Тема I: Многочлены

§4. Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Z}$

М.В.Волков

Уральский федеральный университет

Институт естественных наук и математики

кафедра алгебры и фундаментальной информатики

2021/2022 учебный год

Постановка задачи

В кольце многочленов над полем каждый многочлен степени ≥ 1 однозначно представи́м как произведение неприводимых многочленов. Приводимость/неприводимость данного многочлена зависит от поля!

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:

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

В этой лекции обсуждается, какие многочлены неприводимы над знакомыми нам полями $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$, а также над кольцом $\mathbb{Z}$.

Начнем с простых замечаний о многочленах над произвольным полем.

Теорема Безу

Пусть $f(x)$ – многочлен над полем F и $\alpha \in F$. Остаток от деления $f(x)$ на $x - \alpha$ равен $f(\alpha)$.

Доказательство. Обозначим частное и остаток от деления $f(x)$ на $x - \alpha$ через $q(x)$ и $r(x)$ соответственно. Тогда $f(x) = q(x)(x - \alpha) + r(x)$, где $\deg r < \deg(x - \alpha)$. Последнее означает, что $\deg r \leqslant 0$, т.е. $r \in F$. Подставив α вместо x в равенство $f(x) = q(x)(x - \alpha) + r(x)$, имеем $f(\alpha) = q(\alpha) \cdot 0 + r$, откуда $r = f(\alpha)$. □

Определение

Пусть $f(x)$ — многочлен над полем F. Элемент $\alpha \in F$ называется *корнем* многочлена $f(x)$, если $f(\alpha) = 0$ (другими словами, если α – корень уравнения $f(x) = 0$).

Из теоремы Безу вытекает простое, на важное

Следствие

Пусть $f(x)$ — многочлен над полем F и $\alpha \in F$. Элемент α является корнем многочлена $f(x)$ тогда и только тогда, когда $(x - \alpha) | f(x)$.

Доказательство. Необходимость. В силу теоремы Безу,

$$f(x) = q(x)(x - \alpha) + f(\alpha)$$

для некоторого многочлена $q(x)$. Если α — корень многочлена $f(x)$, то $f(\alpha) = 0$, и потому $f(x) = q(x)(x - \alpha)$.

Достаточность. Если $(x - \alpha) | f(x)$, то $f(x) = q(x)(x - \alpha)$ для некоторого многочлена $q(x)$, откуда

$$f(\alpha) = q(\alpha)(\alpha - \alpha) = q(\alpha) \cdot 0 = 0.$$

□

Корни многочленов над $\mathbb{C}$

Уже упоминалась *основная теорема алгебры комплексных чисел* – в $\mathbb{C}$ есть корни у любого уравнения $f(x) = 0$, где $f(x)$ – многочлен положительной степени с комплексными коэффициентами.

Теперь ее можно переформулировать так:

Основная теорема алгебры комплексных чисел

Любой многочлен положительной степени над полем $\mathbb{C}$ имеет по крайней мере один комплексный корень.

Доказательство мы дадим позднее, а пока применим эту теорему для классификации неприводимых многочленов над полем $\mathbb{C}$.

Многочлены степени 1 называются *линейными двучленами*.

Теорема (классификация неприводимых многочленов над $\mathbb{C}$)

Неприводимыми многочленами над полем $\mathbb{C}$ являются линейные двучлены и только они.

Доказательство. Очевидно, что линейные двучлены неприводимы.

Обратно, пусть f – многочлен, неприводимый над $\mathbb{C}$, и пусть α – его корень. По следствию из теоремы Безу $f = (x - \alpha)g$ для некоторого многочлена g, и из неприводимости f следует, что f и $x - \alpha$ ассоциированы, т.е. f – линейный двучлен. □

Следствие (разложение многочленов над $\mathbb{C}$)

Любой многочлен степени $n > 0$ над полем $\mathbb{C}$ однозначно представи́м как произведение n линейных множителей.

Чтобы классифицировать неприводимые многочлены над полем $\mathbb{R}$, понадобится следующее замечание.

Лемма (о корнях и комплексной сопряженности)

Если f – многочлен над полем $\mathbb{R}$, а $\gamma \in \mathbb{C}$ – его корень, то и число $\overline{\gamma}$ является корнем многочлена f.

Доказательство. Пусть $f = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$. Тогда $\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \cdots + \alpha_1 \gamma + \alpha_0 = 0$. Используя свойства операции сопряжения и тот факт, что $\overline{\alpha} = \alpha$ для всякого $\alpha \in \mathbb{R}$, получаем:

$$
\begin{aligned}
f(\overline{\gamma}) &= \alpha_n \overline{\gamma}^{\,n} + \alpha_{n-1} \overline{\gamma}^{\,n-1} + \cdots + \alpha_1 \overline{\gamma} + \alpha_0 \\
&= \overline{\alpha_n} \cdot \overline{\gamma}^{\,n} + \overline{\alpha_{n-1}} \cdot \overline{\gamma}^{\,n-1} + \cdots + \overline{\alpha_1} \cdot \overline{\gamma} + \overline{\alpha_0} && \text{так как } \alpha_k \in \mathbb{R} \\
&= \overline{\alpha_n} \cdot \overline{\gamma^n} + \overline{\alpha_{n-1}} \cdot \overline{\gamma^{n-1}} + \cdots + \overline{\alpha_1} \cdot \overline{\gamma} + \overline{\alpha_0} && \text{так как } \overline{\gamma}^{\,k} = \overline{\gamma^k} \\
&= \overline{\alpha_n \gamma^n} + \overline{\alpha_{n-1} \gamma^{n-1}} + \cdots + \overline{\alpha_1 \gamma} + \overline{\alpha_0} && \text{так как } \overline{z}\overline{t} = \overline{zt} \\
&= \overline{\alpha_n \gamma^n + \alpha_{n-1} \gamma^{n-1} + \cdots + \alpha_1 \gamma + \alpha_0} = \overline{0} = 0 && \text{так как } \overline{z} + \overline{t} = \overline{z+t}.
\end{aligned}
$$

□

Теорема (классификация неприводимых многочленов над $\mathbb{R}$)

Неприводимы над полем $\mathbb{R}$ линейные двучлены и квадратные трехчлены с отрицательными дискриминантами и только они.

Доказательство. Линейные двучлены неприводимы над любым полем, а квадратные трехчлены с отрицательными дискриминантами неприводимы над $\mathbb{R}$, поскольку не имеют действительных корней.

Обратно, пусть f – многочлен, неприводимый над $\mathbb{R}$, и пусть $\alpha \in \mathbb{C}$ – его корень. Если $\alpha \in \mathbb{R}$, то по следствию из теоремы Безу $f = (x-\alpha)g$ для некоторого $g \in \mathbb{R}[x]$, и из неприводимости f следует, что f и $x-\alpha$ ассоциированы, т.е. f – линейный двучлен. Если $\alpha \notin \mathbb{R}$, то $\overline{\alpha} \neq \alpha$ и по лемме $\overline{\alpha}$ также является корнем многочлена f. По следствию из теоремы Безу многочлен f делится в $\mathbb{C}[x]$ и на $x-\alpha$, и на $x-\overline{\alpha}$. Двучлены $x-\alpha$ и $x-\overline{\alpha}$ взаимно просты, откуда f делится на их произведение

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2(\operatorname{Re}\alpha)x + |\alpha|^2 \in \mathbb{R}[x].$$

Дискриминант трехчлена $p := x^2 - 2(\operatorname{Re}\alpha)x + |\alpha|^2$ отрицателен: $4(\operatorname{Re}\alpha)^2 - 4((\operatorname{Re}\alpha)^2 + (\operatorname{Im}\alpha)^2) = -4(\operatorname{Im}\alpha)^2 < 0$, поскольку $\operatorname{Im}\alpha \neq 0$. Из неприводимости f следует, что $f \sim p$, т.е. f – квадратный трехчлен. □

Разложение многочленов над $\mathbb{R}$

Комбинируя классификацию неприводимых многочленов над $\mathbb{R}$ с теоремой об однозначности разложения многочлена на неприводимые множители получаем важное следствие.

Следствие (разложение многочленов над $\mathbb{R}$)

Любой многочлен степени $n > 0$ над полем $\mathbb{R}$ однозначно представи́м как произведение $k \leq \lfloor \frac{n}{2} \rfloor$ квадратных трехчленов с отрицательными дискриминантами и $n - 2k$ линейных двучленов.

Довольно поучительно заметить, что этот факт «100% действительный» в том смысле, что в нем речь идет только о действительных многочленах и для его **формулировки** комплексные числа не нужны.

При этом любое **доказательство** этого утверждения существенно использует комплексные числа. На самом деле, мы увидим, что это следствие эквивалентно основной теореме алгебры комплексных чисел.

Простейшие дроби над $\mathbb{R}$

Напомним, что *простейшей* называется рациональная дробь вида $\frac{f}{p^n}$, где p – неприводимый многочлен, а $\deg f < \deg p$.

С учетом классификации неприводимых многочленов над $\mathbb{R}$ получаем классификацию простейших дробей над $\mathbb{R}$:

Следствие (простейшие дроби над $\mathbb{R}$)

Следующие дроби из $\mathbb{R}(x)$ и только они являются простейшими:

- $\frac{A}{x-c}^n$;
- $\frac{Ax+B}{(x^2+px+q)^n}$, *где* $p^2-4q<0$.

Неприводимые многочлены над $\mathbb{Z}$

Напомним, что примитивный многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$ тогда и только тогда, когда этот многочлен неприводим над полем $\mathbb{Q}$ (одно из следствий леммы Гаусса).

Следующее утверждение дает полезное *достаточное* условие неприводимости многочлена над $\mathbb{Z}$, которое по традиции называется *критерием Эйзенштейна*. Так же, как морская свинка – не морская и не свинка, критерий Эйзенштейна – не критерий (в общепринятом в математике смысле) и не Эйзенштейна (был впервые опубликован Теодором Шёнеманом в 1846 г., т.е. за 4 года до публикации Фердинанда Готтхольда Макса Эйзенштейна (1823–1852) в том же самом журнале).

Критерий Эйзенштейна

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ – многочлен с целыми коэффициентами. Если существует такое простое число p, что старший коэффициент a_n не делится на p, все остальные коэффициенты $a_{n-1}, \ldots, a_0$ делятся на p, а свободный член a_0 не делится на p^2, то многочлен f неприводим над $\mathbb{Q}$.

Доказательство. От противного. Предположим, что $f = gh$, где $g(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_0$ и $h(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_0$ – многочлены ненулевой степени над $\mathbb{Q}$. Из леммы Гаусса следует, что их можно считать многочленами над $\mathbb{Z}$. Ясно, что $a_0 = b_0 c_0$. Поскольку a_0 делится на p, но не делится на p^2, из простоты числа p вытекает, что p делит одно из чисел b_0 и c_0, но не оба одновременно. Предположим, что p делит b_0, но не делит c_0. Если p делит все коэффициенты многочлена g, то оно делит и все коэффициенты многочлена f, включая a_n. Следовательно, существует индекс i такой, что p не делит b_i. Пусть i – минимальный индекс с таким свойством. Ясно, что $\deg g < \deg f$, и потому $i \leq k < n$. В частности, p делит a_i. По определению произведения многочленов имеем

$$a_i = b_i c_0 + b_{i-1} c_1 + b_{i-2} c_2 + \cdots .$$

Поскольку p делит a_i и b_j для всех $j < i$, из этого равенства вытекает, что p делит $b_i c_0$. Но это невозможно, так как p не делит ни b_i, ни c_0. □

Критерий Эйзенштейна: комментарии

Критерий Эйзенштейна показывает, что с точки зрения строения неприводимых многочленов поле $\mathbb{Q}$ разительно отличается от $\mathbb{R}$ и $\mathbb{C}$.
В самом деле, всякий неприводимый над $\mathbb{C}$ многочлен линеен, а всякий неприводимый над $\mathbb{R}$ многочлен имеет степень $\leqslant 2$.
В то же время в силу критерия Эйзенштейна степень неприводимого над $\mathbb{Q}$ многочлена может быть любой. Например, неприводимым над $\mathbb{Q}$ является многочлен $x^n - 2$, где n — произвольное натуральное число.

Критерий Эйзенштейна не является *необходимым* для неприводимости многочлена над $\mathbb{Q}$. Для примера рассмотрим $f(x) = x^3 + 4$. Единственное простое число, которое делит свободный член многочлена $f(x)$, – это 2, и свободный член $f(x)$ делится на 2^2. Поэтому критерий Эйзенштейна к многочлену $f(x)$ не применим.Тем не менее, $f(x)$ неприводим.

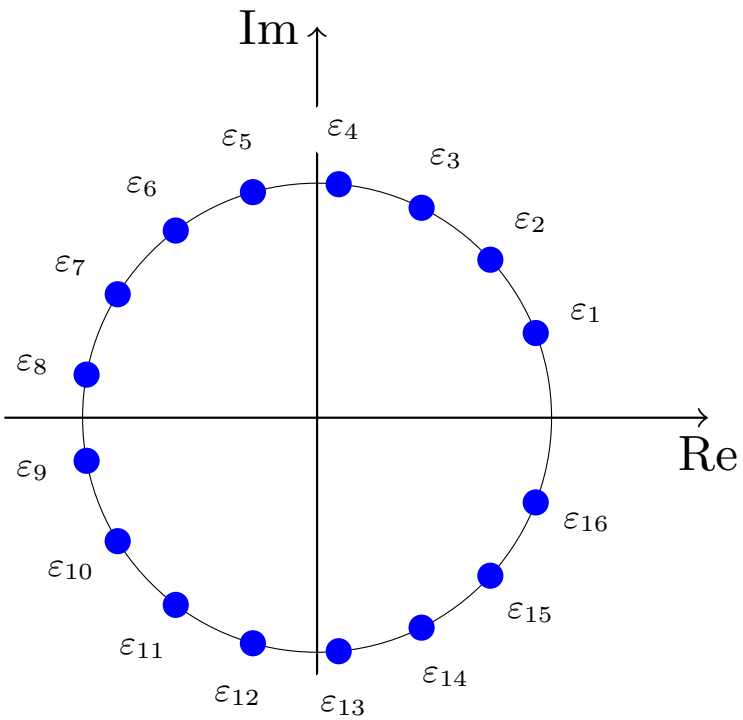
Действительно, если $f(x) = g(x)h(x)$ для некоторых $g(x), h(x) \in \mathbb{Z}[x]$, то $f(x-1) = g(x-1)h(x-1)$, т.е. если $f(x)$ приводим, то и $f(x-1)$ таков. Но

$$f(x-1) = (x-1)^3 + 4 = x^3 - 3x^2 + 3x - 1 + 4 = x^3 - 3x^2 + 3x + 3,$$

и применим критерий Эйзенштейна с $p = 3$. Значит, и $f(x)$ неприводим.

Использованный только что прием позволяет доказать неприводимость *многочлена деления круга* $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$, где p – простое.

Название объясняется равенством $f(x) = \dfrac{x^p - 1}{x - 1}$, из которого видно, что корни $f(x)$ суть комплексные корни p-й степени из 1, т.е. все вершины правильного p-угольника, вписанного в окружность $|z| = 1$, кроме (1,0).



Корни многочлена деления круга 16-й степени

Неприводимость многочлена деления круга (2)

Действительно, если $f(x) = g(x)h(x)$ для некоторых $g(x), h(x) \in \mathbb{Z}[x]$, то $f(x+1) = g(x+1)h(x+1)$, т.е. если $f(x)$ приводим, то и $f(x+1)$ таков. Однако

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + C_p^1 x^{p-2} + \cdots + C_p^{p-1}.$$

Здесь все коэффициенты, кроме старшего, делятся на p, так как p – простое число, которое присутствует в числителе коэффициента

$$C_p^k = \frac{p(p-1)\cdots(p-k+1)}{k!},$$

но отсутствует в его знаменателе (ведь $k < p$). Свободный член $C_p^{p-1} = p$ не делится на p^2, поэтому по критерию Эйзенштейна многочлен $f(x+1)$ неприводим. Значит, и многочлен деления круга неприводим.

Обобщенный критерий Эйзенштейна

Мы доказали критерий Эйзенштейна для многочленов с целыми коэффициентами, но то же доказательство проходит без изменений для многочленов над любой областью с однозначным разложением.

В качестве примера рассмотрим многочлен $x^2 + y^2 + 1 \in \mathbb{Z}[x, y]$. Его можно мыслить как элемент кольца $\mathbb{Z}[y][x]$ многочленов от x с коэффициентами из ООР $D = \mathbb{Z}[y]$. Свободный член $x^2 + y^2 + 1$ как многочлена от x есть $p := y^2 + 1$. Элемент p неразложим в D, и обобщенный критерий Эйзенштейна применим к $x^2 + p = x^2 + y^2 + 1$. Итак, многочлен $x^2 + y^2 + 1$ неприводим в $\mathbb{Z}[x, y]$.

Как же узнать, приводим ли данный многочлен над $\mathbb{Z}$, если критерий Эйзенштейна к нему неприменим? Есть концептуально простая процедура, которую принято называть *алгоритмом Кронекера*. Алгоритм впервые опубликовал Фридрих Теодор фон Шуберт (aka Фёдор Иванович Шуберт, 1758–1825) в 1793 г. в трудах С.-Петербургской академии наук. Леопольд Кронекер переоткрыл тот же самый алгоритм в 1882 г.

Пусть $f(x) \in \mathbb{Z}[x]$ имеет степень n. Если $f(x) = g(x)h(x)$ для некоторых $g(x), h(x) \in \mathbb{Z}[x]$, то один из многочленов $g(x), h(x)$ имеет степень $\leqslant \lfloor \frac{n}{2} \rfloor$. Пусть $\deg g(x) \leqslant \lfloor \frac{n}{2} \rfloor$; тогда $g(x)$ определяется значениями в $m := \lfloor \frac{n}{2} \rfloor + 1$ различных точках. Рассмотрим m различных целых чисел a_i, $i = 1, \ldots, m$, и подсчитаем $f(a_i)$. Если $f(a_i) = 0$ для какого-то i, то $(x - a_i) | f(x)$. Если $f(a_i) \neq 0$ для всех i, из равенств $f(a_i) = g(a_i)h(a_i)$ имеем $g(a_i) | f(a_i)$ в $\mathbb{Z}$. Поскольку числа $f(a_i)$ имеют конечное число целых делителей, можно перебрать всевозможные наборы значений для $g(a_i)$. По каждому такому набору строим интерполяционный многочлен степени $< m$ и проверяем, делит ли он $f(x)$. Если делит, то $f(x)$ приводим, а если ни один из таких «кандидатов в делители» не делит $f(x)$, то многочлен $f(x)$ неприводим.

Алгоритм Кронекера – пример

Рассмотрим $f(x) = x^5 - x^4 - 2x^3 - 8x^2 + 6x - 1$. Если многочлен $f(x)$ приводим, то он имеет делитель $g(x)$ степени $\leqslant 2$. Такой делитель определяется значениями в 3 точках. Подсчитаем $f(0) = -1$, $f(1) = -5$, $f(2) = -21$. Делители этих чисел: для первого ± 1, для второго ± 1, ± 5, для третьего ± 1, ± 3, ± 7, ± 21. Всего получается $2 \cdot 4 \cdot 8 = 64$ комбинации. Комбинации, отличающиеся лишь знаком, дают интерполяционные многочлены, отличающиеся лишь знаком, поэтому из каждой пары таких «противоположных» комбинаций можно проверять одну.
Остаются 32 случая, перебирая которые, найдем многочлен

$$g(x) = x^2 - 3x + 1,$$

делящий $f(x)$; этот делитель соответствует тройке значений

$$(g(0), g(1), g(2)) = (1, -1, -1).$$

Понятно, что «вручную» алгоритм Кронекера использовать трудно, так как уже для многочленов небольших степеней перебор становится очень утомительным. Сейчас имеются намного более эффективные алгоритмы, которые позволяют быстро разлагать на множители многочлены степени более 1000 с более чем 1000-значными коэффициентами.