Линейная Алгебра

Игорь Энгель

10 июня 2020 г.

Содержание

1. Комплексные числа

Замечание.

В $\mathbb{R}$ существуют неприводимые многочлены с $\deg p(x) \geqslant 2$.

Это неудобно.

Хотим найти поле содержащие $\mathbb{R}$ в котором таких многочленов нет.

***Определение* 1.1.** Пусть K, L - поля. K - подкольцо внутри L. Тогда L называется расширением поля K.

Рассмотрим многочлен $x^2 + 1$. Назовём его корень i.

1. $i \in L$
2. $\mathbb{R} \subset L$
3. Тогда $a + bi \in L$ если $a, b \in \mathbb{R}$

Так-же поле L содержит выражения вида $a + bi + ci^2$, но так-как i^2 по определению равен -1. Значит, такие выражения сводятся к $a' + bi$. Аналогично для больших степеней.

Рассмотрим операции поля:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i = a' + b'i.$$

Значит, эти выражения задают подкольцо в L.

Возьмём множество пар вещественных чисел $\mathbb{R}^2$.

Введём на нём сложение: $\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle$.

Введём умножения: $\langle a, b\rangle \cdot \langle c, d\rangle = \langle ac - bd, ad + bc\rangle$.

Заметим, что сущетсвует корень многочлена $x^2 + 1 \in \mathbb{R}^2[x]$: $\langle 0, 1\rangle \cdot \langle 0, 1\rangle = \langle 0 - 1, 0 + 0\rangle = \langle -1, 0\rangle$.

Теорема 1.1. $\mathbb{R}^2$ с этими операциями - кольцо.

Доказательство. $\mathbb{R}^2$ - абелева группа, как произведение абелевых групп.

Коммутативность:

$$\langle a, b\rangle \cdot \langle c, d\rangle = \langle ac - bd, ad + bc\rangle = \langle ca - db, da + cb\rangle = \langle c, d\rangle \cdot \langle a, b\rangle .$$

Дистрибутивность:

$$\begin{aligned}
&\langle a, b\rangle \cdot (\langle c, d\rangle + \langle e, f\rangle) \\
&\quad = \langle a, b\rangle \cdot \langle c + e, d + f\rangle \\
&\quad = \langle a(c + e) - b(d + f), a(d + f) + b(c + e)\rangle \\
&\quad = \langle ac + ae - (bd + bf), ad + af + bc + be\rangle \\
&\quad = \langle ac - bd, ad + bc\rangle + \langle ae - bf, af + be\rangle \\
&\quad = \langle a, b\rangle \cdot \langle c, d\rangle + \langle a, b\rangle \cdot \langle e, f\rangle
\end{aligned}$$

Ассоциативность:

$$\begin{aligned}
&\langle a, b\rangle \cdot (\langle c, d\rangle \cdot \langle e, f\rangle) \\
&\quad = \langle a, b\rangle \cdot \langle ce - df, cf + de\rangle \\
&\quad = \langle a(ce - df) - b(cf + de), a(cf + de) - b(ce - df)\rangle \\
&\quad = \langle ace - adf - bcf - bde, acf + ade - bce - bdf\rangle \\
&\quad = \langle e(ac - bd) - f(ad + bc), e(ad - bc) + f(ac - bd)\rangle \\
&\quad = \langle ac - bd, ad + bc\rangle \cdot \langle e, f\rangle \\
&\quad = (\langle a, b\rangle \cdot \langle c, d\rangle) \cdot \langle e, f\rangle
\end{aligned}$$

Единица:

$$\langle 1, 0\rangle \cdot \langle a, b\rangle = \langle 1a - 0b, 1b + 0a\rangle = \langle a, b\rangle\,.$$ □

***Определение* 1.2.** Полем комплексных чисел $\mathbb{C}$ называется $\langle \mathbb{R}^2, +, \cdot\rangle$

Элементы $\mathbb{C}$ записываются как $a + bi$ (соответсвуют элементам вида $\langle a, b\rangle$)

Теорема 1.2. $\mathbb{C}$ - поле

Доказательство. Найдём обратный элемент для $a + bi$.

$$(a + bi)(a - bi) = a^2 - b^2 i^2 = a^2 + b^2.$$

Если $a + bi \neq 0$, то $a^2 + b^2 \neq 0$.

Поделим:

$$\frac{(a + bi)(a - bi)}{a^2 + b^2} = 1.$$

Значит, $\frac{a-bi}{a^2+b^2}$ - обратный к $a + bi$. □

Замечание. В $\mathbb{C}$ любой вещественный многочлен степени 2 раскладывается на линейные множители.

Доказательство. Рассмотрим многочлен $x^2 + bx + c$. $b, c \in \mathbb{R}$.

Тогда его корни имеют вид

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Если $D = b^2 - 4c \geqslant 0$, то у него есть вещественный корень.

Если $D < 0$, то вещественных корней нет.

Тогда $D = -1 \cdot |D|$.

$$x_{1,2} = \frac{-b \pm \sqrt{(-1)|D|}}{2} = \frac{-b \pm \sqrt{|D|}\sqrt{-1}}{2} = \frac{-b \pm |D|i}{2}.$$ □

Свойства. Пусть $z = a + bi \in \mathbb{C}$.

$a = \operatorname{Re} z$ - вещественная часть

$b = \operatorname{Im} z$ - мнимая часть

$\overline{z} = a - bi$ - комплексно-сопряжённое к z число

$|z| = \sqrt{a^2 + b^2}$ - модуль z

***Определение* 1.3.** R_1, R_2 - кольца. $f : R_1 \to R_2$ называется гомоморфизмом колец, если

1. $f(a + b) = f(a) + f(b)$
2. $f(a \cdot b) = f(a) \cdot f(b)$
3. $f(1) = 1$ - если кольцо с единицей.

***Определение* 1.4.** Если $f : R_1 \mapsto R_2$ гомоморфизм колец и биекция, то f - изоморфизм колец.

Утверждение 1.3. Комплексное сопряжения - изоморфзим $\mathbb{C} \mapsto \mathbb{C}$.

Доказательство.

$$\overline{(a+bi)+(c+di)} = \overline{(a+c)+(b+d)i} = (a+c)-(b+d)i.$$

$$\overline{a+bi} + \overline{c+di} = (a-bi)+(c-di) = (a+c)-(b+d)i.$$

$$\overline{(a+bi)(c+di)} = \overline{(ac-bd)+(ad+bc)i} = (ac-bd)-(ad+bc)i.$$

$$\overline{a+bi} \cdot \overline{c+di} = (a-bi)(c-di) = (ac-(-b)(-d)) + (a(-d)+(-b)c)i = (ac-bd)-(ad+bc)i.$$

$$\overline{1+0i} = 1+0i.$$

□

Лемма. $\psi : R_1 \mapsto R_2$ гомоморфизм колец.

$g(x) \in R_1[x]$ - многочлен. $\lambda \in R_1$ - корень $g(x)$

Построим многочлен $\psi(g) = \psi(a_0) + \psi(a_1)x + \ldots \psi(a_n)x^n$

Тогда $\psi(\lambda) \in \mathbb{R}_2$ - корень $\psi(g)$

Доказательство.

$$a_1\lambda + a_2\lambda^2 + \ldots + a_n\lambda^n = 0.$$

$$\psi(a_1\lambda + a_2\lambda + \ldots + a_n\lambda^n) = \psi(0) = 0.$$

$$\psi(a_1\lambda + a_2\lambda^2 + \ldots + a_n\lambda) = \psi(a_1)\psi(\lambda) + \psi(a_2)\psi(\lambda)^2 + \ldots + \psi(a_n)\psi(\lambda)^n = \psi(g)(\psi(\lambda)) = 0.$$

□

Утверждение 1.4. Если $\varphi : \mathbb{C} \mapsto \mathbb{C}$ - изоморфизм колец, и $\forall x \in \mathbb{R} \quad \varphi(x) = x$, то либо $\forall z \in \mathbb{C} \quad \varphi(z) = z$, либо $\forall z \in \mathbb{C} \quad \varphi(z) = \overline{z}$

Доказательство. $\varphi(a + bi) = \varphi(a) + \varphi(b)\varphi(i) = a + b\varphi(i)$.

$\varphi(x^2 + 1) = x^2 + 1$.

Значит $\varphi(i)$ тоже корень $x^2 + 1$. Значит, либо $\varphi(i) = i$, либо $\varphi(i) = -i$. □

Утверждение 1.5. $|z| = \sqrt{z\overline{z}}$

Доказательство. $z\overline{z} = (a + bi)(a - bi) = a^2 + b^2$. □

Утверждение 1.6. $|z_1 z_2| = |z_1||z_2|$

Доказательство. $|z_1 z_2|^2 = z_1 z_2 \cdot \overline{z_1 z_2} = z_1\overline{z_1}z_2\overline{z_2} = |z_1|^2|z_2|^2$. □

***Определение* 1.5.** Аргументом $z = a + bi \neq 0$ называется угол между вещественной прямой и радиус-вектором точки задаваемой этим числом на комплексной плоскости. И обозначается $\operatorname{Arg} z \in \mathbb{R}/(2\pi\mathbb{Z})$.

Утверждение 1.7. $z_1, z_2 \neq 0$. $\operatorname{Arg} z_1 z_2 = \operatorname{Arg} z_1 + \operatorname{Arg} z_2$.

Доказательство. $\operatorname{Arg} \frac{z_1}{|z_1|} = \operatorname{Arg} z_1$, значит можно доказывать только для элементов с $|z| = 1$.

$|z_1| = |z_2| = 1$. Пусть $\varphi = \operatorname{Arg} z_1$, $\psi = \operatorname{Arg} z_2$.

Тогда $z_1 = \cos\varphi + i\sin\varphi$, $z_2 = \cos\psi + i\sin\psi$.

$$z_1 z_2 = (\cos\varphi\cos\psi - \sin\varphi\sin\psi) + i(\cos\varphi\sin\psi + \cos\psi\sin\varphi) = \cos(\varphi+\psi) + i\sin(\varphi+\psi). \qquad \square$$

Доказательство. Факт: Пусть есть изометрия плоскости у которой ести единственная неподвижная точка, то эта изометрия - поворот.

Введём расстояние между комплексными числами - $\rho(z_1, z_2) = |z_1 - z_2|$. Оно соответсвует обычному расстоянию на плоскости.

$|z_1| = |z_2| = 1$.

При $z_1 = 1$ тривиально, предположим что $z_1 \neq 1$.

Рассмотрим отображения $x \mapsto z_1 x$.

Докажем что это изометрия: $|z_1 x - z_1 y| = |z_1(x - y)| = |z_1||x - y| = |x - y|$.

Заметим, что $z_1 x = x \iff x(z_1 - 1) = 0 \iff x = 0$.

Значит, заданное отображение - поворот вокруг начала координат. При этом, так-как $z_1 \cdot 1 = z_1$, то это поворот на угол $\operatorname{Arg} z_1$. Значит, $\operatorname{Arg} z_1 x = \operatorname{Arg} z_1 + \operatorname{Arg} x \implies \operatorname{Arg} z_1 z_2 = \operatorname{Arg} z_1 + \operatorname{Arg} z_2$. $\square$

***Определение* 1.6.** Тригонометрическая форма записи комплексного числа $z \neq 0$ с аргументом $\varphi = \operatorname{Arg} z$:

$$a + bi = z = |z|\frac{z}{|z|} = |z|(\cos\varphi + i\sin\varphi) =: |z|e^{i\varphi}.$$

Свойство. $z_1 = r_1 e^{i\varphi_1}$, $z_2 = r_2 e^{i\varphi_2}$.

$z_1 z_2 = r_1 r_2 e^{i\varphi_1} e^{i\varphi_2} = r_1 r_2 e^{i(\varphi_1+\varphi_2)}$

Замечание.

$$e^x = 1 + x + \frac{x^2}{2!} + \ldots \frac{x^j}{j!} + \ldots.$$

$$e^{ix} = 1 + ix + \frac{-x}{2!} + \frac{-ix}{3!} + \frac{x}{4!} + \ldots.$$

При чётных степенях:

$$1 - \frac{x^2}{2} + \frac{x^4}{4!} + \ldots + (-1)^k \frac{x^{2k}}{2k!} = \cos x.$$

При нечётных:

$$ix - \frac{ix^3}{3!} + \ldots + (-1)^k \frac{ix^{2k+1}}{(2k+1)!} = i\sin x.$$

$$e^{ix} = \cos x + i\sin x.$$

Теорема 1.8. В комплексных числах есть корни уравнения вида $x^n = a$

Доказательство. Если $a = 0$, то сущетсвует единственный корень кратности n - $x = 0$.

Предположим что $a \neq 0$.

$$a = re^{i\varphi}$$

$$x = se^{i\alpha}.$$

$$x^n = s^n e^{in\alpha}.$$

$$s^n = r \implies s = \sqrt[n]{r}.$$

$$n\alpha = \varphi + 2\pi k \implies \alpha = \frac{\varphi}{n} + \frac{2\pi}{n}k.$$

$$x_k = \sqrt[n]{r}e^{i\left(\frac{\varphi}{n} + \frac{2\pi}{n}k\right)}.$$

Таких решений n штук, значит это все решения уравнения. □

Пример. Рассмотрим уравнение $x^n = 1 = 1 \cdot e^0$.

Тогда $\varepsilon_k = e^{i \cdot \frac{2\pi k}{n}}$.

***Определение* 1.7.** R - кольцо, $x \in R$ удовлетворяющий $x^n = 1$. Тогда x - корнеь степени n из единицы.

***Определение* 1.8.** K - поле, тогда $\varepsilon \in K$ называется первообразным корнем степени n из единицы, если $\operatorname{ord} \varepsilon = n$.

Замечание. Все первообразные корни степени n из единицы в $\mathbb{C}$ имеют вид ε_k, где k взаимно просто с n.

Теорема 1.9 (Основная теорема алгебры)**.** Любой неконстантный многочлен $p(x) \in \mathbb{C}[x]$ имеет хотя-бы один корень в $\mathbb{C}$.

Без доказательства.

***Определение* 1.9.** Поле K называется алгебраически замкнутым, если у любого неконстантного многочлена $p(x) \in K[x]$ есть корень в K.

Лемма. K - алгебраически замкнутое поле. $p(x) \in K[x]$, $n = \deg p \geqslant 1$, тогда p имеет ровно n корней с учётом кратности.

Доказательство. Если $n = 1$, то есть ровно один корень.

Пусть $n > 1$, так-как K замкнуто, то существует корень λ.

Тогда $p(x) = p'(x)(x - \lambda)$.

По индукции у $p'(x)$ ровно $n - 1$ корень с учётом кратности, и один корень у $x - \lambda$. Итого, n корней. □

Замечание. Любой многочлен $f(x) \in \mathbb{C}[x]$ представляется в виде

$$f(x) = c(x - \lambda_1) \ldots (x - \lambda_n).$$

Лемма. Если $\lambda \in \mathbb{C}$ - корень $p(x) \in \mathbb{R}[x]$, то $\overline{\lambda}$ - тоже корень.

Доказательство. Заметим, что $p(x) = \overline{p}(x)$. Значит, их корни совпадают. Но $\overline{\lambda}$ - корень $\overline{p}(x)$. $\square$

Утверждение 1.10. Если $p(x) \in \mathbb{R}[x]$ неприводимый, то либо $p(x) = c(x-\lambda)$, либо $p(x) = x^2 + bx + c$ и $b^2 - 4c < 0$.

Доказательство. То, что эти многочлены неприводимы тривиально.

Предположим что p неприводим и $\deg p > 2$.

Заметим, что p имеет комплексный корень λ. Тогда $p \vdots_{\mathbb{C}} (x-\lambda)$ и $p \vdots_{\mathbb{C}} (x-\overline{\lambda})$.

$\lambda \neq \overline{\lambda}$, так-как p неприводим.

Тогда $p(x) = p'(x)((x-\lambda)(x-\overline{\lambda})) = p'(x)\left(x^2 - \lambda x - \overline{\lambda}x + \lambda\overline{\lambda}\right) = p'(x)\,(x^2 - 2\operatorname{Re}\lambda x + |\lambda|^2)$.

Предположим что $p(x) \not\vdots_{\mathbb{R}} (x-\lambda)(x-\lambda')$.

Тогда они взаимно простые. Тогда

$$a(x)p(x) + b(x)(x-\lambda)(x-\overline{\lambda}) = 1.$$

Но $p(\lambda) = 0$ и $(\lambda-\lambda)(\lambda-\overline{\lambda}) = 0$. Противоречие.

Значит, $p' \in \mathbb{R}[x]$, и p приводим. Противоречие, значит неприводимых многочленов степени больше 2 не существует. $\square$