Лекция №6

Тема: Вычисление рациональных корней. Неприводимость многочленов над полем рациональных чисел

План лекции:

1. Теорема Безу для рационального корня многочлена с целыми коэффициентами
2. Теоремы о делимости для многочленов над полем рациональных чисел
3. Теорема о приводимости многочленов второй и третьей степеней
4. Критерий Эйзенштейна
5. Примеры

Литература:

1.Окунев Л. Я. Высшая алгебра. – М.: Изд-во «Просвещение», 1966. – 336. (Параграфы 17-18).

Текст лекции

Частным случаем многочлена (уравнения) с действительными коэффициентами является многочлен (уравнение) с рациональными коэффициентами. Действительные корни такого многочлена могут быть как рациональными, так и иррациональными числами. Вопрос о вычислении иррациональных корней тесно связан с методами приближенного вычисления действительных корней многочленов с действительными коэффициентами. Эти методы излагаются в курсе приближённых вычислений, а здесь мы рассмотрим один из простых способов нахождения рациональных корней. Итак пусть

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (1)$$

—уравнение n-й степени ($n > 1$) с рациональными коэффициентами. Мы будем предполагать, что уравнение (1) имеет целые коэффициенты; в противном случае мы умножили бы обе части уравнения на общий знаменатель коэффициентов и получили бы уравнение с целыми коэффициентами и с теми же корнями, что и первоначальное уравнение.

Предлагаемый вниманию читателей метод вычисления рациональных корней основан на следующей теореме.

Теорема 1. *Если несократимая дробь* $\frac{l}{m}$ (l, m — *целые числа и* $m > 0$) *является рациональным корнем уравнения* (1), *то* l *есть делитель свободного члена* a_n, *а* m — *делитель старшего коэффициента* a_0.

Доказательство. Так как $\frac{l}{m}$ есть корень уравнения (1), то

$$a_0\frac{l^n}{m^n}+a_1\frac{l^{n-1}}{m^{n-1}}+\ldots+a_{n-1}\frac{l}{m}+a_n=0.$$

Умножим обе части этого равенства на m^n:

$$a_0l^n+a_1l^{n-1}m+\ldots+a_{n-1}lm^{n-1}+a_nm^n=0.$$

Отсюда:

$$a_0l^n=-m(a_1l^{n-1}+\ldots+a_nm^{n-1}) \tag{2}$$

и

$$a_nm^n=-l(a_0l^{n-1}+\ldots+a_{n-1}m^{n-1}). \tag{3}$$

Правая часть равенства (2) делится, очевидно, на m. Следовательно, на m должна делиться и левая часть равенства (2), т. е. a_0l^n. Но в силу несократимости дроби $\frac{l}{m}$ число l^n взаимно просто с m. Поэтому a_0 должно делиться на m.

Аналогично рассуждаем и относительно равенства (3). Его правая часть делится на l. Следовательно, a_nm^n должно также делиться на l. Отсюда a_n делится на l, так как m^n взаимно просто с l.

Отметим два следствия из только что доказанной теоремы.

Следствие 1. *Целый корень уравнения* (1) *должен быть делителем свободного члена* a_n.

В самом деле, целый корень l можно представить в виде дроби $\frac{l}{1}$, откуда ясно, что l является делителем a_n.

Следствие 2. *Уравнение*

$$f(x)=x^n+a_1x^{n-1}+\ldots+a_n=0$$

со старшим коэффициентом, равным единице, и с целыми коэффициентами $a_1, \ldots, a_n$ *может иметь в качестве рациональных корней только целые корни.*

Действительно, по теореме 1 знаменатель $m>0$ рационального корня $\frac{l}{m}$ должен быть делителем старшего коэффициента, т. е. равен 1. Отсюда корень $\frac{l}{m}=\frac{l}{1}=l$ является целым.

Таким образом, испытывая всевозможные дроби $\frac{l}{m}$ $(m>0)$ с числителем l, делящим a_n, и со знаменателем m, делящим старший коэффициент a_0, мы найдем рациональные корни уравнения (1) или убедимся, что уравнение (1) не имеет рациональных корней. Однако эти испытания можно значительно сократить, стоит только доказать следующие теоремы.

Теорема 2. *Частное от деления многочлена $f(x)$ с целыми коэффициентами на $x - a$, где a — целое число, есть многочлен также с целыми коэффициентами.*

Доказательство. По схеме Горнера первый коэффициент частного b_0 равен старшему коэффициенту a_0 многочлена $f(x)$. Второй коэффициент частного b_1 равен $b_0 a + a_1$. Но a, b_0 и a_1 — целые числа; следовательно, b_1 также целое число. Третий коэффициент частного $b_2 = b_1 a + a_2$ опять-таки является целым, потому что a, b_1 и a_2 — целые и т. д. Наконец, последний коэффициент частного $b_{n-1} = b_{n-2} a + a_{n-1}$ есть целое число, так как a, b_{n-2} и a_{n-1} — целые.

Теорема 3. *Если несократимая дробь $\frac{l}{m} (m > 0)$ является рациональным корнем многочлена*

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$

с целыми коэффициентами, то для любого целого числа k число $f(k)$ делится на $l - km$ при условии, что $l - km \neq 0$.

Доказательство. Умножая многочлен $f(x)$ на m^n, получаем:

$$m^n f(x) = a_0 (mx)^n + m a_1 (mx)^{n-1} + \ldots + m^n a_n,$$

или, полагая $mx = y$,

$$m^n f(x) = \varphi(y) = a_0 y^n + m a_1 y^{n-1} + \ldots + m^n a_n.$$

Так как $\frac{l}{m}$ — корень многочлена $f(x)$, то целое число l должно быть корнем многочлена $\varphi(y)$, в силу чего

$$\varphi(y) = (y - l)\, q(y).$$

По теореме 2 коэффициенты многочлена $q(y)$ должны быть целыми. Отсюда

$$\frac{\varphi(km)}{l - km} = \frac{m^n f(k)}{l - km} = -q(km)$$

должно быть целым числом; иными словами, $m^n f(k)$ делится на $l - km$. Но легко видеть, что m и $l - km$ взаимно просты. В самом деле, если бы m и $l - km$ были не взаимно простыми, то дробь

$$\frac{l - km}{m} = \frac{l}{m} - k$$

была бы сократимой

$$\frac{l - km}{m} = \frac{l_1}{m_1},$$

где $0 < m_1 < m$, и мы имели бы, что $\frac{l_1}{m_1} = \frac{l}{m} - k$, откуда

$$\frac{l}{m} = \frac{l_1 + km_1}{m_1},$$

т. е. в силу неравенства $0 < m_1 < m$ следовала бы сократимость дроби $\frac{l}{m}$, что невозможно.

Теперь теорема становится очевидной — произведение $m^n f(k)$ делится на $l - km$, а m взаимно просто с $l - km$; следовательно, $f(k)$ делится на $l - km$.

Покажем на конкретном примере, как, пользуясь всем этим, следует вычислять рациональные корни уравнения.

Пример. Найти рациональные корни уравнения

$$f(x) = 18x^4 + 9x^3 - 56x^2 - x + 6 = 0.$$

Прежде всего найдем целые корни, для чего мы должны испытать делители ± 1, ± 2, ± 3, ± 6 свободного члена 6. Вычисляем значения $f(1)$ и $f(-1)$: $f(1) = -24$, $f(-1) = -40$. Следовательно, 1 и -1 можно отбросить. Далее, если l — целый корень уравнения, то согласно теореме 3 число $f(1)$ должно делиться на $l - 1$ и $f(-1)$ должно делиться на $l + 1$. Но $f(1) = -24$ не делится на $-6-1 = -7$ и на $6-1 = 5$. Значит, можно отбросить и ± 6. Затем $f(-1) = -40$ не делится на $2 + 1 = 3$; поэтому отбрасываем 2. Остаются, таким образом, -2 и ± 3. При помощи схемы Горнера без труда находим, что $f(-2) = 0$, $f(3) = 1200$ и $f(-3) = 720$. Мы видим, что -2 — корень, а 3 и -3 не могут быть корнями. Сокращаем теперь обе части данного уравнения на $x + 2$. Мы получим уравнение:

$$g(x) = 18x^3 - 27x^2 - 2x + 3 = 0,$$

которое уже не имеет целых корней.

Согласно теореме 1 знаменатель дробного корня $\frac{l}{m}$ $(m > 0)$ многочлена $g(x)$ должен быть делителем 18, а числитель — делителем 3. Мы считаем знаменатель m положительным, относя знак к числителю l. Отсюда $m = 1, 2, 3, 6, 9, 18$ и $l = \pm 1, \pm 3$. Так как $\frac{l}{m}$ должно быть дробным, то получаются такие возможные значения $\frac{l}{m}$:

$$\pm\frac{1}{2}, \quad \pm\frac{1}{3}, \quad \pm\frac{1}{6}, \quad \pm\frac{1}{9}, \quad \pm\frac{1}{18}, \quad \pm\frac{3}{2} \qquad (4)$$

(мы еще учитываем, что l и m взаимно просты). Пользуясь теоремой 3, исключим теперь часть значений (4), а именно испытываем, для каких $\frac{l}{m}$ число $g(1) = -8$ делится на $l - m$ и число $g(-1) = -40$ делится на $l + m$. Без труда находим, что этим условиям делимости удовлетворяют только числа

$$\pm\frac{1}{3}, \quad \frac{1}{9}, \quad \frac{3}{2}.$$

Подставляя эти числа в многочлен $g(x)$ вместо x, убеждаемся, что корнями являются только $\pm\frac{1}{3}$ и $\frac{3}{2}$.

Итак, все четыре корня данного уравнения оказались рациональными:

$$x_1 = -2, \quad x_2 = \frac{1}{3}, \quad x_3 = -\frac{1}{3}, \quad x_4 = \frac{3}{2}.$$

В элементарной алгебре рассматриваются простейшие способы разложения многочлена с рациональными коэффициентами на множители. Для многочленов $f(x)$ второй и третьей степени такое разложение осуществляется довольно просто благодаря следующей теореме: *многочлен $f(x)$ второй и третьей степени с рациональными коэффициентами тогда и только тогда приводим над полем рациональных чисел, когда он имеет по меньшей мере один рациональный корень.*

Доказательство. Пусть $f(x)$ — многочлен второй или третьей степени над полем рациональных чисел. Если $f(x)$ имеет рациональный корень a, то $f(x)$ делится на $x - a$, т. е. $f(x) = (x - a) \cdot f_1(x)$, где $f_1(x)$ — многочлен над тем же самым полем рациональных чисел. При этом степень $f_1(x)$ будет равна 1 или 2. Таким образом, многочлен $f(x)$ оказался приводимым над полем рациональных чисел.

Обратно, если многочлен $f(x)$ приводим над полем рациональных чисел, то по меньшей мере один из множителей $f(x)$ должен быть линейным; в противном случае произведение множителей имело бы степень, превосходящую 3, что невозможно. Следовательно, $f(x) = (x - a) \cdot f_1(x)$, где $x - a$ и $f_1(x)$ — многочлены с рациональными коэффициентами, откуда a — рациональный корень $f(x)$.

Пример. Разложить многочлен $f(x) = x^3 + 3x^2 + 4x + 2$ на неприводимые множители над полем рациональных чисел.

Пользуясь способом нахождения рациональных корней, изложенным в предыдущем параграфе, получаем, что данный многочлен $f(x)$ имеет только один рациональный корень $x = -1$. Делим $f(x)$ на $x + 1$. Это деление можно провести при помощи схемы Горнера. В частном получится $x^2 + 2x + 2$. Многочлен второй степени $x^2 + 2x + 2$ уже не имеет рациональных корней и потому неприводим над полем рациональных чисел. Следовательно,

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

и есть искомое разложение многочлена $f(x)$.

Для многочленов выше третьей степени дело обстоит уже сложнее. Так, например, многочлен четвертой степени может оказаться

приводимым (над полем рациональных чисел) и тогда, когда он не имеет рациональных корней, а именно он может разложиться в произведение двух неприводимых квадратных множителей. Тем не менее и для многочленов выше третьей степени с рациональными коэффициентами существуют методы разложения на множители.

Мы, однако, не будем рассматривать эти практически громоздкие методы и ограничимся решением следующего вопроса: существуют ли многочлены л ю б о й степени $n \geqslant 1$, неприводимые над полем рациональных чисел?

Если некоторые и даже все коэффициенты многочлена $f(x)$ над полем рациональных чисел дробные, то мы можем сделать их целыми, умножая $f(x)$ на соответствующее целое число. При таком преобразовании неприводимый многочлен, очевидно, останется неприводимым, а приводимый — приводимым. В настоящее время известно большое количество критериев, позволяющих быстро обнаружить неприводимость многих многочленов с целыми коэффициентами над полем рациональных чисел. Одним из наиболее распространенных является критерий, предложенный в 1850 г. Эйзенштейном.

Критерий Эйзенштейна. *Если*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \quad (n \geqslant 1)$$

многочлен с целыми коэффициентами, причем $a_0, a_1, \ldots, a_{n-1}$ *делятся на некоторое простое число* p, *старший коэффициент* a_n *не делится на* p *и свободный член* a_0, *делясь на* p, *не делится на* p^2, *то многочлен* $f(x)$ *неприводим* (над полем рациональных чисел).

Из этого критерия сразу получается решение нашего вопроса, а именно: нетрудно теперь убедиться, что *неприводимыми над полем рациональных чисел могут быть многочлены любой заданной степени* $n \geqslant 1$.

В самом деле, многочлен произвольной степени $n \geqslant 1$:

$$x^n + px^{n-1} + px^{n-2} + \ldots + p,$$

где p — некоторое простое число, удовлетворяет всем условиям критерия Эйзенштейна и потому неприводим над полем рациональных чисел.

Таким образом, поле рациональных чисел налагает на неприводимость многочленов меньше ограничений, чем поле действительных чисел и поле комплексных чисел, — мы знаем (см. § 14), что над полем действительных чисел многочлены выше второй степени уже приводимы, а над полем комплексных чисел приводимы многочлены и выше первой степени.

Доказательство критерия Эйзенштейна связано с понятием примитивного многочлена и основано на двух леммах Гаусса.

Многочлен n-й степени с целыми коэффициентами называется *примитивным*, если наибольший общий делитель его коэффициентов равен единице.

Например, многочлен $f(x) = 2x^4 + 5x^3 - 10x^2 + 8x - 4$ примитивен, а многочлен $\varphi(x) = 4x^3 + 6x^2 - 10x + 2$ не является примитивным, так как наибольший общий делитель его коэффициентов равен 2, а не единице.

Теперь рассмотрим леммы Гаусса.

Лемма 1. *Произведение двух примитивных многочленов есть также примитивный многочлен.*

Доказательство. Пусть

$$g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_sx^s,$$
$$h(x) = c_0 + c_1x + c_2x^2 + \ldots + c_tx^t$$

два примитивных многочлена. Перемножим их:

$$g(x)\,h(x) = b_0c_0 + \ldots + (b_0c_{i+j} + b_1c_{i+j-1} + \ldots + b_{i-1}c_{j+1} + b_ic_j + b_{i+1}c_{j-1} + \ldots + b_{i+j}c_0)\,x^{i+j} + \ldots + b_sc_tx^m \quad (m = s + t).$$

Допустим противное: пусть произведение $g(x) \cdot h(x)$ — непримитивный многочлен; тогда его коэффициенты должны иметь наибольший общий делитель d, отличный от единицы. Если p — простой множитель d, то на p должны делиться все коэффициенты $g(x) \cdot h(x)$. Пусть $b_0, b_1, \ldots, b_{i-1}$ делятся на p, но b_i не делится на p (такое b_i, наверное, существует, так как иначе $g(x)$ не было бы примитивным многочленом). Точно так же пусть $c_0, c_1, \ldots, c_{j-1}$ делятся на p, а c_j не делится на p. Коэффициент

$$b_0c_{i+j} + b_1c_{i+j-1} + \ldots + b_{i-1}c_{j+1} + b_ic_j + \ldots + b_{i+j}c_0 \qquad (1)$$

произведения $g(x) \cdot h(x)$ по предположению делится на p. Кроме того, на p делятся, очевидно, и все члены (1), кроме b_ic_j. Следовательно, b_ic_j также должно делиться на p, потому что иначе выражение (1) не делилось бы на p. Отсюда по известному свойству простого числа следует, что по меньшей мере один из сомножителей b_i или c_j произведения b_ic_j должен делиться на p. Мы пришли к противоречию — по условию ни b_i и ни c_j не делятся на p. Лемма доказана.

Лемма 2. *Если многочлен $f(x)$ с целыми коэффициентами приводим над полем рациональных чисел, то его можно разложить на произведение многочленов низшей степени с целыми коэффициентами.*

Доказательство. Поскольку $f(x)$ приводим над полем рациональных чисел, мы можем написать, что

$$f(x) = \varphi(x)\,\psi(x),$$

где $\varphi(x)$, $\psi(x)$ — многочлены с рациональными коэффициентами. Приведем коэффициенты $\varphi(x)$ и $\psi(x)$ к одному знаменателю; получим тогда, что $\varphi(x) = \frac{1}{c}\varphi_1(x)$, $\psi(x) = \frac{1}{d}\psi_1(x)$, причем $\varphi_1(x)$ и $\psi_1(x)$ — многочлены уже с целыми коэффициентами. Затем вынесем за скобку наибольшие общие делители коэффициентов $\varphi_1(x)$ и $\psi_1(x)$. Получим $\varphi(x) = \frac{a}{c}g(x)$, $\psi(x) = \frac{b}{d}h(x)$, где $g(x)$, $h(x)$ — примитивные многочлены. Таким образом,

$$f(x) = \frac{ab}{cd}\,g(x)\,h(x).$$

Всегда можно положить $\frac{ab}{cd} = \frac{q}{r}$, где q и r взаимно просты. Если e_i —

какой-нибудь коэффициент произведения $g(x)h(x)$, то qe_i должно делиться на r, так как $f(x)$ — многочлен с целыми коэффициентами. Но q и r взаимно просты; поэтому e_i должно делиться на r. Мы видим, что r — общий делитель коэффициентов $g(x)h(x)$. По лемме 1 произведение $q(x)h(x)$ примитивно; следовательно, $r = \pm 1$, откуда $\frac{ab}{cd}$ равно целому числу $\pm q$.

Теперь лемма становится очевидной: $f(x)$ разлагается на произведение многочленов $\pm qg(x)$ и $h(x)$ с целыми коэффициентами.

Лемма 2 представляет и самостоятельный интерес, а именно: разложение многочлена на множители над полем рациональных чисел при помощи леммы 2 сводится к более простой задаче разложения многочлена с целыми коэффициентами на множители, имеющими также целые коэффициенты.

Теперь приступим к доказательству критерия Эйзенштейна.

Доказательство. Предположим противное: пусть

$$f(x) = g(x) \cdot h(x),$$

где

$$g(x) = b_0 + b_1x + \ldots + b_rx^r, \qquad h(x) = c_0 + c_1x + \ldots + c_sx^s$$
$$(r > 0, \quad s > 0, \quad r + s = n)$$

— многочлены с целыми коэффициентами (см. лемму 2). Перемножая $g(x)$ и $h(x)$, получаем:

$$g(x)h(x) = b_0c_0 + (b_1c_0 + b_0c_1)x + \ldots + (b_kc_0 + b_{k-1}c_1 + \ldots + b_0c_k)x^k + \ldots + b_rc_sx^n.$$

Отсюда следует, что

$$a_0 = b_0c_0, \quad a_1 = b_1c_0 + b_0c_1, \ldots, a_k = b_kc_0 + b_{k-1}c_1 + \ldots + b_0c_k, \ldots$$
$$a_n = b_rc_s.$$

Коэффициент $a_0 = b_0c_0$ делится на простое число p; поэтому на p должно делиться либо b_0, либо c_0. Пусть, например, b_0 делится на p; тогда c_0 не может делиться на p, так как иначе $a_0 = b_0c_0$ делилось бы на p^2.

Далее, не все коэффициенты $g(x)$ могут делиться на p. В самом деле, если бы имело место противное, то, в частности, $a_n = b_rc_s$ делилось бы на p, а это противоречит условиям критерия. Итак, пусть b_k — первый коэффициент $g(x)$, не делящийся на p. Рассмотрим

$$a_k = b_kc_0 + b_{k-1}c_1 + \ldots + b_0c_k.$$

a_k, b_{k-1}, b_{k-2}, ..., b_0 делятся на p, Следовательно, на p делятся a_k, $b_{k-1}c_1$, $b_{k-2}c_2$, ..., b_0c_k, а потому делится на p и b_kc_0. Получилось противоречие: ни b_k, ни c_0 не делятся на p, а потому их произведение b_kc_0 не может делится на простое число p.

Итак, предположение о том, что $f(x)$ приводим (над полем рациональных чисел), неверно.

Примеры. **1.** К многочлену $f(x) = x^5 + 5x + 9$ критерий неприводимости непосредственно применить нельзя, так как нельзя подобрать простого числа p, на которое одновременно делились бы 5 и 9. Но мы можем положить $x = y + 1$ и тогда получится:

$$f(y + 1) = \varphi(y) = y^5 + 5y^4 + 10y^3 + 10y^2 + 10y + 15.$$

Теперь требования критерия выполняются при $p = 5$. Следовательно, $\varphi(y)$ и тем самым $f(x)$ неприводимы.

2. Рассмотрим многочлен

$$f(x) = x^{p-1} + x^{p-2} + \ldots + 1 \ (p \text{ — простое число}).$$

Чтобы можно было применить критерий Эйзенштейна, полагаем, как и выше, $x = y + 1$. Получаем:

$$(x - 1)f(x) = (x - 1)(x^{p-1} + x^{p-2} + \ldots + 1) = x^p - 1,$$

$$\text{или } yf(y + 1) = y\varphi(y) = (y + 1)^p - 1 =$$

$$= y^p + py^{p-1} + \frac{p(p-1)}{2}y^{p-2} + \ldots + py,$$

откуда

$$\varphi(y) = y^{p-1} + py^{p-2} + \frac{p(p-1)}{2}y^{p-3} + \ldots + p.$$

Мы видим, что все коэффициенты, кроме старшего, делятся на простое число p, причем последний коэффициент p не делится на p^2, значит, $\varphi(y)$ и тем самым $f(x)$ неприводимы.