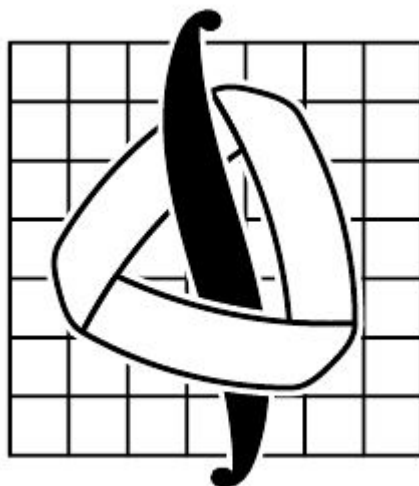


МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
Механико–математический факультет



Конспект лекций по теории чисел

4-й курс, первый поток, 7-й семестр, осень 2017 г.

Лектор: Олег Николаевич Герман

Москва, 2018 г.

Предисловие

Внимание! Это не курс лекций и не методичка, а всего лишь конспект, набранный в вёрстке \LaTeX и не претендующий на окончательную истину. В данном документе не исключены опечатки. Использовать на свой страх и риск. Авторы не несут ответственности за успешность подготовки по данному материалу, а также за его использование в качестве "шпоры".

Данный конспект по теории чисел состоит из 14-ти лекций, прочитанных Олегом Николаевичем Германом — доцентом кафедры теории чисел. Курс был прочитан на 7-ом семестре четвёртого курса мехмата МГУ осенью 2017 года. Он состоит из трёх больших разделов:

1. Асимптотический закон распределения простых чисел:

$$\pi(x) = \sum_{p \leq x} 1 \sim \frac{x}{\ln x}.$$

2. Теорема Дирихле о простых числах в арифметических прогрессиях: Если $(l, m) = 1$, то существует бесконечное количество таких простых p , что $p \equiv l \pmod{m}$.
3. Теоремы о том, что e и π — иррациональные и трансцендентные числа.

Конспект был подготовлен и за \TeX ан студентами Артемием Соколовым, группа 405 (нечётные лекции) и Артемием Геворковым, группа 402 (чётные лекции). За основу был взят конспект Юлии Зайцевой. Также в перспективе планируется добавить решения всех упражнений из курса.

Данная версия документа была скомпилирована 1 февраля 2018 г. Последняя версия .PDF, а также все исходные файлы всегда будут доступны в репозитории по (кликабельной) ссылке:

<https://github.com/arvego/numbertheory-sem7>

Если найдена ошибка или опечатка — пожалуйста, сообщите нам.

Спасибо Юлии Зайцевой, Виталию Лобачевскому, Всеволоду Гусеву, Кириллу Сосову, Сергею Джунусову, Айку Эминяну, Александру Думаревскому и команде Алгебрача за поиск ошибок и помощь в оформлении данного материала.

Содержание

1	Асимптотический закон распределения простых чисел	4
1.1	Игры с $\pi(x), \theta(x), \psi(x)$	4
1.2	Оценки Чебышева	5
1.3	Дзета-функция Римана	6
1.4	Воспоминания из былых времен	6
1.5	Преобразование Абеля	9
2	Теорема Дирихле о простых числах в арифметических прогрессиях	15
2.1	Свойства характеров	15
2.2	L -функции Дирихле	16
3	Диофантовы приближения	22
3.1	Основные сведения	22
3.2	Иррациональность e и π	25
3.3	Трансцендентность числа e	25
4	Алгебраические и трансцендентные числа	27
4.1	Основные сведения	27
4.2	Целые алгебраические числа	28
4.3	Конечные расширения \mathbb{Q}	29
4.4	Нормальные расширения	31
4.5	Трансцендентность π	33

1 Асимптотический закон распределения простых чисел

Замечание. Впредь, если мы будем писать сумму вида $\sum_{\dots p \dots} \dots$, то мы будем иметь в виду, что p – простое число.

1.1 Игры с $\pi(x), \theta(x), \psi(x)$

Изучение распределения простых чисел непосредственно связано с изучением следующих функций:

- $\pi(x) = \sum_{p \leq x} 1$ – количество простых чисел, не превосходящих x ;
- $\theta(x) = \sum_{p \leq x} \ln p = \ln \left(\prod_{p \leq x} p \right)$ – θ -функция Чебышева;
- $\psi(x) = \sum_{p^\alpha \leq x} \ln(p) = \sum_{p^\alpha \leq x} \left[\frac{\ln(x)}{\ln(p)} \right] \ln(p) = \ln(\text{НОК}(1, 2, \dots, [x]))$ – ψ -функция Чебышева.

Как эти функции связаны? Оказывается, следующим соотношением:

Лемма 1.1.

$$\varliminf \frac{\theta(x)}{x} = \varliminf \frac{\psi(x)}{x} = \varliminf \frac{\pi(x)}{x/\ln(x)}, \quad x \rightarrow \infty.$$

Доказательство. Заметим, что

$$\theta(x) \leq \psi(x) \leq \sum_{p \leq x} \left[\frac{\ln(x)}{\ln(p)} \right] \ln(p) = \ln(x) \sum_{p \leq x} 1 = \pi(x) \ln(x)$$

$$\varliminf \frac{\theta(x)}{x} \leq \varliminf \frac{\psi(x)}{x} \leq \varliminf \frac{\pi(x)}{x/\ln x}$$

Будем рассматривать простые числа на отрезке $[x^\alpha, x]$ для некоторого фиксированного $0 < \alpha < 1$. Тогда

$$\theta(x) = \left(\sum_{p \leq x} \ln(p) \right) \geq \left(\sum_{x^\alpha < p \leq x} \ln(p) \right) > \left(\ln(x^\alpha) \sum_{x^\alpha < p \leq x} 1 \right) = \alpha \ln(x) (\pi(x) - \pi(x^\alpha)) \geq \alpha \ln(x) (\pi(x) - x^\alpha).$$

$$\frac{\theta(x)}{x} > \alpha \left(\frac{\pi(x)}{x/\ln x} - \frac{\ln(x)}{x^{1-\alpha}} \right) \quad \forall 0 < \alpha < 1.$$

Тогда для любого $\alpha \in (0, 1)$ получаем, что $\varliminf \frac{\theta(x)}{x} \geq \varliminf \alpha \frac{\pi(x)}{x/\ln x}$.

Значит $\varliminf \frac{\theta(x)}{x} \geq \varliminf \frac{\pi(x)}{x/\ln x}$. ■

1.2 Оценки Чебышева

Теорема 1.1 (Оценки Чебышева). *Существуют $a, b > 0$ такие, что*

$$a \frac{x}{\ln(x)} \leq \pi(x) \leq b \frac{x}{\ln(x)}.$$

Перед доказательством этой теоремы сформулируем и докажем несколько вспомогательных лемм.

Лемма 1.2.

$$\prod_{p \leq n} p \leq 4^n.$$

Доказательство. Будем доказывать методом математической индукции по n .

База. При $n = 2, 3$ утверждение верно.

Переход. Если $n = 2k$ – чётно, то видно, что $\prod_{p \leq 2k} p = \prod_{p \leq 2k-1} p \leq 4^{2k-1} \leq 4^{2k}$.

Если $n = 2k - 1$ – нечётное, то по предложению индукции $\prod_{p \leq n} p = \left(\prod_{p \leq k} p \right) \left(\prod_{k < p \leq 2k-1} p \right) \leq 4^k 4^{k-1} =$

4^n . Заметим, что $\prod_{k < p \leq 2k-1} p < C_{2k-1}^k = \frac{(2k-1)!}{k!(k-1)!}$, т.к. каждое такое простое число входит в числи-

тель, но не входит в знаменатель. Поэтому $\prod_{k < p \leq 2k-1} p \leq C_{2k-1}^k \leq \frac{1}{2} \cdot 2^{2m-1} = 4^{m-1}$. ■

Следствие 1.1. $\theta(n) < n \ln(4)$.

Следствие 1.2. $\theta(x) < x \cdot 3 \ln(2)$.

Доказательство. Пусть $n - 1 < x \leq n$. Тогда $\theta(x) \leq \theta(n) < n \ln(4) < (x + 1) \ln 4 \leq x \cdot 3 \ln 2$. ■

Лемма 1.3. $K := \text{НОК}(1, 2, \dots, 2n + 1) > 4^n$

Доказательство. Рассмотрим $I = \int_0^1 x^n (1 - x)^n dx$. Поскольку на отрезке $[0, 1]$ величина $x(1 - x)$ не превосходит $\frac{1}{4}$, то $I < \frac{1}{4^n}$.

Заметим, что $x^n (1 - x)^n = a_n x^n + \dots + a_{2n} x^{2n}$ – многочлен с целыми коэффициентами. Тогда $I = \frac{a_n}{n+1} + \dots + \frac{a_{2n}}{2n+1}$, и $K \cdot I \in \mathbb{Z}$. Причём K и I оба больше нуля, т.е. $K \cdot I \geq 1$. Откуда следует, что $K \geq \frac{1}{I} > 4^n$. ■

Следствие 1.3. $\psi(2n + 1) > n \ln(4)$.

Следствие 1.4. $\psi(x) > x \frac{\ln(2)}{2}$ при $x \geq 6$.

Доказательство. Пусть $2n + 1 \leq x < 2n + 3$. Тогда $\psi(x) \geq \psi(2n + 1) > n \ln(4) > \frac{x-3}{2} \ln 4 = (x-3) \ln(2) \geq x \frac{\ln(2)}{2}$. ■

Доказательство. (Теоремы 1.1.)

Применим следствия 1.2 и 1.4. Тогда при $x \geq 6$ выполнено $\frac{\theta(x)}{x} < 3 \ln 2, \frac{\psi(x)}{x} > \frac{\ln 2}{2}$.

Учитывая Лемму 1.1 получаем, что $\overline{\lim} \frac{\pi(x)}{x/\ln x} \leq 3 \ln 2$ и $\underline{\lim} \frac{\pi(x)}{x/\ln x} \geq \frac{\ln 2}{2}$. ■

Теорема 1.2 (Асимптотический Закон Распределения Простых Чисел).

$$\pi(x) \sim \frac{x}{\ln x}.$$

1.3 Дзета-функция Римана

Положим при $\operatorname{Re}(s) > 1$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Будем писать $s = \sigma + it$. Мы докажем, что $\zeta(s)$ – аналитическая функция на $\operatorname{Re}(s) > 1$, и аналитически продолжим её на $\operatorname{Re}(s) > 0$ (можно и на всю \mathbb{C} , будет единственный полюс в точке 1).

Теорема 1.3 (Гипотеза Римана). *Нетривиальные нули ζ -функции лежат на прямой $\operatorname{Re}(s) = \frac{1}{2}$.*

Отступление:

Предположим, что p_1, p_2, \dots, p_r – все простые. Тогда $\sum_{k=0}^{\infty} \frac{1}{p_j^k} = \frac{1}{1 - \frac{1}{p_j}}$. Следовательно,

$$\sum_{(k_1, \dots, k_r)} \frac{1}{p_1^{k_1} \dots p_r^{k_r}} = \prod_{j=1}^r \frac{1}{1 - \frac{1}{p_j}} - \text{сходится}.$$

Но слева – сумма гармонического ряда. Противоречие.

1.4 Воспоминания из былых времен

Теорема 1.4 (Вейерштрасса). *Пусть в области Ω функции $f_n(s)$ аналитичны и ряд $\sum_{n=1}^{\infty} f_n(s)$ сходится равномерно (по Ω). Тогда он сходится к функции $f(x)$, аналитической в Ω , причём $f'(s) = \sum_{n=1}^{\infty} f'_n(s)$ – также сходится равномерно.*

Признак (Вейерштрасса). *Если в Ω справедливо $|f_n(s)| < c_n$, и $\sum_{n=1}^{\infty} c_n$ сходится, то ряд $\sum_{n=1}^{\infty} f_n(s)$ равномерно сходится в Ω .*

Определение 1.1. Функция $f : \mathbb{N} \rightarrow \mathbb{C}$ называется *арифметической* функцией. Если $f \not\equiv 0$ и $f(ab) = f(a)f(b)$ для любых a, b таких, что $(a, b) = 1$, то функция называется *мультипликативной*.

А если равенство $f(ab) = f(a)f(b)$ выполнено для абсолютно всех $a, b \in \mathbb{N}$, то функция называется *вполне мультипликативной*.

Сверткой Дирихле двух арифметических функций $f(n)$ и $g(n)$ является функция

$$(f * g)(n) = (g * f)(n) = \sum_{k|n} f(k)g\left(\frac{n}{k}\right)$$

Формула обращения Мебиуса гласит, что если $F = f * \mathbf{1}$, то $f = F * \mu$, где $\mu(n)$ – функция Мебиуса¹

Определение 1.2. Рядом Дирихле называется ряд вида $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, где $a_n \in \mathbb{Z}$.

Несложно видеть, что если $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, а $G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$, то $F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s}$.

Заметим, что $1 = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, где $a_1 = 1$, а остальные $a_i = 0, (i \neq 1)$. Хотим найти "обратную" функцию к $\zeta(s)$.

Известно, что $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$, где $\mu(n)$ – функция Мёбиуса.

Теорема 1.5. Пусть $\operatorname{Re}(s) > 1$. Тогда:

- 1) ряд $\sum_{n=1}^{\infty} \frac{1}{n^s}$ сходится абсолютно и задаёт аналитическую функцию $\zeta(s)$;
- 2) $\zeta'(s) = - \sum_{n=1}^{\infty} \frac{\ln(n)}{n^s}$;
- 3) $\zeta(s) \neq 0$ и $\frac{\zeta'(s)}{\zeta(s)} = - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$, где $\Lambda(n) = \begin{cases} \ln(p), & n = p^k, k \geq 1, \\ 0, & \text{иначе} \end{cases}$ – функция Мангольдта.

Доказательство.

Пункт 1): Обозначим $s = \sigma + it$. Тогда $\left| \frac{1}{n^s} \right| = \frac{1}{n^\sigma}$, $\sigma > 1$ – таким образом, абсолютная сходимость есть. При этом в области $\Omega_\delta = \{s \in \mathbb{C} \mid \operatorname{Re}(s) > 1 + \delta\}$, $\delta > 0$, сходимость будет равномерной, ибо $\left| \frac{1}{n^s} \right| = \frac{1}{n^\sigma} < \frac{1}{n^{1+\delta}}$, а ряд $\sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}}$ сходится. Но тогда по признаку Вейерштрасса $\sum_{n=1}^{\infty} \frac{1}{n^s}$ равномерно сходится в Ω_δ . По теореме 1.4 сумма ряда является аналитической в Ω_δ (каждая $\frac{1}{n^s}$ является целой функцией s). И это справедливо для всех δ .

Пункт 2): По теореме 1.4 в каждой Ω_δ : $\left(\frac{1}{n^s} \right)' = \left(e^{-s \ln n} \right)'$. Далее очевидно.

Пункт 3): Заметим, что в области Ω_δ :

$$\left| \frac{\Lambda(n)}{n^s} \right| = \frac{\Lambda(n)}{n^\sigma} \leq \frac{\ln n}{n^\sigma} < \frac{\ln(n)}{n^{1+\delta}},$$

¹ $\mu(n) = \begin{cases} 1, n = 1, \\ 0, \exists p^2 | n, \\ (-1)^r, n = p_1 \dots, p_r. \end{cases}$

а мы знаем, что ряд $\sum_{n=1}^{\infty} \frac{\ln(n)}{n^{1+\delta}}$ сходится. Тогда по признаку Вейерштрасса $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ сходится в Ω_δ равномерно. По теореме 1.4 сходится к аналитической функции, причём абсолютно. Перемножим два абсолютно сходящихся ряда:

$$\left(\sum_{k=1}^{\infty} \frac{1}{k^s} \right) \left(\sum_{l=1}^{\infty} \frac{\Lambda(l)}{l^s} \right) = \sum_{k,l=1}^{\infty} \frac{\Lambda(l)}{(kl)^s} = \sum_{n=1}^{\infty} \frac{\sum_{l|n} \Lambda(l)}{n^s} \stackrel{(*)}{=} \sum_{n=1}^{\infty} \frac{\ln(n)}{n^s} = -\zeta'(s).$$

(*) пусть $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, тогда $\sum_{l|n} \Lambda(l) = \sum_{j=1}^r \left(\sum_{\beta_j=1}^{\alpha_j} \Lambda(p_j^{\beta_j}) \right) = \sum_{j=1}^r \ln(p_j^{\alpha_j}) = \ln(n)$.

Итак, при $\operatorname{Re}(s) > 1$ имеем

$$-\zeta'(s) = \zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

Из аналитичности всех функций: пусть s_0 – ноль $\zeta(s)$ кратности $k > 0$, тогда s_0 – ноль $\zeta'(s)$ кратности $k - 1$. Так как мы перемножаем две функции, то их кратности должны складываться. Значит, $k - 1 = k + \text{нечто неотрицательное}$. Получаем противоречие. Почему кратность обязательно конечна? Предположим противное, пусть она бесконечна и тогда $\zeta(s)|_{\operatorname{Re}(s)>1} \equiv 0$ – противоречие. ■

Лемма 1.4. Пусть f – вполне мультипликативная функция, ряд $\sum_{n=1}^{\infty} f(n)$ абсолютно сходится и

$$S = \sum_{n=1}^{\infty} f(n). \text{ Тогда}$$

$$S = \prod_p (1 - f(p))^{-1}.$$

Доказательство. Положим $S(x) = \prod_{p \leq x} (1 - f(p))^{-1}$, покажем, что $S(x) \xrightarrow{x \rightarrow \infty} S$. Заметим, что из

мультипликативности f следует $f(1) = 1$ и что $|f(n)| < 1$ при $n \geq 2$ (т.к. иначе $f(n^k) = f(n)^k \not\rightarrow 0$, а члены ряда обязаны $\rightarrow 0$ из его абсолютной сходимости). Далее, при простом p : $\frac{1}{1 - f(p)} =$

$$\sum_{k=0}^{\infty} f(p)^k = \sum_{k=0}^{\infty} f(p^k). \text{ Следовательно, } S(x) = \prod_{p \leq x} (1 - f(p))^{-1} = \prod_{p \leq x} \sum_{k=0}^{\infty} f(p^k) = \sum_{\substack{n \in \mathbb{N}: \\ \forall p|n \ p \leq x}} f(n) \text{ (такие } n$$

$$\text{зовутся "x-гладкими"). Стало быть, } |S - S(x)| = \left| \sum_{\substack{n \in \mathbb{N}: \\ \exists p|n \ p > x}} f(n) \right| \leq \sum_{\substack{n \in \mathbb{N}: \\ \exists p|n \ p > x}} |f(n)| \leq \sum_{n > x} |f(n)| \xrightarrow{x \rightarrow \infty} 0$$

(т.к. последний ряд – хвост сходящегося). ■

Теорема 1.6 (формула Эйлера). Пусть $\operatorname{Re}(s) > 1$. Тогда

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s} \right)^{-1}.$$

Доказательство. Возьмём (и положим) $f(n) = \frac{1}{n^s}$ и применим лемму 1.4. Тогда

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s} \right)^{-1}.$$

■

Лемма 1.5. $\psi(x) = \sum_{n \leq x} \Lambda(n)$ (ну, т.е. $\psi(n) - \psi(n-1) = \Lambda(n)$).

Доказательство. Следует из определений $\psi(x)$ и $\Lambda(n)$. ■

1.5 Преобразование Абеля

Лемма 1.6. (*Преобразование Абеля*) Пусть $\{a_n\}_{n \in \mathbb{N}}$ – последовательность комплексных чисел. Пусть $g(x) \in C^1([1; \infty), \mathbb{C})$, $A(x) = \sum_{n \leq x} a_n$. Тогда для любого $N \in \mathbb{R}$ выполнено

$$\sum_{n \leq N} a_n g(n) = A(N)g(N) - \int_1^N A(x)g'(x)dx.$$

Доказательство.

$$A(N)g(N) - \sum_{n \leq N} a_n g(n) = \sum_{n \leq N} a_n (g(N) - g(n)) = \sum_{n \leq N} a_n \int_n^N g'(x)dx.$$

Положим $\varphi_n(x) = a_n$, если $x \geq n$ или 0, если $x < n$. Тогда

$$\sum_{n \leq N} a_n \int_n^N g'(x)dx = \sum_{n \leq N} \int_1^N \varphi_n(x)g'(x)dx = \int_1^N \left(\sum_{n \leq N} \varphi_n(x) \right) g'(x)dx = \int_1^N A(x)g'(x)dx.$$

■

Теорема 1.7.

$$\zeta(s) = 1 + \frac{1}{s-1} - s \int_1^{+\infty} \frac{\{x\}}{x^{1+s}} dx,$$

причем интеграл в правой части сходится в полуплоскости $\operatorname{Re}(s) > 0$ и задает аналитическую функцию.

Доказательство. При $\operatorname{Re}(s) > 1$ выполнено $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Используя преобразование Абеля с параметрами $a_n = 1$ и $g(x) = \frac{1}{x^s}$ получим, что

$$\begin{aligned} \sum_{n=1}^N \frac{1}{n^s} &= N \frac{1}{N^s} + s \int_1^N \frac{[x]}{x^{1+s}} = \frac{1}{N^{s-1}} + s \left(\int_1^N \frac{1}{x^s} - \int_1^N \frac{\{x\}}{x^{1+s}} \right) = \\ &= \frac{1}{N^{s-1}} + s \left(\frac{1}{s-1} - \frac{1}{(s-1)N^{s-1}} - \int_1^N \frac{\{x\}}{x^{1+s}} \right) = 1 + \frac{1}{s-1} - \frac{1}{(s-1)N^{s-1}} - s \int_1^N \frac{\{x\}}{x^{1+s}}. \end{aligned}$$

Поскольку $s = \sigma + it$, где $\sigma > 1$, и $|N^{s-1}| = N^{\sigma-1}$, то при $N \rightarrow \infty$ третье слагаемое стремится к 0, а последнее стремится к несобственному интегралу в условии теоремы.

Итак, при $\operatorname{Re}(s) > 1$ выполнено равенство

$$\zeta(s) = 1 + \frac{1}{s-1} - s \int_1^\infty \frac{\{x\}}{x^{1+s}} dx.$$

Как только мы докажем, что этот интеграл задает аналитическую функцию в $\operatorname{Re}(s) > 0$, мы получим две функции, которые аналитичны в $\operatorname{Re}(s) > 0$ и совпадают в $\operatorname{Re}(s) > 1$, откуда будет следовать, что они совпадают везде².

Положим

$$f_n(s) = \int_n^{n+1} \frac{\{x\}}{x^{s+1}} dx = \int_n^{n+1} \frac{x-n}{x^{s+1}} dx = \int_n^{n+1} \frac{1}{x^s} dx - n \int_n^{n+1} \frac{1}{x^{s+1}} dx.$$

Первый интеграл аналитичен³ в \mathbb{C} , второй отличается от первого просто сдвигом на 1.

Таким образом, $f_n(s)$ аналитична в \mathbb{C} . При $\operatorname{Re}(s) = \sigma > \delta > 0$ получим, что

$$|f_n(s)| \leq \int_n^{n+1} \frac{dx}{x^{1+\sigma}} \leq \frac{1}{n^{1+\sigma}} < \frac{1}{n^{1+\delta}}$$

Поскольку ряд $\sum_{n=1}^\infty \frac{1}{n^{1+\delta}}$ сходится, то по признаку Вейерштрасса ряд $\sum_{n=1}^\infty f_n(s)$ сходится равномерно, поэтому задает аналитическую функцию. ■

Следствие 1.5. У функции $\zeta(s)$ полюс первого порядка с вычетом 1, поскольку $\operatorname{Res}_{s=1} \frac{1}{s-1} = 1$.

Лемма 1.7. При $\operatorname{Re}(s) > 1$ выполнено

$$\frac{\zeta'(s)}{\zeta(s)} = -s \int_1^\infty \frac{\psi(x)}{x^{1+s}} dx.$$

Доказательство. При $\operatorname{Re}(s) > 1$ имеем

$$\frac{\zeta'(s)}{\zeta(s)} = - \sum_{n=1}^\infty \frac{\Lambda(n)}{n^s}$$

Используя преобразование Абеля с параметрами $a_n = \Lambda(n)$, $g(x) = \frac{1}{x^s}$ и тот факт, что $\sum_{n \leq x} \Lambda(n) =$

$\psi(x)$ получим, что

$$\sum_{n=1}^N \frac{\Lambda(n)}{n^s} = \frac{\psi(N)}{N^s} + s \int_1^N \frac{\psi(x)}{x^{1+s}} dx.$$

Поскольку мы знаем, что у отношения $\frac{\psi(x)}{x}$ верхний и нижний пределы ограничены, то при $\operatorname{Re}(s) > 1$

$$\frac{\psi(N)}{N^{1+s}} \rightarrow 0 \text{ при } N \rightarrow \infty.$$

Таким образом, при $N \rightarrow \infty$ пределы выражений $\sum_{n=1}^N \frac{\Lambda(n)}{n^s}$ и $s \int_1^N \frac{\psi(x)}{x^{1+s}} dx$ существуют и равны, откуда следует утверждение леммы. ■

²Теорема единственности

³При $s \neq 1$ это просто разность степеней, а почему есть аналитичность в точке $s = 1$? Упражнение!

Лемма 1.8. Пусть $0 < r < 1, \varphi \in \mathbb{R}$. Тогда

$$|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})| \leq 1.$$

Доказательство. Положим $M = |(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})|$. Тогда

$$\begin{aligned} \ln(M) &= 3\ln(|1-r|) + 4\ln(|1-re^{i\varphi}|) + \ln(|1-re^{2i\varphi}|) = \operatorname{Re}(3\ln(1-r) + 4\ln(1-re^{i\varphi}) + \ln(1-re^{2i\varphi})) = \\ &= -\sum_{n=1}^{\infty} \frac{r^n}{n} \operatorname{Re}(3 + 4e^{in\varphi} + e^{2in\varphi}) = -\sum_{n=1}^{\infty} \frac{r^n}{n} (\cos 2n\varphi + 4\cos n\varphi + 3) = -\sum_{n=1}^{\infty} \frac{r^n}{n} 2(\cos n\varphi + 1)^2 \leq 0. \end{aligned}$$

Следовательно, $M \leq 1$. ■

Лемма 1.9. При $s = \sigma + it, \sigma > 1$ выполнено неравенство

$$|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \geq 1.$$

Доказательство. Положим $r = \frac{1}{p^\sigma}, e^{i\varphi} = p^{-it}$. Применим лемму 1.8 и формулу Эйлера 1.6. ■

Теорема 1.8. $\zeta(1+it) \neq 0$ при всех $t \in \mathbb{R} \setminus \{0\}$.

Доказательство. Предположим противное: пусть $\zeta(1+it_0) = 0$. Тогда при $\sigma \rightarrow 1+$:

$$\zeta^3(\sigma)\zeta^4(\sigma+it_0)\zeta(\sigma+2it_0) = O\left(\frac{1}{(\sigma-1)^3}(\sigma-1)^4 \cdot 1\right) = O_{\sigma \rightarrow 1}(\sigma-1). \text{ (Т.к. } \zeta(\sigma) \rightarrow +\infty \text{ при } \sigma \rightarrow 1+,$$

точнее, $\zeta(\sigma) = O\left(\frac{1}{\sigma-1}\right)$ ибо полюс порядка 1; $\zeta(1+it_0) = 0 \xrightarrow{\text{из мульт.пл.}} \zeta(\sigma+it_0) = O(\sigma-1);$

$\zeta(1+2it_0)$ – какая-то константа, полюса там нет из аналитичности функции в $\operatorname{Re}(s) > 0$ везде, кроме 1). Итак, получили $\zeta^3(\sigma)\zeta^4(\sigma+it_0)\zeta(\sigma+2it_0) = O_{\sigma \rightarrow 1}(\sigma-1)$, но по Лемме 1.9 её модуль ≥ 1 при любом $\sigma > 1$. Противоречие.

(Из Леммы 1.9 также можно ещё одним способом получить, что в полуплоскости $\operatorname{Re}(s) > 1$ у ζ -функции нет корней: если бы существовал корень $s = \sigma + it$, то $|\zeta^3(\sigma)\zeta^4(s)\zeta(\sigma+2it)| \geq 1$, противоречие). ■

Лемма 1.10. $\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1}$ аналитична при $\operatorname{Re}(s) \geq 1$.

Доказательство. Знаем, что при $\operatorname{Re}(s) > 1$ оба слагаемых – аналитические функции. Мы также доказали, что $\zeta(s) = \frac{f(s)}{s-1}$, где $f(s)$ точно аналитична при $\operatorname{Re}(s) > 0$ и $f(s) \neq 0$ при $\operatorname{Re}(s) \geq 1$.

Отсюда следует, что $\frac{\zeta'(s)}{\zeta(s)} = \frac{f'(s)}{f(s)} - \frac{1}{s-1}$, где f аналитична при $\operatorname{Re}(s) > 0$, а значит, что f' тоже. В $\operatorname{Re}(s) \geq 1$ у знаменателя нет нулей. ■

Положим $F(s) := -\frac{1}{s} \frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$.

Лемма 1.11. Справедливы следующие утверждения

1) $F(s)$ аналитична в $\operatorname{Re}(s) \geq 1$.

$$2) F(s) = \int_1^{+\infty} \frac{\psi(x) - x}{x^{1+s}} dx \text{ при } \operatorname{Re}(s) > 1.$$

Доказательство. По порядку.

- 1) $F(s) = -\frac{1}{s} \left(\frac{\zeta'(s)}{\zeta(s)} + \frac{s}{s-1} \right) = -\frac{1}{s} \left(\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1} + 1 \right) - \frac{1}{s}$ аналитична, а второй множитель аналитичен по Лемме 1.10.
- 2) При $\operatorname{Re}(s) > 1$ $\frac{\zeta'(s)}{\zeta(s)} = -s \int_1^{+\infty} \frac{\psi(x) dx}{x^{1+s}}$, $\frac{1}{s-1} = \int_1^{+\infty} \frac{dx}{x^s}$. Оба интеграла сходятся абсолютно, поэтому можно их складывать:

$$F(s) = \int_1^{+\infty} \frac{\psi(x) dx}{x^{1+s}} - \int_1^{+\infty} \frac{dx}{x^s} = \int_1^{+\infty} \frac{\psi(x) - x}{x^{1+s}} dx.$$

■

Теорема 1.9. В интегральном представлении $F(s)$ можно перейти к пределу в $\operatorname{Re}(s) > 1$, т.е.

$$F(1) = \int_1^{+\infty} \frac{\psi(x) - x}{x^2} dx.$$

Лемма 1.12. Если интеграл $\int_1^{+\infty} \frac{\psi(x) - x}{x^2} dx$ сходится (это будет следовать из Теоремы 1.9), то $\psi(x) \sim x$.

Доказательство. Возьмём $\varepsilon > 0$:

$$\int_x^{(1+\varepsilon)x} \frac{\psi(u) - u}{u^2} du \geq \varepsilon x \frac{\psi(x) - (1+\varepsilon)x}{(1+\varepsilon)^2 x^2} = \frac{\varepsilon}{(1+\varepsilon)^2} \left(\frac{\psi(x)}{x} - (1+\varepsilon) \right).$$

Из сходимости интеграла слева при фиксированном ε получаем $\int_x^{(1+\varepsilon)x} \frac{\psi(u) - u}{u^2} du \xrightarrow{x \rightarrow \infty} 0$. Следовательно, $\overline{\lim}_{x \rightarrow \infty} \frac{\varepsilon}{(1+\varepsilon)^2} \left(\frac{\psi(x)}{x} - (1+\varepsilon) \right) \leq 0$ при фиксированном ε . Отсюда $\overline{\lim}_{x \rightarrow \infty} \frac{\psi(x)}{x} \leq 1 + \varepsilon$, а т.к. это верно для любого x , то $\overline{\lim}_{x \rightarrow \infty} \frac{\psi(x)}{x} \leq 1$. И наоборот, меняя знак неравенства, получаем $\overline{\lim}_{x \rightarrow \infty} \frac{\psi(x)}{x} \geq 1 - \varepsilon$, а т.к. это верно для любого ε , то $\overline{\lim}_{x \rightarrow \infty} \frac{\psi(x)}{x} \geq 1$. ■

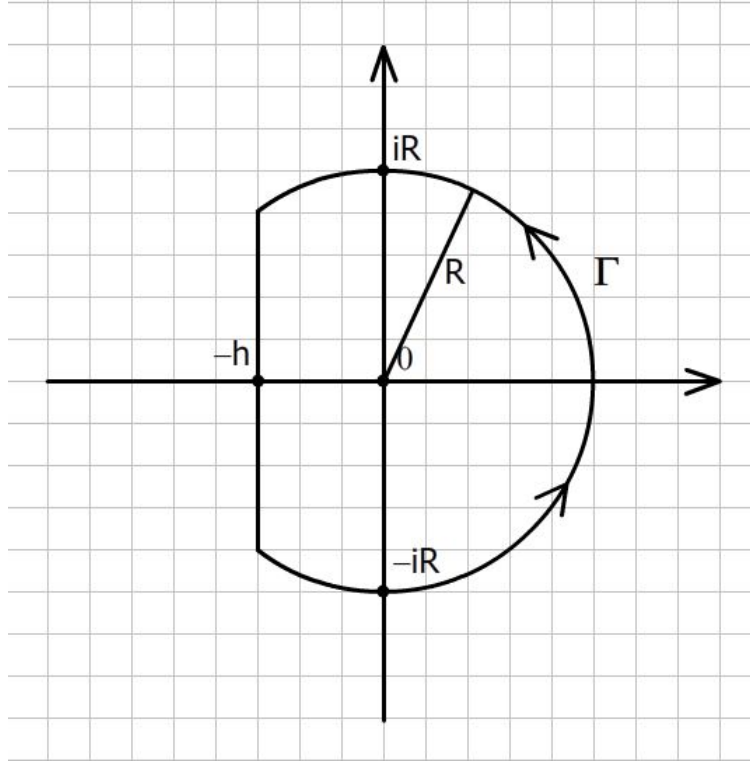
Доказательство. (Теоремы 1.9).

Положим $F_T(s) = \int_1^T \frac{\psi(x) - x}{x^{1+s}} dx$, $T > 1$. Поскольку $\int_n^{n+1} \frac{dx}{x^s}$ — целая функция, т.к. $\psi(x)$ на отрезке $[n, n+1]$ постоянна, то $\int_1^T \frac{\psi(x) - x}{x^{1+s}} dx$ является суммой целых функций вида $\int_n^{n+1} \frac{dx}{x^s} \Rightarrow F_T(s)$ — целая. Нужно показать, что $F_T(1) \rightarrow F(1)$ при $T \rightarrow \infty$. По определению предела, возьмём $\varepsilon > 0$ и рассмотрим следующий интеграл

$$I(T) = \frac{1}{2\pi i} \int_{\Gamma} (F(1+s) - F_T(1+s)) T^s \left(\frac{s}{R^2} + \frac{1}{s} \right) ds, \quad R = \frac{1}{\varepsilon}.$$

$F(s)$ аналитична в $\operatorname{Re}(s) \geq 1 \Rightarrow F(1+s)$ аналитична в $\operatorname{Re}(s) \geq 0$. То есть, она аналитична на отрезке $[-iR, iR]$ (см. Рис. 1). Если $F(s)$ аналитична в точке, то она аналитична в некоторой окрестности

этой точки. Применяя это к каждой точке нашего отрезка, получаем его покрытие открытыми кругами и выделяем конечное подпокрытие по компактности $[-iR, iR]$. Теперь выбираем h так, чтобы прямоугольник был внутри объединения кругов, т.е. чтобы $F(1+s)$ была аналитична на нарисованном контуре ($h = h(\varepsilon)$).



(Рис. 1)

Значит, в $I(T)$: $F(1+s)$ – аналитична в области (по построению), $F_T(1+s)$ – везде целая, T^s – целая (экспонента), $\frac{s}{R^2}$ – целая, $\frac{1}{s}$ – полюс порядка 1 в нуле. Следовательно, по теореме Коши о вычетах

$$I(T) = (F(1) - F_T(1))T^0 = F(1) - F_T(1).$$

■

Лемма 1.13.

При $\sigma = \operatorname{Re}(s) > 0$: $|F(1+s) - F_T(1+s)| \leq A \frac{T^{-\sigma}}{\sigma};$

при $\sigma = \operatorname{Re}(s) < 0$: $|F_T(1+s)| \leq A \frac{T^{-\sigma}}{-\sigma},$

где A такое, что $\left| \frac{\psi(x)}{x} - 1 \right| \leq A$ при $x \geq 1$.

Доказательство.

$$\sigma > 0: \quad |F(1+s) - F_T(1+s)| = \left| \int_T^{+\infty} \frac{\psi(x) - x}{x^{2+s}} dx \right| \leq A \int_T^{+\infty} \frac{dx}{x^{1+\sigma}} = A \frac{T^{-\sigma}}{\sigma};$$

$$\sigma < 0: \quad |F_T(1+s)| = \left| \int_1^T \frac{\psi(x) - x}{x^{2+s}} dx \right| \leq A \int_1^T \frac{dx}{x^{1+\sigma}} = A \frac{T^{-\sigma}}{-\sigma}.$$

■

Лемма 1.14. Если $|s| = R$, то $\frac{s}{R^2} + \frac{1}{s} = \frac{2\operatorname{Re}(s)}{R^2}$

Доказательство.

$$\frac{s}{R^2} + \frac{1}{s} = \frac{1}{R} \left(\frac{s}{R} + \frac{R}{s} \right) = \frac{1}{R} \cdot 2 \operatorname{Re} \left(\frac{s}{R} \right) = \frac{2 \operatorname{Re}(s)}{R^2}. \quad \blacksquare$$

Лемма 1.15. При $T > 1$ и $x \in \mathbb{R}$ выполнено $xT^{-x} \leq \frac{1}{e \ln(T)}$.

Доказательство. Считаем производную $(xT^{-x})' = (1 - x \ln(T))T^{-x}$. Она обращается в 0 в точке $x_0 = \frac{1}{\ln(T)}$. Ну и несложно видеть, что функция при $x < x_0$ возрастает, при $x > x_0$ убывает, значит максимум значения функции равен $\frac{1}{\ln(T)} T^{-\frac{1}{\ln(T)}} = \frac{1}{e \ln(T)}$. \blacksquare

Положим $\Gamma_1 = \Gamma \cap \{s \in \mathbb{C} \mid \operatorname{Re}(s) \geq 0\}$, $\Gamma_2 = \Gamma \cap \{s \in \mathbb{C} \mid \operatorname{Re}(s) \leq 0\}$.

Тогда $I(T) = I_1(T) + I_2(T) = \frac{1}{2\pi i} \int_{\Gamma_1} \dots + \frac{1}{2\pi i} \int_{\Gamma_2} \dots$

По Лемме 1.13

$$|I_1(t)| \leq \frac{1}{2\pi} \int_{\Gamma_1} A \frac{T^{-\sigma}}{\sigma} T^\sigma \frac{2\sigma}{R^2} ds = \frac{1}{2\pi} \frac{2A}{R^2} = A\varepsilon$$

$$I_2(T) = I_3(T) - I_4(T) = \frac{1}{2\pi i} \int_{\Gamma_2} F(1+s) T^s \left(\frac{s}{R^2} + \frac{1}{s} \right) ds - \frac{1}{2\pi i} \int_{\Gamma_2} F_T(1+s) T^s \left(\frac{s}{R^2} + \frac{1}{s} \right) ds.$$

По Лемме 1.13, $I_4(T)$ оценивается точно так же, как и $I_1(T)$, только надо заменить контур Γ_1 на Γ_3 . Это можно сделать, так как у подынтегральной функции нет полюсов вне контура $\Gamma_3 \cup \Gamma_2$ (полюс только 0). Таким образом, $|I_4(T)| \leq A\varepsilon$.

Осталось оценить $I_3(T) = \int_{\Gamma_2} F(1+s) T^s \left(\frac{s}{R^2} + \frac{1}{s} \right) ds$.

Заметим, что

1. на малых дугах $\left| T^s \left(\frac{s}{R^2} + \frac{1}{s} \right) \right| = \frac{2\sigma}{R^2} T^\sigma \stackrel{\text{Лемма 1.14}}{=} \frac{2\sigma T^{-|\sigma|}}{R^2} \stackrel{\text{Лемма 1.15}}{\leq} \frac{2}{R^2} \frac{1}{e \ln(T)}$;
2. на вертикальном отрезке $T^s = T^{-h}$;
3. на Γ_2 верно $|F(1+s) \left(\frac{s}{R^2} + \frac{1}{s} \right)| \leq C = C(\varepsilon)$ – не зависит от T .

Следовательно, $I_3(T) \rightarrow 0$ при $T \rightarrow +\infty$. То есть, $\exists T_0(\varepsilon) : \forall T > T_0$ выполняется $|I_3(T)| < \varepsilon$.

Итак, $|I(T)| \leq |I_1(T)| + |I_4(T)| + |I_3(T)| \leq A\varepsilon + A\varepsilon + \varepsilon = (2A + 1)\varepsilon$.

Теорема 1.9 \Rightarrow Лемма 1.12. Леммы 1.1 и 1.12 \Rightarrow Теорема 1.2 – АЗРПЧ.

2 Теорема Дирихле о простых числах в арифметических прогрессиях

Теорема 2.1 (Дирихле). Пусть $l, m \in \mathbb{Z}, (l, m) = 1, m \geq 2$. Тогда существует бесконечно много простых p таких, что $p \equiv l \pmod{m}$.

Замечание. При фиксированном m таких прогрессий ровно $\varphi(m)$ штук.

Число простых до x в этой прогрессии на самом деле $\frac{1}{\varphi(m)} \frac{x}{\ln x}$, то есть эти простые распределены по прогрессии равномерно. Но доказывать мы это, конечно же, не будем.

2.1 Свойства характеров

Определение 2.1. Пусть $m \in \mathbb{N}, m \geq 2$. Функция $\chi : \mathbb{Z} \rightarrow \mathbb{C}$ называется *числовым характером* (Дирихле) по модулю m , если

1. $\forall a \in \mathbb{Z}$ выполняется $\chi(a + m) = \chi(a)$;
2. $\chi(a) = 0 \Leftrightarrow (a, m) \neq 1$;
3. $\chi(ab) = \chi(a)\chi(b)$.

Замечание. Несложно провести биекцию $\chi : \mathbb{Z} \rightarrow \mathbb{C} \leftrightarrow \bar{\chi} : \mathbb{Z}_m^* \rightarrow \mathbb{C}^*$.

Замечание. $|\chi(a)| = 0$, если $(a, m) \neq 1$; иначе. Для начала заметим, что $\chi(1) = \chi(1 \cdot 1) = \chi(1)^2$, и поскольку $\chi(1) \neq 0$, то $\chi(1) = 1$. Вспомним, что если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$ (Малая теорема Ферма). Тогда $\chi(a)^{\varphi(m)} = \chi(a^{\varphi(m)}) = \chi(1) = 1$. Таким образом, мы получили, что $\chi(a) \in \sqrt[\varphi(m)]{1}$.

Вспомним теорему с первого курса: \mathbb{Z}_m^* циклическая $\Leftrightarrow m = 1, 2, 4, p^k, 2p^k$ для простого p .⁴

Предложение 2.1. \mathbb{Z}_m^* разлагается в прямое произведение циклических групп.

Лемма 2.1. Пусть η_1, \dots, η_r – произвольный набор корней из 1 степеней d_1, \dots, d_r соответственно (т.е. $\eta_i^{d_i} = 1$). Тогда $\exists! \chi : \chi(g_i) = \eta_i$.

Доказательство. Для $(a, m) = 1$ полагаем $\chi(a) = \eta_1^{\alpha_1} \dots \eta_r^{\alpha_r}$, где $\bar{a} = \bar{g}_1^{\alpha_1} \dots \bar{g}_r^{\alpha_r}$. Для $(a, m) \neq 1$ полагаем $\chi(a) = 0$. Достаточно проверить, что если $(a, m) = 1, (b, m) = 1$, то $\chi(ab) = \chi(a)\chi(b)$.

Пусть $\bar{a} = \bar{g}_1^{\alpha_1} \dots \bar{g}_r^{\alpha_r}, \bar{b} = \bar{g}_1^{\beta_1} \dots \bar{g}_r^{\beta_r}, \bar{c} = \bar{g}_1^{\gamma_1} \dots \bar{g}_r^{\gamma_r}$, где $0 \leq \alpha_i, \beta_i, \gamma_i \leq d_i - 1, i = 1 \dots r$. Тогда $\gamma_i \equiv \alpha_i + \beta_i \pmod{d_i}$. Следовательно, т.к. η_i – корень из 1 степени d_i , получаем

$$\chi(a)\chi(b) = \eta_1^{\alpha_1} \dots \eta_r^{\alpha_r} \cdot \eta_1^{\beta_1} \dots \eta_r^{\beta_r} = \eta_1^{\gamma_1} \dots \eta_r^{\gamma_r} = \chi(ab).$$

■

Лемма 2.2. Если $a \not\equiv 1 \pmod{m}$, то $\exists \chi : \chi(a) \neq 1$.

⁴Это эквивалентно наличию первообразного корня по искомому модулю

Доказательство. Очевидно из Леммы 2.1: если $(a, m) \neq 1$, то все характеры подходят; если $(a, m) = 1$, то $\bar{a} = \bar{g}_1^{\alpha_1} \dots \bar{g}_r^{\alpha_r} \pmod{m}$, $0 \leq \alpha_i \leq d_i - 1$. Т.к. $a \not\equiv 1 \pmod{m}$, то $\exists \alpha_i \neq 0$, можно положить, что это $\alpha_1 > 0$.

Положим $\chi(g_1) = \eta_1 = e^{\frac{2\pi i}{d_1}}$, $\chi(g_j) = \eta_j = 1$, $\forall j = 2, \dots, r$. Тогда, т.к. по Лемме 2.1 характер существует, то $\chi(a) = e^{\frac{2\pi i}{d_1} \alpha_1} \neq 1$. ■

Определение 2.2. Характер χ_0 , где $\chi_0(a) = \begin{cases} 1, & (a, m) = 1, \\ 0, & (a, m) \neq 1 \end{cases}$ называется *главным характером*.

Ясно, что $\chi \cdot \chi_0 = \chi$, где операция \cdot – поточечное перемножение функций. Для любого χ существует обратное χ^{-1} : $\chi^{-1}(a) = \begin{cases} \chi(a)^{-1}, & \chi(a) \neq 0, \\ 0, & \chi(a) = 0. \end{cases}$ В общем, ясно, что характеры образуют группу.

Задача 2.1. Доказать, что группа характеров изоморфна \mathbb{Z}_m^* .

Характеров по модулю m ровно $\varphi(m)$ штук (следует из Леммы 2.1, $d_1 \dots d_r = |\mathbb{Z}_m^*| = \varphi(m)$).

Лемма 2.3. Справедливы следующие равенства

$$\begin{aligned} 1) \sum_{a=1}^m \chi(a) &= \begin{cases} \varphi(m), & \text{если } \chi = \chi_0, \\ 0, & \text{иначе.} \end{cases} \\ 2) \sum_{\chi} \chi(a) &= \begin{cases} \varphi(m), & \text{если } a \equiv 1 \pmod{m}, \\ 0, & \text{иначе.} \end{cases} \end{aligned}$$

Доказательство. По порядку.

1) Если $\chi = \chi_0$, то всё понятно.

Если $\chi \neq \chi_0$, то $\exists b \in \mathbb{Z} : \chi(b) \neq 0, 1$. Положим $s = \sum_{a=1}^m \chi(a)$, тогда $s\chi(b) = \sum_{a=1}^m \chi(ab) = \sum_{a=1}^m \chi(a) = s \Rightarrow s = 0$.

2) Если $a \equiv 1 \pmod{m}$, то всё понятно.

Если $(a, m) \neq 1$, то сумма из нулей равна нулю (действительно).

Если $(a, m) = 1$ и $a \not\equiv 1 \pmod{m}$, то по Лемме 2.2 можно взять характер χ_1 : $\chi_1(a) \neq 0, 1$.

Положим $s = \sum_{\chi} \chi(a)$, тогда $s\chi_1(a) = \sum_{\chi} \chi(a)\chi_1(a) = \sum_{\chi} \chi(a) = s \Rightarrow s = 0$. ■

Следствие 2.1. Если $\chi \neq \chi_0$, то $\left| \sum_{n=1}^m \chi(n) \right| \leq \varphi(m)$.

2.2 L-функции Дирихле

Пусть $m \geq 2$, χ – характер по модулю m .

Определение 2.3. $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ называется L -функцией Дирихле.

Лемма 2.4. При $\operatorname{Re}(s) > 1$

- 1) Ряд $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ сходится абсолютно, задаёт аналитическую функцию;
- 2) $L'(s, \chi) = - \sum_{n=1}^{\infty} \frac{\chi(n) \ln(n)}{n^s}$;
- 3) $L(s, \chi) \neq 0$ и $\frac{L'(s, \chi)}{L(s, \chi)} = - \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^s}$.

Доказательство. Доказательство этой теоремы очень схоже с доказательством теоремы 1.5. Напомним, что $s = \sigma + it$.

- 1) $\left| \frac{\chi(n)}{n^s} \right| \leq \frac{1}{n^\sigma} \Rightarrow$ сходится абсолютно при $\sigma > 1$. Но для аналитичности предела нам необходима равномерная сходимость. В области $\Omega_\delta = \{\operatorname{Re}(s) > 1 + \delta\}$ $\left| \frac{\chi(n)}{n^s} \right| \leq \frac{1}{n^\sigma} \leq \frac{1}{n^{1+\delta}}$ – общий член сходящегося ряда. значит, по признаку Вейерштрасса в Ω_δ наша последовательность равномерна. Следовательно, по теореме 1.4 (Вейерштрасса) ряд сходится к аналитической функции.
- 2) В первом пункте мы воспользовались теоремой Вейерштрасса, которая, в частности, гласит, что наш ряд можно почленно дифференцировать.
- 3) $L(s, \chi) \cdot \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^s} = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^s} = \sum_{k, n \in \mathbb{N}} \frac{\chi(k) \chi(n) \Lambda(n)}{(kn)^s} = \sum_{k, n \in \mathbb{N}} \frac{\chi(kn) \Lambda(n)}{(kn)^s} = \sum_{\substack{n \in \mathbb{N} \\ d|n}} \frac{\chi(n) \Lambda(d)}{n^s} = \sum_{n \in \mathbb{N}} \frac{\chi(n) \ln(n)}{n^s} = -L'(s, \chi).$

Итак, получили $L(s, \chi) \cdot \sum_{n=1}^{\infty} \frac{\chi(n) \Lambda(n)}{n^s} = -L'(s, \chi).$

Если s_0 – ноль порядка $k \in \mathbb{N}$, то порядок нуля левой части будет больше или равен 0, т.к. мы умножаем на некую аналитическую функцию. Но порядок нуля правой части равен $k - 1$. Противоречие.

Осталось показать, почему $L(s, \chi) \neq 0$: $\left| \sum_{n=2}^{\infty} \frac{1}{n^\sigma} \right| \leq \sum_{n=2}^{\infty} \frac{1}{n^\sigma} = \frac{1}{\alpha^\sigma} \sum_{n=2}^{\infty} \frac{1}{\left(\frac{n}{2}\right)^\sigma}$ – первый множитель

стремится к 0, второй множитель ограничен некой константой $C \Rightarrow \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = 1 + \sum_{n=2}^{\infty} \frac{\chi(n)}{n^s}.$

Второе слагаемое по модулю стремится к 0 при $\sigma \rightarrow \infty$. Следовательно, $L(s, \chi) \neq 0$ для некоторого s . ■

Лемма 2.5. При $\operatorname{Re}(s) > 1$ выполнено

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s} \right)^{-1}.$$

Доказательство. Поскольку функция $\frac{\chi(p)}{p^s}$ вполне мультипликативна, то по лемме 1.4 все следует. ■

Следствие 2.2.

$$L(s, \chi_0) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right).$$

Доказательство. Подставим $\chi = \chi_0$. χ – характер по модулю $m \Rightarrow \chi(p) = 0 \Leftrightarrow p|m$. $\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$, однако это представление верно только при $\operatorname{Re}(s) > 1$. Равенство везде следует из аналитичности L -функции, ζ -функции и $\left(1 - \frac{1}{p^s}\right)$. ■

Замечание. Обобщенная гипотеза Римана звучит, что с некоторой оговоркой все нули L -функции Дирихле лежат на $\operatorname{Re}(s) = \frac{1}{2}$.

Следствие 2.3. В $\operatorname{Re}(s) > 0$ у $L(s, \chi_0)$ ровно один полюс в $s = 1$ порядка 1 с вычетом $\frac{\varphi(m)}{m}$, и в $\{\operatorname{Re}(s) > 0\} \setminus \{1\}$ функция $L(s, \chi_0)$ аналитична.

Доказательство. Вспомним, что $\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$. У $\zeta(s)$ вычет в 1 равен 1, и функция $\left(1 - \frac{1}{p^s}\right)$ аналитична в 1. ■

Лемма 2.6. Если $\chi \neq \chi_0$, то $L(s, \chi)$ аналитична при $\operatorname{Re}(s) > 0$ (то есть полюс пропадает!).

Доказательство. Применим преобразование Абеля к $a_n = \chi(n)$, $g(x) = \frac{1}{x^s}$. Тогда $A(x) = \sum_{n \leq x} a_n = \sum_{n \leq x} \chi(n)$, и используя следствие 2.1 $|A(x)| \leq \varphi(m)$.

$$\sum_{n=1}^N \frac{\chi(n)}{n^s} = A(N) \frac{1}{N^s} + s \int_1^N \frac{A(x)}{x^{s+1}} dx.$$

Так как $|A(N)| \leq \varphi(m)$, то первое слагаемое стремится к 0 при $N \rightarrow \infty$ и $\operatorname{Re}(s) > 0$.

Рассмотрим $\int_1^N \frac{A(x)}{x^{1+s}} = \sum_{n=1}^{N-1} \varphi_n(s)$, где $\varphi_n(s) = \int_n^{n+1} \frac{A(x)}{x^{1+s}} -$ аналитическая в \mathbb{C}^5

Покажем, что ряд $\sum_{n=1}^{\infty} \varphi_n(s)$ задает аналитическую функцию в $\operatorname{Re}(s) > 0$. При $\operatorname{Re}(s) > \delta > 0$

$$|\varphi_n(s)| \leq \int_n^{n+1} \frac{\varphi(m)}{x^{1+\sigma}} dx \leq \frac{\varphi(m)}{n^{2+\sigma}} < \frac{\varphi(m)}{n^{2+\delta}} - \text{общий член сходящегося ряда} \Rightarrow$$

$\sum_{n=1}^{\infty}$ сходится равномерно при $\operatorname{Re}(s) > \delta \Rightarrow$ по теореме Вейерштрасса ряд сходится к аналитической функции.

Тогда в предыдущем равенстве

$$\sum_{n=1}^N \frac{\chi(n)}{n^s} = A(N) \frac{1}{N^s} + s \int_1^N \frac{A(x)}{x^{1+s}} dx$$

⁵Упражнение!

первое слагаемое стремится к 0, а второе сходится к аналитической функции, значит и вся сумма стремится к аналитической функции. ■

Лемма 2.7. При $\chi \neq \chi_0$ выполнено $L(1, \chi) \neq 0$.

Доказательство.

Случай 1: $\chi^2 \neq \chi_0$. По лемме 1.8 из I части

$$|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})| \leq 1 \text{ при } 0 < r < 1.$$

Положим $r = \frac{1}{p^\sigma}$, $e^{i\varphi} = \chi(p)$ для каждого простого p .

Тогда при $\sigma > 1$:

$$|L^3(\sigma, \chi_0)L^4(\sigma, \chi)L(\sigma, \chi^2)| = \prod_p \left| \left(1 - \frac{\chi_0(p)}{p^\sigma}\right)^3 \left(1 - \frac{\chi(p)}{p^\sigma}\right)^4 \left(1 - \frac{\chi^2(p)}{p^\sigma}\right) \right|^{-1} \geq 1.$$

Поскольку $\chi^2 \neq \chi_0$, то у $L(\sigma, \chi^2)$ в 1 есть значение. Предположим, что $L(1, \chi) = 0$. Тогда $L(\sigma, \chi) = O(\sigma - 1)$ при $\sigma \rightarrow 1 + 0$.

При этом $L(\sigma, \chi_0) = O(\frac{1}{\sigma - 1})$ при $\sigma \rightarrow 1 + 0$ – полюс порядка 1.

$L(\sigma, \chi^2) = O(1)$, т.к. $\chi^2 \neq \chi_0$. Отсюда $|L^3(\sigma, \chi_0)L^4(\sigma, \chi)L(\sigma, \chi^2)| = O(\frac{1}{(\sigma - 1)^3}(\sigma - 1)^4 \cdot 1) = O(\sigma - 1)$ при $\sigma \rightarrow 1 + 0$, т.е. $\rightarrow 0$, что противоречит неравенству выше.

Случай 2: $\chi^2 = \chi_0$.

Заметим, что если рассуждать похожим образом, то мы получим $O(1)$, и ничего не выйдет.

Пусть $L(1, \chi) = 0$. Рассмотрим $F(s) = \zeta(s)L(s, \chi)$. Первая функция дает в точке 1 имеет полюс порядка 1, а вторая в точке 1 дает ноль порядка 1, значит она аналитична при $\operatorname{Re}(s) > 1$. Докажем, что

- 1) ряд $F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ сходится абсолютно при $\operatorname{Re}(s) > 1$, причем $F^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \frac{\ln(n)^k a_n}{n^s}$,
- 2) $a_n \geq 0$,
- 3) $a_{r^2} \geq 1, \forall r \in \mathbb{N}$,
- 4) $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ расходится при $s = \frac{1}{2}$.

Пункт 1):

Надо доказать, что $\sum_{n=1}^{\infty} \frac{|a_n|}{n^s}$ сходится при $\operatorname{Re}(s) > 1$. При $\operatorname{Re}(s) > 1 + \delta, \delta > 0$ выполнено $\frac{a_n}{n^s} \leq \frac{|a_n|}{n^\sigma} <$

$\frac{|a_n|}{n^{1+\delta}}$ – общий член сходящегося ряда. Следовательно, по признаку Вейерштрасса ряд $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ сходится равномерно. Но тогда по Теореме 1.4 Вейерштрасса этот ряд задаёт аналитическую функцию, причём его можно почленно дифференцировать.

Пункт 2):

$$a_n = \sum_{d|n} \chi(d) = \prod_{j=1}^r \sum_{\beta_j=0}^{a_j} \chi(p_j)^{\beta_j} = \prod_{j=1}^r a_{n_j},$$

$$\text{где } a_{n_j} = 1 + \chi(p_j) + \dots + \chi(p_j)^{\alpha_j} = \begin{cases} 1, & \chi(p_j) = 0, \\ \frac{1 - \chi(p_j)^{1+\alpha_j}}{1 - \chi(p_j)}, & \chi(p_j) \neq 0, 1, \\ 1 + \alpha_j, & \chi(p_j) = 1. \end{cases}$$

То есть

$$a_{n_j} = \begin{cases} 1 + \alpha_j, & \chi(p_j) = 1, \\ 1, & \chi(p_j) = 0 \text{ или } \chi(p_j) = -1, \alpha_j \neq 2, \\ 0, & \chi(p_j) = -1, \alpha_j \neq 2. \end{cases}$$

Из того, что $a_{n_j} \geq 0$, следует $a_n \geq 0$.

Пункт 3): Очевидно из 2).

Пункт 4): Следует из 2) и 3).

$F(s)$ аналитична в $\operatorname{Re}(s) > 0$, поэтому в круге $|s - 2| < 2$ на вещественной прямой выполняется

$$\begin{aligned} F(\sigma) &= \sum_{k=0}^{\infty} \frac{F^{(k)}(2)}{k!} (\sigma - 2)^k = \sum_{k=0}^{\infty} \frac{(\sigma - 2)^k}{k!} \sum_{n=1}^{\infty} (-1)^k \frac{(\ln n)^k a_n}{n^2} = \sum_{k=0}^{\infty} \frac{(2 - \sigma)^k}{k!} \sum_{n=1}^{\infty} \frac{(\ln n)^k a_n}{n^2} = \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n^2} \sum_{k=0}^{\infty} \frac{(\ln n)^k (2 - \sigma)^k}{k!} = \sum_{n=1}^{\infty} \frac{a_n}{n^2} n^{2-\sigma} = \sum_{n=1}^{\infty} \frac{a_n}{n^{\sigma}}. \end{aligned}$$

В частности, при $\sigma = \frac{1}{2}$: $F\left(\frac{1}{2}\right) = \sum_{n=1}^{\infty} \frac{a_n}{n^{\frac{1}{2}}}$. Но мы доказали, что он расходится. Противоречие. ■

Доказательство. (Теоремы 2.1 Дирихле). При $\operatorname{Re}(s) > 1$ $-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}$.

Пусть далее $s = \sigma \in \mathbb{R}$, $s > 1$. $\Lambda(n) = \begin{cases} \ln p, & n = p^k, k \geq 1, \\ 0, & \text{иначе.} \end{cases}$ Тогда

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_p \frac{\ln p \chi(p)}{p^s} + \sum_p \sum_{k=2}^{\infty} \frac{\ln p \cdot \chi(p^k)}{p^{ks}}$$

(первое слагаемое для $n = p$, второе – для $n = p^k$). Покажем, что второе слагаемое ограничено константой, не зависящей от s при $s > 1$:

$$\left| \sum_p \sum_{k=2}^{\infty} \frac{\ln p \cdot \chi(p^k)}{p^{ks}} \right| \leq \sum_p \sum_{k=2}^{\infty} \frac{\ln p}{p^{ks}} = \sum_p \ln p \frac{1/p^2}{1 - 1/p} \leq 2 \sum_p \frac{\ln p}{p^2} < 2 \sum_n \frac{\ln n}{n^2} < \infty.$$

Итак, для любого характера χ по модулю m :

$$\sum_p \frac{\chi(p) \ln p}{p^s} = -\frac{L'(s, \chi)}{L(s, \chi)} + O(1). \quad (*)$$

Поскольку $(l, m) = 1$, то $\exists v \in \mathbb{Z} : vl \equiv 1 \pmod{m}$ (т.е. обратный). Домножим (*) на $\chi(v)$ и просуммируем по всем характерам:

$$\sum_p \frac{\ln p}{p^s} \sum_{\chi} \chi(pv) = - \sum_{\chi} \chi(v) \frac{L'(s, \chi)}{L(s, \chi)} + O(1),$$

$$\sum_{\chi} \chi(pv) = \begin{cases} 0, & pv \not\equiv 1 \pmod{m}, \\ \varphi(m), & pv \equiv 1 \pmod{m}. \end{cases}$$

Но $pv \equiv 1 \pmod{m}$, следовательно, $p \equiv l \pmod{m}$ т.к. $pl \equiv 1 \pmod{m}$. Значит,

$$\sum_{p \equiv l \pmod{m}} \frac{\ln p}{p^s} = -\frac{1}{\varphi(m)} \sum_{\chi} \chi(v) \frac{L'(s, \chi)}{L(s, \chi)} + O(1).$$

Перейдём к пределу при $s \rightarrow 1+$. Если $p \equiv l \pmod{m}$ конечное количество, то слева предел конечен. Докажем, что правая часть стремится к бесконечности (т.е. в левой части бесконечное число слагаемых):

При $\chi \neq \chi_0$ $\frac{L'(s, \chi)}{L(s, \chi)} = O(1)$ при $s \rightarrow 1+$.

При $\chi = \chi_0$ $L(s, \chi) = \frac{f(s)}{s-1}$, где $f(s)$ аналитична в 1 и $f(1) \neq 0$.

Значит,

$$\frac{L'(s, \chi_0)}{L(s, \chi_0)} = -\frac{1}{s-1} + \frac{f'(s)}{f(s)} = -\frac{1}{s-1} + O(1) \xrightarrow{\text{при } s \rightarrow 1+} \infty.$$

То есть мы показали, что правая часть стремится к бесконечности при $s \rightarrow 1+$. Следовательно,

$$\sum_{p \equiv l \pmod{m}} \frac{\ln p}{p^s} = \frac{1}{\varphi(m)(s-1)} + O(1).$$

Из последнего равенства можно, в частности, получить, что $\sum_p \frac{\ln p}{p^s} = \frac{1}{s-1} + O(1)$. ■

Each lecture
should begin
with Dirichlet's
approximation
theorem



3.1 Основные сведения

Пусть $\theta \in \mathbb{R}$. Насколько маленькой можно сделать разность $|\theta - \frac{p}{q}|$ так, чтобы $|\theta - \frac{p}{q}| < f(a)$ (p и q — не простые).

Характеристика θ : насколько хорошо она приближается $\frac{p}{q}$. Мы знаем, что существуют иррациональные числа ($\sqrt{2}, \sqrt{3}, \dots$). Легко доказать, что корни многочленов с целыми коэффициентами (алгебраические числа) не будут рациональными. Например, у многочлена $x^2 - x - 1 = 0$ корень $\varphi = \frac{1+\sqrt{5}}{2}$, а у него корни имеют вид $\frac{\text{делитель} - 1}{\text{делитель} 1} \in \{\pm 1\}$ — ± 1 оба не корни.

А вдруг все числа алгебраические? Нет, алгебраических чисел счётное количество. Это доказал Ливуилль через теорию приближений: он показал, что алгебраические числа не могут приближаться "слишком хорошо". Т.е. для алгебраических чисел не найдётся такой f , для которой будет бесконечно много решений.

Утверждение 3.1. Если $\theta = \frac{a}{b} \in \mathbb{R}$, то $\forall \frac{p}{q} \in \mathbb{Q} \setminus \{0\}$ такая, что $\left| \theta - \frac{p}{q} \right| > \frac{1/b}{q}$.

Доказательство. $\left| \frac{a}{b} - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}$, т.к. $|aq - bp| \in \mathbb{Z} \neq 0$. ■

Теорема 3.1 (Дирихле о приближении).

Пусть $\theta \in \mathbb{R}$, $T \in \mathbb{N}$. Тогда $\exists \frac{p}{q} \in \mathbb{Q} : \left| \theta - \frac{p}{q} \right| < \frac{1}{qT}$, $1 \leq q \leq T$.

Доказательство.

Хотим: $|q\theta - p| < \frac{1}{T}$. Можно считать, что $\theta \in [0, 1)$, потом просто прибавить целую часть.

Рассмотрим числа $\{n\theta\}$, $n = 0, 1, \dots, T$. Разобьём отрезок $[0, 1]$ на полуинтервалы $\left[\frac{k}{T}, \frac{k+1}{T}\right)$, $k = 0, 1, \dots, T-1$ (т.е. на T равных). По принципу Дирихле $\exists n_1, n_2 : (n_1 - n_2)\theta - ([n_1\theta] - [n_2\theta]) < \frac{1}{T}$. Остаётся положить $q = n_1 - n_2$, $p = [n_1\theta] - [n_2\theta]$; $q \geq 1$, $q \leq T$ (т.е. $n_1, n_2 \leq T$). ■

Следствие 3.1. Если $\theta \in \mathbb{R} \setminus \mathbb{Q}$, то неравенство $|\theta - \frac{p}{q}| < \frac{1}{q^2}$ имеет бесконечно много решений в $\frac{p}{q} \in \mathbb{Q}$.

Доказательство. От противного: пусть $\frac{p_1}{q_1}, \dots, \frac{p_k}{q_k}$ – все решения $|\theta - \frac{p}{q}| < \frac{1}{q^2}$. Положим $\delta = \min_i |\theta - \frac{p_i}{q_i}| > 0$, $T = \lceil \frac{1}{\delta} \rceil$ (любое $T > \frac{1}{\delta}$). По теореме 3.1 Дирихле $\exists \frac{p}{q}$, $q \leq T$: $|\theta - \frac{p}{q}| < \frac{1}{qT} \leq \frac{1}{q^2}$. Т.е. $\frac{p}{q}$ должно быть среди $\frac{p_i}{q_i}$. Но $|\theta - \frac{p}{q}| < \frac{1}{qT} < \frac{\delta}{q} \leq \delta$, т.е. оно ближе, чем наименьшее δ . Противоречие. ■

Мера иррациональности числа $\theta = \sup_s : \{|\theta - \frac{p}{q}| < \frac{1}{q^s}\}$ имеет бесконечно много решений $\frac{p}{q}$.

В качестве $\frac{p}{q}$ можно брать подходящие дроби в разложении θ в цепную дробь.

Определение 3.1. Иррациональное число θ называется *плохо приближаемым*, если $\exists C = C(\theta) > 0$ такое, что $\forall \frac{p}{q}$ выполняется $|\theta - \frac{p}{q}| \geq \frac{C}{q^2}$.

Известно (существует такая теорема), что число плохо приближаемо тогда и только тогда, когда неполные частные при разложении в цепную дробь ограничены. Например, для квадратичной иррациональности неполные частные периодичны⁶, а значит и ограничены, т.е. квадратичные иррациональности плохо приближаемы.

Отныне и далее мы будем подразумевать, что θ – вещественное число, а α – комплексное.

Определение 3.2. Число $\alpha \in \mathbb{C}$ называется *алгебраическим*, если существует ненулевой многочлен $f(x)$ с рациональными (или целыми) коэффициентами такой, что $f(\alpha) = 0$. Такой многочлен $f(x)$ называется *аннулирующим многочленом для числа α* .

Определение 3.3. Степенью алгебраического числа $\deg \alpha$ называется минимальная степень аннулирующего многочлена.

Теорема 3.2 (Лиувилля). Пусть θ – вещественное алгебраическое число степени d . Тогда $\exists C = C(\theta) > 0$ такое, что для любого $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$ справедливо $|\theta - \frac{p}{q}| \geq \frac{C}{q^d}$, или, другими словами, $\mu(\theta) \leq d$.

Доказательство. Случай $d = 1$ уже доказан в первом утверждении в разделе.

Пусть далее $\theta \notin \mathbb{Q}$. Рассмотрим многочлен $f(x)$ степени d с целыми коэффициентами такой, что $f(\theta) = 0$.

⁶Теорема Лагранжа с 1-го курса

Заметим, что для любого $\frac{p}{q} \in \mathbb{Q}$ выполнено $f\left(\frac{p}{q}\right) \neq 0$. Действительно, так как иначе бы многочлен $\frac{f(x)}{x - \frac{p}{q}}$ был бы аннулирующим многочленом для α степени $d - 1$.

Поскольку $f(x)$ с целыми коэффициентами, то $q^d f\left(\frac{p}{q}\right) \in \mathbb{Z} \Rightarrow \left|q^d f\left(\frac{p}{q}\right)\right| \geq 1 \Rightarrow \left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$.

Если $\left|\theta - \frac{p}{q}\right| \geq 1$, то для любого $\frac{p}{q}$ $\left|\theta - \frac{p}{q}\right| \geq \frac{1}{q^d}$.

Пусть теперь $\left|\theta - \frac{p}{q}\right| < 1$, т.е. $\frac{p}{q} \in [\theta - 1, \theta + 1]$. Тогда

$$\frac{1}{q^d} \leq \left|f\left(\frac{p}{q}\right)\right| = \left|f\left(\frac{p}{q}\right) - f(\theta)\right| = \left|\left(\frac{p}{q} - \theta\right) f'(\xi)\right| \leq M \cdot \left|\theta - \frac{p}{q}\right|, \text{ где } M = \max_{[\theta-1, \theta+1]} |f'(x)|.$$

Таким образом, $\left|\theta - \frac{p}{q}\right| \geq \frac{1}{Mq^d}$, и искомое $C = \min\left(1, \frac{1}{M}\right)$. ■

Определение 3.4. Если $\theta \in \mathbb{R}$ таково, что $\forall n \in \mathbb{N}$ неравенство $\left|\theta - \frac{p}{q}\right| < \frac{1}{q^n}$ имеет бесконечное количество решений в $\frac{p}{q} \in \mathbb{Q}$, то число θ называется *луивиллевым* (= число Луивилля). Числа, не являющиеся луивиллевыми, называются *диофантовыми*.

Предложение 3.1. Луивиллевы числа трансцендентны.

Доказательство. Предположим противное, т.е. пусть θ алгебраическое. Тогда для него верна теорема Луивилля, а именно

$$\exists C > 0 : \forall \frac{p}{q} \in \mathbb{Q} \setminus \{0\} \text{ выполнено } \left|\theta - \frac{p}{q}\right| \geq \frac{C}{q^d}.$$

Тогда при $n \geq d$ из неравенства $\left|\theta - \frac{p}{q}\right| < \frac{1}{q^{n+1}}$ следует, что $q \leq \frac{1}{C}$.

Кроме того, $|q\theta - p| \leq 1 \Rightarrow |p| \leq 1 + q|\theta| < 1 + \frac{|\theta|}{C}$.

То есть числа q и p ограничены, значит и количество решений. Противоречие. ■

Пример 3.1. Число $\theta = \sum_{n=0}^{\infty} \frac{1}{2^n!}$ - луивиллево.

Доказательство. Пусть $m \in \mathbb{N}$. Рассмотрим $N \geq m$. Обозначим через $\frac{p}{q} = \sum_{n=1}^N \frac{1}{2^n!}$. Тогда $\left|\theta - \frac{p}{q}\right| =$

$$\sum_{n=N+1}^{\infty} \frac{1}{2^n!} \leq 2 \cdot \frac{1}{2^{(N+1)!}} = \frac{2}{q^{N+1}} \leq \frac{1}{q^N} \leq \frac{1}{q^m}.$$

Таким образом, неравенство $\left|\theta - \frac{p}{q}\right| \leq \frac{1}{q^m}$ имеет бесконечное число решений. ■

Кругозора ради добавим, что существует следующая очень сложная

Теорема 3.3 (Туэ-Зигеля-Рота). Пусть θ - иррациональное алгебраическое число. Тогда $\forall \varepsilon > 0$ такое, что $\exists C = C(\theta, \varepsilon)$, что для любых $\frac{p}{q} \in \mathbb{Q}$ справедливо

$$\left|\theta - \frac{p}{q}\right| \geq \frac{C}{q^{2+\varepsilon}} = \frac{2}{q^{N+1}} \leq \frac{1}{q^N} \leq \frac{1}{q^m}.$$

Таким образом, неравенство $\left| \theta - \frac{p}{q} \right| \leq \frac{1}{q^m}$ имеет бесконечное количество решений.

3.2 Иррациональность e и π

Теорема 3.4. $e \notin \mathbb{Q}$.

Доказательство. Вспомним, что $e = \sum_{n=0}^{\infty} \frac{1}{n!}$. Пусть $e = \frac{p}{q} \in \mathbb{Q}$. Тогда $q!e \in \mathbb{N}$. Несложно видеть, что

$$\mathbb{N} \ni \sum_{n=q+1}^{\infty} \frac{q!}{n!} = \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+1)(q+2)(q+3)} + \dots < \sum_{k=1}^{\infty} \frac{1}{(q+1)^k} \leq 1.$$

Получаем противоречие. ■

Теорема 3.5. $\pi \notin \mathbb{Q}$.

Доказательство. Пусть $\pi = \frac{p}{q}$, $p, q \in \mathbb{N}$. Положим $f_n(x) = q^n \frac{x^n(\pi - x)^n}{n!} = \frac{x^n(q - px)^n}{n!} = \frac{q(x)}{n!}$, где $g(x) \in \mathbb{Z}[x]$.

Рассмотрим $I_n = \int_0^{\pi} f_n(x) \sin(x) dx$, $I_n \geq 0$.

Положим $F_n(x) = f_n(x) - f_n''(x) + f_n^{(4)}(x) - \dots = \sum_{k=0}^{\infty} (-1)^k f_n^{(2k)}(x)$.

Поскольку $f_n(x) = f_n(\pi - x)$, то $f_n^{(k)}(x) = f_n^{(k)}(\pi - x)$ для чётных k . Из этого мы видим, что $F_n(x) = F_n(\pi - x)$.

Заметим, что $(F_n'(x) \sin x - F_n(x) \cos x)' = f_n(x) \sin x$.

$I_n = (F_n'(x) \sin x - F_n(x) \cos x)_0^{\pi} = F_n(0) + F_n(\pi)$.

$$|f(x) \sin x| \leq \frac{b^n \left(\frac{\pi}{2}\right)^{2n}}{n!} \rightarrow 0 \text{ при } n \rightarrow \infty,$$

$$I_n = 2F_n(0) = 2 \sum_{k=0}^{\infty} (-1)^k f^{(2k)}(0) \in \mathbb{Z}.$$

Итак, последовательность $\{I_n\}$ положительна, целочисленна, и стремится к нулю, в чём и заключается противоречие. ■

3.3 Трансцендентность числа e

Теорема 3.6. Число e трансцендентно.

Доказательство. Предположим противное: пусть $\exists a_0, \dots, a_m \in \mathbb{Z} : \sum_{k=0}^m a_k e^k = 0$, где не все $a_k = 0$.

Считаем, что $(a_0, \dots, a_m) = 1$. Ортогональным дополнением к (a_0, \dots, a_m) является полуплоскость Π , проходящая через $(1, e, e^2, \dots, e^m)$. При этом в гиперплоскости можно выбрать базис из целочисленных векторов.

Разбиваем все точки \mathbb{Z}^{m+1} на параллельные слои \mathbb{Z}^m (любое $b \in \mathbb{Z}^{m+1}$ лежит в слое с номером $\langle a, b \rangle$). Расстояние между слоями одинаковое и (при условии, что $(a_0, \dots, a_m) = 1$) оно равно $\Delta = \frac{1}{\sqrt{a_0^2 + a_1^2 + \dots + a_m^2}}$. Построим последовательность $\mathcal{B}^{(n)} \in \mathbb{Z}^{m+1}$ такую, что

- 1) расстояние от $\mathcal{B}^{(n)}$ до $\langle (1, e, e^2, \dots, e^m) \rangle$ меньше Δ ,
- 2) точка $\mathcal{B}^{(n)}$ не лежит в Π .

Напомним, что $\int_0^\infty x^k e^{-x} dx = \Gamma(k+1) = k!$ Тогда можно брать $\int_0^\infty f(x) e^{-x} dx$ для многочленов f .

Положим $f_n(x) = \frac{x^{n-1}(x-1)^n \dots (x-m)^n}{(n-1)!}$. Возьмём $\mathcal{B}_k^{(n)} = \int_0^{+\infty} f_n(x+k) e^{-x} dx$, $k = 0, \dots, m$.

Покажем, что $\mathcal{B}_0^{(n)} e^k - \mathcal{B}_k^{(n)} \xrightarrow{n \rightarrow \infty} 0$:

$$\text{При } k = 0 \text{ это просто } 0. \text{ Пусть } k \neq 0: \left| \mathcal{B}_0^{(n)} e^k - \mathcal{B}_k^{(n)} \right| = \left| e^k \int_0^\infty f_n(x) e^{-x} dx - \int_0^\infty f_n(x+k) e^{-x} dx \right| =$$

$$e^k \left| \int_0^\infty f_n(x) e^{-x} dx - \int_k^\infty f_n(y) e^{-y} dy \right| = e^k \left| \int_0^k f_n(x) e^{-x} dx \right| \leq e^m m \frac{m^{n+nm-1}}{(n-1)!} = \frac{e^m m^{m(n+1)}}{(n-1)!} \xrightarrow{n \rightarrow \infty} 0.$$

То есть $\mathcal{B}_0^{(n)} (1, e, e^2, \dots, e^m)^T - \mathcal{B}^{(n)} \xrightarrow{n \rightarrow \infty} 0$. Следовательно, последовательность точек $\mathcal{B}^{(n)}$ стремится к прямой $\langle (1, e, e^2, \dots, e^m) \rangle$ и, начиная с некоторого n , расстояние станет меньше Δ .

Покажем теперь, что $\mathcal{B}_k^{(n)} \in \mathbb{Z}$, где $k = 0, \dots, m$:

При $k = 0$:

$$\mathcal{B}_0^{(n)} = \frac{1}{(n-1)!} \sum_k \left[\text{коэффициент в } x^{n-1}(x-1)^n \dots (x-m)^n \text{ при } x^k \right] \cdot \int_0^\infty x^k e^{-x} dx =$$

$$= \frac{1}{(n-1)!} ((-1)^{mn} m!^n (n-1)! + A_n n! + \dots + A_N N!) \equiv (-1)^{mn} m!^n \pmod{n}.$$

При $k \geq 1$:

$$\mathcal{B}_k^{(n)} = \int_0^{+\infty} f_n(x+k) e^{-x} dx = \sum_j \left[\text{коэффициент в } \frac{(x+k)^{n-1}(x+k-1)^n \dots x^n \dots}{(n-1)!} \text{ при } x^j \right] \cdot j! =$$

$$\frac{1}{(n-1)!} (C_n n! + C_{n+1} (n+1)! + \dots + C_N N!) \equiv 0 \pmod{n}.$$

Покажем, наконец, что для бесконечно многих n $\sum_{k=0}^m a_k \mathcal{B}_k^{(n)} \neq 0$ (то есть, что $\mathcal{B}^{(n)} \notin \Pi$):

$$\sum_{k=0}^m a_k \mathcal{B}_k^{(n)} \equiv a_0 (-1)^{mn} m!^n \pmod{n}.$$

Тогда при $(n, a_0 m!) = 1$, где $a_0 m!$ – некоторое фиксированное число, ряд будет не равен нулю. ■

4 Алгебраические и трансцендентные числа

4.1 Основные сведения

Множество алгебраических чисел будем обозначать \mathbb{A} .

Пусть $f(x) \in \mathbb{Q}[x]$, $f(\alpha) = 0$, $\deg f = \deg \alpha$. Тогда $f(x)$ неприводим над \mathbb{Q} . Следовательно, если $g(x) \in \mathbb{Q}[x]$, $g(\alpha) = 0$, $\deg g = \deg \alpha (= \deg f)$, то $\text{НОД}(f(x), g(x)) = h(x) \in \mathbb{Q}[x]$, при этом $h(\alpha) = 0 = \deg h = \deg f$, то есть, если $h|f$, $h|g$, $\deg h = \deg f = \deg g$ то они три все пропорциональны.

Определение 4.1. Унитарный многочлен $p_\alpha(x) \in \mathbb{Q}[x]$ называется *минимальным многочленом* α , если $p_\alpha(\alpha) = 0$ и $\deg p_\alpha = \deg \alpha$.

Оказывается, что \mathbb{A} – алгебраически замкнутое поле, т.е. корень многочлена с алгебраическими коэффициентами тоже будет алгебраическим числом.

Для доказательства нам сначала понадобятся несколько лемм.

Теорема 4.1 (О симметрических многочленах).

Пусть R – ассоциативное коммутативное кольцо с единицей и без делителей нуля.

Пусть $f(x_1, \dots, x_m) \in R[x_1, \dots, x_m]$ – симметрический многочлен.

Тогда $\exists g(x_1, \dots, x_m) \in R[x_1, \dots, x_m] : f(x_1, \dots, x_m) = g(s_1(x_1, \dots, x_m), \dots, s_m(x_1, \dots, x_m))$, где $s_k(x_1, \dots, x_m)$ – k -ый симметрический многочлен.

Лемма 4.1. Пусть $f(x, y) \in R[x, y]$. Тогда $\exists g(x, y_1, \dots, y_m) \in R[x, y_1, \dots, y_m] : f(x, y_1) \cdot \dots \cdot f(x, y_m) = g(x, s_1(y_1, \dots, y_m), \dots, s_m(y_1, \dots, y_m))$.

Доказательство. $f(x, y_1) \cdot \dots \cdot f(x, y_m) \in R[x][y_1, \dots, y_m]$, т.е. он симметричный по y_1, \dots, y_m над $R[x]$. По Теореме 4.1 существует искомый многочлен g , причём g – многочлен от (x, y_1, \dots, y_m) над R . ■

Лемма 4.2. Пусть $f(x, y) \in \mathbb{Q}[x, y]$, $\alpha \in \mathbb{A}$, $\deg \alpha = n$, $\alpha_1 = \alpha$, $\alpha_2, \dots, \alpha_n$ – корни $p_\alpha(x)$ ⁷. Тогда $F(x) = \prod_{k=1}^n f(x, \alpha_k) \in \mathbb{Q}[x]$.

Доказательство. Применим Лемму 4.1:

$$\prod_{k=1}^n f(x, \alpha_k) = g(s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n)).$$

По теореме Виета все $s_i(\alpha_1, \dots, \alpha_n)$ выражаются через коэффициенты многочлена p_α и, следовательно, $s_i(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$. ■

Теорема 4.2. \mathbb{A} – поле.

Доказательство. Пусть $\alpha, \beta \in \mathbb{A}$. Хотим проверить что $\{\alpha @ \beta | @ \in \{+, -, /, \cdot\}\}$.

Сложение:

Рассмотрим $F_1(x) = \prod_{k=1}^m p_\alpha(x - \beta_k)$, где $\beta_1 = \beta$, β_2, \dots, β_m – корни $p_\beta(x)$. Тогда по Лемме 4.2:

⁷Они попарно различны как корни любого неприводимого многочлена $f(x)$. Иначе бы у $f'(x)$ и $f(x)$ был этот корень общим, но $\deg(f') < \deg(f)$ – противоречие с неприводимостью.

$F_1(x) \in \mathbb{Q}[x]$. При этом $F_1(\alpha + \beta) = \dots p_\alpha(\alpha) \dots = 0$.

Вычитание:

Если β – алгебраическое, то алгебраическим будет и $-\beta$. Тогда $\alpha - \beta$ – тоже алгебраическое. Ну или так: $F_2(x) = \prod_{k=1}^m p_\alpha(x + \beta) \in \mathbb{Q}[x]$, $F_2(\alpha - \beta) = 0$.

Деление:

$$F_3(x) = \prod_{k=1}^m p_\alpha(x\beta_k) \in \mathbb{Q}[x], F_3\left(\frac{\alpha}{\beta}\right) = 0.$$

Умножение:

$$F_4(x) = \prod_{k=1}^m \beta_k^m p_\alpha\left(\frac{x}{\beta_k}\right) \in \mathbb{Q}[x], F_4(\alpha\beta) = 0. \quad \blacksquare$$

4.2 Целые алгебраические числа

Определение 4.2. Алгебраическое число α называется *целым алгебраическим*, если $p_\alpha(x) \in \mathbb{Z}[x]$. Множество всех целых алгебраических чисел обозначим через $\mathbb{Z}_\mathbb{A}$.

Пример 4.1.

- Пусть $\alpha \in \mathbb{Q}$. Тогда $\alpha \in \mathbb{Z}_\mathbb{A} \Leftrightarrow \alpha \in \mathbb{Z}$.
- $\sqrt{2} \in \mathbb{Z}_\mathbb{A}$
- $a, b, d \in \mathbb{Z} \Rightarrow a + b\sqrt{d} \in \mathbb{Z}_\mathbb{A}$
- $\frac{1+\sqrt{5}}{2} \in \mathbb{Z}_\mathbb{A}$

Определение 4.3. Многочлен $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ называется *примитивным*, если $(a_n, a_{n-1}, \dots, a_1, a_0) = 1$.

Лемма 4.3 (Гаусса). *Произведение примитивных многочленов примитивно.*

Доказательство. Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + a_1 x + a_0$, $g(x) = b_m x^m + b_{m-1} x^{m-1} + b_1 x + b_0$.

А также рассмотрим $h(x) = f(x)g(x) = c_{m+n} x^{m+n} + \dots + c_1 x + c_0$.

Пусть существует простое p такое, что $p|c_k, \forall 0 \leq k \leq m+n$.

Пусть $r = \min k|a_k|p, s = \min k|b_k|p$.

Тогда $c_{r+s} = \sum_{i+j=r+s} a_i b_j \equiv a_r b_s \not\equiv 0 \pmod p$, т.е. $p \nmid c_{r+s}$. Получаем противоречие. ■

Теорема 4.3. *Если существует унитарный многочлен $f(x) \neq 0 \in \mathbb{Z}[x] : f(\alpha) = 0$, то $\alpha \in \mathbb{Z}_\mathbb{A}$.*

Доказательство. $p_\alpha(x)|f(x)$ в $\mathbb{Q}[x]$, т.е. $\exists g(x) \in \mathbb{Q}[x] : f(x) = g(x)p_\alpha(x)$.

Покажем, что $g(x), p_\alpha(x) \in \mathbb{Z}[x]$.

Пусть A, B – НОК знаменателей коэффициентов $g(x)$ и $p_\alpha(x)$ соответственно. Тогда $Ag(x)$ и $Bp_\alpha(x)$ – примитивные многочлены.

$ABf(x) = Ag(x)Bp_\alpha(x)$ – примитивный многочлен по лемме 4.3 Гаусса. Тогда $AB = 1 \Rightarrow A = B = 1$. ■

Лемма 4.4. Пусть $f(x, y) \in \mathbb{Z}[x, y]$. Пусть $\alpha = \alpha_1, \dots, \alpha_n$ – сопряженные к $\alpha \in \mathbb{Z}_\mathbb{A}$. Тогда $F(x) = \prod_{i=1}^n f(x, \alpha_i) \in \mathbb{Z}[x]$.

Доказательство. Аналогично доказательству леммы 4.2. ■

Теорема 4.4. $\mathbb{Z}_{\mathbb{A}}$ – кольцо.

Доказательство. Пусть $\alpha, \beta \in \mathbb{Z}_{\mathbb{A}}$. Пусть $\alpha = \alpha_1, \dots, \alpha_n$ – сопряженные к α , $\beta = \beta_1, \dots, \beta_m$ – сопряженные к β . Тогда, по Лемме 4.4:

$$F_1(x) = \prod_{i=1}^m p_{\alpha}(x - \beta_i) \in \mathbb{Z}[x],$$

$$F_2(x) = \prod_{i=1}^m p_{\alpha}(x + \beta_i) \in \mathbb{Z}[x],$$

$$F_3(x) = \prod_{i=1}^m \beta_i^{\deg p_{\alpha}} p_{\alpha}(x/\beta_i) \in \mathbb{Z}[x].$$

Тогда все три многочлена унитарны и $F_1(\alpha + \beta) = F_2(\alpha - \beta) = F_3(\alpha\beta) = 0$. Применив Теорему 4.3, получаем условие теоремы. ■

Задача 4.1. $\forall \alpha \in \mathbb{A} \exists d \in \mathbb{Z}$ такое, что $d\alpha \in \mathbb{Z}_{\mathbb{A}}$.

4.3 Конечные расширения \mathbb{Q}

Пусть $\alpha_1, \dots, \alpha_n$ – произвольные алгебраические числа.

Определение 4.4. $\mathbb{Q}(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f, g \in \mathbb{Q}[x_1, \dots, x_n], g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$ – расширение \mathbb{Q} , порожденное $\alpha_1, \dots, \alpha_n$.

Задача 4.2. Доказать, что $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ – минимальное по включению поле, содержащее и \mathbb{Q} , и $\alpha_1, \dots, \alpha_n$.

Лемма 4.5. Пусть $E = \mathbb{Q}(\theta)$, $\deg(\theta) = n$. Тогда любой элемент $\alpha \in E$ однозначно представим в виде $\alpha = c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}$, $c_i \in \mathbb{Q}$.

Доказательство.

Докажем существование: рассмотрим $\alpha = \frac{f(\theta)}{g(\theta)} \in E$. Заметим, что поскольку $g(\theta) \neq 0$, то $(p_{\theta}(x), g(x)) = 1$, т.е. $\exists u(x), v(x) \in \mathbb{Q}[x] : u(x)p_{\theta}(x) + v(x)g(x) = 1$.

Тогда $u(\theta)p_{\theta}(\theta) + v(\theta)g(\theta) = 1$. Отсюда $\frac{1}{g(\theta)} = v(\theta)$ и, стало быть, $\alpha = f(\theta)v(\theta)$.

Положим $h(x) = f(x)v(x)$. Поделим $h(x)$ с остатком на $p_{\theta}(x) : h(x) = q(x)p_{\theta}(x) + r(x)$, $\deg r(x) < \deg \theta$. Тогда $\alpha = h(\theta) = r(\theta)$, $\deg r(x) < n$, $r(x) \in \mathbb{Q}[x]$.

Докажем единственность: пусть $\alpha = c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1} = d_0 + d_1\theta + d_{n-1}\theta^{n-1}$. Тогда

$(c_0 - d_0) + (c_1 - d_1)\theta + \dots + (c_{n-1} - d_{n-1})\theta^{n-1} = 0$ – обнуляющий многочлен θ степени не более $\deg(\theta) - 1$.

Следовательно, по определению $\deg(\theta): \forall i: c_i = d_i$. ■

Таким образом, $\mathbb{Q}(\theta)$ – линейное пространство над \mathbb{Q} размерности n с базисом $1, \theta, \dots, \theta^{n-1}$.

Теорема 4.5 (О примитивном элементе). Пусть $E = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Тогда $\exists \theta \in E: E = \mathbb{Q}(\theta)$.

Определение 4.5. Такое θ называется *примитивным элементом* E (над \mathbb{Q}).

Следствие 4.1. Любое конечное расширение \mathbb{Q} является конечномерным пространством над \mathbb{Q} .

Определение 4.6. Размерность E как линейного пространства над \mathbb{Q} называется *степенью расширения*. Обозначается $[E: \mathbb{Q}]$.

Обозначим $\mathbb{Z}_E = E \cap \mathbb{Z}_{\mathbb{A}}, \mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$.

Доказательство. (Теоремы 4.5)

Достаточно доказать для двух чисел: $E = \mathbb{Q}(\xi, \eta)$.

Пусть $\xi_1 = \xi, \xi_2, \dots, \xi_m$ – сопряженное к ξ , $\eta_1 = \eta, \eta_2, \dots, \eta_l$ – сопряженное к η . Возьмём $c \in \mathbb{Q}$: все числа $\xi_i + c\eta_j$ попарно различны. Положим $\theta = \xi + c\eta$, утверждается, что θ – искомое. Обозначим $K = \mathbb{Q}(\theta)$, тогда $\mathbb{Q} \subset K \subset E$ – расширение полей. Покажем, что $\xi, \eta \in K$ – отсюда будет следовать, что $E \subset K$, т.е. $E = K$.

Рассмотрим $p_\xi(x), p_\eta(x)$, пусть $f(x) = p_\xi(\theta - cx)$, где $\theta \in K, c \in \mathbb{Q}, p_\xi \in \mathbb{Q}[x]$. Тогда $f(x) \in K[x]$. Заметим, что

$$f(\eta) = p_\xi(\theta - c\eta) = p_\xi(\xi) = 0, \text{ т.е. } \eta - \text{корень } f(x).$$

Так как f и p_η оба имеют коэффициенты из K , то рассмотрим $d(x) = \text{НОД}(f(x), p_\eta(x))$. Ясно, что $d(\eta) = 0 \Rightarrow (x - \eta) | d(x)$; $p_\eta(x)$ имеет корни $\eta_1, \eta_2, \dots, \eta_l$. Поэтому, $d \subset \{\eta_1, \eta_2, \dots, \eta_l\}$.

Пусть $d(\eta_i) = 0$. Так как $d | f$, то $f(\eta_i) = 0$, но $f(\eta_i) = p_\xi(\theta - c\eta_i)$. То есть, $\theta - c\eta_i = \xi_j$ для некоторого j (корни p_ξ), но $\theta = \xi_j + c\eta_i$ только когда $i = j = 1$. Следовательно, η – единственный корень $d(x)$. Так как d делит p_η , и у p_η нет кратных корней, то $d(x) = x - \eta$. Но $d(x) \in K[x] \Rightarrow \eta \in K$. Тогда $\xi = \theta - c\eta \in K$, ведь $\theta \in K$ (по определению K), $c \in \mathbb{Q}, \eta \in K$. ■

Теорема 4.6.

Поле \mathbb{A} алгебраически замкнуто. То есть, если $f(x) \in \mathbb{A}[x]$, то $\exists \beta \in \mathbb{A}: f(\beta) = 0$.

Доказательство. Пусть $f(x) = \alpha_n x^n + \dots + \alpha_1 x + \alpha_0 \in \mathbb{A}[x]$. Так как \mathbb{A} – поле, то не теряя общности можно считать, что $\alpha_n = 1$. Рассмотрим $E = \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1}, \alpha_n)$. По теореме 4.5 о примитивном элементе: $E = \mathbb{Q}(\theta)$ для некоторого θ , $\deg(\theta) = m$. Тогда $\alpha_i = r_i(\theta)$, где $r_i(x) \in \mathbb{Q}[x]$, $\deg(r_i) \leq m - 1$. То есть

$$f(x) = x^n + r_{n-1}(\theta)x^{n-1} + \dots + r_1(\theta)x + r_0(\theta).$$

Пусть $\theta_1, \theta_2, \dots, \theta_m$ – все сопряжены к θ . Рассмотрим

$$F(x) = \prod_{j=1}^m [x^n + r_{n-1}(\theta_j)x^{n-1} + \dots + r_1(\theta_j)x + r_0(\theta_j)],$$

заметим, что $f(x, y) = x^n + r_{n-1}(y)x^{n-1} + \dots + r_1(y)x + r_0(y) \in \mathbb{Q}[x, y]$. По лемме 4.2: $F(x) \in \mathbb{Q}[x]$, при этом $f(x) | F(x)$ в $\mathbb{C}[x]$. Следовательно, все корни $f(x)$ лежат в \mathbb{A} . ■

4.4 Нормальные расширения

Определение 4.7. Пусть E – конечное расширение поля \mathbb{Q} . Отображение $\sigma: E \rightarrow \mathbb{C}$ называется *вложением*, если это инъективный гомоморфизм полей.

Теорема 4.7. Если $[E: \mathbb{Q}] = n$, то существует ровно n различных вложений E в \mathbb{C} . При этом, если $E = \mathbb{Q}(\theta)$ и $\theta_1, \dots, \theta_m$ – все сопряжённые к θ , то отображение $\sigma: E \rightarrow \mathbb{C}$ ($\alpha \cdot r(\theta) \mapsto r(\theta_i)$, где $r(x) \in \mathbb{Q}[x]$) является вложением E в \mathbb{C} .

Доказательство. Покажем, что любое $\alpha \in E$ при вложении переходит в какое-то своё сопряжённое: Пусть σ – вложение. Тогда $0 \neq \sigma(1) = \sigma(1 \cdot 1) = \sigma(1)\sigma(1) \Rightarrow \sigma(1) = 1$.

Тогда $\sigma(k) = \sigma(1 + 1 + \dots + 1) = \sigma(1) + \sigma(1) + \dots + \sigma(1) = k$, $\sigma(-1) + \sigma(1) = \sigma(0) = 0 \Rightarrow \sigma(-1) = -1$. Значит, $\forall k \in \mathbb{Z} \sigma(k) = k$.

Далее, $\forall k \in \mathbb{N} \sigma(k)\sigma(\frac{1}{k}) = \sigma(1) = 1$, откуда $\forall k \in \mathbb{Q} \sigma(k) = k$. Стало быть, если $f \in \mathbb{Q}[x]$, то $\forall \alpha \in E \sigma(f(\alpha)) = f(\sigma(\alpha))$. В частности, $p_\alpha(\sigma(\alpha)) = \sigma(p_\alpha(\alpha)) = \sigma(0) = 0 \Rightarrow \sigma(\alpha)$ – сопряжённое к α . Возьмём $\alpha = \theta$, тогда $\sigma: \theta \mapsto \theta_i$, где i зависит от σ . И тогда $\forall r(x) \in \mathbb{Q}[x]: \sigma(r(\theta)) = r(\sigma(\theta)) = r(\theta_i)$. Пусть $\sigma_i: E \rightarrow \mathbb{C}$ ($\alpha = r(\theta) \mapsto r(\theta_i)$). Почему это вложение?

Пусть $\alpha, \beta \in E$, $\alpha = r(\theta)$, $\beta = s(\theta)$, $r(x), s(x) \in \mathbb{Q}[x]$, $\deg(r) \leq n-1$, $\deg(s) \leq n-1$.

$\alpha + \beta = (r + s)(\theta)$, $\alpha \cdot \beta = u(\theta)$, где $u(x)$ – остаток от деления $r(x)s(x)$ на $p_\theta(x)$. Аналогично, $r(\theta_i)s(\theta_i) = u(\theta_i)$.

Тогда

$$\sigma_i(\alpha) + \sigma_i(\beta) = r(\theta_i) + s(\theta_i) = (r + s)(\theta_i) = \theta_i((r + s)(\theta)) = \sigma_i(\alpha + \beta).$$

$$\sigma_i(\alpha)\sigma_i(\beta) = r(\theta_i)s(\theta_i) = u(\theta_i) = \sigma_i(u(\theta)) = \sigma_i(r(\theta)s(\theta)) = \sigma_i(\alpha\beta).$$

Если $\sigma_i(\alpha) = 0$ для некоторого $\alpha \neq 0$, то $1 = \sigma_i(1 = \sigma_i(\alpha)\sigma_i(\alpha^{-1})) = 0$. Противоречие. ■

Теорема 4.8. Пусть $[E: \mathbb{Q}] = n$, $\sigma_1, \dots, \sigma_n$ – все вложения E в \mathbb{C} , $\alpha \in E$, $\deg(\alpha) = d$. Тогда $d|n$ и множество $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$ состоит из всех сопряжений к α , каждое из которых повторяется $\frac{n}{d}$ раз.

Доказательство. $\alpha = r(\theta)$, $r(x) \in \mathbb{Q}[x]$, $\deg(r) \leq n-1$. Рассмотрим $F(x) = \prod_{i=0}^n (x - \sigma_i)(\alpha)$. Тогда

$F(x) = \prod_{i=1}^n (x - r(\theta_i))$ и по лемме 4.2 $F(x) \in \mathbb{Q}[x] \Rightarrow p_\alpha(x)|F(x)$. Пусть k максимальное такое, что

$p_\alpha^k(x)|F(x)$. Рассмотрим $\frac{F(x)}{p_\alpha^k(x)} = g(x) \in \mathbb{Q}[x]$. Если у g есть корни (если $g \neq \text{const}$), то его корни – какие-то сопряжённые с α . Следовательно, $p_\alpha(x)|g(x)$ – противоречие с максимальнойностью k . Значит, $g(x) = 1$, $F(x) = p_\alpha^k(x)$, $n = kd$. ■

Следствие 4.2. $\sigma(\alpha) = \alpha$ при всех вложениях E в $\mathbb{C} \Leftrightarrow \alpha \in \mathbb{Q}$.

Доказательство.

(\Leftarrow) Очевидно.

(\Rightarrow) Из теоремы 4.8. ■

Определение 4.8. Если для любого вложения σ расширения E справедливо $\sigma(E) = E$, то E называется *нормальным*.

Лемма 4.6. Пусть E – конечное расширение \mathbb{Q} , σ – вложение E в \mathbb{C} . Пусть $\sigma(E) \subset E$. Тогда $\sigma(E) = E$.

Доказательство. E – конечномерное линейное пространство над \mathbb{Q} , $\sigma : E \rightarrow E$ – линейное отображение с нулевым ядром. Следовательно, $\dim \sigma(E) = \dim E$ и $\sigma(E) = E$. ■

Пример 4.2.

- $\mathbb{Q}(\sqrt{2})$ – нормально;
- $\mathbb{Q}(\sqrt[3]{2})$ – не нормально.

Теорема 4.9. Пусть $E = \mathbb{Q}(\alpha_1, \dots, \alpha_m)$ и пусть все сопряженные ко всем α_i лежат в E . Тогда E – нормально.

Доказательство. Пусть $\alpha \in E$. Тогда $\alpha = \frac{f(\alpha_1, \dots, \alpha_m)}{g(\alpha_1, \dots, \alpha_m)}$, $f, g \in \mathbb{Q}[x_1, \dots, x_m]$.

Если σ – вложение E в \mathbb{C} , то $\sigma(\alpha) = \frac{f(\sigma(\alpha_1), \dots, \sigma(\alpha_m))}{g(\sigma(\alpha_1), \dots, \sigma(\alpha_m))} \in E$.

Таким образом, $\sigma(E) \subset E$. Применяя лемму 4.6 получаем, что $\sigma(E) = E$, т.е. E нормально. ■

Если E нормально, то все вложения E в \mathbb{C} – автоморфизмы E . Можно брать их композиции, существует обратный элемент. Получается группа автоморфизмов E , называемой *группой Галуа*.

Пример 4.3. Группа Галуа $\mathbb{Q}(\sqrt{2})$ изоморфна \mathbb{Z}_2 .

Пусть E – конечное расширение \mathbb{Q} , $[E : \mathbb{Q}] = n$, $\sigma_1, \dots, \sigma_n$ – все вложения E в \mathbb{C} .

Определение 4.9. Для каждого $\alpha \in E$ *нормой относительно E* называется величина

$$N(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

Пример 4.4. $E = \mathbb{Q}(\sqrt{2})$: $N(\alpha + \beta\sqrt{2}) = (\alpha + \beta\sqrt{2})(\alpha - \beta\sqrt{2}) = \alpha^2 - 2\beta^2$.

Теорема 4.10.

1. Если $\alpha \in E$ и $p_\alpha(x) = x^d + \dots + a_1x + a_0$, то $N(\alpha) = (-1)^n a_0^{\frac{n}{d}}$.
2. Если $\alpha \in E$, то $N(\alpha) \in \mathbb{Q}$. Если $\alpha \in \mathbb{Z}_E = \mathbb{Z}_{\mathbb{A}} \cap E$, то $N(\alpha) \in \mathbb{Z}$.
3. $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.
4. $N(\alpha\beta) = N(\alpha)N(\beta)$, $N(\frac{\alpha}{\beta}) = \frac{N(\alpha)}{N(\beta)}$.

Доказательство.

1. Следует из теоремы 4.8 и теоремы Виета.
2. Следует из первого пункта.
3. Следует из определения вложения.
4. Следует из определения вложения.

■

4.5 Трансцендентность π

Теорема 4.11 (Линдемана-Вейерштрасса). Пусть $\alpha_0, \dots, \alpha_m$ – различные алгебраические числа. Тогда $e^{\alpha_0}, \dots, e^{\alpha_m}$ линейно независимы (ЛНЗ) над \mathbb{A} .

Теорема 4.12 (Об экспоненциальной линейной форме). Пусть $\alpha_0, \dots, \alpha_m \in \mathbb{A}, a_0, \dots, a_m \in \mathbb{A}$. Пусть $A(x) = \sum_{k=0}^m a_k e^{\alpha_k x} = \sum_{l=0}^{\infty} \left(\sum_{k=0}^m a_k \frac{\alpha_k^l}{l!} \right) x^l \in \mathbb{Q}[[x]] \setminus \{0\}$. Тогда $A(1) \neq 0$.

Теорема 4.13. 4.12 \Rightarrow 4.11.

Доказательство. Нужно показать, что $A(1) \neq 0$. Тогда мы применим 4.12 и получим, что $\forall a_0, \dots, a_m$ $A(1) \neq 0$, т.е. линейная комбинация $e^{\alpha_0}, \dots, e^{\alpha_m}$ не 0, и утверждение теоремы выполнено.

Можно считать, что все $a_0, \dots, a_m \neq 0$.

Тогда $A(x) = \sum_{k=0}^m a_k e^{\alpha_k x} \neq 0$, т.к. вронскиан W

$$W(e^{\alpha_0 x}, \dots, e^{\alpha_m x}) = \begin{vmatrix} e^{\alpha_0 x} & e^{\alpha_1 x} & \dots & e^{\alpha_m x} \\ \alpha_0 e^{\alpha_0 x} & \alpha_1 e^{\alpha_1 x} & \dots & \alpha_m e^{\alpha_m x} \\ \dots & \dots & \dots & \dots \\ \alpha_0^m e^{\alpha_0 x} & \alpha_1^m e^{\alpha_1 x} & \dots & \alpha_m^m e^{\alpha_m x} \end{vmatrix} = \exp \left(\left(\sum_{k=0}^m \alpha_k \right) x \right) V(\alpha_0, \dots, \alpha_m) \neq 0,$$

где $V(x_1, \dots, x_m)$ является Вандермондом для чисел x_1, \dots, x_m .

Почему $A(x) \in \mathbb{Q}[[x]]$? Рассмотрим нормальное расширение E поле \mathbb{Q} , содержащее $a_0, \dots, a_m, \alpha_0, \dots, \alpha_m$. (Например, можно взять все сопряженные к ним и добавить к \mathbb{Q} , по теореме 4.9 будет нормальное расширение).

Пусть $[E : \mathbb{Q}] = \eta, \sigma_1, \dots, \sigma_\eta$ – все автоморфизмы E над \mathbb{Q} . Тогда $A(x) = E[[x]]$.

Определим $\sigma_1, \dots, \sigma_\eta$ на $E[[x]]$ так:

$$\sigma_i : \sum_{l=0}^{\infty} \gamma_l x^l \mapsto \sum_{l=0}^{\infty} \sigma_i(\gamma_l) x^l$$

$$\sigma_i(A(x)) = \sum_{l=0}^{\infty} \left(\sum_{k=0}^m \sigma_i(a_k) \frac{\sigma_i(\alpha_k)^l}{l!} \right) x^l = \sum_{k=0}^m \sigma_i(a_k) e^{\sigma_i(\alpha_k) x} = A_i(x)$$

Поскольку $A(x) \neq 0$, то $A_i(x) \neq 0$.

Рассмотрим $B(x) = \prod_{i=1}^{\eta} A_i(x) \in E[[x]], B(x) \neq 0$.

Заметим, что

$$\sigma_i(B(x)) = \sigma_i \left(\prod_{i=1}^{\eta} A_i(x) \right) = \prod_{i=1}^{\eta} \sigma_i(A_i(x)) = \prod_{i=1}^{\eta} \sigma_i(\sigma_j(x)) = \prod_{i=1}^{\eta} \sigma_j(A_i(x)) = B(x) \Rightarrow B(x) \in \mathbb{Q}[[x]].$$

$$B(x) = \prod_{i=1}^{\eta} \sum_{k=0}^n \sigma_i(a_k) e^{\sigma_i(\alpha_k) x} = \sum_{l=0}^L b_l e^{\beta_l x}.$$

По Теореме 4.12 $B(1) \neq 0$. Тогда $B(1) = \prod_{j=1}^{\eta} A_j(1) \neq 0 \Rightarrow \forall j A_j(1) \neq 0$. А для тождественного σ_j имеем $A_j(x) = A(x)$ получаем, что $A(1) \neq 0$. ■

Лемма 4.7. Пусть $b_0, \dots, b_m, \beta_0, \dots, \beta_m \in \mathbb{C}$, пусть $\sum_{k=0}^m b_k e^{\beta_k} = 0$. Рассмотрим многочлен $f(x) = f_n(x) = (x - \beta_0)^n (x - \beta_1)^{n+1} \dots (x - \beta_m)^{n+1}$, пусть $g(x) = \frac{1}{n!} \sum_{l \geq n} f^{(l)}(x)$ (с некоторого l они все станут равны нулю). Тогда

$$\left| \sum_{k=0}^m b_k g(\beta_k) \right| \leq \frac{c^{n+1}}{n!}, \quad \text{где } c = c(b_0, \dots, b_m, \beta_0, \dots, \beta_m) \text{ — не зависит от } n.$$

Доказательство. Положим $F(x) = \sum_{l \geq 0} f^{(l)}(x)$. Нужно доказать, что $\left| \sum_{k=0}^m b_k F(\beta_k) \right| \leq c^{n+1}$. Заметим,

что $F(0)e^{\beta_k} - F(\beta_k) = e^{\beta_k} \int_0^{\beta_k} e^{-z} f(z) dz$ (по частям).

Домножим на b_k и просуммируем по k от 0 до m :

$$F(0) \sum_{k=0}^m b_k e^{\beta_k} - \sum_{k=0}^m b_k F(\beta_k) = \sum_{k=0}^m \left[b_k \int_0^{\beta_k} e^{\beta_k - z} f(z) dz \right] \text{ — хотим оценить модуль правой части.}$$

$$\left| \sum_{k=0}^m \left[b_k \int_0^{\beta_k} e^{\beta_k - z} f(z) dz \right] \right| \leq \sum_{k=0}^m |b_k| e^r \cdot (2r)^{(m+1)(n+1)} \leq c^{n+1}, \quad \text{где } r = \max_{0 \leq k \leq m} |\beta_k|$$

$$\text{для } c = (2r)^{m+1} e^r \cdot \max \left(1, \sum_{k=0}^m |b_k| \right).$$

■

Доказательство. (теоремы об экспоненциальной линейной форме (Т.Э.Л.Ф.)).

Пусть E — нормальное расширение поля \mathbb{Q} , содержащее $a_0, \dots, a_m, \alpha_0, \dots, \alpha_m$, $[E: \mathbb{Q}] = \nu$, $\sigma_1, \dots, \sigma_\nu$ — все автоморфизмы E над \mathbb{Q} (аналогично доказательству теоремы 4.13 о Т.Э.Л.Ф. \Rightarrow Т.Л.-В.). Можно считать, что $a_0, \dots, a_m \in \mathbb{Z}_A$ ($\in \mathbb{Z}_E$), так как существует $\tilde{d} \in \mathbb{Z} \setminus \{0\}$ такое, что все $\tilde{d}a_0, \tilde{d}a_1, \dots, \tilde{d}a_m \in \mathbb{Z}_A$. От замены то, что дано, и то, что требуется доказать, не поменяется.

Пусть $d \in \mathbb{N}$ — такое, что $d\alpha_0, d\alpha_1, \dots, d\alpha_m \in \mathbb{Z}_E$. Предположим противное: пусть $A(1) = 0$. Тогда продлеваем наши автоморфизмы $\sigma_1, \dots, \sigma_\nu$ на $E[[x]]$ как в доказательстве теоремы о Т.Э.Л.Ф \Rightarrow Т.Л.-В. То есть можно рассматривать $(\sigma_i A)(x)$.

Так как $A(x) \in \mathbb{Q}[[x]]$, то $(\sigma_i A)(x) = A(x) \quad \forall i = 1, 2, \dots, \nu$. Следовательно, $\sum_{k=0}^m \sigma_i(a_k) e^{\sigma_i(\alpha_k)x} = (\sigma_i A)(x) = A(x)$, т.е.

$$\sum_{k=0}^m \sigma_i(a_k) e^{\sigma_i(\alpha_k)} = A(1) = 0, \quad i = 1, 2, \dots, \nu.$$

Положим $f(x) = f_n(x) = (x - \alpha_0)^n (x - \alpha_1)^{n+1} \dots (x - \alpha_m)^{n+1}$, $g(x) = g_n(x) = \frac{1}{n!} \sum_{l \geq n} f^{(l)}(x)$. Положим

$I = I_n = d^{m(n+1)} \sum_{k=0}^m a_k g(\alpha_k)$. Покажем, что $I \in \mathbb{Z}_E$:

$$I = \sum_{k=0}^m a_k \sum_{l \geq n} d^{m(n+1)} \frac{1}{n!} f^{(l)}(\alpha_k) = \sum_{k=0}^m a_k \cdot (\text{целое алгебраическое число}), \text{ т.к. } d^{m(n+1)} f(x) = d^{-n} h(dx),$$

где $h(t) = (t - d\alpha_0)^n (t - d\alpha_1)^{n+1} \dots (t - d\alpha_m)^{n+1}$ (т.е. $h(t) \in \mathbb{Z}_E$). Следовательно, $d^{m(n+1)} \frac{1}{l!} f^{(l)}(\alpha_k) =$

$d^{-n+l} \frac{1}{l!} h^{(l)}(d\alpha_k) \in \mathbb{Z}_E$ при $l \leq n$. Далее,

$$I = d^{m(n+1)} \frac{1}{n!} f^{(n)}(\alpha_0) + (n+1) \sum_{k=0}^m \sum_{l \geq n+1} a_k \frac{l!}{(n+1)!} d^{m(n+1)} \frac{1}{l!} f^{(l)}(\alpha_k) = a_0 \prod_{k=1}^m (d\alpha_0 - d\alpha_k)^{n+1} + (n+1)J,$$

где $J \in \mathbb{Z}_E$.

Следовательно, $I \in \mathbb{Z}_E$, причём $I \neq 0$, если $\left(n+1, N \left(a_0 \prod_{k=1}^m (d\alpha_0 - d\alpha_k) \right) \right) = 1$.

Таких n бесконечно много: $n+1$ – простое, $\rightarrow \infty$. Но тогда и $\sigma_i(I) \in \mathbb{Z}_E$ и $\sigma_i(I) \neq 0$ при "хороших" n .

Но $\sigma_i(I) = d^{m(n+1)} \sum_{k=0}^m \sigma_i(a_k) g_i(\sigma_i(\alpha_k))$, где $f_i(x) = (\sigma_i f)(x) = (x - \sigma_i(\alpha_0))^n (x - \sigma_i(\alpha_1))^{n+1} \dots (x - \sigma_i(\alpha_m))^{n+1}$, $g_i(x) = (\sigma_i g)(x) = \frac{1}{n!} \sum_{l \geq n} f_i^{(l)}(x)$. Применим Лемму 4.7 для $b_k = \sigma_i(a_k)$, $\beta_i = \sigma_i(\alpha_k)$, $i = 1, 2, \dots, \nu$. Получим

$$|\sigma_i(I)| \leq d^{m(n+1)} \frac{c_i^{n+1}}{n!} \leq \frac{c^{n+1}}{n!}, \text{ где } c = d^m \max_i (c_i).$$

Итак, все $\sigma_i(I) \in \mathbb{Z}_E$, $\sigma_i(I) \neq 0$ при "хороших" n , $\sigma_i(I) \rightarrow 0$ при $n \rightarrow \infty$.

Следовательно, $N(I) = \prod_{i=1}^{\nu} \sigma_i(I) \rightarrow 0$ при $n \rightarrow \infty$ и $N(I) \neq 0$ при "хороших" n . Но $N(I) \in \mathbb{Z}$! Противоречие. ■

Следствие 4.3 (из теоремы Л.-В.). Если $\alpha \in \mathbb{A} \setminus \{0\}$, то $e^\alpha \notin \mathbb{A}$.

Доказательство. Пусть $\alpha_0 = 0$, $\alpha_1 = \alpha$. По теореме Л.-В. $e^{\alpha_0} = 1$ и $e^{\alpha_1} = e^\alpha$ линейно независимы над \mathbb{A} . ■

Следствие 4.4. Число π – трансцендентно.

Доказательство. Предположим противное. Тогда $\alpha_0 = 0$, $\alpha_1 = i\pi$. По теореме Л.-В. $e^{\alpha_0} = 1$, $e^{\alpha_1} = -1$ линейно независимы над \mathbb{A} , но они линейно зависимы. Противоречие. ■

Следствие 4.5. Если $\alpha \in \mathbb{A} \setminus \{1\}$, то $\ln(\alpha) \notin \mathbb{A}$.

Следствие 4.6. Если $\alpha \in \mathbb{A} \setminus \{0\}$, то $\sin(\alpha)$, $\cos(\alpha)$, $\operatorname{tg}(\alpha) \notin \mathbb{A}$.

Доказательство. $\sin(\alpha) = \frac{1}{2i} e^{i\alpha} - \frac{1}{2i} e^{-i\alpha}$. $i\alpha \neq -i\alpha$ и принадлежит $\mathbb{A} \Rightarrow$ для $0, i\alpha, -i\alpha$ по теореме Л.-В. 1, $e^{i\alpha}$, $e^{-i\alpha}$ ЛНЗ, а если бы $\sin(\alpha) \in \mathbb{A}$, то это было бы ЛЗ. ■

Следствие 4.7. Если $\beta_1, \dots, \beta_k \in \mathbb{A}$ ЛНЗ над \mathbb{Q} , то $e^{\beta_1}, \dots, e^{\beta_k}$ – алгебраически независимы над \mathbb{A} .

Доказательство. Пусть $f(x_1, \dots, x_k) \in \mathbb{A}[x_1, \dots, x_k]$. Тогда $f(e^{\beta_1}, \dots, e^{\beta_k}) = \sum_{(n_1, \dots, n_k)} a_{n_1 \dots n_k} e^{n_1 \beta_1 + \dots + n_k \beta_k} =: \alpha_{n_1 \dots n_k}$ – все попарно различны, т.к. β_1, \dots, β_k ЛНЗ над \mathbb{Q} . По теореме Л.-В. $e^{n_1 \beta_1 + \dots + n_k \beta_k}$ ЛНЗ над \mathbb{A} , следовательно, вся сумма не обращается в ноль. ■