§6. Коммутативные кольца и поля. Комплексные числа.

6.1. Коммутативная и некоммутативная алгебра. Своё знакомство с алгеброй мы начали с формул и структур, относившихся к отображениям множеств. С известной долей условности эту часть алгебры можно назвать *некоммутативной алгеброй*, поскольку основная операция, которая в ней используется — композиция отображений — некоммутативна. В этом разделе мы познакомимся с *коммутативной алгеброй* — формулами и структурами, главными действующими лицами в которых являются объекты типа чисел и числовых функций, которые можно складывать и перемножать друг с другом так, что обе эти операции коммутативны. Простейшие алгебраические структуры, аксиоматизирующие свойства чисел и числовых функций — это коммутативные кольца и поля. Примерами полей являются числовые поля $\mathbb{Q}$ и $\mathbb{R}$, а примерами коммутативных колец — целые числа $\mathbb{Z}$, а также многочлены $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ и $\mathbb{R}[x]$ с целыми, рациональными и вещественными коэффициентами.

Оговоримся, что деление алгебры на «коммутативную» и «некоммутативную» довольно искусственно. Мы уже видели в примере (n° 4.4.3), что числовые группы можно воспринимать как группы преобразований числовой прямой. Важнейшим источником информации о коммутативных кольцах и полях являются сохраняющие операции отображения между ними (*гомоморфизмы*), которые сами по себе живут в некоммутативном мире. С другой стороны, представление какой-нибудь группы преобразований как группы автоморфизмов некоторой коммутативной алгебраической структуры часто позволяет увидеть такие свойства этой группы, которые были совершенно не очевидны при другом её представлении. Так что коммутативный и некоммутативный миры тесно переплетаются друг с другом.

Следующее далее определение формализуют стандартные свойства сложения и умножения чисел.

6.2. Определение поля. Множество $\mathbb{F}$ называется *полем*, если на нём заданы две операции

$$\mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} \ :$$

сложение $(a, b) \longmapsto a + b$ и умножение $(a, b) \longmapsto ab$ со свойствами:

1) аксиомы сложения
   - а) коммутативность (переместительный закон): $a + b = b + a \quad \forall\, a, b \in \mathbb{F}$
   - б) ассоциативность (сочетательный закон): $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in \mathbb{F}$
   - в) существование нейтрального элемента (нуля): $\exists\, 0 \in \mathbb{F} : \quad a + 0 = a \quad \forall\, a \in \mathbb{F}$
   - г) существование противоположного: $\forall\, a \in \mathbb{F} \quad \exists\, (-a) \in \mathbb{F} : \quad a + (-a) = 0$
2) аксиомы умножения
   - а) коммутативность: $ab = ba \quad \forall\, a, b \in \mathbb{F}$
   - б) ассоциативность: $a(bc) = (ab)c \quad \forall\, a, b, c \in \mathbb{F}$
   - в) существование нейтрального элемента (единицы): $\exists\, 1 \in \mathbb{F} : \quad a \cdot 1 = a \quad \forall\, a \in \mathbb{F}$
   - г) существование обратного: $\forall\, a \in \mathbb{F},\ a \neq 0 \quad \exists\, a^{-1} \in \mathbb{F} : \quad a \cdot a^{-1} = 1$
3) аксиома дистрибутивности (распределительный закон): $a(b + c) = ab + ac \quad \forall\, a, b \in \mathbb{F}$
4) аксиома нетривиальности: $0 \neq 1$

Первые два набора аксиом утверждают, что всё поле $\mathbb{F}$ является абелевой группой относительно сложения[1], а множество $\mathbb{F}^* \overset{\text{def}}{=} \mathbb{F} \smallsetminus \{0\}$ всех ненулевых элементов поля $\mathbb{F}$ представляет собою

[1] групповая структура, операцией в которой является сложение, называется *аддитивной* групповой структурой; единицей аддитивной группы служит элемент 0 (в аддитвной структуре он называется *нейтральным элементом*), аддитвно обратные элементы называются *противоположными*; новые названия необходимы для того, чтобы отличать аддитивную групповую структуру от *мультипликативной* групповой структуры, операцией в которой служит умножение; стандартные названия из теории групп («единица», «обратный элемент») используются для мультипликативной групповой структуры

абелеву группу относительно умножения. Последние две аксиомы регулируют взаимодействие этих двух структур между собой. Как мы уже видели в (n° 4.3), из аксиом группы вытекает, что единица и нуль единственны, а противоположный и обратный элементы $-a$ и a^{-1} к данному элементу $a \in \mathbb{F}$ однозначно определяются по a.

Из аксиом поля автоматически следуют и некоторые другие интуитивно ожидаемые свойства действий.

Упражнение 6.1. Покажите, что в любом поле $\mathbb{F}$ для любого $a \in \mathbb{F}$ выполняются равенства $0 \cdot a = 0$ и $(-1) \cdot a = (-a)$ (последнее означает, что умножая a на число, противоположное единице, мы получим число противоположное a, чего *a priori* не требовалось; решение можно подглядеть в сноске ([1])).

Отметим, что требование $a \neq 0$ в аксиоме (2г) необходимо, поскольку иначе мы имели бы $1 = 0 \cdot 0^{-1} = 0$, что противоречит последней аксиоме[2].

Простейшим полем является поле $\mathbb{F}_2$, состоящее из двух элементов 0 и 1, таких что $0 + 1 = 1 \cdot 1 = 1$, а все остальные суммы и произведения равны нулю (включая $1 + 1 = 0$). Элементы этого поля можно интерпретировать как «ложь» и «истину», после чего сложение и умножение превращаются, соответственно, в логические операции «исключающее или» и «и». Таким образом, формулы и вычисления в поле $\mathbb{F}_2$ — это то, что называется «алгеброй высказываний».

Упражнение 6.2. Проверьте, что $\mathbb{F}_2$ действительно является полем и напишите многочлен от x, равный «не x», а также многочлен от x и y, равный «x или[3] y».

Примером поля, послужившим первоисточником для введения этого понятия, является поле рациональных чисел $\mathbb{Q}$, которое можно определить как множество классов эквивалентности выражений вида p/q с $p, q \in \mathbb{Z}$ и $q \neq 0$, где два выражения p/q и r/s считаются эквивалентными тогда и только тогда, когда $ps = qr$ в $\mathbb{Z}$. Сложение и умножение классов определяется формулами

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}\,, \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \tag{6-1}$$

Упражнение 6.3. Проверьте, что эти определения корректны (не зависят от выбора представителей в классе эквивалентных дробей) и удовлетворяют аксиомам поля.

Более сложным примером поля является поле действительных чисел $\mathbb{R}$. У множества $\mathbb{R}$ имеется несколько различных определений[4]. Мы будем предполагать, что читатель знаком с этими определениями и понимает, почему они эквивалентны друг другу. Отметим, что какое бы из определений множества $\mathbb{R}$ не использовалось, задание на $\mathbb{R}$ операций сложения и умножения требует достаточно серьёзной работы, и проверка выполнения аксиом поля для этих двух операций составляет стандартный набор теорем из начального курса анализа. Мы полагаем, что читатель знает эти теоремы.

6.3. Поле комплексных чисел (геометрическое определение). Рассмотрим вещественную координатную плоскость $\mathbb{R}^2$ с фиксированной прямоугольной системой координат OXY с началом в точке $O = (0, 0)$ и координатными осями OX и OY, направленными вдоль векторов $(1, 0)$ и $(0, 1)$, которые мы будем обозначать символами 1 И i (см. рис. 6◇1). Точки z этой плоскости мы будем называть *комплексными числами*, а саму плоскость обозначим через $\mathbb{C}$.

Координаты (x, y) комплексного числа z обозначаются через $\mathrm{Re}\,(z) = x$, $\mathrm{Im}\,(z) = y$ и называются *действительной* и *мнимой* частями комплексного числа. Каждому комплексному числу z можно сопоставить его *радиус-вектор* $x \cdot 1 + y \cdot i$ — это вектор с началом в точке O и концом

---

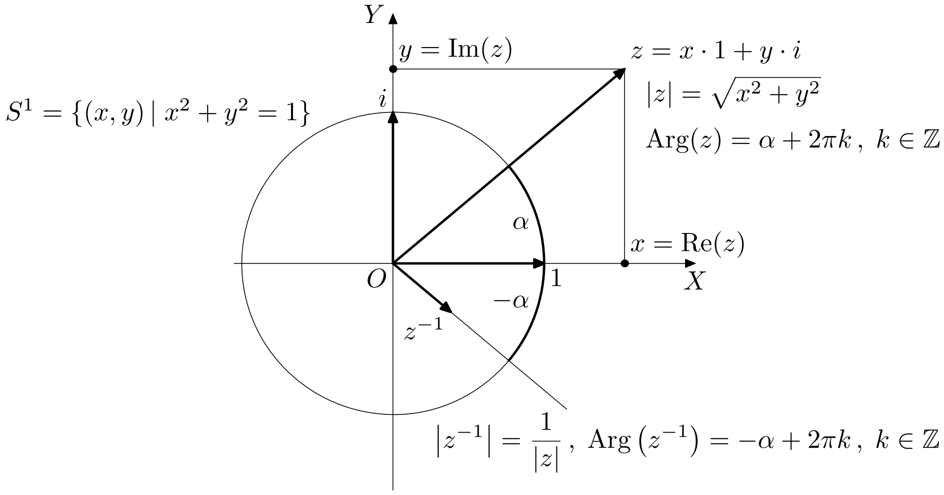
[1] РЕШЕНИЕ: обозначая $a \cdot 0$ через b, будем иметь $b + a = a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a(0 + 1) = a \cdot 1 = a$; прибавляя к обеим частям этого равенства $(-a)$, получаем $b = 0$; наконец, $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0$, откуда $(-1) \cdot a = -a$

[2] на самом деле аксиома (4) равносильна требованию $\mathbb{F} \neq \{0\}$: при $0 = 1$ мы имели бы $\forall a \in \mathbb{F}\;\; a = a \cdot 1 = a \cdot 0 = 0$

[3] здесь имеется в виде «не исключающее или», т. е. многочлен должен принимать значение 1 тогда и только тогда, когда *хотя бы одна* из переменных равна 1

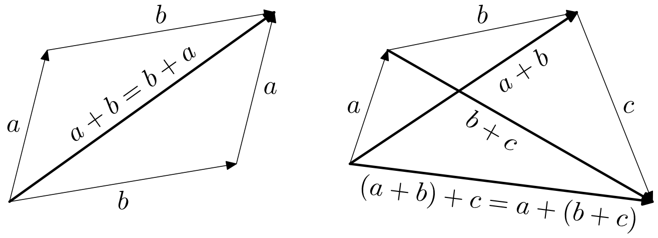
[4] три наиболее употребительных: множество классов эквивалентности десятичных (или привязанных к любой другой позиционной системе счисления, например, двоичных) дробей, множество дедекиндовых сечений множества $\mathbb{Q}$, а также множество классов эквивалентности рациональных последовательностей Коши

в точке z, который мы будем обозначать тем же символом z, что и саму точку. Точке $O = (0,0)$ при этом сопоставляется нулевой вектор 0.



6◇1. Атрибуты комплексного числа $z = x \cdot 1 + y \cdot i$.

Каждый радиус-вектор $z = x\cdot 1 + y\cdot i$ имеет длину $|z| = \sqrt{x^2+y^2}$, также называемую *модулем* числа z, и *аргумент* $\mathrm{Arg}\,(z) \overset{\text{def}}{=} \{\alpha + 2\pi k \mid k \in \mathbb{Z}\} \subset \mathbb{R}$, представляющий собою множество всех углов[1], поворот на которые совмещает направление оси OX с направлением радиус-вектора z (все такие углы отличаются на целое число полных оборотов и образуют смежный класс подгруппы $2\pi\mathbb{Z} \subset \mathbb{R}$ из примера (n° 5.1.6)).



6◇2. Коммутативность и ассоциативность сложения векторов.

Сложение комплексных чисел определяется как сложение отвечающих им радиус-векторов: суммой двух точек z_1 и z_2 называется точка, радиус вектор которой равен сумме $z_1 + z_2$ радиус-векторов точек z_1 и z_2. В координатах это описывается формулой

$$(x_1 \cdot 1 + y_1 \cdot i) + (x_2 \cdot 1 + y_2 \cdot i) = (x_1 + x_2) \cdot 1 + (y_1 + y_2) \cdot i\,.$$

Сложение векторов, как известно, коммутативно и ассоциативно (см. рис. 6◇2), обладает нейтральным элементом $z = 0$, и у всякого вектора есть противоположный. Таким образом, комплексные числа образуют абелеву группу относительно сложения.

[1] напомним, что углы в математике измеряются действительными числами (ср. с примером (n° 5.1.6)), а именно *ориентированный угол* луча OZ с осью OX по определению равен длине пути, который надо пройти по единичной окружности с центром в O от точки её пересечения с лучём OX до точки её пересечения с лучём OZ, причём длина берется со знаком «+», если движение происходит против часовой стрелки, и со знаком «−», если по часовой стрелке; существенно, что такая дуга *не единственна* — она определена с точностью до *любого целого числа оборотов*; поэтому угол не есть конкретное число, но целое счётное множество действительных чисел, составляющих арифметическую прогрессию с разностью 2π; множество всех этих чисел принято обозначать $\mathrm{Arg}\,(\measuredangle XOZ) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}$, где α — какое-то одно из значений угла, и называть *аргументом* луча OZ (в старину сказали бы, что аргумент является *многозначной функцией* от луча OZ, а сейчас мы говорим, что это смежный класс ядра универсального накрытия единичной окружности числовою прямою, описанного в примере (n° 5.1.6))

Произведением комплексных чисел z_1 и z_2 называется число $z_1 z_2$, радиус-вектор которого задаётся условиями

$$|z_1 z_2| \stackrel{\text{def}}{=} |z_1| \cdot |z_2| \,, \quad \operatorname{Arg}(z_1 z_2) \stackrel{\text{def}}{=} \operatorname{Arg}(z_1) + \operatorname{Arg}(z_2) \tag{6-2}$$

(иными словами, при умножении комплексных чисел их модули перемножаются, а аргументы складываются). Это умножение очевидно коммутативно и ассоциативно. Единичным элементом для него является число $1 \in \mathbb{C}$ (единичный направляющий вектор оси OX), а умножение на нулевой вектор обладает свойством $0 \cdot z = 0 \quad \forall z \in \mathbb{C}$. Обратным к ненулевому элементу z является число z^{-1} с

$$|z^{-1}| = 1/|z| \,, \quad \operatorname{Arg}(z^{-1}) = -\operatorname{Arg}(z) \tag{6-3}$$

(см. рис. 6◇1). Таким образом, относительно умножения ненулевые комплексные числа также образуют коммутативную группу.

Левое регулярное представление мультипликативной группы комплексных чисел (см. n° 4.4.1) имеет простую геометрическую интерпретацию: умножение на фиксированное число $a \in \mathbb{C}$

$$\lambda_a : \mathbb{C} \xrightarrow{z \mapsto az} \mathbb{C}$$

представляет собою *поворотную гомотетию*[1] плоскости $\mathbb{C}$ относительно начала координат на угол $\operatorname{Arg}(a)$ с коэффициентом $|a|$. Таким образом устанавливается биекция между отличными от нуля точками $a \in \mathbb{C}$ и поворотными гомотетиями относительно начала координат с ненулевым коэффициентом. Эта биекция является изоморфизмом мультипликативных групп — композиция поворотных гомотетий λ_a и λ_b это в точности поворотная гомотетия λ_{ab} (где под ab понимается произведение комплексных чисел, вычисленное по формуле (6-2)) с коэффициентом $|a||b|$ на угол $\operatorname{Arg}(a) + \operatorname{Arg}(b)$.

6.3.1. ПРЕДЛОЖЕНИЕ. *Комплексные числа образуют поле.*

Доказательство. Из всех свойств поля нам осталось проверить только дистрибутивность (3). На геометрическом языке формула $a(b+c) = ab + ac$ переписывается как $\lambda_a(b+c) = \lambda_a(b) + \lambda_a(c)$ и означает, что поворотные гомотетии перестановочны со сложением векторов, или — что то же самое — что любая поворотная гомотетия λ_a переводит параллелограмм в параллелограмм. Но это действительно так, поскольку всякий поворот и всякая гомотетия переводят параллелограмм в параллелограмм. □

6.3.2. Алгебраическое представление комплексных чисел. Прежде всего заметим, что ось OX в поле $\mathbb{C}$ можно отождествить с полем вещественных чисел $\mathbb{R}$ — сложение и умножение комплексных чисел, лежащих на оси OX, в точности совпадает со сложением и умножением чисел вещественной числовой прямой. Поэтому разложение $z = x \cdot 1 + y \cdot i$ радиус-вектора z по базисным векторам $1 = (1,0)$ и $i = (0,1)$ с вещественными коэффициентами $x = \operatorname{Re}(z)$ и $y = \operatorname{Im}(z)$ является *верным равенством в поле* $\mathbb{C}$ — сложение и умножение в этой формуле могут восприниматься как сложение и умножение комплексных чисел. Следуя обычной традиции опускать знаки произведений и умножение на единицу, формулу $z = x \cdot 1 + y \cdot i$ обычно сокращают до $z = x + iy$.

Пользуясь аксиомой дистрибутивности и равенством $i^2 = -1$, мы можем вычислить произведение комплексных чисел $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$, изначально определённое нами геометрически формулой (6-2), по обычным правилам раскрытия скобок:

$$z_1 z_2 = (x_1 + iy_1)(x_2 + iy_2) = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1) \,. \tag{6-4}$$

Обратное к числу $z = x + iy$ число z^{-1} так же легко выражается через x и y:

$$z^{-1} = \frac{1}{x+iy} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x-iy}{x^2+y^2} = \frac{x}{|z|^2} - \frac{iy}{|z|^2} \,, \tag{6-5}$$

[1] напомним, что *поворотной гомотетией* относительно точки O на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки O и растяжения в ϱ раз относительно O (поскольку растяжения коммутируют с поворотами, всё равно, в каком порядке эта композиция выполняется)

откуда $\mathrm{Re}\,\left(z^{-1}\right)=\mathrm{Re}\,(z)/|z|^2$ и $\mathrm{Im}\,\left(z^{-1}\right)=-\mathrm{Im}\,(z)/|z|^2$. Число $\overline{z}\overset{\text{def}}{=}x-iy$ называется *комплексно сопряжённым* к числу $z=x+iy$. В терминах комплексного сопряжения формулу для обратного числа можно записать в виде $z^{-1}=\overline{z}/|z|^2$. Геометрически, комплексное сопряжение

$$\mathbb{C}\xrightarrow{z\mapsto\overline{z}}\mathbb{C}$$

представляет собою симметрию комплексной плоскости относительно вещественной оси OX. С алгебраической точки зрения сопряжение является инволютивным автоморфизмом поля $\mathbb{C}$, т. е. $\forall\, z\in\mathbb{C}$ $\overline{\overline{z}}=z$ и $\forall\, z_1,z_2\in\mathbb{C}$ $\overline{z_1+z_2}=\overline{z}_1+\overline{z}_2$, $\overline{z_1z_2}=\overline{z}_1\overline{z}_2$.

6.3.3. Пример: тригонометрия. Рассмотрим комплексные числа

$$z_1=\cos\varphi_1+i\sin\varphi_1\ ,\quad z_2=\cos\varphi_2+i\sin\varphi_2\ ,$$

лежащие на единичной окружности $S^1=\{z\,:\,|z|=1\}$. Тогда произведение z_1z_2 , вычисленное по формуле (6-2) и вычисленное по формуле (6-4) , имеют вид

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

откуда $\cos(\varphi_1+\varphi_2)=\cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2$ и $\sin(\varphi_1+\varphi_2)=\cos\varphi_1\sin\varphi_2+\sin\varphi_1\cos\varphi_2$. Тем самым, нами *доказаны* тригонометрические формулы сложения аргументов. На самом деле не только эти формулы, но и всё казуистическое изобилие формул школьной тригонометрии есть не что иное, как бесформенный шлейф случайных следствий того простого факта, что комплексные числа образуют поле и вычислять с ними можно по обычным правилам «раскрытия скобок».

Вот ещё один пример. Пусть $z=\cos\varphi+i\sin\varphi$. Тогда $z^n=\cos(n\varphi)+i\sin(n\varphi)$ можно вычислить, раскрывая скобки в $(\cos\varphi+i\sin\varphi)^n$ по формуле (1-9) из §1. Мы получаем равенство

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

которое заключает в себе тригонометрические формулы для кратных углов:

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

Упражнение 6.4. Докажите, что при нечётном n функция $\sin(n\varphi)/\sin\varphi$ является многочленом от $\sin^2\varphi$. Найдите его степень, корни и старший коэффициент. Выпишите этот многочлен явно для $n=3$ и $n=5$. Наконец, докажите для нечётных n тождество

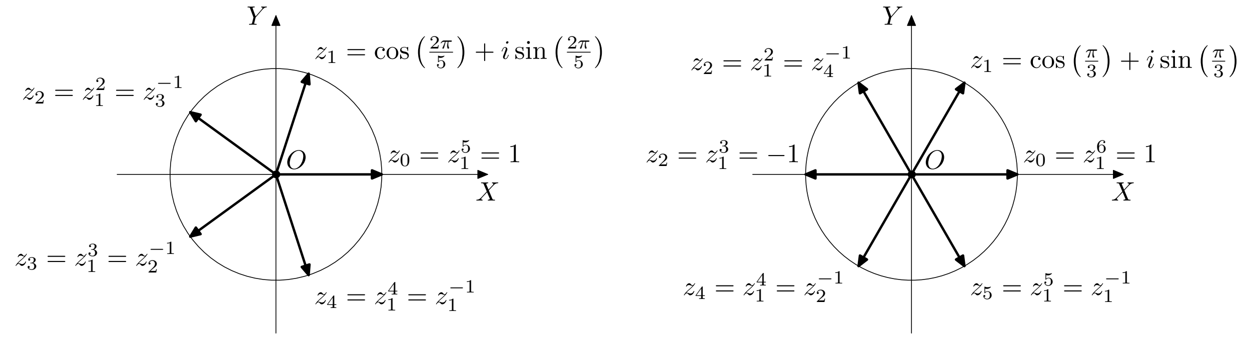
$$\frac{\sin(n\varphi)}{\sin\varphi}=(-4)^{\frac{n-1}{2}}\prod_{\nu=1}^{\frac{n-1}{2}}\left(\sin^2\varphi-\sin^2\frac{2\pi\nu}{n}\right)$$

6.3.4. Пример: корни из единицы и уравнение $z^n=a$. Решим в поле $\mathbb{C}$ уравнение $z^n=1$. Сравнивая модули левой и правой части, получаем $|z^n|=|z|^n=1$, откуда $|z|=1$. Обозначая через φ угол радиус-вектора z с осью OX и сравнивая аргументы левой и правой части уравнения, получаем

$$n\varphi\in\mathrm{Arg}\,(1)=\{2\pi k\mid k\in\mathbb{Z}\}\ ,$$

откуда $\varphi\in\{2\pi k/n\mid k\in\mathbb{Z}\}$. Таким образом, уравнение $z^n=1$ имеет ровно n корней $z_0,z_1,\dots,z_{n-1}$, которые располагаются в вершинах правильного n-угольника, вписанного в единичную окружность так, что вершина z_0 находится в точке 1 (см. рис. 6◇3, где $n=5$, 6):

$$z_k=\cos(2\pi k/n)+i\sin(2\pi k/n)\ ,\quad \text{где } k=0,\,1,\,\dots\,,\,(n-1)\ .$$



6◇3. Корни уравнений $z^5 = 1$ и $z^6 = 1$.

В частности, мы видим, что корни образуют циклическую группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-той степени из* 1. Мы уже встречались с нею в примерах (n° 2.1.2), (n° 2.2.2) и (n° 5.1.7). В качестве образующей этой группы можно взять, например, корень $z_1 = \cos(2\pi/n) + i\sin(2\pi/n)$. Тогда $z_k = z_1^k$ для всех $k = 0, 1, \dots, (n-1)$. Образующие группы $\boldsymbol{\mu}_n$ называются *первообразными корнями* степени n из единицы. На рис. 6◇3 все четыре отличных от 1 корня пятой степени из единицы являются первообразными, а среди корней 6-той степени из единицы первообразными являются только z_1 и $z_5 = z_1^{-1}$.

Многочлен, корнями которого являются первообразные корни n-той степени из 1 и только они, называется *многочленом деления круга на n частей* (или *n-тым циклотомическим многочленом*). Например, пятый и шестой циклотомические многочлены равны

$$f_5(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4) = z^4 + z^3 + z^2 + z + 1$$
$$f_6(z) = (z - z_1)(z - z_4) = z^2 - z + 1\,.$$

Упражнение 6.5*. Покажите, что при любом $n \in \mathbb{N}$ циклотомический многочлен $f_n(z)$ является неприводимым[1] над $\mathbb{Q}$ многочленом с целыми коэффициентами степени $\varphi(n)$ (где $\varphi(n)$ — это количество натуральных чисел, меньших n и взаимно простых с n).

Комментарий: Эта задача вместе с другими полезными фактами о циклотомических многочленах (включая несколько более или менее явных формул для них) содержится в «задачах семинаров» в дополнительном листке $6\frac{1}{2}$.

Упражнение 6.6. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ в радикалах от натуральных чисел.

Подсказка: для этого достаточно решить в радикалах уравнение деления круга $z^4 + z^3 + z^2 + z + 1 = 0$, которое сводится к квадратному уравнению делением обеих частей на z^2 и заменой $t = z + z^{-1}$.

Рассмотрим теперь уравнение $z^n = a$. Рассуждая как и выше, получаем

$$|z| = \sqrt[n]{|a|}\,, \quad n\varphi \in \operatorname{Arg}(a) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}\,,$$

где α — угол радиус-вектора a с осью OX. Таким образом, $\varphi \in \left\{ \frac{\alpha}{n} + \frac{2\pi k}{n} \;\middle|\; k \in \mathbb{Z} \right\}$, т. е. корни уравнения $z^n = a$ располагаются в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{|a|}$ с центром в нуле так, что радиус-вектор одной из его вершин располагается под углом α/n к оси OX.

Упражнение 6.7. Явно выразите действительные и мнимые части корней квадратного уравнения $z^2 = a$ через действительную и мнимую части числа a при помощи четырёх арифметических операций и извлечения квадратных корней из вещественных чисел.

6.4. Определение коммутативного кольца. Множество K с двумя операциями, удовлетворяющими всем аксиомам поля, за исключением требования существования обратного элемента, называется *коммутативным кольцом с единицей*. Если, кроме аксиомы существования обратного, из списка аксиом поля исключить ещё аксиому существования единицы, а с нею и аксиому $0 \neq 1$, множество K, удовлетворяющее оставшимся аксиомам, будет называется просто *коммутативным кольцом*. Модельные примеры колец с единицами, не являющихся полями — это кольцо целых чисел $\mathbb{Z}$, а также кольца многочленов с коэффициентами в произвольном коммутативном кольце с единицей. Примеры коммутативных колец без единицы доставляют чётные

[1] т. е. не раскладывающимся в произведение двух многочленов строго меньшей степени с рациональными коэффициентами

целые числа, многочлены с чётными целыми коэффициентами и многочлены с нулевым свободным членом и коэффициентами в любом коммутативном кольце.

Упражнение 6.8. Покажите, что свойства из упр. 6.1 остаются в силе в любом коммутативном кольце с единицей.

Как явствует из определения, основным отличием колец от полей является возможное отсутствие для некоторых элементов кольца обратных к ним элементов относительно умножения. Элемент a коммутативного кольца называется *обратимым*, если в этом кольце существует такой элемент a^{-1}, что $a^{-1}a = 1$. В противном случае элемент a называется *необратимым*. Так, в кольце $\mathbb{Z}$ обратимыми элементами являются только 1 и -1. В кольце $\mathbb{Q}[x]$ многочленов с рациональными коэффициентами обратимыми элементами являются ненулевые константы (многочлены степени нуль). Как следствие, между элементами коммутативного кольца возникает нетривиальное *отношение делимости*. Говорят, что элемент *a делится* на элемент b, если в кольце существует элемент q, такой что $a = bq$. Это обстоятельство записывается как $b|a$ (читается «b делит a») или как $a \,\vdots\, b$ (читается «a делится на b»).

6.4.1. Пример: гауссовы целые числа. Рассмотрим в поле комплексных чисел подмножество

$$\mathbb{Z}[i] \stackrel{\text{def}}{=} \{z = x + iy \mid x, y, \in \mathbb{Z}\} .$$

Числа этого множества располагаются на комплексной плоскости в точках с целочисленными координатами и называются *гауссовыми целыми числами*. Они образуют коммутативное кольцо с единицей относительно операций сложения и умножения комплексных чисел. В $\mathbb{Z}[i]$ имеется ровно 4 обратимых элемента: ± 1 и $\pm i$.

Кольцо $\mathbb{Z}[i]$ имеет много арифметических приложений. Например, вычисления в этом кольце существенно проясняют классическую задачу об описании всех натуральных чисел, представимых в виде суммы двух квадратов целых чисел (нуль при этом тоже допускается в качестве одного из квадратов). Связано это с тем, что квадратичная форма $x^2 + y^2$ над кольцом $\mathbb{Z}[i]$ разлагается в произведение двух линейных множителей: $x^2+y^2 = (x+iy)(x-iy)$, и задача представления натурального числа в виде суммы квадратов двух целых чисел сводится к задаче разложения натурального числа (рассматриваемого как элемента $\mathbb{Z}[i]$) в произведение двух комплексно сопряженных множителей, также лежащих в $\mathbb{Z}[i]$. Отсюда немедленно вытекает, что составное число $m = m_1m_2$, оба сомножителя в котором представимы в виде суммы двух квадратов:

$$m_1 = a_1^2 + b_1^2 = (a_1 + ib_1)(a_1 - ib_1) = z_1\overline{z}_1 \ , \quad m_2 = a_2^2 + b_2^2 = (a_2 + ib_2)(a_2 - ib_2) = z_2\overline{z}_2 \ ,$$

также может быть представлено в виде суммы двух квадратов:

$$m = z_1z_2 \cdot \overline{z_1z_2} = |z_1z_2|^2 = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2 \ .$$

Если доказать для кольца $\mathbb{Z}[i]$ аналог теоремы об однозначности разложения на простые множители (что вскоре будет нами сделано), то предыдущее вычисление полностью сведёт задачу о разложении натурального числа в сумму двух квадратов к вопросу о том, какие *простые* натуральные числа остаются простыми в $\mathbb{Z}[i]$, а какие начинают раскладываться на множители. Мы ещё вернёмся к этой задаче в дальнейшем[1].

Упражнение 6.9. Докажите, что для представимости числа $n \in \mathbb{N}$ в виде суммы двух квадратов целых чисел необходимо и достаточно, чтобы это число имело вид $n = p_1 \cdot p_2 \cdot \dots \cdot p_s \cdot k^2$, где $k \in \mathbb{Z}$ — любое, а $p_1, p_2, \dots, p_s$ — натуральные простые числа, представимые в виде суммы двух квадратов.

Упражнение 6.10*. Докажите, что простое $p \in \mathbb{N}$ тогда и только тогда представимо в виде суммы двух квадратов, когда оно имеет остаток 1 от деления на 4.

[1] впрочем, любознательный читатель уже сейчас может обратиться к замечательной книжке: *К. Айэрленд, М. Роузен. Классическое введение в современную теорию чисел.* М., «Мир», 1987 (или любое другое издание), где найдёт как завершение этой истории, так и разные другие изящные вычисления с гауссовыми числами