Лекция 16.

Гайфуллин Сергей Александрович

МГУ

16 ноября, 2021

Определение

Коммутативное ассоциативное кольцо с единицей без делителей нуля называется областью целостности.

Примеры: $\mathbb{Z}$, поле.

Определение

Пусть R – коммутативное ассоциативное кольцо с единицей. Многочлен над R – это финитная (то есть с конечным числом ненулевых элементов) последовательность $(a_0, a_1, a_2, \ldots)$, где $a_i \in R$.

Определим операции сложения и умножения на многочленах.
По определению
$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$.
Очевидно, что сумма двух финитных последовательностей – финитная последовательность.

По определению

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots),$$

где $c_k = \sum_{j=0}^{k} a_j b_{k-j}$.

Рассмотрим множество многочленов $R[x]$ с коэффициентами из R с операциями $+$ и $\cdot$

Предложение

$(R[x], +, \cdot)$ – коммутативное ассоциативное кольцо с единицей.

Доказательство. Все аксиомы очевидны, кроме ассоциативности умножения. Пусть
$((a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots)) \cdot (c_0, c_1, c_2, \ldots) = (d_0, d_1, d_2, \ldots)$
и $(a_0, a_1, a_2, \ldots) \cdot ((b_0, b_1, b_2, \ldots) \cdot (c_0, c_1, c_2, \ldots)) = (f_0, f_1, f_2, \ldots)$.
Обозначим $(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (u_0, u_1, u_2, \ldots)$,
$(b_0, b_1, b_2, \ldots) \cdot (c_0, c_1, c_2, \ldots) = (v_0, v_1, v_2, \ldots)$.

Продолжение доказательства

Имеем

$$d_k = \sum_{j=0}^{k} u_j c_{k-j} = \sum_{j=0}^{k} \sum_{i=0}^{j} a_i b_{j-i} c_{k-j} = \sum_{p+q+r=k} a_p b_q c_r.$$

Аналогично

$$f_k = \sum_{i=0}^{k} a_i v_{k-i} = \sum_{i=0}^{k} \sum_{s=0}^{k-i} a_i b_s c_{k-i-s} = \sum_{p+q+r=k} a_p b_q c_r.$$

Заметим, что единицей кольца является элемент $(1, 0, 0, \ldots)$. При этом элементы $(r, 0, 0 \ldots)$ складываются и умножаются также, как и элементы кольца R. Таким образом, отождествим элемент $(r, 0, 0 \ldots) \in R[x]$ и $r \in R$ и получим вложение колец $R \subset R[x]$ (инъективный гомоморфизм).

Обозначим $(0, 1, 0, \ldots) \in R[x]$ через x.

Лемма

x^n – это последовательность, в которой на n-ом месте стоит единица, а остальные элементы – нули.

Доказательство. Индукция по n. База очевидна. Шаг индукции.

$$x^n = x^{n-1} \cdot x = (0, 0, \ldots, 0, 1, 0 \ldots) \cdot (0, 1, 0, \ldots).$$

При этом при $(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$, выполнено $c_k = \sum_{j=0}^{k} a_j b_{k-j}$. У нас не равно 0 только a_1 и b_{n-1}. Таким образом, единственное c_i не равное нулю – это $c_n = 1$. Таким образом, многочлен $f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ может быть записан как $f(x) = a_0 + a_1 x + \ldots + a_n x^n$.

Определение

Степень $\deg f$ многочлена $f \neq (0, 0, \ldots)$ равна максимальному n такому, что $a_n \neq 0$.

Теорема

1) $\deg(f+g) \leq \max(\deg f, \deg g)$;
2) Если R – целостное кольцо, то $\deg(fg) = \deg f + \deg g$.

Доказательство. Пусть $f = (a_0, a_1, \ldots, a_m, 0, 0, \ldots)$, $g = (b_0, b_1, \ldots, b_n, 0, 0, \ldots)$. Тогда $f + g = (a_0 + b_0, a_1 + b_1, \ldots)$, при $j > \max(m, n)$ элемент с номером j будет нулевой. Пусть $fg = (c_0, c_1, \ldots)$. Тогда $c_k = \sum_{j=0}^{k} a_j b_{k-j}$. Если $k > m + n$, то $c_k = 0$. При этом $c_{m+n} = a_m b_n \neq 0$, так как R целостное. Значит, $\deg(fg) = m + n$.

Следствие

Кольцо многочленов над целостным кольцом целостное.

Пример

В $\mathbb{Z}_4[x]$ выполнено $(2x+1)^2 = 1$.

Задача

Найдите обратимый многочлен положительной степени в $\mathbb{Z}_6[x]$.

Существует естественный гомоморфизм из кольца многочленов $R[x]$ в кольцо функций $R \to R$, который переводит многочлен $a_0 + a_1 x + \ldots + a_n x^n$ в функцию

$$\{r \mapsto a_0 + a_1 r + \ldots + a_n r^n\}.$$

Данный гомоморфизм не всегда сюръективен. Например, при $R = \mathbb{Z}_2$ функций конечное число, а многочленов – бесконечное. Однако мы докажем на следующей лекции, что если R – бесконечное поле, то данный гомоморфизм инъективен. И в этом случае будем в дальнейшем отождествлять многочлен и его образ при данном гомоморфизме (то есть многочлен формальный и многочлен как функцию).

Теорема (основная теорема алгебры)

Любой многочлен $f \in \mathbb{C}[x]$ положительной степени имеет комплексный корень, то есть число z_0 такое, что $f(z_0) = 0$.

Основные понятия матанализа над $\mathbb{C}$

Определение

Пусть $z_0 \in \mathbb{C}$. Тогда ε-окрестность точки z_0 – это

$$U_\varepsilon(z_0) = \{z \in \mathbb{C} : |z - z_0| < \varepsilon\}.$$

Определение

Пусть $z_1, z_2, \ldots, z_n, \ldots$ – последовательность комплексных чисел. Будем говорить, что она имеет предел $w \in \mathbb{C}$, при $n \to \infty$, если для любого $\varepsilon > 0 \in \mathbb{R}$ существует $N \in \mathbb{N}$ такое, что для любого $n > N$ выполнено $z_n \in U_\varepsilon(w)$.

Лемма

Пусть $z_j = x_j + iy_j$ и $w = u + iv$. Тогда

$$\lim_{n\to\infty} z_n = w \Leftrightarrow \begin{cases} \lim\limits_{n\to\infty} x_n = u; \\ \lim\limits_{n\to\infty} y_n = v. \end{cases}$$

Доказательство.

$$\lim_{n\to\infty} z_n = w \Leftrightarrow \lim_{n\to\infty} |z_n - w| = 0 \Leftrightarrow$$

$$\Leftrightarrow \lim_{n\to\infty} \sqrt{(x_i - u)^2 + (y_i - v)^2} = 0 \Leftrightarrow$$

$$\Leftrightarrow \lim_{n\to\infty} (x_i - u)^2 + (y_i - v)^2 = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \lim\limits_{n\to\infty} x_n = u; \\ \lim\limits_{n\to\infty} y_n = v. \end{cases}$$

Следствие

Пусть $\lim\limits_{n\to\infty} z_n = w$ и $\lim\limits_{n\to\infty} z'_n = w'$. Тогда $\lim\limits_{n\to\infty}(z_n + z'_n) = w + w'$ и $\lim\limits_{n\to\infty}(z_n z'_n) = ww'$.

Доказательство. По условию $x_n \to u$, $y_n \to v$, $x'_n \to u'$, $y'_n \to v'$.
Тогда, $z_n + z'_n = (x_n + x'_n) + i(y_n + y'_n)$. Но $x_n + x'_n \to u + u'$, $y_n + y'_n \to v + v'$. Значит, $z_n + z'_n \to w + w'$.

Аналогично,
$z_n z'_n = (x_n + iy_n)(x'_n + iy'_n) = (x_n x'_n - y_n y'_n) + i(x_n y'_n + x'_n y_n)$. Но $(x_n x'_n - y_n y'_n) \to uu' - vv'$, $(x_n y'_n + x'_n y_n) \to uv' + u'v$. Отсюда

$$z_n z'_n \to (uu' - vv') + i(uv' + u'v) = ww'.$$

Определение

Пусть $f : \mathbb{C} \to \mathbb{C}$ – функция. Тогда $\lim\limits_{z \to w} f(z) = c \in \mathbb{C}$, если для каждого $\varepsilon > 0 \in \mathbb{R}$ найдется $\delta > 0 \in \mathbb{R}$ такое, что при $z \in U_\delta(w)$ выполнено $f(z) \in U_\varepsilon(c)$.

Совершенно аналогично утверждениям для последовательностей доказываются следующие утверждения.

Лемма

Пусть $c = a + ib$. Тогда $\lim\limits_{z \to w} f(z) = c \Leftrightarrow \begin{cases} \lim\limits_{z \to w} \mathrm{Re}(f(z)) = a; \\ \lim\limits_{z \to w} \mathrm{Im}(f(z)) = b. \end{cases}$

Следствие

Пусть $\lim\limits_{z \to w} f(z) = c$ и $\lim\limits_{z \to w} g(z) = d$. Тогда $\lim\limits_{z \to w} (f(z) + g(z)) = c + d$ и $\lim\limits_{z \to w} (f(z)g(z)) = cd$.

Определение

Функция $f : \mathbb{C} \to \mathbb{C}$ называется непрерывной в точке w, если $\lim\limits_{z \to w} f(z) = f(w)$.

Из доказанного выше следует следующая лемма.

Лемма

Сумма и произведение непрерывных функций – это непрерывная функция.

Следствие

Многочлен $f(z) \in \mathbb{C}[z]$ задает непрерывную функцию $\mathbb{C} \to \mathbb{C}$.

Определение

Подмножество $L \subset \mathbb{C}$ называется открытым, если для любого $z \in L$ существует $\varepsilon > 0 \in \mathbb{R}$ такой, что $U_\varepsilon(z) \subset L$.
Подмножество $S \subset \mathbb{C}$ называется замкнутым, если $\mathbb{C} \setminus S$ открыто.

Лемма

Пусть S замкнуто. Тогда если $z_i \in S$ при всех i и существует предел $\lim\limits_{n\to\infty} z_n = w$, то $w \in S$.

Доказательство. Предположим $w \notin S$. Тогда найдется $\varepsilon > 0 \in \mathbb{R}$ такой, что $U_\varepsilon(w) \cap S = \varnothing$. Однако начиная с некторого номера $z_n \in U_\varepsilon(w)$. Противоречие.

Определение

Подмножество $K \subset \mathbb{C}$ называется компактом, если K замкнуто и ограничено, то есть существует $N \in \mathbb{R}$ такое, что $K \subset \{z : |z| < N\}$.

Лемма

Из любой последовательности в компакте K можно выбрать сходящуюся подпоследовательность.

Доказательство. Пусть есть последовательность $z_n = x_n + iy_n \in K$. Тогда последовательность x_n ограничена, а значит, можно найти такую подпоследовательность в z_n, что x_n для нее сходятся. Можно считать, что это верно для всей $\{z_n\}$. Аналогично, последовательность y_n ограничена, а значит, мы можем перейти к подпоследовательности, в которой $\{y_n\}$ сходится. Так как последовательности $\{x_n\}$ и $\{y_n\}$ для этой подпоследовательности имеют предел, то и сама подпоследовательность имеет предел. В силу замкнутости K, предел лежит в K.

Теорема

Непрерывная функция $h\colon \mathbb{C} \to \mathbb{R}$ достигает на компакте K минимального значения.

Доказательство. Пусть $M = \inf\limits_{z \in K} h(z)$. Тогда существует последовательность $z_n \in K$ такая, что $\lim\limits_{n \to \infty} h(z_n) = M$.

Выберем из этой последовательности сходящуюся подпоследовательность. Так как функция непрерывна, ее значение в предельной точке этой подпоследовательности равно M.

Лемма о возрастании модуля

Пусть $f(z) \in \mathbb{C}[z]$ – многочлен положительной степени. Тогда $\lim\limits_{|z|\to\infty} |f(z)| = \infty$. То есть для каждого $C \in \mathbb{R}$ существует $D \in \mathbb{R}$ такое, что при $|z| > D$ выполнено $|f(z)| > C$.

Доказательство. Заметим, что $|z| \to \infty \Leftrightarrow \frac{1}{z} \to 0$.
Пусть

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

Тогда

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

Но при $|z| \to \infty$ выполнено $\frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \ldots + \frac{a_{n-1}}{z} \to 0$. Значит, существует такое $P \in \mathbb{R}$, что при $|z| > P$ выполнено

$$\left| \frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \ldots + \frac{a_{n-1}}{z} \right| < \frac{|a_n|}{2}.$$

Продолжение доказательства

Для модулей комплексных чисел выполнено неравенство треугольника (модуль – длина вектора):

$$|z_1| - |z_2| \leq |z_1 + z_2| \leq |z_1| + |z_2|.$$

Отсюда

$$\left|\frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \ldots + \frac{a_{n-1}}{z} + a_n\right| \geq$$

$$\geq |a_n| - \left|\frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \ldots + \frac{a_{n-1}}{z}\right| > |a_n| - \frac{|a_n|}{2} > \frac{|a_n|}{2}.$$

Тогда $|f(z)| > |z^n| \cdot \frac{|a_n|}{2} > D^n \frac{|a_n|}{2}$. Если D таково, что $D^n \frac{|a_n|}{2} > C$, то $|f(z)| > C$.
Лемма доказана.