Нешина Екатерина, М1-14

Билет 14

Кольцо многочленов от одной переменной над числовым полем. Корни многочлена. Алгебраическая замкнутость поля комплексных чисел.

Определение 1
Множество G с заданной на нём алгебраической операцией $*$ называется *группой*, если:
1) операция ассоциативна: $(a * b) * c = a * (b * c), \forall a, b, c \in G$;
2) операция обладает нейтральным элементом $e \in G : a * e = e * a = a, \forall a \in G$;
3) для любого элемента $a \in G$ существует симметричный элемент $a' \in G : a * a' = a' * a = e$.

Обозначение: G или $\langle G, + \rangle$. Условия 1-3 называются *аксиомами группы*. Группа с коммутативной операцией называется *коммутативной* или *абелевой*. (коммутативность: $a * b = b * a$).

Определение 1.1 *Мультипликативная группа* - группа, где обратный элемент это a^{-1}, а нейтральный это единица.

Определение 1.2 *Аддитивная группа* - нейтральный элемент это 0, противоположный(симметричный) это $-a$.

Примеры:
1) $\langle \mathbb{Z}, + \rangle$; $\langle \mathbb{Q}, + \rangle$; $\langle \mathbb{R}, + \rangle$ - аддитивные абелевы группы;
2) $\langle \mathbb{Q} \backslash 0, \cdot \rangle$; $\langle \mathbb{R} \backslash 0, \cdot \rangle$ - мультипликативные абелевы группы;

Определение 2
Подмножество H группы G называется *подгруппой* группы G, если оно само является группой относительно алгебраической операции в G.

Определение 3
Две группы G_1 и G_2 с операциями $*_1$ и $*_2$ называются *изоморфными*, если существует биективное отображение $f : G_1 \to G_2$, которое сохраняет групповую операцию, т.е. $f(a *_1 b) = f(a) *_2 f(b), \forall a, b \in G_1$.

Обозначение: $G_1 \simeq G_2$. Само отображение f называют *изоморфизмом*.

Определение 4
Непустое множество K, наделенное двумя алгебраическими операциями - сложением и умножением, называется *кольцом*, если эти операции удовлетворяют следующим аксиомам: $\forall a, b, c \in K$
1) $a + b = b + a$;
2) $(a + b) + c = a + (b + c)$;
3) $\exists 0 \in K : a + 0 = 0 + a$;
4) $\forall a \in K \exists - a \in K : a + (-a) = (-a) + a = 0$;
5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
6) $(a + b) \cdot c = a \cdot b + b \cdot c$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Определение 5
Кольцо называется *коммутативным*, если умножение в нём коммутативно;
Кольцо называется *кольцом с единицей*, если операция умножения обладает нейтральным элементом.

Примеры:
Множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ - аддитивные абелевы группы;

Определение 6

Полем P называется коммутативное кольцо с единицей, содержащее не менее двух элементов, в котором каждый отличны от нуля элемент имеет обратный элемент, а именно:

1) $a + b = b + a$ - коммутативность сложения;
2) $(a + b) + c = a + (b + c)$ - ассоциативность сложения;
3) $\exists 0 \in P : a + 0 = 0 + a$ - существование нулевого элемента;
4) $\forall a \in P \exists - a \in P : a + (-a) = (-a) + a = 0$ - существование противоположного элемента;
5) $a \cdot b = b \cdot a$ - коммутативность умножения;
6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ - ассоциативность умножения;
7) $\exists e \in P \backslash 0 : a \cdot e = e \cdot a$ - существование единичного элемента;
8) $\forall a \in P(a \neq 0) \exists a^{-1} \in P : a \cdot a^{-1} = e$ - существование обратного элемента для ненулевых элементов;
9) $(a + b) \cdot c = a \cdot b + b \cdot c$, $a \cdot (b + c) = a \cdot b + a \cdot c$. - дистрибутивность;

Определение 7

Комплексные числами называются упорядоченные пары (a, b) вещественных чисел, для которых понятие равенства, суммы, произведения и отождествления с вещественными числами вводятся согласно следующим правилам (аксиомам):

1) $(a, b) = (c, d) \leftrightarrow a = c, b = d$; 2) $(a, b) + (c, d) = (a + c, b + d)$; 3) $(a, b) \cdot (c, d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$; 4) пара $(a, 0)$ отождествляется с действительным числом a.

Обозначения: $z = (a, b), \mathbb{C}$ - множество всех комплексных чисел.

Определение 8

Комплексные числа - это числа вида $z = a + b \cdot i$, где a, b - вещественные числа, а i - мнимая единица, то есть число, для которого выполняется $i^2 = -1$.

Теорема 1: Операция сопряжения комплексного числа обладает следующими свойствами:

1) $\overline{\overline{z}} = z$;
2) $z = \overline{z} \leftrightarrow z \in \mathbb{R}$;
3) $\overline{z} + z = 2 \cdot a, \forall z = a + b \cdot i$;
4) $\overline{z} \cdot z = a^2 + b^2, \forall z = a + b \cdot i$;
5) $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}$; $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$; $\overline{(z_1/z_2)} = \overline{z_1}/\overline{z_2}, z_2 \neq 0$.

Определение 9

Модулем комплексного числа $z = a + b \cdot i$ называется число $r = \sqrt{a^2 + b^2}$. Обозначение: $|z|$.

Определение 10

Аргументом комплексного числа $z \neq 0$ называется угол φ между положительным направлением оси абсцисс и радиус-вектором точки M, отсчитываемый от оси абсцисс в любом направлении, при этом положительным считается направление против часовой стрелки.

Обозначение: $argz$.

Теорема 2:

Любоме комплексное число $z \neq 0$ может быть записано в виде $z = r \cdot (cos\varphi + i \cdot sin\varphi)$, где $r = |z|, \varphi = argz$.

Теорема 3:

При умножении комплексных чисел их модули умножаются, а аргументы складываются; при делении комплексных чисел их модули делятся, а аргументы вычитаются.

Теорема 4:

Если $z = r \cdot (cos\varphi + i \cdot sin\varphi), n \in \mathbb{Z}$, то $z^n = r^n \cdot (cosn\varphi + i \cdot sinn\varphi)$.

Теорема 5:

Для ненулевого числа $z = r \cdot (cos\varphi + i \cdot sin\varphi)$ существует ровно n различных корней $\alpha_1, \alpha_2, ..., \alpha_n$ n-й степени:

$$\alpha_k = \sqrt[n]{r} \cdot (cos\tfrac{\varphi + 2\pi k}{n} + i \cdot sin\tfrac{\varphi + 2\pi k}{n}), k = \overline{0, n-1}.$$

Определение 11

Пусть P - поле. *Многочленом (полиномом) n-ой степени от переменной x над полем P* называется выражение

$$a_0 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_n \cdot x^n,$$

где $a_i, i = \overline{0, n}$, - фиксированные числа из поля P и $a_n \neq 0$. Эти числа называются *коэффициентами многочлена*, а число a_n – *старшим коэффициентом*. Число $0 \in P$ по определению считается многочленом с нулевыми коэффициентами и называется *нулевым многочленом*.

Обозначение: $f(x)$ или $f_n(x)$ - многочлен, $degf-$степень многочлена, $P[x]$ - множество всех многочленов от пепременной x над полем P. Итак,

$$f(x) = \sum_{k=0}^{n} a_k \cdot x^k \in P[x], degf = n$$

Определение 12

Суммой многочленов $f(x) = \sum_{k=0}^{n} a_k \cdot x^k$ и $g(x) = \sum_{k=0}^{s} b_k \cdot x^k$ называется многочлен

$$h(x) = \sum_{k=0}^{max(n,s)} c_k \cdot x^k, c_k = a_k + b_k.$$

Обозначение: $f(x) + g(x)$.

Определение 13

Произведением многочленов $f(x) = \sum_{k=0}^{n} a_k \cdot x^k$ и $g(x) = \sum_{k=0}^{s} b_k \cdot x^k$ называется многочлен

$$h(x) = \sum_{k=0}^{n+s} c_k \cdot x^k, \text{где } c_k = \sum_{i+j=k} a_i \cdot b_j, k = \overline{0, n+s}.$$

Обозначение: $f(x) \cdot g(x)$.

Теорема 6:

Множество $P[x]$ всех многочленов над полем P является *коммутативным кольцом с единицей и без делителей нуля.*

Доказательство:

Проверим все аксиомы кольца. Прежде всего отметим, что $P[x]$ - аддитивная абелева группа: коммутативность и ассоциативность сложения очевидны, нулём является нулевой многочлен, противоположным к многочлену $f(x) = \sum_{k=0}^{n} a_k \cdot x^k$ является многочлен $-f(x) = \sum_{k=0}^{n} (-a_k) \cdot x^k$. Коммутативность умножения следует из определения. Докажем ассоциативность умножения.

Пусть $f_n(x) = \sum_{k=0}^{n} a_k \cdot x^k$, $g_s(x) = \sum_{k=0}^{s} b_k \cdot x^k$, $h_p(x) = \sum_{k=0}^{p} c_k \cdot x^k$. Обозначим через $\alpha_k, \beta_k, \gamma_k$ и δ_k коэффициенты при x^k у многочленов $f(x) \cdot g(x), g(x) \cdot h(x), (f(x) \cdot (g(x)) \cdot h(x))$ и $f(x) \cdot (g(x) \cdot h(x))$ соответственно. Токгда из определения произведения получаем:

$$\gamma_k = \sum_{i+j=k} \alpha_i \cdot c_j = \sum_{i+j=k} (\sum_{r+t=i} a_r \cdot b_t) \cdot c_j = \sum_{r+t+j=k} a_r \cdot b_t \cdot c_j,$$

$$\delta_k = \sum_{r+i=k} a_r \cdot \beta_i = \sum_{r+i=k} a_r \cdot (\sum_{t+j=i} b_t \cdot c_j) = \sum_{r+t+j=k} a_r \cdot b_t \cdot c_j,$$

т.е. $\gamma_k = \delta_i$. Отсюда, если учесть, что $deg(fg)h = degf(gh) = n + s + p$, следует равенство $(f(x)g(x))h(x) = f(x)(g(x)h(x))$.

Роль единицы при умножении многочленов играет число 1, рассматриваемое как многочлен нулевой степени.

Справедливость аксиомы дистрибутивности вытекает из равенства $\sum_{i+j=k}(a_i + b_i) \cdot c_j = \sum_{i+j=k} a_i \cdot c_j + \sum_{i+j=k} b_i \cdot c_j$, так как левая часть этого равенства является коэффициентом при x^k в многочлене $(f(x) + g(x))h(x)$, а правая часть - коэффициентом при той же степени x в многочлене $f(x)h(x) + g(x)h(x)$.

Наконец, из $degfg = degf + degg$ следует, что в $P[x]$ нет делителей нуля.

Теорема доказана.

Следствие:

Множество $P[x]$ является линейным пространством над полем P.

Теорема 7:

Для любых двух многочленов $f(x), g(x) \in P[x]$, где $g(x) \neq 0$ существует, и притом единственная, пара многочленов $q(x), r(x) \in P[x]$ такая, что:

$$f(x) = g(x)q(x) + r(x),$$
$$\textit{где либо } r(x) = 0,$$
$$\textit{либо } degr < degg.$$

Корни многочленов

Определение 14

Если $f(x) = \sum_{k=0}^{n} a_k \cdot x^k$ - многочлен над полем P, c - некоторое число из поля P, то число $f(c) = \sum_{k=0}^{n} a_k \cdot c^k$ называется *значением многочлена* $f(x)$ *при* $x = c$.

Теорема 8 (теорема Безу):

Остаток от деления многочлена $f(x)$ на $x - c$ равен $f(c)$.

Доказательство:

Разделим согласно теореме 7 многочлен $f(x)$ на многочлен $x - c$. Тогда $f(x) = (x - c) \cdot q(x) + r(x)$, где $degr < deg(x - c) = 1$,так что $r(x) = r$ - константа. Беря значение обеих частей этого равенства при $x = c$, получим, что $r = f(c)$.

Теорема доказана.

Следствие:

Число $c \in P$ является корнем многочлена $f(x) \in P[x]$ тогда и только тогда, когда многочлен $f(x)$ делится на $x - c$ в кольце $P[x]$.

Говорят, что корень c имеет **кратность** m, если рассматриваемый многочлен делится на $(x-c)^m$ и не делится на $(x-c)^{m+1}$. Например, многочлен $x^2 - 2x + 1$ имеет единственный корень, равный 1, кратности 2. Выражение «кратный корень» означает, что кратность корня больше единицы.

Алгебраическая замкнутость поля $\mathbb{C}$

Определение 15

Поле P называется *алгебраически замкнутым*, если любой многочлен $f(x) \in P[x]$ степени $n \geq 1$ обладает в P хотя бы одним корнем.

Теорема 9 (основная теорема алгебры):

Поле $\mathbb{C}$ комплексных чисел алгебраически замкнуто.

Лемма 1

Пусть $f(z) = a_1 \cdot z + a_2 \cdot z^2 + ... + a_n \cdot z^n$ - многочлен с нулевым свободным членом. Тогда для любого $\varepsilon > 0$ найдётся $\delta > 0$ такое, что для всех z, для которых $|z| < \delta$, выполняется неравенство $|f(z)| < \varepsilon$.

Доказательство:

Пусть $|z| < 1$. Тогда в силу $||z_1| - |z_2|| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|$ и $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

$$|f(z)| = |z| \cdot |a_1 + a_2 \cdot z + ... + a_n \cdot z^{n-1}| \leq |z| \cdot (|a_1| + |a_2| + ... + |a_n|).$$

Положим $M = |a_1| + |a_2| + ... + |a_n|$ и возьмём $\delta = min(1, \epsilon/M)$. Тогда для всех z, для которых $|z| < \delta$, выполняется неравенство $|f(z)| \leq |z| \cdot M < \epsilon/M \cdot M = \epsilon$.

Лемма доказана.

Лемма 2

Многочлен $f(z) = a_0 + a_1 \cdot z + a_n \cdot z^n$ есть непрерывная функция во всех точках комплексной плоскости.

Доказательство:

Пусть z_0 - произвольное комплексное число. Разложим многочлен $f(z)$ по степеням $z - z_0 : f(z) = c_0 + c_1 \cdot (z - z_0) + ... + c_n \cdot (z - z_0)^n$. Тогда $c_0 = f(z_0)$, так что $f(z) - f(z_0) = c_1 \cdot (z - z_0) + ... + c_n \cdot (z - z_0)^n$.

Правая часть представляет собой многочлен от $z - z_0$ с нулевым свободным членом. По лемме 1 для любого $\epsilon > 0$ найдётся $\delta > 0$ такое, что $|f(z) - f(z_0)| < \epsilon$ для всех z, для которых $|z - z_0| < \delta$.

Лемма доказана.

Лемма 3

Модуль многочлена есть непрерывная функция.

Доказательство:

Утверждение вытекает из леммы 2 и свойств модулья комплексных чисел ($||z_1|-|z_2|| \leq |z_1 \pm z_2| \leq |z_1|+|z_2|$): $|f(z) - f(z_0)| \geq ||f(z)| - |f(z_0)||$.

Лемма доказана.

Лемма 4

Если $f(z)$ - многочлен степени $n \geq 1$, то для любого $M > 0$ существует $R > 0$ такое, что для всех z, для которых $|z| > R$, выполняется неравенство $|f(z)| > M$.

Доказательство:

Пусть $f(z) = a_0 + a_1 \cdot z + ... + a_n \cdot z^n$. Запишем его в виде

$$(1) f(z) = a_n \cdot z^n \cdot (1 + \frac{a_{n-1}}{a_n} \cdot z^{-1} + ... + \frac{a_0}{a_n} \cdot z^{-n}) = a_n \cdot z^n \cdot (1 + g(z^{-1}))$$

,

где $g(z^{-1})$ - многочлен от z^{-1} с нулевым свободным членом. Всилу леммы 1 для $\epsilon = 1/2$ найдётся $\delta > 0$такое, что при $|z^{-1}| < \delta$ имеет место неравенство $|g(z^{-1})| < 1/2$. Модуль $a_n \cdot z^n$ может быть сделан сколь угодно большим, именно при $|z| > \sqrt[n]{2 \cdot M/|a_n|}$ будет $|a_n \cdot z^n| > 2 \cdot M$. Возьмём $R = max(\sqrt[n]{2 \cdot M/|a_n|}, 1/\delta)$. Тогда если $|z| > R$, то $|z^{-1}| < \delta$ и $z > \sqrt[n]{2 \cdot M/|a_n|}$, так что согласно (1)

$$|f(z)| = |a_n \cdot z^n| \cdot |1 + g(z^{-1})| \geq |a_n \cdot z^n| \cdot |1 - |g(z^{-1})|| > 2 \cdot M \cdot (1 - 1/2) = M$$

.

Лемма доказана.

Определение 16

Число $z_0 = x_0 + i \cdot y_0$ называется *пределом последовательности* $z_n = x_n + i \cdot y_n$, если для любого $\epsilon > 0$ существует натуральное число N такое, что $|z_n - z_0| < \epsilon$ для всех $n > N$.

Обозначение: $\lim_{n\to\infty} z_n = z_0$.

Определение 17

Последовательность z_n называется *ограниченной* , если существует число $R > 0$ такое, что $|z_n| \leq R$.

Лемма 5

Из любой ограниченной последовательности z_n можно можно выделить сходящуюся последовательность.

Доказательство:

Пусть $z_n = x_n + i \cdot y_n$ и $|z_n| \leq R$, тогда $|x_n| \leq R$, так что x_n - ограниченная последовательность действительных чисел. Из неё согласно теореме Больцано-Вейерштрасса можно выделить сходящуюся подпоследовательность $x_{n_k} \to x_0$. Рассмотрим соответствующую подпоследовательность мнимых частей y_{n_k}. Она ограничена, и из неё также можно выделить сходящуюся подпоследовательность $y_{n_{k_m}} \to y_0$. Тогда соответствующая подпоследовательность $z_{n_{k_m}}$ сходится к $z_0 = x_0 + i \cdot y_0$.

Лемма доказана.

Лемма 6

Точная нижняя грань модуля многочлена достигается, т.е. существует число z_0 такое, что $|f(z_0)| \leq |f(z)|$ при всех комплексных z.

Доказательство:

Рассмотрим множество всевозможных значений модуля многочлена $f(z)$. Так как $|f(z)| \geq 0$, то это множество ограничено снизу и, следовательно, имеет точную нижнюю грань. Обозначим её через m. Тогда для любого натурального числа n можно найти комплексное число z_n такое, что

$$|f(z_n)| \leq m + \frac{1}{n}$$

.

Воспользуемся леммой 4: для $M = m + 1$ найдём R такое, что при $|z| > R$ будет $|f(z)| > M \geq m + \frac{1}{n}$. Отсюда и из $|f(z_n)| \leq m + \frac{1}{n}$ следует,что $|z_n| \leq R$. Последовательность z_n оказалась ограниченной, и из неё согласно лемме 5 можно выделить сходящуюся подпоследовательность $z_{n_k} \to z_0$. Тогда в силу непрерывности $|f(z)|$ (лемма 3)

$$\lim_{k\to\infty} |f(z_{n_k})| = |f(z_0)|.$$

С другой стороны, из $|f(z_n)| \leq m + \frac{1}{n}$ и определения нижней грани имеем $m \leq |f(z_{n_k})| \leq m + \frac{1}{n_k}$,поэтому

$$\lim_{k\to\infty} |f(z_{n_k})| = m.$$

Сопоставление $\lim_{k\to\infty} |f(z_{n_k})| = |f(z_0)|$ и $\lim_{k\to\infty} |f(z_{n_k})| = m$ приводит к требуемому равенству

$$|f(z_0)| = m.$$

Лемма доказана.

Лемма 7 (лемма Даламбера

Если $f(z)$ - многочлен степени $n \geq 1$ и $f(z_0) \neq 0$, то найдётся число z_1 такое, что $|f(z_1)| < |f(z_0)|$.

Доказательство:

Разложим многочлен $f(z)$ по степеням $z - z_0$:

$$f(z) = c_0 + c_1 \cdot (z - z_0) + ... + c_n \cdot (z - z_0)^n.$$

Очевидно, что $c_0 = f(z_0) \neq 0$. Пусть c_k - первый ненулевой коэффициент в $f(z) = c_0 + c_1 \cdot (z - z_0) + ... + c_n \cdot (z - z_0)^n$ после c_0 (такой коэффициент имеется, так как $f(z)$ не константа). Тогда

$f(z) = c_0 + c_k \cdot (z - z_0)^k + c_{k+1} \cdot (z - z_0)^{k+1} + ... + c_n \cdot (z - z_0)^n = c_0 \cdot (1 + \frac{c_k}{c_0} \cdot (z - z_0)^k + \frac{c_k}{c_0} \cdot (z - z_0)^k \cdot (\frac{c_{k+1}}{c_k} \cdot (z - z_0) + ... + \frac{c_n}{c_k} \cdot (z - z_0)^{n-k})) = c_0 \cdot (1 + \frac{c_k}{c_0} \cdot (z - z_0)^k + \frac{c_k}{c_0} \cdot (z - z_0)^k \cdot g(z - z_0))$, (2)

где $g \cdot (z - z_0) = \frac{c_{k+1}}{c_k} \cdot (z - z_0) + ... + \frac{c_n}{c_k} \cdot (z - z_0)^{n-k}$ - многочлен от $z - z_0$ с нулевым свободным членом. По лемме 1 для $\epsilon = 1/2$ найдётся такое δ, что если $|z - z_0| < \delta$, то $|g(z - z_0)| < 1/2$.

Оценим правую часть (2). Пусть $\frac{c_k}{c_0} = R \cdot (cos\theta + isin\theta), z - z_0 = r \cdot (cos\varphi + isin\varphi)$. Выберем r так, чтобы $R \cdot r^k < 1$. Для этого нужно взять $r < \sqrt[k]{1/R}$. Далее положим $\theta + k \cdot \varphi = \pi$, т.е. возьмём $\varphi = (\pi - \theta)/k$. При таком выборе $\frac{c_k}{c_0} \cdot (z - z_0)^k = -R \cdot r^k$. Теперь положим $z_1 = z_0 + r \cdot (cos\varphi + isin\varphi)$ при $r < min(\delta, \sqrt[k]{1/R})$ и $\varphi = (\pi - \theta)/k$.

Тогда из (2) следует, что $f(z_1) = c_0 \cdot (1 - R \cdot r^k - R \cdot r^k \cdot g(z_1 - z_0))$, и тем самым

$|f(z_1)| = |c_0| \cdot |1 - R \cdot r^k - R \cdot r^k \cdot g(z_1 - z_0)| \leq |c_0| \cdot (|1 - R \cdot r^k| + R \cdot r^k \cdot |g(z_1 - z_0)|) \leq$ */в силу выбора r и $|g(z - z_0)| < 1/2$/* $\leq |c_0| \cdot (1 - R \cdot r^k + R \cdot r^k/2) = |c_0| \cdot (1 - R \cdot r^k/2) < |c_0| = |f(z_0)|$.

Лемма доказана.

Доказательство основной теоремы:

Пусть $f(z)$ - произвольный многочлен над полем $\mathbb{C}$ от комплексной переменной z степени $n \geq 1$. Согласно лемме 6 множество всевозможных значений $|f(z)|$ имеет точную нижнюю грань m,которая достигается в некоторой точке z_0, так что $|f(z_0)| = m$. Тогда $f(z_0) = 0$, так как в противном случае, если $f(z_0) \neq 0$, то согласно лемме 7 найдётся точка z_1, для которой $|f(z_1)| < |f(z_0)| = inf|f(z)|$, что невозможно. Таким образом, z_0 - корень $f(z)$ и поле $\mathbb{C}$ комплексных чисел алгебраически замкнуто.

Теорема доказана.

§50. Каноническое разложение многочлена над полем комплексных чисел

Теорема 50.1. *Для любого многочлена $f(z) = \sum_{k=0}^{n} a_k z^k \in \mathbb{C}[z]$ степени $n \geq 1$ существуют числа $c_1, c_2, \ldots, c_n \in \mathbb{C}$ такие, что*

$$f(z) = a_n(z - c_1)(z - c_2)\ldots(z - c_n). \tag{50.1}$$

Это разложение единственно с точностью до порядка сомножителей.

Доказательство. Из алгебраической замкнутости поля $\mathbb{C}$ следует существование корня $c_1 \in \mathbb{C}$ многочлена $f(z)$. Тогда в кольце $\mathbb{C}[z]$ многочлен $f(z)$ делится (теорема 49.1) на многочлен $z - c_1$, так что $f(z) = (z - c_1)f_1(z)$, где $f_1(z) \in \mathbb{C}[z]$, $\deg f_1 = n - 1$. Если $n - 1 \geq 1$, то к многочлену $f_1(z)$ также применима основная теорема алгебры и, следовательно, $f(z) = (z-c_1)(z-c_2)f_2(z)$, где $f_2(z) \in \mathbb{C}[z]$, $\deg f_2 = n-2$, $c_2 \in \mathbb{C}$. Применив эти рассуждения n раз, найдем числа $c_1, c_2, \ldots, c_n \in \mathbb{C}$ такие, что

$$f(z) = (z - c_1)(z - c_2)\ldots(z - c_n)f_n, \tag{50.2}$$

где $\deg f_n = 0$ и, следовательно, f_n – константа. Сравнив коэффициенты при z^n в обеих частях равенства (50.2), получим, что $f_n = a_n$. Тем самым доказано существование разложения (50.1).

Докажем его единственность. Пусть существует другое разложение:

$$f(z) = a_n(z - d_1)(z - d_2)\ldots(z - d_n). \tag{50.3}$$

Каждое число c_i из первого разложения встречается среди чисел $d_1, \ldots, d_n$ второго разложения, так как в противном случае для $c_i \neq$

d_j, $j = \overline{1, n}$, из (50.1) получим, что $f(c_i) = 0$, а из (50.3) – что $f(c_i) \neq 0$. Аналогично каждое число d_j встречается в первом разложении.

Покажем теперь, что если $c_i = d_j$, то c_i встречается в (50.1) столько же раз, сколько d_j в (50.3). Пусть c_i равно d_j и встречается в (50.1) k раз, а в (50.3) – m раз и пусть $k > m$. Положим $(z - c_i)^m = \varphi(z)$. Тогда

$$\varphi(z)(z - c_i)^{k-m} \prod_{c_s \neq c_i} (z - c_s) = \varphi(z) \prod_{d_s \neq d_j} (z - d_s),$$

откуда следует, что

$$\varphi(z)\left((z - c_i)^{k-m} \prod_{c_s \neq c_i} (z - c_s) - \prod_{d_s \neq d_j} (z - d_s)\right) = 0.$$

Так как в кольце $\mathbb{C}[z]$ нет делителей нуля и $\varphi(z) \neq 0$, то

$$(z - c_i)^{k-m} \prod_{c_s \neq c_i} (z - c_s) = \prod_{d_s \neq d_j} (z - d_s).$$

Положив в этом равенстве $z = c_i$, придем к противоречию. Итак, $k \leq m$. Аналогично показывается, что $m \leq k$. Значит, $k = m$. ■

Теорема 50.2 (о каноническом разложении многочлена над полем $\mathbb{C}$). *Для любого многочлена $f(z) = \sum_{k=0}^{n} a_k z^k \in \mathbb{C}[z]$ степени $n \geq 1$ существуют числа $c_1, c_2, \ldots, c_m \in \mathbb{C}$, где $c_i \neq c_j$ при $i \neq j$, и числа $k_1, k_2, \ldots, k_m \in \mathbb{N}$, где $k_1 + k_2 + \ldots + k_m = n$, такие, что*

$$f(z) = a_n(z - c_1)^{k_1}(z - c_2)^{k_2} \ldots (z - c_m)^{k_m}. \tag{50.4}$$

Это разложение единственно с точностью до порядка сомножителей.