Лекция 2: Деление в кольце многочленов от n переменных

(2.1) Проблема принадлежности идеалу в кольце $k[x]$.

Увидим, что кольцо $k[x]$ является кольцом главных идеалов, т.е. любой идеал в $k[x]$ однопорождён.

Предложение 2.1: Любой идеал в $k[x]$ может быть записан в виде $\langle f \rangle$, где f — некоторый многочлен из $k[x]$. Более того, f единственный с точностью до умножения на ненулевую константу из поля k.

Доказательство: Заметим, что нулевой идеал в $k[x]$ имеет вид $\langle 0 \rangle$. Далее полагаем, что I — ненулевой идеал в $k[x]$. Пусть f — ненулевой многочлен наименьшей степени, лежащий в I. Очевидно, что $\langle f \rangle \subset I$. Докажем обратное включение, с этой целью возьмём $g \in I$ и поделим его на f:

$$g = qf + r,$$

где либо $r = 0$, либо $\deg(r) < \deg(f)$. Так как $r = g - qf \in I$, то неравенство r нулю противоречило бы выбору f. Поэтому остаток $r = 0$, и $g = qf \in I$, т.е. $I \subset \langle f \rangle$. Равенство $I = \langle f \rangle$ доказано.

Если $\langle f \rangle = \langle g \rangle$, то $f \in \langle g \rangle$, и мы можем записать $f = hg$ для некоторого многочлена $h \in k[x]$. Тогда справедливо равенство

$$\deg(f) = \deg(h) + \deg(g), \tag{2.1}$$

влекущее $\deg(f) \geq \deg(g)$. Так как $g \in \langle f \rangle$, то аналогично получается неравенство $\deg(g) \geq \deg(f)$. Тем самым степени многочленов f и g совпадают. Как следует из (2.1) $\deg(h) = 0$, т.е h является ненулевой константой. ◀

Пример 2.1: Выясним, лежит ли $x^3 + 4x^2 + 3x - 7$ в идеале $\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

1) Идеал $\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$ порождается наибольшим общим делителем $\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$. Известно, что

$$\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) = \gcd(x^3 - 3x + 2, \gcd(x^4 - 1, x^6 - 1)).$$

Найдём $\gcd(x^4 - 1, x^6 - 1) = \gcd(x^6 - 1, x^4 - 1) = \gcd(x^4 - 1, x^2 - 1) = \gcd(x^2 - 1, 0) = x^2 - 1$,

$\gcd(x^3 - 3x + 2, x^2 - 1) = \gcd(x^2 - 1, -2x + 2) = \gcd(x - 1, 0) = x - 1.$

Таким образом,

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle = \langle x - 1 \rangle.$$

2) Для ответа на вопрос „$x^3+4x^2+3x-7 \in \langle x-1\rangle$?" достаточно поделить исследуемый многочлен на порождающую:

$$x^3+4x^2+3x-7 = (x^2+5x+8)(x-1)+1.$$

Поскольку остаток не равен 0, то мы заключаем, что

$$x^3+4x^2+3x-7 \notin \langle x^3-3x+2,\, x^4-1,\, x^6-1\rangle.$$

Для решения задачи принадлежности идеалу в $k[x_1,\dots,x_n]$ мы будем поступать схожим образом: 1) находить „хороший" базис для идеала (так называемый базис Грёбнера); 2) применять алгоритм деления в кольце $k[x_1,\dots,x_n]$.

2.2 Мономиальные порядки

Алгоритм деления многочленов из $k[x]$ опирается 1) на том факте, что мы можем упорядочить мономы от одной переменной по возрастанию степеней:

$$1 < x < x^2 < \dots < x^m < x^{m+1} < \dots;$$

2) соотношение между мономами x^k, x^l сохраняется при умножении на моном x^m: $x^k < x^l \Rightarrow x^{k+m} < x^{k+l}$.

Наша задача ввести упорядочение на множестве всех мономов из $k[x_1,\dots,x_n]$ максимально похожим на естественное упорядочение для мономов от одной переменной образом.

Заметим, что существует 1-1 соответствие между мономами из $k[x_1,\dots,x_n]$ и точками $\mathbb{Z}^n_{\geq 0}$: $x^\alpha := x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n} \xrightarrow{1:1} \alpha=(\alpha_1,\dots,\alpha_n)$.

Поэтому любой порядок на $\mathbb{Z}^n_{\geq 0}$ задаёт порядок на множестве мономов; и наоборот: $\alpha < \beta \Leftrightarrow x^\alpha < x^\beta$.

Определение 2.1. Мономиальным порядком $<$ на $k[x_1,\dots,x_n]$ называется линейный порядок на $\mathbb{Z}^n_{\geq 0}$ (или на множестве мономов), т.ч.

1) если $\alpha<\beta$ и $\gamma \in \mathbb{Z}^n_{\geq 0}$, то $\alpha+\gamma<\beta+\gamma$;

2) $(\mathbb{Z}^n_{\geq 0}, <)$ является вполне упорядоченным множеством, т.е. всякое непустое подмножество $\mathbb{Z}^n_{\geq 0}$ содержит наименьший элемент.

Лемма 2.1: Пусть $<$ – линейный порядок на $\mathbb{Z}^n_{\geq 0}$. Тогда $(\mathbb{Z}^n_{\geq 0}, <)$ – вполне упорядоченное множество $\Leftrightarrow$ когда всякая строго убывающая последовательность

$$\alpha_1 > \alpha_2 > \alpha_3 > \dots, \quad \alpha_i \in \mathbb{Z}^n_{\geq 0},$$

обрывается

Доказательство: Докажем, что $(\mathbb{Z}^n_{\geq 0}, <)$ – не ВУМ $\Leftrightarrow$ когда существует бесконечная строго убывающая последовательность в $\mathbb{Z}^n_{\geq 0}$.

Если $(\mathbb{Z}^n_{\geq 0}, <)$ – не ВУМ, то существует подмножество $S \subset \mathbb{Z}^n_{\geq 0}$, которое не содержит наименьшего элемента. Выберем $\alpha_1 \in S$, поскольку в S нет наименьшего элемента, найдётся $\alpha_2 \in S: \alpha_1 > \alpha_2$. Аналогично, найдётся $\alpha_3 \in S$: $\alpha_2 > \alpha_3$. Продолжая, мы получим бесконечную строго убывающую последовательность

(2.2) $\quad \alpha_1 > \alpha_2 > \alpha_3 > \dots$.

Пусть нам дана бесконечная строго убывающая последовательность (2.2). Тогда непустое подмножество $\{\alpha_1, \alpha_2, \alpha_3, \dots\} \subset \mathbb{Z}^n_{\geq 0}$ не имеет наименьшего элемента, поэтому $(\mathbb{Z}^n_{\geq 0}, <)$ не является ВУМ. ◀

Определение 2.3: (лексикографический порядок) Пусть $\alpha = (\alpha_1, \dots, \alpha_n)$ и $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Будем говорить, что $\alpha < \beta$ лексикографически ($\alpha <_{lex} \beta$), если первая ненулевая координата вектора $\beta - \alpha$ положительна.

Согласно договорённости $x^\alpha <_{lex} x^\beta$, если $\alpha <_{lex} \beta$.

NB: здесь мы считаем, что $x_1 > x_2 > \dots > x_n$.

Предложение 2.2: Лексикографический порядок является мономиальным порядком на $\mathbb{Z}^n_{\geq 0}$.

Доказательство: Из определения очевидно, что лексикографический порядок – это линейный порядок.

1) Пусть $\alpha <_{lex} \beta$ и $\gamma \in \mathbb{Z}^n_{\geq 0}$. Поскольку $(\beta + \gamma) - (\alpha + \gamma) = \beta - \alpha$, первая отличная от нуля координата вектора $(\beta + \gamma) - (\alpha + \gamma)$ такая же как у вектора $\beta - \alpha$. Следовательно, $\alpha + \gamma < \beta + \gamma$.

2) Предположим, что $(\mathbb{Z}^n_{\geq 0}, <_{lex})$ — не ВУМ. По предложению 1.2 тогда должна существовать бесконечно убывающая последовательность

$$\alpha_1 >_{lex} \alpha_2 >_{lex} \alpha_3 >_{lex} \dots$$

элементов $\alpha_i \in \mathbb{Z}^n_{\geq 0}$.

Из определения лексикографического порядка следует, что первые координаты векторов α_i образуют невозрастающую последовательность неотрицательных чисел. Но тогда найдётся целое $k > 0$ такое, что первые координаты векторов α_i совпадают, если $i \geq k$.

Исходя, из определения лексикографического порядка, нетрудно увидеть, что вторые координаты векторов $\alpha_k, \alpha_{k+1}, \dots$ тоже образуют невозрастающую последовательность в $\mathbb{Z}_{\geq 0}$. Следовательно, начиная с некоторого номера, вторые координаты векторов $\alpha_k, \alpha_{k+1}, \dots$ будут совпадать. Таким образом, рассматривая последовательности оставшихся координат, мы получим, что для некоторого l все векторы в последовательности $\alpha_l, \alpha_{l+1}, \dots$ будут равны. А это противоречит тому, что $\alpha_l >_{lex} \alpha_{l+1}$. Предположение, $(\mathbb{Z}^n_{\geq 0}, <)$ не является ВУМ, приводит к противоречию. ◀

Определение 2.4: (степенной лексикографический порядок)

Пусть $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Будем говорить, что $\alpha <_{deglex} \beta \iff$ либо $|\alpha| < |\beta|$, либо $|\alpha| = |\beta|$ и справедливо $\alpha <_{lex} \beta$.

Определение 2.5: (степенной обратный лексикографический порядок)

Пусть $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Будем говорить, что $\alpha <_{drevlex} \beta \iff$ либо $|\alpha| < |\beta|$, либо $|\alpha| = |\beta|$ и отличная от нуля рдината вектора $\beta - \alpha$ с наибольшим номером отрицательна.

Если зафиксирован мономиальный порядок $<$ на $k[x_1, \dots, x_n]$, то для многочлена $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \dots, x_n]$

1) мультистепень — $\operatorname{mdeg} f := \max\{\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0\}$;
2) старший коэффициент — $\operatorname{lc} f := a_{\operatorname{mdeg} f}$;
3) старший моном — $\operatorname{lm} f := x^{\operatorname{mdeg} f}$;
4) старший член — $\operatorname{lt} f := \operatorname{lc} f \cdot \operatorname{lm} f$.

Очевидно, что для ненулевых $f, g \in k[x_1, \ldots, x_n]$ выполняются

1) $\operatorname{mdeg}(fg) = \operatorname{mdeg} f + \operatorname{mdeg} g$;

2) $\operatorname{mdeg}(f+g) \leq \max\{\operatorname{mdeg} f, \operatorname{mdeg} g\}$ при $f+g \neq 0$.

2.3 Алгоритм деления в $k[x_1, \ldots, x_n]$

Наша цель — поделить многочлен $f \in k[x_1, \ldots, x_n]$ на набор многочленов $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, т.е. получить представление

(2.3) $$f = a_1 f_1 + \ldots + a_s f_s + r,$$

где частные $a_1, \ldots, a_s$ и остаток r лежат в $k[x_1, \ldots, x_n]$. При этом мы должны оговорить, что будем понимать под остатком.

Пример 2.2: Будем работать в кольце $\mathbb{Q}[x, y]$, используя lex: $x > y$.

Поделим $f = \underline{x^2y} + xy^2 + y^2$ на $(f_1, f_2) = (\underline{xy} - 1, \underline{y^2} - 1)$.
Первоначально имеем

$$f = 0 \cdot (xy-1) + 0 \cdot (y^2-1) + \underline{x^2y} + xy^2 + y^2. \quad (0\text{-шаг})$$

Далее сократив $\operatorname{lt} f$ с помощью $\operatorname{lt} f_1$, получим

$$f - x f_1 = xy^2 + x + y^2,$$

или по-другому

$$f = x(xy-1) + 0(y^2-1) + \underline{xy}^2 + x + y^2. \quad (1\text{ шаг})$$

Продолжая, приходим к ситуации, к-ой не бывает в случае одной переменной:

$$f = (x+y)(xy-1) + 0(y^2-1) + \underline{x} + y^2 + y, \quad (2\text{ шаг})$$

где x не делится ни на $\operatorname{lt} f_1$, ни на $\operatorname{lt} f_2$, но y^2 делится на $\operatorname{lt} f_2$.
Сокращая y^2, приходим к

$$f = \overbrace{(x+y)}^{a_1}(xy-1) + \overset{a_2}{1} \cdot (y^2-1) + \overbrace{x+y+1}^{r}, \quad (3\text{ шаг}).$$

где многочлен $x+y+1$ уже можно считать остатком, поскольку ни один его моном не делится на старшие члены многочленов из набора (f_1, f_2). ◀

Теорема 2.1: Пусть $<$ — мономиальный порядок на $k[x_1,\dots,x_n]$, $F=(f_1,\dots,f_s)\subset k[x_1,\dots,x_n]$. Тогда любой многочлен $f\in k[x_1,\dots,x_n]$ может быть записан в виде (2.3), где либо $r=0$, либо ни один из мономов, составляющих r, не делится ни на один из $\mathrm{lt} f_1,\dots,\mathrm{lt} f_s$ (такой r будем называть **остатком от деления** f на F). Более того, если $a_if_i\neq 0$, то

(2.4) $$\operatorname{mdeg} f \geq \operatorname{mdeg}(a_if_i).$$

Доказательство: Мы покажем, что желаемое представление (2.3) есть результат работы **алгоритма деления** в $k[x_1,\dots,x_n]$:

Вход: $f_1,\dots,f_s, f$
Выход: $a_1,\dots,a_s, r$
Инициализация: $a_1:=0,\ \dots,\ a_s:=0,\ r:=0,\ p:=f$
Пока $p\neq 0$
  $i:=\min(\{j:\mathrm{lt} f_j \text{ делит } \mathrm{lt}\, p\}\cup\{s+1\})$ # т.е. i — номер
  Если $i\neq s+1$ # первого многочлена
    $a_i:=a_i+\mathrm{lt}\,p/\mathrm{lt} f_i$ # в наборе F старший
    $p:=p-(\mathrm{lt}\,p/\mathrm{lt} f_i)f_i$ # член которого делит $\mathrm{lt}\,p$.
  Иначе
    $r:=r+\mathrm{lt}\,p$
    $p:=p-\mathrm{lt}\,p$

Будем нумеровать состояние переменных перед итерациями цикла с помощью верхнего индекса: $a_1^{(k)},\dots,a_s^{(k)}, p^{(k)}, r^{(k)}$. Тогда для всех возможных значений k справедливо равенство

$$f=a_1^{(k)}f_1+\dots+a_s^{(k)}f_s+p^{(k)}+r^{(k)}.$$

Алгоритм остановится, если при некотором k_0 многочлен $p^{(k_0)}=0$, в этом случае мы получим требуемое разложение (2.3).

Покажем, что алгоритм действительно завершает свою работу за конечное число шагов. Если $p^{(k+1)}=p^{(k)}-(\mathrm{lt}\,p^{(k)}/\mathrm{lt} f_i)f_i$, то

(2.5) $$\operatorname{mdeg} p^{(k+1)}<\operatorname{mdeg} p^{(k)},$$

так как $\mathrm{lt}\big((\mathrm{lt}\,p^{(k)}/\mathrm{lt} f_i)f_i\big)=(\mathrm{lt}\,p^{(k)}/\mathrm{lt} f_i)\,\mathrm{lt} f_i=\mathrm{lt}(p^{(k)})$. Если же $p^{(k+1)}=p^{(k)}-\mathrm{lt}\,p^{(k)}$, то мы снова имеем неравенство (2.5). Таким образом последовательность $\{\operatorname{mdeg} p^{(k)}\}$ убывает. Если бы алгоритм не завершался, то это была бесконечно убывающая последовательность, и мы получили бы противоречие с тем, что $<$ — мономиальный порядок. Поэтому при каком-то k_0 многочлен $p^{(k_0)}=0$, т.е. алгоритм останавливается.

Остаётся установить неравенство (2.4). Заметим, что каждое слагаемое в a_i имеет вид $\operatorname{lt} p^{(k)} / \operatorname{lt} f_i$. Начальное значение $p^{(0)} = f$, поэтому в силу только что доказанного, $\operatorname{lt} p^{(k)} < \operatorname{lt} f$ для всех k. Следовательно, для всех $i \in \{1, \dots, s\}$

$$\operatorname{lt}(a_i f_i) = \operatorname{lt} a_i \operatorname{lt} f_i = \frac{\operatorname{lt} p^{(k_i)}}{\operatorname{lt} f_i} \cdot \operatorname{lt} f_i = \operatorname{lt} p^{k_i} < \operatorname{lt} f.$$ ◀

Если в результате деления f на $(f_1, \dots, f_s)$ остаток $r = 0$, то многочлен $f \in \langle f_1, \dots, f_s \rangle$. Однако обратное неверно.

Пример 2.3: Пусть $f_1 = xy + 1$, $f_2 = y^2 - 1$ из $\mathbb{Q}[x, y]$ с lex: $x > y$. Поделив многочлен $f = xy^2 - x$ на (f_1, f_2), получим

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y).$$

Однако $xy^2 - x = x(y^2 - 1) \in \langle f_1, f_2 \rangle$. ◀