Глава 1

Лекция 1. Алгебраические числа (всё без доказательства.)

Комплексное число α называется *алгебраическим*, если существует многочлен $p(x) \in \mathbb{Q}[x]$, $p(x) \neq 0$, с условием $p(\alpha) = 0$. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Такой многочлен определяется по числу α

единственным способом и называется *минимальным многочленом* числа α. Он будет обозначаться $p_\alpha(x)$. *Степенью* алгебраического числа α называется степень его минимального многочлена $p_\alpha(x)$, она обозначается $\deg\alpha$. Если

$$p_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Q}[x],$$

и $a_j = \frac{A_j}{A_n}, j = 1, \ldots, n-1$, где A_n - наименьший общий знаменатель коэффициентов $p_\alpha(x)$, то величина

$$H(\alpha) = \max(|A_0|, \ldots, |A_n|)$$

называется *высотой* алгебраического числа α. Все корни

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$$

минимального многочлена $p_\alpha(x)$ называются *сопряженными* с α числами. Символом $\overline{|\alpha|}$ будет обозначаться максимум модулей чисел, сопряженных с α.

Теорема 1. *Если α и β - алгебраические числа, то числа $\alpha+\beta, \alpha-\beta, \alpha\cdot\beta$, а в случае, если $\beta \neq 0$, то и $\frac{\alpha}{\beta}$ являются алгебраическими числами.*

Таким образом, все алгебраические числа образуют поле. Мы будем обозначать его $\mathbb{A}$. Для любых $\alpha, \beta \in \mathbb{A}$ справедливы неравенства

$$\overline{|\alpha+\beta|} \leq \overline{|\alpha|} + \overline{|\beta|}, \quad \overline{|\alpha\cdot\beta|} \leq \overline{|\alpha|}\cdot\overline{|\beta|}.$$

Теорема 2. *Поле всех алгебраических чисел алгебраически замкнуто.*

Алгебраическое число α называется *целым алгебраическим*, если его минимальный многочлен имеет целые коэффициенты, т.е. $p_\alpha(x) \in \mathbb{Z}[x]$.

Теорема 3. *Сумма, разность и произведение двух целых алгебраических чисел α и β также являются целыми алгебраическими числами.*

Теорема 4. *Если α - алгебраическое число, то существует число $d \in \mathbb{Z}, d > 0$, такое, что $r\alpha$ - целое алгебраическое число.*

Определение 1. *Пусть $\alpha_1, \ldots, \alpha_m$ - произвольные алгебраические числа. Множество всех чисел вида*

$$\frac{P(\alpha_1, \ldots, \alpha_m)}{Q(\alpha_1, \ldots, \alpha_m)},$$

где $P, Q \in \mathbb{Q}[x_1, \ldots, x_m]$, замкнуто относительно операций сложения, вычитания, умножения и деления на ненулевое число. Поэтому оно является полем. Это поле будет обозначаться $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ и называться конечным расширением $\mathbb{Q}$ алгебраическими числами $\alpha_1, \ldots, \alpha_m$ или просто конечным расширением.

Если $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, то множество целых алгебраических чисел K образует согласно теореме 3 кольцо, в дальнейшем обозначаемое $\mathbb{Z}_K$.

Теорема 5. *Пусть θ - алгебраическое число степени n. Тогда каждый элемент α поля $K = \mathbb{Q}(\theta)$ имеет единственное представление в виде*

$$\alpha = c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}. \tag{1}$$

Поле K есть линейное пространство над $\mathbb{Q}$ размерности n.

Теорема 6 (О примитивном элементе). *Пусть $\alpha_1, \ldots, \alpha_m \in \mathbb{A}$ и $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ Тогда существует $\theta \in \mathbb{A}$ такое, что $K = \mathbb{Q}(\theta)$ (примитивный элемент).*

Следствие 1. *Любое конечное расширение $K \supset \mathbb{Q}$ является конечномерным линейным пространством над $\mathbb{Q}$. Степень любого примитивного элемента поля K равна размерности этого пространства.*

Определение 2. *В условиях теоремы 6 размерность линейного пространства K над $\mathbb{Q}$ называется* степенью *расширения $K \supset \mathbb{Q}$. Обозначается $[K : Q]$.*

Определение 3. *Пусть $K \supset \mathbb{Q}$ - конечное расширение. Отображение $\sigma : K \to \mathbb{C}$ называется вложением, если σ является гомоморфизмом, т.е. сохраняет арифметические операции и есть взаимно однозначное отображение K на $\sigma(K)$ (изоморфизм).*

Теорема 7. *Существует в точности $n = [K : \mathbb{Q}]$ вложений K в поле $\mathbb{C}$. Если $K = \mathbb{Q}(\theta)$ и $\theta_1, \ldots, \theta_n$ - числа, сопряженные с θ, то все отображения $K \to \mathbb{C}$, задаваемые для числа (1) равенствами*

$$\sigma_j(\alpha) = c_0 + c_1\theta_j + \ldots + c_{n-1}\theta_j^{n-1}, \quad j = 1, \ldots, n,$$

являются вложениями K в $\mathbb{C}$.

Определение 4. *Конечное расширение $K \supset \mathbb{Q}$ называется* нормальным, *если для любого вложения $\sigma : K \to \mathbb{C}$ имеем $\sigma(K) = K$, т.е. отображение σ является автоморфизмом поля K.*

Теорема 8. *Пусть поле $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ содержит все числа, сопряженные с каждым из α_j. Тогда $K \supset \mathbb{Q}$ - нормальное расширение.*

Определение 5. *Пусть K - конечное расширение $\mathbb{Q}$, $n = [E : Q]$, $\sigma_1, \ldots, \sigma_n$ - все вложения K в $\mathbb{C}$. Для любого числа $\alpha \in K$ его норма $N(\alpha)$ и след $S(\alpha)$ определяется равенствами*

$$N(\alpha) = \prod_{j=1}^{n} \sigma_j(\alpha), \tag{2}$$

$$S(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha). \tag{3}$$

Теорема 9. *1) Для любого числа $\alpha \in K$, его норма $N(\alpha)$ и след $S(\alpha)$ есть рациональные числа. Если же $\alpha \in \mathbb{Z}_K$, то $N(\alpha) \in \mathbb{Z}, S(\alpha) \in \mathbb{Z}$.*
2) Для любых чисел $\alpha, \beta \in K$ и $\lambda \in \mathbb{Q}$ справедливы равенства

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta), \tag{4}$$

$$S(\alpha + \beta) = S(\alpha) + S(\beta), \tag{5}$$

$$S(\lambda \cdot \alpha) = \lambda \cdot S(\alpha). \tag{6}$$

Теорема 10. *Пусть $K \supset \mathbb{Q}$ -конечное расширение, $[K : \mathbb{Q}] = n$. Тогда существуют числа $\omega_1, \ldots, \omega_n \in \mathbb{Z}_K$ такие, что*

$$\mathbb{Z}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

Целое число

$$\Delta = \det \|S(\omega_i \cdot \omega_j)\|_{1 \le i,j \le n}$$

отлично от нуля. Оно называется дискриминантом поля K.

Литература

[1] Боревич З.И., Шафаревич И.Р., Теория чисел, М., Наука, 1972.

[2] Ван дер Варден Б.Л., Современная алгебра, М., Наука, 1976.

[3] Гекке Э., Лекции по теории алгебраических чисел, М., ГИТТЛ, 1940.

Глава 2

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

Из теоремы 1 следует также трансцендентность натуральных логарифмов отличных от 0 и 1 алгебраических чисел и, в частности, трансцендентность $\pi = i^{-1}\ln(-1)$. Если $b = \ln a \neq 0$ есть алгебраическое число, то $e^b = a$ должно быть трансцендентным.

Линдеман сформулировал без доказательства еще более общую теорему, указав, что она может быть доказана с использованием тех же идей.

Теорема 2. *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 1 следует из этого утверждения при $m = 1, \alpha_0 = 0, \alpha_1 = a$.

Доказательство теоремы 2 было опубликовано К.Вейерштрассом в 1885г.. В настоящее время ее принято называть теоремой Линдемана - Вейерштрасса.

В настоящее время известны и иные методы доказательства теоремы Линдемана - Вейерштрасса. При этом фактически доказываются утверждения, эквивалентные теореме 2.

Теорема 3. *Для любых алгебраических чисел $\beta_1, \ldots, \beta_r$ линейно независимых над $\mathbb{Q}$, числа*

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

алгебраически независимы над $\mathbb{Q}$.

Эта теорема была первым утверждением об алгебраической независимости каких - либо чисел.

Следующий ослабленный вариант теоремы 2 также эквивалентен ей.

Теорема 4. *Для любого конечного расширения $\mathbf{K}$ поля рациональных чисел существует положительная постоянная c, зависящая только от $\mathbf{K}$ такая, что для каждого набора различных чисел $\gamma_1, \ldots, \gamma_N \in \mathbf{K}$ среди значений экспоненциальной функции*

$$e^{\gamma_1}, \ \ldots, \ e^{\gamma_N}$$

имеется не менее cN чисел, линейно независимых над $\mathbb{Q}$.

Докажем эквивалентность теорем 2 - 4.

Теорема 2 $\Longrightarrow$ **Теорема 4** $\Longrightarrow$ **Теорема 3** $\Longrightarrow$ **Теорема 2**

Теорема 2 $\Longrightarrow$ **Теорема 4.** Это утверждение, очевидно, выполняется с c=1.

Теорема 4 $\Longrightarrow$ **Теорема 3.** Пусть $\mathbf{K} = \mathbb{Q}(\beta_1, \ldots, \beta_r)$, n - достаточно большое натуральное число, $N = (n+1)^r$, а числа $\gamma_1, \ldots, \gamma_N$ есть упорядоченный каким-либо способом набор чисел

$$k_1\beta_1 + \cdots + k_r\beta_r, \qquad 0 \le k_i \le n.$$

Согласно теореме 4 в этой ситуации среди чисел e^{γ_i} имеется не менее $c(n+1)^r$ чисел, линейно независимых над $\mathbb{Q}$. С другой стороны, если числа

$e^{\beta_1}, \ldots, e^{\beta_r}$ алгебраически зависимы над $\mathbb{Q}$, то существует многочлен $P \in \mathbb{Z}[x_1, \ldots, x_r]$ такой, что $P(e^{\beta_1}, \ldots, e^{\beta_r}) = 0$. Обозначим $q = \deg P$. Тогда равенства

$$e^{k_1\beta_1+\ldots+k_r\beta_r} P(e^{\beta_1}, \ldots, e^{\beta_r}), \quad 0 \le k_i \le n - q$$

дают $(n-q)^r$ линейных соотношений над $\mathbb{Q}$ между числами e^{γ_i}. Легко видеть, что эти соотношения линейно независимы, так что среди чисел $e^{\gamma_i},\ 1 \le i \le (n+1)^r$, имеется не более чем $(n+1)^r - (n-q)^r = O(n^{r-1})$ линейно независимых над $\mathbb{Q}$, что, конечно, противоречит при достаточно большом n нижней оценке, полученной выше с помощью теоремы 4.

Теорема 3 $\Longrightarrow$ Теорема 2. Пусть $\alpha_1, \ldots, \alpha_r$ - максимальный набор линейно независимых над $\mathbb{Q}$ чисел среди $\alpha_0, \ldots, \alpha_m$. Легко видеть, что все числа $\alpha_i, 0 \le i \le m$, являются целочисленными линейными комбинациями чисел $\beta_1 = \dfrac{\alpha_1}{v}, \ldots, \beta_r = \dfrac{\alpha_r}{v}$ с некоторым натуральным числом v. Предположение о линейной зависимости над $\mathbb{A}$ чисел $e^{\alpha_0}, \ldots, e^{\alpha_m}$ влечет существование нетривиальной функции $R \in \mathbb{A}(x_1, \ldots, x_r)$, обращающейся в нуль при подстановке чисел e^{β_i} вместо $x_i,\ i = 1, ..., r$, и, следовательно, алгебраическую зависимость над $\mathbb{A}$ чисел e^{β_i}. Но тогда числа e^{β_i} алгебраически зависимы и над $\mathbb{Q}$, вопреки теореме 3.