незамкнуто. Тогда имеется многочлен $a_m x^m + \ldots + a_1 x + a_0$, не имеющий корней. Уравнение $F(x,y) = a_m x^m + a_{m-1}x^{m-1}y + \ldots + a_1 x y^{m-1} + a_0 y^m = 0$ имеет единственное решение $(0,0)$. Система

$$\begin{cases} P_1 = 0 \\ P_2 = 0 \end{cases}$$

эквивалентна уравнению $F(P_1(x_1,\ldots,x_n), P_2(x_1,\ldots,x_n)) = 0$. Далее проводим индукцию по числу уравнений системы.

1.27. а) $(x^2-2)(x^3-2)$;

б) $\begin{cases} (x^2-2)(x^3-2)(y^2+1)=0 \\ (y-1)(y^2+1)=0 \end{cases}$

или $(x^2-2)^2(x^3-2)^2+y^2=0$.

8.2. К главе 2

2.5. Воспользоваться предыдущей задачей.

2.13. Воспользоваться леммой о линейном представлении НОД.

2.15. Если f_1 делится на f_2, а f_2 на f_1, то степени этих многочленов совпадают и они отличаются на ненулевую константу.

2.17. $x(x-1)(x-2)$.

2.18. Рассмотреть идеал, порожденный 2 и x.

2.19. 1) $x^{17}, x^{16}y, \ldots, y^{17}$;
2) y, x^2.

2.20. $x-y, x-z, x-t$. В самом деле, $f(x,y,z,t)-f(x,x,z,t) = (x-y)f_1(x,y,z,t)$. Поэтому

$$f(x,y,z,t) = (x-y)f_1(x,y,z,t) + (x-z)f_2(x,z,t) +$$

$$+(x-t)f_3(x,t) + f(x,x,x,x).$$

Где в рассуждениях существенно, что поле $\mathbb{K}$ бесконечно ?

2.21. Подходят базисы типа $\{z,y,x\}$, $\{x+y+z, y+z, z\}$, $\{x+y^2-z^4, -y+5z^7, 2z\}$, $\{x-2x^3+y-2y^2+z, z+y-2y^2-2x^2, z-2y^2+x^3\}$.

2.22. Рассмотреть идеал, порожденный множеством M, и показать, что конечный базис в нем можно выбрать из элементов M.

2.23. Можно рассмотреть кольцо $\mathbb{K}[x_1, x_2, \ldots]$ от счетного числа переменных и в качестве I взять идеал $(x_1, x_2, \ldots)$, состоящий из многочленов с нулевым свободным членом. Здесь существенно что каждый многочлен зависит лишь от конечного числа переменных. Можно также в качестве R взять множество последовательностей $(a_1, a_2, \ldots)$, $a_i \in \mathbb{K}$ с покоординатным сложением и умножением, а в качестве I – множество последовательностей, у которых лишь конечное число членов отлично от нуля.

2.28. б) $(x+1)(x^2+x+1)=0$.

2.30. $S_1 : x^2y=0$, $S_2 : xy^2=0$.

8.3. К главе 3

3.2. $(x-1)(x-4)(x-7)=0$, $(x-1)(x-4)(y-8)=0, \ldots,$ $(z-3)(z-6)(z-9)=0$ (всего 27 уравнений). На самом деле данные три точки можно задать и тремя уравнениями, например $x+1=y=z-1, (x-1)(x-4)(x-7)=0$, однако первый способ представляется более универсальным.

3.3. е) Множество корней ненулевого многочлена от одной переменной конечно;

ж) Рассмотреть пересечение данного множества с осью Ox и воспользоваться предыдущим пунктом.

3.4. а) Следует объединить уравнения системы, задающие многообразия.

б) Если одно многообразие задано системой $f_i=0$, а другое системой $g_j=0$, то система $f_ig_j=0$ задает объединение многообразий.

3.7. а) $((x-2)(x-3)(x-4)(x-5))$.
б) $(x-y, x-z)$.
в) (x^4-y^2).
г) $(x-y)$.

3.8. а) Положим степень одночлена $x^iy^jz^k$ равной $3i+4j+5k$. Ясно, что степень произведения одночленов равна сумме их степеней. Произвольный многочлен f можно представить в виде $f = f_0+f_1+\ldots+f_N$, где f_l – сумма всех одночленов степени l. Проверьте, что если $f \in J(X)$, то и $f_l \in J(X)$ для любого l (это свойство идеала называется *однородностью*). Для этого покажите, что $f_l(1,1,1) = 0$. Проверьте также, что элементы наименьшей степени в идеале $J(X)$ – это $a = y^2 - xz$ (степени 8), $b = x^3 - yz$ (степени 9) и $c = z^2 - x^2y$ (степени 10). Предположим, что идеал $J(X)$ порожден элементами g и h. Обозначим через g' и h' компоненты многочленов g и h степени ≤ 10. Тогда a, b и c должны выражаться через g' и h' с числовыми коэффициентами (сравните степени !). Это противоречит линейной независимости многочленов a, b и c.

б) Подходит система $x^4 = y^3$, $x^5 = z^3$, $y^5 = z^4$. В самом деле, если $x = 0$, то $y = z = 0$, иначе положим $t = \frac{y}{x}$. Тогда

$$t^3 = \frac{y^3}{x^3} = x,\ t^4 = \frac{y^4}{x^4} = y,\ t^5 = \frac{y^5}{x^5} = \frac{y^5}{z^3} = z.$$

3.13. а) (x), б) (x, y), в) (x, y), г) $(x^2 + y^2 + z^2)$ (см. следующую задачу).

3.14. Если $I = (f)$ и $f = f_1^{k_1} \ldots f_s^{k_s}$ – разложение на неприводимые множители, то $r(I) = (f_1 \ldots f_s)$ (воспользоваться теоремой о факториальности кольца многочленов).

3.15. 1) Рассмотреть идеал $(x^2 + 1)$.

2) По теореме Гильберта о нулях $f^s = h_1 f_1+\ldots+h_m f_m$ для некоторых многочленов h_j с комплексными коэффициентами. Пусть $h_j = r_j + iq_j$, где r_j и q_j – многочлены с вещественными коэффициентами. Тогда $f^s = r_1 f_1 + \ldots + r_m f_m$.

3.18. Если $f^k \in r(I)$, то существует такое s, что $(f^k)^s \in I$. Отсюда $f \in r(I)$.

3.20. Уравнения $1 = 0$ и $x^2 = -1$ не пропорциональны.

3.21. Если $r(I(S)) = (f)$, то система эквивалента уравнению $f = 0$. Обратно, если система эквивалентна уравнению $f = 0$, то идеал $r((f))$ является главным (задача 3.14). Идеал системы в этой ситуации главным быть не обязан: рассмотрите систему $x^2y = 0$, $xy^2 = 0$.

3.22. Здесь идеал (x, y) является радикальным.

8.4. К главе 4

4.3. а) Вообще говоря нет: набор вида $(0, k)$ меньше набора $(1, 0)$. Опишите все наборы w, для которых число наборов, меньших w, конечно.

б) Воспользоваться индукцией по n.

4.5. а) (4,3);

б) Отрезок (или точку);

в) Вершины $(0, 0, 0)$, $(4, 0, 0)$, $(0, 4, 0)$, $(0, 0, 4)$, $(3, 3, 0)$, 8 ребер, 5 граней.

4.11. После подстановки $y = 0$ многочлен не делится на x^2.

4.15. Воспользоваться задачей 4.3 б).

4.20. Редукция многочлена $\widetilde{F}_{i,j}$ при помощи f_{m+1} равна нулю.

4.25. В точности тогда, когда среди f_i есть многочлен, который делит все остальные.

4.26. Воспользоваться задачей 4.16.

4.32. Построим базисы Гребнера в обеих идеалах, затем построим минимальные редуцированные базисы Гребнера. Остается проверить их совпадение. Можно также решать задачу вхождения во второй идеал для $f_1, \ldots, f_k$ и обратно.

Вычисление базисов Гребнера.

1) $x^2 - 1$, $(x-1)y$, $(x+1)z$, yz;

2) $x^2 - 1$, $(x-1)y$, $(x-1)z$;

3) $xy^2z - xyz$, $x^2y^2 - z$, $x^2yz - z^2$, $yz^2 - z^2$, $x^2z^2 - z^3$;

4) $x^2y + xz + y^2z$, $xz^2 - zy$, $xyz - y^2$, $y^3 + y^2z^3 + yz^2$, $xy^2 + y^2z^2 + zy$;

5) $x^2y - y,\ 2y^2 + z,\ 2z^2 + z,\ xz + z$;

6) $xz + yz^3,\ xy + yz^3,\ yz^4 - yz,\ y^2z - yz^2$.

8.5. К главе 5

5.3. 1) Пусть $f^p \in I$. Тогда $1 = (1 - yf)(1 + yf + \ldots + y^{p-1}f^{p-1}) + f^py^p$. Обратно, если $(f_1, \ldots, f_m, 1 - yf)$ совпадает со всем кольцом, то многочлен f обращается в нуль на множестве общих нулей многочленов $f_1, \ldots, f_m$ не только над полем $\mathbb{K}$, но и над любым полем, содержащим $\mathbb{K}$ (рассмотрите представление $1 = f_1h_1 + \ldots + f_mh_m + (1 - yf)h$). По теореме Гильберта о нулях, примененной к алгебраически замкнутому полю[1], содержащему поле $\mathbb{K}$ (известно, что такое найдется для любого $\mathbb{K}$), f лежит в радикале идеала $(f_1, \ldots, f_m)$. Последнее не зависит от того, рассматриваются многочлены $f_1, \ldots, f_m, f$ над полем $\mathbb{K}$ или каким-либо его расширением.

2) Многочлен f принадлежит радикалу идеала $(f_1, \ldots, f_m)$ тогда и только тогда, когда в базисе Гребнера идеала $(f_1, \ldots, f_m, 1 - yf)$ содержится ненулевая константа.

5.5. После линейной замены переменных можно считать, что $l = x_n$. Тогда нужно найти элемент x_n^s в минимальном базисе Гребнера для лексикографического порядка $x_1 > \ldots > x_n$ или убедиться, что такого элемента там нет.

5.13. а) Это в точности дополнения до конечных подмножеств;

б) Дополнения до алгебраических кривых; дополнения до конечных подмножеств.

5.16. Можно считать, что переменная x_1 входит в многочлен F. Покажем, что набор $\{x_2, \ldots, x_n\}$ является свободным. Если значения переменных $x_2, \ldots, x_n$ на множестве решений лежат на гиперповерхности $H(x_2, \ldots, x_n) = 0$, то по теореме

[1] Заметим, что в доказательстве теоремы Гильберта о нулях использовалось лишь одно свойство поля комплексных чисел – его алгебраическая замкнутость.

Гильберта о нулях для некоторого $s \in \mathbb{N}$ многочлен H^s делится на F – противоречие.

5.17. Вытекает из теоремы 5.14 и задачи 5.13, 1).

5.18. Если поднабор зависим, переменные из этого поднабора связаны алгебраическим уравнением, что противоречит свободности набора.

5.19. Для системы $xy = 0$, $xz = 0$ набор $\{y, z\}$ является единственным максимальным свободным набором, поэтому свободный набор $\{x\}$ нельзя включить в максимальный.

5.20. Эти условия эквивалентны тому, что каждая переменная принимает на множестве решений лишь конечное число значений.

5.23. Взяв в качестве максимального свободного набора набор $\{x, y\}$, получим $U = Oxy$.

Решение систем.

1) $x = 1$, $y \in \mathbb{C}$, $z = 0$ или $x = -1$, $y = 0$, $z \in \mathbb{C}$.

Базис Гребнера при $x > y > z : x^2 - 1,\ xy - y,\ xz + z,\ yz$.

2) $x = y = z = 0$ или $x = -1$, $y = \frac{1 \pm i\sqrt{3}}{2}$, $z = \frac{-1 \pm i\sqrt{3}}{2}$.

Базис Гребнера при $x > y > z : x - z^2 - z,\ y + z^2,\ z^2 + z^3 + z^4$.

3) $x = \frac{-3 \pm i\sqrt{7}}{2}$, $y = \frac{1 \pm i\sqrt{7}}{4}$, $z = \frac{5 \mp i\sqrt{7}}{8}$.

Базис Гребнера при $x > y > z : x + 4z - 1,\ -3 + 4z + 2y,\ 4z^2 - 5z + 2$.

4) $x = 0$, $y \in \mathbb{C}$, $z = 0$;
$x \in \mathbb{C}$, $y = 0$, $z = 0$;
$x \in \mathbb{C}$, $y = 1$, $z = x^2$.
Базис Гребнера при $x > y > z : x^2y^2 - z,\ x^2yz - z^2,\ -z^3 + x^2z^2,\ xy^2z - xyz,\ -z^2 + z^2y$.

5) $x \in \mathbb{C}$, $y = 0$, $z = 0$ или $x = -1$, $y = \pm\frac{1}{2}$, $z = -\frac{1}{2}$.

Базис Гребнера при $x > y > z$: $x^2y - y$, $xz + z$, $2y^2 + z$, $2z^2 + z$.

6) $x = 1$, $y = 1$, $z = 0$;
$x = -1 \pm i\sqrt{2}$, $y = \mp i\sqrt{2}$, $z = -1 \mp i\sqrt{2}$;
$x = \pm\, i\sqrt{2}$, $y = -\frac{1}{2}$, $z = 1 \pm \frac{i\sqrt{2}}{2}$.

Базис Гребнера при $y > z > x$: $-x^2 + 2y - 1$, $2z - 2 + x^3 + x$, $(x^2 + 2x + 3)(x^2 + 2)(x - 1)^2$.

7) $(0, 0, 0)$; $(1, 0, 1)$; $(-1, 2, -3)$.

Базис Гребнера при $y > z > x$: $x - x^2 + y$, $x^2 - 2x^3 + z$, $-x^2 + x^4$.

8) $x = 0$, $y = 0$, $z \in \mathbb{C}$ или $x = \frac{1 \pm i\sqrt{3}}{2}$, $y = \frac{1 \mp i\sqrt{3}}{2}$, $z = \frac{-1 \mp i\sqrt{3}}{2}$.

Базис Гребнера при $x > y > z$: $x + y + yz$, $y^2 + z^2y$, $yz + z^2y + z^3y$.

9) $x = y = z = 0$ или $x = \frac{1}{2}$, $y = -\frac{1}{2}$, $z = -\frac{1}{2}$ или $x = \frac{-1 \pm i\sqrt{3}}{4}$, $y = -\frac{1}{2}$, $z = \frac{1 \pm i\sqrt{3}}{4}$.

Базис Гребнера при $x > y > z$: $yz + x^2 + z$, $xz - 2z^3$, $y^2 + 2z^3$, $2z^2y + z^2$, $z^2 + 8z^5$.

10) $x = 0$, $y = 0$, $z = \pm 1$.

Базис Гребнера при $x > z > y$: $x^2 + z^2y + yz$, $y^2 - zx + x$, $xy + z^2 - 1$, $-z^2 + 1 + z^3 - z + y^3$,
$y^2z^2 - y^2$, y^4.

8.6. К главе 7

7.4. Достаточно доказать, что найдутся такие номера $i < j$, для которых x^{a_j} делится на x^{a_i}, а это в точности лемма Диксона.

7.8. Универсальный базис состоит из одного многочлена f. В самом деле, для любого порядка старший член многочлена fg делится на старший член f.

Литература о базисах Гребнера

[1] Бухбергер Б., Алгоритмический метод в теории полиномиальных идеалов — в книге "Компьютерная алгебра. Символьные и алгебраические вычисления", М.: Мир, 1986. - 392 стр.

[2] Уфнаровский В. А., Комбинаторные и асимптотические методы в алгебре - ВИНИТИ, Современные проблемы математики, Фундаментальные направления, том 57, Москва, 1990 (параграф 2).

[3] Дэвенпорт Дж., Сирэ И., Турнье Э., Компьютерная алгебра, - М.: Мир, 1991. - 350 стр. (глава 3).

[4] Латышев В.Н., Комбинаторная теория колец. Стандартные базисы, - М.: МГУ, 1988. - 68 стр.

[5] Прасолов В. В., Многочлены – М.: МЦНМО, 2000. - 335 стр. (глава 6).

[6] Кокс Д., Литтл Дж., О'Ши, Д., Идеалы, многообразия и алгоритмы – М. Мир, 2000. - 687 стр.

[7] Eisenbud D. Commutative Algebra with a View Toward Algebraic Geometry – Graduate Texts in Math. 150, Springer-Verlag, New York, 1995 (глава 15).

[8] Sturmfels B. Gröbner Bases and Convex Polytopes – AMS, Providence, RI, 1995.

[9] Adams W.W., Loustaunau P., An introduction to Gröbner Bases – AMS, Graduated Studies in Math. Vol. III, 1994.

[10] Becker T., Kredel H., Weispfenning V., Gröbner Bases: A Computational Approach to Commutative Algebra, Graduated Texts in Math., Springer, New York, 1993.