1 Комплексные числа

1.1 Построение поля комплексных чисел

Мы рассмотрим расширение поля действительных чисел, построив поле так называемых *комплексных чисел*. По определению комплексное число — это пара действительных чисел (a, b). Комплексные числа можно складывать и умножать по следующим правилам:

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b)(c, d) = (ac - bd, ad + bc). \tag{1}$$

Множество всех таких пар мы обозначим через $\mathbb{C}$, имея ввиду, что на нём действуют вышеопределённые бинарные операции.

Теорема 1.1. *Множество $\mathbb{C}$ является полем относительно операций сложения и умножения (1).*

Доказательство. Докажем сначала, что $\mathbb{C}$ — коммутативное кольцо (с единицей). Для этого существует два способа.

Способ 1. Проверим вручную определения кольца. Нулём является пара $(0, 0)$, противоположным к паре (x, y) является пара $(-x, -y)$.

Ассоциативность следует из следующих вычислений:

$$\begin{aligned}\big((a, b)(c, d)\big)(f, g) &= (ac - bd, ad + bc)(f, g) = \\ &= \big((ac - bd)f - (ad + bc)g, (ac - bd)g + (ad + bc)f\big) = \\ &= (acf - bdf - adg - bcg, acg - bdg + adf + bcf).\end{aligned}$$

$$\begin{aligned}(a, b)\big((c, d)(f, g)\big) &= (a, b)\big(cf - dg, cg + df\big) = \\ &= \big(a(cf - dg) - b(cg + df), a(cg + df) + b(cf - dg)\big) = \\ &= (acf - adg - bcg - bdf, acg + adf + bcf - bdg).\end{aligned}$$

Как легко видеть эти выражения совпадают.

Проверим дистрибутивность. Получаем

$$\begin{aligned}(a, b)&\big((c, d) + (f, g)\big) = \\ &= (a, b)(c + f, d + g) = \big(a(c + f) - b(d + g), a(d + g) + b(c + f)\big) = \\ &= (ac + af - bd - bg, ad + ag + bc + bf).\end{aligned}$$

$$\begin{aligned}(a, b)(c, d) + (a, b)(f, g) &= (ac - bd, ad + bc) + (af - bg, ag + bf) = \\ &(ac - bd + af - bg, ad + bc + ag + bf).\end{aligned}$$

Эти выражения тоже совпадают.

Кроме того, в кольце $\mathbb{C}$ существует единица — это элемент $(1, 0)$:

$$(1, 0)(a, b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a, b),$$

$$(a, b)(1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b),$$

и это кольцо коммутативно:

$$(a, b)(c, d) = (ac - bd, ad + bc), \qquad (c, d)(a, b) = (ca - db, cb + da).$$

Способ 2. Отождествим пару (a, b) со следующей матрицей:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Используя правила умножения матриц, легко проверить, что такое отождествление сохраняет сумму и произведение:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -b-d \\ b+d & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix}.$$

При этом единице $(1, 0)$ в кольце $\mathbb{C}$ соответствует единичная матрица E, а противоположному элементу соответствует противоположная матрица. Теперь тот факт, что $\mathbb{C}$ — кольцо следует из того, что $M_2(\mathbb{R})$ — кольцо. Фактически мы отождествили $\mathbb{C}$ с подкольцом кольца $M_2(\mathbb{R})$.

Теперь остаётся доказать, что $\mathbb{C}$ — поле. Это следует следующего вычисления

$$(a, b)\left(\frac{a}{\sqrt{a^2+b^2}}, -\frac{b}{\sqrt{a^2+b^2}}\right) = (1, 0).$$

верного для любых действительных a и b одновременно не равных нулю. □

Теперь мы можем ввести обозначение $i = (0, 1)$. Легко проверить, что $i^2 = (-1, 0)$.

Лемма 1.2. *Отображение $\iota : \mathbb{R} \to \mathbb{C}$, заданное правилом $\iota(a) = (a, 0)$ является инъективным гомоморфизмом колец.*

Доказательство. Отображение ι инъективно по определению. Остаётся доказать, что ι сохраняет операции сложения и умножения. Это следует из следующих вычислений:

$$\iota(a) + \iota(b) = (a, 0) + (b, 0) = (a + b, 0) = \iota(a + b),$$

$$\iota(a)\iota(b) = (a, 0)(b, 0) = (ab - 00, a0 + 0b) = (ab, 0) = \iota(ab).$$

□

Теперь мы можем отождествить каждое действительно число a с его образом $\iota(a)$. При этом мы получаем $i^2 = -1$. Так как для любого комплексного числа (a, b) выполнено

$$(a, b) = (a, 0) + (b, 0)(0, 1) = (a, 0) + (b, 0)i,$$

то мы можем представить любое комплексное число z (с использованием вышеупомянутого отождествления) в виде

$$z = a + bi, \text{ для соответствующих } a, b \in \mathbb{R}.$$

Такое представление называется *алгебраической формой записи* комплексного числа. Мы будем использовать обозначения $a = \operatorname{Re} z$ и $b = \operatorname{Im} z$. Эти числа называются соответственно *действительной* и *мнимой* частью комплексного числа z.

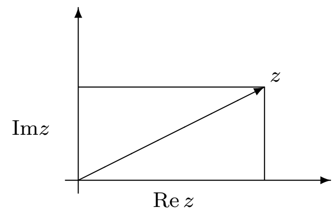
Замечание. Мы ввели комплексные числа как пары действительных чисел. Существуют и альтернативные способы. Например, мы могли бы ввести поле комплексных чисел как подкольцо кольца матриц $M_2(\mathbb{R})$ как в доказательстве теоремы 1.1. Наверное, самым естественным способом введения поля комплексных чисел было бы присоединение к полю действительных чисел $\mathbb{R}$ элемента i, удовлетворяющего свойству $i^2 = -1$. Эту интуитивную идею можно превратить в строго определение, если рассмотреть фактор кольцо

$$\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$$

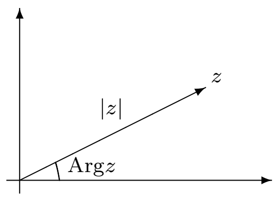
и обозначить через i образ элемента x при естественном гомоморфизме $\mathbb{R}[x] \to \mathbb{C}$. Остаётся ещё обсудить вопрос почему $\mathbb{R}$ вкладывается в $\mathbb{C}$ как подкольцо и почему любой элемент из $\mathbb{C}$ можно единственным образом представать в виде $a+bi$ для $a, b \in \mathbb{R}$. Обсуждение этих вопросов увело бы нас слишком далеко от основного содержания этих лекций. Поэтому мы остановились на более наглядном определении поля комплексных чисел в виде множества пар действительных чисел с операциями (1).

1.2 Модуль и аргумент

Мы будем изображать комплексные числа на плоскости, считая первую компоненту абсциссой, а вторую ординатой.



Рассмотрим, что произойдёт, если задать туже точку z на плоскости в полярной системе координат.



Формулой мы можем записать

$$|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}.$$

Это число называется *модулем* комплексного числа z. Рассмотрим теперь случай $z \neq 0$. Как известно угол в полярных координатах определён не однозначно, а с точностью до $2\pi k$. Используя наши знания о факторкольцах, мы можем определить *аргумент* $\operatorname{Arg} z$ как элемент из факторгруппы $\mathbb{R}/2\pi\mathbb{Z}$, каждый представитель $\varphi \in \operatorname{Arg} z$ которого удовлетворяет соотношениям

$$\cos\varphi = \frac{\operatorname{Re} z}{|z|}, \quad \sin\varphi = \frac{\operatorname{Im} z}{|z|}.$$

В прочем, мы будем понимать сами функции cos и sin как функции из $\mathbb{R}/2\pi\mathbb{Z}$ в $\mathbb{R}$, получаемые из обычных тригонометрических функций следующим образом:

$$\cos(\varphi + 2\pi\mathbb{Z}) = \cos\varphi, \quad \sin(\varphi + 2\pi\mathbb{Z}) = \sin\varphi.$$

Тогда мы можем записать

$$\cos \mathrm{Arg} z = \frac{\mathrm{Re}\, z}{|z|}, \quad \sin \mathrm{Arg} z = \frac{\mathrm{Im} z}{|z|}.$$

Мы получили, что любое комплексное число z можно записать в виде

$$z = r(\cos\varphi + i\sin\varphi),$$

где $r = |z|$ и $\varphi \in \mathrm{Arg} z$, если $z \neq 0$. Эта запись не однозначна по двум причинам: во первых даже если $z \neq 0$, то φ определён с точностью до $2\pi k$; если $z = 0$, то в качествеφ можно взять любое число. Эта запись называется *тригонометрической формой записи* комплексного числа

1.3 Сложение и умножение

Обе формы записи комплексного числа: алгебраическая и тригонометрическая имеют свои преимущества. Вот первой форме легко складывать числа, а во второй их умножать:

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

$$r(\cos\varphi + i\sin\varphi) \cdot r'(\cos\varphi' + i\sin\varphi') = rr'(\cos(\varphi + \varphi') + \sin(\varphi + \varphi')).$$

Последняя формула следует из формул косинуса и синуса суммы. Таким образом мы заключаем, что модуль произведения двух комплексных чисел равен произведению их модулей. При этом, если оба числа ненулевые, то аргумент их произведения равен сумме их аргументов. В качестве следствия из последней формулы получаем формулу *Муавра*

$$(r(\cos\varphi + i\sin\varphi))^n = r^n(\cos(n\varphi) + i\sin(n\varphi)).$$

Кроме того, полезно (и легко запомнить) формулу *Эйлера*

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

Из этой формулы легко “получить” формулы косинуса и синуса суммы, если считать, что экспонента суммы равна произведению экспонент (что выглядит вполне естественно и известно из школьного курса математики). Здесь кавычки стоят потому, что как раз формулы косинуса и синуса суммы позволяют установить правило для экспоненты суммы. Однако такое соображение бывает полезно тем, кто забыл тригонометрические формулы, но помнит формулу Эйлера (что, согласитесь, гораздо проще).

Теперь мы можем определить

$$e^{a+ib} = e^a e^{ib} = e^a(\cos b + i\sin b).$$

Таким образом может быть записано любое комплексное число, кроме нуля. Такая форма записи комплексного числа называется *экспоненциальной*.

1.4 Сопряжение

Сопряжённым к комплексному числу $z = a + ib$ называется число $\bar{z} = a - ib$. В тригонометрической форме получаем

$$\overline{r(\cos\varphi + i\sin\varphi)} = r(\cos\varphi - i\sin\varphi) = r(\cos(-\varphi) + i\sin(-\varphi)).$$

Отсюда следует, что

$$\overline{e^z} = e^{\bar{z}}.$$

Через сопряжённое число удобно выразить действительную и мнимые части, модуль и обратное число:

$$\operatorname{Re} z = \frac{z+\bar{z}}{2}, \qquad \operatorname{Im} z = \frac{z-\bar{z}}{2i}, \qquad |z| = \sqrt{z\bar{z}}, \qquad z^{-1} = \frac{\bar{z}}{|z|^2}.$$

Кроме того $\bar{\bar{z}} = z$ и $|\bar{z}| = |z|$.

Теорема 1.3. *Любой автоморфизм поля $\mathbb{R}$ тождественный.*

Доказательство. Пусть $\varphi : \mathbb{R} \to \mathbb{R}$ — автоморфизм поля $\mathbb{R}$. Докажем последовательно следующие утверждения:

1. $\varphi(x) > 0$, если $x > 0$.
2. φ монотонное.
3. $\varphi(n) = n$ для любого $n \in \mathbb{Z}$.
4. $\varphi(q) = q$ для любого $q \in \mathbb{Q}$.
5. $\varphi(x) = x$ для любого $x \in \mathbb{R}$.

1 $\varphi(x) = \varphi(\sqrt{x}^2) = \varphi(\sqrt{x})^2 > 0$.
2 Пусть $x < y$. Тогда $y - x > 0$. Согласно пункту 1 получаем $\varphi(y - x) > 0$. Отсюда $\varphi(y) - \varphi(x) > 0$ и $\varphi(y) > \varphi(x)$.
3 Пусть n — натуральное число. Тогда

$$\varphi(n) = \varphi(1 + \dots + 1) = \varphi(1) + \dots + \varphi(1) = n\varphi(1) = n.$$

Отсюда $\varphi(-n) = -\varphi(n) = -n$. Остаётся заметить, что $\varphi(0) = 0$.
4 Пусть $q = a/b$, где $a, b \in \mathbb{Z}$ и $b \neq 0$. Согласно пункту 3, получаем

$$a = \varphi(a) = \varphi(qb) = \varphi(q)\varphi(b) = \varphi(q)b.$$

Отсюда $\varphi(q) = a/b = q$.
5 Пусть $s < x < r$ для $r, s \in \mathbb{Q}$. Согласно пунктам 2 и 3 получаем

$$s = \varphi(s) < \varphi(x) < \varphi(r) = r.$$

Так как эти неравенства верны для любых рациональных r и s удовлетворяющих неравенствам $s < x < r$, то $\varphi(x) = x$. □

Теорема 1.4. *Отображение из $\mathbb{C}$ в себя, заданное формулой $z \mapsto \bar{z}$, является единственным нетождественным авторморфизмом поля $\mathbb{C}$ переводящим $\mathbb{R}$ в себя.*

Доказательство. Докажем сначала, что сопряжение — автоморфизм. Для этого заметим, что

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

$$\begin{aligned}\overline{(a+ib)(c+id)} = \overline{ac-bd+i(ad+bc)} = ac-bd-i(ad+bc) = \\ = ac-(-b)(-d)+i(a(-d)+(-b)c) = (a-ib)(c-id) = \overline{(a+ib)(c+id)}.\end{aligned}$$

Пусть теперь $\varphi : \mathbb{C} \to \mathbb{C}$ — автоморфизм, переводящий $\mathbb{R}$ в себя. Применяя теорему 1.3 к ограничению φ на $\mathbb{R}$, получаем, что $\varphi(x) = x$ для любого $x \in \mathbb{R}$. Теперь мы можем заметить, что

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1.$$

Так как уравнение $z^2+1=0$ имеет в $\mathbb{C}$ только два решения $z=i$ или $z=-i$, то $\varphi(i)=i$ или $\varphi(i)=-i$. В первом случае получаем

$$\varphi(a+ib) = \varphi(a) + \varphi(i)\varphi(b) = a+ib$$

для любых $a, b \in \mathbb{R}$, и φ — тождественный автоморфизм. Во втором случае получаем

$$\varphi(a+ib) = \varphi(a) + \varphi(i)\varphi(b) = a-ib$$

для любых $a, b \in \mathbb{R}$, и φ — автоморфизм сопряжения. □

1.5 Основная теорема алгебры

Поле $\mathbb{F}$ называется *алгебраически замкнутым*, если любой многочлен $f \in \mathbb{F}[x]$ степени больше нуля (непостоянный многочлен) имеет хотя бы один корень в $\mathbb{F}$.

Лемма 1.5. *Пусть $\mathbb{F}$ — алгебраически замкнутое поле. Тогда любой многочлен $f \in \mathbb{F}[x]$ представляется в виде $c(x-\alpha_1)\cdots(x-\alpha_n)$ для некоторых $c, \alpha_1, \ldots, \alpha_n \in \mathbb{F}$.*

Доказательство. Если $f=0$, то такое представление существует при $c=0$ и любых n и $\alpha_1, \ldots, \alpha_n$. Теперь предположим, что $\deg f > 0$ и докажем утверждение индукцией по этой степени. База индукции, это случай $\deg f = 1$. В это случае $f = a_1x - a_0 = a_1(x - a_0/a_1)$ и утверждение выполнено.

Пусть теперь $\deg f > 1$. По определению f имеет корень, скажем α_1. По теореме Безу $f = (x-\alpha_1)g$ для некоторого $g \in \mathbb{F}[x]$. Мы знаем, что

$$\deg f = \deg(x-\alpha_1) + \deg g = 1 + \deg g,$$

откуда $\deg g = \deg f - 1$ и $1 \leqslant \deg g < \deg f$. Поэтому к g применимо утверждение леммы:

$$g = c(x-\alpha_2)\cdots(x-\alpha_n)$$

для некоторых $c, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$. Выражая отсюда f, получаем требуемое разложение. □

Теорема 1.6 (Основная теорема алгебры)**.** *Поле $\mathbb{C}$ алгебраически замкнуто.*

Существует много доказательств этой теоремы от чисто топологических до почти полностью алгебраических. Мы не будем приводить их здесь.