0.1 Дискриминант

Определение 1. Пусть K/F — конечное сепарабельное расширение, $[K:F]=n$ и $\alpha_1,\ldots,\alpha_n\in K$. Тогда *дискриминант* набора $\alpha_1,\ldots,\alpha_n$ — это

$$\operatorname{disc}(\alpha_1,\ldots,\alpha_n)\overset{\text{def}}{=}\det\bigl(\operatorname{Tr}_{K/F}(\alpha_i\alpha_j)\bigr).$$

Так как расширение K/F сепарабельно, у нас есть ровно $n=[K:F]$ вложений $\sigma_1,\ldots,\sigma_n\colon K\to\mathbb{C}$ (на самом деле, мы знаем, что в $\mathbb{Q}^{alg}$).

Утверждение 1. $\operatorname{disc}(\alpha_1,\ldots,\alpha_n)=(\det(\sigma_i(\alpha_j))^2$.

Доказательство. Положим $\sigma_i(\alpha_j)=A$ и рассмотрим A^tA, тогда

$$(A^tA)_{ij}=\sum_{k=1}^n\sigma(\alpha_i)\sigma_k(\alpha_j)=\sum_{k=1}^n\sigma_k(\alpha_i\alpha_j)=\operatorname{Tr}_{K/F}(\alpha_i\alpha_j).$$

□

Посмотрим теперь, как след меняется при линейном преобразовании. Пусть $(\beta_1,\ldots,\beta_n)=(\alpha_1,\ldots,\alpha_n)M,\ M\in M_n(F)$.

Утверждение 2. $\operatorname{disc}(\alpha_1,\ldots,\alpha_n)=\operatorname{disc}(\beta_1,\ldots,\beta_n)\cdot(\det M)^2$.

Доказательство. Действительно, это напрямую следует из предложения 1:

$$\operatorname{disc}(\beta_1,\ldots,\beta_n)=\det(\sigma_i(\alpha_j))^2=\det\left(\sigma_i(\alpha_j)\right)M^2=\operatorname{disc}(\beta_1,\ldots,\beta_n)\cdot(\det M)^2.$$

□

Утверждение 3. $\operatorname{disc}(\alpha_1,\ldots,\alpha_n)=0\Leftrightarrow\alpha_1,\ldots,\alpha_n$ *— линейно зависимы.*

Доказательство. Пусть $\alpha_1,\ldots,\alpha_n$ — линейно зависимы, $e_1,\ldots,e_n$ — базис K/F.

$$(\alpha_1,\ldots,\alpha_n)=(e_1,\ldots,e_n)M,\quad \det M=0.$$

Значит, по предложению 2 мы имеем $\operatorname{disc}(\alpha_1,\ldots,\alpha_n)=0$. Теперь докажем в обратную сторону. Предположим, что $\alpha_1,\ldots,\alpha_n$ — линейно независимы, но $\operatorname{disc}(\alpha_1,\ldots,\alpha_n)=\det\bigl(\operatorname{Tr}_{K/F}(\alpha_i\alpha_j)\bigr)=0$. Рассмотрим систему линейных уравнений

$$\operatorname{Tr}_{K/F}((x_1\alpha_1+\ldots+x_n\alpha_n)\alpha_j)=0,\ldots 1\le j\le n.$$

Так как матрица коэффициентов этой системы — $\operatorname{Tr}_{K/F}(\alpha_i\alpha_j)$, а она вырождена, система имеет нетривиальное решение $(x_1,\ldots,x_n)$. Так как $\alpha_1,\ldots,\alpha_n$ — линейно независимы,

$$y=x_1\alpha_1+\ldots+x_n\alpha_n\ne 0.$$

С другой стороны, $\operatorname{Tr}_{K/F}(y\alpha_j)=0\,\forall j$. Так как α_i образуют базис K/F, по линейности мы получаем, что $\operatorname{Tr}_{K/F}(yu)=0\ \forall u\in K$. Но, так как расширение K/F сепарабельно, $\operatorname{Tr}_{K/F}$ должен быть невырожденной формой[1].

□

Лемма 1. Пусть $B\subset A$ — свободные абелевы группы ранга n. Пусть $\omega_1,\ldots,\omega_n$ — базис A, а $\left\{\sum_{j=1}^n a_{ij}w_j\right\}$ — базис B, $a_{ij}\in\mathbb{Z}$. Тогда $|A/B|=|\det(a_{ij})|$.

[1]Этим утверждением из теорией полей мы пользуемся без доказательств. Доказательство этого утверждения можно прочитать в S. Lang “Algebra”.

Доказательство. Приведём матрицу (a_{ij}) нормальной форме Смита. Перечислим теперь элементы A/B: это в точности элементы $x_1\omega_1 + \ldots + x_n\omega_n,\ 0 \le x_i \le a_{ii} - 1$. Если мы докажем, что это в точности все попарно-различные элементы группы A/B, то утверждение будет ясно.

Пусть $\sum_{i=1}^n x_i\omega_i = \sum_{i=1}^n y_i\omega_i$, тогда $\sum_{i=1}^n (x_i - y_i)\omega_i \in B$. Посмотрим на коэффициент при ω_{11}, он может получаться только из первой строки матрицы (так как матрица верхнетреугольная), тогда $\ell a_{11} = x_1 - y_1$, но это равенство возможно только в случае, когда $x_1 = y_1$ (так как есть ограничения на x_i и y_i). Далее мы проделаем аналогичное рассуждение $\sum_{i=2}^n (x_i - y_i)\omega_i \in B$ и в итоге получим, что все такие элементы разлчины.

Теперь рассмотрим $a = x_1\omega_1 + \ldots + x_n\omega_n,\ x_i \in \mathbb{Z}$. Поделим с остатком: $x_1 = a_{11}q + r,\ 0 \le r < a_{11}$, и рассмотрим $x_1\omega_1 + \ldots + x_n\omega_n - q(a_{11}\omega_1 + \ldots + a_{1n}\omega_n) = r\omega_1 + x_2'\omega_2 + \ldots$. Так как мы вычли из a элемент из B, класс $\overline{a} \in A/B$ не изменился, а старшим коэффициентом стал r, лежащий в нужном диапазоне. Продолжая в том же духе, мы полчми, что все коэффициенты лежат в нужном диапазоне. □

Как мы помним, $\mathcal{O}_K$ — свободная абелева группа ранга $n = [K : \mathbb{Q}]$ и $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$, а базис $(\omega_1, \ldots, \omega_n)$ мы называем *целым базисом.*

Определение 2. Пусть $K/\mathbb{Q}$ — расширение степени n, $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$. Тогда

$$\operatorname{disc}(K) \overset{\text{def}}{=} \operatorname{disc}(\omega_1, \ldots, \omega_k).$$

Замечание. Дискриминант поля не зависит от выбора целого базиса. Действительно, если у нас есть какой-то другой целый базис $(u_1, \ldots, u_n)$, то

$$(\omega_1, \ldots, \omega_n)M = (u_1, \ldots, u_n), \quad M \in \mathrm{SL}_n(\mathbb{Z}).$$

$$(u_1, \ldots, u_n)M^{-1} = (\omega_1, \ldots, \omega_n)$$
$$\operatorname{disc}(u_1, \ldots, u_n) = \operatorname{disc}(\omega_1, \ldots, \omega_n) \cdot \underbrace{(\det M)^2}_{=1}$$

Пусть $K = \mathcal{O}(\theta)$, $\theta \in \mathcal{O}_K$, положим $\operatorname{ind}(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]] = |\mathcal{O}_K/\mathbb{Z}[\theta]|$.

Утверждение 4. *В описанной выше сиутации* $\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \operatorname{ind}(\theta)^2 \cdot \operatorname{disc}(K)$.

Доказательство. Пусть $\omega_1, \ldots, \omega_n$ — целый базис. Тогда

$$(1, \theta, \ldots, \theta^{n-1}) = (\omega_1, \ldots, \omega_n)M \implies \operatorname{disc}(1, \ldots, \theta^{n-1}) = \operatorname{disc}(K)(\det M)^2.$$

Нетрудно заметить, что по лемме 1 мы имеем $|\det M| = \operatorname{ind}(\theta)$.

□

Пример 1. Пусть $K = \mathbb{Q}(\theta)$, где $\theta^3 - \theta - 1 = 0$. Как мы помним из домашнего задания, $\operatorname{disc}(1, \theta, \theta^2) = -23$. Пользуясь предложением 4 мы получаем, что $-23 = (\operatorname{ind}(\theta))^2 \cdot \operatorname{disc} K \implies \operatorname{ind}\theta = 1$, из чего следует, что $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Пример 2. Пусть $K = \mathbb{Q}(\theta)$, где $\theta^3 - \theta - 4 = 0$. Как мы помним, $\operatorname{disc}(1, \theta, \theta^2) = -4 \cdot 107 = (\operatorname{ind}\theta)^2 \cdot \operatorname{disc} K$, Тогда $\operatorname{ind}\theta = 1$ или $\operatorname{ind}\theta = 2$. С другой стороны, так как $\frac{\theta + \theta^2}{2} \in \mathcal{O}_K, \notin \mathbb{Z}[\theta]$, $\operatorname{ind}(\theta) \ne 1$. Значит, $\operatorname{ind}\theta = 2$, из чего мы имеем разложение

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\frac{\theta + \theta^2}{2}.$$

Домашнее задание 1. Задачи:

1. Предположим, что K/F — расширение Галуа, $[K : F]$ — нечётна. Докажите, что тогда для любого базиса $e_1, \ldots, e_n$ расширения K/F будет выполнено $\operatorname{disc}(e_1, \ldots, e_n) \in F^{*2}$.
2. Рассмотрим $K = \mathbb{Q}(\sqrt[p]{1})$. Тогда $\zeta, \zeta^2, \ldots \zeta^{p-1}$ образуют базис $K/\mathbb{Q}$. Докажите, что $|\operatorname{disc}(\zeta, \zeta^2, \ldots, \zeta^{p-1})| = p^{p-2}$. *Hint:* тут можно действовать строго согласно определению 1.

3. Пусть $K/\mathbb{Q}$ — расширение степени n, $K = \mathbb{Q}(\theta)$, где $\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0$ и пусть p — такое простое число, что $v_p(a_0) = 1$ и $v_p(a_i) \geq 1$. Докажите, что тогда $p \nmid \operatorname{ind}(\theta)$.
4. Докажите, что если $K = \mathbb{Q}(\sqrt[p]{1})$, где p — простое, то $\mathcal{O}_K = \mathbb{Z}[\zeta]$, где $\zeta^p = 1$.
5. Тут были еще задачи, я их не успел записать, но сфоткал.

Приведём сейчас другое, конструктивное доказательство того, что $\mathcal{O}_K$ — конечнопорожденная абелева группа.

Возьмем $\omega_1, \omega_2, \ldots, \omega_n \in \mathcal{O}_K$, где $\omega_1, \ldots, \omega_n$ — базис K на $\mathbb{Q}$. Тогда $\operatorname{disc}(\omega_1, \ldots, \omega_n) \in \mathbb{Z}$, возьмем набор $(\omega_1, \ldots, \omega_n)$ с минимальным модулем дискриминанта. Докажем, что тогда он и будет целым базисом.

Возьмем $x \in \mathcal{O}_K,\ x = \sum a_i\omega_i,\ a_i \in \mathbb{Q}$ и покажем, что $a_i \in \mathbb{Z}$. Предположим противное, не умаляя общности $a_1 \notin \mathbb{Z}$.

$$x \in \mathcal{O}_K \implies \sum \{a_i\}\omega_i = x - \sum [a_i]\omega_i \in \mathcal{O}_K.$$

Перейдём к набору $(\sum\{a_i\}\omega_i, \omega_2, \ldots, \omega_n)$. Покажем, что модуль его дискриминанта уменьшился. Действительно,

$$(\sum\{a_i\}\omega_i, \omega_2, \ldots, \omega_n) = (\omega_1, \ldots, \omega_n) \cdot \begin{pmatrix} \{a_1\} & \ldots & \ldots & \ldots \\ \{a_2\} & 1 & \ldots & \ldots \\ \vdots & \vdots & \ddots & \vdots \\ \{a_n\} & \ldots & \ldots & 1 \end{pmatrix}.$$

а определитель матрицы, написаной справа равен $\{a_1\} \leq 1$.