Лекция 19

Пусть $f = a_n x^n + \ldots + a_0 \in R[x]$ – многочлен с коэффициентами из области целостности R. В этот многочлен можно подставлять элементы из R и тогда значение многочлена будет лежать также в R. Таким образом любой многочлен f задаёт функцию $R \to R$. Обозначим эту функцию φ_f. Легко видеть, что отображение $f \to \varphi_f$ – гомоморфизм, то есть при сложении многочленов функции также складываются, а при умножении многочленов – умножаются. Однако данный гомоморфизм из пространства многочленов в пространство функций может быть не инъективным. В самом деле, если R – конечная область целостности, то многочлен

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

задаёт тождественно нулевую функцию $R \to R$, хотя сам многочлен не нулевой.

Пример 1. *Пусть p – простое число. По малой теореме Ферма многочлены x^p и x задают одну и ту же функцию на поле $\mathbb{Z}_p$.*

Таким образом стоит различать формальное равенство многочленов (все коэффициенты одинаковые) и функциональное равенство многочленов (задают одну и ту же функцию). Конечно же из формального равенства всегда следует функциональное. Обратное, как мы видели, не верно. Однако для бесконечных областей целостности это верно.

Теорема 1. *Пусть R – бесконечная область целостности. Тогда из функционального равенства многочленов из $R[x]$ следует формальное равенство.*

Доказательство. Пусть два не равных формально многочлена f и g из $R[x]$ функционально равны. Рассмотрим их расность. Это многочлен $h(x) = f(x) - g(x)$ с ненулевыми коэффициентами, задающий тождественно нулевую функцию. Пусть степень f равна m. Возьмём различные элементы $c_1, \ldots, c_m \in R$. Так как $h(c_1) = 0$, мы получаем $h(x) = (x - c_1)h_1(x)$. Подставим в это выражение c_2, получим $0 = h(c_2) = (c_2 - c_1)h_1(c_2)$. Так как $c_1 \neq c_2$ и R без делителей нуля, получаем $h_1(c_2) = 0$. Тогда $h(x) = (x - c_1)(x - c_2)h_2(x)$. Продолжая таким образом, получим $h(x) = a_n(x - c_1)\ldots(x - c_n)$. Но подставив c_{n+1} в это выражение, мы не получим ноль. Противоречие. □

Далее мы переходим к изучению многочленов над полем F.

Определение 1. Наибольший общий делитель (НОД) двух многочленов – это многочлден, который является их общим делителем максимальной степени.

Ясно, что по данному определению НОД двух многочленов определён не совсем однозначно. Его как минимум можно умножать на ненулевые константы. Однако хотелось бы доказать, что НОД определён однозначно с точностью до умножения на ненулевую константу. Мы скоро это докажем.

Приведём здесь алгоритм Евклида. Через некоторое время мы докажем, что результатом его работы является НОД.

Алгоритм Евклида Пусть нам даны 2 многочлена $f, g \in F[x]$ (хотя бы 1 из них ненулевой). Составим следующую матрицу

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

Далее будем делать с этой матрицей элементарные преобразования столбцов 1 типа с коэффициентами многочленами. Наша цель – получить в верхней строке на одном из мест ноль. А именно, мы будем делать следующие операции: рассматриваем (ненулевые, иначе мы уже закончили выполнение алгоритма) многочлены, стоящие в верхней строке, пусть это на некотором шаге $s(x)$ и $t(x)$. Пусть у s степень не меньше, чем у t. Разделим s на t с остатком. Получим $s(x) = q(x)t(x) + r(x)$. Вычтем 2-ой столбец матрицы из 1-го с коэффициентом $q(x)$. Это и будет шагом алгоритма. При этом на месте $(1, 1)$ в нашей матрице появится $r(x)$. Когда мы получим в одном из мест 1-ой строки ноль, мы в ответ выдаём элементы другого столбца: $\begin{pmatrix} d(x) \\ u(x) \\ v(x) \end{pmatrix}$. Алгоритм закончен.

Лемма 1. *На каждом этапе алгоритма Евклида в каждорм столбце матрицы* $\begin{pmatrix} a(x) \\ b(x) \\ c(x) \end{pmatrix}$ *выполнено равенство* $a(x) = b(x)f(x) + c(x)g(x)$.

Доказательство. Докажем это утверждение по индукции по количеству шагов алгоритма, приводящих к данной матрице.

База индукции. Для начальной матрицы

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

данное свойство выполняется для обоих столбцов.

Шаг индукции. Пусть для некоторой матрицы

$$\begin{pmatrix} s(x) & t(x) \\ l_1(x) & l_2(x) \\ p_1(x) & p_2(x) \end{pmatrix}$$

данные условия выполняются. То есть $s(x) = l_1(x)f(x) + p_1(x)g(x)$, $t(x) = l_2(x)f(x) + p_2(x)g(x)$. Сделаем элементарное преобразование столбцов. Например, прибавим 1-й столбец ко 2-му с коэффициентом $q(x)$. Первый столбец не поменяется, поэтому для него условие будет выпролнено. Второй столбец станет

$$\begin{pmatrix} t + qs \\ l_2 + ql_1 \\ p_2 + qp_1 \end{pmatrix}.$$

Имеем

$$(l_2 + ql_1)f + (p_2 + qp_1)g = l_2f + p_2g + q(l_1f + l_2g) = t + qs.$$

□

Лемма 2. *Алгоритм Евклида заканчивает работу за конечное число шагов при подаче на вход любой пары не равных нулю одновременно многочленов.*

Доказательство. Заметим, что при каждом шаге алгоритма уменьшается сумма $\deg s + \deg t$, где s и t – многочлены в верхней строке матрицы. Так как эта сумма изначально равнна $\deg f + \deg g$, то есть конечна, число шагов конечно. □

Лемма 3. *Пусть $d(x)$ – это многочлен (верхний из итогового столбца) полученный с помощью алгоритма Евклида. Тогда f делится на d и g делится на d.*

Доказательство. Будем идти от конечной матрицы к начальной (в алгоритме Евклида). И будем доказывать, что элементы верхней строки делятся на $d(x)$ индукцией по количеству m сделанных (обратно) шагов.

База. $m = 0$, верхняя строка состоит из $d(x)$ и 0.

Шаг индукции. Если верхняя строка была (ad, bd) и мы прибавили, например, первый столбец ко второму с коэффициентом c, то получим $(ad, (b + ca)d)$. Оба элемента делятся на d.

Итак, конечная (при движении с конца) верхняя строка имеет вид (f, g) и оба её элемента делятся на d. □

Теорема 2. *Пусть d – многочлен, полученный применением алгоритма Евклида к многочленам f и g. Тогда выполнено*

1) $d(x)$ является НОД $f(x)$ и $g(x)$;

2) Если $h(x)$ – общий делитель $f(x)$ и $g(x)$, то $d(x)$ делится на $h(x)$;

3) Любой НОД $f(x)$ и $g(x)$ имеет вид $\lambda d(x)$, где $\lambda \in F \setminus \{0\}$;

4) Существуют многочлены $u(x)$ и $v(x)$ такие, что $d(x) = u(x)f(x) + v(x)g(x)$.

Доказательство. Пункт 4) следует из леммы 1, применённой к конечной матрице алгоритма Евклида.

2) Если $h \mid f$ и $h \mid g$, то $h \mid uf + vg = d$. (Знак $''\mid''$ означает "делит")

1) Допустим, что $d(x)$ не является НОД $f(x)$ и $g(x)$. Однако, по лемме 3, d является общим делителем $f(x)$ и $g(x)$. Тогда существует общий делитель h многочленов $f(x)$ и $g(x)$ такой, что $\deg h > \deg d$. Однако по пункту 2) выполнено $h \mid d$. Противоречие. Значит, $d(x)$ является НОД $f(x)$ и $g(x)$.

3) Пусть $l(x)$ – другой общий делитель f и g. Тогда $\deg l = \deg d$. По пункту 2) $l \mid d$. Частное d и l имеет степень 0, а значит, является константой. □

Определение 2. Два элемента a и b кольца R с единицей называются *ассоциированными*, если $a = bc$, где c – обратимый элемент R.

Замечание 1. Если $a = bc$, то $b = ac^{-1}$, поэтому отношение ассоциированности симметрично. Так как 1 – обратимый элемент R, отношение ассоциированности рефлексивно. И так как произведение двух обратимых элементов обратимо, данное отношение транзитивно. Получаем, что ассоциированность – отношение эквивалентности и все элементы R распадаются на классы ассоциированности.

Определение 3. Пусть A – область целостности. Тогда ненулевой необратимый элемент $a \in A$ называется *неприводимым*, если из того, что $a = bc$ следует, что либо b, либо c обратим.

Заметим, что обратимые элементы кольца $F[x]$, где F – поле, это ненулевые константы.

Лемма 4. *Пусть F – поле. Элемент $ax + b \in F[x]$, $a \neq 0$ является неприводимым элементом $F[x]$.*

Доказательство. Допустим $ax + b = gh$. Тогда $\deg g + \deg h = 1$. То есть один из многочленов g или h – ненулевая константа, то есть обратимый элемент. □

Теорема 3. *Неприводимые элементы $\mathbb{C}[x]$ – это в точности линейные многочлены.*

Доказательство. Пусть $f(x) \in \mathbb{C}[x]$ – многочлен. Пусть $\deg f = n$. Тогда $f(x) = a(x - c_1) \dots (x - c_n)$. Если $n > 1$, то f можно разложить на произведение $(x - c_1)$ и $a(x - c_2) \dots (x - c_n)$. Оба множителя не обратимы. Значит, f не неприводим. Пусть $\deg f = 0$. Тогда f – либо 0, либо обратимый элемент. Если же $\deg f = 1$, то f – неприводимый многочлен по лемме 4. □

Замечание 2. Легко видеть, что определение неприводимого элемента $F[x]$ можно переговорить так: многочлен над полем F приводим тогда и только тогда, когда он разлагается в произведение многочленов меньшей степени.

Теорема 4. *Неприводимые элементы $\mathbb{R}[x]$ – это в точности линейные многочлены и квадратичные многочлены с отрицательным дискриминантом.*

Доказательство. Пусть $f(x) \in \mathbb{R}[x]$ – многочлен. Пусть $\deg f = n$. Если $n > 2$, то как было доказано ранее, f разлагается в произведение многочленов 1 и 2 степени. Следовательно, f не является неприводимым. Если f – квадратичный многочлен с неотрицательным дискриминантом, то он разлагается на линейные, а следовательно, он приводим. Константа – либо 0, либо обратимый элемент. Остаются только линейные многочлены, которые неприводимы по лемме 4 и квадратичные с отрицательным дискриминантом. Если квадратичный многочлен приводим, он делится на линейный, и следовательно, имеет корень. Таким образом, квадратичные многочлены с отрицательным дискриминантом неприводимы. □

Определение 4. ненулевой необратимый элемент a области целоствности A называется *простым*, если из $a \mid bc$ следует, что $a \mid b$ или $a \mid c$.

Лемма 5. *В кольце $F[x]$, где F – поле, простые и неприводимые элементы совпадают.*

Доказательство. Пусть f – простой многочлен. Допустим, что он приводимый. Тогда $f = gh$, где многочлены g и h имеют меньшую степень. Тогда $f \mid gh$, но $f \nmid g$ и $f \nmid h$. Противоречие.

Пусть теперь f – неприводимый многочлен. И пусть $f \mid gh$. Докажем, что $f \mid g$ или $f \mid h$. Если $f \mid g$, то всё доказано. Иначе НОД(f,g)=1. Следовательноб существуют многочлены u и v такие, что $uf + vg = 1$. Домножим обе части этого равенства на h, получим

$$ufh + vgh = h.$$

Левая часть этого равенства делится на f. Значит, $f \mid h$. Отсюда следует, что f простой. □

Определение 5. Кольцо R называется *факториальным*, если R – это область целостности такая, что любой необратимый элемент $r \in R$ однозначно с точностью до перестановки множителей и ассоциированности множителей разлагается в произведение неприводимых элементов.

Пример 2. *Кольцо $\mathbb{Z}$ факториально. (Это утверждение называется основной теоремой арифметики.) При этом обратимые элементы $\mathbb{Z}$ – это ± 1. Имеем*

$$-6 = 2 \cdot (-3) = (-3 \cdot 2 = 3 \cdot (-2).$$

Всё это одно и то же разложение -6 на неприводимые множители с точностью до перестановки множителей и ассоциированности.

Теорема 5. *Пусть F – поле. Тогда кольцо $F[x]$ факториально.*

Доказательство. Докажем, что любой многочлен можно разложить на неприводимые. Докажем это индукцией по $n = \deg f$.

База индукции. $n = 1$. В этом случае многочлен f неприводим по лемме 4. То есть он разлагается в произведение из одного множителя.

Шаг индукции. Пусть для всех $n < k$ утверждение доказано. Докажем для $n = k$. Возьмём $f \in F[x]$, $\deg f = k$. Если f неприводим, то разложение получено. Иначе $f = gh$, где степени g и h меньше k. Значит, для g и h есть разложения на неприводимые. Перемножив их, получим разложение f на неприводимые.

Теперь докажем единственность разложения. Пусть $f = p_1 \dots p_m = q_1 \dots q_r$ – два разложения f на неприводимые. Тогда p_1 – простой элемент, а значит, из $p_1 \mid (q_1 \dots q_r)$ следует, что найдётся номер j такой, что элемент q_j делится на p_1. Переупорядочив, элементы $q_1, \dots, q_r$, можно считать $j = 1$. Тогда $q_1 = sp_1$. Но q_1 – неприводимый многочлен. Значит, s – ненулевая константа. Можно поделить q_1 на s и умножить q_2 на s, при этом разложение не изменится с точностью до ассоциированности множителей. В таком случае, можно считать $q_1 = p_1$. Имеем

$$0 = p_1 \dots p_m - q_1 \dots q_r = p_1(p_2 \dots p_m - q_2 \dots q_r).$$

Так как R – область целостности и $p_1 \neq 0$, получаем $p_2 \dots p_m = q_2 \dots q_r$. Аналогично рассуждая, получаем, что можно считать $q_2 = p_2$ и $p_3 \dots p_m = q_3 \dots q_r$ и т.д. В итоге получаем, что (с точностью до перестановки и ассоциированности) $m = r$ и $p_i = q_i$ для всех $1 \leq i \leq m$. □

Пример 3. *Приведём пример нефакториального кольца, чтобы не было ощущения, что все кольца факториальны. Рассмотрим*

$$R = \{a_0 + a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{R}, n \in \mathbb{N}\}.$$

R – кольцо многочленов без линейного члена. Несложно видеть, что R – кольцо и более того, область целостности. При этом элементы x^2 и x^3 неприводимы в R. В самом деле, любое разложение, например, X^3 на множители в R является разложением x^3 на множители в $\mathbb{R}[x]$. Значит, оно должно иметь вид $x^2 \cdot x$, но $x \notin R$. При этом

$$x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3$$

это два разных разложения x^6 на неприводимые множители.