Алгебра 7
23.10.97

Дискриминант. Целые числа

Часть 1. Теорема Паскаля.

Теорема. Точки пересечения противоположных сторон шестиугольника, вписанного в окружность S, лежат на одной прямой.

Доказательство: Пусть $l_1, l_2, \dots, l_6$ — линейные уравнения сторон шестиугольника, занумерованных по часовой стрелке. Таким образом, $l_i \in \mathbb{R}[x, y]$. Сами стороны (точнее, прямые, их содержащие) мы будем обозначать теми же символами. Рассмотрим кривую третьей степени C_λ, заданную уравнением $l_1 l_3 l_5 - \lambda l_2 l_4 l_6 = 0$. Пересечение $C_\lambda \cap S$ заведомо содержит 6 вершин нашего шестиугольника. Возьмем какую-нибудь точку $A \in S$, отличную от этих вершин, и положим $\lambda = \frac{l_1 l_3 l_5(A)}{l_2 l_4 l_6(A)}$. Тогда $A \in C_\lambda$, т.е. пересечение квадрики S и кубики C_λ содержит 7 точек. По теореме Безу из предыдущей лекции получаем $S \subset C_\lambda$. Значит, $C_\lambda = S \cup L$, причем по соображениям степени кривая L обязана быть прямой. Однако точки пересечения противоположных сторон $P_1 = l_1 \cap l_4$, $P_2 = l_2 \cap l_5$, $P_3 = l_3 \cap l_6$ лежат на C_λ, но не лежат на S. Значит, они лежат на прямой L. $\square$

Часть 2. Дискриминант расширения полей.

Напомним утверждения задач 7,8 к 7 октября (это простые задачи, их обязательно надо решить).

Пусть L/K — конечное расширение полей, $a \in L$. След, определитель и характеристический многочлен K-линейного оператора $l \mapsto al$, $L \to L$, обозначаются соответственно через $Tr_{L/K}(a), N_{L/K}(a), \chi_{L/K}(a, t)$ и называются *следом, нормой* и *характеристическим многочленом* элемента a над K. Если $K \subset L \subset M$ — башня конечных расширений и $a \in M$, то

a) $Tr_{M/K}(a) = Tr_{L/K}(Tr_{M/L}(a))$;

b) $N_{M/K}(a) = N_{L/K}(N_{M/L}(a))$;

c) $\chi_{M/K}(a,t) = N_{L(t)/K(t)}(\chi_{M/L}(a,t))$;

d) Минимальный многочлен элемента a над K равен $\pm\chi_{K(a)/K}(a,t)$;

e) $\chi_{M/K}(a,t)$ является, с точностью до знака, степенью минимального многочлена a над K;

f) Если M/K — расширение Галуа с группой Галуа G, то $Tr_{M/K}(a) = \sum_{g\in G} g(a)$, $N_{M/K}(a) = \prod_{g\in G} g(a)$, $\chi_{M/K}(a,t) = \prod_{g\in G}(g(a)-t)$.

Далее, $Tr_{M/K}(a) = 0$ $\forall a \in M$ тогда и только тогда, когда расширение M/K несепарабельно. Если же расширение M/K сепарабельно, то K-билинейная форма на $M:$ $B_{M/K}(x,y) := Tr_{M/K}(xy)$ невырождена.

Например, пусть $K = \mathbb{Q} \subset \mathbb{Q}(i) = M$. Тогда для $z \in \mathbb{Q}(i)$ имеем $Tr(z) = z + \overline{z}$, $N(z) = z\overline{z}$, $\chi(z,t) = (z-t)(\overline{z}-t)$, а матрица билинейной формы B в базисе $\{1, i\}$ имеет вид $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$.

Приложение. Задача 6 к 14 октября: докажем, что $a_1 = 1, a_2 = \sqrt{2}, a_3 = \sqrt{3}, a_4 = \sqrt{5}, a_5 = \sqrt{6}, a_6 = \sqrt{10}, a_7 = \sqrt{15}, a_8 = \sqrt{30}$ линейно независимы над $\mathbb{Q}$, т.е. что они образуют базис поля $M = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ над $K = \mathbb{Q}$. Для этого достаточно проверить, что 8×8-матрица билинейной формы $B_{M/K}(a_i, a_j)$ невырождена. Вычислим ее. Пусть $[M:K] = k$. Тогда для рационального числа q имеем $Tr_{M/K}(q) = kq$, поэтому на диагонали нашей матрицы стоят числа $k, 2k, 3k, 5k, 6k, 10k, 15k, 30k$. Докажем, что вне диагонали стоят нули.

Например, $a_3a_5 = \sqrt{3}\cdot\sqrt{6} = 3\sqrt{2}$. Надо проверить, что $Tr_{M/K}(3\sqrt{2}) = 0$. Положим $L = \mathbb{Q}(\sqrt{2})$ и рассмотрим башню полей $M \supset L \supset K$. По свойству a) следов в башне имеем $Tr_{M/K}(3\sqrt{2}) = Tr_{L/K}(Tr_{M/L}(3\sqrt{2})) = Tr_{L/K}(3m\sqrt{2}) = 3m\sqrt{2} - 3m\sqrt{2} = 0$, где $m = [M:L]$.

Итак, наша матрица диагональна, а значит, невырождена. Следовательно, элементы $a_1, \ldots, a_8$ линейно независимы. $\square$

Определение. Дискриминантом $D(\beta_1, \ldots, \beta_n)$ базиса расширения полей $L:K$ называется определитель матрицы $B = \|Tr_{L/K}(\beta_i\beta_j)\|$.

Пусть $\{\alpha_1, \ldots, \alpha_n\}$ — другой базис поля L над K, и $C = (c_ij)$ — матрица перехода, т.е. $\alpha_i = \sum_{j=1}^n c_{ij}\beta_j$. Пусть $A = \|Tr_{L/K}(\alpha_i, \alpha_j)\|$ — матрица формы следа в базисе $\{\alpha_1, \ldots, \alpha_n\}$. Тогда линейная алгебра учит нас, что $A = C^TBC$ и $D(\alpha_1, \ldots, \alpha_n) = \det^2 C \cdot D(\beta_1, \ldots, \beta_n)$.

Утверждение. Пусть $L : K$ — расширение Галуа с группой Галуа $G = \{ g_1, \dots, g_n \}$. Пусть $\{ \alpha_1, \dots, \alpha_n \}$ — базис L над K. Тогда $D(\alpha_1, \dots, \alpha_n) = \det^2 \|g_i(\alpha_j)\|$.

Доказательство: По свойству f) следов в расширении Галуа имеем $A = \|Tr(\alpha_i\alpha_j)\| = \| \sum_{k=1}^n g_k(\alpha_i\alpha_j)\| = X^T X$, где $X = \|g_i(\alpha_j)\|$. $\square$

Предложение. Пусть $L : K$ — расширение Галуа, $\beta \in L$ — примитивный элемент, $f \in K[t]$ — унитарный минимальный многочлен элемента β (в частности, $\deg f = n$). Тогда

$$D(1, \beta, \dots, \beta^{n-1}) = D(f) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\beta))$$

Кстати, $f'(\beta)$ называется дифферентой, т.е. дискриминант является нормой дифференты.

Доказательство: $D(1, \beta, \dots, \beta^{n-1}) = \det^2 \|g_i(\beta^j)\| = \det^2 \|(g_i(\beta))^j\| =$
$= \prod_{i>k}(g_i(\beta) - g_j(\beta))^2 = D(f)$. Между тем, $N_{L/K}(f'(\beta)) = \prod_{i=1}^n g_i(f'(\beta)) = \prod_{i=1}^n f'(g_i(\beta))$. Но $g_1(\beta), \dots g_n(\beta)$ — это множество корней многочлена f. Как мы видели в прошлой лекции при вычислении дискриминанта многочлена, $\prod_{i=1}^n f'(g_i(\beta)) = \prod_{i\neq j}(g_i(\beta) - g_j(\beta))$. Доказательство окончено.

Часть 3. Целые алгебраические числа.

Определение. Число $\alpha \in \mathbb{C}$ называется алгебраическим, если оно является корнем многочлена с целыми коэффициентами. Алгебраическое число называется *целым (алгебраическим)*, если оно является корнем многочлена с целыми коэффициентами и *старшим коэффициентом 1*, т.е унитарного целочисленного многочлена.

Например, число $\frac{-1+\sqrt{-3}}{2}$ — целое (это корень многочлена $x^3 - 1$), а число $\frac{1}{2}$ — не целое. Вообще, если рациональное число q является корнем многочлена $x^n + a_1 x^{n-1} + \ldots + a_n$ с целыми коэффициентами, то $q \in \mathbb{Z}$ (иначе знаменатель q^n ни с чем не мог бы сократиться).

Заменяя кольцо $\mathbb{Z}$ в предыдущем определении на произвольное кольцо $A \subset \mathbb{C}$, получаем определение числа *целого над* A.

Говорят, что кольцо $B \supset A$ является *конечным* A*-модулем*, если найдется конечное множество $\{ \beta_1, \dots, \beta_n \} \subset B$ такое, что всякий элемент $\beta \in B$

выражается в виде $\beta = \alpha_1\beta_1 + \ldots + \alpha_n\beta_n$ для некоторых $\alpha_1, \ldots, \alpha_n \in A$. Это аналог понятия конечного расширения полей (конечномерного векторного пространства над полем).

Теорема. a) Если число β целое над кольцом A, то кольцо $A[\beta]$ является конечным A-модулем;

b) Если кольцо $B \supset A$ является *конечным A-модулем*, то любое число $\beta \in B$ является целым над A.

Доказательство: a) Пусть β является корнем многочлена $x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$. Тогда в качестве системы образующих кольца $A[\beta]$ можно взять множество $\{1, \beta, \ldots, \beta^{n-1}\}$. Например, $\beta^n = -\alpha_1\beta^{n-1} - \ldots - \alpha_n \cdot 1$.

b) Пусть $\{\beta_1, \ldots, \beta_n\}$ — система образующих B над A. Тогда $\beta \cdot \beta_i = \sum_{j=1}^n \alpha_{ij}\beta_j$ для некоторых $\alpha_{ij} \in A$. Иначе говоря, матрица $X = \|\alpha_{ij}\| - \beta \mathrm{Id}$ с элементами из B аннулирует всякую образующую β_i. Если домножить эту матрицу слева на матрицу Y, состоящую из алгебраических дополнений, получим $YX = \det(X)\mathrm{Id}$. Таким образом, $\det(X) \in B$ аннулирует все образующие β_i, а значит и все кольцо B, откуда $\det(X) = 0$. Но $\det(X)$ — не что иное, как характеристический многочлен $\chi(\|\alpha_{ij}\|, \beta)$. Он имеет старший коэффициент 1 и все остальные коэффициенты из A. $\square$

Следствие. a) Сумма и произведение двух целых алгебраических чисел является целым алгебраическим;

b) Если α — корень многочлена $x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$, где $\alpha_1, \ldots, \alpha_n$ — целые алгебраические, то α тоже целое алгебраическое.

Доказательство: Если кольцо B является конечным A-модулем, а кольцо C является конечным B-модулем, то C является конечным A-модулем: в качестве системы образующих C над A можно взять $\{\beta_i\gamma_j\}$, где $\{\beta_i\}$ — множество образующих B над A, а $\{\gamma_j\}$ — множество образующих C над B. $\square$