Глава II. Теорема Дирихле о простых числах в арифметической прогрессии.

Лекция 7.
Характеры и L — функции Дирихле.

Основной результат.

Теорема 6 (Дирихле, 1837г.)

Любая арифметическая прогрессия, разность которой и первый член суть взаимно простые натуральные числа, содержит бесконечное подмножество, состоящее из простых чисел.

Основной результат.

Теорема 6 (Дирихле, 1837г.)

Любая арифметическая прогрессия, разность которой и первый член суть взаимно простые натуральные числа, содержит бесконечное подмножество, состоящее из простых чисел.

Прогрессии, о которых идёт речь в сформулированной теореме, имеют вид $mn + \ell$, где $n = 0, 1, 2, \ldots$, а m и ℓ — натуральные числа, $(m, \ell) = 1$. При $m = 1$ или $m = 2$ утверждение теоремы тривиально. Поэтому далее будем считать, что $m > 2$.

§2. Характеры Дирихле

Зафиксируем некоторое целое число $m \geq 3$.
Комплекснозначная функция $\chi(n)$, определённая на множестве всех целых чисел, называется *характером Дирихле или числовым характером по модулю* m, если она удовлетворяет условиям:
а) $\chi(n) \neq 0$ тогда и только тогда, когда $(n, m) = 1$;

§2. Характеры Дирихле

Зафиксируем некоторое целое число $m \geq 3$.
Комплекснозначная функция $\chi(n)$, определённая на множестве всех целых чисел, называется *характером Дирихле или числовым характером по модулю* m, если она удовлетворяет условиям:
а) $\chi(n) \neq 0$ тогда и только тогда, когда $(n, m) = 1$;
б) $\chi(n)$ периодична с периодом m;

§2. Характеры Дирихле

Зафиксируем некоторое целое число $m \geq 3$.
Комплекснозначная функция $\chi(n)$, определённая на множестве всех целых чисел, называется *характером Дирихле или числовым характером по модулю* m, если она удовлетворяет условиям:
а) $\chi(n) \neq 0$ тогда и только тогда, когда $(n, m) = 1$;
б) $\chi(n)$ периодична с периодом m;
в) для любых целых чисел u, v выполняется
$\chi(uv) = \chi(u) \cdot \chi(v)$ (свойство вполне мультипликативности).

§2. Характеры Дирихле

Зафиксируем некоторое целое число $m \geq 3$.
Комплекснозначная функция $\chi(n)$, определённая на множестве всех целых чисел, называется *характером Дирихле или числовым характером по модулю m*, если она удовлетворяет условиям:
а) $\chi(n) \neq 0$ тогда и только тогда, когда $(n, m) = 1$;
б) $\chi(n)$ периодична с периодом m;
в) для любых целых чисел u, v выполняется
$\chi(uv) = \chi(u) \cdot \chi(v)$ (свойство вполне мультипликативности).
Характер

$$\chi_0(n) = \begin{cases} 1, & (n,m)=1, \\ 0, & (n,m) > 1 \end{cases}$$

называется *главным характером*.

Характеры Дирихле

Свойства характеров.

1. $\chi(1) = 1$.

Действительно, $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1) \neq 0$.

Характеры Дирихле

Свойства характеров.

1. $\chi(1) = 1$.

Действительно, $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1) \neq 0$.

2. Для чисел n, взаимно простых с модулем m, значение $\chi(n)$ есть корень из единицы степени $\varphi(m)$.

Согласно теореме Эйлера имеем $n^{\varphi(m)} \equiv 1 \pmod{m}$. Поэтому

$$1 = \chi(1) = \chi(n^{\varphi(m)}) = \chi(n)^{\varphi(m)}.$$

Характеры Дирихле

Свойства характеров.
1. $\chi(1) = 1$.
Действительно, $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1) \neq 0$.
2. Для чисел n, взаимно простых с модулем m, значение $\chi(n)$ есть корень из единицы степени $\varphi(m)$.
Согласно теореме Эйлера имеем $n^{\varphi(m)} \equiv 1 \pmod{m}$. Поэтому

$$1 = \chi(1) = \chi(n^{\varphi(m)}) = \chi(n)^{\varphi(m)}.$$

3. Для всех n выполняется неравенство

$$|\chi(n)| \leq 1.$$

Действительно, все ненулевые значения характера являются корнями из 1.

Характеры Дирихле

Теорема 7

Для каждого $m \geq 2$ существует в точности $\varphi(m)$ характеров.

Теорема 7

Для каждого $m \geq 2$ существует в точности $\varphi(m)$ характеров.

Доказательство. Для каждого целого числа c, взаимно простого с m, будем называть *показателем c* наименьшее натуральное число d, для которого

$$c^d \equiv 1 \pmod{m}.$$

Группа $\mathbb{Z}_m^*$ обратимых элементов кольца $\mathbb{Z}_m$ конечна и абелева, а потому разлагается в прямое произведение циклических подгрупп:

$$\mathbb{Z}_m^* = H_1 \times \ldots \times H_r, \qquad H_j = (\overline{c_j}), \quad |H_j| = d_j, \quad d_1 \cdots d_r = \varphi(m).$$

Иначе говоря, если $\overline{n} \in \mathbb{Z}_m^*$, то $\overline{n} = \overline{c}_1^{k_1} \times \ldots \times \overline{c}_r^{k_r}$. На языке сравнений это можно переписать так: если $(n, m) = 1$, то $n \equiv c_1^{k_1} \cdots c_r^{k_r} \pmod{m}$, $0 \leq k_j < d_j$, и $c_i^{d_j} \equiv 1 \pmod{m}$.

Пусть ξ_k какой-нибудь корень из 1 степени d_k, $k = 1, \ldots, r$. Обозначим $\xi = (\xi_1, \ldots, \xi_r)$. Построим функцию

$$\chi_\xi(n) = \begin{cases} 0, & \text{если (n,m)>1;} \\ \xi_1^{k_1} \cdots \xi_r^{k_r}, & \text{если n } \equiv c_1^{k_1} \cdots c_r^{k_r} \pmod{m}. \end{cases}$$

Пусть ξ_k какой-нибудь корень из 1 степени d_k, $k = 1, \ldots, r$. Обозначим $\xi = (\xi_1, \ldots, \xi_r)$. Построим функцию

$$\chi_\xi(n) = \begin{cases} 0, & \text{если (n,m)>1;} \\ \xi_1^{k_1} \cdots \xi_r^{k_r}, & \text{если n } \equiv c_1^{k_1} \cdots c_r^{k_r} \pmod{m}. \end{cases}$$

Она — характер, все условия в определении проверяются непосредственно. Покажем теперь, что разным наборам корней ξ и ν соответствуют разные характеры. Действительно, если $\xi_i \neq \nu_i$, то $\chi_\xi(c_i) = \xi_i \neq \nu_i = \chi_\nu(c_i)$. Значит, количество построенных характеров совпадает с количеством наборов ξ, а их имеется $d_1 \cdots d_r = \varphi(m)$.

Характеры Дирихле

Теперь докажем, что других характеров нет. Пусть χ произвольный характер по модулю m. Покажем, что он определяется значениями на образующих группы. Пусть $\tau_i = \chi(c_i)$. Поскольку $c_j^{d_j} \equiv 1 \pmod{m}$, то $1 = \chi(1) = \chi(c_j^{d_j}) = \chi(c_j)^{d_j}$. Таким образом $\tau = (\tau_1, \ldots, \tau_r)$ это набор корней из единицы соответствующих степеней. Поэтому, если $(n, m) = 1$, то $n \equiv c_1^{k_1} \cdots c_r^{k_r} \pmod{m}$ с некоторым набором целых чисел $k_1, k_2, \ldots, k_r$, $0 \leq k_i < d_i$ и

$$\chi(n) = \chi(c_1^{k_1} \cdots c_r^{k_r}) = \tau_1^{k_1} \cdots \tau_r^{k_r}.$$

Значит, χ уже содержится в построенном множестве характеров и теорема 7 полностью доказана.

Характеры Дирихле

Лемма 1

Выполняются равенства

$$\sum_{n=1}^{m} \chi(n) = \begin{cases} \varphi(m), & \chi = \chi_0; \\ 0, & \chi \neq \chi_0. \end{cases} \tag{1}$$

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(m), & n \equiv 1 \pmod{m}; \\ 0, & n \not\equiv 1 \pmod{m}. \end{cases} \tag{2}$$

Докажем первое равенство

$$\sum_{n=1}^{m} \chi(n) = \begin{cases} \varphi(m), & \chi = \chi_0; \\ 0, & \chi \neq \chi_0. \end{cases}$$

Если $\chi = \chi_0$, утверждение очевидно.

Докажем первое равенство

$$\sum_{n=1}^{m} \chi(n) = \begin{cases} \varphi(m), & \chi = \chi_0; \\ 0, & \chi \neq \chi_0. \end{cases}$$

Если $\chi = \chi_0$, утверждение очевидно. Далее $\chi \neq \chi_0$. Это значит, что характеру χ соответствует набор корней $(\xi_1, \ldots, \xi_r)$, в котором есть $\xi_j \neq 1$. Если $(n, m) \neq 1$, то $\chi(n) = 0$, так что

$$\sum_{n=1}^{m} \chi(n) = \sum_{n=1,(n,m)=1}^{m} \chi(n) = \sum_{0 \leq k_i < d_i} \xi_1^{k_1} \cdots \xi_r^{k_r} = \prod_{\ell=1}^{r} \left(\sum_{k_\ell=0}^{d_\ell - 1} \xi_\ell^{k_\ell} \right),$$

при $\ell = j$ имеем $\displaystyle\sum_{k=0}^{d_j-1} \xi_j^k = \frac{\xi_j^{d_j} - 1}{\xi_j - 1} = 0.$

Первое равенство доказано.

Если $n \equiv 1 \pmod{m}$, то для любого характера имеем $\chi(n) = \chi(1) = 1$ и второе утверждение

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

выполняется.

Если $n \equiv 1 \pmod{m}$, то для любого характера имеем $\chi(n) = \chi(1) = 1$ и второе утверждение

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

выполняется. Если $(n, m) \neq 1$, то для любого характера χ имеем равенство $\chi(n) = 0$. В этом случае все слагаемые суммы равны нулю и второе равенство также выполняется. Далее считаем $(n, m) = 1$. Тогда $n \equiv c_1^{k_1} \cdots c_r^{k_r} \pmod{m}$, где существует показатель степени k_j, $0 < k_j < d_j$.

Если $n \equiv 1 \pmod m$, то для любого характера имеем $\chi(n) = \chi(1) = 1$ и второе утверждение

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

выполняется. Если $(n, m) \neq 1$, то для любого характера χ имеем равенство $\chi(n) = 0$. В этом случае все слагаемые суммы равны нулю и второе равенство также выполняется. Далее считаем $(n, m) = 1$. Тогда $n \equiv c_1^{k_1} \cdots c_r^{k_r} \pmod m$, где существует показатель степени k_j, $0 < k_j < d_j$. Имеем

$$\sum_{\chi} \chi(n) = \sum_{(\xi_1, \ldots, \xi_r)} \xi_1^{k_1} \cdots \xi_r^{k_r} = \prod_{\ell=1}^{r} \left(\sum_{\xi : \xi^{d_\ell} = 1} \xi^{k_\ell} \right).$$

При $\ell = j$ и $\eta = e^{2\pi i \frac{k_j}{d_j}} \neq 1$ находим

$$\sum_{\xi : \xi^{d_j} = 1} \xi^{k_j} = \sum_{r=0}^{d_j - 1} e^{2\pi i \frac{k_j r}{d_j}} = \sum_{r=0}^{d_j - 1} \eta^r = \frac{\eta^{d_j} - 1}{\eta - 1} = 0.$$

Лемма 2

Пусть $\chi(n)$ - неглавный характер по модулю m и $S(x) = \sum_{1 \le n \le x} \chi(n)$. Тогда при любом действительном $x \ge 1$ выполняется неравенство $|S(x)| < m$.

Доказательство. Функция $\chi(n)$ периодична с периодом m и согласно лемме 1 удовлетворяет равенству $\sum_{n=1}^{m} \chi(n) = 0$. Определим целые числа q, r условиями $[x] = mq + r, 0 \le r < m$. В согласии со сказанным выше имеем равенства

$$S(x) = S([x]) = q \sum_{n=1}^{m} \chi(n) + \sum_{n=mq+1}^{mq+r} \chi(n) = \sum_{n=1}^{r} \chi(n).$$

Каждое значение характера по абсолютной величине не превосходит 1. Поэтому $|S(x)| \le r < m$. Лемма 2 доказана.

§3. L-функции Дирихле.

Пусть $m \geq 2$. Для каждого характера Дирихле $\chi(n)$ по модулю m определим L-функцию

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{3}$$

Лемма 3

1. Если $\chi \neq \chi_0$, то ряд (3) сходится в области $\Re s > 0$. Определяемая им функция аналитична в этой области.

2. Ряд, определяющий $L(s, \chi_0)$ сходится в области $\Re s > 1$. Функция $L(s, \chi_0)$ аналитична в этой области.

Пусть $\delta > 0$ и χ произвольный характер по модулю m. В области $\Re s \geq 1 + \delta$ справедливы неравенства

$$\left| \frac{\chi(n)}{n^s} \right| \leq \frac{1}{n^\sigma} \leq \frac{1}{n^{1+\delta}}.$$

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}. \qquad \left|\frac{\chi(n)}{n^s}\right|\le\frac{1}{n^\sigma}\le\frac{1}{n^{1+\delta}}.$$

Ряд равномерно сходится в области $\sigma=\Re s>1+\delta$ и определяет там аналитическую функцию. В силу произвольности $\delta>0$ можно утверждать, что функция $L(s,\chi)$ аналитична в области $\Re s>1$. Это доказывает утверждения леммы для $L(s,\chi_0)$.

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}. \qquad \left|\frac{\chi(n)}{n^s}\right|\le\frac{1}{n^\sigma}\le\frac{1}{n^{1+\delta}}.$$

Ряд равномерно сходится в области $\sigma=\Re s>1+\delta$ и определяет там аналитическую функцию. В силу произвольности $\delta>0$ можно утверждать, что функция $L(s,\chi)$ аналитична в области $\Re s>1$. Это доказывает утверждения леммы для $L(s,\chi_0)$. Далее считаем, что $\chi\neq\chi_0$. С помощью формулы суммирования Абеля находим

$$\sum_{n=1}^{N}\frac{\chi(n)}{n^s}=\frac{S(N)}{N^s}+s\int_1^N S(x)x^{-s-1}dx. \tag{4}$$

В области $\sigma=\Re s>0$ выполняются неравенства $\left|\frac{S(N)}{N^s}\right|<\frac{m}{N^\sigma}$ и $\left|\frac{S(x)}{x^{s+1}}\right|\le\frac{m}{x^{\sigma+1}}$. Из этих оценок следует, что правая часть (4) имеет предел при $N\to+\infty$, а также, что для каждого неглавного характера χ ряд, определяющий L-функцию Дирихле, сходится в области $\Re s>0$.

Переходя в равенстве

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

к пределу при $N \to +\infty$, находим

$$L(s,\chi) = s \int_1^{\infty} S(x) x^{-s-1} dx = s \sum_{n=1}^{\infty} \int_n^{n+1} S(x) x^{-s-1} dx.$$

Для функций $f_n(s) = \int_n^{n+1} S(x) x^{-s-1} dx$ имеем

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

Итак, функции $f_n(s)$ аналитичны в области $\sigma > 0$, а в области $\sigma > \delta > 0$ выполняется неравенство $|f_n(s)| \leq \frac{m}{n^{\sigma+1}} \leq \frac{m}{n^{1+\delta}}$. Отсюда следует равномерная сходимость ряда $\sum_{n=1}^{\infty} f_n(s)$ в области $\sigma > \delta$ и аналитичность в этой же области его суммы и функции $L(s,\chi)$. В силу произвольности $\delta > 0$ заключаем, что функция Дирихле $L(s,\chi)$ аналитична в области $\Re s > 0$.

Для того, чтобы аналитически продолжить функцию $L(s, \chi_0)$ в область $\Re s > 0$, воспользуемся леммой 1 из лекции 3.

Лемма 4 (Формула Эйлера для L функций)

Для любого характера χ в области $\Re s > 1$ справедливо тождество

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

где произведение берётся по всем простым числам.

Доказательство.

Воспользуемся вполне мультипликативностью функции $\frac{\chi(n)}{n^s}$, абсолютной сходимостью ряда для $L(s, \chi)$ и леммой 1 из лекции 3. □

Тогда

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

$$=\prod_{p\nmid m}\left(1-\frac{1}{p^s}\right)^{-1}.$$

Тогда

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

$$=\prod_{p\nmid m}\left(1-\frac{1}{p^s}\right)^{-1}.$$

Поэтому

$$L(s,\chi_0)=\zeta(s)\prod_{p\mid m}\left(1-\frac{1}{p^s}\right),\quad \mathrm{Res}>1$$

$$L(s,\chi_0) = \zeta(s)\prod_{p|m}\left(1-\frac{1}{p^s}\right), \quad \mathrm{Res} > 1 \tag{5}$$

Дзета-функция аналитична в области $\Re s > 0$ и имеет полюс первого порядка в $s = 1$. Функция $\prod_{p|m}\left(1-\frac{1}{p^s}\right)$ аналитична во всей комплексной плоскости и не обращающается в нуль в точке $s = 1$. Поэтому равенство (5) аналитически продолжает $L(s,\chi_0)$ во всю правую комплексную полуплоскость, где $L(s,\chi_0)$ имеет полюс первого порядка в точке $s = 1$.

Конец
седьмой лекции.

Лекция 8. Завершение доказательства теоремы Дирихле о простых числах в арифметических прогрессиях.

§4. Поведение L-функций в точке $s = 1$

Теорема 8

Если $\chi \neq \chi_0$, *то* $L(1, \chi) \neq 0$.

§4. Поведение L-функций в точке $s = 1$

Теорема 8

Если $\chi \neq \chi_0$, *то* $L(1, \chi) \neq 0$.

Доказательство разобьём на две части.

1. Пусть сначала χ не действительный характер, т.е. среди его значений есть не действительные. Это равносильно тому, что $\chi^2 \neq \chi_0$. Настало время ещё раз применить лемму 2 из доказательства теоремы 4 об отсутствии нулей дзета-функции Римана на едининой прямой.

§4. Поведение L-функций в точке $s = 1$

Теорема 8

Если $\chi \neq \chi_0$, *то* $L(1, \chi) \neq 0$.

Доказательство разобьём на две части.

1. Пусть сначала χ не действительный характер, т.е. среди его значений есть не действительные. Это равносильно тому, что $\chi^2 \neq \chi_0$. Настало время ещё раз применить лемму 2 из доказательства теоремы 4 об отсутствии нулей дзета-функции Римана на едининой прямой. Рассмотрим

$$P := L(s, \chi_0)^3 L(s, \chi)^4 L(s, \chi^2) =$$

$$= \prod_{p \nmid m} \left(\left(1 - \frac{1}{p^s}\right)^3 \left(1 - \frac{\chi(p)}{p^s}\right)^4 \left(1 - \frac{\chi^2(p)}{p^s}\right) \right)^{-1}.$$

Если считать, что s действительное число, большее 1, а $r := \frac{1}{p^s}$, $\chi(p) = e^{i\varphi}$, тогда $\chi^2(p) = e^{2i\varphi}$. По лемме каждый множитель в произведении P не меньше 1, а значит, $P \geq 1$.

$$P = L(s, \chi_0)^3 L(s, \chi)^4 L(s, \chi^2)$$

Предположим теперь, что $L(1, \chi) = 0$. Функция $L(s, \chi)$ аналитична в точке $s = 1$, поэтому $L(s, \chi) = O(s - 1)$ при $s \to 1+$. Так как $\chi^2 \neq \chi_0$, то $L(s, \chi^2) = O(1)$. Кроме того,

$$L(s, \chi_0) = O\left(\frac{1}{s-1}\right).$$

Из этих оценок следует, что

$$P = O\left(\frac{1}{(s-1)^3} \cdot (s-1)^4 \cdot 1\right) = O(s-1),$$

а это противоречит ранее полученному свойству $P \geq 1$.

2. Пусть теперь χ действительный характер, то есть $\chi^2 = \chi_0$. В этом случае $P = (L(s, \chi_0)L(s, \chi))^4$. Рассмотрим функцию $F(s) := \zeta(s)L(s, \chi)$.

2. Пусть теперь χ действительный характер, то есть $\chi^2 = \chi_0$. В этом случае $P = (L(s, \chi_0)L(s, \chi))^4$. Рассмотрим функцию $F(s) := \zeta(s)L(s, \chi)$. Дальнейшему доказательству предпошлём лемму.

Лемма 1

В области $\Re s > 1$ функция $F(s) = \zeta(s)L(s, \chi)$ аналитична и представима в виде ряда

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad a_n \in \mathbb{Z}, \qquad a_n \geq 0, \quad a_{k^2} \geq 1, \qquad (1)$$

причём в точке $s = \frac{1}{2}$ ряд расходится. В полуплоскости $\Re s > 1$ ряд (1) можно почленно дифференцировать, т.е.

$$F^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \frac{a_n (\ln n)^k}{n^s}. \qquad (2)$$

Ряды для $\zeta(s)$ и $L(s,\chi)$ абсолютно сходятся в области $\Re s > 1$. Перемножая их по известным правилам, находим

$$F(s) = \sum_{u=1}^{\infty} \frac{1}{u^s} \sum_{v=1}^{\infty} \frac{\chi(v)}{v^s} = \sum_{u,v\geq 1} \frac{\chi(v)}{(uv)^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{v|n} \chi(v) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

где $a_n = \sum_{v|n} \chi(v)$. Причём ряд для $F(s)$ также абсолютно сходится в области $\Re s > 1$.

Поскольку $\chi(n) = \pm 1$ или $\chi(n) = 0$, то $a_n \in \mathbb{Z}$. Осталось проверить неотрицательность. Пусть $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, тогда $v = p_1^{\beta_1} \cdots p_r^{\beta_r}$ $(\beta_j \leq \alpha_j)$, и

$$a_n = \sum_{\beta_1,\ldots,\beta_r} \chi(p_1^{\beta_1} \cdots p_r^{\beta_r}) = \prod_{j=1}^{r} \left(\sum_{\beta_j=0}^{\alpha_j} \chi(p_j)^{\beta_j} \right) = a_{n1} \cdots a_{nr},$$

где

$$a_{nj} = \begin{cases} \alpha_j + 1, & \chi(p_j) = 1; \\ 1, & \chi(p_j) = 0; \\ 0, & \chi(p_j) = -1, \text{ и } \alpha_j \text{ нечётно}; \\ 1, & \chi(p_j) = -1, \text{ и } \alpha_j \text{ чётно}. \end{cases}$$

При $n = k^2$ степени чётны, поэтому $a_{nj} \neq 0$, значит, $a_n \geq 1$.

Если предположить, что ряд $F(s)$ сходится при $s = \frac{1}{2}$, то есть

$$\sum_{n=1}^{\infty} \frac{a_n}{n^{1/2}} < \infty, \quad \text{то, тем более,} \quad \sum_{k=1}^{\infty} \frac{a_{k^2}}{k} < \infty,$$

а поскольку $a_{k^2} \geq 1$, то получаем, что гармонический ряд $\sum_{k=1}^{\infty} \frac{1}{k}$ тоже должен сходиться, что неверно.

Если предположить, что ряд $F(s)$ сходится при $s = \frac{1}{2}$, то есть

$$\sum_{n=1}^{\infty} \frac{a_n}{n^{1/2}} < \infty, \quad \text{то, тем более,} \quad \sum_{k=1}^{\infty} \frac{a_{k^2}}{k} < \infty,$$

а поскольку $a_{k^2} \geq 1$, то получаем, что гармонический ряд $\sum_{k=1}^{\infty} \frac{1}{k}$ тоже должен сходиться, что неверно.
Утверждение об аналитиности и почленной дифференцируемости ряда (1) в полуплоскости $\Re s > 1$ следует по теореме Вейерштрасса из равномерной сходимости ряда (1) в области $\Re s > 1 + \delta$ при любом $\delta > 0$. Ряд же сходится равномерно, поскольку в этой области справедливо неравенство

$$\left| \frac{a_n}{n^s} \right| \leq \frac{a_n}{n^{1+\delta}}$$

и ряд (1) для функции $F(s)$ сходится в точке $s = 1 + \delta$. Так как число $\delta > 0$ можно взять сколь угодно малым, то равенство (2) справедливо в полуплоскости $\Re s > 1$.

Вернёмся к доказательству второй части теоремы. Предположим, что $L(1,\chi)=0$. Тогда функция $F(s)$ имеет устранимую особенность в точке $s=1$ и аналитична в остальных точках полуплоскости $\Re s>0$ (полюс исчезнет). Значит, функцию $F(s)$ можно разложить в ряд Тейлора в точке $s=2$, причём радиус круга сходимости будет равен расстоянию от точки $s=2$ до ближайшей особенности, т.е. будет не меньше 2. Пусть далее s действительное, $0<s<1$. Тогда $|s-2|<2$ и

$$F(s)=\sum_{k=0}^{\infty}\frac{F^{(k)}(2)}{k!}(s-2)^k=\sum_{k=0}^{\infty}\frac{(s-2)^k}{k!}(-1)^k\sum_{n=1}^{\infty}\frac{a_n\ln^k n}{n^2}=$$

$$=\sum_{k=0}^{\infty}\sum_{n=1}^{\infty}\frac{(2-s)^k a_n\ln^k n}{n^2 k!}.$$

Члены последнего двойного ряда неотрицательны и он сходится. Как известно, в сходящемся двойном ряде с неотрицательными членами можно поменять порядок суммирования, и при этом сумма нового двойного ряда не изменится. Поэтому

$$F(s) = \sum_{k=0}^{\infty}\sum_{n=1}^{\infty} \frac{(2-s)^k a_n \ln^k n}{n^2 k!} = \sum_{n=1}^{\infty} \frac{a_n}{n^2} \sum_{k=0}^{\infty} \frac{(2-s)^k \ln^k n}{k!} =$$

$$= \sum_{n=1}^{\infty} \frac{a_n}{n^2} \cdot e^{(2-s)\ln n} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Следовательно, ряд $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ при любом действительном $s, 0 < s < 1$, сходится, что противоречит доказанному в лемме 1 факту о расходимости этого ряда в точке $s = \frac{1}{2}$.
Итак, мы доказали, что $L(1, \chi) \neq 0$ для неглавных характеров. Теорема 8 доказана полностью.

Лемма 2

В области $\Re s > 1$ *имеет место равенство*

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

где Λ *— функция Мангольдта. Ряд сходится абсолютно и* $L(s,\chi) \neq 0$ *в указанной области.*

Лемма 2

В области $\Re s > 1$ *имеет место равенство*

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

где Λ *— функция Мангольдта. Ряд сходится абсолютно и* $L(s,\chi) \neq 0$ *в указанной области.*

Имеет место очевидная оценка

$$\left|\frac{\Lambda(n)\chi(n)}{n^s}\right| \leq \frac{\ln n}{n^\sigma}.$$

Отсюда легко следует абсолютная и равномерная сходимость в оластях $\Re s > 1$ и $\Re s > 1 + \delta$ соответственно при любом фиксированном $\delta > 0$. Согласно теореме Вейерштрасса можно утверждать, что сумма ряда аналитична в области $\Re s > 1 + \delta$. Учитывая, что $\delta > 0$ может быть выбрано сколь угодно малым, заключаем, что сумма ряда аналитична в области $\Re s > 1$.

Проверим выполнение тождества из леммы. Для этого перемножим два абсолютно сходящихся в области $\Re s > 1$ ряда — ряд, стоящий в правой части тождества и ряд для $L(s, \chi)$. Имеем

$$L(s,\chi)\sum_{k=1}^{\infty}\frac{\Lambda(k)\chi(k)}{k^s} = \sum_{l=1}^{\infty}\frac{\chi(l)}{l^s}\sum_{k=1}^{\infty}\frac{\Lambda(k)\chi(k)}{k^s} =$$

$$= \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\sum_{k|n}\Lambda(k) = \sum_{n=1}^{\infty}\frac{\chi(n)\ln n}{n^s} = -L'(s,\chi).$$

Выражение после второго равенства получено в результате группировки попарных произведений, имеющих одинаковые значения $k \cdot \ell = n$ и упорядочения их по возрастанию n. Последнее равенство получится, если почленно продифференцировать ряд, определяющий функцию $L(s, \chi)$.

$$L(s,\chi)\sum_{k=1}^{\infty}\frac{\Lambda(k)\chi(k)}{k^s} = -L'(s,\chi) \qquad (3)$$

Докажем теперь отсутствие нулей у $L(s,\chi)$ в области $\Re s > 1$. Допустим, что функция $L(s,\chi)$ обращается в нуль в точке s_0 с условием $\Re s_0 > 1$. Кратность нуля обозначим буквой $r \geq 1$. При дифференцировании кратность нуля уменьшается на единицу (в нашем случае $r \geq 1$). Поэтому кратность нуля производной, стоящей в правой части (3) равна $r-1$. А функция в левой части имеет кратность нуля в точке s_0 не менее r (второй сомножитель аналитичен в точке s_0). Получившееся противоречие завершает доказательство леммы.

Теперь можно приступить к основному результату Дирихле, доказанному в 1837-1839 годах.

Теорема 9 (Дирихле)

Если m и ℓ натуральные взаимно простые числа, то последовательность $mn + \ell$, $n = 0, 1, 2, \ldots$ содержит бесконечно много простых чисел.

При $m = 1$ или $m = 2$ утверждение, очевидно, выполняется. Далее будем считать, что $m \geq 3$. Пусть χ — произвольный характер по модулю m. Из леммы 2 следует, что логарифмическая производная функции $L(s, \chi)$ в области $\Re s > 1$ может быть представлена в виде абсолютно сходящегося ряда

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n\geq 2} \frac{\Lambda(n)\chi(n)}{n^s} = \sum_{k\geq 1, p} \frac{\ln p \cdot \chi(p^k)}{p^{ks}}$$

Второе равенство выполняется в силу определения функции Мангольдта $\Lambda(n)$, слагаемые в правой части расположены в порядке возрастания чисел p^k.

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{k\geq 1,p} \frac{\ln p \cdot \chi(p^k)}{p^{ks}} = \sum_{p} \frac{\ln p \cdot \chi(p)}{p^s} + \sum_{k\geq 2,p} \frac{\ln p \cdot \chi(p^k)}{p^{ks}}.$$

Как указывалось на предыдущем слайде, первая сумма написанной выше строки абсолютно сходится. Поэтому при любой перестановке её членов и любой группировке их, ряд остаётся сходящимся, а сумма его не меняется. Это объясняет второе равенство.

Докажем, что последняя сумма ограничена на множестве действительных чисел $s \geq 1$.

$$\left| \sum_{k\geq 2,p} \frac{\ln p \cdot \chi(p^k)}{p^{ks}} \right| \leq \sum_{k\geq 2,p} \frac{\ln p}{p^k} = \sum_{p} \ln p \sum_{k=2}^{\infty} \frac{1}{p^k} =$$

$$= \sum_{p} \frac{\ln p}{p^2 - p} \leq \sum_{n=2}^{\infty} \frac{\ln n}{n^2 - n} = c < \infty.$$

Таким образом, установлено соотношение:

$$\sum_p \frac{\ln p \cdot \chi(p)}{p^s} = -\frac{L'(s,\chi)}{L(s,\chi)} + O(1), \quad \Re s > 1. \tag{4}$$

Числа m и ℓ взаимно просты по условию, значит, найдётся целое число d, удовлетворяющее сравнению $\ell d \equiv 1 \pmod m$. Для каждого характера χ умножим сравнение (4) на ненулевое число $\chi(d)$ и просуммируем результаты по всем χ:

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

Вспомним, что

$$\sum_\chi \chi(n) = \begin{cases} \varphi(m), & n \equiv 1 \pmod m; \\ 0, & n \not\equiv 1 \pmod m. \end{cases} \tag{5}$$

Итак, в $\sum_p \chi(pd)$ ненулевыми будут лишь слагаемые, у которых $p \equiv \ell \pmod m$. Что касается правой части, то в ней особым является только слагаемое главного характера, все остальные в силу теоремы 8 не имеют полюсов и потому их можно включить в $O(1)$. В итоге получаем

$$\varphi(m) \cdot \sum_{p \equiv l(m)} \frac{\ln p}{p^s} = -\chi_0(d) \frac{L'(s, \chi_0)}{L(s, \chi_0)} + O(1).$$

Итак, в $\sum_p \chi(pd)$ ненулевыми будут лишь слагаемые, у которых $p \equiv \ell \pmod m$. Что касается правой части, то в ней особым является только слагаемое главного характера, все остальные в силу теоремы 8 не имеют полюсов и потому их можно включить в $O(1)$. В итоге получаем

$$\varphi(m) \cdot \sum_{p \equiv l(m)} \frac{\ln p}{p^s} = -\chi_0(d) \frac{L'(s, \chi_0)}{L(s, \chi_0)} + O(1).$$

А мы знаем, что $L(s, \chi_0) = \frac{f(s)}{s-1}$, причём $f(1) \neq 0$. Стало быть, $\frac{L'}{L} = -\frac{1}{s-1} + \frac{f'}{f}$. Кроме того, $\chi_0(d) = 1$. Поэтому

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

Итак, в $\sum_p \chi(pd)$ ненулевыми будут лишь слагаемые, у которых $p \equiv \ell \pmod m$. Что касается правой части, то в ней особым является только слагаемое главного характера, все остальные в силу теоремы 8 не имеют полюсов и потому их можно включить в $O(1)$. В итоге получаем

$$\varphi(m) \cdot \sum_{p \equiv l(m)} \frac{\ln p}{p^s} = -\chi_0(d)\frac{L'(s,\chi_0)}{L(s,\chi_0)} + O(1).$$

А мы знаем, что $L(s,\chi_0) = \frac{f(s)}{s-1}$, причём $f(1) \neq 0$. Стало быть, $\frac{L'}{L} = -\frac{1}{s-1} + \frac{f'}{f}$. Кроме того, $\chi_0(d) = 1$. Поэтому

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

Справа стоит функция, стремящаяся к бесконечности при $s \to 1$, а слева сумма, которая стремится к бесконечности лишь в случае, когда слагаемых в ней бесконечное количество. Теорема Дирихле доказана.

Конец
восьмой лекции.

Глава III. Алгебраические и трансцендентные числа.

Лекция 9.

§1. Свойства алгебраических чисел.

Определение. *1. Комплексное число* α *называется* алгебраическим, *если найдется отличный от нуля многочлен* $f(x) \in \mathbb{Q}[x]$, *для которого* $f(\alpha) = 0$.
2. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Этот многочлен называется минимальным многочленом α. *Его степень называется* степенью α *и будет обозначаться* $\deg \alpha$.

§1. Свойства алгебраических чисел.

Определение. *1. Комплексное число* α *называется* алгебраическим*, если найдется отличный от нуля многочлен* $f(x) \in \mathbb{Q}[x]$*, для которого* $f(\alpha) = 0$*.*
2. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Этот многочлен называется минимальным многочленом α*. Его степень называется* степенью α *и будет обозначаться* $\deg \alpha$*.*
Например, любое рациональное число a является алгебраическим, как корень многочлена $f(x) = x - a \in \mathbb{Q}[x]$. Указанный многочлен, очевидно, является минимальным многочленом числа a, и потому $\deg a = 1$.

§1. Свойства алгебраических чисел.

Определение. *1. Комплексное число* α *называется* алгебраическим*, если найдется отличный от нуля многочлен* $f(x) \in \mathbb{Q}[x]$*, для которого* $f(\alpha) = 0$*.*
2. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Этот многочлен называется минимальным многочленом α*. Его степень называется* степенью α *и будет обозначаться* $\deg \alpha$*.*
Например, любое рациональное число a является алгебраическим, как корень многочлена $f(x) = x - a \in \mathbb{Q}[x]$. Указанный многочлен, очевидно, является минимальным многочленом числа a, и потому $\deg a = 1$.
Число $a = i$ - корень неприводимого многочлена $x^2 + 1 \in \mathbb{Q}$, есть алгебраическое число степени 2.

§1. Свойства алгебраических чисел.

Определение. *1. Комплексное число* α *называется* алгебраическим*, если найдется отличный от нуля многочлен* $f(x) \in \mathbb{Q}[x]$*, для которого* $f(\alpha) = 0$.
2. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Этот многочлен называется минимальным многочленом α*. Его степень называется* степенью α *и будет обозначаться* $\deg \alpha$.
Например, любое рациональное число a является алгебраическим, как корень многочлена $f(x) = x - a \in \mathbb{Q}[x]$. Указанный многочлен, очевидно, является минимальным многочленом числа a, и потому $\deg a = 1$.
Число $a = i$ - корень неприводимого многочлена $x^2 + 1 \in \mathbb{Q}$, есть алгебраическое число степени 2.
Многочлен $x^3 - 7$ не имеет рациональных корней и потому неприводим над полем $\mathbb{Q}$. Его корень $\sqrt[3]{7}$ есть алгебраическое число степени 3, а $x^3 - 7$ — минимальный многочлен числа $\sqrt[3]{7}$.

Укажем некоторые свойства минимального многочлена.

Лемма 1

1. Минимальный многочлен любого алгебраического числа неприводим.

Укажем некоторые свойства минимального многочлена.

Лемма 1

1. Минимальный многочлен любого алгебраического числа неприводим.

2. Если $f(x)$ – минимальный многочлен числа α, которое также является корнем многочлена $g(x) \in \mathbb{Q}[x]$, то многочлен $g(x)$ делится на $f(x)$.

Укажем некоторые свойства минимального многочлена.

Лемма 1

1. Минимальный многочлен любого алгебраического числа неприводим.

2. Если $f(x)$ – минимальный многочлен числа α, которое также является корнем многочлена $g(x) \in \mathbb{Q}[x]$, то многочлен $g(x)$ делится на $f(x)$.

3. Неприводимый многочлен со старшим коэффициентом 1 служит минимальным многочленом для каждого из своих корней.

Укажем некоторые свойства минимального многочлена.

Лемма 1

1. Минимальный многочлен любого алгебраического числа неприводим.

2. Если $f(x)$ – минимальный многочлен числа α, которое также является корнем многочлена $g(x) \in \mathbb{Q}[x]$, то многочлен $g(x)$ делится на $f(x)$.

3. Неприводимый многочлен со старшим коэффициентом 1 служит минимальным многочленом для каждого из своих корней.

4. Все корни минимального многочлена различны.

Укажем некоторые свойства минимального многочлена.

Лемма 1

1. Минимальный многочлен любого алгебраического числа неприводим.
2. Если $f(x)$ – минимальный многочлен числа α, которое также является корнем многочлена $g(x) \in \mathbb{Q}[x]$, то многочлен $g(x)$ делится на $f(x)$.
3. Неприводимый многочлен со старшим коэффициентом 1 служит минимальным многочленом для каждого из своих корней.
4. Все корни минимального многочлена различны.

Множество всех алгебраических чисел будем обозначать буквой $\mathbb{A}$.

Пусть α алгебраическое число, и его минимальный многочлен $f(x) \in \mathbb{Q}[x]$ может быть разложен в произведение двух многочленов $u(x), v(x) \in \mathbb{Q}[x]$ меньшей степени. Из равенства

$$0 = f(\alpha) = u(\alpha)v(\alpha)$$

следует $g(\alpha) = 0$ или $h(\alpha) = 0$. В любом случае получаем противоречие, ведь $f(x)$ имеет минимальную степень среди всех ненулевых многочленов кольца $\mathbb{Q}[x]$, обращающихся в нуль в точке α.

Пусть α алгебраическое число, и его минимальный многочлен $f(x) \in \mathbb{Q}[x]$ может быть разложен в произведение двух многочленов $u(x), v(x) \in \mathbb{Q}[x]$ меньшей степени. Из равенства

$$0 = f(\alpha) = u(\alpha)v(\alpha)$$

следует $g(\alpha) = 0$ или $h(\alpha) = 0$. В любом случае получаем противоречие, ведь $f(x)$ имеет минимальную степень среди всех ненулевых многочленов кольца $\mathbb{Q}[x]$, обращающихся в нуль в точке α.

Для доказательства второго утверждения разделим многочлен $g(x)$ на $f(x)$ с остатком

$$g(x) = f(x)q(x) + r(x), \qquad \deg r(x) < \deg f(x).$$

Справедливы равенства

$$0 = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Из определения минимального многочлена, равенства $r(\alpha) = 0$ и неравенства $\deg r(x) < \deg f(x)$ следует $r(x) = 0$, т.е. многочлен $g(x)$ делится на $f(x)$ без остатка.

Пусть $g(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ – неприводимый многочлен из кольца $\mathbb{Q}[x]$ и β – его корень. Обозначим минимальный многочлен числа β через $f(x)$. Согласно второму утверждению леммы имеем $f(x)|g(x)$. По условию многочлен $g(x)$ неприводим, значит, $g(x) = cf(x)$, где c – некоторая константа. Старшие коэффициенты многочленов $f(x)$, $g(x)$ равны единице, поэтому $g(x) = f(x)$ и $g(x)$ есть минимальный многочлен β. Третье утверждение леммы доказано.

Пусть $g(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ – неприводимый многочлен из кольца $\mathbb{Q}[x]$ и β – его корень. Обозначим минимальный многочлен числа β через $f(x)$. Согласно второму утверждению леммы имеем $f(x)|g(x)$. По условию многочлен $g(x)$ неприводим, значит, $g(x) = cf(x)$, где c – некоторая константа. Старшие коэффициенты многочленов $f(x)$, $g(x)$ равны единице, поэтому $g(x) = f(x)$ и $g(x)$ есть минимальный многочлен β. Третье утверждение леммы доказано.
Пусть $f(x)$ – минимальный многочлен алгебраического числа α и β – кратный корень $f(x)$. По первому утверждению леммы многочлен $f(x)$ неприводим и тогда по третьему утверждению он есть минимальный многочлен β. Так как β есть кратный корень многочлена $f(x)$, то производная $f'(x) \in \mathbb{Q}[x]$ также имеет β своим корнем. Согласно второму утверждению леммы имеем $f(x)|f'(x)$, что невозможно, так как $\deg f'(x) < \deg f(x)$. Итак, многочлен $f(x)$ не имеет кратных корней.

Если α – алгебраическое число степени n, то корни $\alpha_1, \ldots, \alpha_n$ его минимального многочлена называются числами, *сопряженными* с α. Докажем, что множество всех алгебраических чисел замкнуто относительно арифметических операций.

Теорема 9

Если α и β – алгебраические числа, то числа $\alpha + \beta$, $\beta - \alpha$, $\alpha\beta$, а в случае, если $\alpha \neq 0$, то и β/α являются алгебраическими числами.

Из этой теоремы следует, что множество всех алгебраических чисел является полем. Коммутативность и ассоциативность операций сложения и умножения, а также дистрибутивность умножения выполняются, поскольку они имеют место в поле комплексных чисел. Числа 0 и 1 являются алгебраическими.

Элементарные симметрические многочлены.

Напоминание. Пусть **A** – некоторое коммутативное кольцо с единицей и $t_1, \ldots, t_n$ — переменные. Многочлен $F(t_1, \ldots, t_n) \in \mathbf{A}[t_1, \ldots, t_n]$ называется *симметрическим*, если он не меняется при любой перестановке переменных. Чтобы привести примеры симметрических многочленов введем еще одну переменную x и рассмотрим равенство

$$(x - t_1) \cdots (x - t_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n.$$

Здесь буквами $\sigma_1, \ldots, \sigma_n$ обозначены многочлены

$$\begin{aligned}
\sigma_1 &= t_1 + t_2 + \cdots + t_n, \\
\sigma_2 &= t_1 t_2 + t_1 t_3 + \cdots + t_{n-1} t_n, \\
&\cdots\cdots\cdots\cdots\cdots \\
\sigma_n &= t_1 t_2 \cdots t_n.
\end{aligned}$$

Эти многочлены обладают свойством симметрии и называются *элементарными симметрическими многочленами*.

Теорема о симметрических многочленах: *Пусть*

$$F[t_1, \ldots, t_n] \in \mathbf{A}[t_1, \ldots, t_n]$$

– симметрический многочлен степени d. Тогда существует многочлен $G[z_1, \ldots, z_n] \in \mathbf{A}[z_1, \ldots, z_n]$ степени не выше d, такой, что

$$F[t_1, \ldots, t_n] = G[\sigma_1, \ldots, \sigma_n].$$

Теорема о симметрических многочленах: *Пусть*

$$F[t_1, \ldots, t_n] \in \mathbf{A}[t_1, \ldots, t_n]$$

– симметрический многочлен степени d. Тогда существует многочлен $G[z_1, \ldots, z_n] \in \mathbf{A}[z_1, \ldots, z_n]$ степени не выше d, такой, что

$$F[t_1, \ldots, t_n] = G[\sigma_1, \ldots, \sigma_n].$$

Например, имеет место тождество

$$t_1^2 + t_2^2 + \ldots + t_n^2 = \sigma_1^2 - 2\sigma_2.$$

Следствием теоремы о симметрических многочленах является

Лемма 2

Пусть $P(x, y) \in \mathbb{Q}[x, y]$ – многочлен от двух переменных с рациональными коэффициентами. Пусть также α – алгебраическое число степени n и $\alpha_1, \ldots, \alpha_n$ – все сопряженные с ним числа. Тогда

$$P(x, \alpha_1) \cdot P(x, \alpha_2) \cdot \ldots \cdot P(x, \alpha_n) = R(x), \qquad (1)$$

есть многочлен от переменной x с коэффициентами из поля рациональных чисел $\mathbb{Q}$.

Пусть $\mathbf{A} = \mathbb{Q}[x]$ – кольцо многочленов от переменной x. Рассмотрим произведение $P(x, t_1) \cdot P(x, t_2) \cdot \ldots \cdot P(x, t_n)$, где $t_1, \ldots, t_n$ – переменные. Этот многочлен не меняется при любой перестановке переменных $t_1, \ldots, t_n$, в произведении лишь меняются местами сомножители. Так что это произведение есть симметрический многочлен от переменных $t_1, \ldots, t_n$ с коэффициентами из кольца $\mathbf{A} = \mathbb{Q}[x]$.

Из теоремы о симметрических многочленах следует теперь, что для некоторого многочлена $Q(x, z_1, \ldots, x_n)$ с рациональными коэффициентами выполняется равенство

$$P(x, t_1) \cdot P(x, t_2) \cdot \ldots \cdot P(x, t_n) = Q(x, \sigma_1, \sigma_2, \ldots, \sigma_n), \qquad (2)$$

где $\sigma_1, \ldots, \sigma_n$ — элементарные симметрические многочлены. Заменим в (3) переменные $t_1, \ldots, t_n$ числами $\alpha_1, \ldots, \alpha_n$. Тогда левая часть (3) примет такой же вид, как и левая часть (1). Если $p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in \mathbb{Q}[x]$ – минимальный многочлен числа α, то согласно теореме Виета выполняются равенства

$$\sigma_1(\alpha_1, \ldots, \alpha_n) = -a_1, \quad \sigma_2(\alpha_1, \ldots, \alpha_n) = a_2, \ \ldots \ ,$$
$$\sigma_n(\alpha_1, \ldots, \alpha_n) = (-1)^n a_n.$$

Правая часть равенства (3) после указанной выше подстановки примет вид $Q(x, -a_1, a_2, \ldots, (-1)^n a_n) = R(x) \in \mathbb{Q}[x]$.

Доказательство теоремы 9.

Будем считать $\alpha \neq 0$, иначе утверждение тривиально. Пусть $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ – числа, сопряженные с α, а $g(x)$ – минимальный многочлен числа β. По лемме 2 многочлены

$$R_1(x) = \prod_{j=1}^{n} g(x + \alpha_j), \qquad R_2(x) = \prod_{j=1}^{n} g(x - \alpha_j),$$

$$R_3(x) = \prod_{j=1}^{n} g(x\alpha_j), \qquad R_4(x) = \prod_{j=1}^{n} \alpha_j^m g(x\alpha_j^{-1})$$

принадлежат кольцу $\mathbb{Q}[x]$. Так как $\alpha = \alpha_1$, то

$$g(\beta - \alpha + \alpha_1) = g(\alpha + \beta - \alpha_1) = g(\beta\alpha^{-1} \cdot \alpha_1) = g(\alpha\beta \cdot \alpha_1^{-1}) = g(\beta) = 0,$$

и, значит, $R_1(\beta - \alpha) = 0$, $R_2(\alpha + \beta) = 0$, $R_3(\beta/\alpha) = 0$ и $R_4(\alpha\beta) = 0$. Таким образом, каждое из чисел $\beta - \alpha$, $\alpha + \beta$, β/α и $\alpha\beta$ есть корень многочлена с рациональными коэффициентами. Поэтому все они – алгебраические числа. Теорема 9 доказана.

§2. Целые алгебраические числа.

Алгебраическое число α называется *целым алгебраическим*, если его минимальный многочлен имеет целые коэффициенты.

Примеры.

1. Число $\alpha = \frac{1}{\sqrt{2}}$ не есть целое алгебраическое, так-как его минимальный многочлен $x^2 - \frac{1}{2} \notin \mathbb{Z}[x]$.
2. Число $\alpha = \frac{1+\sqrt{5}}{2}$ — целое алгебраическое, так как его минимальный многочлен $x^2 - x - 1$ имеет целые коэффициенты.
3. Рациональное число является целым алгебраическим тогда и только тогда, когда оно целое.

§2. Целые алгебраические числа.

Алгебраическое число α называется *целым алгебраическим*, если его минимальный многочлен имеет целые коэффициенты.

Примеры.

1. Число $\alpha = \frac{1}{\sqrt{2}}$ не есть целое алгебраическое, так-как его минимальный многочлен $x^2 - \frac{1}{2} \notin \mathbb{Z}[x]$.
2. Число $\alpha = \frac{1+\sqrt{5}}{2}$ — целое алгебраическое, так как его минимальный многочлен $x^2 - x - 1$ имеет целые коэффициенты.
3. Рациональное число является целым алгебраическим тогда и только тогда, когда оно целое.

Многочлен с целыми коэффициентами называется *примитивным*, если его коэффициенты взаимно просты в совокупности.

Лемма Гаусса.

Лемма 3

Произведение примитивных многочленов есть примитивный многочлен.

Достаточно доказать лемму для двух многочленов.
Пусть $A(x) = \sum_{i=0}^{n} a_i x^i$, $B(x) = \sum_{j=0}^{m} b_j x^j$. Тогда $A(x)B(x) = C(x) = \sum_{k=0}^{n+m} c_k x^k$, где $c_k = \sum_{i+j=k} a_i b_j$.
Предположим, что многочлен C не примитивный, тогда найдётся простое число p, делящее все его коэффициенты. В силу примитивности многочленов A и B, у них найдутся коэффициенты, не делящиеся на p. Выберем среди них коэффициенты с минимальными номерами, пусть это будут a_u и b_v. Имеем $c_{u+v} = \sum_{k+l=u+v} a_k b_l$. В силу минимальности u и v, если $k < u$, то $p \mid a_k$, а если $l < v$, то $p \mid b_l$. Поэтому $c_{u+v} \equiv a_u b_v \not\equiv 0 \pmod{p}$. Противоречие.

Следствие 1

Если $A(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in \mathbb{Z}[x]$ *и* $A(\alpha) = 0$, *то* α *целое алгебраическое.*

Заметим, что в этом утверждении не требуется неприводимость многочлена $A(x)$.
Пусть $f(x)$ — минимальный многочлен числа α. Многочлены $A(x)$ и $f(x)$ имеют общий корень α. Многочлен $f(x)$ неприводим над $\mathbb{Q}$, поэтому $f(x) \mid A(x)$ в кольце $\mathbb{Q}[x]$. Имеем $A(x) = f(x)Q(x)$, где $Q(x) \in \mathbb{Q}[x]$. Старшие коэффициенты многочленов $A(x)$ и $f(x)$ равны 1, значит, и старший коэффициент $Q(x)$ равен единице. Пусть $q_r > 0$ — наименьший общий знаменатель коэффициентов многочлена Q, то есть

$$Q(x) = x^r + \frac{q_{r-1}}{q_r}x^{r-1} + \ldots + \frac{q_0}{q_r}.$$

Числа $q_0 \ldots, q_{r-1}, q_r$ взаимно просты в совокупности, иначе q_r не был бы наименьшим общим знаменателем коэффициентов $Q(x)$.

Многочлен $Q(x)$ представим в виде $Q(x) = \frac{1}{q_r} U(x)$, где $U(x)$ примитивный многочлен. Аналогично $f(x) = \frac{1}{p_s} V(x)$, где $V(x)$ примитивный. Но тогда $A(x) = \frac{1}{q_r p_s} U(x)V(x)$ и $U(x)V(x) = q_r p_s A(x)$. По лемме Гаусса многолен $U(x)V(x)$ примитивен, а по условию $A(x) \in \mathbb{Z}[x]$, поэтому $q_r p_s = 1$, и $p_s = q_r = 1$. Значит, $f(x) \in \mathbb{Z}[x]$ и α целое алгебраическое число.

Теорема 10

Множество целых алгебраических чисел замкнуто относительно операций сложения, вычитания и умножения.

Для доказательства достаточно проверить, что в условиях данной теоремы построенные в доказательстве теоремы 9 полиномы $R_1(x), R_2(x), R_4(x)$ лежат в кольце $\mathbb{Z}[x]$ и их старшие коэффициенты равны 1. Это обеспечит выполнимость условий следствия 1 и, значит, справедливость теоремы 10. Само доказательство дословно повторяет доказательство теоремы 9, с заменой в теореме о симметрических многоленах и лемме 2 кольца $\mathbb{Q}$ на кольцо $\mathbb{Z}$.

Лемма 4

Если α алгебраическое число, то для него найдется $d \in \mathbb{N}$, для которого $d\alpha$ целое алгебраическое.

Пусть $f(x)$ минимальный многолен числа α, $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Q}[x]$. Пусть d общий знаменатель всех a_i. Домножим многочлен $f(x)$ на d^n и выделим в мономе степени k множитель $(d\alpha)^k$:

$$0 = d^n \cdot f(\alpha) = (d\alpha)^n + da_{n-1}(d\alpha)^{n-1} + \ldots + d^n a_0.$$

Значит, многочлен $A(x) = x^n + da_{n-1}x^{n-1} + \ldots + d^n a_0$ обращается в нуль при подстановке $d\alpha$ вместо x, а в силу выбора d имеем $A \in \mathbb{Z}[x]$.

§3. Теорема о примитивном элементе.

Пусть $\xi_1, \ldots, \xi_m$ – алгебраические числа. Обозначим символом $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ наименьшее поле, содержащее все числа ξ_i, а также поле рациональных чисел $\mathbb{Q}$, т.е. множество чисел вида

$$\frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \qquad A, B \in \mathbb{Q}[\xi_1, \ldots, \xi_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0.$$

Говорят, что числа $\xi_1, \ldots, \xi_m$ порождают поле $\mathbb{Q}(\xi_1, \ldots, \xi_m)$. Из теоремы 10 следует, что все его элементы являются алгебраическими числами.

§3. Теорема о примитивном элементе.

Пусть $\xi_1, \ldots, \xi_m$ – алгебраические числа. Обозначим символом $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ наименьшее поле, содержащее все числа ξ_i, а также поле рациональных чисел $\mathbb{Q}$, т.е. множество чисел вида

$$\frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \qquad A, B \in \mathbb{Q}[\xi_1, \ldots, \xi_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0.$$

Говорят, что числа $\xi_1, \ldots, \xi_m$ порождают поле $\mathbb{Q}(\xi_1, \ldots, \xi_m)$. Из теоремы 10 следует, что все его элементы являются алгебраическими числами.
Рассмотрим сначала структуру таких полей в случае $m = 1$.

Лемма 5

Пусть ξ алгебраическое число степени n. Тогда каждый элемент α поля $\mathbb{Q}(\xi)$ единственным образом представляется в виде

$$\alpha = r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \qquad r_j \in \mathbb{Q}. \tag{3}$$

Освобождение от знаменателей.

Пусть $p(x)$ – минимальный многочлен ξ. Каждый элемент $\alpha \in \mathbb{Q}(\xi)$ может быть представлен в виде $\alpha = \frac{A(\xi)}{B(\xi)}$, где $A(x), B(x) \in \mathbb{Q}[x]$, $B(\xi) \neq 0$. Многочлен $p(x)$ неприводим. Если $p(x)$ – делитель $B(x)$, то каждый корень $p(x)$ и, в частности, ξ, должен быть корнем многочлена $B(x)$. Но это неверно. Значит многочлены $p(x)$ и $B(x)$ взаимно просты. В этом случае существуют такие многочлены $u(x), v(x) \in \mathbb{Q}[x]$, что

$$u(x)p(x) + v(x)B(x) = 1.$$

Подставляя сюда $x = \xi$ и пользуясь тем, что $p(\xi) = 0$, находим $v(\xi)B(\xi) = 1$ и $\alpha = A(\xi)v(\xi)$.

Освобождение от знаменателей.

Пусть $p(x)$ – минимальный многочлен ξ. Каждый элемент $\alpha \in \mathbb{Q}(\xi)$ может быть представлен в виде $\alpha = \frac{A(\xi)}{B(\xi)}$, где $A(x), B(x) \in \mathbb{Q}[x]$, $B(\xi) \neq 0$. Многочлен $p(x)$ неприводим. Если $p(x)$ – делитель $B(x)$, то каждый корень $p(x)$ и, в частности, ξ, должен быть корнем многочлена $B(x)$. Но это неверно. Значит многочлены $p(x)$ и $B(x)$ взаимно просты. В этом случае существуют такие многочлены $u(x), v(x) \in \mathbb{Q}[x]$, что

$$u(x)p(x) + v(x)B(x) = 1.$$

Подставляя сюда $x = \xi$ и пользуясь тем, что $p(\xi) = 0$, находим $v(\xi)B(\xi) = 1$ и $\alpha = A(\xi)v(\xi)$. Разделим теперь многочлен $A(x)v(x)$ на $p(x)$ с остатком, т.е. определим многочлены $q(x), r(x) \in \mathbb{Q}[x]$ условиями

$$A(x)v(x) = q(x)p(x) + r(x), \qquad \deg r(x) < \deg p(x) = n.$$

Подставляя $x = \xi$ в последнее равенство, находим $\alpha = r(\xi)$, что доказывает (3).

Теорема о примитивном элементе

Существование двух многочленов $r(x), s(x) \in \mathbb{Q}[x]$ с условиями

$$\alpha = r(\xi), \quad \alpha = s(\xi), \qquad \deg r(x) < n, \quad \deg s(x) < n,$$

означало бы, что $r(\xi) = s(\xi)$ и, согласно второму из свойств минимальных многочленов, что $p(x)|(r(x) - s(x))$. Степень делимого меньше $n = \deg p(x)$, поэтому $r(x) = s(x)$.

Теорема о примитивном элементе

Существование двух многочленов $r(x), s(x) \in \mathbb{Q}[x]$ с условиями

$$\alpha = r(\xi), \quad \alpha = s(\xi), \qquad \deg r(x) < n, \quad \deg s(x) < n,$$

означало бы, что $r(\xi) = s(\xi)$ и, согласно второму из свойств минимальных многочленов, что $p(x)|(r(x) - s(x))$. Степень делимого меньше $n = \deg p(x)$, поэтому $r(x) = s(x)$.

Теорема 11 (О примитивном элементе.)

Всякое поле $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, порожденное алгебраическими числами $\xi_1, \ldots, \xi_m$, может быть порождено одним числом. Другими словами, существует такое число $\theta \in E$, что $E = \mathbb{Q}(\theta)$.

Теорема о примитивном элементе

Существование двух многочленов $r(x), s(x) \in \mathbb{Q}[x]$ с условиями

$$\alpha = r(\xi), \quad \alpha = s(\xi), \qquad \deg r(x) < n, \quad \deg s(x) < n,$$

означало бы, что $r(\xi) = s(\xi)$ и, согласно второму из свойств минимальных многочленов, что $p(x)|(r(x) - s(x))$. Степень делимого меньше $n = \deg p(x)$, поэтому $r(x) = s(x)$.

Теорема 11 (О примитивном элементе.)

Всякое поле $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, порожденное алгебраическими числами $\xi_1, \ldots, \xi_m$, может быть порождено одним числом. Другими словами, существует такое число $\theta \in E$, что $E = \mathbb{Q}(\theta)$.

Число θ, порождающее поле E, называется его *примитивным элементом*.

Пример.

Рассмотрим, например, поле $\mathbb{Q}(\sqrt{2},\sqrt{3})$ и число $\theta=\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. Справедливы равенства

$$(\theta-\sqrt{2})^2=3,\qquad (\theta-\sqrt{3})^2=2,$$

из которых следует, что

$$\sqrt{2}=\frac{\theta^2-1}{2\theta},\qquad \sqrt{3}=\frac{\theta^2+1}{2\theta}.$$

Поэтому $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\theta)$ и $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\theta)$.

Доказательство теоремы 11.

Докажем сначала нужное утверждение для поля, порожденного двумя алгебраическими числами, т.е. будем считать, что $E = \mathbb{Q}(\alpha, \beta)$. Пусть степени чисел α, β равны соответственно m и n, а

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0, \quad g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$$

– их минимальные многочлены. Корни этих многочленов, т.е. числа сопряженные с α, β, обозначим $\alpha_1, \ldots, \alpha_m$ и $\beta_1, \ldots, \beta_n$ соответственно. При этом будем считать $\alpha = \alpha_1$, $\beta = \beta_1$. Все числа α_i, равно как и числа β_j, различны между собой. Выберем $c \in \mathbb{Q}$ так, чтобы

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1, \qquad \text{при} \qquad (i, k) \neq (1, 1). \tag{4}$$

Это, очевидно, можно сделать, ведь каждое уравнение $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ при $(i, k) \neq (1, 1)$ имеет не более одного решения, а поле $\mathbb{Q}$ бесконечно.

Доказательство теоремы 11.

Положим $\theta = \alpha + c\beta$ и обозначим $L = \mathbb{Q}(\theta)$. Справедливо включение $L \subset \mathbb{Q}(\alpha, \beta)$. В дальнейших рассуждениях будет использоваться многочлен

$$h(x) = f(\theta - cx) \in L[x].$$

Принадлежащие кольцу $L[x]$ многочлены $g(x)$ и $h(x)$ имеют общий корень β, ведь $h(\beta) = f(\theta - c\beta) = f(\alpha) = 0$. Если $d(x)$ – их наибольший общий делитель, то с некоторыми многочленами $u(x), v(x) \in L[x]$ выполняется равенство $g(x)u(x) + h(x)v(x) = d(x)$. Из этого равенства следует, что число β является корнем многочлена $d(x) \in L[x]$.
Так как $d(x)$ – делитель неприводимого над полем $\mathbb{Q}$ многочлена $g(x)$, то $d(x)$ не имеет кратных корней.
Предположим, что $\deg d(x) > 1$. Тогда многочлен $d(x)$ имеет корень γ, отличный от β. Все корни $d(x)$ содержатся среди корней многочлена $g(x)$. Поэтому $\gamma = \beta_k$ с некоторым номером $k > 1$.

Завершение доказательства теоремы 11.

Учитывая, что γ является также корнем многочлена $h(x)$, т.е. $0 = h(\gamma) = f(\theta - c\gamma)$, заключаем, что $\theta - c\gamma = \alpha_i$ с некоторым номером i. Но тогда $\theta = \alpha_i + c\beta_k$ вопреки (4).
Получившееся противоречие доказывает, что $\deg d(x) = 1$, т.е. $d(x) = ax + b \in L[x]$. Но тогда $\beta = -b/a \in L$ и $\alpha = \theta - c\beta \in L$. Следовательно, $\mathbb{Q}(\alpha, \beta) = L = \mathbb{Q}(\theta)$, чем и завершается доказательство теоремы 11 для полей, порожденных двумя числами.

Завершение доказательства теоремы 11.

Учитывая, что γ является также корнем многочлена $h(x)$, т.е. $0 = h(\gamma) = f(\theta - c\gamma)$, заключаем, что $\theta - c\gamma = \alpha_i$ с некоторым номером i. Но тогда $\theta = \alpha_i + c\beta_k$ вопреки (4).

Получившееся противоречие доказывает, что $\deg d(x) = 1$, т.е. $d(x) = ax + b \in L[x]$. Но тогда $\beta = -b/a \in L$ и $\alpha = \theta - c\beta \in L$. Следовательно, $\mathbb{Q}(\alpha, \beta) = L = \mathbb{Q}(\theta)$, чем и завершается доказательство теоремы 11 для полей, порожденных двумя числами.

Пусть теперь $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$. Если считать теорему доказанной для полей, порожденных $m - 1$ числом, то $\mathbb{Q}(\xi_1, \ldots, \xi_{m-1}) = \mathbb{Q}(\eta)$ для некоторого алгебраического числа η. Так что $E = \mathbb{Q}(\eta, \xi_m)$. Пользуясь уже доказанным утверждением для полей, порожденных двумя числами, заключаем, что с некоторым $\theta \in E$ будет выполняться равенство $E = \mathbb{Q}(\theta)$.

Следствие 2

Каждое поле, порожденное конечным количеством алгебраических чисел, есть конечномерное линейное пространство над $\mathbb{Q}$.

Действительно, пусть $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$ — поле, порожденное алгебраическими числами $\xi_1, \ldots, \xi_m$, и $\theta \in E$ примитивный элемент E. Согласно лемме 5 каждый элемент α поля $E = \mathbb{Q}(\theta)$ единственным образом представляется в виде

$$\alpha = r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}, \qquad r_j \in \mathbb{Q}, \tag{5}$$

где $n = \deg \theta$. Отсюда следует, что $E = \mathbb{Q}(\theta)$ есть конечномерное линейное пространство над полем $\mathbb{Q}$ с базисом $1, \theta, \theta^2, \ldots, \theta^{n-1}$.

Степенью расширения $E \supset \mathbb{Q}$ или *степенью поля* E над полем рациональных чисел называется размерность линейного пространства E над $\mathbb{Q}$. Она обозначается символом $[E : \mathbb{Q}]$, то есть $[E : \mathbb{Q}] = \dim_{\mathbb{Q}} E = \deg \theta$.

Конец
девятой лекции.

Лекция 10.
Теорема о примитивном элементе. Алгебраическая замкнутость поля алгебраических чисел. Нормальные расширения.

§3. Теорема о примитивном элементе.

Пусть $\xi_1, \ldots, \xi_m$ – алгебраические числа. Обозначим символом $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ наименьшее поле, содержащее все числа ξ_i, а также поле рациональных чисел $\mathbb{Q}$, т.е. множество чисел вида

$$\frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \qquad A, B \in \mathbb{Q}[\xi_1, \ldots, \xi_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0.$$

Говорят, что числа $\xi_1, \ldots, \xi_m$ порождают поле $\mathbb{Q}(\xi_1, \ldots, \xi_m)$. Из теоремы 10 прошлой лекции следует, что все его элементы являются алгебраическими числами.

§3. Теорема о примитивном элементе.

Пусть $\xi_1, \ldots, \xi_m$ – алгебраические числа. Обозначим символом $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ наименьшее поле, содержащее все числа ξ_i, а также поле рациональных чисел $\mathbb{Q}$, т.е. множество чисел вида

$$\frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \qquad A, B \in \mathbb{Q}[\xi_1, \ldots, \xi_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0.$$

Говорят, что числа $\xi_1, \ldots, \xi_m$ порождают поле $\mathbb{Q}(\xi_1, \ldots, \xi_m)$. Из теоремы 10 прошлой лекции следует, что все его элементы являются алгебраическими числами.

Теорема 11 (О примитивном элементе.)

Всякое поле $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, порожденное алгебраическими числами $\xi_1, \ldots, \xi_m$, может быть порождено одним числом. Другими словами, существует такое число $\theta \in E$, что $E = \mathbb{Q}(\theta)$.

§3. Теорема о примитивном элементе.

Пусть $\xi_1, \ldots, \xi_m$ – алгебраические числа. Обозначим символом $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ наименьшее поле, содержащее все числа ξ_i, а также поле рациональных чисел $\mathbb{Q}$, т.е. множество чисел вида

$$\frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \qquad A, B \in \mathbb{Q}[\xi_1, \ldots, \xi_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0.$$

Говорят, что числа $\xi_1, \ldots, \xi_m$ порождают поле $\mathbb{Q}(\xi_1, \ldots, \xi_m)$. Из теоремы 10 прошлой лекции следует, что все его элементы являются алгебраическими числами.

Теорема 11 (О примитивном элементе.)

Всякое поле $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, порожденное алгебраическими числами $\xi_1, \ldots, \xi_m$, может быть порождено одним числом. Другими словами, существует такое число $\theta \in E$, что $E = \mathbb{Q}(\theta)$.

Число θ, порождающее поле E, называется его *примитивным элементом*.

Доказательство теоремы 11.

Докажем сначала нужное утверждение для поля, порожденного двумя алгебраическими числами, т.е. будем считать, что $E = \mathbb{Q}(\alpha, \beta)$. Пусть степени чисел α, β равны соответственно m и n, а

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0, \quad g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$$

– их минимальные многочлены. Корни этих многочленов, т.е. числа сопряженные с α, β, обозначим $\alpha_1, \ldots, \alpha_m$ и $\beta_1, \ldots, \beta_n$ соответственно. При этом будем считать $\alpha = \alpha_1$, $\beta = \beta_1$. Все числа α_i, равно как и числа β_j, различны между собой. Выберем $c \in \mathbb{Q}$ так, чтобы

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1, \qquad \text{при} \qquad (i, k) \neq (1, 1). \qquad (1)$$

Это, очевидно, можно сделать, ведь каждое уравнение $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ при $(i, k) \neq (1, 1)$ имеет не более одного решения, а поле $\mathbb{Q}$ бесконечно.

Доказательство теоремы 11.

Положим $\theta = \alpha + c\beta$ и обозначим $L = \mathbb{Q}(\theta)$. Справедливо включение $L \subset \mathbb{Q}(\alpha, \beta)$. В дальнейших рассуждениях будет использоваться многочлен

$$h(x) = f(\theta - cx) \in L[x].$$

Принадлежащие кольцу $L[x]$ многочлены $g(x)$ и $h(x)$ имеют общий корень β, ведь $h(\beta) = f(\theta - c\beta) = f(\alpha) = 0$. Если $d(x)$ – их наибольший общий делитель, то с некоторыми многочленами $u(x), v(x) \in L[x]$ выполняется равенство $g(x)u(x) + h(x)v(x) = d(x)$. Из этого равенства следует, что число β является корнем многочлена $d(x) \in L[x]$.
Так как $d(x)$ – делитель неприводимого над полем $\mathbb{Q}$ многочлена $g(x)$, то $d(x)$ не имеет кратных корней.
Предположим, что $\deg d(x) > 1$. Тогда многочлен $d(x)$ имеет корень γ, отличный от β. Все корни $d(x)$ содержатся среди корней многочлена $g(x)$. Поэтому $\gamma = \beta_k$ с некоторым номером $k > 1$.

Завершение доказательства теоремы 11.

Учитывая, что γ является также корнем многочлена $h(x)$, т.е. $0 = h(\gamma) = f(\theta - c\gamma)$, заключаем, что $\theta - c\gamma = \alpha_i$ с некоторым номером i. Но тогда $\theta = \alpha_i + c\beta_k$ вопреки (1).
Получившееся противоречие доказывает, что $\deg d(x) = 1$, т.е. $d(x) = ax + b \in L[x]$. Но тогда $\beta = -b/a \in L$ и $\alpha = \theta - c\beta \in L$. Следовательно, $\mathbb{Q}(\alpha, \beta) = L = \mathbb{Q}(\theta)$, чем и завершается доказательство теоремы 11 для полей, порожденных двумя числами.

Завершение доказательства теоремы 11.

Учитывая, что γ является также корнем многочлена $h(x)$, т.е. $0 = h(\gamma) = f(\theta - c\gamma)$, заключаем, что $\theta - c\gamma = \alpha_i$ с некоторым номером i. Но тогда $\theta = \alpha_i + c\beta_k$ вопреки (1).

Получившееся противоречие доказывает, что $\deg d(x) = 1$, т.е. $d(x) = ax + b \in L[x]$. Но тогда $\beta = -b/a \in L$ и $\alpha = \theta - c\beta \in L$. Следовательно, $\mathbb{Q}(\alpha, \beta) = L = \mathbb{Q}(\theta)$, чем и завершается доказательство теоремы 11 для полей, порожденных двумя числами.

Пусть теперь $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$. Если считать теорему доказанной для полей, порожденных $m - 1$ числом, то $\mathbb{Q}(\xi_1, \ldots, \xi_{m-1}) = \mathbb{Q}(\eta)$ для некоторого алгебраического числа η. Так что $E = \mathbb{Q}(\eta, \xi_m)$. Пользуясь уже доказанным утверждением для полей, порожденных двумя числами, заключаем, что с некоторым $\theta \in E$ будет выполняться равенство $E = \mathbb{Q}(\theta)$.

Следствие 1

Каждое поле, порожденное конечным количеством алгебраических чисел, есть конечномерное линейное пространство над $\mathbb{Q}$.

Действительно, пусть $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$ — поле, порожденное алгебраическими числами $\xi_1, \ldots, \xi_m$, и $\theta \in E$ примитивный элемент E. Согласно лемме 5 прошлой лекции каждый элемент α поля $E = \mathbb{Q}(\theta)$ единственным образом представляется в виде

$$\alpha = r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}, \qquad r_j \in \mathbb{Q}, \tag{2}$$

где $n = \deg \theta$. Отсюда следует, что $E = \mathbb{Q}(\theta)$ есть конечномерное линейное пространство над полем $\mathbb{Q}$ с базисом $1, \theta, \theta^2, \ldots, \theta^{n-1}$.

Степенью расширения $E \supset \mathbb{Q}$ или *степенью поля* E над полем рациональных чисел называется размерность линейного пространства E над $\mathbb{Q}$. Она обозначается символом $[E : \mathbb{Q}]$, то есть $[E : \mathbb{Q}] = \dim_{\mathbb{Q}} E = \deg \theta$.

§4. Алгебраическая замкнутость поля алгебраических чисел.

Теорема 12

Если число ξ – корень многочлена

$$\varphi(x) = \alpha_m x^m + \ldots + \alpha_1 x + \alpha_0, \qquad \alpha_m \neq 0,$$

с алгебраическими коэффициентами α_i, то ξ – алгебраическое число.

Иными словами, эта теорема утверждает, что поле всех алгебраических чисел нельзя расширить, присоединив к нему корень какого-либо многочлена с алгебраическими коэффициентами. Это свойство называется *алгебраической замкнутостью*. Поле комплексных чисел также обладает этим свойством.

Не уменьшая общности можно считать, что $\alpha_m = 1$. Согласно теореме о примитивном элементе для некоторого алгебраического числа θ выполняется равенство $E = \mathbb{Q}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \mathbb{Q}(\theta)$. Обозначим $n = \deg \theta$. По лемме **??** существуют такие многочлены $a_j(x) \in \mathbb{Q}[x]$, $0 \le j < m$, что $\deg a_j(x) < n$ и $\alpha_j = a_j(\theta)$.
Пусть $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ – числа, сопряженные с θ. Обозначим

$$P(x, y) = x^m + a_{m-1}(y)x^{m-1} + \ldots + a_1(y)x + a_0(y) \in \mathbb{Q}[x, y].$$

По лемме 2 из лекции 9

$$R(x) = \prod_{j=1}^{n} P(x, \theta_j) \in \mathbb{Q}[x].$$

Так как $P(\xi, \theta_1) = 0$, то $R(\xi) = 0$ и значит, ξ – алгебраическое число.

§5. Нормальные расширения.

Пусть $E \supset \mathbb{Q}$ — конечно порождённое расширение. Отображение $\sigma : E \to \mathbb{C}$ называется *вложением*, если σ сохраняет арифметические операции и есть взаимно однозначное отображение E на $\sigma(E)$.

§5. Нормальные расширения.

Пусть $E \supset \mathbb{Q}$ — конечно порождённое расширение. Отображение $\sigma : E \to \mathbb{C}$ называется *вложением*, если σ сохраняет арифметические операции и есть взаимно однозначное отображение E на $\sigma(E)$.

Теорема 13

Пусть E — конечно порождённое расширение $\mathbb{Q}$ и $n = [E : \mathbb{Q}]$. Существует в точности n вложений E в $\mathbb{C}$. Если $E = \mathbb{Q}(\theta)$ и $\theta_1, \ldots, \theta_n$ числа, сопряженные с θ, то все отображения $\sigma_i : E \to \mathbb{C}$, задаваемые для

$$\alpha = c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}, \quad c_j \in \mathbb{Q},$$

равенствами

$$\sigma_i(\alpha) = c_0 + c_1\theta_i + \ldots + c_{n-1}\theta_i^{n-1}, \qquad 1 \leq i \leq n,$$

суть различные вложения E в $\mathbb{C}$.

Докажем сначала, что σ_j отображает множество E на $\sigma_j(E)$ взаимно однознано. Пусть $\alpha = g(\theta)$, $\beta = h(\theta)$, где $g(x), h(x)$ — многочлены из $\mathbb{Q}[x]$ степени не выше $n-1$, и $\sigma_j(\alpha) = \sigma_j(\beta)$. Тогда $g(\theta_j) = h(\theta_j)$. Учитывая, что $\deg \theta_j = n > \deg(g(x) - h(x))$, заключаем, что $g(x) = h(x)$ и $\alpha = g(\theta) = h(\theta) = \beta$. Взаимная однозначность доказана.

Для доказательства того, что σ_j сохраняет операцию сложения обозначим $\varphi(x) = g(x) + h(x), \deg \varphi(x) \leq n-1$. Тогда $\alpha + \beta = \varphi(\theta)$ и

$$\sigma_j(\alpha + \beta) = \varphi(\theta_j) = g(\theta_j) + h(\theta_j) = \sigma_j(\alpha) + \sigma_j(\beta).$$

Обозначим $f(x)$ минимальный многочлен числа θ, $\deg f(x) = n$. Существуют многолены $q(x), r(x) \in \mathbb{Q}[x], \deg r(x) \leq n-1$ такие, что

$$g(x)h(x) = q(x)f(x) + r(x).$$

Тогда, поскольку $f(\theta) = f(\theta_j) = 0$ и $\alpha\beta = g(\theta)h(\theta) = r(\theta)$ имеем

$$\sigma_j(\alpha\beta) = r(\theta_j) = g(\theta_j)h(\theta_j) = \sigma_j(\alpha)\sigma_j(\beta).$$

Докажем аналогичные утверждения для разности и отношения.
Если $\alpha - \beta = \gamma$, то $\alpha = \beta + \gamma$, $\sigma_j(\alpha) = \sigma_j(\beta) + \sigma_j(\gamma)$ и
$\sigma_j(\alpha - \beta) = \sigma_j(\gamma) = \sigma_j(\alpha) - \sigma_j(\beta)$.
Если $\gamma = \frac{\alpha}{\beta}$, где $\beta \neq 0$, то $\alpha = \beta\gamma$, $\sigma_j(\alpha) = \sigma_j(\beta)\sigma_j(\gamma)$ и

$$\sigma_j\left(\frac{\alpha}{\beta}\right) = \sigma_j(\gamma) = \frac{\sigma_j(\alpha)}{\sigma_j(\beta)}.$$

Здесь использовалось то, что $\sigma_j(\beta) \neq 0$, ведь по доказанному ранее отображение σ_j взаимно однозначно и $\sigma_j(0) = 0$.
Утверждение о том, что σ_j сохраняет арифметические операции, т.е. σ_j гомоморфизм доказано.
Все σ_j различны, поскольку $\sigma_j(\theta) = \theta_j \neq \theta_i = \sigma_i(\theta)$ при $i \neq j$.

Теперь докажем, что других вложений, кроме определённых в теореме 13, нет. Пусть σ произвольное вложение. Тогда при натуральном n и целых $p, q > 0$ имеем

$$\sigma(0) = \sigma(0+0) = \sigma(0) + \sigma(0) \Rightarrow \sigma(0) = 0;$$
$$\sigma(1) = \sigma(1 \cdot 1) = \sigma(1) \cdot \sigma(1) \Rightarrow \sigma(1) = 1;$$
$$\sigma(n) = \sigma(\underbrace{1+1+\cdots+1}_{n}) = \underbrace{\sigma(1)+\cdots+\sigma(1)}_{n} = n\sigma(1) = n;$$
$$\sigma(-n) = \sigma(0-n) = \sigma(0) - \sigma(n) = 0 - n = -n;$$
$$\sigma\left(\frac{p}{q}\right) = \frac{\sigma(p)}{\sigma(q)} = \frac{p}{q}.$$

Итак, σ есть тождественное отображение на множестве рациональных чисел. Подействовав на равенство

$$f(\theta) = \theta^{\nu} + a_{\nu-1}\theta^{\nu-1} + \ldots + a_0 = 0, \qquad a_j \in \mathbb{Q},$$

вложением σ, получим

$$\sigma(\theta)^{\nu} + a_{\nu-1}\sigma(\theta)^{\nu-1} + \ldots + a_0 = 0.$$

Так что число $\sigma(\theta)$ должно совпадать с одним из корней θ_j многочлена $f(x)$. А тогда отображение σ совпадает с σ_j. Действительно, пусть $\alpha = r(\theta)$, тогда $\sigma(\alpha) = r(\sigma(\theta) = r(\theta_j)$. По теореме о примитивном элементе каждое конечно порождённое расширение поля $\mathbb{Q}$ может быть представлено в виде $\mathbb{Q}(\theta)$. Это доказывает также и первое утверждение теоремы.

Рассмотрим теперь вопрос, как устроены образы фиксированного алгебраического числа под действием вложений.

Теорема 14

Пусть $E \supset \mathbb{Q}$, $\nu = [E : \mathbb{Q}]$, $\alpha \in E$, $\deg \alpha = m$. *Тогда* $m \mid \nu$ *и множество* $\sigma_1(\alpha), \ldots, \sigma_\nu(\alpha)$ *состоит из сопряженных числа* α. *Каждое их них повторяется в этом множестве ровно* $\frac{\nu}{m}$ *раз.*

Пусть $E = \mathbb{Q}(\theta)$ и $\alpha = r(\theta)$. Тогда многочлен

$$F(x) = \prod_{j=1}^{\nu}(x - \sigma_j(\alpha)) = \prod_{j=1}^{\nu}(x - r(\theta_j)),$$

по следствитю из теоремы о симметрических многочленах лежит в $\mathbb{Q}[x]$. Обозначим минимальный многочлен числа α символом $f(x)$ и разделим многочлен $F(x)$ на максимально возможную степень $f(x)$, т.е. представим $F(x)$ в виде

$$F(x) = f(x)^k d(x), \qquad f(x) \nmid d(x), \quad k \geq 0. \tag{3}$$

$$F(x) = \prod_{j=1}^{\nu}(x - \sigma_j(\alpha)) = \prod_{j=1}^{\nu}(x - r(\theta_j)),$$

$$F(x) = f(x)^k d(x), \qquad f(x) \nmid d(x), \quad k \geq 0. \tag{4}$$

Докажем, что $d(x) \in \mathbb{Q}$. Если $\deg d \geq 1$ и β корень $d(x)$, то $F(\beta) = 0$. Значит, найдется индекс j, для которого $\beta = \sigma_j(\alpha)$ — корень многочлна $f(x)$. Подействуем на равенство $f(\alpha) = 0$ вложением σ_j. В результате получится $f(\sigma_j(\alpha) = 0$, то есть $f(\beta) = 0$. Стало быть, многочлены $f(x)$ и $d(x)$ имеют общий корень. Оба они лежат в кольце $\mathbb{Q}[x]$ и $f(x)$ неприводим, поэтому $f(x) \mid d(x)$ вопреки (3). Получившееся противоречие означает, что $d(x)$ не имеет корней. Поскольку старшие коэффициенты у многоленов $F(x)$ и $f(x)$ равны 1, то $d(x) = 1$ и $F(x) = f(x)^k$. Слева стоит многочлен степени ν, а справа степени km, отсюда и следует, что, во первых, $m \mid \nu$, а во вторых, множество корней $F(x)$ состоит из всех корней $f(x)$, причём каждый корень повторяется k раз.

Выше было доказано, что рациональные числа не меняются под действием вложений. Верно и обратное утверждение.

Следствие 2

Если число $\alpha \in E$ остаётся неизменным под действием всех вложений поля E в $\mathbb{C}$, то оно рационально.

Предположим, что $\deg \alpha \geq 2$. Тогда в силу предыдущей теоремы в наборе $\sigma_1(\alpha), \ldots, \sigma_\nu(\alpha)$ должно быть хотя бы два различных числа, а это противоречит условию.

Расширение $E \supset \mathbb{Q}$ называется *нормальным*, если для любого вложения $\sigma : E \to \mathbb{C}$ выполняется равенство $\sigma(E) = E$.

Примеры.

1. $E = \mathbb{Q}(\sqrt{2})$. Здесь только два вложения:

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}, \qquad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}, \quad a, b \in \mathbb{Q}$$

Ясно, что для обоих вложений выполняется равенство $\sigma(E) = E$. Поле E нормальное.

2. $F = \mathbb{Q}(\sqrt[3]{2})$. Многочлен $x^3 - 2$ имеет три корня: $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$, $\xi^2\sqrt[3]{2}$, где $\xi = e^{\frac{2\pi i}{3}}$. Рассмотрим вложение σ поля F в поле $\mathbb{C}$

$$\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \to a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4}.$$

Так как F — действительное поле, но $\sigma(\sqrt[3]{2}) = \xi\sqrt[3]{2}$ — не действительное число, то $\sigma(F) \neq F$. Значит, $F \supset \mathbb{Q}$ не нормальное расширение.

Достаточное условие нормальности

Теорема 15

Пусть $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, где $\xi_1, \ldots, \xi_m$ суть алгебраические числа, и все сопряженные каждого из ξ_i принадлежат E. Тогда E нормально.

Пусть α произвольный элемент из поля E. Тогда справедливо представление:

$$\alpha = \frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \quad A, B \in \mathbb{Q}[x_1, \ldots, x_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0.$$

Подействуем вложением σ на это равенство. Учитывая, что $B(\sigma(\xi_1), \ldots, \sigma(\xi_m)) = \sigma(B(\xi_1, \ldots, \xi_m)) \neq 0$, получаем

$$\sigma(\alpha) = \frac{A(\sigma(\xi_1), \ldots, \sigma(\xi_m))}{B(\sigma(\xi_1), \ldots, \sigma(\xi_m))}.$$

Так как $\sigma(\xi_i)$ сопряжено с ξ_i, то, согласно условию, при любом i находим $\sigma(\xi_i) \in E$. Значит, $\sigma(\alpha) \in E$ и $\sigma(E) \subset E$.

Достаточное условие нормальности

Докажем теперь обратное включение. Пусть $E = \mathbb{Q}(\theta)$, $\theta_1, \ldots, \theta_\nu$ — числа, сопряженные с θ. Образ θ при отображении σ — одно из сопряжённых с θ чисел, пусть это будет θ_k. Числа $1, \theta_k, \ldots, \theta_k^{\nu-1} \in E$ образуют базис E (степень θ_k равна ν), и потому всякое $\beta \in E$ можно представить в виде

$$\beta = r_0 + r_1\theta_k + \ldots + r_{\nu-1}\theta_k^{\nu-1}.$$

Найдём прообраз этого элемента: именно, положим

$$\alpha = r_0 + r_1\theta + \ldots + r_{\nu-1}\theta^{\nu-1} \in E.$$

Ясно что $\sigma(\alpha) = \beta$. А это и означает, что $E \subset \sigma(E)$.

Если E нормальное расширение, то отображение, обратное к вложению, тоже является вложением, и композиция двух вложений снова вложение. Иначе говоря, вложения образуют группу.
Группа автоморфизмов нормального расширения называется его *группой Галуа*.

§6. Норма в конечно порождённых расширениях

Пусть E расширение $\mathbb{Q}$ и $\nu = [E : \mathbb{Q}]$, $\sigma_1, \ldots, \sigma_\nu$ вложения E в $\mathbb{C}$. *Нормой* элемента α из E в $\mathbb{Q}$ называется число

$$N(\alpha) = \prod_{j=1}^{\nu} \sigma_j(\alpha).$$

Теорема 16 (Свойства нормы)

1. Если $\alpha \in E$, $\nu = [E : \mathbb{Q}]$ и $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Q}[x]$ — минимальный многочлен α, то $N(\alpha) = (-1)^\nu a_0^{\nu/d}$. В частности, если $\alpha \in \mathbb{Q}$, то $N(\alpha) = \alpha^\nu$.

2. Для любого числа $\alpha \in E$ его норма $N(\alpha)$ принадлежит $\mathbb{Q}$, а, если α — целое алгебраическое число, то $N(\alpha) \in \mathbb{Z}$.

3. Из равенства $N(\alpha) = 0$ следует $\alpha = 0$. Обратное также верно.

4. Для любых чисел α, β поля E справедливо равенство $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$.

Доказательства свойств нормы.

1. Пусть $\alpha_1, \ldots, \alpha_d$ все числа, сопряжённые с α. Применяя теорему 15 из предыдущей лекции и обозначая $k = \frac{\nu}{d}$, получаем, что

$$N(\alpha) = (\alpha_1 \cdots \alpha_d)^k = \left((-1)^d a_0\right)^k = (-1)^\nu a_0^k.$$

Здесь использовалась формула Виета $\alpha_1 \cdots \alpha_d = (-1)^d a_0$.
2. Утверждение следует из первого свойства нормы и того факта, что $a_0 \in \mathbb{Q}$. А в случае целого алгебраического α имеем $a_0 \in \mathbb{Z}$.
3. Если $N(\alpha) = 0$, то найдётся индекс j, для которого $\sigma_j(\alpha) = 0$. Учитывая, что σ_j вложение, заключаем $\alpha = 0$. Обратное утверждение очевидно.
4.

$$N(\alpha \cdot \beta) = \prod_{j=1}^{\nu} \sigma_j(\alpha \cdot \beta) = \prod_{j=1}^{\nu} \sigma_j(\alpha)\sigma_j(\beta) = N(\alpha)N(\beta).$$

Конец
десятой лекции.

Лекция 11.
Нормальные расширения. Норма в конечно порождённых расширениях. Теорема Лиувилля и существование трансцендентных чисел. Иррациональность e.

§5. Нормальные расширения (продолжение).

Расширение $E \supset \mathbb{Q}$ называется *нормальным*, если для любого вложения $\sigma : E \to \mathbb{C}$ выполняется равенство $\sigma(E) = E$.

Примеры.

1. $E = \mathbb{Q}(\sqrt{2})$. Здесь только два вложения:

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}, \qquad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}, \quad a, b \in \mathbb{Q}$$

Ясно, что для обоих вложений выполняется равенство $\sigma(E) = E$. Поле E нормальное.

2. $F = \mathbb{Q}(\sqrt[3]{2})$. Многочлен $x^3 - 2$ имеет три корня: $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$, $\xi^2\sqrt[3]{2}$, где $\xi = e^{\frac{2\pi i}{3}}$. Рассмотрим вложение σ поля F в поле $\mathbb{C}$

$$\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \to a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4}.$$

Так как F — действительное поле, но $\sigma(\sqrt[3]{2}) = \xi\sqrt[3]{2}$ — не действительное число, то $\sigma(F) \neq F$. Значит, $F \supset \mathbb{Q}$ не нормальное расширение.

Теорема 17 (Достаточное условие нормальности)

Пусть $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, *где* $\xi_1, \ldots, \xi_m$ *суть алгебраиеские числа, и все сопряженные каждого из* ξ_i *принадлежат* E. *Тогда* E *нормально.*

Пусть α произвольный элемент из поля E. Тогда справедливо представление:

$$\alpha = \frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \quad A, B \in \mathbb{Q}[x_1, \ldots, x_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0.$$

Подействуем вложением σ на это равенство. Учитывая, что $B(\sigma(\xi_1), \ldots, \sigma(\xi_m)) = \sigma(B(\xi_1, \ldots, \xi_m)) \neq 0$, получаем

$$\sigma(\alpha) = \frac{A(\sigma(\xi_1), \ldots, \sigma(\xi_m))}{B(\sigma(\xi_1), \ldots, \sigma(\xi_m))}.$$

Так как $\sigma(\xi_i)$ сопряжено с ξ_i, то, согласно условию, при любом i находим $\sigma(\xi_i) \in E$. Значит, $\sigma(\alpha) \in E$ и $\sigma(E) \subset E$.

Достаточное условие нормальности

Докажем теперь обратное включение. Пусть $E = \mathbb{Q}(\theta)$, $\theta_1, \ldots, \theta_\nu$ — числа, сопряженные с θ. Образ θ при отображении σ — одно из сопряжённых с θ чисел, пусть это будет θ_k. Числа $1, \theta_k, \ldots, \theta_k^{\nu-1} \in E$ образуют базис E (степень θ_k равна ν), и потому всякое $\beta \in E$ можно представить в виде

$$\beta = r_0 + r_1\theta_k + \ldots + r_{\nu-1}\theta_k^{\nu-1}.$$

Найдём прообраз этого элемента: именно, положим

$$\alpha = r_0 + r_1\theta + \ldots + r_{\nu-1}\theta^{\nu-1} \in E.$$

Ясно что $\sigma(\alpha) = \beta$. А это и означает, что $E \subset \sigma(E)$.

Если E нормальное расширение, то отображение, обратное к вложению, тоже является вложением, и композиция двух вложений снова вложение. Иначе говоря, вложения образуют группу.
Группа автоморфизмов нормального расширения называется его *группой Галуа*.

§6. Норма в конечно порождённых расширениях

Пусть E расширение $\mathbb{Q}$ и $\nu = [E : \mathbb{Q}]$, $\sigma_1, \ldots, \sigma_\nu$ вложения E в $\mathbb{C}$. *Нормой* элемента α из E в $\mathbb{Q}$ называется число

$$N(\alpha) = \prod_{j=1}^{\nu} \sigma_j(\alpha).$$

Теорема 18 (Свойства нормы)

1. Если $\alpha \in E$, $\nu = [E : \mathbb{Q}]$ и $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Q}[x]$ — минимальный многочлен α, то $N(\alpha) = (-1)^\nu a_0^{\nu/d}$. В частности, если $\alpha \in \mathbb{Q}$, то $N(\alpha) = \alpha^\nu$.

2. Для любого числа $\alpha \in E$ его норма $N(\alpha)$ принадлежит $\mathbb{Q}$, а, если α — целое алгебраическое число, то $N(\alpha) \in \mathbb{Z}$.

3. Из равенства $N(\alpha) = 0$ следует $\alpha = 0$. Обратное также верно.

4. Для любых чисел α, β поля E справедливо равенство $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$.

Доказательства свойств нормы.

1. Пусть $\alpha_1, \ldots, \alpha_d$ все числа, сопряжённые с α. Применяя теорему 15 из предыдущей лекции и обозначая $k = \frac{\nu}{d}$, получаем, что

$$N(\alpha) = (\alpha_1 \cdots \alpha_d)^k = \left((-1)^d a_0\right)^k = (-1)^\nu a_0^k.$$

Здесь использовалась формула Виета $\alpha_1 \cdots \alpha_d = (-1)^d a_0$.
2. Утверждение следует из первого свойства нормы и того факта, что $a_0 \in \mathbb{Q}$. А в случае целого алгебраического α имеем $a_0 \in \mathbb{Z}$.
3. Если $N(\alpha) = 0$, то найдётся индекс j, для которого $\sigma_j(\alpha) = 0$. Учитывая, что σ_j вложение, заключаем $\alpha = 0$. Обратное утверждение очевидно.
4.

$$N(\alpha \cdot \beta) = \prod_{j=1}^{\nu} \sigma_j(\alpha \cdot \beta) = \prod_{j=1}^{\nu} \sigma_j(\alpha)\sigma_j(\beta) = N(\alpha)N(\beta).$$

§7. Приближение алгебраических чисел рациональными.

Любое комплексное число, отличное от корней многочленов с рациональными коэффициентами, называется **трансцендентным** (Лейбниц).

§7. Приближение алгебраических чисел рациональными.

Любое комплексное число, отличное от корней многочленов с рациональными коэффициентами, называется **трансцендентным** (Лейбниц).
В 1844г. Ж. Лиувилль доказал, что алгебраические числа не могут слишком хорошо приближаться рациональными. Это свойство позволило ему построить первые примеры трансцендентных чисел.

§7. Приближение алгебраических чисел рациональными.

Любое комплексное число, отличное от корней многочленов с рациональными коэффициентами, называется **трансцендентным** (Лейбниц).
В 1844г. Ж. Лиувилль доказал, что алгебраические числа не могут слишком хорошо приближаться рациональными. Это свойство позволило ему построить первые примеры трансцендентных чисел. Если α – комплексное число, то для любого рационального числа $\frac{p}{q}$ выполняется неравенство $\left|\alpha - \frac{p}{q}\right| \geq |\Im\alpha|$ и ясно, что к числу α из $\mathbb{C} \setminus \mathbb{R}$ нельзя приблизиться рациональным на расстояние меньшее $|\Im\alpha|$.

§7. Приближение алгебраических чисел рациональными.

Любое комплексное число, отличное от корней многочленов с рациональными коэффициентами, называется **трансцендентным** (Лейбниц).
В 1844г. Ж. Лиувилль доказал, что алгебраические числа не могут слишком хорошо приближаться рациональными. Это свойство позволило ему построить первые примеры трансцендентных чисел. Если α – комплексное число, то для любого рационального числа $\frac{p}{q}$ выполняется неравенство $\left|\alpha - \frac{p}{q}\right| \geq |\Im\alpha|$ и ясно, что к числу α из $\mathbb{C} \setminus \mathbb{R}$ нельзя приблизиться рациональным на расстояние меньшее $|\Im\alpha|$. С другой стороны рациональные числа всюду плотны на действительной прямой и, могут приближать любое действительное число с любой точностью. Задача становится содержательной, если оценивать расстояние, например, в зависимости от знаменателя приближающего рационального числа.

Теорема Лиувилля и начало доказательства.

Теорема 19 (Лиувилль)

Пусть α – действительное алгебраическое число степени $\nu \geq 2$. Тогда найдётся константа $c > 0$, зависящая только от α, такая, что для любого рационального числа $\frac{p}{q}$, $q > 0$, выполняется неравенство

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^{\nu}}. \tag{1}$$

Пусть $f(x) \in \mathbb{Q}[x]$ – минимальный многочлен числа α и d – общий знаменатель коэффициентов $f(x)$. Пусть также $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_\nu$ – числа, сопряженные с α. Многочлен $f(x)$ неприводим. Поскольку степень его ν не меньше 2, то $f(x)$ не имеет рациональных корней и, значит, $dq^{\nu} f(p/q)$ целое отличное от нуля число. Но тогда $dq^{\nu}|f(p/q)| \geq 1$. Рассмотрим теперь два случая:

1) Пусть $\left|\alpha - \frac{p}{q}\right| \leq 1$. Тогда

$$\left|\alpha_j - \frac{p}{q}\right| \leq |\alpha_j - \alpha| + \left|\alpha - \frac{p}{q}\right| \leq |\alpha - \alpha_j| + 1, \quad j = 2, \ldots, \nu.$$

Из этих неравенств следует

$$1 \leq dq^n \left|f(p/q)\right| = dq^\nu \left|\alpha - \frac{p}{q}\right| \cdot \prod_{j=2}^{\nu} \left|\alpha_j - \frac{p}{q}\right| \leq$$

$$\leq dq^\nu \left|\alpha - \frac{p}{q}\right| \cdot \prod_{j=2}^{\nu} \left(|\alpha - \alpha_j| + 1\right).$$

Обозначив $c = d^{-1} \prod_{j=2}^{\nu} \left(|\alpha - \alpha_j| + 1\right)^{-1}$, получаем отсюда нужное неравенство.

Достаточное условие трансцендентности.

2) В случае $\left|\alpha - \frac{p}{q}\right| > 1$ можно взять ту же константу c, что и в первом случае. Она, очевидно, удовлетворяет неравенству $c < 1$, поэтому

$$\left|\alpha - \frac{p}{q}\right| > 1 \geq \frac{1}{q^\nu} > \frac{c}{q^\nu}.$$

Теорема Лиувилля доказана.

Следствие 1

Если $\alpha \in \mathbb{R}$ и для любого $m \geq 2$ неравенство $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$ имеет бесконечно много решений $\frac{p}{q} \in \mathbb{Q}$, то α трансцендентно.

1) Докажем сначала, что $\alpha \notin \mathbb{Q}$. Предположим, что это не так, и $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b > 0$. Возьмём $m = 2$. По условию существует бесконечно много рациональных чисел p/q, удовлетворяющих неравенствам $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. Среди них есть, конечно, решения со сколь угодно большими знаменателями q. С другой стороны,

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \left|\frac{aq - bp}{bq}\right| \geq \frac{1}{bq}.$$

Сопоставляя полученные неравенства, заключаем, что $\frac{1}{q^2} > \frac{1}{bq}$ и, значит, $q < b$. Получившееся противоречие доказывает иррациональность α.

2) Докажем, что α не есть алгебраическое число степени большей, чем 1. Предположим противное, и пусть $\deg \alpha = \nu \geq 2$. Положим $m = \nu + 1$. По условию следствия существует бесконечно много рациональных чисел $\frac{p}{q}$, удовлетворяющих неравенствам $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m} = \frac{1}{q^{\nu+1}}$. А с другой стороны по теореме 19 с некоторой константой $c > 0$, не зависящей от p и q, должно выполняться неравенство $\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^\nu}$. Сопоставляя эти неравенства, получаем: $\frac{c}{q^\nu} < \frac{1}{q^{\nu+1}}$. Но тогда $q < \frac{1}{c}$ вопреки бесконечности множества рациональных решений неравенства из условия следствия.

Существование трансцендентных чисел.

Укажем теперь конкретное трансцендентное число.

Следствие 2

Число α, определенное рядом

$$\alpha = \sum_{k=0}^{\infty} 2^{-k!},$$

трансцендентно.

Члены этого ряда "быстро"стремятся к нулю, а общий знаменатель его первых n членов растет "не очень быстро". Эти свойства позволяют построить последовательность хороших рациональных приближений к числу α, что обеспечивает с помощью следствия 1 трансцендентность α.

Для каждого натурального n определим целые числа

$$q_n = 2^{n!}, \qquad p_n = \sum_{k=0}^{n} 2^{n!-k!}.$$

Рациональное число

$$\frac{p_n}{q_n} = \sum_{k=0}^{n} 2^{-k!}$$

равно частичной сумме ряда, определяющего α. Поскольку члены ряда положительны, то

$$\alpha - \frac{p_n}{q_n} = \sum_{k=n+1}^{\infty} 2^{-k!} > 0.$$

Учитывая, что $(k+1)! > k!$, получаем $2^{-(k+1)!}/2^{-k!} < \frac{1}{2}$ и

$$\alpha - \frac{p_n}{q_n} = \sum_{k=n+1}^{\infty} 2^{-k!} < 2^{-(n+1)!}\left(1 + \frac{1}{2} + \frac{1}{4} + \ldots\right) =$$

$$= \frac{2}{2^{(n+1)!}} < \frac{1}{2^{n!n}} = \frac{1}{q_n^n}.$$

Из этих неравенств следует, что для любого $m \geq 2$ неравенствам

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$$

удовлетворяет бесконечное количество различных рациональных чисел $\frac{p_n}{q_n}$, $n > m$. В согласии со следствием 1 можно утверждать теперь, что α – трансцендентное число.

Ясно, что таким способом, выбирая вместо 2 другие натуральные основания, можно построить множество примеров трансцендентных чисел. Например, выбрав ряд с членами $10^{-k!}$, получим число, записываемое в десятичной системе нулями и единицами. Причем расстояния между соседними единицами будут возрастать очень быстро. Это число также трансцендентно.

Ясно, что таким способом, выбирая вместо 2 другие натуральные основания, можно построить множество примеров трансцендентных чисел. Например, выбрав ряд с членами $10^{-k!}$, получим число, записываемое в десятичной системе нулями и единицами. Причем расстояния между соседними единицами будут возрастать очень быстро. Это число также трансцендентно.

Иное доказательство существования трансцендентных чисел было предложено в 1874г. Г. Кантором, установившим счетность множества алгебраических чисел и несчетность множества действительных чисел. Таким образом, множество действительных чисел не может исчерпываться алгебраическими числами. Более того, трансцендентные числа составляют множество большей мощности, чем алгебраические. Впрочем, это рассуждение не позволяет строить примеры трансцендентных чисел.

§8. Иррациональность и трансцендентность числа e.

В 1737г. Эйлер, воспользовавшись разложением числа e в бесконечную цепную дробь, доказал иррациональность e.

Теорема 20 (Доказательство Фурье)

Число e иррационально.

§8. Иррациональность и трансцендентность числа e.

В 1737г. Эйлер, воспользовавшись разложением числа e в бесконечную цепную дробь, доказал иррациональность e.

Теорема 20 (Доказательство Фурье)

Число e иррационально.

Представим число e в виде ряда и умножим его на $n!$. Получим

$$n!e = n!\sum_{k=0}^{\infty}\frac{1}{k!} = \sum_{k=0}^{n}\frac{n!}{k!} + \sum_{k=n+1}^{\infty}\frac{n!}{k!} = p_n + r_n. \quad \text{Поэтому}$$

$$0 < n!e - p_n = r_n < \frac{1}{n+1} + \frac{1}{(n+1)^2} + \ldots = \frac{1}{n} \leq 1.$$

Предположим, что $e = \frac{a}{b}$ с целыми $a, b, b > 0$. Положим $n = b$. Так как $n!e - p_n \in \mathbb{Z}$ (факториал убьёт знаменатель e), то неравенства $0 < n!e - p_n < 1$ невозможны. Противоречие.

В 1873г. Эрмит предложил при любом $m \in \mathbb{Z}, m > 0$, аналитическую конструкцию целых чисел $b_0, b_1, \ldots, b_m$ таких, что все разности $b_0 e^k - b_k,\ 1 \leq k \leq m$, близки к нулю, и на этой основе доказал следующую теорему.

Теорема 21

Число e трансцендентно.

В 1873г. Эрмит предложил при любом $m \in \mathbb{Z}, m > 0$, аналитическую конструкцию целых чисел $b_0, b_1, \ldots, b_m$ таких, что все разности $b_0 e^k - b_k,\ 1 \leq k \leq m$, близки к нулю, и на этой основе доказал следующую теорему.

Теорема 21

Число e трансцендентно.

Сформулированное утверждение равносильно линейной независимости чисел $1, e, e^2, \ldots, e^m$ над $\mathbb{Q}$ для любого $m \geq 1$. За почти 150 лет, прошедших после опубликования работы Эрмита, было предложено множество различных вариантов рассуждений. Мы приведем здесь доказательство, опубликованное в 1890г. Т. Стилтьесом.

В основе конструкции Эрмита совместных рациональных приближений к степеням числа e лежит следующее тождество

$$\int_0^x e^{-t} f(t) dt = F(0) - F(x) e^{-x}, \qquad f(x) \in \mathbb{C}[x] \tag{2}$$

$$F(x) = \sum_{k=0}^{M} f^{(k)}(x), \quad M = \deg f(x), \tag{3}$$

В основе конструкции Эрмита совместных рациональных приближений к степеням числа e лежит следующее тождество

$$\int_0^x e^{-t} f(t) dt = F(0) - F(x)e^{-x}, \qquad f(x) \in \mathbb{C}[x] \tag{2}$$

$$F(x) = \sum_{k=0}^{M} f^{(k)}(x), \quad M = \deg f(x), \tag{3}$$

Для доказательства продифференцируем правую часть (2)

$$\left(F(0) - F(x)e^{-x}\right)' = e^{-x}(F(x) - F'(x)) = e^{-x} f(x)$$

Получившееся выражение совпадает с производной левой части. Осталось учесть, что обе части доказываемого тождества совпадают при $x = 0$.
Если $f(x) \in \mathbb{Z}$, то и $F(x) \in \mathbb{Z}$. Интегрировать в тождестве (2) можно, например, по отрезку в комплексной плоскости, соединяющему точки 0 и x.

Конец
одиннадцатой лекции.

Лекция 12.
Трансцендентность e. Иррациональность π.
Теорема Линдемана-Вейерштрасса.

В 1873г. Эрмит предложил при любом $m \in \mathbb{Z}, m > 0$, аналитическую конструкцию целых чисел $b_0, b_1, \ldots, b_m$ таких, что все разности $b_0 e^k - b_k,\ 1 \leq k \leq m$, близки к нулю, и на этой основе доказал следующую теорему.

Теорема 17

Число e трансцендентно.

В 1873г. Эрмит предложил при любом $m \in \mathbb{Z}, m > 0$, аналитическую конструкцию целых чисел $b_0, b_1, \ldots, b_m$ таких, что все разности $b_0 e^k - b_k,\ 1 \leq k \leq m$, близки к нулю, и на этой основе доказал следующую теорему.

Теорема 17

Число e трансцендентно.

Сформулированное утверждение равносильно линейной независимости чисел $1, e, e^2, \ldots, e^m$ над $\mathbb{Q}$ для любого $m \geq 1$. За почти 150 лет, прошедших после опубликования работы Эрмита, было предложено множество различных вариантов рассуждений. Мы приведем здесь доказательство, опубликованное в 1890г. Т. Стилтьесом.

В основе конструкции Эрмита совместных рациональных приближений к степеням числа e лежит следующее тождество

$$\int_0^x e^{-t} f(t) dt = F(0) - F(x) e^{-x}, \qquad f(x) \in \mathbb{C}[x] \qquad (1)$$

$$F(x) = \sum_{k=0}^{M} f^{(k)}(x), \quad M = \deg f(x), \qquad (2)$$

В основе конструкции Эрмита совместных рациональных приближений к степеням числа e лежит следующее тождество

$$\int_0^x e^{-t} f(t)dt = F(0) - F(x)e^{-x}, \qquad f(x) \in \mathbb{C}[x] \qquad (1)$$

$$F(x) = \sum_{k=0}^{M} f^{(k)}(x), \quad M = \deg f(x), \qquad (2)$$

Для доказательства продифференцируем правую часть (1)

$$\left(F(0) - F(x)e^{-x}\right)' = e^{-x}(F(x) - F'(x)) = e^{-x} f(x)$$

Получившееся выражение совпадает с производной левой части. Осталось учесть, что обе части доказываемого тождества совпадают при $x = 0$.
Если $f(x) \in \mathbb{Z}$, то и $F(x) \in \mathbb{Z}$. Интегрировать в тождестве (1) можно, например, по отрезку в комплексной плоскости, соединяющему точки 0 и x.

Пусть n - натуральное число, впоследствии достаточно большое, а многочлен $f(x) \in \mathbb{Z}[x]$ при некотором натуральном m обладает свойством

$$f^{(i)}(0) = f^{(i)}(1) = \ldots = f^{(i)}(m) = 0, \quad 0 \leq i < n, \tag{3}$$

Тогда при любом $k = 0, 1, 2, \ldots, m$ имеем

$$F(k) = \sum_{i=0}^{M} f^{(i)}(k) = \sum_{i=n}^{M} f^{(i)}(k) = n! b_k,$$

где b_k - целые числа. В последней сумме каждое слагаемое делится на $n!$. Это следует из тождества

$$\frac{1}{i!} (x^r)^{(i)} = \begin{cases} 0, & \text{если} \quad r < i; \\ \frac{r!}{i!(r-i)!} x^{r-i}, & \text{если} \quad r \geq i. \end{cases} \tag{4}$$

Из тождества (1) находим

$$b_0 e^k - b_k = \frac{e^k}{n!} \int_0^k e^{-t} f(t) dt, \qquad 0 \le k \le m. \tag{5}$$

Из тождества (1) находим

$$b_0 e^k - b_k = \frac{e^k}{n!} \int_0^k e^{-t} f(t) dt, \qquad 0 \le k \le m. \tag{5}$$

Предположим, теперь, что число e алгебраическое. Тогда при некотором натуральном m и с некоторыми целыми коэффициентами $a_0, \ldots, a_m$ выполняется равенство

$$a_m e^m + \ldots + a_1 e + a_0 = 0, \quad a_0 a_m \neq 0. \tag{6}$$

Умножим теперь (5) на a_k и просуммируем по всем $k = 0, \ldots, m$, получим:

$$b_0 \underbrace{\sum_{k=0}^{m} a_k e^k}_{=0} - \sum_{k=0}^{m} a_k b_k = \sum_{k=0}^{m} a_k \frac{e^k}{n!} \int_0^k f(x) e^{-x} dx, \quad \text{и}$$

$$a_0 b_0 + \ldots + a_m b_m = -\sum_{k=0}^{m} a_k \frac{e^k}{n!} \int_0^k e^{-t} f(t) dt.$$

Положим, следуя Стилтьесу,

$$f(x) = x^n(x-1)^{n+r_1}\cdots(x-m)^{n+r_m},$$

где параметры $r_1, \ldots, r_m$ в дальнейшем будут выбраны равными 0 или 1. Ясно, что такой многочлен удовлетворяет условиям (3) и

$$\max_{0\le t\le m} |f(t)| < c^{n+1}, \tag{7}$$

где $c = c(m)$ - положительная константа, зависящая только от m,

$$a_0 b_0 + \ldots + a_m b_m = -\sum_{k=0}^{m} a_k \frac{e^k}{n!} \int_0^k e^{-t} f(t) dt.$$

Обозначив

$$u_k(x) = \begin{cases} 1, & \text{если } x \leq k, \\ 0, & \text{если } x > k, \end{cases}$$

последнее равенство можно переписать в виде

$$a_0 b_0 + \ldots + a_m b_m = -\frac{1}{n!} \int_0^m e^{-t} f(t) G(t) dt = I = O\left(\frac{c^{n+1}}{n!}\right), \tag{8}$$

где

$$G(t) = \sum_{k=0}^{m} a_k e^k u_k(t).$$

Отличная от тождественного нуля функция

$$G(t) = \sum_{k=0}^{m} a_k e^k u_k(t)$$

знакопостоянна на интервалах между целыми точками. Выберем теперь показатели $r_1, \ldots, r_m$ так, чтобы функции $G(t)$ и $f(t)$ при переходе через каждую целую точку $1, \ldots, m$ одновременно меняли бы знак или сохраняли его. Тогда под интегралом в правой части равенства (8) стоит знакопостоянная функция. Кроме того, она отлична от нуля на интервале $(m-1, m)$. Это обеспечивает условие $I \neq 0$.
Но правая часть (8), т.е. интеграл I, есть целое число по модулю меньшее 1 при достаточно большом n. Получившееся противоречие завершает доказательство теоремы 17.
Трансцендентность e доказана.

§9. Иррациональность π.

Теорема 18 (Эрмит)

Число π иррационально.

§9. Иррациональность π.

Теорема 18 (Эрмит)

Число π иррационально.

Пусть $f(x) \in \mathbb{C}[x]$ и $F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \ldots$. Тогда

$$\left(F'(x)\sin x - F(x)\cos x\right)' = \left(F(x) + F^{(2)}(x)\right)\sin x = f(x)\sin x$$

и

$$J = \int_0^{\pi} f(x)\sin x dx = F(\pi) + F(0).$$

§9. Иррациональность π.

Теорема 18 (Эрмит)

Число π иррационально.

Пусть $f(x) \in \mathbb{C}[x]$ и $F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \ldots$. Тогда

$$\left(F'(x)\sin x - F(x)\cos x\right)' = \left(F(x) + F^{(2)}(x)\right)\sin x = f(x)\sin x$$

и

$$J = \int_0^{\pi} f(x)\sin x dx = F(\pi) + F(0).$$

Предположим, что $\pi = \frac{a}{b}$ и обозначим

$$f(x) = \frac{b^n x^n (\pi - x)^n}{n!} = \frac{x^n (a - bx)^n}{n!}.$$

Так как $f(x) > 0$ и $\sin x > 0$ на интервале $(0, \pi)$, то $J > 0$. Кроме того,

$$J < \pi \frac{b^n \pi^{2n}}{n!} = \frac{b^n \pi^{2n+1}}{n!} \to 0, \quad \text{при} \quad n \to \infty.$$

Поэтому можно выбрать n таким большим, чтобы $J \in (0, 1)$. Далее, $f(\pi - x) = f(x)$, поэтому $f^{(2k)}(\pi - x) = f^{(2k)}(x)$, в частности, $f^{(2k)}(\pi) = f^{(2k)}(0)$. Значит, $F(\pi) = F(0)$.

Так как $f(x) > 0$ и $\sin x > 0$ на интервале $(0, \pi)$, то $J > 0$. Кроме того,

$$J < \pi \frac{b^n \pi^{2n}}{n!} = \frac{b^n \pi^{2n+1}}{n!} \to 0, \quad \text{при} \quad n \to \infty.$$

Поэтому можно выбрать n таким большим, чтобы $J \in (0, 1)$. Далее, $f(\pi - x) = f(x)$, поэтому $f^{(2k)}(\pi - x) = f^{(2k)}(x)$, в частности, $f^{(2k)}(\pi) = f^{(2k)}(0)$. Значит, $F(\pi) = F(0)$.Осталось показать, что $F(0) \in \mathbb{Z}$. В самом деле,

$$F(0) = \sum_{k \geq 0} (-1)^k f^{(2k)}(0) = \sum_{2k \geq n} (-1)^k f^{(2k)}(0).$$

Аналогично предыдущей теореме показывается, что это выражение целое. Снова получаем противоречие, связанное с тем, что в интервале $(0, 1)$ нет целых чисел.

§10. Теорема Линдемана - Вейерштрасса.

В 1882г. Ф.Линдеман, внес в рассуждения Эрмита ряд новых идей и доказал трансцендентность числа π. Этим была решена знаменитая проблема квадратуры круга. Фактически Линдеман установил значительно более общее утверждение.

Теорема 19

Если a - отличное от нуля алгебраическое число, то число e^a трансцендентно.

Из теоремы 19 следует также трансцендентность натуральных логарифмов отличных от 0 и 1 алгебраических чисел и, в частности, трансцендентность $\pi = i^{-1}\ln(-1)$.
Линдеман сформулировал без доказательства еще более общую теорему, указав, что она может быть доказана с использованием тех же идей.

Теорема 20

Если $\alpha_0, \alpha_1, \ldots, \alpha_m, m \geq 1$ *различные алгебраические числа, то*

$$e^{\alpha_0}, e^{\alpha_1}, \ldots, e^{\alpha_m}$$

линейно независимы над полем всех алгебраических чисел $\mathbb{A}$.

Теорема 19 следует из этого утверждения при
$m = 1, \alpha_0 = 0, \alpha_1 = a$.
Доказательство теоремы 20 было опубликовано К.Вейерштрассом в 1885г.. В настоящее время ее принято называть теоремой Линдемана - Вейерштрасса.
Излагаемое ниже доказательство этой теоремы по существу следует Линдеману и обобщает надлежащим образом рассуждения Эрмита.

Лемма 1

Пусть $\alpha_0, \ldots, \alpha_m$ *- комплексные числа, многочлены* $f(t)$ *и* $g(t)$ *определены равенствами*

$$f(t) = (t-\alpha_0)^n (t-\alpha_1)^{n+1} \cdots (t-\alpha_m)^{n+1}, \quad g(t) = \frac{1}{n!} \sum_{k \geq n} f^{(k)}(t), \tag{9}$$

где n *- натуральное число. Если при этом функция*

$$A(t) = a_0 e^{\alpha_0 t} + \cdots + a_m e^{\alpha_m t}, \quad a_i \in \mathbb{C},$$

отлична от тождественного нуля и удовлетворяет условию $A(1) = 0$*, то справедливо неравенство*

$$|a_0 g(\alpha_0) + a_1 g(\alpha_1) + \ldots + a_m g(\alpha_m)| < \frac{c_1^{n+1}}{n!}, \tag{10}$$

где c_1 *- положительная величина, зависящая только от* $a_0, \ldots, a_m$, $\alpha_0, \ldots, \alpha_m$ *и не зависящая от* n.

Доказательство.

Из тождества Эрмита (см. тождество (2) предыдущей лекции) следуют равенства

$$\frac{1}{n!}F(0)e^{\alpha_k} - g(\alpha_k) = \frac{e^{\alpha_k}}{n!}\int_0^{\alpha_k} e^{-t}f(t)dt, \quad k = 0, \ldots, m, \quad (11)$$

где интегрирование ведется по отрезкам с концами в точках 0 и α_k. Умножив при каждом k равенство (11) на a_k, сложив все получившиеся выражения и воспользовавшись условием $A(1) = 0$, найдем

$$\sum_{k=0}^{m} a_k g(\alpha_k) = -\frac{1}{n!}\sum_{k=0}^{m} a_k e^{\alpha_k}\int_0^{\alpha_k} e^{-t}f(t)dt.$$

Применяя к правой части очевидную оценку $\max\limits_{|t|\le r}|f(t)| \le c^{n+1}$, где $r = \max\limits_{0\le i\le m}|\alpha_i|$, а $c = \max(1, (2r)^{m+1})$, получаем (10). □

Предложение 1

Пусть $a_0, \ldots, a_m$, $\alpha_0, \ldots, \alpha_m$ *- алгебраические числа, функция* $A(t)$ *определена равенством*

$$A(t) = a_0 e^{\alpha_0 t} + \cdots + a_m e^{\alpha_m t} \neq 0.$$

Если ряд Тейлора $A(t)$ *в окрестности точки* $t = 0$ *имеет рациональные коэффициенты, то* $A(1) \neq 0$.

$$A(t) = a_0 e^{\alpha_0 t} + \cdots + a_m e^{\alpha_m t} \neq 0.$$

Обозначим буквой E - нормальное расширение поля рациональных чисел, порожденное числами $a_0, \ldots, a_m,\ \alpha_0, \ldots, \alpha_m$ и всеми их сопряженными. Степень расширения $E \supset \mathbb{Q}$ обозначим буквой ν.

$$A(t) = a_0 e^{\alpha_0 t} + \cdots + a_m e^{\alpha_m t} \neq 0.$$

Обозначим буквой E - нормальное расширение поля рациональных чисел, порожденное числами $a_0, \ldots, a_m,\ \alpha_0, \ldots, \alpha_m$ и всеми их сопряженными. Степень расширения $E \supset \mathbb{Q}$ обозначим буквой ν.

Сделаем теперь несколько замечаний упрощающего характера.

1) Не уменьшая общности, *коэффициенты* $a_0, \ldots, a_m$ *можно считать целыми алгебраическими числами.* Иначе функцию $A(t)$ можно домножить на лежащий в $\mathbb{Z}$ общий знаменатель чисел a_j, и доказывать предложение 1 для получившейся таким способом новой функции.

$$A(t) = a_0 e^{\alpha_0 t} + \cdots + a_m e^{\alpha_m t} \neq 0.$$

Обозначим буквой E - нормальное расширение поля рациональных чисел, порожденное числами $a_0, \ldots, a_m,\ \alpha_0, \ldots, \alpha_m$ и всеми их сопряженными. Степень расширения $E \supset \mathbb{Q}$ обозначим буквой ν.

Сделаем теперь несколько замечаний упрощающего характера.

1) Не уменьшая общности, *коэффициенты $a_0, \ldots, a_m$ можно считать целыми алгебраическими числами.* Иначе функцию $A(t)$ можно домножить на лежащий в $\mathbb{Z}$ общий знаменатель чисел a_j, и доказывать предложение 1 для получившейся таким способом новой функции.

2) *Числа α_i можно предполагать отличными друг от друга*, ведь, объединив слагаемые с одинаковыми экспоненциальными функциями, мы не изменим $A(t)$.

$$A(t) = a_0 e^{\alpha_0 t} + \cdots + a_m e^{\alpha_m t} \neq 0.$$

Обозначим буквой E - нормальное расширение поля рациональных чисел, порожденное числами $a_0, \ldots, a_m,\ \alpha_0, \ldots, \alpha_m$ и всеми их сопряженными. Степень расширения $E \supset \mathbb{Q}$ обозначим буквой ν.

Сделаем теперь несколько замечаний упрощающего характера.

1) Не уменьшая общности, *коэффициенты $a_0, \ldots, a_m$ можно считать целыми алгебраическими числами.* Иначе функцию $A(t)$ можно домножить на лежащий в $\mathbb{Z}$ общий знаменатель чисел a_j, и доказывать предложение 1 для получившейся таким способом новой функции.

2) *Числа α_i можно предполагать отличными друг от друга*, ведь, объединив слагаемые с одинаковыми экспоненциальными функциями, мы не изменим $A(t)$.

3) По крайней мере один из коэффициентов a_j отличен от нуля. *Будем считать, что $a_0 \neq 0$.*

Пусть $d \in \mathbb{N}$ таково, что все числа $d\alpha_j$ целые алгебраические.

Лемма 2

Выражение

$$I = d^{m(n+1)} \left(a_0 g(\alpha_0) + \ldots + a_m g(\alpha_m)\right)$$

есть целое алгебраическое число.

Пусть $d \in \mathbb{N}$ таково, что все числа $d\alpha_j$ целые алгебраические.

Лемма 2

Выражение

$$I = d^{m(n+1)} \left(a_0 g(\alpha_0) + \ldots + a_m g(\alpha_m)\right)$$

есть целое алгебраическое число.

Имеем

$$d^{m(n+1)} f(x) = \frac{1}{d^n}(dx - d\alpha_0)^n \cdot (dx - d\alpha_1)^{n+1} \cdot \qquad (12)$$

$$\cdot \ldots \cdot (dx - d\alpha_m)^{n+1} = \frac{1}{d^n} h(dx),$$

где

$$h(t) = (t - d\alpha_0)^n (t - d\alpha_1)^{n+1} \cdots (t - d\alpha_m)^{n+1} \in \mathbb{Z}_E[t].$$

Применяя тождество (5) из предыдущей лекции к тождеству (12), получаем

$$d^{m(n+1)}\frac{1}{\ell!}f^{(\ell)}(\alpha_j) = d^{-n+\ell}\frac{1}{\ell!}h^{(\ell)}(d\alpha_j) \in \mathbb{Z}_E, \quad \ell \geq n.$$

Значит,

$$d^{m(n+1)}g(\alpha_j) = \sum_{\ell \geq n}\frac{\ell!}{n!}\frac{d^{m(n+1)}}{\ell!}f^{(\ell)}(\alpha_j) \in \mathbb{Z}_E,$$

откуда и следует утверждение леммы

$$I = d^{m(n+1)}\left(a_0 g(\alpha_0) + \ldots + a_m g(\alpha_m)\right) \in \mathbb{Z}_E.$$

Лемма 3

Существуют сколь угодно большие целые n такие, что

$$I \neq 0 \quad \textit{и} \quad |N(I)| \geq 1.$$

Лемма 3

Существуют сколь угодно большие целые n такие, что

$$I \neq 0 \quad \textit{и} \quad |N(I)| \geq 1.$$

Посчитаем $I \pmod{(n+1)}$. При любом j, $0 \leq j \leq m$, имеем

$$\frac{d^{m(n+1)}}{n!} \sum_{\ell \geq n+1} f^{(\ell)}(\alpha_j) = \sum_{\ell \geq n+1} \frac{\ell!}{n!} \frac{d^{m(n+1)}}{\ell!} f^{(\ell)}(\alpha_j) = (n+1)\gamma_j.$$

Здесь $\gamma_j \in \mathbb{Z}_E$.

Лемма 3

Существуют сколь угодно большие целые n такие, что

$$I \neq 0 \quad \textit{и} \quad |N(I)| \geq 1.$$

Посчитаем $I \pmod{(n+1)}$. При любом j, $0 \leq j \leq m$, имеем

$$\frac{d^{m(n+1)}}{n!} \sum_{\ell \geq n+1} f^{(\ell)}(\alpha_j) = \sum_{\ell \geq n+1} \frac{\ell!}{n!} \frac{d^{m(n+1)}}{\ell!} f^{(\ell)}(\alpha_j) = (n+1)\gamma_j.$$

Здесь $\gamma_j \in \mathbb{Z}_E$.Так что, левые части этих равенств делятся на $n+1$ в кольце $\mathbb{Z}_E$, и справедливы следующие равенства и сравнения по модулю $n+1$

$$I \equiv d^{m(n+1)} a_0 g(\alpha_0) \equiv d^{m(n+1)} a_0 \frac{1}{n!} f^{(n)}(\alpha_0) =$$

$$= d^{m(n+1)} a_0 (\alpha_0 - \alpha_1)^{n+1} \cdot \ldots \cdot (\alpha_0 - \alpha_m)^{n+1} = a_0 \prod_{j=1}^{m} (d\alpha_0 - d\alpha_j)^{n+1}.$$

Обозначим буквой S произведение норм отличных от нуля целых алгебраических чисел $d(\alpha_0 - \alpha_j), 1 \leq j \leq m$, и a_0, т.е.

$$S = N(a_0) \prod_{j=1}^{m} N\big(d(\alpha_0 - \alpha_j)\big).$$

Выберем теперь n делящимся на S, т.е. $n = Sq$, $q \in \mathbb{Z}, q > 0$. Тогда числа S и $n + 1 = Sq + 1$ взаимно просты.

Обозначим буквой S произведение норм отличных от нуля целых алгебраических чисел $d(\alpha_0 - \alpha_j), 1 \leq j \leq m$, и a_0, т.е.

$$S = N(a_0) \prod_{j=1}^{m} N\big(d(\alpha_0 - \alpha_j)\big).$$

Выберем теперь n делящимся на S, т.е. $n = Sq$, $q \in \mathbb{Z}, q > 0$. Тогда числа S и $n + 1 = Sq + 1$ взаимно просты.
Если $I = 0$, то в кольце $\mathbb{Z}_E$ имеет место делимость

$$(n+1) | a_0 \prod_{j=1}^{m} (d\alpha_0 - d\alpha_j)^{n+1}.$$

Но тогда норма правой части будет делиться на норму левой, т.е. на $(n+1)^\nu$ и, значит, $(n+1)^\nu | S^{n+1}$. Последняя делимость невозможна, т.к. числа $n+1$ и S взаимно просты. Это противоречие доказывает, что при указанном выборе n выполняется $I \neq 0$. Так как $N(I) \neq 0$ и $N(I) \in \mathbb{Z}$, то $|N(I)| \geq 1$.

Доказательство предложения 1

Пусть $\sigma_1, \ldots, \sigma_\nu$ все автоморфизмы поля E. Для каждого числа $\beta \in E$ будем обозначать $\beta^{(j)} = \sigma_j(\beta)$ - образ β при автоморфизме σ_j. Для каждого степенного ряда $f(t) = \beta_0 + \beta_1 t + \beta_2 t^2 + \ldots$ с коэффициентами из E и автоморфизма σ будем обозначать $\sigma(f)$ - ряд с коэффициентами $\sigma(\beta_j)$. Так, $\sigma(e^{\alpha t}) = \sum_{\ell \geq 0} \frac{\sigma(\alpha)^\ell}{\ell!} t^\ell = e^{\sigma(\alpha)t}$.

Доказательство предложения 1

Пусть $\sigma_1, \ldots, \sigma_\nu$ все автоморфизмы поля E. Для каждого числа $\beta \in E$ будем обозначать $\beta^{(j)} = \sigma_j(\beta)$ - образ β при автоморфизме σ_j. Для каждого степенного ряда $f(t) = \beta_0 + \beta_1 t + \beta_2 t^2 + \ldots$ с коэффициентами из E и автоморфизма σ будем обозначать $\sigma(f)$ - ряд с коэффициентами $\sigma(\beta_j)$. Так, $\sigma(e^{\alpha t}) = \sum_{\ell \geq 0} \frac{\sigma(\alpha)^\ell}{\ell!} t^\ell = e^{\sigma(\alpha)t}$. Ясно, что для любых рядов $f(t)$ и $g(t)$ с коэффициентами из E

$$\sigma(f(t) + g(t)) = \sigma(f(t)) + \sigma(g(t)), \tag{13}$$
$$\sigma(f(t)g(t)) = \sigma(f(t))\sigma(g(t)), \quad \sigma(f'(t)) = (\sigma(f(t)))'.$$

В частности, эти равенства означают, что для функций $A_j(t) = \sigma_j(A(t))$, $j = 1, ..., \nu$, справедливо представление

$$A_j(t) = \sum_{\ell=0}^{m} a_\ell^{(j)} e^{\alpha_\ell^{(j)} t}. \tag{14}$$

Доказательство предложения 1

Согласно условию предложения 1 коэффициенты разложения $A(t)$ в ряд Тейлора в точке $t = 0$ есть рациональные числа. Отсюда следует, что разложения всех функций $A_j(t)$ в окрестности точки $t = 0$ одинаковы и, значит,

$$A(t) = A_1(t) = \ldots = A_\nu(t).$$

Предположив теперь, что $A(1) = 0$, получим равенства $A_j(1) = 0$, $j = 1, 2, ..., \nu$.

Доказательство предложения 1

Согласно условию предложения 1 коэффициенты разложения $A(t)$ в ряд Тейлора в точке $t = 0$ есть рациональные числа. Отсюда следует, что разложения всех функций $A_j(t)$ в окрестности точки $t = 0$ одинаковы и, значит,

$$A(t) = A_1(t) = \ldots = A_\nu(t).$$

Предположив теперь, что $A(1) = 0$, получим равенства $A_j(1) = 0$, $j = 1, 2, ..., \nu$. Справедливы также равенства

$$I^{(j)} = a_0^{(j)} g_j(\alpha_0^{(j)}) + \ldots + a_m^{(j)} g_j(\alpha_m^{(j)}),$$

где $g_j(t) = \sigma_j(g(t))$. Принимая теперь во внимание (13), (14), (9), Лемму 1 и определение числа I, получаем неравенства

$$|I^{(j)}| \leq \frac{(d^m c_2)^{n+1}}{n!}, \quad 1 \leq j \leq \nu, \tag{15}$$

где c_2 - некоторая константа, не зависящая от n.

Доказательство предложения 1

Используя (15), можно оценить норму $N(I)$ числа I

$$|N(I)| = |I^{(1)} \dots I^{(\nu)}| \leq \frac{c_3^{n+1}}{(n!)^\nu}. \qquad (16)$$

Выберем теперь делящееся на S число n столь большим, что $(n!)^\nu > c_3^{n+1}$. Так как I - целое алгебраическое число, то его норма $N(I)$ принадлежит $\mathbb{Z}$ и оценка (16) означает, что должно выполняться равенство $N(I) = 0$. Но это противоречит свойству $I \neq 0$.
Это противоречие доказывает невозможность равенства $A(1) = 0$ и завершает доказательство предложения 1.

Доказательство теоремы Линдемана — Вейерштрасса.

Предположение о линейной зависимости чисел e^{α_i} над $\mathbb{A}$ означает существование равенства

$$a_0 e^{\alpha_0} + \cdots + a_m e^{\alpha_m} = 0$$

с алгебраическими коэффициентами a_j, не все из них равны 0. Согласно условию теоремы 20 все показатели α_j различны, поэтому функция $A(t)$, определенная в формулировке предложения 1 отлична от тождественного нуля, а выписанное выше равенство означает, что $A(1) = 0$.
Определим расширение $E \supset \mathbb{Q}$, его автоморфизмы $\sigma_1, \ldots, \sigma_\nu$, а также функции $A_j(t)$ как в доказательстве предложения 1.

Доказательство теоремы Линдемана — Вейерштрасса.

Рассмотрим теперь отличную от тождественного нуля функцию

$$B(t) = \prod_{j=1}^{\nu} A_j(t) = b_0 e^{\beta_0 t} + b_1 e^{\beta_1 t} + \ldots + b_M e^{\beta_M t}.$$

Доказательство теоремы Линдемана — Вейерштрасса.

Рассмотрим теперь отличную от тождественного нуля функцию

$$B(t) = \prod_{j=1}^{\nu} A_j(t) = b_0 e^{\beta_0 t} + b_1 e^{\beta_1 t} + \ldots + b_M e^{\beta_M t}.$$

Все числа b_j и β_j принадлежат полю E. Коэффициенты ряда Тейлора в окрестности точки $t = 0$ для функции $B(t)$ также принадлежат E, и для любого автоморфизма σ поля E имеем

$$\sigma(B(t)) = \prod_{j=1}^{\nu} \sigma(A_j(t)) = \prod_{j=1}^{\nu} \sigma\sigma_j(A(t)) = \prod_{j=1}^{\nu} \sigma_j(A(t)) = B(t).$$

Следовательно, все коэффициенты ряда Тейлора для $B(t)$ являются рациональными числами, т.е. функция $B(t)$ удовлетворяет условиям предложения 1. Но равенство $A(1) = 0$, в силу определения функции $B(t)$, влечет за собой $B(1) = 0$, вопреки утверждению предложения 1. Получившееся противоречие и завершает доказательство теоремы 20.

Конец
двенадцатой лекции.

Лекция 13.
Следствия из теоремы Линдемана-Вейерштрасса.
Невозможность квадратуры круга.

Теоремы Линдемана и Линдемана - Вейерштрасса.

На прошлой лекции были доказаны две теоремы

Теорема 22 (Теорема Линдемана)

Если a - отличное от нуля алгебраическое число, то число e^a трансцендентно.

Теорема 23 (Теорема Линдемана-Вейерштрасса)

Если $\alpha_0, \alpha_1, \ldots, \alpha_m, m \geq 1$ различные алгебраические числа, то

$$e^{\alpha_0}, e^{\alpha_1}, \ldots, e^{\alpha_m}$$

линейно независимы над полем всех алгебраических чисел $\mathbb{A}$.

Теорема 22 следует из теоремы 23 при $m = 1, \alpha_0 = 0, \alpha_1 = a$.

Выведем из теоремы 22 некоторые известные результаты.

Следствие 1 (Эрмит)

Число e трансцендентно.

Приведём два доказательства этого утверждения. Пусть $\alpha_0 = 0, \alpha_1 = 1, \cdots, \alpha_m = m$. Тогда по теореме 22 числа $1, e, \cdots, e^m$ линейно независимы над полем алгебраических чисел $\mathbb{A}$ и потому линейно независимы над полем $\mathbb{Q}$.
Второе доказательство: воспользуемся теоремой 22 при $a = 1$.

Следствие 2 (Линдеман)

Если β алгебраическое число, отличное от 0 и 1, то при любом выборе ветви логарифма число $\log\beta$ трансцендентно.

Действительно, $e^{\log\beta} = \beta \in \mathbb{A}$. Далее см. теорему 22.

Следствие 3 (Линдеман)

Число π трансцендентно.

Предположим, что $\pi \in \mathbb{A}$. Тогда $a = 2\pi i \in \mathbb{A}$. Согласно теореме 22 число $e^{2\pi i} = 1$ должно быть трансцендентным. Но $1 \in \mathbb{A}$.

Следствие 4

Для любого ненулевого $\alpha \in \mathbb{A}$ числа

$$\sin\alpha, \quad \cos\alpha, \quad \operatorname{tg}\alpha$$

трансцендентны.

Предположим, что $\sin\alpha = \beta$ и $\beta \in \mathbb{A}$. Тогда

$$\frac{1}{2i}e^{i\alpha} - \frac{1}{2i}e^{-i\alpha} - \beta e^0 = 0.$$

. Но это невозможно согласно теореме 23. Трансцендентность $\cos\alpha$ доказывается аналогино, так как $\cos\alpha = \frac{e^{i\alpha}+e^{-i\alpha}}{2}$. Если $\operatorname{tg}\alpha = \beta$ при $\beta \in \mathbb{A}$, то находим $(\beta + i)e^{i\alpha} - (\beta - i)\ e^{-i\alpha} = 0$, где по крайней мере один из коэффициентов $\beta + i$ или $\beta - i$ отличен от нуля. Теперь результат следует из теоремы 23.

Следствие 5

Пусть $\beta_1, \cdots, \beta_r$ алгебраические числа, линейно независимые над $\mathbb{Q}$. Тогда

$$e^{\beta_1}, \cdots, e^{\beta_r}$$

алгебраически независимы над $\mathbb{Q}$.

Допустим, что $e^{\beta_1}, \cdots, e^{\beta_r}$ алгебраически зависимы над $\mathbb{Q}$. Тогда существует такой ненулевой многочлен $P(x_1, \cdots, x_r) \in \mathbb{Q}[x_1, \cdots, x_r]$, что $P(e^{\beta_1}, \cdots, e^{\beta_r}) = 0$ т.е.,

$$\sum_{(k_1, \cdots, k_r)} a_{k_1, \cdots, k_r} \; e^{k_1\beta_1 + \cdots, + k_r\beta_r} = 0.$$

Здесь не все коэффициенты $a_{k_1, \cdots, k_r}$ равны нулю и все лежат в $\mathbb{Q}$. Отметим, что все числа $k_1\beta_1 + \cdots + k_r\beta_r$ различны, так как $\beta_1, \cdots, \beta_r$ линейно независимы над $\mathbb{Q}$. Получилось противоречие с теоремой 23.

§12. Невозможность квадратуры круга.

Знаменитая проблема квадратуры круга может быть сформулирована так
построить на плоскости квадрат, площадь которого равнялась бы площади заданного круга.
При этом "построить"означает построить с помощью циркуля и линейки - инструментов, находившихся в распоряжении древнегреческих геометров. Многочисленные попытки найти требуемое построение продолжались в течение четырех тысячелетий до тех пор, пока в 1882г. Ф.Линдеман не доказал, что такого построения не существует. Это утверждение будет доказано ниже.

Невозможность квадратуры круга.

Когда говорят о построении с помощью циркуля и линейки, имеют ввиду, что по заданному условиями набору точек, отрезков, окружностей или других геометрических объектов требуется построить некоторый новый отрезок, точку, окружность и т.п., используя только эти инструменты. Причем с их помощью разрешается выполнять лишь две основные операции

1) провести с помощью линейки прямую линию через две заданные или построенные ранее точки;
2) провести циркулем окружность с центром в заданной или построенной ранее точке радиуса, равного расстоянию между двумя заданными или построенными точками.

Любая геометрическая фигура, которая может быть построена, задается совокупностью прямых, окружностей и точек. Например, для построения квадрата достаточно построить четыре его вершины.

Невозможность квадратуры круга.

В результате выполнения в определенном порядке указанных операций на плоскости возникнет множество прямых, окружностей и некоторых точек их пересечения, содержащее искомые точки, прямые или окружности. Не все точки пересечения этих прямых и окружностей в действительности необходимы для построения. Перенумеруем теперь заданные условием точки, прямые и окружности в некотором порядке, а затем прямые, окружности и используемые для построения точки пересечения в порядке их возникновения. Тогда на чертеже появится конечная последовательность прямых, окружностей и точек, содержащая все искомые геометрические объекты. Каким же образом в процессе построения могут возникать новые прямые, окружности и точки?

Невозможность квадратуры круга.

Перечислим все имеющиеся возможности.

а) Новая прямая может быть построена лишь с помощью линейки, приложенной к двум, построенным ранее точкам.

б) Новая окружность может быть построена лишь с помощью циркуля, помещенного в построенную ранее точку. При этом радиус ее равен расстоянию между двумя построенными ранее точками.

в) Новая точка может быть построена, как пересечение двух построенных прямых.

г) Новая точка может быть построена, как пересечение построенных прямой и окружности.

д) Новая точка может быть построена, как пересечение двух построенных окружностей.

е) Новая точка может быть построена с помощью операции, которую мы назовем "произвольный выбор".

Поясним подробнее, что здесь имеется ввиду.

Невозможность квадратуры круга.

Иногда, при выполнении построения бывает безразлично, где взять необходимую точку. Тогда говорят, "возьмем произвольную точку"на плоскости, на построенной ранее прямой и т.п.. Рассмотрим, например, следующую древнюю и часто возникавшую на практике задачу: *построить с помощью циркуля и линейки центр нарисованной окружности.* Ясно, что построение центра не может начаться ни с одной из перечисленных выше операций а)-д). Одно из классических решений этой задачи начинается с произвольного выбора трех точек A, B и C на окружности с тем, чтобы впоследствии с помощью циркуля и линейки, так как это объясняется в школьном курсе геометрии, построить центр окружности, описанной вокруг треугольника ABC, т.е. центр заданной окружности.

Невозможность квадратуры круга.

Сделав эти вступительные замечания, предположим, что существует построение с помощью циркуля и линейки, решающее проблему квадратуры круга, т.е. позволяющее для любого заданного круга построить равновеликий ему квадрат. Введем на плоскости систему координат, поместив ее начало в центр заданного круга и выбрав в качестве единицы измерения длины радиус заданного круга. Всякая точка во введенной на плоскости системе координат может быть задана парой чисел $(x; y)$, прямая и окружность уравнениями в канонической форме, соответственно, $ax + by + c = 0$ и $(x - x_0)^2 + (y - y_0)^2 = r^2$, где (x_0, y_0) - координаты центра и r - радиус окружности.

Невозможность квадратуры круга.

Определим теперь на плоскости класс алгебраических точек, прямых и окружностей. Точку будем называть алгебраической, если ее координаты есть алгебраические числа, прямую - если она может быть задана уравнением с алгебраическими коэффициентами. Окружность будем называть алгебраической, если величина ее радиуса и координаты центра есть алгебраические числа. В частности, заданная на предыдущем слайде окружность имеет уравнение $x^2 + y^2 = 1$ и потому является алгебраической.

Невозможность квадратуры круга.

Покажем, что операции а)-д), примененные к алгебраическим объектам, в результате также дают алгебраические точки, прямые и окружности. В самом деле:
а) Прямая, проведенная через две точки с алгебраическими координатами (x_1, y_1) и (x_2, y_2), задается уравнением

$$(x_2 - x_1)(y - y_1) - (y_2 - y_1)(x - x_1) = 0.$$

Это уравнение в канонической форме имеет алгебраические коэффициенты и потому определяет алгебраическую прямую.
б) Окружность с алгебраическим центром, радиус которой есть алгебраическое число, по определению является алгебраической.

Невозможность квадратуры круга.

в) Две пересекающиеся прямые, задаваемые уравнениями $a_i x + b_i y + c_i = 0, i = 1, 2$, с алгебраическими коэффициентами a_i, b_i, c_i имеют общую точку с координатами, удовлетворяющими системе уравнений

$$\begin{cases} a_1 x + b_1 y = c_1, \\ a_2 x + b_2 y + c_2. \end{cases}$$

Решение этой системы, найденное, например, по формулам Крамера, имеет алгебраические координаты x, y. Так что точка пересечения двух алгебраических прямых является алгебраической.

Невозможность квадратуры круга.

г) Точки пересечения алгебраических прямой и окружности имеют координаты x, y, удовлетворяющие системе уравнений

$$\begin{cases} ax + by = c, \\ (x - x_0)^2 + (y - y_0)^2 = r^2, \end{cases}$$

с алгебраическими коэффициентами. Не уменьшая общности можно считать, что $b \neq 0$. Выразив из первого уравнения системы неизвестную y через x и подставив это выражение вместо y во второе уравнение, получим квадратное уравнение относительно x, коэффициенты которого будут алгебраическими числами. Но тогда алгебраическими числами будут оба корня x_1 и x_2 получившегося квадратного уравнения, а, следовательно, и вторые кординаты $y_i = -(ax_i + c) \cdot b^{-1}$ точек пересечения. Итак, обе точки пересечения (x_1, y_1) и (x_2, y_2) будут алгебраическими.

Невозможность квадратуры круга.

д) Координаты x, y точек пересечения двух алгебраических окружностей удовлетворяют системе уравнений

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = r_1^2, \\ (x - x_2)^2 + (y - y_2)^2 = r_2^2, \end{cases}$$

с алгебраическими коэффициентами. Вычитая второе уравнение системы из первого, мы, как легко проверить, получим линейное уравнение с алгебраическими коэффициентами. А затем, как и в предыдущем случае, проверяем, что координаты точек пересечения есть алгебраические числа. Этим доказано, что точки пересечения двух алгебраических окружностей будут алгебраическими.

Невозможность квадратуры круга.

Следующая операция e) - "произвольный выбор". Заметим, что точки с алгебраическими (и даже рациональными) координатами всюду плотны на плоскости. Это означает, что сколь угодно близко к любой точке плоскости находятся точки с алгебраическими координатами.

Невозможность квадратуры круга.

Следующая операция e) - "произвольный выбор". Заметим, что точки с алгебраическими (и даже рациональными) координатами всюду плотны на плоскости. Это означает, что сколь угодно близко к любой точке плоскости находятся точки с алгебраическими координатами.Кроме того, они будут всюду плотны на алгебраических прямых и окружностях. Действительно, в любой окрестности точки (x_1, y_1), лежащей, например, на алгебраической окружности, найдется точка (x_2, y_2) с абсциссой x_2 - рациональным числом, принадлежащая этой же окружности. Но тогда вторая координата y_2 должна быть алгебраическим числом, так что точка (x_2, y_2) будет алгебраической.

Невозможность квадратуры круга.

Следующая операция e) - "произвольный выбор". Заметим, что точки с алгебраическими (и даже рациональными) координатами всюду плотны на плоскости. Это означает, что сколь угодно близко к любой точке плоскости находятся точки с алгебраическими координатами.Кроме того, они будут всюду плотны на алгебраических прямых и окружностях. Действительно, в любой окрестности точки (x_1, y_1), лежащей, например, на алгебраической окружности, найдется точка (x_2, y_2) с абсциссой x_2 - рациональным числом, принадлежащая этой же окружности. Но тогда вторая координата y_2 должна быть алгебраическим числом, так что точка (x_2, y_2) будет алгебраической.Это означает, что если все точки, прямые и окружности, получившиеся в результате операций, предшествовавших "произвольному выбору были алгебраическими, то и при "произвольном выборе"мы можем построить алгебраическую точку.

Невозможность квадратуры круга.

Сказанное выше можно резюмировать так. Построение с помощью циркуля и линейки, реализующее квадратуру алгебраического круга $x^2 + y^2 = 1$, может быть выполнено таким образом, что все встречающиеся в нем точки, прямые и окружности будут алгебраическими. В частности, это означает, что алгебраическими будут и все вершины квадрата, получающегося в конце построения, и равновеликого по площади заданному кругу.

Если $(x_1, y_1), (x_2, y_2)$ - соседние вершины квадрата, то его площадь, как легко видеть, равна $(x_2 - x_1)^2 + (y_2 - y_1)^2$ и является алгебраическим числом. Но эта же площадь по условию должна равняться площади заданного круга, т.е. числу π.

Таким образом, получается противоречие с теоремой Линдемана о трансцендентности числа π, означающее, что квадратура круга с помощью циркуля и линейки невозможна.

Невозможность квадратуры круга.

В 1837г. П.Вантцель еще до доказательства трансцендентности π показал, что при заданном отрезке единичной длины с помощью циркуля и линейки могут быть построены только отрезки, длины которых выражаются числами, являющимися корнями квадратных уравнений с рациональными коэффициентами, корнями квадратных уравнений, коэффициенты которых являются корнями квадратных уравнений с рациональными коэффициентами, и т.д., и, следовательно, отрезки, длины которых выражаются числами, получающимися после последовательного решения ряда квадратных уравнений. Этот факт, уточняющий приведенные выше рассуждения, служит причиной невозможности решения и двух других старинных задач на построение с помощью циркуля и линейки: задачи *трисекции угла* и задачи *удвоения куба*.

Конец курса.