Лекция 1
Поля

▷Аксиомы поля ▷Расширения поля рациональных чисел ▷Поле комплексных чисел ▷Геометрические и алгебраические вычисления с комплексными числами ▷Правила раскрытия скобок и тригонометрические тождества ▷Гомоморфизмы полей

§1. Определение и примеры полей

1.1. Что такое поле. Интуитивно наиболее привычной алгебраической структурой является структура поля. Говоря наивно, поле — это такая «числовая область», в которой определены все четыре действия арифметики со всеми своими обычными свойствами. Модельный образец поля — это рациональные числа $\mathbb{Q}$. Строгое определение таково.

1.2. Определение. *Множество k называется полем, если на нём заданы две бинарные операции*[1]*, которые называют сложением: $(a,b) \longmapsto a+b$ и умножением: $(a,b) \longmapsto a\cdot b = ab$, и при этом выполнены следующие свойства:*

Аксиомы поля

1) Аксиомы сложения

   а) коммутативность (переместительный закон): $a+b=b+a \quad \forall a,b\in k$

   б) ассоциативность (сочетательный закон): $a+(b+c)=(a+b)+c \quad \forall a,b,c\in k$

   в) существование нейтрального элемента (нуля): $\exists 0\in k: \quad a=0=a \quad \forall a\in k$

   г) существование противоположного: $\forall a\in k \quad \exists(-a)\in k: \quad a+(-a)=0$

2) Аксиомы умножения

   а) коммутативность: $ab=ba \quad \forall a,b\in k$

   б) ассоциативность: $a(bc)=(ab)c \quad \forall a,b,c\in k$

   в) существование единицы: $\exists 1\in k: \quad a\cdot 1=a \quad \forall a\in k$

   г) существование обратного: $\forall a\in k,\ a\neq 0 \quad \exists a^{-1}\in k: \quad a\cdot a^{-1}=1$

[1] т. е. два правила, сопоставляющие каждой паре элементов $a,b\in k$ некие новые элементы из k, или, более научно, — два отображения из $k\times k$ в k

3) Аксиома дистрибутивности (распределительный закон):

$$a(b+c) = ab + ac \quad \forall a, b \in k$$

4) Аксиома нетривиальности: $0 \neq 1$

1.2.1. Логические комментарии. Следуя современной моде, мы дали «максимально выжатый» список аксиом, из которого исключены все утверждения, являющиеся следствием остальных. Этот идущий от *логистиковков* (термин А.Пуанкаре) стиль подачи нового материала, бесспорно, не самый удобный для читателя: естественно было бы включить в наши аксиомы и такие (интуитивно ожидаемые из опыта работы с рациональными числами) дополнительные свойства операций:

Доп.1: В любом поле нуль единственен.

Доп.2: В любом поле единица единственна.

Доп.3: $\forall a \in k$ противоположный элемент $(-a)$ тоже единственен, в том смысле, что он однозначно определяется по a (отсюда и обозначение, зависящее лишь от a).

Доп.4: $\forall a \in k$, $a \neq 0$ обратный элемент a^{-1} также единственен.

Доп.5: $\forall a \in k \quad a \cdot 0 = 0$.

Доп.6: $(-1) \cdot a = (-a)$ (здесь в левой части стоит произведение элемента a на элемент, противоположный единице, а справа – элемент противоположный к a, и a priori неясно, с чего бы им совпадать)

1.2.2. Предложение. *Дополнительные свойства следуют из аксиом.*

Доказательство. *Доп.1*: Пусть 0_1 и 0_2 – любые два нуля. Тогда $0_2 = 0_2 + 0_1 = 0_1$ (первое равенство написано по аксиоме 1в для 0_1, а второе — по аксиоме 1в для 0_2). Таким образом два нуля равны.

Доп.2: аналогично.

Доп.3: Пусть $(-a)_1$ и $(-a)_2$ – любые два элемента, дающие 0 в сумме с a. Тогда $(-a)_1 = (-a)_1 + 0 = (-a)_1 + (a + (-a)_2) = ((-a)_1 + a) + (-a)_2 = 0 + (-a)_2 = (-a_2)$.

Доп.4: аналогично.

Доп.5: Пусть $a \cdot 0 = b$. Тогда $b + a = a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a(0+1) = a \cdot 1 = a$. Таким образом, $b + a$ и a – это две разных записи для одного и того же элемента. Прибавляя к этому элементу $(-a)$, мы получим новый элемент, который также допускает две разных записи: $b = b + a + (-a)$ и $0 = a + (-a)$. Тем самым $b = 0$.

Доп.6: Надо проверить, что $(-1) \cdot a + a = 0$. Имеем: $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = a \cdot ((-1) + 1) = a \cdot 0 = 0$ (по (Доп.5)). Предложение доказано.

1.2.3. Замечание. Рассуждение при доказательстве свойства (Доп.5) есть не что иное, как подробное объяснение привычной школьной процедуры *прибавления к обеим частям равенства одного и того же числа*. В дальнейшем такие подробности читателю предлагается восстанавливать самостоятельно.

Задача 1.1. Докажите, что аксиома нетривиальности $(0 \neq 1)$ равносильна требованию, чтобы $k \neq \{0\}$.

Задача 1.2. Докажите, что требование $a \neq 0$ в аксиоме 2г существования обратного необходимо, ибо нуль не может иметь обратного в силу остальных аксиом.

1.3. Вычитание и деление. Определим еще две бинарных операции в поле k:

Вычитание: $(a,b) \longmapsto a - b \stackrel{\text{def}}{=} a + (-b)$ (определено для любых элементов поля)

Деление: $(a,b) \longmapsto a/b \stackrel{\text{def}}{=} ab^{-1}$ (определено $\forall a$ и $b \neq 0$).

Задача 1.3. Докажите, что $a - b$ можно было бы определить как единственный элемент из k, который в сумме с b дает a, и дайте аналогичное определение (с доказательством!) для a/b.

1.4. Примеры полей. Поле *рациональных чисел* $\mathbb{Q}$ (т.е. совокупность обыкновенных дробей с общеизвестными правилами действий над ними) является, как уже отмечалось, «основным первоисточником» для абстрактного определения поля.

Поле *вещественных чисел* $\mathbb{R}$ можно описывать двумя способами: либо как *пополнение* поля $\mathbb{Q}$ (*сечениями Дедекинда* или *последовательностями Коши*), либо независимо от $\mathbb{Q}$ как множество *бесконечных десятичных дробей*. В любом случае определение операций в $\mathbb{R}$ и проверка выполнения аксиом поля требуют определенной работы, которой посвящены первые главы стандартного курса анализа. Я буду предполагать, что эта работа была проделана вами в школе. Я буду считать также, что вы умеете изображать действительные числа *геометрически* — как точки *ориентированной числовой прямой*.

В каждом из трёх подходов к определению поля $\mathbb{R}$ имеется конструкция, отождествляющая поле $\mathbb{Q}$ с некоторым подмножеством в поле $\mathbb{R}$ причём это отождествление согласовано с операциями, так что всё равно – вычислять с рациональными числами как с обыкновенными дробями (т.е. по стандартным правилам поля $\mathbb{Q}$), или же как с действительными числами (по правилам действий в поле $\mathbb{R}$).

1.5. Подполя и расширения. Подмножество k в поле K называется *подполем*, если оно удовлетворяет аксиомам поля относительно тех операций сложения и умножения, которые имеются в K. Это равносильно тому, что все четыре арифметических операции над элементами из k не выводят за пределы k. *Расширением поля* k называется любое поле K, содержащее k в качестве *подполя*.

Например, $\mathbb{R}$ есть расширение поля $\mathbb{Q}$. В алгебре и теории чисел часто возникают другие расширения поля $\mathbb{Q}$.

1.5.1. Пример: $\mathbb{Q}[\sqrt{2}] \stackrel{\text{def}}{=} \{a+b\sqrt{2} \mid \quad a,b \in \mathbb{Q}\}$. На совокупности чисел вида $a+b\sqrt{2}$ можно определить сложение и умножение, просто раскрывая скобки (с учётом того, что $(\sqrt{2})^2 = 2$):

$$\begin{aligned}(a+b\sqrt{2}) + (c+\sqrt{2}) &\stackrel{\text{def}}{=} (a+c)+(b+d)\sqrt{2}.\\ (a+b\sqrt{2})\cdot(c+d\sqrt{2}) &\stackrel{\text{def}}{=} (ac+2bd)+(cb+ad)\sqrt{2}\end{aligned}$$

Задача 1.4. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ – это поле.

Подсказка: Для нахождение обратного элемента надо *домножить на сопряженное*:

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

1.5.2. Расширения поля $\mathbb{Q}$, , обобщающие предыдущую конструкция, можно строить следующим образом. Рассмотрим множество $\mathbb{Q}[\vartheta]$ выражений вида

$$\mathbb{Q}[\vartheta] \stackrel{\text{def}}{=} \{\xi = x_0\vartheta^{n-1} + x_1\vartheta^{n-1-1} + \cdots + x_{n-1-1}\vartheta + x_{n-1} \mid \text{ все } x_\nu \in \mathbb{Q}\}$$

где ϑ удовлетворяет алгебраическому уравнению

$$A(\vartheta) = a_0\vartheta^n + a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n = 0$$

При помощи этого уравнения степени ϑ^m с $m \geq n$ можно заменять на меньшие точно также, как и в предыдущем примере:

$$\vartheta^m = -a_n^{-1}\vartheta^{m-n}(a_0\vartheta^{n-1} + a_1\vartheta^{n-1-1} + \cdots + a_{n-1-1}\vartheta + a_{n-1})$$

А это, как и выше, позволяет определить на совокупности чисел вида $\xi = x_0\vartheta^{n-1} + x_1\vartheta^{n-1-1} + \cdots + x_{n-1-1}\vartheta + x_{n-1}$ сложение и умножение, которые следует делать по обычным правилам раскрытия скобок и приведения подобных слагаемых, но заменяя все возникающие по ходу дела степени ϑ с показателями, большими $(n-1)$, на степени, показатель которых лежит в требуемых пределах от 0 до $(n-1)$.

Задача 1.5. Проверьте, что в $\mathbb{Q}[\vartheta]$ выполняются все аксиомы поля, кроме аксиомы существования обратного элемента 2г.

Видимая трудность, возникающая при проверке аксиомы 2г, — подыскать замену трюку «умножения на сопряжённое». То, что реально требуется от этого трюка, — это возможность для каждого выражения $X(\vartheta) = x_0\vartheta^{n-1} + x_1\vartheta^{n-1-1} + \cdots + x_{n-1-1}\vartheta + x_{n-1}$ подобрать другое выражение $\bar{X}(\vartheta) = \bar{x}_0\vartheta^{n-1} + \bar{x}_1\vartheta^{n-1-1} + \cdots + \bar{x}_{n-1-1}\vartheta + \bar{x}_{n-1}$, так чтобы

$$X(\vartheta)\cdot\bar{X}(\vartheta) = q + Y(\vartheta)\cdot A(\vartheta),$$

где $q \in \mathbb{Q}$ – рациональное число, а из правого слагаемого выносится $A(\vartheta)$, так что согласно правилам действий в $\mathbb{Q}[\vartheta]$ это слагаемое обратится в нуль (ибо $A(\vartheta) = 0$). Поэтому будем иметь:

$$\frac{1}{X(\vartheta)} = \frac{\bar{X}(\vartheta)}{X(\vartheta)\bar{X}(\vartheta)} = \frac{1}{q}\bar{X}(\vartheta) \in \mathbb{Q}[\vartheta]$$

В случае $\vartheta^2 = 2$ из n° 1.5.1 возможность для такого манёвра у нас была: если $X(\vartheta) = x_0 + x_1\vartheta$, то полагая $\bar{X}(\vartheta) = x_0 - x_1\vartheta$, получаем $X(\vartheta)\bar{X}(\vartheta) = x_0^2 - \vartheta^2 x_1^2 - x_1^2(\vartheta^2 - 2)$. Разумеется, такая возможность есть не всегда.

Задача 1.6. Докажите, что $\mathbb{Q}[\vartheta]$ с $\vartheta^2 + \vartheta + 1 = 0$ является полем, а $\mathbb{Q}[\zeta]$ с $\zeta^3 + 1 = 0$ – не является.

Указание: число $1 + \zeta \in \mathbb{Q}[\zeta]$ необратимо в $\mathbb{Q}[\zeta]$, а все числа $x_0 + x_1\vartheta$ (составляющие $\mathbb{Q}[\vartheta]$) обратимы в $\mathbb{Q}[\vartheta]$.

Задача 1.7. Каким должно быть соотношение $a_0\vartheta^n + a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n = 0$ для того, чтобы совокупность чисел $\mathbb{Q}[\vartheta]$ составляла поле?

Утешение. Это трудная задача, и если не получается, – не волнуйтесь: её исчерпывающее решение будет дано в следующих двух лекциях.

1.6. Поле «мнимых» чисел. Заметим, что для конструкции расширения $\mathbb{Q}[\vartheta]$ поля $\mathbb{Q}$ совершенно безразлично *наличие настоящего числа* $\vartheta \in \mathbb{R}$, удовлетворяющего уравнению $a_0\vartheta^n + a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n = 0$. Иными словами, мы можем воспринимать ϑ не как действительное число, а как формальную букву, а элементы $\mathbb{Q}[\vartheta]$ — как формальные слова, над которыми производятся формальные преобразования по некоторым правилам.

За примером далеко ходить не надо. Положим $\mathbb{M} = \mathbb{R}[i]$, где $i^2 + 1 = 0$. Иначе говоря, $\mathbb{M}$ есть множество записей вида $a + bi$ с *вещественными* a и b, которые складываются и перемножаются по обычным правилам с учетом равенства $i^2 = -1$:

$$(a+bi)+(c+di) \stackrel{\text{def}}{=} (a+c)+(b+d)i$$
$$(a+bi)(c+di) \stackrel{\text{def}}{=} (ac-bd)+(ad+bc)i$$

1.6.1. Предложение. $\mathbb{M}$ – *поле.*

Доказательство. Коммутативность, ассоциативность и дистрибутивность сложения и умножения почти очевидны (однако проверьте их обязательно!). Нуль есть число $0+0i$, единица есть $1+0i$ (проверьте!). Противоположным к $a+bi$ будет $-a-bi$, обратным —

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

Ясно, что $0 \neq 1$. Предложение доказано.

1.6.2. Замечание. Поля $\mathbb{Q}[\vartheta]$, где ϑ – «настоящие» числа типа $\sqrt{2}$, возникали еще в античных рассуждениях, которые происходили на геометрическом языке и не приводили к методологическим спорам, поскольку имели ясный геометрический смысл. Например, $\sqrt{5}$ – это гипотенуза прямоугольного треугольника со сторонами 1 и 2, а $\mathbb{Q}[\sqrt{5}]$ – это все отрезки, которые можно отложить, используя стороны этого треугольника и теорему Фалеса. Вычисления в поле $\mathbb{M} = \mathbb{R}[i]$ начали появляться в средние века при решении уравнений и имели несколько мистическую окраску, ибо необходимость прибегать к i с $i^2 = -1$ для того, чтобы найти вещественный корень кубического уравнения с рациональными коэффициентами напоминает «сделку с дьяволом». Подсознательный протест против описанной выше конструкции поля $\mathbb{M}$ возник, я думаю, и у многих из вас. Причина в том, что математические построения лишь тогда входят в сознание с абсолютной ясностью и вызывают внутреннее удовлетворение, когда за ними стоят геометрические образы. Поэтому наряду с формально-алгебраической конструкцией поля $\mathbb{M}$, которое мы временно назовём *полем мнимых чисел*, мы дадим сейчас наглядно-геометрическое построение поля *комплексных чисел* $\mathbb{C}$, восходящее к Гауссу, Риману и Клейну (XIX век). Впоследствии эти два поля будут отждествлены, и название и обозначение для первого из них (не являющиеся общеупотребительными) мы после n° 2.8.2 применять никогда не будем.

§2. Комплексные числа

2.1. Что такое комплексные числа. Фиксируем на плоскости ориентированную прямую OX с отмеченной *начальной точкой* O и будем интерпритировать её как *числовую прямую*, изображающую поле $\mathbb{R}$ действительных чисел. Каждой точке z плоскости сопоставим её *радиус-вектор* $\vec{Oz}$ (в частности, начальной точке сопоставим нулевой вектор $\vec{O}$). Далее мы не будем различать точки и их радиус-векторы, ибо из контекста всегда будет ясно, что имеется в виду под z: сама точка z или вектор $\vec{Oz}$. Оснащённая таким образом плоскость называется *комплексной плоскостью*, а точки этой плоскости (и их радиус-векторы) называются *комплексными числами*.

У каждого комплексного числа z (радиус-вектора $\vec{Oz}$) имеются две важные геометрические характеристики:

модуль $|z|$ — это длина вектора $\vec{Oz}$;

аргумент $\mathrm{Arg}(z)$ — это *ориентированный угол* луча $[Oz)$ с лучом $[OX)$.

Про ориентированный угол надо сказать особо. По определению, он равен ориентированной длине той дуги[2] единичной окружности с центром в O, по которой надо поворачивать луч $[OX)$, чтобы совместить его с лучём $[Oz)$ (длина берется со знаком «+» при движении против часовой стрелки, и с «−» – в противном случае). Видно, что такая дуга определена *не однозначно*, а с точностью до *любого целого числа оборотов*. Таким образом, Arg(z) не есть конкретное число, но целое счётное множество действительных чисел, составляющих арифметическую пргрессию с разностью 2π. Это записывают в виде

$$\mathrm{Arg}(z) = \varphi + 2\pi n,\ n \in \mathbb{Z}\ ,$$

где φ – одно из значений угла. В старину сказали бы, что $\mathrm{Arg}(z)$ есть *многозначная функция* от комплексного числа z.

2.2. Определение операций. Сложение и умножение радиусов-векторов определим правилами:

сложение: обычное сложение векторов на плоскости;

умножение: премножение модулей и одновременное сложение аргументов, так что

$$\begin{aligned} |z_1 \cdot z_2| &= |z_1||z_2| \\ \mathrm{Arg}(z_1 \cdot z_2) &= \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2)\ , \end{aligned}$$

Важно осознать, что для векторов, лежащих на действительной числовой прямой OX, эти правила определяют обычные действия с действительными числами (минус на минус дает плюс и т.п.). То, что такая геометрическая формулировка действий была придумана лишь в XIX веке ясно показывает, насколько трудно увидеть из одномерного мира, что этот мир есть срез двумерной геометрии.

2.3. Теорема. *Комплексные числа составляют поле.*

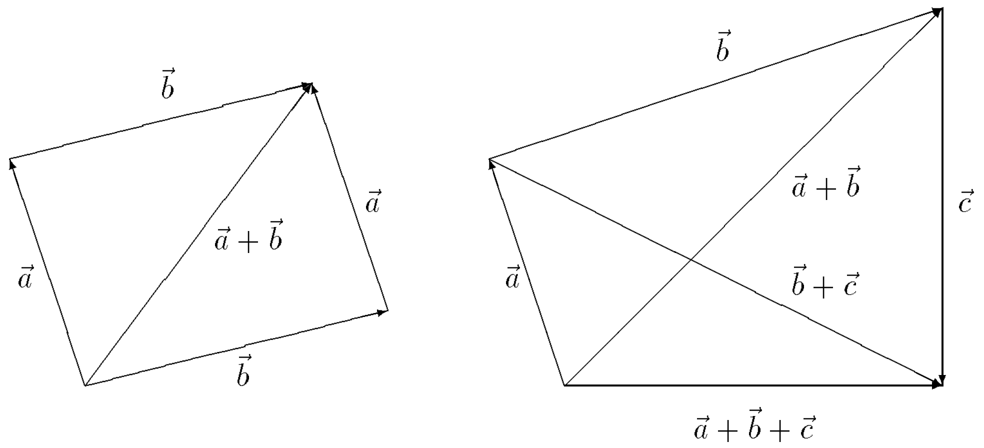

Рис. 1. Правило параллелограмма и правило треугольника

Доказательство. Аксиомы сложения хорошо известны из школьного курса геометрии как *правила сложения векторов*. Например, коммутативность есть не что иное, как *правило параллелограмма*, а ассоциативность следуют из *правила треугольника* (см. рис.рис.1). Коммутативность и ассоциативность умножения очевидны из определения. Единицей служит

[2] напомню, что длина дуги — это *действительным число*

единичный вектор $\overrightarrow{01}$, лежащий на действительной оси (ибо его модуль равен 1, а угол – 0). Очевидно, что $0 \neq 1$.

Обратным к числу z будет число z^{-1}, модуль которого равен $|z|^{-1}$, а аргумент равен $\mathrm{Arg}(z^{-1}) = -\mathrm{Arg}(z)$ (луч на котором лежит z^{-1} симметричен лучу на котором лежит z относительно действительной оси).

Для проверки дистрибутивности заметим, что преобразование плоскости, состоящее в умножении всех точек на фиксированное комплексное число a: $z \mapsto az$ суть композиция поворота на угол $\mathrm{Arg}(a)$ вокруг 0 и гомотетии с коэффициентом $|a|$ относительно 0 (всё равно в каком порядке). Такое преобразование называется *поворотной гомотетией*. Аксиома дистрибутивности утверждает, что всё равно: применить поворотную гомотетию к сумме векторов $\vec{b}+\vec{c}$, либо применить её отдельно к $\vec{b}$ и отдельно к $\vec{c}$, а затем сложить полученные векторы. Но это очевидно, ибо и при повороте и при гомотетии параллелограмм для вычисления суммы $\vec{b}+\vec{c}$ перейдет в точности в параллелограмм для вычисления суммы их образов. Теорема доказана.

□

Задача 1.8. Убедитесь, что преобразование плоскости $z \mapsto z^{-1}$ является композицией осевой симметрии относительно действительной прямой OX и инверсии относительно единичной окружности $|z| = 1$.

2.3.1. Раскрытие скобок. Неформальное следствие состоит в том, что с геометрическими комплексными числами можно вычислять по всем правилам школьной алгебры. В частности, справедливы «формулы сокращенного умножения», из которых нам будут особенно полезны следующие две.

Задача 1.9. Докажите, что в любом поле имеют место равенства:

$$\text{а)} \quad (a^m - b^m) : (a-b) = a^{m-1} + a^{m-2}b + a^{m-3}b^2 + \cdots + ab^{m-2} + b^{m-1}$$

$$\text{б)} \quad (a_1 + a_2 + \cdots + a_k)^n = \sum_{\nu_1+\ldots+\nu_k=n} \frac{n!}{\nu_1!\nu_2!\cdots\nu_k!} a_1^{\nu_1} a_2^{\nu_2} \cdots a_k^{\nu_k}$$

(суммирование производится по всем различным упорядоченным наборам неотрицательных целых чисел $(\nu_1, \nu_2, \ldots, \nu_k)$, сумма которых равна n).

Замечания к пункту (б):

1. Применительно к «любому полю» условие требует уточнения, поскольку коэффициент в правой части (б) – *натуральное число*. В произвольном поле этот коэффициент обозначает (по определению) сумму соответствующего количества *единиц этого поля*. В следующей лекции мы увидим, что это может отличаться от интуитивного представления о натуральном числе. Однако в поле комплексных чисел мы получим *настоящее натуральное число*, которое можно воспринимать как натуальную точку действительной прямой.

2. Определение коэффициента при $a_1^{\nu_1} a_2^{\nu_2} \cdots a_k^{\nu_k}$ тесно связано с комбинаторной задачей подсчета количества всевозможных слов , которые можно составить из n букв, из которых ν_1 штук букв a_1, ν_2 штук букв a_2, … , ν_k штук букв a_k. Прежде, чем выводить общую формулу, потренируйтесь, подсчитав, сколько слов (не обязательно осмысленных) можно получить, переставляя буквы в словах: рок, урок, шнурок, курок, колобок (хорошая идея — выписывать слова подряд по алфавиту).

2.4. Алгебраическая запись формул. Для алгебраической записи векторов на комплексной плоскости удобно ввести прямоугольные координаты OXY, ось OX которых совпадает с действительной прямой. Базисные векторы осей OX и OY обозначаются $\vec{1}$ и $\vec{\imath}$ (напомню, что $\vec{1}$ есть единица поля $\mathbb{C}$ (см.рис.рис.2)).

Произвольный вектор z имеет координаты: (x, y) – проекции точки z на оси. Таким образом вектор $\overrightarrow{Oz}$ может быть выражен через базисные векторы $\vec{1}$ и $\vec{\imath}$ в виде

$$\overrightarrow{0z} = x \cdot \vec{1} + y \cdot \vec{\imath}.$$

Поскольку умножение вектора на плоскости на вещественное число совпадает (как легко видеть) с умножением этого вектора как комплексного числа на то же вещественное число, но уже рассматриваемое как комплексное, предыдущая формула представляет собой *соотношение в поле* $\mathbb{C}$. Обычно его записывают не столь помпезно как выше, а в виде:

$$z = x + yi,$$

опуская стрелку над i и $\vec{1}$ (т.к. умножение на единицу поля вообще принято опускать). Эта запись называется *алгебраическим представлением* комплексного числа z и черезвычайно удобна, поскольку по теореме Теор.2.3 и следствию зад.1.9 мы вольны в вычислениях с такими записями пользоваться всем арсеналом школьных тождеств. Важно отметить, что действительные числа x и y в представлении $z = x+yi$ *однозначно* определяются по z (как координаты). Они обозначаются $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$ и называются *действительной и мнимой частью* числа z. Если $\mathrm{Arg}(z) = \varphi$, то имеют место очевидные формулы:

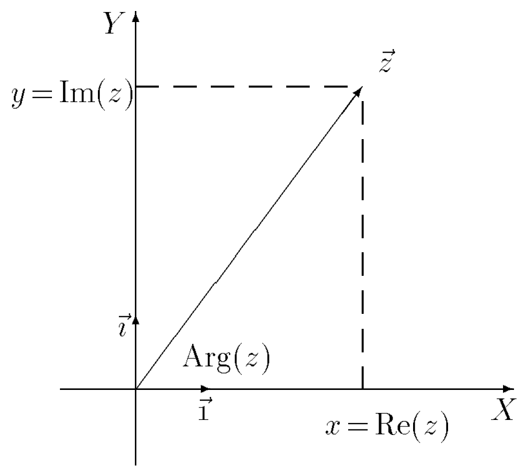

Рис. 2. Координаты на $\mathbb{C}$

$$x = |z|\cos(\varphi) \quad y = |z|\sin(\varphi)$$

$$|z| = \sqrt{x^2 + y^2} \quad \mathrm{Arg}(z) = \arccos\left(x/\sqrt{x^2+y^2}\right) + 2\pi n = \arcsin\left(y/\sqrt{x^2+y^2}\right) + 2\pi n$$

Итак, всякий $z \in \mathbb{C}$ представляется в виде

$$z = x + iy = |z|(\cos\varphi + i\sin\varphi),$$

и эти выражения суть алгебраические равенства в поле $\mathbb{C}$, с которым мы можем вычислять пользуясь правилами раскрытия скобок, тождествами сокращённого умножения и т.п.

2.5. Примеры вычислений с комплексными числами. Комплексные числа являются удивительно гибким и могучим инструментом практически во всех областях естествознания. Причина в том, что при вычислениях с комплексными числами одинаково хорошо работают оба математических языка – и алгебраический язык формул, и геометрический язык картинок.

2.5.1. Корни из -1. Прямо из определения умножения получаем: $i^2 = i \cdot i = -1$ (т.к. $\mathrm{Arg}(i^2) = 2 \cdot \pi/2 = \pi$ и $|i^2| = 1$. Поэтому имеем разложение $z^2 + 1 = (z+i)(z-i)$, из которого следует, что уравнение $z^2 + 1 = 0$ имеет в поле $\mathbb{C}$ два корня: i и $-i$.

Задача 1.10. Докажите, что в произвольном поле уравнение

$$(x-a_1)(x-a_2)\cdots(x-a_k)=0$$

имеет ровно k корней $\qquad x=a_1,\ \ldots,a_k.$

2.5.2. Основные тригонометрическин тождества. Пусть z_1 и z_2 – два числа, лежащие на единичной окружности: $|z_1|=|z_2|=1$. Тогда $z_1=\cos\varphi_1+i\sin\varphi_1$ и $z_2=\cos\varphi_2+i\sin\varphi_2$. По определению умножения, $|z_1z_2|=1$ и $\operatorname{Arg}(z_1z_2)=\varphi_1+\varphi_2$, то есть

$$z_1z_2=\cos(\varphi_1+\varphi_2)+i\sin(\varphi_1+\varphi_2)$$

С другой стороны, из дистрибутивности получаем

$$\begin{aligned} z_1z_2 &= (\cos\varphi_1+i\sin\varphi_1)(\cos\varphi_2+i\sin\varphi_2)= \\ &= \Big(\cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2\Big)+i\Big(\cos\varphi_1\sin\varphi_2+\sin\varphi_1\cos\varphi_2\Big) \end{aligned}$$

(мы воспользовались тем, что $i^2=-1$). Сравнивая действительные и мнимые части, немедленно получаем основные тригонометрические тождества:

$$\begin{aligned} \cos(\varphi_1+\varphi_2) &= \cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2 \\ \sin(\varphi_1+\varphi_2) &= \cos\varphi_1\sin\varphi_2+\sin\varphi_1\cos\varphi_2 \end{aligned}$$

Это рассуждение наводит на мысль, что всё казуистическое изобилие формул школьной тригонометрии есть лишь бесформенная тень от стройного сооружения, построенного по простым правилам — аксиомам поля, выполненным в поле комплексных чисел $\mathbb{C}$.

2.5.3. Кратные углы. Пусть $|z|=1$ и $z=\cos\varphi+i\sin\varphi$. Тогда по определению: $z^n=\cos(n\varphi)+i\sin(n\varphi)$. С другой стороны, по формуле бинома (которая получается из п.(б) зад.1.9 при $k=2$, когда коэффициенты при $a_1^{\nu_1}a_2^{\nu_2}=a_1^{\nu}a_2^{n-\nu}$ принимают вид $\frac{n!}{\nu!(n-\nu)!}$ и обозначаются $\binom{n}{\nu}$ или C_n^k; они называются *биномиальными коэффициентами*) имеем:

$$\begin{aligned} & z^n=(\cos\varphi+i\sin\varphi)^n= \\ &= \cos^n\varphi+i\binom{n}{1}\cos^{n-1}\varphi\sin\varphi-\binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi-i\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi+\cdots= \\ &= \left[\binom{n}{0}\cos^n\varphi-\binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi+\binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi-\cdots\right]+ \\ &\qquad +i\cdot\left[\binom{n}{1}\cos^{n-1}\varphi\sin\varphi-\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi+\binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi-\cdots\right] \end{aligned}$$

Отсюда получаем формулы для кратных углов:

$$\begin{aligned} \cos(n\varphi) &= \binom{n}{0}\cos^n\varphi-\binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi+\binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi-\cdots \\ \sin(n\varphi) &= \binom{n}{1}\cos^{n-1}\varphi\sin\varphi-\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi+\binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi-\cdots \end{aligned}$$

Задача 1.11. Докажите, что при нечётном n функция $\sin(n\varphi)/\sin\varphi$ является многочленом от $\sin^2\varphi$ и найдите его степень, корни и старший коэффициент. Выпишите этот многочлен явно для $n=3$ и $n=5$.

Задача 1.12. Докажите для нечётных n тождество:

$$\frac{\sin(n\varphi)}{\sin\varphi} = (-4)^{\frac{n-1}{2}} \prod_{\nu=1}^{\frac{n-1}{2}} \left(\sin^2\varphi - \sin^2\frac{2\pi\nu}{n}\right)$$

Задача 1.13. В единичную окружность с ценром в начале координат вписан правильный m-угольник (m – нечётно) так, что одна из вершин находится в точке (1,0). Многоугольник поворачивают на угол φ вокруг начала координат против часовой стрелки. Вычислите произведение ординат вершин повернутого многоугольника.

2.6. Уравнение деления круга. Решим в поле $\mathbb{C}$ так называемое *уравнеие деления круга на n частей*: $z^n = 1$. Оно раносильно двум геометрическим соотношениям на вектор z: $|z|^n = 1$ и $n\text{Arg}(z) = 0 + 2\pi k$ (где $k \in \mathbb{Z}$ — любое). Отсюда получаем ровно n различных корней, располагающихся на единичной окружности в вершинах правильного n-угольника (см.рис. рис.3 для $n = 5$):

$$|z_\nu| = 1, \quad \text{Arg}(z_\nu) = 2\pi\nu/n, \text{ где } \nu = 0, 1, \ldots, (n-1)$$

Задача 1.14. Выразите $\cos 36°$ и $\sin 36°$ в радикалах.
Указание: после деления обеих частей на $z - 1$, уравнение $z^5 - 1 = 0$ становится *возвратным* и сводится к квадратному подстановкой $t = z + 1/z$.

2.7. Гомоморфизмы. Предыдущие вычисления показывают, что геометрическое поле комплексных чисел $\mathbb{C}$ «ничем не отличается» от формального поля мнимых чисел $\mathbb{M}$, веденного в n° 1.6. Для придания точного смысла фразе «ничем не отличается» придумано понятие гомоморфизма. Для сравнения множеств обычно используют их отображения друг в друга. Если множества имеют какую-либо алгебраическую структуру, то рассматривают не любые отображения, а только отображения, сохраняющие эту структуру. Такие отображения называют *гомоморфизмами*. В случае полей точное определение звучит так:

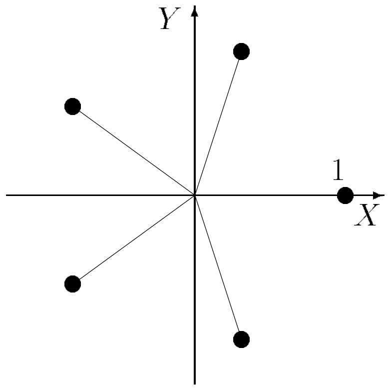

Рис. 3. Корни уравнения $z^5 = 1$

2.8. Определение. *Отображение полей $\sigma\colon K \longrightarrow L$ называется **гомоморфизмом**, если $\forall a, b \in K$ в поле L выполняются соотношения*

$$\begin{aligned} \sigma(a+b) &= \sigma(a) + \sigma(b) \\ \sigma(ab) &= \sigma(a)\sigma(b) \end{aligned}$$

Оказывается, требование совместимости с алгебраической структурой накладывает на отображение очень жёсткие ограничения.

2.8.1. Предложение. *Для любого гомоморфизма полей $\sigma\colon K \longrightarrow L$ обязательно выполнены следующие свойства:*

а) $\sigma(0) = 0$
б) $\sigma(1) = 1$, *если только* $\sigma(K) \neq \{0\}$
в) $\sigma(a-b) = \sigma(a) - \sigma(b)$ $\forall a, b \in K$
г) $\sigma(a/b) = \sigma(a)/\sigma(b)$, *если только* $b \neq 0$ *и* $\sigma(K) \neq \{0\}$

Более того: либо $\sigma(K) = \{0\}$, либо σ — вложение (то есть переводит разные элементы из K в разные элементы из L)

Терминологическое замечаеие. Гомоморфизм, переводщий всё поле K в нуль поля L, называется *тривиальным*, или *нулнвым*. Гомоморфизм, являющийся одновременно вложением, называется *инъективным* или *мономорфизмом*. Гомоморфизм, являющийся взаимнооднозначным, называется *изоморфизмом*.

Доказательство. (а): $\forall a \in K$ имеем

$$\sigma(a) = \sigma(a+0) = \sigma(a) + \sigma(0)\ .$$

Вычитая из левой и правой частей этого равенства $\sigma(a)$, получим $\sigma(0) = 0$.
(б): аналогично, только надо выбрать a так, чтобы $\sigma(a) \neq 0$ (т.е. был обратим).
(в): вычтем из левой и правой частей равенства $\sigma(a-b) + \sigma(b) = \sigma(a-b+b) = \sigma(a)$ число $\sigma(b)$.
(г): аналогично в).

Наконец, для доказательства последнего утверждения допустим, что σ не является вложением. Тогда найдутся $b, c \in K$ такие, что $b \neq c$ и $\sigma(b) = \sigma(c)$. Т.к. $d = b - c \neq 0$, оно обратимо в K. Но $\sigma(d) = \sigma(b) - \sigma(c) = 0$, и поэтому $\forall a \in K$ имеем $\sigma(a) = \sigma(add^{-1}) = \sigma(a)\sigma(d)\sigma(d^{-1}) = 0$. Таким образом, $\sigma(K) = \{0\}$ и σ тривиален. Предложение доказано.

2.8.2. Пример. Поле комплексных чисел $\mathbb{C}$ изоморфно полю мнимых чисел $\mathbb{M}$. Изоморфизм задаётся сопоставлением числу $\alpha + i\beta \in \mathbb{R}[i] = \mathbb{M}$ вектора с координатами (α, β) на комплексной плоскости $\mathbb{C}$. Мы отождествим $\mathbb{C}$ с $\mathbb{M}$ посредством этого изоморфизма и далее не будем их различать (и пользоваться обозначением $\mathbb{M}$).

2.8.3. Пример. Имеется ровно один нетождественный изоморфизм поля $\mathbb{C}$ на себя, сохраняющий неподвижным вещественное подполе $\mathbb{R} \subset \mathbb{C}$. Он переводит $z = x + iy$ в $\bar{z} = x - iy$ и называется *комплексным сопряжением*. Действительно, если $\mathbb{R}$ неподвижно, то $\sigma(x+iy) = x + y\sigma(i)$, и σ однозначно определяется заданием $\sigma(i)$. Поскольку $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, значение $\sigma(i)$ есть корень уравнения $t^2 = -1$. У этого уравнения в поле $\mathbb{C}$ имеется ровно два корня: i и $-i$. Тем самым, если нетривиальный гомомрфизм существует, то он совпадает с комплексным сопряжением. Остаётся проверить, что отображение $z \mapsto \bar{z}$ и в самом деле гомомрфизм.

Задача 1.15. Сделайте это.

2.8.4. Замечание. Интуитивно, последнее утверждение в предложении из Пр.2.8.1 означает, что два поля K и L либо вообще «несравнимы» (то есть между ними нет нетривиальных гомоморфизмов), либо одно из них можно отождествить с подполем в другом. Важно отметить, что отождествить поле K с подполем в L можно, как правило, многими разными способами.

2.8.5. Пример. Имеется ровно два вложения поля $\mathbb{Q}[\sqrt{2}]$ в поле $\mathbb{C}$. Образ обоих содержится в вещественном подполе $\mathbb{R} \subset \mathbb{C}$. Первое — тождественно, а второе переводит $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ в $a - b\sqrt{2} \in \mathbb{R} \subset \mathbb{C}$. Действительно, пусть $\sigma\colon \mathbb{Q}[\sqrt{2}] \hookrightarrow \mathbb{C}$ — вложение. Тогда $\sigma(a + b\sqrt{2}) = a + b\sigma(\sqrt{2})$ (ибо при $k \in \mathbb{N}$, $k = \underbrace{1 + 1 + \ldots + 1}_{k\ \text{раз}}$ имеем $\sigma(k) = k\sigma(1) = k$, а значит и для любого рационального $a = p/q$ получим $\sigma(a) = \sigma(p)/\sigma(q) = p/q = a$). Тем самым, σ однозначно определяется значением $\sigma(\sqrt{2})$. Но $\sigma(\sqrt{2}) \in \mathbb{C}$ обязан быть корнем уравнения $z^2 = 2$ (почему?), а у такого уравнения в поле $\mathbb{C}$ ровно два корня: $\sqrt{2}$ и $-\sqrt{2}$. Поэтому имеется ровно две возможности: $\sigma(\sqrt{2}) = \sqrt{2}$ и $\sigma(\sqrt{2}) = -\sqrt{2}$.

Задача 1.16. Докажите, что поле $\mathbb{Q}[\vartheta]$ (где $\vartheta^2 + \vartheta + 1 = 0$) допускает ровно два вложения в поле $\mathbb{C}$. При одном из них ϑ переходит в $(-1 + i\sqrt{3})/2$, при другом — в $(-1 - i\sqrt{3})/2$.

Задача 1.17. Докажите, что поле $\mathbb{Q}[\vartheta]$ (где $\vartheta^3 + \vartheta + 1 = 0$) допускает три вложения в $\mathbb{C}$. Образ одного из них содержится в $\mathbb{R}$, а образы двух других — комплексно сопряжены.