141, ДЗ 4, Неприводимые многочлены

Задачи

Задача 1. Доказать неприводимость в $\mathbb{Q}[x]$ многочлена

$$x^5 + 2x^3 + +3x^2 - 6x - 5$$

воспользовавшись редукцией по какому-то модулю.

Задача 2. Доказать неприводимость в $\mathbb{Q}[x]$ многочлена

$$x^5 - 6x^3 + +2x^2 - 4x + 5.$$

Задача 3. Доказать неприводимость в $\mathbb{Q}[x]$ многочлена

$$x^5 - 12^4 + 36x - 12$$

Задача 4. Доказать неприводимость многочлена $x^5 - x + 1$ над полем $\mathbb{F}_5$

Но бывают и другие задачи:

Задача 5. Покажите, что многочлен $(x - a_1) \dots (x - a_n) - 1$ неприводим над $\mathbb{Z}$ при различных целых a_i.

Задача 6. Покажите, что многочлен $x^{105} - 9$ неприводим над $\mathbb{Z}$

Многочлены

Обсудим, что происходит с кольцом целочисленных многочленов и кольцом от многих переменных.

Определение. Пусть $f(x)$ – многочлен над факториальным кольцом R. Тогда содержанием f называется $\mathrm{cont}(f) = $ НОД(a_i), где a_i коэффициенты f.

Тут есть некоторая вольность – надо помнить, что наибольший общий делитель определён с точностью до обратимых множителей. Следующее следствие тоже называют леммой Гаусса.

Лемма 1. Если $f(x) = g(x)h(x)$, где $f, g, h \in R[x]$, то $\mathrm{cont}(f) = \mathrm{cont}(g)\,\mathrm{cont}(h)$

Следующая лемма по существу показывает, что разложение в $R[x]$ и $Q(R)[x]$ по сути одно и тоже.

Лемма 2. Пусть для многочлена $f(x) \in R[x]$ имеет место разложение $f(x) = g(x)h(x)$, где $g(x)h(x) \in Q(R)[x]$. Тогда существуют такая константа $c \in Q(R)$, что $cg \in R[x]$ и $c^{-1}h \in R[x]$, что означает, что $f(x) = cg(x)c^{-1}h(x)$ – есть произведение двух многочленов из $R[x]$ пропорциональных исходным.

Теорема 1. Пусть R – факториальное кольцо. Тогда кольцо $R[x]$ факториально. Более того, имеет место следующее описание простых элементов кольца $R[x]$:
1) $\mathrm{cont}(f) = 1$ и f неприводим в $Q(R)[x]$.
2) $f = p \in R$ – простой в R.

Признаки неприводимости для многочленов

Теперь наша задача поговорить про неприводимость многочленов над целыми числами или над $\mathbb{Q}$. Прежде всего отметим, что обе задачи тесно связаны. А именно, если взять многочлен с рациональными коэффициентами, то домножив его на подходящую рациональную константу мы получим многочлен с целыми коэффициентами и содержанием 1, который по доказанному ранее неприводим тогда и только тогда, когда неприводим исходный. Обратно, неприводимость целочисленных многочленов интересна только в случае, когда содержание этих многочленов равно единице. А в этом случае это эквивалентно рациональной неприводимости. Однако все теоремы я буду формулировать в общем контексте.

Теорема 2 (Редукционный критерий)**.** Пусть R факториальное кольцо, $f \in R[x]$ многочлен, а p – простой элемент. Тогда, если старший коэффициент f не делится на p и $\overline{f}$ неприводим в кольце $R/p[x]$, то он неприводим над $Q(R)$.

Вот примеры о том, как пользоваться этим критерием и что не надо забывать про условие со старшим коэффициентом.

Примеры:

1) Многочлен $x^3 + x + 1$ неприводим над $\mathbb{F}_2 = \mathbb{Z}/2$, потому что у него нет корней. Следовательно многочлены $3x^3 + 8x^2 + 5x + 7$ и скажем, $5x^3 - 4x^2 + x + 15$ неприводимы над $\mathbb{Q}$.

2) Рассмотрим многочлен $px^2 + x$. Он приводим, но по модулю p – неприводим.

3) Критерий из теоремы сформулирован не в самом сильном виде. А именно, представим себе, например, что по модулю 2 многочлен степени пять разложился в произведение двух неприводимых степени 2 и 3, а по модулю 3 – в виде произведения степени 4 и 1. Ясно, что он неприводим.

4) Не стоит забывать, что если многочлен неприводим над $\mathbb{R}$, то он так же неприводим над $\mathbb{Q}$. Это, правда, очень слабый критерий, но в комбинации с пунктом 3) может что-то дать.

Есть, однако, такие многочлены, которые неприводимы, но раскладываются по модулю любого простого. Например,

$$x^4+1 = (x-e^{\frac{i\pi}{8}})(x-e^{\frac{3i\pi}{8}})(x-e^{\frac{5i\pi}{8}})(x-e^{\frac{7i\pi}{8}}) = (x^2+i)(x^2-i) = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1) = (x^2+\sqrt{-2}x+1)(x^2-\sqrt{-2}x+1).$$

Он не имеет корней, а любые множители степени 2 имеют нерациональный коэффициент. С другой стороны по любому простому модулю либо из -1, либо из 2 либо из -2 извлекается корень.

Покажем теперь некоторый критерий неприводимости, который применим в случае, если разложение по модулю p получилось неудачное. А именно, представим себе, что $f(x) \equiv x^n \bmod p$. То есть развалился в произведение максимально возможного числа одинаковых множителей. Оказывается, что в этом случае неприводимость многочлена f зависит от его класса по модулю p^2. Точнее:

Теорема 3 (Признак Эйзенштейна)**.** Пусть R – факториальное кольцо и $f(x) = a_0 + \cdots + a_n x^n$. Если $a_n \not\vdots p$, все $a_i \vdots p$ $i < n$, но $a_0 \not\vdots p^2$, то многочлен $f(x)$ неприводим.

Всё, что мы пока обсуждали не говорит ничего о том, как же разложить многочлен на неприводимые множители. Обсудим, почему эта задача в принципе разрешима.

Итак, пусть есть целочисленный многочлен $f(x)$ и мы хотим разложить его на множители. Мы будем искать разложение на целочисленные многочлены, заметим, что хотя бы один из них имеет степень меньшую, чем $[\frac{n}{2}]$. Вспомним о задаче интерполяции. Если g – искомый делитель f, то g определяется своими значениями в $[\frac{n}{2}]+1$ точке, например в точках $0, 1, \ldots, [\frac{n}{2}]$. Более того, $f(i) \vdots g(i)$. Таким образом набор $g(0), \ldots, g([\frac{n}{2}])$ состоит из делителей $f(0), \ldots, f([\frac{n}{2}])$. Найти все такие наборы – конечный перебор. По каждому набору значений многочлен g восстанавливается однозначно.

Это очень неэффективный алгоритм разложения многочлена на множители. Он был предложен Кронекером ещё в 19-ом веке. В настоящее время известен полиномиальный алгоритм решения этой задачи.

Прежде чем продвинуться дальше в исследовании разложения многочленов от одной переменной на множители стоит немного поговорить о задаче разложения многочленов от нескольких переменных. Сейчас мы увидим ещё один не трюк от Кронекера, который позволит свести эту задачу к предыдущей.

Теорема 4. Пусть R – кольцо. Тогда различным разложениям $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ соответствуют различные разложения $\hat{f} = f(x, x^d, x^{d^2}, \ldots, x^{d^{n-1}})$ для d больших $\max_{i=1}^{n}\{\deg_{x_i} f\}$.

Доказательство. Пусть $f = g_1 h_1 = g_2 h_2$ и пусть $g_1 \neq g_2$. Покажем, что $\hat{g_1} \neq \hat{g_2}$. Для этого посмотрим что происходит с мономом x^α при указанном преобразовании. Он переходит в многочлен $x^{\alpha_1+\alpha_2 d+\cdots+\alpha_n d^{n-1}}$. По условию все $\alpha_i < d$ как степени при переменных x_i. Тогда моном $x^{\alpha_1+\alpha_2 d+\cdots+\alpha_n d^{n-1}}$ может быть получен только из монома x^α. Заметим теперь, что $\deg_{x_i} g_j \leq \deg f < d$. Следовательно мономы многочленов $g_j(x)$ так же однозначно восстанавливаются по мономам $\hat{g_j}$. □

К сожалению, не стоит ожидать взаимооднозначного соответствия между разложениями многочленов f и $\hat{f}$. Например, многочлен x_2^2 раскладывается на два множителя одним способом. При $d = 3$ его образ есть x^6 у которого 3 различных разложения.