Тема I: Многочлены

§1. Делимость многочленов

Многочлены над полем

М.В.Волков

Уральский федеральный университет

Институт естественных наук и математики

кафедра алгебры и фундаментальной информатики

2021/2022 учебный год

Определения

Вспомним одно определение из курса «Введение в математику»

Коммутативное ассоциативное кольцо без делителей нуля называется *областью целостности*. Часто говорят просто «область».

Примеры: кольцо целых чисел $\mathbb{Z}$, любое поле, кольцо многочленов $F[X]$ над произвольным полем F, и вообще, кольцо многочленов $D[X]$ над произвольной областью D.

Мы будем изучать делимость в кольце многочленов над областью с 1, но некоторые базовые определения и свойства делимости приведем для произвольной области D с 1.

Элемент $a \in D$ *делится* на $b \in D$, если существует элемент $c \in D$ такой, что $a = bc$. В этом случае b называют *делителем* a и пишут $b|a$.

Отношение $|$ рефлексивно (в силу наличия 1) и транзитивно (в силу ассоциативности умножения), но, вообще говоря, не антисимметрично.
Элементы, которые делят друг друга, называют *ассоциированными*.
Обозначение: $a \sim b$. Ясно, что $\sim$ – отношение эквивалентности.
Один из классов этой эквивалентности – $\{0\}$, другой – группа всех обратимых элементов области D.
В $\mathbb{Z}$ классы ассоциированности суть $\{0\}$, $\{\pm 1\}$, $\{\pm 2\}$, ...

Замечание 1 (характеризация ассоциированности в области с 1)

Пусть D – область с 1. Элементы $a, b \in D$ ассоциированы тогда и только тогда, когда $a = bu$ для некоторого обратимого элемента $u \in D$.

Доказательство. Если $a = bu$, то $b|a$ по определению. Если к тому же элемент u обратим, то умножив равенство $a = bu$ на u^{-1}, получим $au^{-1} = b$, откуда $a|b$. Итак, a и b делят друг друга, т.е. $a \sim b$.

Обратно, пусть $a|b$ и $b|a$, т.е. $a = bc$ и $b = ad$ для некоторых c и d. Подставив 2-е равенство в 1-е, получим $a = adc$, откуда $a(1 - dc) = 0$. Если $a = 0$, то $b = 0$, и $a = b \cdot 1$. Если $a \neq 0$, то поскольку в D нет делителей нуля, $1 - dc = 0$, откуда $cd = 1$ и c – обратимый элемент. □

Замечание 2 (связь делимости с операциями кольца)

Если $a|b$, то $a|bc$ для любого c, а если $a|b_1$ и $a|b_2$, то $a|(b_1 \pm b_2)$.

Доказательство – упражнение. □

Определение

Необратимый элемент p области D называется *неразложимым*, если p непредстави́м как произведение двух элементов, не ассоциированных с p.

$$\forall a, b, c \in D\ (pc \neq 1)\ \&\ (p = ab \to (p \sim a) \vee (p \sim b)).$$

Пример: неразложимые элементы кольца $\mathbb{Z}$ суть в точности числа $\pm p$, где p – простое число.

Определение

Область называется *областью с однозначным разложением* (*ООР*), если каждый ее ненулевой необратимый элемент представи́м в виде произведения неразложимых, причем такое представление однозначно с точностью до порядка сомножителей и ассоциированности.

Однозначность с точностью до порядка сомножителей и ассоциированности означает, что если $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_k$, где все $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_k$ неразложимы, то $k = n$, а множители произведения $q_1 q_2 \cdots q_n$ можно переставить так, что в получившемся после перестановки произведении первый множитель будет ассоциирован с p_1, второй – с p_2, $\ldots$, n-й – с p_n.

Области с однозначным разложением

Известный вам со школы пример области с однозначным разложением – кольцо $\mathbb{Z}$. Это так называемая *основная теорема арифметики* (которую, впрочем, в школе обычно не доказывают).

Однозначность разложения настолько привычна, что складывается впечатление, что она выполняется всегда. Увы, это далеко не так.

Вот простой пример области, в которой каждый необратимый элемент представи́м как произведение неразложимых, но однозначности нет:

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

Имеем $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Можно проверить, что каждое из чисел 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ – неразложимый элемент кольца $\mathbb{Z}[\sqrt{-5}]$, но ни один из этих элементов не ассоциирован в $\mathbb{Z}[\sqrt{-5}]$ ни с одним другим.

Даже когда однозначность разложения есть, доказать это бывает непросто. *Пример ООР*: кольцо целых гауссовых чисел $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$. *Вопрос на дом*: почему равенства $5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$ не противоречат только что высказанному утверждению, что $\mathbb{Z}[i]$ есть ООР?

Однозначность разложения и теорема Ферма

Деление с остатком в кольце многочленов

Наша ближайшая цель – доказать, что для любого поля F кольцо многочленов $F[x]$ является областью с однозначным разложением.

Основной инструмент здесь – деление многочленов с остатком.

Определение, обозначение и соглашение

Степень ненулевого многочлена $f(x) = a_0 + a_1x + a_2x^2 + \dots$ – это наибольшее n такое, что $a_n \neq 0$. Степень f обозначается через $\deg f$. Степень нулевого многочлена равна $-\infty$, причем символ $-\infty$ меньше любого целого числа и $n + (-\infty) = -\infty + n := -\infty$ для любого целого n.

Теорема о делении многочленов с остатком

Пусть F — поле и $f, g \in F[x]$, причем $g \neq 0$. Тогда существуют такие однозначно определенные многочлены $q, r \in F[x]$, что

$$f = qg + r \text{ и } \deg r < \deg g.$$

Многочлен q называется (*неполным*) *частным*, а многочлен r – *остатком* от деления f на g. Заметим, что если $r = 0$, то g делит f в обычном смысле.

Доказательство теоремы о делении многочленов с остатком

Доказательство. Существование многочленов q и r. При $\deg f < \deg g$ достаточно положить $q := 0$, $r := f$. Пусть теперь $k := \deg f \geq m := \deg g$, $f = \alpha x^k +$ члены меньших степеней, $g = \beta x^m +$ члены меньших степеней.

Проведем индукцию по $k - m$. Если $k - m = 0$, т.е. $k = m$, положим $q := \dfrac{\alpha}{\beta}$ и $r := f - \dfrac{\alpha}{\beta} g$; тогда $f = qg + r$ и $\deg r < \deg g$.

Пусть $k - m > 0$. Положим $h := f - \dfrac{\alpha}{\beta} x^{k-m} g$. Старший член многочлена $\dfrac{\alpha}{\beta} x^{k-m} g$ равен αx^k, и потому $\deg h < k$. Применяя к многочленам h и g предположение индукции, получаем, что существуют такие многочлены q_1, r, что $h = q_1 g + r$ и $\deg r < \deg g$. Но тогда

$$f = \frac{\alpha}{\beta} x^{k-m} g + h = \frac{\alpha}{\beta} x^{k-m} g + q_1 g + r = \left(\frac{\alpha}{\beta} x^{k-m} + q_1 \right) g + r,$$

что дает требуемое равенство $f = qg + r$ с суммой $\dfrac{\alpha}{\beta} x^{k-m} + q_1$ в роли q.

Доказательство теоремы о делении многочленов с остатком (2)

Единственность многочленов q *и* r. Предположим, что $f = q_1 g + r_1$ и $f = q_2 g + r_2$ для некоторых многочленов q_1, q_2, r_1 и r_2 таких что $\deg r_1, \deg r_2 < \deg g$. Из равенства $q_1 g + r_1 = q_2 g + r_2$ получаем $(q_1 - q_2)g = r_2 - r_1$. Но если $q_1 - q_2 \neq 0$, то это невозможно, так как $\deg\big((q_1 - q_2)g\big) \geqslant \deg g$, а $\deg(r_2 - r_1) < \deg g$. Следовательно, $q_1 - q_2 = 0$, откуда $q_1 = q_2$ и $r_1 = r_2$. □

Замечание

Доказательство дает алгоритм построения частного и остатка.

Пример: поделим «уголком» $6x^3 - 2x^2 + x + 3$ на $x^2 - x + 1$ с остатком.

$$\begin{array}{rl|l} & 6x^3 - 2x^2 + x + 3 & x^2 - x + 1 \\ - & 6x^3 - 6x^2 + 6x & \hline & & 6x + 4 \\ \hline & 4x^2 - 5x + 3 & \\ - & 4x^2 - 4x + 4 & \\ \hline & -x - 1 & \end{array}$$

Частное $6x + 4$, остаток $-x - 1$.

Определение

Пусть F – поле и $f, g \in F[x]$. Многочлен $h \in F[x]$ называется *наибольшим общим делителем* (НОД) многочленов f и g, если $h|f$, $h|g$ и для любого $p \in F[x]$ из того, что $p|f$ и $p|g$, следует, что $p|h$.

НОД многочленов определен с точностью до ассоциированности.

Теорема о наибольшем общем делителе

Для любых ненулевых многочленов f и g над полем F существует наибольший общий делитель и для некоторых многочленов $u, v \in F[x]$

$$\text{НОД}(f, g) = uf + vg.$$

Доказательство. Рассмотрим множество $I := \{uf + vg \mid u, v \in F[x]\}$. Оно содержит ненулевые многочлены (например, сами f и g). Покажем, что ненулевой многочлен наименьшей степени в I есть $\text{НОД}(f, g)$.

Наибольший общий делитель (2)

Итак, пусть d – ненулевой многочлен наименьшей степени в $I = \{uf + vg \mid u, v \in F[x]\}$. Прежде всего, проверим, что $d|f$ и $d|g$.

Поделим f на d с остатком: $f = qd + r$, где $\deg r < \deg d$. Имеем $d = u_0 f + v_0 g$ для каких-то многочленов $u_0, v_0 \in F[x]$, откуда $r = f - qd = f - q(u_0 f + v_0 g) = (1 - qu_0)f + (-qv_0)g \in I$.
Поскольку $\deg r < \deg d$, а d – ненулевой многочлен наименьшей степени в I, заключаем, что $r = 0$ и $f = qd$, т.е. $d|f$. Аналогично, $d|g$.

Если $p \in F[x]$ таков, что $p|f$ и $p|g$, то по свойствам делимости $p|(u_0 f + v_0 g)$, т.е. $p|d$. Итак, $d = \text{НОД}(f, g)$. □

Приведенное доказательство компактно, но неконструктивно.
Способ практического вычисления $\text{НОД}(f, g)$, а также таких многочленов $u, v \in F[x]$, что $\text{НОД}(f, g) = uf + vg$ дает *алгоритм Евклида*.

Алгоритм Евклида

Пусть даны ненулевые многочлены f и g. Без ограничения общности предположим, что $\deg f \geqslant \deg g$.
Если $g|f$, то НОД$(f, g) = g$.
Если $g \nmid f$, разделим f на g с остатком: $f = q_1 g + r_1$.
Если $r_1|g$, то процесс закончен, иначе разделим g на r_1 с остатком: $g = q_2 r_1 + r_2$.
Если $r_2|r_1$, то процесс закончен, иначе разделим r_1 на r_2 с остатком: $r_1 = q_3 r_2 + r_3$.
Продолжаем этот процесс, пока один из получающихся остатков не разделится на следующий. Если процесс в какой-то момент закончится, последний ненулевой остаток и будет равен НОД(f, g).

Теорема (корректность алгоритма Евклида)

Для любых ненулевых многочленов f и g процесс в алгоритме Евклида заканчивается за конечное число шагов и последний ненулевой остаток равен НОД(f, g).

Доказательство. Поскольку $\deg g, \deg r_1, \deg r_2, \cdots \in \mathbb{N} \cup \{0\}$ и $\deg g > \deg r_1 > \deg r_2 > \cdots$, процесс должен завершиться.

Выпишем всю последовательность получения остатков:

$$\begin{aligned}
f &= q_1 g + r_1;\\
g &= q_2 r_1 + r_2;\\
r_1 &= q_3 r_2 + r_3;\\
r_2 &= q_4 r_3 + r_4;\\
&\ldots\ldots\ldots\ldots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1};\\
r_{n-2} &= q_n r_{n-1} + r_n;\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned} \qquad (*)$$

Последнее равенство означает, что $r_n | r_{n-1}$. Поднимаясь на строчку выше, мы видим, что r_n делит правую часть равенства, а значит, $r_n | r_{n-2}$. Еще поднимаемся на одну строку и получаем, что $r_n | r_{n-3}$. И так далее, доходим до второй строки сверху и получаем, что $r_n | g$. Рассматривая первую строку, получаем, что $r_n | f$. Итак, r_n – общий делитель многочленов f и g.

Идя по последовательности (*) сверху вниз, покажем, что если $h | f$ и $h | g$, то $h | r_n$. Из первого равенства $r_1 = f - q_1 g$; отсюда по свойствам делимости $h | r_1$. Рассматривая следующее равенство, получаем $r_2 = g - q_2 r_1$, откуда $h | r_2$. Итак, опускаясь по равенствам (*), получим, что $h | r_s$ при всех $s = 3, \ldots, n$. Поэтому $r_n = \text{НОД}(f, g)$. □

Алгоритм Евклида (3)

Взглянем еще раз на последовательность получения остатков:

$$
\begin{aligned}
f &= q_1 g + r_1;\\
g &= q_2 r_1 + r_2;\\
r_1 &= q_3 r_2 + r_3;\\
r_2 &= q_4 r_3 + r_4;\\
&\ldots\ldots\ldots\ldots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1};\\
r_{n-2} &= q_n r_{n-1} + r_n;\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}
\qquad (*)
$$

Из предпоследнего равенства можно выразить r_n через r_{n-1} и r_{n-2} с некоторыми полиномиальными коэффициентами: $r_n = r_{n-2} - q_n r_{n-1}$.
Подставим в это равенство выражение r_{n-1} из предыдущей строки:

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = (1 + q_{n-1} q_n) r_{n-2} - q_n r_{n-3}.$$

Так r_n выражено с коэффициентами $(1 + q_{n-1} q_n)$ и $-q_n$ через r_{n-2} и r_{n-3}.
Подставим в полученное равенство выражение для r_{n-2} и т.д.
Продолжая этот процесс, придём к выражению r_n через f и g с некоторыми полиномиальными коэффициентами u и v.
Итак, алгоритм Евклида позволяет находить и сам НОД данных многочленов, и его представление в виде комбинации этих многочленов с полиномиальными коэффициентами.

Определение

Многочлены f и g называются *взаимно простыми*, если их НОД равен 1.

Предложение о взаимно простых многочленах

Пусть f, g и h — многочлены над полем F.

1) *Если f и g взаимно просты, $f|h$ и $g|h$, то $(fg)|h$.*
2) *Если f и g взаимно просты и $f|(gh)$, то $f|h$.*

Доказательство. 1) Пусть $h = fp = gq$ для некоторых многочленов p и q. Так как f и g взаимно просты, существуют многочлены u и v такие, что выполняется равенство $1 = uf + vg$. Умножая обе части этого равенства на h, получим $h = huf + hvg$, откуда $h = gquf + fpvg = fg(qu + pv)$.

2) По условию $gh = fp$ для некоторого многочлена p. Так как f и g взаимно просты, $uf + vg = 1$ для некоторых многочленов u и v. Следовательно, $huf + hvg = h$, откуда $h = huf + fpv = f(hu + pv)$. □

Неприводимые многочлены

Неразложимые элементы кольца многочленов $D[x]$ принято называть *неприводимыми* многочленами.
Важно понимать, что приводимость/неприводимость данного многочлена зависит от того, над какой областью рассматривается этот многочлен!

Примеры. 1) Многочлен $x^2 - 2$ неприводим над $\mathbb{Q}$, но приводим над $\mathbb{R}$:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

2) Многочлен $x^2 + 1$ неприводим над $\mathbb{R}$, но приводим над $\mathbb{C}$:

$$x^2 + 1 = (x - i)(x + i).$$

Этот же многочлен приводим над двухэлементным полем:

$$x^2 + 1 = (x + 1)(x + 1).$$

3) Многочлен $2x + 2$ неприводим над $\mathbb{Q}$, но приводим над $\mathbb{Z}$:

$$2x + 2 = 2(x + 1).$$

Предложение о неприводимых многочленах

Если g — неприводимый многочлен над полем F и g делит произведение некоторых многочленов $h_1 \cdots h_m$, то g делит один из многочленов h_i.

Доказательство. Индукция по m с очевидной базой.

Шаг индукции. Пусть $m > 1$. Положим $d := \text{НОД}(g, h_m)$. Тогда $g = qd$ для некоторого многочлена q. В силу неприводимости многочлена g один из многочленов d и q ассоциирован с g. Если d ассоциирован с g, то $g|d$, откуда $g|h_m$. Если q ассоциирован с g, то d – многочлен нулевой степени, т.е. ненулевой элемент поля. Поэтому многочлены g и h_m взаимно просты. В силу п. 2) предложения о взаимно простых многочленах в этом случае g делит произведение $h_1 \cdots h_{m-1}$, и по предположению индукции g делит один из сомножителей этого произведения. □

Теорема о разложении многочлена на неприводимые множители

Кольцо многочленов над полем – область с однозначным разложением.

Напомним, что область D называется областью с однозначным разложением, если каждый ее ненулевой необратимый элемент представи́м как произведение неразложимых, причем это представление однозначно с точностью до порядка сомножителей и ассоциированности. В кольце многочленов $F[x]$ над полем F обратимыми являются в точности элементы поля, т.е. многочлены нулевой степени. Поэтому теорема означает, что в $F[x]$ каждый многочлен степени $n \geq 1$ однозначно представи́м как произведение неприводимых многочленов.

Доказательство. Индукция по n. База индукции $n = 1$ следует из того, что многочлены первой степени над полем неприводимы.
Шаг индукции – *существование*. Рассмотрим произвольный многочлен f степени $n > 1$. Если f неприводим, доказывать нечего. Если f приводим, то $f = gh$, где g и h необратимы в $F[x]$. Как отмечено, в $F[x]$ обратимы многочлены нулевой степени. Поэтому $\deg g, \deg h \geqslant 1$ и, поскольку $\deg f = \deg g + \deg h$, имеем $\deg g, \deg h < \deg f = n$. Многочлены g и h можно разложить в произведение неприводимых по предположению индукции. Перемножая разложения g и h, получим разложение f.

Шаг индукции – *единственность*. Рассмотрим произвольный многочлен f степени $n > 1$ и пусть $f = g_1 \cdots g_k = h_1 \cdots h_m$, где $g_1, \ldots, g_k, h_1, \ldots, h_m$ — неприводимые над F многочлены. Многочлен g_1 делит $h_1 \cdots h_m$. В силу предложения о неприводимых многочленах g_1 делит h_i для некоторого i. Не ограничивая общности, можно считать, что $i = 1$ (в противном случае можно переставить сомножители в произведении $h_1 \cdots h_m$). Итак, $h_1 = wg_1$ для некоторого многочлена w. Поскольку многочлен h_1 неприводим, один из многочленов w и g_1 ассоциирован с h_1. Если w ассоциирован с h_1, то $g_1 \in F$, что невозможно. Следовательно, $w \in F$ и $g_1 \sim h_1$. Сократим на g_1 равенство

$$g_1 g_2 \cdots g_k = w g_1 h_2 \cdots h_m.$$

Если $k = 1$, в левой части останется 1, а значит, $m = 1$, и все доказано. Если $k > 1$, получим $g_2 \cdots g_k = (wh_2) \cdots h_m$. Степень многочлена $f_1 := \dfrac{f}{g_1}$ меньше $\deg f = n$, а значит, к его разложениям $f_1 = g_2 \cdots g_k = (wh_2) \cdots h_m$ применимо предположение индукции. Отсюда $k - 1 = m - 1$, т.е. $k = m$, и для каждого из многочленов $g_2, \ldots, g_k$ найдется ассоциированный с ним многочлен среди $(wh_2), \ldots, h_m$. □

Пьер Ферма́ (1601–1665) написал на полях своего экземпляра латинского перевода «Арифметики» Диофанта (греческого математика III века н.э.): «Наоборот, невозможно разложить куб на два куба, биквадрат на два биквадрата и вообще никакую степень, большую квадрата, на две степени с тем же показателем. Я нашёл этому поистине чудесное доказательство, но поля книги слишком узки для него.»
В привычных нам обозначениях Ферма утверждает, что при $n \geq 3$

$$x^n + y^n = z^n$$

не имеет решений в целых числах. Это — так называемая «*Великая*» или «*Последняя*» *теорема Ферма*. Исходя из того круга идей, которыми владел Ферма, понятно, что его «чудесное доказательство» основывалось на разложении левой части

$$x^n + y^n = (x+y)(x+\varepsilon y)(x+\varepsilon^2 y)\cdots(x+\varepsilon^{n-1} y),$$

где ε – корень n-й степени из -1, и на (само собой разумеющейся в те времена) однозначности разложения на неразложимые множители в $\mathbb{Z}[\varepsilon]$. Однако на самом деле при $n \geq 23$ однозначности **нет** (Куммер).

Вернуться обратно