Глава 5

Многочлены

Всюду в этой главе через F обозначено произвольное поле, а через K — произвольное кольцо.

5.1. Основные определения и простейшие свойства

Пусть K — произвольное кольцо. *Многочленом*, или *полиномом*, от переменной x называется выражение вида

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \tag{5.1}$$

где $a_j \in K$ $(j = 0, 1, \ldots, n)$, а x — символ, называемый *независимой переменной*. Многочлены, как правило, мы будем обозначать латинскими буквами, рядом с которыми иногда в скобках ставить имя независимой переменной. Например, многочлен (5.1) обозначим f, или, что эквивалентно, $f(x)$, тогда можно записать:

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n. \tag{5.2}$$

Величины a_j называются *коэффициентами* многочлена, а выражения a_jx^{n-j} — *членами* (или *мономами*) многочлена f, при этом $n-j$ называется *степенью* монома. Если $a_0 \neq 0$, то n называется *степенью* многочлена, а a_0x^n — его старшим членом. Степень многочлена обозначается $\deg f$. Многочлен $f = 0$ называется *нулевым*; его степень не определена. Многочлены 1-й, 2-й и 3-й степени называются *линейными*, *квадратными* и *кубическими* соответственно. Многочлены нулевой степени вместе с нулевым многочленом называют *константами*. В записи (5.2) члены с нулевым коэффициентом обычно опускают. Также используют другие обычные соглашения при работе с алгебраическими выражениями, например, вместо $1 \cdot x^4 + (-2) \cdot x^3 + 0 \cdot x^2 + (-1) \cdot x + (-5)$ пишут $x^4 - 2x^3 - x - 5$. Помимо записи (5.2), в которой члены записаны в порядке убывания степеней, часто используется запись с упорядочением членов по возрастанию степеней и др. записи. Два многочлена (5.2) и

$$g = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m \tag{5.3}$$

равны, если $m = n$ и $a_j = b_j$ $(j = 0, 1, \ldots, n)$.

Таким образом, мы принимаем алгебраическую точку зрения на многочлены. Возможна также другая — «функциональная» — точка зрения, по которой многочлены рассматриваются как функции $f : K \to K$. Эквивалентность этих точек зрения на многочлены над числовыми полями мы установим в теореме 5.65. Над конечными полями эти точки зрения не эквивалентны. Например, неравные многочлены $\overline{1}$ и $x^2 + x + \overline{1}$ над полем $\mathbb{Z}_2$ задают одну и ту же функцию (тождественную $\overline{1}$).

Множество всех многочленов с коэффициентами из кольца K обозначим $K[x]$. Это множество называют еще множеством многочленов *над* кольцом K.

Многочлены из $K[x]$ можно складывать и умножать. При этом снова получается многочлен из $K[x]$. Сложение и умножение многочленов выполняется по обычным правилам преобразования алгебраических выражений. Для определения суммы многочленов f и g, определенных согласно (5.2) и (5.3), предположим, что $m = n$ (чтобы это условие выполнялось припишем, если необходимо, к f или g нужное количество членов с нулевыми коэффициентами). Тогда *суммой* многочленов f и g называется многочлен

$$f + g = (a_0 + b_0)x^n + (a_1 + b_1)x^{n-1} + \ldots + (a_{n-1} + b_{n-1})x + (a_n + b_n).$$

Произведением многочленов f и g, определенных согласно (5.2) и (5.3) (при любых соотношениях между m и n), называется

$$fg = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + \ldots + (a_{n-1}b_m + a_nb_{m-1})x + a_nb_m,$$

т. е.

$$fg = c_0x^{n+m} + c_1x^{n+m-1} + \ldots + c_{n+m-1}x + c_{n+m}, \quad \text{где} \quad c_k = \sum_{i+j=k} a_ib_j. \tag{5.4}$$

Из определения суммы многочленов получаем:

Утверждение 5.1. *Пусть f, g — многочлены из $K[x]$. Тогда $f + g = 0$, либо*

$$\deg(f + g) \leq \max\{\deg f, \deg g\}.$$

Если $f \neq 0$ и $g \neq 0$, то

$$\deg(fg) \leq \deg f + \deg g.$$

Если при этом K не содержит делителей нуля, то

$$\deg(fg) = \deg f + \deg g. \tag{5.5}$$

Теорема 5.2. *Пусть K — некоторое кольцо. Тогда множество многочленов $K[x]$ образует кольцо. Это кольцо является ассоциативным, коммутативным, содержит единицу и не содержит делителей нуля тогда и только тогда, когда кольцо K соответственно ассоциативно, коммутативно, содержит единицу и не содержит делителей нуля. В частности, если F — поле, то $F[x]$ — ассоциативное, коммутативное кольцо с единицей и без делителей нуля.*

Доказательство. Операции сложения и умножения обладают следующими легко проверяемыми свойствами: для любых многочленов f, g и h справедливо

1) $f + g = g + f$ (*коммутативность сложения*),

2) $f + (g + h) = (g + f) + h$ (*ассоциативность сложения*),

3) $fg = gf$, если K — коммутативное кольцо (*коммутативность умножения*),

4) $f(gh) = (gf)h$, если K — ассоциативное кольцо (*ассоциативность умножения*),

5) $f(g + h) = fg + fh$ (*дистрибутивность*),

6) $(g+h)f = gf + hf$ (*дистрибутивность*).

Докажем, например, ассоциативность умножения многочленов, если K — ассоциативное кольцо. Если f и g определены согласно (5.2) и (5.3) соответственно и

$$h = c_0 x_l + c_1 x_{l-1} + \ldots + c_{l-1} x + c_l,$$

то

$$f(gh) = d_0 x_{n+m+l} + d_1 x_{n+m+l-1} + \ldots + d_{n+m+l-1} x + d_{n+m+l},$$

где, согласно (5.4) (мы пользуемся дистрибутивностью в кольце K),

$$d_s = \sum_{i+t=s} a_i \left(\sum_{j+k=t} b_j c_k \right) = \sum_{i+j+k=s} a_i b_j c_k = \sum_{t+k=s} \left(\sum_{i+j=t} a_i b_j \right) c_k.$$

Аналогично, если

$$(fg)h = e_0 x_{n+m+l} + e_1 x_{n+m+l-1} + \ldots + e_{n+m+l-1} x + e_{n+m+l},$$

то

$$e_s = \sum_{t+k=s} \left(\sum_{i+j=t} a_i b_j \right) c_k = d_s \quad (s = 1, 2, \ldots, m+n+l),$$

откуда $f(gh) = (gf)h$.

Легко видеть, что в $K[x]$ константа 0 (и только она) является *нейтральным* элементом относительно сложения, т. е. для любого $f \in K[x]$ справедливо $f + 0 = f$. Для многочлена $f \in K[x]$ *противоположным* (относительно сложения) является

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

Под операцией вычитания тогда понимается $g - f = g + (-f)$.

Если кольцо K содержит единицу 1, то $K[x]$ также содержит 1. Константа 1 (и только она) является *нейтральным* элементом относительно умножения в $K[x]$.

Из (5.5) получаем, что если в K нет делителей нуля, то в $K[x]$ также нет делителей нуля, т. е. из равенства $fg = 0$ следует, что $f = 0$ или $g = 0$. ∎

Упражнение 5.3. Сколько существует многочленов степени m с коэффициентами из кольца $\mathbb{Z}_n$?

5.2. Деление многочлена с остатком

В следующих трех разделах и в разделе 5.10 рассматривается теория делимости многочленов *над произвольным полем* F (не над кольцом!). Эта теория во многом совпадает с соответствующей теорией целых чисел. А именно: на множестве $F[x]$, так же как и на $\mathbb{Z}$, вводятся операция деления с остатком, понятия делимости, наибольшего общего делителя, взаимно простых элементов и т. п., причем основные результаты (и часто их доказательства) практически идентичны (с некоторыми оговорками).

Теорема 5.4. *Для любого многочлена $f \in F[x]$ и любого ненулевого многочлена $g \in F[x]$ существуют и единственны многочлены q и r из $F[x]$, такие, что*

$$f = qg + r,$$

где $r = 0$ или $\deg r < \deg g$. Многочлен q называется частным, *а r —* остатком *при делении f на g.*

Доказательство. Существование Если $f = 0$ или $n < m$, где $n = \deg f$, $m = \deg g$, то положим $p = 0$, $r = f$. В противном случае положим

$$f_1 = f - \frac{a_0}{b_0} x^{n-m} g, \qquad (\alpha_1)$$

где a_0, b_0 — коэффициенты при старших членах многочленов f, g соответственно;

$$f_2 = f_1 - \frac{a_{01}}{b_0} x^{n_1-m} g, \qquad (\alpha_2)$$

где $n_1 = \deg f_1$, а a_{01} — коэффициент при старшем члене многочлена f_1;

$$f_3 = f_2 - \frac{a_{02}}{b_0} x^{n_2-m} g, \qquad (\alpha_3)$$

где $n_2 = \deg f_2$, а a_{02} — коэффициент при старшем члене многочлена f_2 и т. д. Вычисления будем продолжать до тех пор, пока не будет получен многочлен

$$f_s = f_{s-1} - \frac{a_{0s-1}}{b_0} x^{n_{s-1}-m} g, \qquad (\alpha_s)$$

такой, что $f_s = 0$ или $n_s = \deg f_s < m$. Суммируя равенства (α_1), (α_2), $\ldots$, (α_s), получаем

$$f_s = f - \frac{1}{b_0}(a_0 x^{n-m} + a_{01} x^{n_1-m} + \ldots + a_{0s-1} x^{n_{s-1}-m}) g.$$

Пусть

$$r = f_s, \quad q = \frac{1}{b_0}(a_0 x^{n-m} + a_{01} x^{n_1-m} + \ldots + a_{0s-1} x^{n_{s-1}-m}).$$

Легко видеть, что r и q удовлетворяют требуемым свойствам.
Единственность Предположим, что нашлись многочлены r, r_1, q, q_1, такие, что

$$f = qg + r = q_1 g + r_1, \qquad (5.6)$$

причем $\deg r < \deg g$, $\deg r < \deg g$. Докажем тогда, что $q = q_1$ и $r = r_1$. Действительно, из (5.6) получаем

$$(q - q_1) g = r_1 - r. \qquad (5.7)$$

Если $q \neq q_1$, то $\deg((q - q_1)g) \geq \deg g$, что не возможно, так как $\deg(r_1 - r) < \deg g$. Если же $q = q_1$, то из (5.7) получаем, что $r_1 = r$. ∎

Для частного и остатка при делении многочленов будем использовать такие же обозначения, что для частного и остатка при делении целых чисел:

$$q = f \text{ div } g, \qquad r = f \text{ mod } g.$$

Замечание 5.5. Приведенное доказательство существования частного и остатка является конструктивным, т. е. доказательством путем описания соответствующего алгоритма построения

искомых объектов. При ручных вычислениях приведенный алгоритм обычно реализуется с помощью схемы деления «уголком»:

$$
\begin{array}{l|l}
f & g \\
\hline
\dfrac{a_0}{b_0}x^{n-m}g & \dfrac{a_0}{b_0}x^{n-m} + \dfrac{a_{01}}{b_0}x^{n_1-m} + \ldots + \dfrac{a_{0,s-1}}{b_0}x^{n_{s-1}-m} \\
\hline
f_1 & \\
\dfrac{a_{01}}{b_0}x^{n_1-m}g & \\
\hline
f_2 & \\
\dfrac{a_{02}}{b_0}x^{n_2-m}g & \\
\hline
\ddots & \\
f_{s-1} & \\
\dfrac{a_{0,s-1}}{b_0}x^{n_{s-1}-m}g & \\
\hline
f_s &
\end{array}
$$

Пример 5.6. Разделим с остатком $x^4 + 2x^3 - 2x + 1$ на $2x^2 + x + 1$ (в кольце $\mathbb{Q}[x]$):

$$
\begin{array}{rl|l}
x^4 + 2x^3 & - 2x + 1 & 2x^2 + x + 1 \\
\hline
x^4 + \frac{1}{2}x^3 + \frac{1}{2}x^2 & & \frac{1}{2}x^2 + \frac{3}{4}x - \frac{5}{8} \\
\hline
\frac{3}{2}x^3 - \frac{1}{2}x^2 & - 2x + 1 & \\
\frac{3}{2}x^3 + \frac{3}{4}x^2 + \frac{3}{4}x & & \\
\hline
- \frac{5}{4}x^2 - \frac{11}{4}x + 1 & & \\
- \frac{5}{4}x^2 - \frac{5}{8}x - \frac{5}{8} & & \\
\hline
- \frac{17}{8}x + \frac{13}{8} & &
\end{array}
$$

Итак, получены частное $q = \frac{1}{2}x^2 + \frac{3}{4}x - \frac{5}{8}$ и остаток $r = -\frac{17}{8}x + \frac{13}{8}$.

Упражнение 5.7. Разделить с остатком: f на g:

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

Упражнение 5.8. (Задача из «Всеобщей арифметики» Ньютона) Разделить с остатком многочлен $x^4 - \frac{7}{2}a^2x^2 + 3a^2x - \frac{1}{2}a^4$ на многочлен $x^2 - 2ax + a^2$.

Замечание 5.9. Обратим внимание, что операция деления с остатком определена на множестве $F[x]$, а не $K[x]$. Легко привести примеры, когда частное и остаток от деления двух многочленов из $K[x]$ (например, $\mathbb{Z}[x]$) уже не принадлежат $K[x]$. Однако если если старший коэффициент b_0 делителя обратим в кольце K (т. е. элемент $1/b_0$ существует и принадлежит K), то частное и остаток принадлежат $K[x]$.

Упражнение 5.10. Пусть $f, g \in \mathbb{Z}[x]$, $n = \deg f$, $m = \deg g$ и b_0 — коэффициент при старшей степени многочлена g. Докажите, что все многочлены, получающиеся в процессе работы и на выходе алгоритма деления $b_0^{n-m+1} f$ на g, имеют целые коэффициенты. Деление многочлена $b_0^{n-m+1} f$ на g называется *псевдоделением* f на g. Как по частному и остатку, полученным при псевдоделении, получить частное и остаток от деления f на g?

5.3. Делимость. Наибольший общий делитель. Алгоритм Евклида

Пусть f и g — многочлены из $F[x]$, причем $g \neq 0$. Будем говорить, что g является *делителем* f, или, просто, что f *делится* (нацело) на g, и писать $f \vdots g$, если для некоторого $q \in F[x]$ имеем $f = qg$, т. е. $f \bmod g = 0$. В этом случае также будем использовать естественное обозначение $f/g = f \operatorname{div} g$. Если f не делится на g, то будем писать $f \not\vdots g$.

Упражнение 5.11. Докажите следующие свойства:

1) Если $f \vdots g$ и $g \vdots h$, то $f \vdots h$.
2) Если $f \vdots g$ и $h \vdots g$, то $(f + h) \vdots g$.
3) Если $f \vdots g$, то $fh \vdots g$ для любого h.
4) Любой многочлен делится на произвольную ненулевую константу.
5) Если $f \vdots g$, то $f \vdots cg$ для любой ненулевой константы c.
6) Для того, чтобы многочлен f делился на многочлен g той же степени, необходимо и достаточно, чтобы $f = cg$ для некоторой константы c.
7) Для того, чтобы $f \vdots g$ и $g \vdots f$, необходимо и достаточно, чтобы $f = cg$ для некоторой константы c.

Многочлен d называется *общим делителем* многочленов f и g, если $f \vdots d$ и $g \vdots d$. Общий делитель d называется *наибольшим* (сокращенно, НОД), если он делится на любой другой общий делитель многочленов f и g.

Теорема 5.12. *Для любых $f \in F[x]$ и $g \in F[x]$, одновременно не равных нулю, их наибольший общий делитель d существует и определен однозначно с точностью до множителя c, где c — произвольная ненулевая константа.*

Доказательство. Вначале докажем, что если НОД существует, то он определен с точностью до множителя c. Действительно, если d, d_1 — наибольшие общие делители многочленов f и g, то $d \vdots d_1$ и $d_1 \vdots d$, поэтому по пункту 7) упражнения 5.11 имеем $d = cd_1$ для некоторой константы c.

Приведем конструктивное доказательство существования наибольшего общего делителя. Опишем хорошо известный *алгоритм Евклида* нахождения НОД. Если $f \neq 0$, а $g = 0$, то, очевидно, в качестве наибольшего общего делителя можно взять f, поэтому, не нарушая общности, можно считать, что $g \neq 0$ (напомним, что f и g не равны нулю одновременно).

На нулевой итерации разделим f на g, в частном получим q_1, в остатке — r_1. Если $r_1 \neq 0$, то перейдем к первой итерации, на которой разделим g на r_1, в частном получим q_2, в остатке — r_2. На i-й итерации разделим r_{i-1} на r_i, в в частном получим q_{i+1}, в остатке — r_{i+1}. Вычисления продолжаются до тех пор, пока на некоторой, скажем, s-й, итерации вычисленный в результате очередного деления остаток r_{s+1} не будет нулевым. Докажем, что r_s является наибольшим общим делителем многочленов f и g.

Имеем

$$f = q_1 g + r_1, \qquad (\beta_0)$$

$$g = q_2 r_1 + r_2, \tag{β_1}$$

$$r_1 = q_3 r_2 + r_3, \tag{β_2}$$

$$r_{s-3} = q_{s-1} r_{s-2} + r_{s-1}, \tag{β_{s-2}}$$

$$r_{s-2} = q_s r_{s-1} + r_s, \tag{β_{s-1}}$$

$$r_{s-1} = q_{s+1} r_s. \tag{β_s}$$

Из равенства (β_s) следует, что $r_{s-1} \vdots r(s)$. Поэтому в правой части равенства (β_{s-1}) первое слагаемое делится на r_s. Так как второе слагаемое, очевидно, также делится на r_s, то вся правая часть равенства (β_{s-1}) делится на r_s, поэтому на r_s делится и левая часть этого равенства, т. е. r_{s-2}. В правой части равенства (β_{s-2}) на r_s также делятся оба слагаемых и, следовательно, $r_{s-2} \vdots r_s$. Рассматривая эти равенства далее снизу вверх (легко провести индукцию), приходим к выводу, что на r_s делятся правые части в (β_0) и (β_1), т. е. $f \vdots r_s$ и $g \vdots r_s$, т. е. r_s — общий делитель многочленов f и g.

Теперь покажем, что любой общий делитель d многочленов f и g является также делителем многочлена r_s. Так как $f \vdots d$ и $g \vdots d$, то из (β_0) получаем, что $r_1 \vdots d$. Далее, так как $g \vdots d$ и $r_1 \vdots d$, то из (β_1) получаем, что $r_2 \vdots d$. Рассматривая далее эти равенства сверху вниз (легко провести индукцию), приходим к выводу, что $r_s \vdots d$. ∎

Замечание 5.13. В алгоритме Евклида многочлены r_j $(j = 1, 2, \ldots, s)$ можно умножать на произвольные константы. Легко видеть, что доказательство теоремы 5.12 распространяется и на такую модификацию алгоритма.

Итак, НОД двух ненулевых многочленов существует и определен с точностью до постоянного множителя. Чтобы избежать многозначности, среди всех возможных НОД двух многочленов f, g можно выбрать многочлен со старшим коэффициентом 1 (если это не так, то разделим многочлен на старший коэффициент). Именно его мы будем обозначать НОД(f, g).

Теорема 5.14. *Пусть f, g, d — ненулевые многочлены из $F[x]$ и d — НОД многочленов f и g. Тогда найдутся такие u, v из $F[x]$, что*

$$uf + vg = d, \tag{5.8}$$

причем $\deg u < \deg g$, *а* $\deg v < \deg f$. *Многочлены u и v называются* коэффициентами Безу.

Доказательство. Очевидно, что достаточно научиться находить коэффициенты Безу по крайней мере для одного из возможных НОД, например, для НОД, выдаваемого алгоритмом Евклида. Применим к f и g алгоритм Евклида. В ходе его работы получим последовательности частных $q_1, q_2, \ldots, q_{s+1}$ и остатков $r_1, r_2, \ldots, r_s$. На первой итерации запишем два тривиальных равенства:

$$f = 1 \cdot f + 0 \cdot g, \tag{γ_{-1}}$$

$$g = 0 \cdot f + 1 \cdot g, \tag{γ_0}$$

и вычтем из первого второе, умноженное на q_1. Тогда согласно (β_0) в левой части получим r_1. В правой части соберем множители у f и у g:

$$r_1 = 1 \cdot f + (-q_1) \cdot g. \tag{γ_1}$$

На второй итерации вычтем из равенства (γ_0) равенство (γ_1), умноженное на q_2. Согласно (β_1) в левой части получим r_2. В правой части снова соберем множители у f и у g:

$$r_2 = (-q_2) \cdot f + (1 + q_1 q_2) \cdot g. \qquad (\gamma_2)$$

На третьей итерации из (γ_1) вычтем (γ_2), умноженное на q_3. Согласно (β_2) в левой части получим r_3. В правой части снова соберем множители у f и у g:

$$r_3 = (1 + q_2 q_3) \cdot f + (-q_1 - q_3 - q_1 q_2 q_3) \cdot g. \qquad (\gamma_3)$$

Будем выполнять такие преобразования далее. На k-й итерации $(k = 1, 2, \ldots, s)$, вычитая из равенства (γ_{k-2}) равенство (γ_{k-1}), умноженное на q_k, получим

$$r_k = u_k f + v_k g, \qquad (\gamma_k)$$

где u_k, v_k — некоторые многочлены. На s-й итерации получим

$$d = r_s = u_s f + v_s g. \qquad (\gamma_s)$$

Можно считать, что многочлены u_s и v_s ненулевые[1]. Если $\deg u_s < \deg g$ и $\deg v_s < \deg f$, то u_s и v_s — искомые коэффициенты Безу. В противном случае выполним следующую процедуру.

Пусть, для определенности, $\deg u_s \geq \deg g$. Разделим u_s на g: $u_s = qg + r$. Теперь из (γ_s) получаем

$$d = rf + (v_s + qf)g.$$

Обозначим $u = r$, $v = v_s + qf$. Имеем $uf + vg = d$ и $\deg u < \deg g$. Покажем, что $\deg v < \deg f$, тем самым завершив доказательство теоремы. Предположим противное: $\deg v \geq \deg f$, тогда $\deg(uf) < \deg g + \deg f$, но $\deg(vg) \geq \deg g + \deg f$, поэтому

$$\deg d = \deg(uf + vg) \geq \deg g + \deg f,$$

что противоречит тому, что d — НОД многочленов f и g. ∎

Алгоритм нахождения коэффициентов Безу, описанный при доказательстве теоремы 5.14, называется *расширенным алгоритмом Евклида.*

Пример 5.15. Найдем НОД и коэффициенты Безу многочленов $f = x^4 - 3$, $g = x^3 + 2x^2 + x + 1$. При делении f на g получаем частное и остаток:

$$q_1 = x - 2, \qquad r_1 = 3x^2 + x - 1.$$

При делении g на r_1 получаем

$$q_2 = \frac{1}{3}x + \frac{5}{9}, \qquad r_2 = \frac{7}{9}x + \frac{14}{9}.$$

При делении r_1 на $\dfrac{9}{7} \cdot r_2 = x + 2$ получаем

$$q_3 = 3x - 5, \qquad r_3 = 9.$$

[1] Если $uf + vg = d$ и один из многочленов u или v — нулевой: для определенности, $v = 0$, то $d \vdots f$, но так как $f \vdots d$ и $g \vdots d$, то u — константа и многочлены f, g, d отличаются друг от друга константными множителями. Поэтому многочлены u и v можно заменить на ненулевые константы, так, что равенство $uf + vg = d$ останется выполненным.

Остаток при делении r_2 на r_3 равен нулю, следовательно, cr_3, где c — произвольная ненулевая константа, является наибольшим общим делителем многочленов f и g. Итак, НОД многочленов f и g с точностью до ненулевого константного множителя равен 1.

Для нахождения коэффициентов Безу воспользуемся алгоритмом из доказательства теоремы 5.14. Имеем

$$f = 1 \cdot f + 0 \cdot g, \tag{5.9}$$

$$g = 0 \cdot f + 1 \cdot g. \tag{5.10}$$

Вычитая из равенства (5.9) равенство (5.10), умноженное на $q_1 = x - 2$, получаем

$$r_1 = 3x^2 + x - 1 = 1 \cdot f + (-x + 2) \cdot g. \tag{5.11}$$

Вычитая из равенства (5.10) равенство (5.11), умноженное на $q_2 = \frac{1}{3}x + \frac{5}{9}$, получаем

$$r_2 = \frac{7}{9}x + \frac{14}{9} = \left(-\frac{1}{3}x - \frac{5}{9}\right) \cdot f + \left(\frac{1}{3}x^2 - \frac{1}{9}x - \frac{1}{9}\right) \cdot g,$$

откуда

$$\frac{9}{7} \cdot r_2 = x + 2 = \left(-\frac{3}{7}x - \frac{5}{7}\right) \cdot f + (3x^2 - x - 1) \cdot g. \tag{5.12}$$

Вычитая из равенства (5.11) равенство (5.12), умноженное на $q_3 = 3x - 5$, получаем

$$r_3 = 9 = \left(\frac{9}{7}x^2 - \frac{18}{7}\right) \cdot f + \left(-\frac{9}{7}x^3 + \frac{18}{7}x^2 - \frac{9}{7}x + \frac{9}{7}\right) \cdot g,$$

откуда

$$1 = \left(\frac{1}{7}x^2 - \frac{2}{7}\right) \cdot f + \left(-\frac{1}{7}x^3 + \frac{2}{7}x^2 - \frac{1}{7}x + \frac{1}{7}\right) \cdot g.$$

Итак,

$$u = \frac{1}{7}x^2 - \frac{2}{7}, \qquad v = -\frac{1}{7}x^3 + \frac{2}{7}x^2 - \frac{1}{7}x + \frac{1}{7}.$$

Упражнение 5.16. Найти НОД и коэффициенты Безу для многочленов:

1) $f = 2x^6 + x^5 + 15x^3 - 4x^4 + 5x^2 - 2x - 1$, $g = 2x^4 + 5x^3 - x$;

2) $f = 4x^5 - 23x^4 + 47x^3 - x^2 - 48x - 36$, $g = 4x^3 - 15x^2 + 5x + 18$.

Иногда удобно использовать другой алгоритм нахождения коэффициентов Безу, основанный на *методе неопределенных коэффициентов*. Этот способ предполагает, что НОД d многочленов f и g уже известен. Во-первых, вместо f и g рассмотрим многочлены $f_1 = f/d$ и $g_1 = g/d$. Из (5.8) получаем

$$1 = uf_1 + vg_1. \tag{5.13}$$

Далее запишем u и v с неопределенными коэффициентами, учитывая, что $\deg u < \deg g$, и приравняем коэффициенты при одинаковых степенях в левой и правой частях равенства (5.13). Из полученной линейной системы определим коэффициенты многочленов u и v. Другой способ составить систему для определения этих коэффициентов заключается в следующем. Выберем $\deg u + \deg g$ различных чисел (по числу неопределенных коэффициентов). Для облегчения вычислений желательно, чтобы среди этих чисел были корни многочленов f и g. Последовательно подставляя эти числа вместо x в (5.13), получим линейную систему, из которой определим неизвестные коэффициенты.

Пример 5.17. Найдем коэффициенты Безу многочленов $f = x^6 + 2x^5 + 4x^4 + 4x^3 + 2x^2 - 1$ и $g = x^5 + x^4 + x^2 - 5x + 2$, если известен их НОД $d = x^3 + 2x - 1$. Имеем $f_1 = f/d = x^3 + 2x^2 + 2x + 1$, $g_1 = g/d = x^2 + x - 2$. Равенство (5.13) примет вид

$$1 = (a_0x + a_1)(x^3 + 2x^2 + 2x + 1) + (b_0x^2 + b_1x + b_2)(x^2 + x - 2).$$

Последовательно подставляя в него вместо x числа $-2, -1, 0, 1, 2$, получим систему

$$\begin{cases} 6a_0 - 3a_1 = 1, \\ -2b_0 + 2b_1 - 2b_2 = 1, \\ a_1 - 2b_2 = 1, \\ 6a_0 + 6a_1 = 1, \\ 42a_0 + 21a_1 + 16b_0 + 8b_1 + 4b_2 = 1, \end{cases}$$

из которой находим $a_0 = 1/6$, $a_1 = 0$, $b_0 = -1/6$, $b_1 = -1/6$, $b_2 = -1/2$. Таким образом,

$$u = \frac{1}{6}x, \qquad v = -\frac{1}{6}x^2 - \frac{1}{6}x - \frac{1}{2}.$$

Упражнение 5.18. Пусть $f, g, h \in F[x]$. Докажите, что для того, чтобы многочлен h можно было представить в виде $h = u_1f + v_1g$, где u_1 и v_1 — некоторые многочлены из $F[x]$, необходимо и достаточно, чтобы h делился на НОД многочленов f и g. Как u_1 и v_1 можно выразить через коэффициенты Безу многочленов f и g?

Упражнение 5.19. Найти многочлены наименьшей степени u и v, такие, чтобы

1) $(x^4 - 2x^3 - 4x^2 + 6x + 1)u + (x^3 - 5x - 3)v = x^4$;
2) $(x^4 + 2x^3 + x + 1)u + (x^4 + x^3 - 2x^2 + 2x - 1)v = x^3 - 2x$.

Упражнение 5.20. Найти НОД многочленов $x^5 + x^3 + x^2 + 2x + 1$, $x^5 + 2x^4 + x^3 + 1$
1) над полем $\mathbb{Z}_3$;
2) над полем $\mathbb{Q}$.

Упражнение 5.21. Найти НОД многочленов $x^5 + 4x^4 + 3x^3 + x^2 + 4$ и $x^4 + 4x^3 + 4x^2 + 4$
1) над полем $\mathbb{Z}_3$ (все коэффициенты нужно заменить на наименьшие вычеты по модулю 3);
2) над полем $\mathbb{Z}_5$;
3) над полем $\mathbb{Q}$.

Упражнение 5.22. Найти НОД многочленов $x^5 - x^4 - 2x^3 + 2x^2 + 9x - 9$ и $x^5 + x^4 + 4x^3 - x^2 + x - 6$
1) над полем $\mathbb{Z}_3$;
2) над полем $\mathbb{Z}_5$;
3) над полем $\mathbb{Z}_7$;
4) над полем $\mathbb{Q}$.

5.4. Взаимно простые многочлены

Многочлены f и g назовем *взаимно простыми*, если их НОД равен ненулевой константе.

Следствие 5.23. *Для того, чтобы многочлены f и g из $F[x]$ были взаимно простыми необходимо и достаточно, чтобы в $F[x]$ существовали такие u и v, что $uf + vg = 1$.*

Доказательство. Необходимость является прямым следствием теоремы 5.14.
Достаточность. Пусть d — НОД многочленов f и g, поэтому каждое из слагаемых в левой части равенства $uf + vg = 1$ делится на d, а значит на d делится и правая часть: $1 \vdots d$, откуда выводим, что d — ненулевая константа. ∎

Следствие 5.24. *Пусть поле F является подполем поля F'. Для того, чтобы многочлены f и g из $F[x]$ были взаимно простыми необходимо и достаточно, чтобы эти многочлены, рассматриваемые как элементы множества $F'[x]$, были также взаимно простыми.*

Доказательство. Вытекает из следствия 5.23. ∎

Утверждение 5.25. *Если многочлен f взаимно прост с каждым из многочленов g и h, то он взаимно прост и с их произведением gh.*

Доказательство. Так как многочлен f взаимно прост с каждым из многочленов g и h, то по следствию 5.23 найдутся такие u, u_1, v, v_1, что

$$uf + vg = 1,$$
$$u_1 f + v_1 h = 1.$$

Складывая эти два равенства и осуществляя очевидные преобразования, получаем:

$$(uu_1 + fu + v_1 h + vgu_1)f + (vv_1)(gh) = 1,$$

откуда по следствию 5.23 получаем, что многочлены f и gh взаимно просты. ∎

Утверждение 5.26. *Если $fg \vdots h$, причем многочлены f и h взаимно просты, то $g \vdots h$.*

Доказательство. Так как многочлены f и h взаимно просты, то по следствию 5.23 найдутся такие u, v, что $uf + vh = 1$. Умножая обе части этого равенства на g, получаем

$$ufg + vhg = g.$$

Очевидно, второе слагаемое в левой части делится на h. Первое слагаемое левой части делится на h по условию. Следовательно, $g \vdots h$. ∎

Утверждение 5.27. *Если $f \vdots g$ и $f \vdots h$, причем g и h взаимно просты, то $f \vdots gh$.*

Доказательство. Так как $f \vdots g$, то для некоторого q имеем $f = qg$. Но $f \vdots h$. Так как g и h взаимно просты, то по утверждению 5.26 $g \vdots h$, откуда $f \vdots gh$. ∎

Рассмотрим систему многочленов $f_1, f_2, \ldots, f_s$ из $F[x]$. Многочлен d называется их *общим делителем*, если $f_j \vdots d$ $(j = 1, 2, \ldots, s)$. Общий делитель называется *наибольшим*, если он делится на любой другой их общий делитель.

Упражнение 5.28.

1) Пусть d — НОД многочленов $f_1, \ldots, f_{s-1}$. Докажите, что НОД многочленов d и f_s является наибольшим общим делителем многочленов $f_1, f_2, \ldots, f_s$.
2) Пусть d — НОД многочленов $f_1, \ldots, f_s$. Докажите, что тогда найдутся такие $u_1, u_2, \ldots u_s$, что
$$u_1 f_1 + u_2 f_2 + \ldots + u_s f_s = d.$$

Многочлены $f_1, f_2, \ldots, f_s$ называются *взаимно простыми (в совокупности)*, если их наибольший общий делитель равен ненулевой константе. Многочлены $f_1, f_2, \ldots, f_s$ называются *попарно взаимно простыми*, если при любых i, j, $1 \leq i < j \leq s$ многочлены f_i и f_j взаимно просты.

Очевидно, что если многочлены попарно взаимно просты, то они взаимно просты в совокупности. Легко привести примеры, показывающие, что обратное утверждение в общем случае не верно.

Упражнение 5.29. Докажите, что для того, чтобы многочлены $f_1, f_2, \ldots f_s$ были взаимно простыми необходимо и достаточно, чтобы существовали такие $u_1, u_2, \ldots u_s$, что
$$u_1 f_1 + u_2 f_2 + \ldots + u_s f_s = 1.$$

5.5. Корни многочлена

Пусть K — ассоциативное и коммутативное кольцо с единицей. *Значением* многочлена $f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x]$ в точке $c \in K$ называется число из K, обозначаемое $f(c)$ и равное

$$f(c) = a_0c^n + a_1c^{n-1} + \ldots + a_{n-1}c + a_n \in F. \tag{5.14}$$

Если $f(c) = 0$, то c называется *корнем* многочлена f.

Очевидно, значение от суммы, разности и произведения многочленов совпадает с суммой, разностью и произведением значений соответствующих многочленов в той же точке.

Утверждение 5.30 (Теорема Безу)**.** *Остатком при делении многочлена $f \in K[x]$ на линейный многочлен $x - c \in K[x]$ является константа $f(c) \in K$.*

Доказательство. При делении f на $x - c$ в частном получим многочлен q, а в остатке — константу r:

$$f = q(x - c) + r.$$

Полагая в левой и правой части $x = c$, получаем: $f(c) = q(c)(c - c) + r = r$. ∎

Следствие 5.31.

$$f(c) = 0 \quad \Leftrightarrow \quad f \vdots (x - c).$$

Будем говорить, что корень c многочлена f имеет *кратность* k, если

$$f \vdots (x - c)^k, \qquad f \not\vdots (x - c)^{k+1}.$$

Корень кратности 1, назовем *простым*.

Схема Горнера — это метод деления многочлена f на линейный множитель $x-c$. Разделим f на $x - c$ «в общем виде»:

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = (b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1})(x - c) + r.$$

Раскрывая скобки в правой части равенства и приравнивая коэффициенты из разных частей при равных степенях, получаем

$$\begin{aligned}
a_0 &= b_0 \\
a_1 &= b_1 - b_0c \\
a_2 &= b_2 - b_1c \\
&\ldots\ldots\ldots\ldots\ldots \\
a_{n-1} &= b_{n-1} - b_{n-2}c \\
a_n &= r - b_{n-1}c
\end{aligned}$$

откуда

$$\begin{aligned}
q_0 &= a_0 \\
q_1 &= a_1 + b_0c \\
q_2 &= a_2 + b_1c \\
&\ldots\ldots\ldots\ldots\ldots \\
q_{n-1} &= a_{n-1} + b_{n-2}c \\
r &= a_n + b_{n-1}c
\end{aligned} \tag{5.15}$$

Схема Горнера заключается в вычислении коэффициентов частного и остатка по формулам (5.15). При ручных вычислениях обычно используют таблицу следующего вида:

	a_0	a_1	a_2	$\dots$	a_{n-1}	a_n
c	$b_0 = a_0$	$b_1 = a_1 + b_0c$	$b_2 = a_2 + b_1c$	$\dots$	$b_{n-1} = a_{n-1} + b_{n-2}c$	$r = a_n + b_{n-1}c$

Пример 5.32. Разделим $f = x^4 - 8x^3 + 21x^2 - 21x + 7$ на $x - 2$.

	1	−8	21	−21	7
2	1	−6	9	−3	1

Получили частное $q = x^3 - 6x^2 + 9x - 3$ и остаток $f(2) = 1$.

Упражнение 5.33. С помощью схемы Горнера разделить f на g:
1) $f = x^4 - 2x^2 + 2x^3 - 2x + 2$, $g = x - 2$;
2) $f = x^4 + (-1 + i)x^3 + (25 - 7i)x^2 + (-33 + 16i)x + 11 - 10i$, $g = x - 1 + i$.

Из схемы Горнера следует

$$f(c) = \Big(\dots((a_0c + a_1)c + a_2)c + \dots + a_{n-1}\Big)c + a_n.$$

Заметим, что ту же формулу можно получить простым преобразованием правой части равенства (5.14).

Замечание 5.34. Понятие значения многочлена в точке можно распространить и на многочлены над произвольным ассоциативным, но *не*коммутативным кольцом. Однако тогда необходимо говорить о *правом* и *левом* значении многочлена в точке: соответственно

$$f(c) = a_0c^n + a_1c^{n-1} + \dots + a_{n-1}c + a_n \quad \text{и} \quad (c)f = c^na_0 + c^{n-1}a_1 + \dots + ca_{n-1} + a_n,$$

правом и левом корне многочлена, а также о правом и левом делении многочлена f на g: соответственно

$$f = qg + r \quad \text{и} \quad f = gq + r.$$

Теорема Безу превращается тогда в следующее утверждение: остаток от правого (соответственно левого) деления многочлена f на многочлен $x - c$ равен правому (соответственно левому) значению многочлена f в точке c.

Производной многочлена

$$f = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

называется многочлен[2]

$$f' = a_0nx^{n-1} + a_1(n-1)x^{n-2} + \dots + 2a_{n-2}x + a_{n-1}.$$

Индуктивно определим *производную k-го порядка* (или, просто, *k-ю производную*). Пусть $f^{(k-1)}$ — производная $(k-1)$-го порядка. Производной k-го порядка называется многочлен $f^{(k)} = (f^{(k-1)})'$.

Упражнение 5.35. Пусть $f, g \in K[x]$. Докажите следующие свойства:

[2]Если $n \in \mathbb{N}$ и кольцо K содержит единицу 1, то $n \cdot 1$ означает элемент кольца K, равный $\underbrace{1 + 1 + \dots + 1}_{n}$.

Элемент $n \cdot 1$ кольца K для краткости будем обозначать также просто n.

1) $(f \pm g)' = f' \pm g'$,

2) $(f \cdot g)' = f'g + fg'$,

3) $(f^k)' = kf^{k-1}f'$.

Теорема 5.36. *Корень кратности $k \geq 2$ многочлена f является корнем кратности $k-1$ многочлена f'. Простой корень многочлена f не является корнем многочлена f'.*

Доказательство. Пусть c — корень кратности k многочлена f:

$$f = q(x-c)^k, \qquad q \not\vdots (x-c).$$

Тогда

$$f' = q'(x-c)^k + qk(x-c)^{k-1} = (q'(x-c) + qk)(x-c)^{k-1}.$$

Так как

$$q'(x-c) \vdots (x-c), qk \not\vdots (x-c), \text{то}(q'(x-c) + qk) \not\vdots (x-c),$$

откуда следует доказываемое. ∎

Следствие 5.37. *Для того, чтобы корень многочлена f имел кратность k необходимо и достаточно, чтобы он являлся корнем последовательных производных многочлена f вплоть до $(k-1)$-го порядка и не являлся корнем k-й производной.*

Упражнение 5.38. При каких a, b, c многочлен $x^4 + ax^3 + bx^2 + cx - 1$ имеет -1 корнем не ниже третьей кратности?

Упражнение 5.39. При каких условия многочлен имеет кратный корень:
1) $x^3 + px + q$;
2) $x^4 + px + q$;
3) $x^5 + px + q$?

Упражнение 5.40. Показать, что трехчлен $x^n + px^m + q$, где $q \neq 0$, $m < n$ не может иметь корней выше второй кратности.

Утверждение 5.41. *Пусть ассоциативное, коммутативное кольцо K не содержит делителей нуля. Тогда любой многочлен $f \in K[x]$ степени $n > 0$ имеет в кольце K не более n корней с учетом их кратностей.*

Доказательство. Пусть

$$f = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_s)g = (x-\beta_1)(x-\beta_2)\dots(x-\beta_t)h,$$

где $\alpha_1, \dots, \alpha_s$, $\beta_1, \dots, \beta_t$ — элементы кольца K, $\alpha_i \neq \beta_j$ при $i \neq j$, а многочлены g и h корней в K не имеют. Вычисляя значение многочлена f в точке α_i получим представление 0 в виде произведения ненулевых элементов кольца K, что противоречит тому, что в K нет делителей нуля. ∎

Пример 5.42. Многочлен $x^4 - \overline{1} = (x-\overline{1})(x-\overline{2})(x-\overline{3})(x-\overline{4}) \in \mathbb{Z}_5[x]$ имеет 4 корня в $\mathbb{Z}_5$. Многочлен $x^2 + \overline{2} \in \mathbb{Z}_5[x]$ корней в $\mathbb{Z}_5$ не имеет.

Пример 5.43. Утверждение из упражнения 5.41 не справедливо для многочленов над произвольным кольцом. Например, многочлен $f = x^2 + \overline{5}x \in \mathbb{Z}_6[x]$ в кольце $\mathbb{Z}_6$ имеет 4 корня: $\overline{0}, \overline{1}, \overline{3}, \overline{4}$ — и допускает два разложения: $f = x(x+\overline{5}) = (x+\overline{2})(x+\overline{3})$.

5.5.1. Формула Тейлора

Утверждение 5.44. *Для любой константы $c \in F$ многочлен*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in F[x],$$

можно представить в виде

$$f = b_0(x-c)^n + b_1(x-c)^{n-1} + \ldots + b_{n-1}(x-c) + b_n, \tag{5.16}$$

называемом разложением f по степеням $x-c$. *При этом коэффициенты $b_0, b_1, \ldots, b_n$ определяются единственным образом.*

Доказательство. Чтобы получить разложение (5.16) разделим f с остатком на $x-c$. В остатке, очевидно, получим b_n, а в частном некоторый многочлен f_1. Разделим f_1 с остатком на $x-c$. В остатке, очевидно, получим b_{n-1}, а в частном некоторый многочлен f_2 и т. д. Таким образом, существование разложения (5.16) доказано. Единственность легко доказывается методом от противного. ∎

Пример 5.45. Разложим $f = x^4 - 8x^3 + 21x^2 - 21x + 7$ по степеням $g = x - 2$. Для этого применим схему Горнера сначала к многочленам f и g, затем к их частному f_1 и g и т. д.:

	1	−8	21	−21	7
2	1	−6	9	−3	**1**
2	1	−4	1	**−1**	
2	1	−2	**−3**		
2	1	**0**			
2	**1**				

(5.17)

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

Пример 5.46. С помощью схемы Горнера разложим многочлен $f = (x-2)^4 + 2(x-2)^3 + 2(x-2)^2 - 2$ по степеням x.
1-й способ. Необходимо решить задачу, обратную задаче из примера 5.45. Заполняя таблицу, аналогичную (5.17), *снизу вверх*, получаем:

	1	**−6**	**14**	**−16**	**6**
2	1	−4	6	−4	-2
2	1	−2	2	0	
2	1	0	2		
2	1	2			
2	1				

Итак, $f = x^4 - 6x^3 + 14x^2 - 16x + 6$.
2-й способ. Вместо многочлена f рассмотрим многочлен $g(y) = y^4 + 2y^3 + 2y^2 - 2$, который разложим по степеням $y+2$. Получим $g(y) = (y+2)^4 - 6(y+2)^3 + 14(y+2)^2 - 16(y+2) + 6$, откуда $f = x^4 - 6x^3 + 14x^2 - 16x + 6$.

Упражнение 5.47. С помощью схемы Горнера разложить f по степеням g:
1) $f = x^4 + 3x^3 + 5x^2 + 5x$, $g = x + 1$;
2) $f = x^5$, $g = x - 1$.

Утверждение 5.48 (Формула Тейлора)**.** *Для любой константы $c \in F$ и любого многочлена $f \in F[x]$ степени n справедливо*

$$f = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \ldots + \frac{f^{(n-1)}(c)}{(n-1)!}(x-c)^{n-1} + \frac{f^{(n)}(c)}{n!}(x-c)^n.$$

Доказательство. Взяв k-ю производную от многочлена

$$f = b_0 + b_1(x-c) + b_2(x-c)^2 + \ldots + b_n(x-c)^n$$

и подставив $x = c$, получим $b_k = f^{(k)}(c)/k!$. ∎

Пример 5.49. Для многочлена $f = x^4 - 8x^3 + 21x^2 - 21x + 7$ в примере 5.45 найдено разложение $f = (x-2)^4 - 3(x-2)^2 - (x-2) + 1$, откуда можно сразу получить значения производных в точке 2:

$$f'(2) = -1 \cdot 1! = -1, \quad f''(2) = 0 \cdot 2! = 0, \quad f'''(2) = -3 \cdot 3! = -18, \quad f^{IV}(2) = 1 \cdot 4! = 24.$$

Упражнение 5.50. С помощью схемы Горнера найти значение многочлена и его производных в точке 2:
1) $x^4 - 6x^3 + 10x^2 + x - 9$;
2) $x^4 + (-8+i)x^3 + (25-7i)x^2 + (-35+16i)x + 18 - 10i$.

5.6. «Основная теорема алгебры»

Если любой многочлен $f \in F[x]$, степени не меньшей 1, имеет по крайней мере один корень из F, то поле F называется *алгебраически замкнутым*. Поле $\mathbb{R}$ алгебраически замкнутым не является. Например, многочлен x^2+1 не имеет вещественных корней. Именно это послужило основной причиной построения поля комплексных чисел. Поле $\mathbb{C}$ алгебраически замкнуто, а именно, справедлива

Теорема 5.51 («Основная теорема алгебры»)**.** *Любой многочлен $f \in \mathbb{C}[x]$ степени не меньше 1 имеет по крайней мере один комплексный корень.*

Известно много доказательств «основной теоремы алгебры». Здесь мы приведем одно из них, называемое «дамой с собачкой».

Доказательство. Не нарушая общности, можно считать, что старший коэффициент многочлена равен 1. Кроме того, будем считать, что свободный коэффициент не равен нулю, так как в противном случае 0 является корнем. Итак,

$$f = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{C}[x], \quad a_n \neq 0.$$

Положим $A = \max\{|a_1|, |a_2|, \ldots, |a_n|\}$, $a = \min\left\{1, \dfrac{a_n}{n\max\{A,1\}}\right\}$.

Лемма 5.52 (Лемма о старшем члене)**.** *Если $\alpha \in \mathbb{C}$ и $|\alpha| \geq A+1$, то $|\alpha^n| > |a_1\alpha^{n-1} + \ldots + a_n|$.*

Доказательство.

$$\begin{aligned}
|a_1\alpha^{n-1} + a_2\alpha^{n-2} + \ldots + a_n| &\leq |a_1||\alpha|^{n-1} + |a_2||\alpha|^{n-2} + \ldots + |a_n| \leq \\
&\leq A(|\alpha|^{n-1} + |\alpha|^{n-2} + \ldots + 1) = \\
&= A \cdot \frac{|\alpha|^n - 1}{|\alpha| - 1} \leq \\
&\leq A \cdot \frac{|\alpha|^n - 1}{A} = \\
&= |\alpha|^n - 1,
\end{aligned}$$

откуда следует требуемое неравенство. ∎

Лемма 5.53 (Лемма о младшем члене)**.** *Если* $\alpha \in \mathbb{C}$ *и* $|\alpha| < a$*, то* $|\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha| < |a_n|$.

Доказательство.

$$\begin{aligned}|\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha| &\le |\alpha|^n + |a_1||\alpha|^{n-1} + \ldots + |a_{n-1}||\alpha| < \\ &< a \cdot (a^{n-1} + |a_1|a^{n-2} + \ldots + |a_{n-1}|) \le \\ &\le a \cdot \max\{A, 1\} \cdot (a^{n-1} + a^{n-2} + \ldots + 1) \le \\ &\le a \cdot \max\{A, 1\} \cdot n \le \\ &\le |a_n|.\end{aligned}$$

Лемма доказана. ∎

Для доказательства теоремы исследуем кривые, по которым проходит точка $f(\alpha)$, когда α пробегает на комплексной плоскости окружность $|\alpha| = r$:

$$\alpha = r(\cos\varphi + i\sin\varphi) \qquad (0 \le \varphi < 2\pi).$$

При каждом фиксированном $r > 0$ линия $f(\alpha)$ — некоторая непрерывная замкнутая кривая (замкнутый контур).

Во-первых, докажем, что если $r = A+1$, то 0 находится внутри этого контура. Обозначим

$$g(x) = f(x) - x^n = a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n.$$

Кривая α^n обращается по окружности радиуса r^n вокруг нуля n раз:

$$\alpha^n = r^n(\cos n\varphi + i\sin n\varphi) \qquad (0 \le \varphi < 2\pi).$$

Оказывается, что $f(\alpha)$ также обращается вокруг нуля n раз (уже не обязательно по окружности). Действительно, по лемме о старшем члене $|f(\alpha) - \alpha^n| = |g(\alpha)| < |\alpha^n|$, т. е. $f(\alpha)$ отклоняется от α^n на расстояние, меньшее α^n, следовательно, контур $f(\alpha)$ содержит точку 0 внутри[3].

Во-вторых, докажем, что если $r = a/2$, то 0 находится снаружи контура $f(\alpha)$. Обозначим

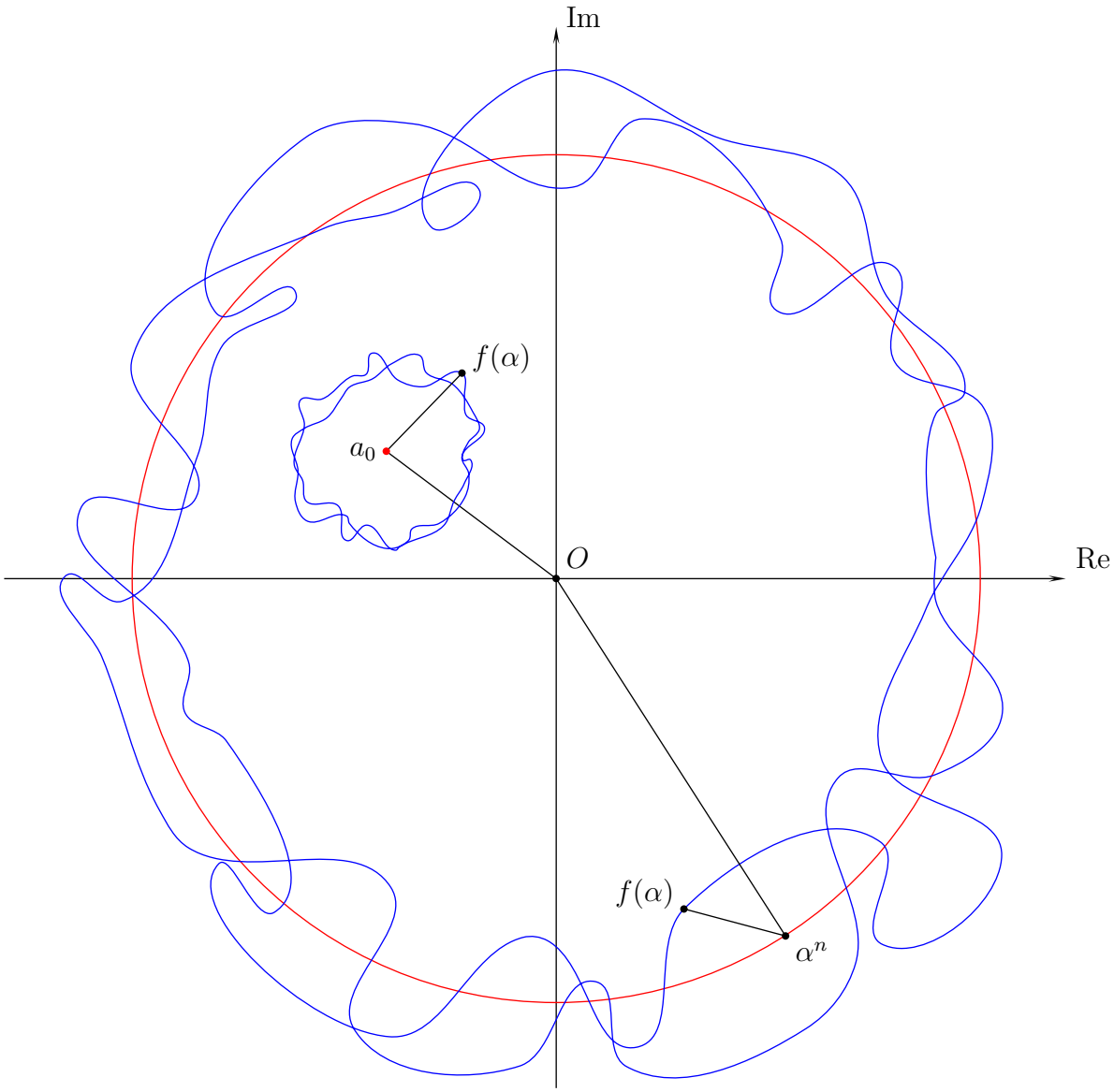
$$h(x) = f(x) - a_n = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x.$$

По лемме о младшем члене $|f(\alpha) - a_n| = |h(\alpha)| < |a_n|$, поэтому кривая $f(\alpha)$ отходит от точки a_n меньше, чем на расстояние $|a_n|$, следовательно, точка 0 лежит вне этой кривой[4].

Если r пробегает все вещественные значения от $A+1$ до $a/2$, то рассматриваемый контур непрерывно меняется. Но так как при $r = A + 1$ точка 0 лежит внутри этого контура, а при $r = a/2$ — снаружи, то при некотором r кривая пересечет точку 0, т. е. для некоторого α получим $f(\alpha) = 0$. ∎

[3]Этому можно дать следующую интерпретацию: α^n — это «дама», $g(\alpha)$ — «поводок», $f(\alpha) = \alpha^n + g(\alpha)$ — «собачка». «Дама» α^n гуляет вокруг точки 0. Неравенство $|g(\alpha)| < |\alpha^n|$ означает, что «поводок» $g(\alpha)$ настолько короток, что «собачка» $f(\alpha)$ не может добежать до нуля и вместе с «дамой» обходит нуль n раз.

[4]Теперь a_n — это «дама», $h(\alpha)$ — «поводок», $f(\alpha) = a_n + h(\alpha)$ — «собачка». «Дама» стоит на месте (в точке a_0), «собачка» бегает вокруг нее. Неравенство $|h(\alpha)| < |a_n|$ означает, что «поводок» $h(\alpha)$ настолько короток, что «собачка» не может добежать до нуля.



Следствие 5.54. *Для любого многочлена*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{C}[x] \quad (a_0 \neq 0)$$

найдутся такие числа $c_1, c_2, \ldots, c_s \in \mathbb{C}$ *и* $k_1, k_2, \ldots, k_s \in \mathbb{N}$, *что*

$$\begin{gathered} f = a_0(x-c_1)^{k_1}(x-c_2)^{k_2}\ldots(x-c_s)^{k_s}, \\ \text{где} \quad k_1 + \ldots + k_s = n, \quad c_i \neq c_j \quad (i \neq j;\ i,j = 1,2,\ldots,s). \end{gathered} \tag{5.18}$$

Для любого многочлена представление вида (5.18) *с указанными свойствами единственно с точностью до перестановки множителей* $(c-c_j)^{k_j}$ $(j = 1,2,\ldots,s)$. *Запись вида* (5.18) *называется* разложением многочлена f на линейные множители.

Доказательство. Существование. Пусть $f \in \mathbb{C}[x]$ и $\deg f \geq 1$. Согласно теореме 5.51 найдется $c_1 \in \mathbb{C}$, такое, что $f(c_1) = 0$. По теореме Безу имеем:

$$f = (x-c_1)f_1,$$

где $f_1 \in \mathbb{C}[x]$. Если $\deg f_1 \geq 1$, то по теореме 5.51 найдется $c_2 \in \mathbb{C}$, такое, что $f(c_2) = 0$, поэтому

$$f = (x - c_1)(x - c_2)f_2,$$

где $f_2 \in \mathbb{C}[x]$. Продолжая эти рассуждения далее (легко провести индукцию), получим

$$f = c_0(x - c_1)(x - c_2)\dots(x - c_n),$$

где c_0 — константа. Легко видеть, что коэффициент при старшей степени равен c_0, поэтому $c_0 = a_0$. После переобозначения получаем (5.18).
Единственность. Предположим, что

$$f = a_0(x - c_1)^{k_1}(x - c_2)^{k_2}\dots(x - c_s)^{k_s} = b_0(x - d_1)^{l_1}(x - d_2)^{l_2}\dots(x - d_t)^{l_t}. \tag{5.19}$$

Во-первых, $a_0 = b_0$.

Во-вторых, докажем, что $\{c_1, c_2, \dots, c_s\} = \{d_1, d_2, \dots, d_t\}$. Предположим противное: для определенности, $c_1 \neq d_j$ $(j = 1, 2, \dots, t)$. Подставив c_1 в обе части равенства (5.19), получаем слева 0, а справа ненулевое значение. Поэтому $s = t$ и мы можем считать, что $c_j = d_j$. Теперь (5.19) имеет вид

$$a_0(x - c_1)^{k_1}(x - c_2)^{k_2}\dots(x - c_s)^{k_s} = a_0(x - c_1)^{l_1}(x - c_2)^{l_2}\dots(x - c_s)^{l_s}. \tag{5.20}$$

Наконец, докажем, что $k_j = l_j$ $(j = 1, 2, \dots,$. Предположим противное: для определенности, $k_1 > l_1$. Тогда по лемме из (5.20) получаем

$$(x - c_1)^{k_1 - l_1}(x - c_2)^{k_2}\dots(x - c_s)^{k_s} = (x - c_2)^{l_2}\dots(x - c_t)^{l_t}. \tag{5.21}$$

Подставив c_1 в обе части равенства (5.21), получаем слева 0, а справа ненулевое значение. ∎

Замечание 5.55. В представлении (5.18) многочлена f в виде произведения множителей вида $(x - c_j)^{k_j}$ $(j = 1, 2, \dots, t)$ показатель степени k_j является кратностью многочлена f.

Следствие 5.56. *Всякий ненулевой многочлен $f \in \mathbb{C}[x]$ степени n имеет с учетом кратности ровно n комплексных корней.*

Заметим, что полученное следствие справедливо для любого алгебраически замкнутого поля.

5.7. Многочлены с действительными коэффициентами

Утверждение 5.57. *Пусть $f \in \mathbb{R}[x]$. Если $c \in \mathbb{C}$ — корень многочлена f, то $\overline{c}$ также является корнем этого многочлена и имеет ту же кратность.*

Доказательство. Пусть $f = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$. Так как $f(c) = 0$, то

$$a_0c^n + a_1c^{n-1} + \dots + a_{n-1}c + a_n = 0,$$

откуда

$$\overline{a_0c^n + a_1c^{n-1} + \dots + a_{n-1}c + a_n} = \overline{0},$$

поэтому

$$\overline{a}_0\overline{c}^n + \overline{a}_1\overline{c}^{n-1} + \dots + \overline{a}_{n-1}\overline{c} + \overline{a}_n = 0.$$

Но $a_j \in \mathbb{R}$ $(j = 1, 2, \ldots, n)$, следовательно, $\overline{a}_j = a_j$, поэтому

$$a_0\overline{c}^n + a_1\overline{c}^{n-1} + \ldots + a_{n-1}\overline{c} + a_n = 0,$$

т. е. $f(\overline{c}) = 0$.

Чтобы показать, что корень $\overline{c}$ имеет ту же кратность, что и c достаточно применить те же рассуждения к производным многочлена f и воспользоваться следствием 5.37. ∎

Следствие 5.58. *Для любого многочлена*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{R}[x] \quad (a_0 \neq 0)$$

найдутся числа $c_1, c_2, \ldots, c_s \in \mathbb{R}$, $p_1, p_2, \ldots, p_t \in \mathbb{R}$, $q_1, q_2, \ldots, q_t \in \mathbb{R}$, $k_1, k_2, \ldots, k_s \in \mathbb{N}$, $l_1, l_2, \ldots, l_t \in \mathbb{N}$, *такие, что*

$$f = a_0(x - c_1)^{k_1} \ldots (x - c_s)^{k_s}(x^2 + p_1x + q_1)^{l_1} \ldots (x^2 + p_tx + q_t)^{l_t}, \tag{5.22}$$

где

$$k_1 + \ldots + k_s + 2l_1 + \ldots + 2l_t = n,$$
$$c_i \neq c_j \quad (i \neq j;\ i, j = 1, 2, \ldots, s),$$
$$x^2 + p_ix + q_i \neq x^2 + p_jx + q_j \quad (i \neq j;\ i, j = 1, 2, \ldots, t),$$

причем многочлены $x^2 + p_jx + q_j$ *вещественных корней не имеют. Для любого многочлена* $f \in \mathbb{R}[x]$ *представление вида* (5.22) *с указанными свойствами единственно с точностью до перестановки множителей.*

Доказательство. Существование. Согласно следствию 5.54 и утверждению 5.57

$$f = a_0(x - c_1)^{k_1} \ldots (x - c_s)^{k_s}(x - d_1)^{l_1}(x - \overline{d}_1)^{l_1} \ldots (x - d_t)^{l_t}(x - \overline{d}_t)^{l_t},$$

где $c_1, c_2, \ldots, c_s \in \mathbb{R}$, $d_1, d_2, \ldots, d_t \in \mathbb{C}$. Теперь разложение (5.22) следует из равенства

$$(x - d_j)(x - \overline{d}_j) = x^2 + p_jx + q_j,$$

в котором $p_j = -d_j - \overline{d}_j = -2\operatorname{Re} d_j \in \mathbb{R}$, $q_j = d_j\overline{d}_j = |d_j|^2 \in \mathbb{R}$.

Единственность. Чтобы по представлению (5.22) получить разложение на линейные множители (5.18) достаточно разложить на линейные множители каждый из квадратных многочленов $x^2 + p_jx + q_j$. Каждый из этих многочленов имеет вещественные коэффициенты и пару комплексно сопряженных корней. Если бы для одного и того же многочлена существовали различные разложения вида (5.22) с указанными свойствами, то мы из них получили бы различные представления (5.18), что противоречит следствию 5.54. ∎

Пример 5.59. Найдем разложение вида (5.22) для многочлена $f = x^4 + 4$. Корнями этого многочлена являются все значения корня 4-й степени из 4, т.е. $\pm 1 \pm i$, поэтому разложение на линейные множители (5.18) имеет вид $f = (x-1-i)(x-1+i)(x+1-i)(x+1+i)$. Перемножая множители, соответствующие комплексно сопряженным корням, получаем требуемое разложение $f = (x^2 - 2x + 2)(x^2 + 2x + 2)$.

Следствие 5.60. *Произвольный многочлен нечетной степени с вещественными коэффициентами имеет по крайней мере один вещественный корень.*

Доказательство. По следствию 5.58, так как степень многочлена нечетна, то в разложении вида (5.22) обязательно найдется по крайней мере один линейный множитель. ∎

Упражнение 5.61. Указанные многочлены разложить а) на линейные множители полем $\mathbb{C}$; б) на линейные и квадратичные множители над полем $\mathbb{R}$:

1) $x^3 + x + 2$;
2) $x^4 + 4$.

5.8. Интерполяционный многочлен

Рассмотрим таблицу чисел

x_0	x_1	$\dots$	x_n
y_0	y_1	$\dots$	y_n

$$, \qquad x_i \neq x_j, \qquad (i \neq j). \tag{5.23}$$

Многочлен $f \in \mathbb{C}[x]$ степени не выше n, удовлетворяющий условиям

$$f(x_j) = y_j \quad (j = 0, 1, \dots, n) \tag{5.24}$$

назовем *интерполяционным многочленом*, относящимся к интерполяционной таблице (5.23).

Теорема 5.62. *Для любой таблицы интерполяции* (5.23) *интерполяционный многочлен существует и единственен.*

Доказательство. Существование. Легко видеть, что многочлен

$$f = \sum_{j=0}^{n} y_j \cdot \frac{(x - x_1) \cdot \ldots \cdot (x - x_{j-1}) \cdot (x - x_{j+1}) \cdot \ldots \cdot (x - x_n)}{(x_j - x_1) \cdot \ldots \cdot (x_j - x_{j-1}) \cdot (x_j - x_{j+1}) \cdot \ldots \cdot (x_j - x_n)}, \tag{5.25}$$

называемый *интерполяционным многочленом в форме Лагранжа*, является интерполяционным для таблицы (5.23).
Единственность. Пусть f, g — два интерполцционных многочлена, соответствующих одной таблице интерполяции (5.23). Рассмотрим многочлен $h = f - g$. Имеем $h(x_j) = 0$ $(j = 0, 1, \dots, n)$. Таким образом, многочлен h степени, не превосходящей n, имеет не менее $n + 1$ корней. По следствию 5.56 получаем, что $h = 0$, т. е. $f = g$. ∎

Пример 5.63. Интерполяционный многочлен Лагранжа для таблицы из 3 значений

x_0	x_1	x_2
y_0	y_1	y_2

имеет вид:

$$f = y_0 \cdot \frac{(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)} + y_1 \cdot \frac{(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)} + y_2 \cdot \frac{(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)}.$$

Пример 5.64. Построим интерполяционный многочлен по таблице

x_j	1	2	3
y_j	-6	-6	-4

По формуле (5.25) имеем

$$f = -6 \cdot \frac{(x - 2)(x - 3)}{(1 - 2)(1 - 3)} - 6 \cdot \frac{(x - 1)(x - 3)}{(2 - 1)(2 - 3)} - 4 \cdot \frac{(x - 1)(x - 2)}{(3 - 1)(3 - 2)} = x^2 - 3x - 4.$$

Следствие 5.65. *Пусть F — некоторое подполе поля $\mathbb{C}$. Для любых многочленов f и g из $F[x]$*

$$f = g \qquad \Leftrightarrow \qquad \forall c \in F \quad f(c) = g(c).$$

Доказательство. Если $f = g$, то, очевидно, $f(c) = g(c)$ для всех $c \in F$. Обратно, пусть $f(c) = g(c)$ для всех $c \in F$, но $f \neq g$. Это противоречит теореме 5.62. Действительно, положим $n = \max\{\deg f,\ \deg g\}$ и рассмотрим в F $n+1$ попарно различных чисел $x_0, x_1, \ldots, x_n$. Интерполяционный многочлен степени, не превосходящей n, принимающий в точках x_j значения $f(x_j) = g(x_j)$ существует и единственен, поэтому $f = g$. ∎

Замечание 5.66. Мы показали, что два многочлена, рассматриваемых с алгебраической точки зрения: т. е. как алгебраические выражения, равны тогда и только тогда, когда совпадают соответствующие им функции. Таким образом, «алгебраическая» точка зрения на многочлены как на формальные выражения совпадает с «функциональной» точкой зрения на них как на функции $f : F \to F$, если F — *числовое* поле. Как мы уже видели, над произвольными полями эти точки зрения различны.

Упражнение 5.67. Найти интерполяционный многочлен по таблице его значений:

1)

x_j	0	1	2	3
y_j	-1	-1	1	11

2)

x_j	0	1	2	3
y_j	-2	-2	-2	4

Упражнение 5.68. В $\mathbb{Z}_7[x]$ найти многочлен f 4-й степени, такой, что $f(0) = 1$, $f(1) = 4$, $f(2) = 6$, $f(3) = 0$, $f(4) = 3$.

5.8.1. Интерполяционный многочлен Ньютона

Рассмотрим еще один способ нахождения интерполяционного многочлена — *метод Ньютона*. Интерполяционный многочлен для таблицы (5.23) ищется в виде

$$f = c_0 + c_1(x - x_0) + c_2(x - x_0)(x - x_1) + \ldots + c_n(x - x_0)(x - x_1)\ldots(x - x_{n-1}). \qquad (5.26)$$

Последовательно полагая $x = x_j$ $(j = 0, 1, \ldots, n)$, находим $c_0, c_1, \ldots c_n$.

Пример 5.69. Методом Ньютона построим интерполяционный многочлен по таблице интерполяции из примера 5.64. Ищем многочлен в виде

$$f = c_0 + c_1(x - x_0) + c_2(x - x_0)(x - x_1). \qquad (5.27)$$

Полагая в (5.27) $x = x_0$, получаем $-6 = c_0$.
Полагая $x = x_1$, получаем $-6 = -6 + c_1(2 - 1)$, откуда $c_1 = 0$.
Полагая $x = x_2$, получаем $-4 = -6 + 0 \cdot (2 - 1) + c_2(3 - 1)(3 - 2)$, откуда $c_2 = 1$.
Итак, $f = -6 + (x - 1)(x - 2) = x^2 - 3x - 4$.

Для эффективного вычисления коэффициентов интерполяционного многочлена f в форме Ньютона введем так называемые разделенные разности. Пусть f — интерполяционный многочлен, построенный по таблице (5.23), а $z_0, z_1, \ldots, z_n$ — некоторые числа из F. *Разделенной разностью первого порядка* называется величина

$$f(z_0, z_1) = \frac{f(z_0) - f(z_1)}{z_0 - z_1},$$

разделенной разностью второго порядка называется

$$f(z_0, z_1, z_2) = \frac{f(z_0, z_1) - f(z_1, z_2)}{z_0 - z_2}$$

и т. д. Вообще, *разделенная разность k-го порядка* определяется через разделенную разность $(k-1)$-го порядка следующим образом:

$$f(z_0, z_1, \ldots, z_k) = \frac{f(z_0, z_1, \ldots, z_{k-1}) - f(z_1, z_2, \ldots, z_k)}{z_0 - z_k}.$$

Заметим, что так как $f(x_0) = y_0$, т. е. x_0 является корнем многочлена $f - y_0$, то $f(x, x_0)$ представляет собой многочлен и степень этого многочлена на 1 меньше степени f. Аналогично, $f(x, x_0, x_1)$ также является многочленом и степень его на 1 меньше степени $f(x, x_0)$ и т. д. Наконец, $f(x, x_0, x_1, \ldots, x_n) = 0$.

Из определения разделенных разностей получаем

$$f = f(x_0) + (x - x_0)f(x, x_1),$$

$$f(x, x_0) = f(x_0, x_1) + (x - x_1)f(x, x_0, x_1),$$

$$f(x, x_0, x_1) = f(x_0, x_1, x_2) + (x - x_2)f(x, x_0, x_1, x_2)$$

и т. д., откуда

$$f = f(x_0) + (x - x_0)f(x_0, x_1) + (x - x_0)(x - x_1)f(x_0, x_1, x_2) + \ldots$$
$$\ldots + (x - x_0)(x - x_1)\ldots(x - x_{n-1})f(x_0, x_1, \ldots, x_n).$$

В силу единственности представления многочлена f в виде (5.26), получаем, что коэффициенты c_j в (5.26) суть разделенные разности, а именно:

$$c_j = f(x_0, x_1, \ldots, x_j) \qquad (j = 0, 1, \ldots, n).$$

Вычислять разделенные разности удобно в таблице следующего вида:

$$\begin{array}{c|cccc}
x_0 & f(x_0) = y_0 & & & \\
 & & f(x_0, x_1) & & \\
x_1 & f(x_1) = y_1 & & f(x_0, x_1, x_2) & \\
 & & f(x_1, x_2) & & \ddots \\
x_2 & f(x_2) = y_2 & & & f(x_0, x_1, \ldots, x_n) \\
\vdots & \vdots & & & \\
 & & f(x_{n-1}, x_n) & & \\
x_n & f(x_n) = y_n & & &
\end{array}$$

Пример 5.70. Построим интерполяционный многочлен f по таблице

x_j	-2	-1	0	1	2
y_j	3	8	17	24	47

Составим таблицу разделенных разностей:

-2	**3**				
		5			
-1	8		**2**		
		9		$\mathbf{-1}$	
0	17		-1		**1**
		7		3	
1	24		8		
		23			
2	47				

Таким образом,

$$f = (x+2)(x+1)x(x-1) - (x+2)(x+1)x + 2(x+2)(x+1) + 5(x+2) + 3.$$

Для раскрытия скобок в (5.26), т. е. нахождения самих коэффициентов интерполяционного многочлена, существует эффективная процедура. Действительно, рассматривая (5.26), заметим, что коэффициент c_0 равен остатку от деления f на $x - x_0$; коэффициент c_1 равен остатку от деления полученного на предыдущем шаге частного на $x - x_1$ и т. д. Таким образом, для раскрытия скобок в (5.26) можно применить схему, аналогичную методу, проиллюстрированному в примере 5.46 (1-й способ).

Пример 5.71. Для многочлена f из примера 5.70 составим следующую таблицу, которую будем заполнять снизу вверх:

	1	**1**	**-2**	**7**	**17**
-2	1	-1	0	7	3
-1	1	-2	2	5	
0	1	-2	2		
1	1	-1			
2	1				

Итак, $f = x^4 + x^3 - 2x^2 + 7x + 17$.

5.9. Формулы Виета

Рассмотрим задачу нахождения коэффициентов многочлена по его корням.

Раскладывая квадратный многочлен x^2+px+1 на линейные множители, раскрывая скобки и приводя подобные, получаем

$$x^2 + px + 1 = (x - c_1)(x - c_2) = x^2 - (c_1 + c_2)x + c_1c_2,$$

откуда

$$p = -(c_1 + c_2), \qquad q = c_1c_2.$$

Это хорошо известные *формулы Виета*, связывающие коэффициенты квадратного многочлена и его корни.

То же самое можно проделать с кубическим многочленом (со старшим коэффициентом 1)

$$x^3 + px^2 + qx + r = (x - c_1)(x - c_2)(x - c_3) = x^3 - (c_1 + c_2 + c_3)x^2 + (c_1c_2 + c_1c_3 + c_2c_3)x - c_1c_2c_3,$$

откуда

$$p = -(c_1 + c_2 + c_3), \qquad q = c_1c_2 + c_1c_3 + c_2c_3, \qquad r = -c_1c_2c_3.$$

Рассмотрим теперь многочлен n-й степени со старшим коэффициентом 1:

$$f = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = (x - c_1)(x - c_2)\ldots(x - c_n).$$

Раскрывая скобки в правой части и собирая коэффициенты при каждой степени, получаем *формулы Виета*:

$$\begin{gathered}
a_1 = -(c_1 + c_2 + \ldots + c_n), \\
a_2 = c_1c_2 + c_1c_3 + \ldots + c_{n-1}c_n, \\
a_3 = -(c_1c_2c_3 + c_1c_2c_4 + \ldots + c_{n-2}c_{n-1}c_n), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_j = (-1)^j \sum_{1 \le i_1 < i_2 < \ldots < i_j \le n} a_{i_1}a_{i_2}\ldots a_{i_j}, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_{n-1} = (-1)^{n-1}(c_1c_2\ldots c_{n-1} + c_1\ldots c_{n-2}c_n + \ldots + c_2c_3\ldots c_n), \\
a_n = (-1)^n c_1c_2\ldots c_n.
\end{gathered} \tag{5.28}$$

Пример 5.72. Найдем многочлен f минимальной степени со старшим коэффициентом 1, у которого 1, 2 — простые корни, а 3 — корень кратности 2. Очевидно этим многочленам является $f = (x-1)(x-2)(x-3)^2$. По формулам (5.28) получаем

$$\begin{gathered}
a_1 = -(1 + 2 + 3 + 3) = -9, \\
a_2 = 1\cdot 2 + 1\cdot 3 + 1\cdot 3 + 2\cdot 3 + 2\cdot 3 + 3\cdot 3 = 29, \\
a_3 = -(1\cdot 2\cdot 3 + 1\cdot 2\cdot 3 + 1\cdot 3\cdot 3 + 2\cdot 3\cdot 3) = -39, \\
a_4 = 1\cdot 2\cdot 3\cdot 3 = 18.
\end{gathered}$$

Поэтому $f = x^4 - 9x^3 + 29x^2 - 39x + 18$.

Упражнение 5.73. По заданным корням построить многочлен наименьшей степени а) с комплексными коэффициентами; б) с вещественными коэффициентами:
1) двойной корень i, простые корни 1, 2, 3;
2) двойной корень 1, простые корни $1 - 2i$, 2, 3.

5.10. Неприводимые многочлены

Пусть F — поле. Многочлен $f \in F[x]$ ненулевой степени называется *неприводимым* над полем F, если он не имеет делителей степени большей 0 и меньшей $\deg f$. В противном случае f назвается *приводимым*. Другими словами, многочлен $f \in F[x]$ ненулевой степени приводим над полем F, если его можно представить в виде $f = gh$, где $g, h \in F[x]$ и $1 \le \deg g < \deg f$, $1 \le \deg h < \deg f$. Очевидно, любой многочлен степени 1 неприводим. Далее, если f неприводим, то и cf неприводим для любой константы c.

Замечание 5.74. Обращаем внимание, что свойство многочлена быть неприводимым зависит от того, над каким полем рассматривается этот многочлен. Например, многочлен $f = x^2+1 = (x-i)(x+i)$, очевидно, неприводим над $\mathbb{R}$ и $\mathbb{Q}$, но приводим над $\mathbb{C}$. Многочлен $f = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ неприводим над $\mathbb{Q}$, но приводим над $\mathbb{C}$ и $\mathbb{R}$.

Легко видеть, что если многочлен степени выше 1 имеет корень из F, то он приводим над F. Обратное в общем случае не верно. Например, многочлен x^4+4 ни рациональных, ни даже вещественных корней не имеет, но раскладывается на рациональные множители, т.е. является приводимым над $\mathbb{Q}$ и $\mathbb{R}$ (см. пример 5.59).

Замечание 5.75. Понятие неприводимого многочлена можно сформулировать не над полем, а над кольцом. В дальнейшем, например, нам понадобится понятие неприводимого многочлена над кольцом $\mathbb{Z}$. Заметим однако, что многие свойства, устанавливаемые в этом разделе для неприводимых над полем многочленов, не верны для многочленов, неприводимых над кольцом.

Следствие 5.76. *Неприводимыми над $\mathbb{C}$ многочленами являются все многочлены первой степени из $\mathbb{C}[x]$ и только они. Неприводимыми над $\mathbb{R}$ многочленами являются все многочлены первой степени из $\mathbb{R}[x]$ и все многочлены второй степени из $\mathbb{R}[x]$ с отрицательным дискриминантом и только они.*

Доказательство. Первая часть утверждения вытекает из следствия 5.54. Вторая часть утверждения вытекает из следствия 5.58. ∎

Утверждение 5.77. *Пусть f — произвольный, а h — неприводимый многочлен. Тогда $f \vdots h$ или многочлены f и h взаимно просты.*

Доказательство. Пусть d — НОД многочленов f и h. Если $\deg d = 0$, то f и h взаимно просты. Пусть $\deg d > 0$. Так как $h \vdots d$, а h — неприводимый, то $h = cd$, где c — ненулевая константа. Так как $f \vdots d$, то $f \vdots h$. ∎

Утверждение 5.78. *Пусть $fg \vdots h$, причем h — неприводимый. Тогда $f \vdots h$ или $g \vdots h$.*

Доказательство. Покажем, что если $f \not\vdots h$, то $g \vdots h$. Действительно, по утверждению 5.77, если $f \not\vdots h$, то f и h взаимно просты. Теперь $g \vdots h$ следует из утверждения 5.26. ∎

Теорема 5.79. *Для любого многочлена $f \in F[x]$ ненулевой степени существуют такие неприводимые многочлены $p_1, p_2, \ldots, p_s$, что*

$$f = p_1 p_2 \ldots p_s. \tag{5.29}$$

Разложение вида (5.29) единственно с точностью до константных множителей и перестановки многочленов p_j.

Доказательство. Существование. Если f — неприводимый, то разложение получено. В противном случае найдутся многочлены g_1 и g_2 степени меньшей $\deg f$, такие, что $f = g_1 g_2$. К ним применим те же рассуждения, и т. д. (можно применить индукцию по степени многочлена), пока не получим требуемого разложения.
Единственность. Покажем, что если

$$p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t \tag{5.30}$$

— два разложения f на неприводимые множители, то $s = t$ и при соответствующей нумерации $p_j = c_j q_j$, где c_j — ненулевая константа ($j = 1, 2, \ldots, s$).

Из (5.30) следует, что $p_1 p_2 \ldots p_s \vdots q_1$. Так как q_1 — неприводимый, то по утверждению 5.78 найдется j, такое, что $p_j \vdots q_1$. Не нарушая общности, будем считать, что $j = 1$, т. е. $p_1 \vdots q_1$.

Так как p_1 неприводим, то $p_1 = c_1 q_1$ для некоторой ненулевой константы c_1. Переобозначим $p_2 = c_1 p_2$. Сокращая равенство на q_1 (напомним, что в $F[x]$ нет делителей нуля), приходим к равенству

$$p_2 p_3 \dots p_s = q_2 q_3 \dots q_t,$$

к которому применяем те же рассуждения, и т. д. (можно применить индукцию), пока не получим $p_s = q_s$. ∎

Следствие 5.80. *Для любого многочлена $f \in F[x]$ ненулевой степени существуют неприводимые многочлены $p_1, p_2, \dots, p_s$ и натуральные числа $k_1, k_2, \dots, k_s$, такие, что*

$$f = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}, \tag{5.31}$$

$p_i \not\vdots p_j$ $(i \neq j)$. Разложение вида (5.31) с указанными свойствами единственно с точностью до константных множителей и перестановки многочленов p_j.

Запись вида (5.31) называется разложением многочлена f на неприводимые множители. *Величина k_j называется* кратностью *множителя p_j.*

Следствие 5.81. *Для любого многочлена $f \in F[x]$ ненулевой степени существуют неприводимые многочлены $p_1, p_2, \dots, p_s$ со старшим коэффициентом 1 и натуральные числа $k_1, k_2, \dots, k_s$, такие, что*

$$f = a_0 p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}, \tag{5.32}$$

$p_i \neq p_j$ $(i \neq j)$, где a_0 — коэффициент при старшем члене многочлена f. Разложение вида (5.32) с указанными свойствами единственно с точностью до перестановки множителей.

Замечание 5.82. Следствия 5.54 и 5.58 являются частными случаями только что установленного следствия 5.81. Разложением многочлена из $\mathbb{C}[x]$ на неприводимые над $\mathbb{C}$ множители является разложение на линейные множители (5.18). Разложением многочлена из $\mathbb{R}[x]$ на неприводимые над $\mathbb{R}$ множители является разложение (5.18).

Следствие 5.83. *Пусть (5.31) — разложение многочлена $f \in F[x]$ на неприводимые множители. Тогда для любого делителя d этого многочлена найдутся такие целые неотрицательные $l_1, l_2, \dots, l_s$ и такое $c \in F$, что*

$$d = c p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}.$$

Доказательство. Если d — произвольный делитель многочлена f, то для некоторого q имеем $f = qd$, поэтому в разложении многочлена d на неприводимые могут встретиться только многочлены $c_1 p_1, c_2 p_2, \dots, c_s p_s$, где c_j — константы $(j = 1, 2, \dots, s)$, так как противное противоречило бы единственности разложения f. ∎

Теорема 5.84. *Пусть*

$$f = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t} \; p_{t+1}^{k_{t+1}} p_{t+2}^{k_{t+2}} \dots p_s^{k_s},$$
$$g = p_1^{l_1} p_2^{l_2} \dots p_t^{l_t} \; p_{s+1}^{l_{s+1}} p_{s+2}^{l_{s+2}} \dots p_r^{l_r},$$

и многочлены p_j неприводимы, $p_i \not\vdots p_j$ $(i \neq j;\ i, j = 1, 2, \dots, r)$, $m_j = \min\{k_j,\ l_j\}$ $(j = 1, 2, \dots, t)$. Тогда

$$d = p_1^{m_1} p_2^{m_2} \dots p_t^{m_t}$$

является наибольшим общим делителем многочленов f и g.

Доказательство. Очевидно, d является делителем как многочлена f, так и многочлена g и по следствию 5.86 любой их общий делитель является делителем многочлена d. ∎

Теорема 5.85. *Неприводимый множитель кратности k многочлена f является неприводимым множителем кратности $k-1$ многочлена f'. Простой неприводимый множитель многочлена f не входит в разложение многочлена f' на неприводимые.*

Доказательство. Аналогично доказательству теоремы 5.36. ∎

Следствие 5.86. *Пусть (5.31) — разложение многочлена $f \in F[x]$ на неприводимые множители. Тогда многочлен*

$$d = p_1^{k_1-1} p_2^{k_2-1} \dots p_s^{k_s-1} \tag{5.33}$$

является наибольшим общим делителем многочленов f и f' и, следовательно,

$$\frac{f}{d} = p_1 p_2 \dots p_s. \tag{5.34}$$

Доказательство. Формула (5.33) следует из теорем 5.84 и 5.85. Соотношение 5.34 непосредственно вытекает из (5.31) и (5.33). ∎

Замечание 5.87. Следствие 5.86 дает алгоритм *избавления от кратных множителей*, т. е. алгоритм построения по заданному многочлену f многочлена g с теми же множителями в разложении на неприводимые, но кратности 1. Заметим, что g имеет те же корни, что и f, но все корни g — простые. В некоторых случаях это позволяет определить все корни многочлена f.

Пример 5.88. Избавимся от кратных множителей в многочлене $f = x^5 + 7x^4 + 10x^3 - 18x^2 - 27x + 27$. Имеем $f' = 5x^4 + 28x^3 + 30x^2 - 36x - 27$. НОД многочленов f и f' (найденный алгоритмом Евклида) равен $d = -9 + x^3 + 5x^2 + 3x$, откуда $f/d = x^2 + 2x - 3 = (x-1)(x+3)$. Последовательным делением f на $x-1$ и $x+3$ (по схеме Горнера) определим кратность корней 1, -3 в многочлене f. Получим $f = (x-1)^2(x+3)^3$.

Рассмотрим еще один способ, позволяющий иногда найти все корни многочлена и сразу указать их кратности. Пусть d_1 — НОД многочлена f и его производной f'; d_2 — НОД многочлена d_1 и его производной d_1'; d_3 — НОД многочленов d_2 и d_2' и т. д. до тех пор, пока не будет получен многочлен d_s нулевой степени. Положим

$$g_1 = \frac{f}{d_1}, \quad g_2 = \frac{d_1}{d_2}, \quad \dots, \quad g_s = \frac{d_{s-1}}{d_s}$$

и далее

$$f_1 = \frac{g_1}{g_2}, \quad f_2 = \frac{g_2}{g_3}, \quad \dots, \quad f_s = g_s.$$

Легко проверить, что все корни многочленов $f_1, f_2, \dots, f_s$ простые, причем корнями многочлена f_j являются все корни кратности j многочлена f и только они ($j = 1, 2, \dots, s$). Корней кратности большей s у f нет.

Пример 5.89. Для многочлена $f = x^7 + 2x^6 + 3x^5 + x^4 - x^3 - 3x^2 - 2x - 1$ получаем

$$d_1 = x^4 + 2x^3 + 3x^2 + 2x + 1, \quad d_2 = x^2 + x + 1, \quad d_3 = 1,$$

далее

$$g_1 = x^3 - 1, \quad g_2 = x^2 + x + 1 \quad , g_3 = x^2 + x + 1,$$

откуда

$$f_1 = x - 1, \quad f_2 = 1, \quad f_3 = x^2 + x + 1 = \left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right) \cdot \left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right).$$

Итак, многочлен f имеет один простой корень 1 и два трехкратных корня $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$.

5.11. Многочлены с рациональными коэффициентами

В данном разделе рассматриваются три взаимосвязанные задачи: проблема отыскания рациональных корней многочлена с рациональными коэффициентами; задача установления неприводимости над $\mathbb{Q}$ заданного многочлена и задача разложения заданного многочлена на неприводимые над $\mathbb{Q}$ многочлены. Оказывается, достаточно научиться решать эти задачи не над полем $\mathbb{Q}$, а над кольцом $\mathbb{Z}$.

Очевидно, произвольный многочлен $f \in \mathbb{Q}[x]$ домножением его коэффициентов на НОК их знаменателей можно превратить в многочлен $g \in \mathbb{Z}[x]$. При этом все корни многочлена f являются корнями многочлена g и наоборот. Таким образом, задача отыскания корней многочлена с рациональными коэффициентами сводится к задаче отыскания корней многочлена с целыми коэффициентами. Кроме того, легко видеть, что f неприводим над $\mathbb{Q}$ тогда и только тогда, когда неприводим над $\mathbb{Q}$ многочлен g. Далее мы установим более сильный результат: многочлен f неприводим над $\mathbb{Q}$ тогда и только тогда, когда g неприводим над $\mathbb{Z}$ и, следовательно, задачи проверки неприводимости над $\mathbb{Q}$ и нахождения разложения на неприводимые над $\mathbb{Q}$ сведена к соответствующим задачам над $\mathbb{Z}$.

Приведем следующее необходимое условие на рациональные корни многочлена с целыми коэффициентами.

Теорема 5.90. *Пусть*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{Z}[x],$$

$p, q \in \mathbb{Z}$, $p \neq 0$, $q \neq 0$, $a_0 \neq 0$, $\text{НОД}(p, q) = 1$, $f(p/q) = 0$, *тогда*

1) $a_0 \vdots q$,

2) $a_n \vdots p$,

3) $f(m) \vdots (p - mq)$ *для любого* $m \in \mathbb{Z}$.

Доказательство. 1), 2) Так как $f(p/q) = 0$, то

$$f\left(\frac{p}{q}\right) = a_0 \cdot \left(\frac{p}{q}\right)^n + a_1 \cdot \left(\frac{p}{q}\right)^{n-1} + \ldots + a_{n-1} \cdot \frac{p}{q} + a_n = 0.$$

Домножая обе части полученного равенства на q^n, получаем

$$a_0p^n + a_1p^{n-1}q + \ldots + a_{n-1}pq^{n-1} + a_nq^n = 0. \tag{5.35}$$

Слагаемые в левой части равенства (5.35) со второго до последнего делятся на q, следовательно, первое слагаемое a_0p^n также делится на q, но так как $\text{НОД}(p, q) = 1$, то $a_0 \vdots q$. Аналогично, слагаемые с первого до предпоследнего в левой части равенства (5.35) делятся на p, следовательно, последнее слагаемое a_nq^n также делится на p, но так как $\text{НОД}(p, q) = 1$, то $a_n \vdots p$.

3) Разделим f на $x - m$. Получим в частном q, а в остатке $f(m)$:

$$f = (x - m)g + f(m). \tag{5.36}$$

Заметим, что $g \in \mathbb{Z}[x]$. Из (5.36) при $x = p/q$ получаем $0 = (p/q - m)g(p/q) + f(m)$. Домножаем обе части этого равенства на q^n и применяем рассуждения, аналогичные пп. 1), 2).

∎

Теорема 5.90 позволяет предложить следующий метод нахождения всех рациональных корней многочлена $f \in \mathbb{Z}[x]$. Для всех делителей p коэффициента a_n и всех делителей q коэффициента a_0, если НОД$(p,q)=1$, проверим (например, с помощью схемы Горнера) равенство $f(p/q)=0$. Проверку целесообразно начать с $q=1$ и всех p, делящих a_n: полученные в результате них значения $f(m)$, где $m=p/q\in\mathbb{Z}$, можно использовать для отсеивания дальнейших пробных p и q с помощью условия $f(m)\vdots(p-mq)$. Как только один из корней p/q найден, многочлен f можно разделить на $x-p/q$ и применим ту же процедуру к частному.

Пример 5.91. Найдем все рациональные корни многочлена $f=6x^6-13x^5-4x^4+24x^3-21x^2+4x+10$. Делителями свободного коэффициента являются числа ±1, ±2, ±5, ±10. Положительными делителями старшего коэффициента являются числа 1, 2, 3, 6. Таким образом, рациональными корнями многочлена f могут являться только следующие числа:

$$\pm1,\ \pm2,\ \pm5,\ \pm10,\ \pm\frac{1}{2},\ \pm\frac{5}{2},\ \pm\frac{1}{3},\ \pm\frac{2}{3},\ \pm\frac{5}{3},\ \pm\frac{10}{3},\ \pm\frac{1}{6},\ \pm\frac{5}{6}.$$

Так как $f(1)=6$, то отсеиваются все числа p/q, для которых $6\not\vdots p-q$, т. е. отсеиваем

$$5,\ 10,\ \frac{10}{3},\ \frac{1}{6},\ -10,\ -\frac{5}{2},\ -\frac{1}{3},\ -\frac{5}{3},\ -\frac{10}{3},\ -\frac{1}{6},\ -\frac{5}{6}.$$

Так как $f(-1)=-24$, то отсеиваются все числа p/q, для которых $-24\not\vdots p+q$, т. е. из оставшихся отсеиваем

$$\frac{5}{2},\ \frac{2}{3},\ \frac{5}{6}.$$

В списке возможных кандидатов остались

$$2,\ \frac{1}{2},\ \frac{1}{3},\ \frac{5}{3},\ -2,\ -5,\ -\frac{1}{2},\ -\frac{2}{3}.$$

Схемой Горнера устанавливая значение многочлена f для каждого из этих чисел, получаем, что его рациональными корнями являются только $5/3$ и $-1/2$.

Упражнение 5.92. Найти все рациональные корни и определить их кратности:
1) $3x^5-5x^4+7x^2-4x^3-8x+4$;
2) $5x^6+10x^3-27x^2-16x^5-10x+3x^4+3$.

Рассмотрим теперь задачи определения неприводимости многочлена над $\mathbb{Q}$ и разложения заданного многочлена на неприводимые.

Ненулевой многочлен $f=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\in\mathbb{Z}[x]$ называется *примитивным*, если его коэффициенты $a_0,a_1,\ldots,a_n$ взаимно просты в совокупности.

Утверждение 5.93 (Лемма Гаусса)**.** *Произведение примитивных многочленов является примитивным многочленом.*

Доказательство. Пусть

$$\begin{aligned} f=gh&=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,\\ g&=b_0x^m+b_1x^{m-1}+\ldots+b_{m-1}x+b_m,\\ h&=c_0x^k+c_1x^{k-1}+\ldots+c_{k-1}x+c_k \end{aligned}$$

и многочлены g и h примитивны. Поэтому для любого простого p найдутся такие s и t, что

$$b_i\vdots p\quad(i=0,1,\ldots,s-1),\quad b_s\not\vdots p, c_j\vdots p\quad(j=0,1,\ldots,t-1),\quad c_t\not\vdots p.$$

Докажем, что $a_{s+t} \not\vdots p$, что докажет примитивность многочлена f. Имеем

$$a_{s+t} = \sum_{i+j=s+t} b_i c_j = \ldots + b_{s-2}c_{t+2} + b_{s-1}c_{t+1} + b_s c_t + b_{s+1}c_{t-1} + b_{s+2}c_{t-2} + \ldots$$

Каждое из слагаемых $b_{s-1}c_{t+1}$, $b_{s-2}c_{t+2}$ и т. д. делится на p, так как $b_i \vdots p$ при $i < s$. Каждое из слагаемых $b_{s+1}c_{t-1}$, $b_{s+2}c_{t-2}$ и т. д. делится на p, так как $c_j \vdots p$ при $j < t$. Но $b_s c_t \not\vdots p$. Следовательно, $a_{s+t} \not\vdots p$. ∎

Теорема 5.94. *Если многочлен $f \in \mathbb{Z}[x]$ допускает разложение на многочлены $g \in \mathbb{Q}[x]$ и $h \in \mathbb{Q}[x]$, то f допускает также разложение на многочлены $cg \in \mathbb{Z}[x]$ и $c_1 h \in \mathbb{Z}[x]$, где c, c_1 — некоторые константы.*

Доказательство. Очевидно, найдутся такие целые p, q, p_1, q_1 что

$$g = \frac{p}{q}\widehat{g}, \quad h = \frac{p_1}{q_1}\widehat{h}, \quad \widehat{g} \in \mathbb{Z}[x], \quad \widehat{h} \in \mathbb{Z}[x],$$

НОД$(p, q) = 1$, НОД$(p_1, q_1) = 1$, причем $\widehat{g}$, $\widehat{h}$ — примитивные. Таким образом,

$$f = gh = \frac{pp_1}{qq_1}\widehat{g}\widehat{h}.$$

Так как $f \in \mathbb{Z}[x]$, то qq_1 должно сократиться с $pp_1\widehat{g}\widehat{h}$. Но по утверждению 5.93 многочлен $\widehat{g}\widehat{h}$ примитивен, поэтому знаменатель qq_1 должен сократиться с pp_1, т. е. $(pp_1)/(qq_1) \in \mathbb{Z}$. Полагая, например, $c = p_1/q_1$, $c_1 = q_1/p_1$, получаем $f = (cg)(c_1 h)$, причем

$$cg = \frac{pp_1}{qq_1}\widehat{g} \in \mathbb{Z}[x], \quad c_1 h = \widehat{h} \in \mathbb{Z}[x].$$

∎

Следствие 5.95. *Многочлен $f \in \mathbb{Z}[x]$ неприводим над $\mathbb{Q}$ тогда и только тогда, когда он неприводим над $\mathbb{Z}$, т. е. не допускает разложения на многочлены ненулевой степени из $\mathbb{Z}[x]$.*

Приведенное следствие существенно облегчает доказательство неприводимости многочленов над полем $\mathbb{Q}$.

Приведем одно из известных достаточных условий неприводимости многочлена над $\mathbb{Q}$.

Теорема 5.96 (Признак Эйзенштейна)**.** *Пусть*

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

— примитивный многочлен, причем существует простое p, такое, что

$$a_0 \not\vdots p, \qquad a_j \vdots p \quad (j = 1, 2, \ldots, n), \qquad a_n \not\vdots p^2,$$

тогда f неприводим над $\mathbb{Z}$ и, следовательно, над $\mathbb{Q}$.

Доказательство. Предположим противное. Пусть $f = gh$, где

$$g = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m \in \mathbb{Z}[x],$$

$$h = c_0x^k + c_1x^{k-1} + \ldots + c_{k-1}x + c_k \in \mathbb{Z}[x].$$

Для определенности будем считать, что $k \leq m$. Имеем

$$a_n = b_mc_k, \tag{γ_0}$$

$$a_{n-1} = b_{m-1}c_k + b_mc_{k-1}, \tag{γ_1}$$

$$a_{n-2} = b_{m-2}c_k + b_{m-1}c_{k-1} + b_mc_{k-2}, \tag{γ_2}$$

$$a_k = b_0c_k + b_1c_{k-1} + \ldots + b_kc_0, \tag{γ_{n-k}}$$

$$a_0 = b_0c_0. \tag{γ_n}$$

Так как $a_n \vdots p$ и $a_n \not\vdots p^2$, то из (γ_0) следует, что один из коэффициентов b_m или c_k делится на p, а другой нет. Рассмотрим случай $b_m \vdots p$, $c_k \not\vdots p$. Противоположный случай рассматривается аналогично.

Так как $a_{n-1} \vdots p$, $b_m \vdots p$ и $c_k \not\vdots p$, то из (γ_1) следует, что $b_{m-1} \vdots p$. Так как $a_{n-2} \vdots p$, $b_{m-1} \vdots p$, $b_m \vdots p$ и $c_k \not\vdots p$, то из (γ_2) следует, что $b_{m-2} \vdots p$. Продолжая аналогичные рассуждения далее, в частности, из (γ_{n-k}) получим, что $b_0 \vdots p$. Теперь из (γ_n) вытекает $a_0 \vdots p$. Противоречие. ∎

Следствие 5.97. *Над $\mathbb{Q}$ существует неприводимый многочлен любой, сколь угодно высокой, степени.*

Доказательство. Таковым, например, является многочлен $x^n - 2$, неприводимость которого легко проверяется с помощью теоремы 5.96, если положить $p = 2$. ∎

Упражнение 5.98. Пользуясь признаком Эйзенштейна, доказать неприводимость над полем $\mathbb{Q}$:
1) $x^4 + 8x^3 - 6x^2 + 12x - 6$;
2) $2x^5 - 9x^3 + 12x^2 - 15x^2 + 6$;
3) $x^4 + 6x^3 + 16x^2 + 20x + 11$.

Пример 5.99. Докажем, что многочлен

$$\Phi_p = x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1},$$

где p — простое, неприводим. Легко видеть, что Φ_p неприводим тогда и только тогда, когда неприводим $\Phi_p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \ldots + (x+1) + 1$. Воспользовавшись формулой бинома Ньютона, после очевидных преобразований получаем многочлен

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \sum_{k=1}^{n-1} \frac{p(p-1)\ldots(p-k+1)}{k!}x^{p-k-1},$$

к которому применим признак Эйзенштейна. Действительно, при $1 \leq k < p$, так как p — простое и $p(p-1)\ldots(p-k+1)/k! \in \mathbb{Z}$, то $(p-1)\ldots(p-k+1)/k! \in \mathbb{Z}$, поэтому

$$\frac{p(p-1)\ldots(p-k+1)}{k!} \vdots p.$$

Старший коэффициент многочлена $\Phi_p(x+1)$ равен 1 и, конечно, $1 \not\vdots p$. Свободный член равен p и, разумеется, $p \not\vdots p^2$. Следовательно, по критерию Эйзенштейна многочлен $\Phi_p(x+1)$ неприводим, поэтому неприводим и Φ_p.

5.12. Метод Шуберта–Кронекера

Метод Шуберта–Кронекера — это классический метод нахождения разложения многочлена с целыми коэффициентами на неприводимые множители. Он основан на двух простых наблюдениях. Пусть $f \in \mathbb{Z}[x]$, $\deg f = n$. Если $f = gh$, где $g \in \mathbb{Z}[x]$ и $h \in \mathbb{Z}[x]$, то $\deg g \leq s$ или $\deg h \leq s$, где $s = \lfloor n/2 \rfloor$. Далее, если $x_0 \in \mathbb{Z}$, то $f(x_0) \vdots g(x_0)$ и $f(x_0) \vdots h(x_0)$.

Метод заключается в следующем. Выбираем $x_0, x_1, \ldots, x_s$ — некоторые попарно различные целые числа. Составляем всевозможные наборы $c_0, c_1, \ldots, c_s$, такие, что c_j — произвольный делитель числа $f(x_j)$ $(j = 0, 1, \ldots, s)$. Для каждого такого набора восстанавливаем многочлен g, такой, что $g(x_j) = c_j$ $(j = 0, 1, \ldots, s)$ (например, по формуле интерполяционного многочлена Лагранжа). Делением проверяем $f \vdots g$. Если $f = gh$, то применяем к многочленам g и h ту же процедуру. Если f не делится ни на один из построенных многочленов g, то f неприводим над $\mathbb{Q}$.

Пример 5.100. С помощью метода Шуберта–Кронекера разложим многочлен $f = x^5 - 5x^4 + 6x^3 + 2x^2 - 4x + 1$ на неприводимые над $\mathbb{Q}$. Многочлен имеет степень $n = 5$, поэтому, если он приводим, то степень одного из его сомножителей g не превосходит $s = \lfloor n/2 \rfloor = 2$. Пусть $x_0 = -1$, $x_1 = 0$, $x_2 = 1$. Имеем $f(-1) = -5$, $f(0) = 1$, $f(1) = 1$. Делителями $f(-1)$ являются числа ± 1, ± 5. Делителями $f(0)$ и $f(1)$ являются числа ± 1. Таким образом, g определяется одной из следующих интерполяционных таблиц:

x	g							
-1	1	1	1	1	5	5	5	5
0	1	1	-1	-1	1	1	-1	-1
1	1	-1	1	-1	1	-1	1	-1

Остальные 8 наборов не рассматриваются, так как определяют многочлены, отличающиеся лишь знаком от многочленов, соответствующих приведенным наборам. Первый набор задает константу 1. Для оставшихся 7 наборов последовательно строим соответствующие интерполяционные многочлены.

По значениям $g(-1) = 1$, $g(0) = 1$, $g(1) = -1$ восстанавливаем интерполяционный многочлен $g = -x^2 - x + 1$. Непосредственным делением проверяем, что $f \not\vdots g$.

По значениям $g(-1) = 1$, $g(0) = -1$, $g(1) = 1$ восстанавливаем интерполяционный многочлен $g = 2x^2 - 1$. Получаем, что $f \not\vdots g$.

По значениям $g(-1) = 1$, $g(0) = -1$, $g(1) = -1$ восстанавливаем интерполяционный многочлен $g = x^2 - x - 1$. Имеем $f \not\vdots g$.

По значениям $g(-1) = 5$, $g(0) = 1$, $g(1) = 1$ восстанавливаем интерполяционный многочлен $g = 2x^2 - 2x + 1$. Имеем $f \not\vdots g$.

По значениям $g(-1) = 5$, $g(0) = 1$, $g(1) = -1$ восстанавливаем интерполяционный многочлен $g = x^2 - 3x + 1$. Получаем $f \vdots g$, а именно,

$$f = (x^2 - 3x + 1)(x^3 - 2x^2 - x + 1). \tag{5.37}$$

Легко проверить, что полученные множители рациональных корней не имеют и поэтому, так как их степени не превосходят 3, неприводимы. Таким образом, (5.37) является разложением f на неприводимые над $\mathbb{Q}$ множители и рассматривать дальнейшие наборы не нужно.

Упражнение 5.101. Разложить на неприводимые множители над полем $\mathbb{Z}_2$ все многочлены 1) 2-й степени; 2) 3-й степени.

Упражнение 5.102. Найти все неприводимые многочлены со старшим коэффициентом 1 над полем $\mathbb{Z}_3$ 1) 2-й степени; 2) 3-й степени.

Упражнение 5.103. Разложить на неприводимые множители:
1) $x^5 + x^3 + x^2 + 1$ над полем $\mathbb{Z}_2$;
2) $x^5 + 2x^4 + x^2 + 2x + 2$ над полем $\mathbb{Z}_3$;
3) $x^5 + 2x^4 + 4x^2 + 3x + 3$ над полем $\mathbb{Z}_5$.

Упражнение 5.104. Разложить на неприводимые множители $x^5 + x^4 - 2x^3 - 2x^2 + 9x + 9$
1) над $\mathbb{Z}_3$; 2) над $\mathbb{Z}_5$; 3) над $\mathbb{Z}_7$; 4) над $\mathbb{Q}$.

Упражнение 5.105. Разложение многочлена $x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ на неприводимые над полем $\mathbb{Z}_2$ имеет вид

$$(x^6 + x^5 + x^4 + x + 1)(x^2 + x + 1),$$

а над полем $\mathbb{Z}_{13}$ —

$$(x^4 + 2x^3 + 3x^2 + 4x + 6)(x^3 + 8x^2 + 4x + 12)(x + 3).$$

Найти его разложение над полем $\mathbb{Q}$ (Д. Кнут).

Упражнение 5.106. Здесь устанавливается связь между взаимной простотой многочленов над полем вычетов и полем $\mathbb{Q}$.
1) Доказать, что если многочлены f и g с целыми коэффициентами взаимно просты над полем $\mathbb{Z}_p$ для некоторого простого p, причем хотя бы один из старших коэффициентов не делится на p, то f и g взаимно просты над полем $\mathbb{Q}$.
2) Привести пример, показывающий, что обратное неверно ни для какого простого p.

Упражнение 5.107. Здесь устанавливается связь между неприводимостью многочлена над полем вычетов и полем $\mathbb{Q}$.
1) Доказать, что если многочлен f с целыми коэффициентами приводим над полем рациональных чисел, то он приводим над полем $\mathbb{Z}_p$ для любого простого p, не делящего старший коэффициент.
2) Привести пример многочлена, приводимого над $\mathbb{Q}$, но неприводимого над $\mathbb{Z}_p$, где p делит старший коэффициент.
3) Существуют многочлены с целыми коэффициентами, неприводимые над $\mathbb{Q}$, но приводимые над $\mathbb{Z}_p$ при любом простом p. Доказать, что таковым является, например, многочлен $x^4 + 1$.

Упражнение 5.108. В поле $\mathbb{Z}_{11}$ найти все решения уравнения:
1) $x^2 = 5$;
2) $x^2 = 6$;
3) $x^2 + 4x + 1 = 0$;
4) $x^2 + 2x + 1 = 0$;
5) $x^2 + 2x + 4 = 0$;
6) $x^7 = 7$;
7) $x^{10} = 1$;
8) $x^3 = a$.

Упражнение 5.109. В поле $\mathbb{Z}_p$ найти все решения уравнения:
1) $x^p = x$; 2) $x^p = a$.

5.13. Границы для комплексных и вещественных корней многочленов

Следующая теорема по существу вытекает из леммы 5.52. Для удобства повторим ее доказательство.

Теорема 5.110. *Пусть*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{C}[x], \quad a_0 \neq 0, \quad A = \max_{j=1,2,\ldots,n} |a_j|$$

и $f(\alpha) = 0$, $\alpha \in \mathbb{C}$, *тогда*

$$|\alpha| < \frac{A}{|a_0|} + 1.$$

Доказательство. Покажем, что если

$$|\alpha| \geq \frac{A}{|a_0|} + 1, \tag{5.38}$$

то α не может быть корнем многочлена f. Действительно,

$$\begin{aligned} f(\alpha) &\geq |a_0| \cdot |\alpha|^n - |a_1\alpha^{n-1} + \ldots + a_n| \geq \\ &\geq |a_0| \cdot |\alpha|^n - A|\alpha|^{n-1} + \ldots + 1| = \\ &= |a_0| \cdot |\alpha|^n - A \cdot \frac{|\alpha|^n - 1}{|\alpha| - 1} > \\ &> |a_0| \cdot |\alpha|^n - A \cdot \frac{|\alpha|^n}{A} \cdot |a_0| = \\ &= 0 \end{aligned}$$

согласно (5.38). Итак, $f(\alpha) > 0$, т. е. α не является корнем. ∎

Теорема 5.111. *Пусть*

$$f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{R}[x], \quad a_0 > 0$$

и k — минимальное, такое, что $a_k < 0$,

$$B = \max_{a_j<0} |a_j|.$$

Тогда для любого положительного вещественного корня α справедливо нервенство

$$\alpha \leq \sqrt[k]{\frac{B}{a_0}} + 1.$$

Доказательство. Пусть $\alpha > \sqrt[k]{\frac{B}{a_0}} + 1$, откуда

$$(x-1)^k > \frac{B}{a_0}. \tag{5.39}$$

Покажем тогда, что α не может быть корнем многочлена f. Имеем

$$\begin{aligned} f(\alpha) &\geq a_0\alpha^n - B(\alpha^{n-k} + \alpha^{n-k-1} + \ldots + \alpha + 1) = \\ &= a_0\alpha^n - B \cdot \frac{\alpha^{n-k+1} - 1}{\alpha - 1} > \\ &> a_0\alpha^n - B \cdot \frac{\alpha^{n-k+1}}{\alpha - 1} = \\ &= \frac{\alpha^{n-k+1}}{\alpha - 1}\left(a_0\alpha^{k-1}(\alpha - 1) - B\right) > \\ &> \frac{\alpha^{n-k+1}}{\alpha - 1}\left(a_0(\alpha - 1)^k - B\right) > \\ &> 0, \end{aligned}$$

где последнее неравенство следует из (5.39). Итак, $f(\alpha) > 0$, т. е. α не является корнем. ∎

Замечание 5.112. Если $a_j \geq 0$ $(j = 0, 1, \ldots, n)$, то положительных корней многочлен f, легко видеть, не имеет.

Замечание 5.113. Для нахождения нижней оценки отрицательных корней многочлена f достаточно применить теорему 5.111 к многочлену

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

Для нахождения нижней оценки положительных корней достаточно применить теорему 5.111 к многочлену

$$x^n f\left(\frac{1}{x}\right) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n.$$

Для нахождения верхней оценки отрицательных корней достаточно применить теорему 5.111 к многочлену

$$x^n f\left(-\frac{1}{x}\right) = a_0 - a_1 x + \ldots + a_{n-1}(-1)^{n-1}x^{n-1} + a_n(-1)^n x^n.$$

5.14. Распределение корней многочленов на вещественной оси

Системой Штурма многочлена f называется конечная последовательность многочленов

$$f_0 = f, f_1, f_2, \ldots, f_s,$$

такая, что

1) многочлены f_j, f_{j+1} не имеют общих вещественных корней $(j = 0, 1, \ldots, s-1)$;

2) если $f_0(\alpha) = 0$, то функция $f_0 f_1$ возрастает в окрестности α, меняя знак с $-$ на $+$;

3) если $f_j(\alpha) = 0$, то $f_{j-1}(\alpha)f_{j+1}(\alpha) < 0$ $(j = 1, 2, \ldots, s-1)$;

4) f_s не имеет вещественных корней.

Пусть $f_0 = f$, $f_1 = f'$ и f_j — взятый с противоположным знаком остаток при делении f_{j-2} на f_{j-1} $(j = 2, 3, \ldots, s)$. Вычисления заканчиваются, когда при делении f_{s-1} на f_s в остатке не будет получен нулевой многочлен (так как степени многочленов f_j убывают, то процесс завершится). Итак,

$$f = q_1 f' - f_2, \tag{δ_1}$$

$$f' = q_2 f_2 - f_3, \tag{δ_2}$$

$$f_{j-1} = q_j f_j - f_{j+1}, \tag{δ_j}$$

$$f_{s-2} = q_{s-1} f_{s-1} - f_s, \tag{δ_{s-1}}$$

$$f_{s-1} = q_s f_s. \tag{δ_s}$$

Таким образом, многочлены f_j лишь множителями отличаются от многочленов, получаемых в алгоритме Евклида, следовательно, f_s есть НОД f и f' и, в частности, по теореме 5.86 f_s — константа тогда и только тогда, когда f не имеет кратных корней.

Теорема 5.114. *Для произвольного многочлена $f \in \mathbb{R}[x]$, не имеющего кратных корней, система Штурма существует. В частности, системой Штурма многочлена f является последовательность $f_0 = f, f_1 = f', f_2, \ldots, f_s$, построенная согласно (δ_0)–(δ_s).*

Доказательство. Для системы, построенной согласно (δ_1)–(δ_s), докажем выполнение свойств 1)–4) в определении системы Штурма.

1) Если $f_j(\alpha) = f_{j+1}(\alpha) = 0$, то согласно (γ_j) $f_{j-1}(\alpha) = 0$. Из рассмотрения (γ_{j-1}) получаем $f_{j-2}(\alpha) = 0$ и т. д. Из рассмотрения (γ_2) и (γ_1) получаем $f(\alpha) = f'(\alpha) = 0$, что не возможно, так как f не имеет кратных корней.

2) Если $f(\alpha) = 0$ и $f'(\alpha) > 0$, то f возрастает в окрестности α, следовательно, ff' возрастает. Если $f(\alpha) = 0$ и $f'(\alpha) < 0$, то f убывает в окрестности α, и следовательно, ff' возрастает.

3) Пусть $f_j(\alpha) = 0$. Подставляя α в левую и правую части равенства (δ_j), получаем $f_{j-1}(\alpha) = -f_{j+1}(\alpha)$, поэтому $f_{j-1}(\alpha) = -f_{j+1}(\alpha) < 0$.

4) Как уже отмечалось, f_s есть НОД многочленов f и f_0. Так как f не имеет кратных корней, то по теореме 5.86 f_s — ненулевая константа, следовательно, f_s корней не имеет.

∎

Замечание 5.115. При построении системы Штурма по формулам (δ_0)–(δ_s) многочлены f_j $(j = 0, 1, \ldots, s)$ можно умножать на произвольные положительные константы. Легко видеть, что доказательство теоремы 5.114 распространяется и на такую систему.

Если в конечной последовательности вещественных чисел $\alpha_0, \alpha_1, \ldots, \alpha_s$ имеется k переходов от одного знака к другому (нулевые числа пропускаем), то говорят, что последовательность содержит k *перемен знака*.

Теорема 5.116 (Штурм)**.** *Пусть многочлен $f \in \mathbb{R}[x]$ не содержит кратных корней и $f(a) \neq 0$, $f(b) \neq 0$, где $a < b$, $a, b \in \mathbb{R}$. Тогда число действительных корней многочлена f, принадлежащих отрезку $[a, b]$, равно $W(a) - W(b)$, где через $W(\alpha)$ обозначено число перемен знака в последовательности значений многочленов системы Штурма $f_0(\alpha), f_1(\alpha), \ldots, f_s(\alpha)$.*

Доказательство. Пусть x движется от a к b. Проследим, как при этом меняется W. Очевидно, W не меняется, когда x проходит через интервал, на котором нет корней ни одного из многочленов системы Штурма. Покажем, во-первых, что W уменьшается на 1, т. е. теряется одна перемена знака, если x проходит через корень многочлена f. Во-вторых, покажем, что W не меняется, когда x проходит через корень одного из многочленов f_j $(j = 1, 2, \ldots, s)$. Это докажет, что число корней на отрезке $[a, b]$ равно $W(a) - W(b)$.

Пусть x проходит через корень α многочлена f. Согласно свойству 2) в определении системы Штурма ff_1 в окрестности α возрастает и, следовательно, при прохождении x через α меняет знак с $-$ на $+$. Это означает, что если в окрестности α многочлен f возрастает, то

$f_1 > 0$:

	$x < \alpha$	$x > \alpha$
f	$-$	$+$
f_1	$+$	$+$
f_2	$*$	$*$
$\vdots$	$\vdots$	$\vdots$
f_s	$*$	$*$

Таким образом, в приведенной таблице число перемен знака в столбце, соответствующем $x < \alpha$, на 1 больше, чем в столбце, соответствующем $x > \alpha$, т.е. теряется одна перемена знака. Если же в окрестности α многочлен f убывает, то $f_1 < 0$:

	$x < \alpha$	$x > \alpha$
f	$+$	$-$
f_1	$-$	$-$
f_2	$*$	$*$
$\vdots$	$\vdots$	$\vdots$
f_s	$*$	$*$

Аналогично приходим к выводу, что теряется одна перемена знака.

Пусть теперь x проходит через корень α одного из многочленов f_j $(j = 1, 2, \ldots, s)$. Согласно свойству 3) в определении системы Штурма $f_{j-1}f_{j+1} < 0$. Это возможно в следующих 4 случаях (два из них соответствуют возрастающей в окрестности α функции f_j, а два — убывающей):

	I.		II.		III.		IV.	
	$x < \alpha$	$x > \alpha$	$x < \alpha$	$x > \alpha$	$x < \alpha$	$x > \alpha$	$x < \alpha$	$x > \alpha$
f_{j-1}	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$+$
f_j	$-$	$+$	$-$	$+$	$+$	$-$	$+$	$-$
f_{j+1}	$+$	$+$	$-$	$-$	$+$	$+$	$-$	$-$

В каждом случае число перемен знака в столбце, соответствующем $x < \alpha$, совпадает с числом перемен знака в столбце, соответствующем $x > \alpha$. Итак, если x проходит через корень многочлена f_j $(j = 1, 2, \ldots, s)$, то W не изменяется. ∎

Локализовать вещественные корни многочлена f — значит найти интервалы на вещественной оси, на каждом из которых содержится ровно один корень и других вещественных корней нет. После того, как корни локализованы, для их уточнения используют различные численные методы (деления пополам, секущих, касательных Ньютона и др.).

Пример 5.117. С помощью теоремы Штурма локализуем вещественные корни многочлена $f = x^5 - 4x - 2$. Теорема 5.111 дает следующую верхнюю оценку на положительные корни: $\alpha \le \sqrt[4]{4/1} = \sqrt{2} < 2$. Применяя ту же теорему к многочлену $-f(-x) = x^5 - 4x + 2$, получаем нижнюю оценку на величину отрицательных корней: $\alpha \ge -\sqrt[4]{4/1} = -\sqrt{2} > -2$. Итак, все вещественные корни многочлена f лежат на интервале $(-2, 2)$.

Построим систему Штурма.

$$f_0 = f, \qquad f_1 = f' = 5x^4 - 4.$$

При делении f_0 на f_1 получаем в остатке $r_2 = -(16/5)x - 2$. Меняем знак у r_2 и домножаем на $5/2$, получаем

$$f_2 = 8x + 5.$$

При делении f_1 на f_2 получаем в остатке $r_3 = -13259/4096$, поэтому

$$f_3 = 1.$$

Полученный многочлен f_3 является наибольшим общим делителем f и f'. Таким образом, f и f' взаимно просты, поэтому f кратных корней не имеет.

Вычислим значения многочленов системы Штурма на концах интервала $(-2, 2)$. Число перемен знаков составит $W(-2) = 3$, $W(2) = 0$ (см. таблицу ниже). Таким образом, многочлен f имеет $W(-2) - W(2) = 3$ вещественных корня. Вычислим значения многочленов системы Штурма в середине интервала $(-2, 2)$. Число перемен знака в точке 0 составит $W(0) = 1$. Следовательно, имеется $W(0) - W(2) = 1$ положительный корень и $W(-2) - W(0) = 2$ отрицательных корня. Для локализации отрицательных корней вычислим значения многочленов системы Штурма в точке -1. Приходим к выводу, что корни локализованы на интервалах $(-2, -1)$, $(-1, 0)$ и $(0, 2)$.

Знаки значений многочленов системы Штурма в рассматриваемых точках сведены в таблицу.

	-2	-1	0	2
$f_0 = f = x^5 - 4x - 2$	$-$	$+$	$-$	$+$
$f_1 = f' = 5x^4 - 4$	$+$	$+$	$-$	$+$
$f_2 = 8x + 5$	$-$	$-$	$+$	$+$
$f_3 = 1$	$+$	$+$	$+$	$+$
W	3	2	1	0

Теорема 5.116 была сформулирована и доказана для случая многочлена f без кратных корней. Если f имеет кратные корни, то НОД многочленов f и f' имеет положительную степень, поэтому f_s в системе, построенной согласно (γ_1)–(γ_s), может не удовлетворять свойству 4) в определении системы Штурма. Тем не менее, справедлив результат, обобщающий теорему 5.116. на случай многочлена с корнями произвольной кратности.

Теорема 5.118. *Пусть f — многочлен из $\mathbb{R}[x]$, такой, что $f(a) \neq 0$, $f(b) \neq 0$, где $a < b$, $a, b \in \mathbb{R}$. Пусть также $f_0, f_1, \ldots, f_s$ — система, построенная согласно (γ_1)–(γ_s). Тогда число действительных корней (без учета их кратности) многочлена f, принадлежащих отрезку $[a, b]$, равно $W(a) - W(b)$, где через $W(\alpha)$ обозначено число перемен знака в последовательности $f_0(\alpha), f_1(\alpha), \ldots, f_s(\alpha)$.*

Доказательство. Многочлен f_s является наибольшим общим делителем многочленов f и f_s. Из (γ_1)–(γ_s) получаем, что каждый из многочленов $f_0, f_1, \ldots, f_s$ делится на f_s. Пусть $g_j = f_j/f_s$ $(j = 0, 1, \ldots, s)$. Легко видеть, что система $g_0, g_1, \ldots, g_s$ является системой Штурма для многочлена $g = f/f_s$, все корни которого по следствию 5.86 (см. также замечание 5.87) совпадают с корнями многочлена f, но имеют кратность 1. Поэтому число корней (без учета кратности) многочлена f совпадает с разностью в числе перемен знака в последовательностях значений $g_0(a), g_1(a), \ldots, g_s(a)$ и $g_0(b), g_1(b), \ldots, g_s(b)$. Но при заданном α последовательность $f_0(\alpha), f_1(\alpha), \ldots, f_s(\alpha)$ получается из последовательности $g_0(\alpha), g_1(\alpha), \ldots, g_s(\alpha)$ умножением на константу $f_s(\alpha)$. Так как $f_s(a) \neq 0$, $f_s(b) \neq 0$ (иначе было бы $f_s(b) = 0$ или $f_s(b) = 0$), то число перемен знака в этих последовательностях одно и то же. ∎

Некоторую информацию о вещественных корнях (иногда достаточно полную) дает теорема Бюдана–Фурье.

Теорема 5.119 (Бюдан–Фурье)**.** *Число вещественных корней ненулевого многочлена* $f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{R}[x]$*, расположенных на интервале* (a, b) *(*$f(a) \neq 0$*,* $f(b) \neq 0$*) с учетом их кратностей равно или на четное число меньше разности между числом перемен знака в последовательности* $f(a), f'(a), f''(a), \ldots, f^{(n)}(a)$ *и числом перемен знака в последовательности* $f(b), f'(b), f''(b), \ldots, f^{(n)}(b)$*.*

Доказательство. Обозначим $N(f)$ — число корней многочлена f на интервале (a, b), а $L(f)$ — разность между числом перемен знака в последовательности $f(a), f'(a), f''(a), \ldots, f^{(n)}(a)$ и числом перемен знака в последовательности $f(b), f'(b), f''(b), \ldots, f^{(n)}(b)$.

Заметим, что $f^{(n)}$ — константа, равная $n!a_0$.

Сначала докажем, что $N(f)$ и $L(f)$ могут отличаться лишь на четное число (т. е. имеют одинаковую четность). Когда x увеличивается и проходит простой корень, f меняет знак. Когда x увеличивается и проходит k-кратный корень, f меняет знак, если k нечетно, и не меняет знака, если k четно. Поэтому $N(f)$ четно, если $f(a)$ и $f(b)$ имеют одинаковые знаки, и $N(f)$ нечетно, если $f(a)$ и $f(b)$ имеют разные знаки. Легко проверить, что аналогичное утверждение справедливо и для $L(f)$, поэтому $N(f)$ и $L(f)$ могут отличаться лишь на четное число.

Теперь докажем, что

$$N(f) \leq N(f') + 1. \tag{5.40}$$

Действительно, по теореме Ролля между любыми двумя корнями многочлена f лежит корень его производной f'. Кроме того, по теореме 5.36 каждый k-кратный корень многочлена f является $(k-1)$-кратным корнем многочлена f'. Отсюда $N(F') \geq N(f) - 1$.

Очевидно,

$$L(f') \leq L(f). \tag{5.41}$$

Теперь индукцией по $\deg f$ докажем, что $N(f) \leq L(f)$. Это завершит доказательство теоремы. Если $\deg f = 0$, то $L(f) = N(f) = 0$. Если $\deg f > 0$, то, используя (5.40), (5.41) и применяя предположение индукции к f', получаем

$$N(f) \leq N(f') + 1 \leq L(f') + 1 \leq L(f) + 1.$$

Но так как $L(f)$ и $N(f)$ могут отличаться лишь на четное число, то $N(f) \leq L(f)$. ∎

Упражнение 5.120. Докажите следующее усиление теоремы 5.119.

Число вещественных корней ненулевого многочлена $f \in \mathbb{R}[x]$, расположенных на интервале (a, b) ($f(a) \neq 0$, $f(b) \neq 0$) с учетом их кратностей равно или на четное число меньше разности между числом перемен знака в последовательности $f(a), f'(a), f''(a), \ldots, f^{(n)}(a)$ и числом перемен знака в последовательности, полученной из $f(b), f'(b), f''(b), \ldots, f^{(n)}(b)$ заменой встречающихся нулей такими ненулевыми числами, что если $f^{(k-1)}(b) \neq 0$, $f^{(k)}(b) = \ldots = f^{(k+l-1)}(b) = 0$, $f^{(k+l)}(b) \neq 0$, то число c_{k+i}, заменяющее $f^{(k+i)}(b)$ $(i = 0, 1, \ldots, l-1)$, имеет тот же знак, что и $f^{(k+l)}(b)$, если $l - i$ четно, и противоположный знак, если $l - i$ нечетно.

Указание: вместо интервала (a, b) рассмотрите интервал $(a, b - \varepsilon)$, где ε — достаточно маленькое число.

Следствие 5.121 (Правило знаков Декарта)**.** *Число положительных корней ненулевого многочлена* $f = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{R}[x]$ *с учетом их кратностей равно или на четное число меньше числа перемен знака в последовательности коэффициентов* $a_0, a_1, \ldots, a_n$*. В частности, если число перемен знака равно* 0 *или* 1*, то* f *соответственно либо не имеет положительных корней, либо имеет ровно один положительный корень.*

Доказательство. Не нарушая общности, можно считать, что $f(0) \neq 0$, так как в противном случае $f = a_0x^n + \ldots + a_{n-r}x^r$, $a_{n-r} \neq 0$, и мы можем разделить f на x^r. При этом ни число

положительных корней, ни число перемен знака в последовательности коэффициентов не изменятся.

Так как $f^{(k)}(0) = k!a_{n-k}$, то число перемен знака в последовательности $f(0), f'(0), \ldots, f^{(n)}(0)$ совпадает с числом перемен знака в последовательности коэффициентов многочлена f. Пусть M — достаточно большое число, такое, что знак в последовательности $f(M), f'(M), \ldots, f^{(n)}(M)$ не меняется и $f(\alpha) \neq 0$ при $\alpha \geq M$. Теперь достаточно применить теорему 5.119 к интервалу $[0, M]$. ∎

Пример 5.122. Правило знаков Декарта, примененное к многочлену $f = x^5 - 4x - 2$ (1 перемена знака) из примера 5.117, сразу приводит к выводу, что f имеем 1 положительный корень. Это же правило, примененное к многочлену $f(-x) = -x^5 + 4x - 2$ (2 перемены знака), позволяет утверждать лишь то, что f имеет либо 2, либо 0 отрицательных корней.

Теперь применим теорему Бюдана–Фурье.

	-2	-1	$-\varepsilon$	0	2
$f = x^5 - 4x - 2$	$-$	$+$	$-$	$-$	$+$
$f' = 5x^4 - 4$	$+$	$+$	$-$	$-$	$+$
$f'' = 20x^3$	$-$	$-$	$-$	0	$+$
$f''' = 60x^2$	$+$	$+$	$+$	0	$+$
$f^{IV} = 120x$	$-$	$-$	$-$	0	$+$
$f^V = 120$	$+$	$+$	$+$	$+$	$+$
W	5	4	3	1	0

Число перемен знака в последовательности значений производной в точках -2, -1, 0 и 2 составит соответственно $W(-2) = 5$, $W(-1) = 4$, $W(0) = 1$, $W(2) = 0$, т. е. имеем один корень на интервале $(-2, -1)$ и 1 корень на интервале $(0, 2)$. Получить информацию о возможных корнях на интервале $(-1, 0)$ в данном случае удается, если вместо 0 рассмотреть точку $-\varepsilon$ для достаточно малого положительного ε, такого, что на интервале $(-\varepsilon, 0)$ многочлен f корней не имеет. Получаем $W(\varepsilon) = 3$. Следовательно, на интервале $(-1, 0)$ находится $W(-1) - W(\varepsilon) = 1$ вещественный корень.

5.15. Алгебраические расширения полей

Пусть $f \in F[x]$ — неприводимый над полем F многочлен и α — некоторый его корень, не принадлежащий F. Минимальное по включению поле, включающее F и содержащее α назовем *алгебраическим расширением* поля F и обозначим $F(\alpha)$. Будем также говорить, что $F(\alpha)$ получено в результате *присоединения к F элемента α*.

Пусть в $F[x]$ нашелся многочлен f, для которого $f(\alpha) = 0$. Мы можем считать, что f неприводим над F, так как в противном случае f можно заменить на тот неприводимый множитель в его разложении, для которого α является корнем.

Теорема 5.123. *Все элементы поля $F(\alpha)$, где α — иррациональный корень неприводимого над F многочлена f степени n, имеют вид*

$$\beta = \gamma_0 + \gamma_1\alpha + \gamma_2\alpha^2 + \ldots + \gamma_{n-1}\alpha^{n-1} \tag{5.42}$$

для произвольных $\gamma_0, \gamma_1, \ldots, \gamma_{n-1} \in F$. По любому $\beta \in F(\alpha)$ величины $\gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ определяются единственным образом.

Иными словами, для любого $\beta \in F(\alpha)$ найдется единственный $g \in F[x]$, либо равный 0, либо степени меньшей n, такой, что $\beta = g(\alpha)$. Для любого $g \in F[x]$ величина $f(\alpha)$ принадлежит $F(\alpha)$.

Доказательство. Так как $F \subseteq F(\alpha)$ и $\alpha \in F(\alpha)$, то в силу замкнутости поля $F(\alpha)$ относительно операций сложения, вычитания и умножения каждое число вида (5.42) принадлежит $F(\alpha)$.

Прежде чем показывать, что других чисел в $F(\alpha)$ нет, докажем что многочлен g, такой, что $\beta = g(\alpha)$ и $\deg g < n$ или $g = 0$, по величине $\beta \in F(\alpha)$ определяется единственным образом. Пусть $g(\alpha) = \widetilde{g}(\alpha)$, где $\widetilde{g} \in F[x]$ и $\deg \widetilde{g} < n$ или $\widetilde{g} = 0$. Тогда α является корнем многочлена $h = g - \widetilde{g}$. Так как α является также корнем многочлена f, то f и h имеют нетривиальный делитель в $\mathbb{C}[x]$ и, по следствию 5.24, в $F[x]$. Но $\deg h < \deg f$ или $h = 0$. Первое по утверждению 5.77 невозможно, так как f неприводим над F, следовательно, $h = 0$, т. е. $g = \widetilde{g}$.

Покажем, что других элементов, кроме чисел вида (5.42), в $F(\alpha)$ нет. Для этого проверим замкнутость множества всех таких чисел относительно операций сложения, вычитания и умножения и замкнутость множества ненулевых чисел такого вида относительно деления. Замкнутость относительно сложения и вычитания очевидна. Для доказательства замкнутости относительно умножения рассмотрим произведение

$$g(\alpha) \cdot \widetilde{g}(\alpha) \tag{5.43}$$

Разделив $h = g\widetilde{g}$ на f получим в остатке многочлен r, такой, что $\deg r < n$ или $r = 0$. Легко видеть, что $h(\alpha) = r(\alpha)$. Замкнутость относительно умножения доказана.

Для доказательства замкнутости множества ненулевых элементов вида (5.42) относительно деления достаточно показать, что для любого ненулевого $g \in F[x]$, степени меньше n, величина $1/g(\alpha)$ может быть представлена в виде (5.42) (такое представление называется *освобождением от иррациональности в знаменателе*). Так как f неприводим над $\mathbb{Q}$, то f и g взаимно просты и, следовательно, существуют коэффициенты Безу $u \in F[x]$ и $v \in F[x]$, такие, что $uf + vg = 1$ и $\deg v < \deg f = n$. Подставляя в последнее равенство вместо x иррациональность α, получаем $v(\alpha)g(\alpha) = 1$, откуда $1/g(\alpha) = v(\alpha)$. Число $v(\alpha)$ имеет вид (5.42). ∎

Пример 5.124. Поле $\mathbb{C}$ является алгебраическим расширением поля $\mathbb{R}$ и получено в результате присоединения к $\mathbb{R}$ корня i (или $-i$) неприводимого над $\mathbb{R}$ многочлена $f = x^2 + 1$. Многочлен f имеет вторую степень и поэтому каждый элемент поля $\mathbb{C} = \mathbb{R}(i)$ согласно (5.42) можно записать в виде $a + bi$, где $a, b \in \mathbb{R}$.

Пример 5.125. Рассмотрим поле $\mathbb{Q}(\sqrt{2})$. Иррациональность $\sqrt{2}$ является корнем неприводимого над $\mathbb{Q}$ многочлена $x^2 - 2$. По теореме 5.123 поле $\mathbb{Q}(\sqrt{2})$ состоит из элементов вида $a + b\sqrt{2}$, где $a, b \in \mathbb{Q}$, в чем легко убедиться и непосредственно.

Пример 5.126. Рассмотрим поле $\mathbb{Q}(\sqrt[4]{3})$. Иррациональность $\alpha = \sqrt[4]{3}$ является корнем неприводимого над $\mathbb{Q}$ многочлена $f = x^4 - 3$. Многочлен f имеет степень 4, поэтому по теореме 5.123 поле $\mathbb{Q}(\sqrt[4]{3})$ состоит из элементов вида $\gamma_0 + \gamma_1\sqrt[4]{3} + \gamma_2\sqrt[4]{9} + \gamma_3\sqrt[4]{27}$, где $\gamma_j \in \mathbb{Q}$ $(j = 0, 1, 2, 3)$.

Для примера представим в таком виде число, обратное $\sqrt[4]{27} + 2\sqrt[4]{9} + \sqrt[4]{3} + 1$, т. е. освободимся от иррациональности в знаменателе дроби

$$w = \frac{1}{\sqrt[4]{27} + 2\sqrt[4]{9} + \sqrt[4]{3} + 1}.$$

Пусть $g = x^3 + 2x^2 + x + 1$. Имеем $f(\sqrt[4]{3}) = 0$ и $w = 1/g(\sqrt[4]{3})$. Многочлены f и g рассматривались в примере 5.15, в котором были найдены коэффициенты Безу

$$u = \frac{1}{7}x^2 - \frac{2}{7}, \qquad v = -\frac{1}{7}x^3 + \frac{2}{7}x^2 - \frac{1}{7}x + \frac{1}{7},$$

такие, что $uf + vg = 1$. Подставляя в последнее равенство вместо x иррациональности $\sqrt[4]{3}$, получаем

$$w = \frac{1}{g(\sqrt[4]{3})} = v(\sqrt[4]{3}) = -\frac{\sqrt[4]{27}}{7} + \frac{2\sqrt[4]{9}}{7} - \frac{\sqrt[4]{3}}{7} + \frac{1}{7}.$$

Упражнение 5.127. Освободиться от иррациональности в знаменателе:

1) $\dfrac{1}{1+2\sqrt[3]{3}-\sqrt[3]{9}}$;

2) $\dfrac{1}{1-2\sqrt[3]{5}+\sqrt[3]{25}}$;

3) $\dfrac{1}{4-3\alpha+\alpha^2}$, если $1-3\alpha+\alpha^3=0$;

4) $\dfrac{1}{1+\alpha-2\alpha^2+\alpha^3}$, если $1-\alpha-3\alpha^2-2\alpha^3+\alpha^4=0$.

Число $\alpha \in \mathbb{C}$ называется *алгебраическим*, если оно является корнем многочлена из $\mathbb{Q}[x]$ или, что эквивалентно, из $\mathbb{Z}[x]$. Множество всех алгебраических чисел обозначим $\mathbb{A}$. Очевидно, что $\mathbb{Q} \subset \mathbb{A}$, так как рациональное число p/q является корнем многочлена первой степени $qx-p$. Можно показать, что число, которое можно представить в виде выражения, содержащего целые числа, знаки арифметических операций и знаки извлечения корня произвольной натуральной степени также является алгебраическим, однако в силу теоремы Абеля не каждое алгебраическое число можно представить таким выражением.

Можно показать, что $\mathbb{A}$ образует алгебраически замкнутое поле.

Комплексные числа, не являющиеся алгебраическими, называются *трансцендентными*. Примерами трансцендентных чисел служат π, e.

Упражнение 5.128. Докажите, что множество алгебраических чисел $\mathbb{A}$ счетно и, следовательно, (так как $\mathbb{C}$ континуально) множество трансцендентных чисел континуально. Указание: Высотой многочлена $f=a_0x^n+a_1x^{n-1}+\ldots+a_n$ называется величина $\|f\|=\max\{|a_0|,|a_1|,\ldots,|a_n|\}$. Докажите, что множество многочленов f из $\mathbb{Z}[x]$ заданной высоты конечно. Представьте $\mathbb{Z}[x]$ в виде счетного объединения конечных множеств.

Ответы и решения

5.3. $p^m(p-1)$.

5.7. 1) Частное $2x^4-2x^3+x^2-10x+16$, остаток $-x-5$; 2) частное $\dfrac{1}{3}x-\dfrac{4}{9}$, остаток $\dfrac{4}{9}x+\dfrac{23}{9}$.

5.8. Частное $x^2+2ax-\dfrac{a^2}{2}$, остаток 0.

5.16. 1) $d=x^2+2x-1$, $u=-2x+1$, $v=2x^3-5x^2+8x-2$; 2) $d=x-2$, $u=-\dfrac{1}{54}x+\dfrac{1}{18}$, $v=\dfrac{1}{54}x^3-\dfrac{5}{54}x^2+\dfrac{1}{6}x$.

5.19. 1) $u=9x^2-26x-21$, $v=-9x^3+44x^2-39x-7$; 2) $u=3x^3+3x^2-7x+2$, $v=-3x^3-6x^2+x+2$.

5.20. 1) x^2+1.
2) 1.

5.21. 1) 1.
2) $x+1$.
3) 1.

5.22. 1) x^2+2x.
2) x^3+x+3.
3) x^3+2x+4.
4) $x-1$.

5.33. 1) Частное $x^3+4x^2+6x+10$, остаток 22;
2) частное $x^3+(25-7i)x-15-16i$, остаток $-20-11i$.

5.38. $a=2$, $b=0$, $c=-2$. *Указание:* Приравнять нулю значение многочлена и его первой и второй производной в точке -1.

5.39. 1) При $\left(\dfrac{q}{2}\right)^2+\left(\dfrac{p}{3}\right)^3=0$;
2) при $\left(\dfrac{q}{3}\right)^3-\left(\dfrac{p}{4}\right)^4=0$;

3) при $\left(\frac{q}{4}\right)^4 + \left(\frac{p}{5}\right)^5 = 0$.

5.47. 1) $(x+1)^4 - (x+1)^3 + 2(x+1)^2 - 2$;
2) $(x-1)^5 + 5(x-1)^4 + 10(x-1)^3 + 10(x-1)^2 + 5(x-1) + 1$.

5.50. 1) $f(2) = 1$, $f'(2) = 1$, $f''(2) = -4$, $f'''(2) = 12$, $f^{IV} = 24$;
2) $f(2) = 2i$, $f'(2) = 1$, $f''(2) = 2 - 2i$, $f'''(2) = 6i$, $f^{IV} = 24$.

5.61. 1) $(x+1)\left(x - \frac{1}{2} - \frac{\sqrt{7}}{2}i\right)\left(x - \frac{1}{2} + \frac{\sqrt{7}}{2}i\right) = (x+1)(x^2 - x + 2)$;
2) $(x-1-i)(x-1+i)(x+1-i)(x+1+i) = (x^2 - 2x + 2)(x^2 + 2x + 2)$.

5.67. 1) $x^3 - 2x^2 + x - 1$;
2) $x^3 - 3x^2 + 2x - 2$.

5.68. $x^4 + x^3 + x + 1$.

5.73. 1) а) $x^5 - (6+2i)x^4 + (10+12i)x^3 - 22ix^2 - (11-12i)x + 6$; б) $x^7 - 6x^6 + 13x^5 - 18x^4 + 23x^3 - 18x^2 + 11x - 6$;
2) а) $x^5 - (8-2i)x^4 + (24-14i)x^3 - (34-34i)x^2 + (23-34i)x - 6 + 12i$; б) $x^6 - 9x^5 + 36x^4 - 86x^3 + 125x^2 - 97x + 30$.

5.92. 1) Простые корни 2, $\frac{2}{3}$;

2) простые корни 3, $\frac{1}{5}$, -1.

5.98. 3) *Указание:* Рассмотреть многочлен $f(x+1)$.

5.101. 1) x^2, $x^2 + 1 = (x+1)^2$, $x^2 + x = x(x+1)$, $x^2 + x + 1$ — неприводимый.
2) x^3, $x^3 + 1 = (x+1)(x^2 + x + 1)$, $x^3 + x = x(x+1)^2$, $x^3 + x + 1$ неприводим, $x^3 + x^2 = x^2(x+1)$, $x^3 + x^2 + 1$ неприводим, $x^3 + x^2 + x = x(x^2 + x + 1)$, $x^3 + x^2 + x + 1 = (x+1)^3$.

5.102. 1) $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$.
2) $x^3 + 2x + 1$, $x^3 + 2x + 2$, $x^3 + x^2 + 2$, $x^3 + 2x^2 + 1$, $x^3 + x^2 + x + 2$, $x^3 + x^2 + 2x + 1$, $x^3 + 2x^2 + x + 1$, $x^3 + 2x^2 + 2x + 2$.

5.103. 1) $(x+1)^3(x^2 + x + 1)$.
2) $(x^2 + 1)(x^3 + 2x^2 + 2x + 2)$.
3) $(x+1)(x^2 + 2x + 4)(x^2 + 4x + 2)$.

5.104. 1) $(x+1)x^2(x^2 + 1)$.
2) $(x+1)(x^2 + 4x + 2)(x^2 + x + 2)$.
3) $(x+1)(x^2 + x + 3)(x^2 + 6x + 3)$.
4) $(x+1)(x^4 - 2x^2 + 9)$.

5.105. Над $\mathbb{Q}$ многочлен неприводим.

5.106. 2) Многочлены x и $x + p$ взаимно просты над $\mathbb{Q}$, но не являются таковыми над $\mathbb{Z}_p$.

5.107. 2) Многочлен $px^2 + (p+1)x + 1 = (x+1)(px+1)$ приводим над $\mathbb{Q}$, но над $\mathbb{Z}_p$ равен $x+1$ и, следовательно, неприводим.

3) Докажем, что $x^4 + 1$ приводим над $\mathbb{Z}_p$ при любом простом p. Так как

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

то достаточно доказать, что одно из чисел: -1, 2 или -2 — является квадратом в $\mathbb{Z}_p$. Однако если ни 2, ни -2 не является квадратом в $\mathbb{Z}_p$, то, согласно **№ ??**, квадратом является их произведение $2 \cdot (-2) = 4 \cdot (-1)$, и, следовательно, квадратом является -1.

5.108. 1) 4, 7; 2) нет решений; 3) 3, 4; 4) 10 (двукратный корень); 5) нет решений;
6) 2; 7) все ненулевые элементы (по малой теореме Ферма);
8) при любом a единственное решение.

5.109. 1) Все элементы поля (малая теорема Ферма); 2) a.

5.127. 1) $\frac{7}{34} + \frac{1}{34}\sqrt[3]{3} + \frac{5}{34}\sqrt[3]{9}$;

2) $\frac{11}{16} + \frac{7}{16}\sqrt[3]{25} + \frac{3}{16}\sqrt[3]{25}$;

3) $\frac{19}{71} + \frac{11}{71}\alpha + \frac{2}{71}\alpha^2$;

4) $\frac{56}{121} + \frac{95}{121}\alpha + \frac{86}{121}\alpha^2 - \frac{40}{121}\alpha^3$.