Лекция 18.

Гайфуллин Сергей Александрович

МГУ

26 ноября, 2021

Следствие

Любой многочлен $f \in \mathbb{C}[z]$ степени n раскладывается на линейные множители и имеет ровно n корней с учетом кратностей.

Предложение

Пусть z – комплексный корень многочлена $f(x) \in \mathbb{R}[x]$. Тогда $\overline{z}$ – также корень f.

Следствие

Любой многочлен с вещественными коэффициентами раскладывается в произведение линейных и квадратичных с отрицательным дискриминантом множителей.

Доказательство. Индукция по степени многочлена. База $\deg f = 0$ и $\deg f = 1$ очевидна. Пусть $f(x) \in \mathbb{R}[x]$. Если $f(x)$ имеет вещественный корень c, то $f(x) = (x - c)g(x)$, при этом $\deg g < \deg f$ и к g можно применить предположение индукции.

Пусть теперь у $f(x)$ есть комплексный корень λ. Тогда $\overline{\lambda}$ – также корень $f(x)$. Значит, $f(x) = (x - \lambda)(x - \overline{\lambda})h(x)$. При этом $(x - \lambda)(x - \overline{\lambda}) = x^2 - 2\mathrm{Re}\lambda + |\lambda|^2$. При этом дискриминант равен $D = 4(\mathrm{Re}\lambda)^2 - 4|\lambda|^2 < 0$. К $h(x)$ можно применить предположение индукции.

Формальное и функциональное равенство многочленов

Формальное равенство многочленов – это совпадение всех коэффициентов. Функциональное равенство многочленов – это совпадение значений при подставлении всех возможных аргументов. Из формального равенства всегда следует функциональное.

Теорема

Пусть R – бесконечная область целостности (например, бесконечное поле). И пусть $f, g \in R[x]$. Если для каждого $r \in R$ выполнено $f(r) = g(r)$, то f и g формально равны.

Доказательство. Рассмотрим $h(x) = f(x) - g(x)$. Для каждого $r \in R$ выполнено $h(r) = 0$. То есть у $h(x)$ есть бесконечное число корней. Однако, мы доказывали, что число корней многочлена над областью целостности не превосходит его степени. Противоречие.

Замечание.

Если R – конечная область целостности, то существует многочлен

$$h(x) = \prod_{r \in R} (x - r),$$

который в каждой точке обращается в ноль, но имеет ненулевые коэффициенты (например, коэффициент при $x^{|R|}$ равен 1). Следовательно, для каждого многочлена $f(x)$ все многочлены вида $f(x) + h(x)s(x)$ функционально равны. Например, если $R = \mathbb{Z}_2$, то $h(x) = x(x-1) = x^2 - x$. Таким образом $x^{m+2} = x^m(x^2 - x) = x^{m+2} - x^{m+1}$. То есть все степени $x^n, n \geq 1$ функционально равны. В самом деле, $x^n(0) = 0$, $x^n(1) = 1$.

Равенство $f(x) = g(x)$ мы будем использовать для формального равенства многочленов.

Далее мы переходим к многочленам над полем F.

Деление с остатком.

Теорема

Пусть F – поле и $f, g \in F[x]$. При этом $g \neq 0$. Тогда существуют единственные многочлены $q, r \in F[x]$ такие, что $f = gq + r$ и либо $\deg r < \deg g$, либо $r = 0$.

Доказательство. Если $f = 0$, то $q = 0$, $r = 0$. Единственность очевидна.
Если $\deg f < \deg g$, то $q = 0$, $r = f$. Единственность очевидна.
Пусть $\deg f \geq \deg g$. Индукция по $\deg f$. Базой является сказанное выше, то есть случаи $\deg f < \deg g$ и $f = 0$.
Шаг индукции. Пусть $f(x) = a_n x^n + \ldots + a_0$,
$g(x) = b_m x^m + \ldots + b_0$. Рассмотрим многочлен

$$\widetilde{f} = f - \frac{a_n}{b_m} x^{n-m} g.$$

Имеем, $\deg \widetilde{f} < \deg f$. Применим предположение индукции.

Продолжение доказательства.

$$\widetilde{f} = f - \frac{a_n}{b_m} x^{n-m} g.$$

По предположению индукции существуют единственные $\widetilde{q}$ и r такие, что $\widetilde{f} = \widetilde{q}g + r$ и $\deg r < \deg g$ или $r = 0$. Тогда

$$f = \left(\widetilde{q} + \frac{a_n}{b_m} x^{n-m} \right) g + r.$$

Если же есть другое представление $f = Qg + R$ с указанными свойствами, то

$$\widetilde{f} = \left(Q - \frac{a_n}{b_m} x^{n-m} \right) g + R,$$

что противоречит единственности деления для $\widetilde{f}$.

Если остаток при делении f на g равен нулю, будем писать $g|f$. При этом выполняется $f = 0$ или $\deg f \geq \deg g$.

Определение.

Пусть $f, g \in F[x] \setminus \{0\}$. Наибольший общий делитель многочленов f и g называется многочлен h такой, что $h|f$, $h|g$ и h имеет максимальную степень среди многочленов с такими свойствами.

Из определения очевидно существование, но единственность не очевидна. Более того, ясно, что если h является НОД f и g, то λh, $\lambda \neq 0 \in F$ тоже НОД этих многочленов. Таким образом НОД определен как минимум с точностью до умножения на ненулевую константу (на самом деле в точности с точностью до умножения на ненулевую константу и мы это скоро докажем). Чтобы избежать этой неоднозначности иногда фиксируют, что старший коэффициент НОД равен 1.
НОД($f \neq 0$, 0)=f. НОД(0,0) не определен.

Алгоритм Евклида.

Сейчас наша цель – построить один из возможных НОД двух многочленов, исследовать его и доказать, что он единственный (с точностью до умножения на ненулевую константу, конечно).

Лемма.

Пусть $f, g, u, v, a, b, c, d \in F[x]$. И пусть для матрицы

$$\begin{pmatrix} u & a & b \\ v & c & d \end{pmatrix}$$

выполнено $u = af + bg$, $v = cf + dg$. Тогда аналогичные равенства (будем называть их равенствами $*$) выполняются и для матрицы, полученной из данной элементарным преобразованием строк первого типа (с коэффициентом – многочленом).

Доказательство.

Можно считать, что получена матрица

$$\begin{pmatrix} u+sv & a+sc & b+sd \\ v & c & d \end{pmatrix}, \qquad s \in F[x].$$

Тогда для нижней строки равенство выполнено, так как она не изменилась. Для верхней строки:

$$u+sv = (af+bg)+s(cf+dg) = (a+sc)f+(b+sd)g.$$

Рассмотрим следующий алгоритм. Стартуем с матрицы

$$\begin{pmatrix} f & 1 & 0 \\ g & 0 & 1 \end{pmatrix}.$$

Если в текущий момент времени у нас матрица

$$\begin{pmatrix} u & a & b \\ v & c & d \end{pmatrix},$$

и $\deg u \geq \deg v$, то делим u на v с остатком: $u = qv + r$. После этого прибавляем вторую строку к первой с коэффициентом $-q$. Получаем

$$\begin{pmatrix} r & a - qc & b - qd \\ v & c & d \end{pmatrix}.$$

Если $\deg u < \deg v$, то делаем симметричную операцию (делим v на u с остатком и т.д.) При такой операции сумма $\deg u + \deg v$ уменьшается. Так мы действуем пока один из многочленов в первом столбце не станет равен нулю. При этом другая строка будет $(\varphi(x), \alpha(x), \beta(x))$.

Теорема

1) $\varphi | f$ и $\varphi | g$.
2) Пусть $h | f$ и $h | g$. Тогда $h | \varphi$.

Доказательство. 1) Все элементарные преобразования обратимы. Пройдем обратно элементарными преобразованиями от матрицы с первым столбцом $\begin{pmatrix} \varphi \\ 0 \end{pmatrix}$ до матрицы с первым столбцом $\begin{pmatrix} f \\ g \end{pmatrix}$. Докажем по индукции, что после k шагов оба многочлена в первом столбце делятся на φ. База $k = 0$, шаг очевиден.
2) Имеем $\varphi = \alpha f + \beta g$ по равенствам $*$. Так как $h | f$ и $h | g$, получаем $h | \varphi$.

Итак, мы получили общий делитель φ многочленов f и g, который делится на все общие делители. Из этого следует, что он максимальной степени. То есть $\varphi = \text{НОД}(f, g)$. С другой стороны, пусть $\deg h = \deg \varphi$ и h – общий делитель f и g. Тогда $\varphi | h$. Следовательно $h = \lambda\varphi$, $\lambda \in F \setminus \{0\}$. Итак, мы доказали следующую теорему.

Теорема

1) В результате алгоритма Евклида получается $\text{НОД}(f, g)$.
2) $\text{НОД}(f, g)$ определен однозначно с точностью до умножения на ненулевую константу.
3) $\text{НОД}(f, g)$ представим в виде линейной комбинации начальных многочленов, то есть

$$\text{НОД}(f, g) = \alpha f + \beta g, \qquad \alpha, \beta \in F[x].$$

Определение

Пусть R – целостное кольцо. Два элемента a и b из R называются ассоциированными, если $a = bc$, где c – обратимый элемент R. (При этом $b = ac^{-1}$.)

Заметим, что обратимый элемент $F[x]$ – это ненулевая константа, поэтому можно говорить, что НОД определен с точностью до ассоциированности.

Определение

Необратимый элемент $r \neq 0 \in R$ целостного кольца называется неприводимым, если из $r = ab$ следует, что либо a, либо b обратим.

Лемма

В кольце $F[x]$ многочлен степени 1 всегда неприводим.

Доказательство. Этот многочлен ненулевой, необратим и если его разложить на два множителя, то один из них – ненулевая константа, то есть обратим.

Теорема

Неприводимые элементы в $\mathbb{C}[x]$ – это только линейные многочлены.

Доказательство. Любой многочлен нулевой степени обратим. Линейные неприводимы. А если $\deg f \geq 2$, то f разлагается на линейные множители и следовательно, не является неприводимым.

Теорема

Неприводимые элементы в $\mathbb{R}[x]$ – это линейные многочлены и квадратичные многочлены с отрицательным дискриминантом.

Доказательство. Любой многочлен нулевой степени обратим. Линейные неприводимы. Если квадратичный имеет неотрицательный дискриминант, то он раскладывается в произведение двух линейных, и значит, не неприводим. Если $\deg f \geq 3$, то f раскладывается в произведение линейных и квадратичных с отрицательным дискриминантом. Следовательно, не является неприводимым.

Определение

Ненулевой необратимый элемент p целостного кольца называется простым, если из $p|ab$ следует $p|a$ или $p|b$.

Теорема

В кольце $F[x]$ любой неприводимый элемент является простым.

Доказательство. Пусть p – неприводимый элемент. Пусть $p|ab$. Если $p|a$, то все доказано. Пусть p не делит a. Тогда НОД$(p, a) = 1$. В самом деле, пусть НОД$(p, a) = d$. Тогда $p = dc$. Так как p неприводим, то либо c обратим, либо d обратим (и тогда считаем $d = 1$). Если обратим c, то $p|d$, $d|a$ и $p|a$. Противоречие. Итак, НОД$(p, a) = 1$. Тогда найдутся такие многочлены u и v, что $1 = ua + vp$. Тогда $b = uab + vbp$ делится на p.

Определение

Целостное кольцо R называется факториальным, если любой элемент r представим в виде конечного произведения неприводимых: $r = p_1 \dots p_n$, причем это разложение единственно с точностью до перестановки и ассоциированности множителей.

Теорема

Кольцо $F[x]$ факториально.

Доказательство. Существование разложения на неприводимые очевидно (разлагаем и когда-то остановимся). Пусть есть два разложения $p_1 \dots p_m = q_1 \dots q_n$ на неприводимые. Докажем индукцией по m, что $m = n$ и каждый p_i ассоциирован с некоторым q_j. База $n = 1$ очевидна. Шаг индукции. Так как p_m прост, существует j такое, что $p_m | q_j$. Так как q_j неприводим, они ассоциированы. Следовательно, $p_m = \lambda q_j$. Так как кольцо целостно, $p_1 \dots p_{m-1} = \lambda \prod_{i \neq j} q_i$. Применяем предположение индукции.