代数数域的判别式

戚天成 ✉

复旦大学 数学科学学院

2024 年 1 月 24 日

设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_1x^{n-1}+a_n$ 是域 K 上多项式, 并设 f 在 K 的代数闭包 $\overline{K}$ 上的所有根为 $\alpha_1,...,\alpha_n$. 回忆 f 的**判别式**为

$$D(f)=a_0^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

根据多项式判别式的定义不难看出它不依赖于根的标号次序. 判别式是用于判断多项式是否有重根的工具. 易见 f 在 $\overline{K}$ 上有重根当且仅当 $D(f)=0$. 多项式的判别式最早可追溯到 A. Cayley(英国, 1821-1895)[Cay48] 和 J. J. Sylvester(英国, 1814-1897)[Syl51] 的工作. 近年来人们利用判别式 (理想) 来研究代数自同构群、代数同构问题、Zariski 消去问题以及 Azumaya 轨迹等问题, 可参见综述 [WZ18].

如果 $f(x)=ax^2+bx+c$ 是特征为零的域 K 上多项式, $a\neq 0$. 那么 $f(x)$ 在 $\overline{K}$ 上有根

$$\alpha_1=\frac{-b+\sqrt{b^2-4ac}}{2a},\alpha_2=\frac{-b-\sqrt{b^2-4ac}}{2a}.$$

于是易计算得到 $D(f)=b^2-4ac$. 这与二次方程的经典判别式一致. 事实上, 对一般的域 K, 由 Vieta 定理知

$$\alpha_1+\alpha_2=-\frac{b}{a},\alpha_1\alpha_2=\frac{c}{a},$$

同样可得 $D(f)=b^2-4ac$. 一般地, K 上多项式的结式总是 K 中元素, 并且可完全借助给定多项式的系数计算: 若记多项式 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_1x^{n-1}+a_n(a_0\neq 0)$ 和其形式导数的结式为 $\mathrm{Res}(f,f')$, 则有

$$D(f)=\frac{(-1)^{n(n-1)/2}}{a_0}\mathrm{Res}(f,f').$$

这份笔记的主要目的是介绍代数数域的判别式与整基的基本概念, 主要参考文献是 [Yic] 和 [Neu13]. 正文主要由如下两部分构成:

(1) 域的有限扩张的迹映射与范数映射的概念与基本性质, 本原元定理以及有限可分扩张到基域代数闭包的嵌入性质 (见 [命题1.6]). 我们将看到有限可分扩张的迹映射可诱导一非退化对称双线性型 (见 [推论1.8]).

(2) n 次有限可分扩张的 n 元子集的判别式, 它与经典多项式的判别式的关系 (见 [例2.3]), 代数数域的整数环作为 $\mathbb{Z}$-模是有限生成自由模 (见 [推论2.8]), 代数数域的整数环是 Dedekind 整区 (见 [推论2.9]), 代数数域的整数环的整基以及代数数域的判别式.

1 迹与范数

Definition 1.1. 设 $K \subseteq L$ 是域的有限扩张, $x \in L$, 并记 $\ell_x : L \to L$ 是 x 决定的左乘变换. 称 K-线性变换 ℓ_x 的迹 $\mathrm{tr}(\ell_x)$ 为 x 关于 K 的**迹**, 记作 $\mathrm{tr}_{L/K}(x)$. 称 ℓ_x 的行列式 $\det(\ell_x)$ 为 x 关于 K 的**范数**, 记作 $N_{L/K}(x)$.

Remark 1.2. 将 $\mathrm{tr}_{L/K} : L \to K, x \mapsto \mathrm{tr}_{L/K}(x)$ 与 $N_{L/K} : L \to K, x \mapsto N_{L/K}(x)$ 分别称为**迹映射**与**范数映射**.

因为迹与范数分别由有限维空间上线性变换的迹与行列式定义, 所以自然具备下面的基本性质.

Proposition 1.3. 设 $K \subseteq L$ 是域的有限扩张, 那么
(1) 任给 $x, y \in L$, 有 $\mathrm{tr}_{L/K}(x+y) = \mathrm{tr}_{L/K}(x) + \mathrm{tr}_{L/K}(y), N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.
(2) 任给 $x \in L, \alpha \in K$, 有 $\mathrm{tr}_{L/K}(\alpha x) = \alpha \mathrm{tr}_{L/K}(x), N_{L/K}(\alpha x) = \alpha^n N_{L/K}(x)$, 其中 $n = [L : K]$.

Lemma 1.4. 设 $K \subseteq L$ 是 n 次域扩张, $x \in L$. 并设 $p(T) = T^m + a_1 T^{m-1} + \cdots + a_{m-1}T + a_m \in K[T]$ 是 x 在 K 上最小多项式. 那么 m 整除 n 且 $\mathrm{tr}_{L/K}(x) = -(n/m)a_1$ $N_{L/K}(x) = (-1)^n (a_m)^{n/m}$.

Proof. 这时 $K(x)$ 作为 K 与 L 的中间域满足 $[K(x) : K] = m$, 因此 m 整除 n. 考虑 $\theta : L \to \mathrm{End}_K L, y \mapsto \ell_y$, 那么 θ 是单 K-线性映射, 所以 x 和 ℓ_x 在 K 上具有相同的最小多项式. 又因为 ℓ_x 在 K 上特征多项式与最小多项式在相伴意义下具有相同的不可约因子, 所以 ℓ_x 在 K 上特征多项式是 $p(T)$ 的某个正整数幂. 比较多项式次数便知 ℓ_x 在 K 上的特征多项式为 $p(T)^{n/m}$. 因此考察 $p(T)^{n/m}$ 的次高次项系数与常数项便得结果. □

Remark 1.5. 如果 $L = K(x)$, 那么 $n = m$. 这时 $\mathrm{tr}_{L/K}(x) = -a_1$ $N_{L/K}(x) = (-1)^m a_m$.

回忆域扩张 $K \subseteq L$ 是**可分扩张**, 如果这是代数扩张且 L 中元素在 K 上最小多项式都没重根. 例如特征为零的域的任何代数扩张可分. 下面的本原元定理告诉我们有限可分扩张总是单扩张.

Primitive Element Theorem. 任何有限可分扩张都是单扩张. 即如果 $L \supseteq K$ 是有限可分扩张, 那么存在 $\alpha \in L$ 使得 $L = K(\alpha)$, 这时称 α 是该域扩张的**本原元**.

Proof. 下面分 K 是无限域或是有限域两种情形讨论证明定理. 如果 K 是无限域, 则任何 K 的有限扩张 L 总可写作 $L = K(\alpha_1, ..., \alpha_n)$ 的形式, 其中每个 $\alpha_j \in L$ 是 K 上代数元. 下面对 n 作归纳来证明结论, 不难看出只需验证 $n = 2$ 的情形即可. 即说明对域扩张 $L = K(\alpha_1, \alpha_2)$, 存在 $c \in L$ 使得 $L = K(c)$. 对 $j = 1, 2$, 设 α_j 在域 K 上的最小多项式为 $p_j(x)$, 那么存在 L 的扩域 E 使得 $p_1(x), p_2(x)$ 均在 E 上分裂 (注意可分扩张的条件保证了 $p_j(x)$ 没有重根). 设为 $p_1(x) = (x - \beta_1) \cdots (x - \beta_s), p_2(x) = (x - \gamma_1) \cdots (x - \gamma_t), \beta_i, \gamma_j \in E$. 不妨设 $\beta_1 = \alpha_1, \gamma_1 = \alpha_2$. 因为 K 是无限集而

$$S = \left\{ \frac{\beta_i - \beta_1}{\gamma_1 - \gamma_j} \middle| 1 \le i \le s, 2 \le j \le t \right\} \subseteq E$$

是有限集, 故存在 $d \in K$ 使得 $d \notin S$. 进而 $\beta_i \neq \beta_1 + d(\gamma_1 - \gamma_j), \forall 1 \le i \le s, 2 \le j \le t$.

Claim. 对 $c = \alpha_1 + d\alpha_2 = \beta_1 + d\gamma_1$ 有 $L = K(\alpha_1, \alpha_2) = K(c)$.

一旦证明该断言便得到结果. 为证此断言只需要说明 $K(\alpha_1, \alpha_2) \subseteq K(c)$. 下证 $\gamma_1 = \alpha_2 \in K(c)$, 考虑域 $K(c)$ 上多项式 $p_2(x)$ 以及 $r(x) = p_1(c - dx)$, 它们有公共零点 γ_1, 所以均可被 γ_1 在 $K(c)$ 上最小多项式 $m(x)$ 整除. 下证 $m(x) = x - \gamma_1$ 来得到 $\gamma_1 \in K(c)$. 一方面, $m(x)$ 在 E 中的零点集是 $\{\gamma_1, ..., \gamma_t\}$ 的子集, 另一方面,

对每个 $2 \le j \le t$, $r(\gamma_j) = p_1(\beta_1 + d(\gamma_1 - \gamma_j)) \neq 0$. 因此 $m(x)$ 在 E 中的零点只有 γ_1. 而 $E \supseteq K$ 是可分扩张表明 $m(x)$ 在 E 上无重根, 由此得到 $m(x) = x - \gamma_1$. 结合 c 的定义立即看到 $\gamma_1 \in K(c)$ 蕴含 $\alpha_1 \in K(c)$.

最后我们验证 K 是有限域时结论成立. 现设 $K \subseteq L$ 是有限域 K 的有限可分扩张, 设 $\mathrm{char}K = p$, 那么 K 包含素域 $\mathbb{F}_p$, 即 p 元域. 下面说明存在 $\alpha \in L$ 使得 $L = \mathbb{F}_p(\alpha)$ 来得到 $L = K(\alpha)$. 设 $|L| = p^m$, 如果 $\alpha \in L$ 满足 $\mathbb{F}_p(\alpha)$ 的元素数目为 $p^n, n < m$, 那么 α 满足多项式 $x^{p^n} - x$, 这说明对每个正整数 $n < m$, L 中满足 $\mathbb{F}_p(\alpha)$ 的元素数目为 $p^n (n < m)$ 的元素 α 的数目不超过 p^n. 注意到

$$p + p^2 + \cdots + p^{m-1} = \frac{p^m - p}{p - 1} < p^m,$$

所以 L 中满足 $\mathbb{F}_p(\alpha) \subsetneq L$ 的元素 α 总数严格小于 p^m. 因此存在 $\alpha \in L$ 使得 $L = \mathbb{F}_p(\alpha)$. □

Proposition 1.6. 设 K 是域, L 是 K 的有限可分扩张, 并设 $n = [L : K]$.
(1) 若记 $\overline{K}$ 是 K 的代数闭包, 那么恰好存在 n 个不同的嵌入 $\sigma_i : L \to \overline{K} (1 \le i \le n)$ 使得 $\sigma_i(a) = a, \forall a \in K$.
(2) 上述 n 个嵌入 $\{\sigma_1, ..., \sigma_n\}$ 是 $\overline{K}$-线性无关的.

Proof. 由本原元定理知可设 $L = K(c)$ 是单扩张, 并设 c 在域 K 上最小多项式是 $m(x)$, 那么有域同构

$$K[x]/(m(x)) \cong L.$$

设 $\alpha_1, ..., \alpha_n$ 是 $m(x)$ 在 $\overline{K}$ 中所有的根, 那么域扩张的可分性说明这些根两两互异. 记 $\sigma_i : L \to \overline{K}, g(c) \mapsto g(\alpha_i)$, 这里 $g(x) \in K[x]$, 则 σ_i 是定义合理的域嵌入且 $\sigma_1, ..., \sigma_n$ 两两互异且固定 K 中元素. 对任何固定 K 中元素的域嵌入 $\tau : L \to \overline{K}$, $\tau(c)$ 为 $m(x)$ 的根, 因此 $\tau \in \{\sigma_1, ..., \sigma_n\}$. 最后证明对 $n \ge 1$ 作归纳来说明 $\{\sigma_1, ..., \sigma_n\}$ 是 $\overline{K}$-线性无关的. 假设 $\{\sigma_1, ..., \sigma_n\}$ 是 $\overline{K}$-线性相关的, 则存在不全为零的元素 $c_1, ..., c_n \in \overline{K}$ 使得 $c_1\sigma_1 + \cdots + c_n\sigma_n = 0$. 那么对满足条件的非零 n 元组 $(c_1, ..., c_n) \in \overline{K}^n$, 总可找到非零分量数目最小的 n 元组. 经过适当重排 $\sigma_1, ..., \sigma_n$ 可不妨设该 n 元组恰好前 d 个分量非零. 设为 $c_1, ..., c_d \in \overline{K}^*$ 使得 $c_1\sigma_1 + \cdots + c_d\sigma_d = 0$. 不妨设 $c_1 = 1$, 那么对任给 $x \in L$ 有 $\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_d\sigma_d(x) = 0$. 选取 $y \in L$ 使得 $\sigma_1(y) \neq \sigma_2(y)$, 那么通过 $\sigma_1(xy) + c_2\sigma_2(xy) + \cdots + c_d\sigma_d(xy) = \sigma_1(x)\sigma_1(y) + \cdots + c_d\sigma_d(x)\sigma_d(y) = 0$. 可得

$$c_2(\sigma_1(y) - \sigma_2(y))\sigma_2(x) + \cdots + c_d(\sigma_1(y) - \sigma_d(y))\sigma_d(x) = 0, \forall x \in L.$$

上式中 $c_2(\sigma_1(y) - \sigma_2(y)) \neq 0$, 这与 d 的选取矛盾. □

Proposition 1.7. 设 K 是域, L 是 K 的有限可分扩张, 并设 $n = [L : K]$. 根据 [命题1.6], 记 $\overline{K}$ 是 K 的代数闭包, 那么恰好存在 n 个不同的嵌入 $\sigma_i : L \to \overline{K} (1 \le i \le n)$ 使得 $\sigma_i(a) = a, \forall a \in K$ 并且 $\{\sigma_1, ..., \sigma_n\}$ 是 $\overline{K}$-线性无关的. 这时对任何 $x \in L$ 有

$$\mathrm{tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x), N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

Proof. 设 $L = K(c)$ 是单扩张, 那么根据 [命题1.6] 的构造过程, $\sigma_1(c), ..., \sigma_n(c)$ 是 c 在 K 上最小多项式的所有根, 结合 $[L : K] = n$ 知 $\sigma_1(c), ..., \sigma_n(c)$ 是 ℓ_c 在 $\overline{K}$ 中所有特征根. 任取 $x \in L$, 则存在 $g(T) \in K[T]$ 使得 $x = g(c)$. 所以由每个 σ_i 是 K-代数同态知 ℓ_x 在 $\overline{K}$ 中的所有特征根是 $\sigma_1(g(c)), ..., \sigma_n(g(c))$. 改写记号得到 ℓ_x 在 $\overline{K}$ 中所有特征根就是 $\sigma_1(x), ..., \sigma_n(x)$. 于是结论明显成立. □

Corollary 1.8. 设 K 是域, L 是 K 的有限可分扩张, 并设 $n=[L:K]$. 那么迹映射诱导的 K-双线性映射

$$(-,-):L\times L\to K,(x,y)\mapsto \mathrm{tr}_{L/K}(xy)$$

是非退化对称双线性型.

Proof. 易见 $(-,-):L\times L\to K$ 是对称的. 假设 $x\in L$ 满足 $(x,y)=0,\forall y\in L$, 下证 $x=0$. 设 $\{\sigma_1,...,\sigma_n\}$ 是 [命题1.6] 中的嵌入, 这时 $\sigma_1(x)\sigma_1(y)+\cdots+\sigma_n(x)\sigma_n(y)=0,\forall y\in L$. 进而由 $\{\sigma_1,...,\sigma_n\}$ 的 K-线性无关性得到 $\sigma_i(x)=0,\forall 1\le i\le n$. 于是由 σ_i 是单 K-线性映射得到 $x=0$. 所以 $(-,-)$ 是非退化的 K-双线性型. □

Corollary 1.9. 设 R 是整区, 有商域 K. 那么对 K 的任何有限可分扩张 L, R 在 L 中的整闭包 $\mathcal{O}$ 满足

$$\mathrm{tr}_{L/K}(\beta)\in\mathcal{O}\cap K,\forall\beta\in\mathcal{O}.$$

如果更进一步 R 是整闭整区, 那么 $\mathrm{tr}_{L/K}(\beta)\in R,\forall\beta\in\mathcal{O}$.

Proof. 考虑 [命题1.6] 给出的嵌入 $\{\sigma_1,...,\sigma_n\}$, [推论1.8] 表明 $\mathrm{tr}_{L/K}(x)=\sigma_1(x)+\cdots+\sigma_n(x),\forall x\in L$. 所以当 $\beta\in\mathcal{O}$ 时, 每个 $\sigma_i(\beta)\in\mathcal{O}$, 进而 $\mathrm{tr}_{L/K}(\beta)\in\mathcal{O}$. 如果 R 进一步整闭, 那么由 $K\cap\mathcal{O}=R$ 便得结论. □

称有理数域的有限扩张为**代数数域**. 如果 L 是代数数域, 称 $\mathbb{Z}$ 在 L 中的整闭包 $\{x\in L|x是\mathbb{Z}上整元\}$ 为代数数域 L 的**整数环**, 记作 $\mathcal{O}_L$. 易见 $\mathcal{O}_L$ 是整区, 之后我们会证明它是 Dedekind 整区 (见 [推论2.9]).

Example 1.10. 设 L 是代数数域, 那么由 $\mathbb{Q}\subseteq L$ 是有限可分扩张知任何 $\beta\in\mathcal{O}_L$ 满足 $\mathrm{tr}_{L/\mathbb{Q}}(\beta)\in\mathbb{Z}$.

Corollary 1.11. 设 K 是域, L 是 K 的有限可分扩张, 并设 $n=[L:K]$ 且 $\alpha_1,...,\alpha_n\in L$. 那么 $\{\alpha_1,...,\alpha_n\}$ 是 K-线性无关集 (所以是 ${}_KL$ 的一个基) 当且仅当 $\det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))_{n\times n}\neq 0$.

Proof. 考虑 K-线性映射 $\varphi:K^n\to L,(k_1,...,k_n)\mapsto k_1\alpha_1+\cdots+k_n\alpha_n$ 和 $\psi:L\to K^n,x\mapsto((\alpha_1,x),...,(\alpha_n,x))$, 其中 $(-,-):L\times L\to K$ 是来自 [推论1.8] 的非退化对称双线性型. 那么 $\psi\varphi:K^n\to K^n$ 在标准基下表示矩阵就是 $(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))_{n\times n}$. 充分性：如果该矩阵可逆, 那么 φ 是单射, 这说明 $\{\alpha_1,...,\alpha_n\}$ 是 K-线性无关集. 必要性：这时 φ 是单射, 因此由 $\dim_K L=n$ 知 φ 是 K-线性同构. 结合 [推论1.8] 知 ψ 是单射. 因此 $\psi\varphi$ 是单 K-线性映射, 故也是同构. 于是 $(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))_{n\times n}$ 自然可逆. □

Remark 1.12. 若记 A 是下面的矩阵, 通过 [命题1.7] 易计算验证 $(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))_{n\times n}=A^TA$.

$$A=\begin{pmatrix}\sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n)\\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n)\\ \vdots & \vdots & & \vdots\\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n)\end{pmatrix}$$

2 判别式与整基

在 [推论1.11] 中我们看到如果 $L\supseteq K$ 是域的 n 次有限可分扩张, 那么对 $\{\alpha_1,...,\alpha_n\}\subseteq L$, $\{\alpha_1,...,\alpha_n\}$ 是 L 作为 K-线性空间的基当且仅当 $\det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))_{n\times n}\neq 0$.

Definition 2.1. 设 K 是域, L 是 K 的有限可分扩张, 并设 $n=[L:K]$ 且 $\alpha_1,...,\alpha_n\in L$. 称 $\det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))_{n\times n}$ 是 $\{\alpha_1,...,\alpha_n\}$ 的**判别式**, 记作 $D_{L/K}(\alpha_1,...,\alpha_n)$.

Remark 2.2. 因此 [推论1.11] 表明 $\{\alpha_1,...,\alpha_n\}$ 是 K-线性无关集等价于它们的判别式 $D_{L/K}(\alpha_1,...,\alpha_n)\neq 0$.

Example 2.3. 设 $L\supseteq K$ 是域的 n 次可分扩张, β 是该域扩张的本原元. $\{\sigma_1,...,\sigma_n\}$ 是 [命题1.6] 中的嵌入, 满足 $\sigma_1(\beta),...,\sigma_n(\beta)$ 是 β 在 K 上最小多项式的所有根. 那么这时

$$D_{L/K}(1,\beta,...,\beta^{n-1})=\det\begin{pmatrix}\sigma_1(1)&\sigma_1(\beta)&\cdots&\sigma_1(\beta^{n-1})\\ \sigma_2(1)&\sigma_2(\beta)&\cdots&\sigma_2(\beta^{n-1})\\ \vdots&\vdots&&\vdots\\ \sigma_n(1)&\sigma_n(\beta)&\cdots&\sigma_n(\beta^{n-1})\end{pmatrix}\det\begin{pmatrix}\sigma_1(1)&\sigma_1(\beta)&\cdots&\sigma_1(\beta^{n-1})\\ \sigma_2(1)&\sigma_2(\beta)&\cdots&\sigma_2(\beta^{n-1})\\ \vdots&\vdots&&\vdots\\ \sigma_n(1)&\sigma_n(\beta)&\cdots&\sigma_n(\beta^{n-1})\end{pmatrix}.$$

利用 Vandermonde 行列式计算公式立即得到 $D_{L/K}(1,\beta,...,\beta^{n-1})$ 是 β 在 K 上最小多项式的经典判别式.

Example 2.4. 设 L 是代数数域, $\{\alpha_1,...,\alpha_n\}\subseteq L$. 那么 $\{\alpha_1,...,\alpha_n\}$ 是 $\mathbb{Q}$-线性无关集 $\Leftrightarrow D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n)\neq 0$.

Remark 2.5. 特别地, 对 $\{\alpha_1,...,\alpha_n\}\subseteq\mathcal{O}_L$, $\{\alpha_1,...,\alpha_n\}$ 是 $\mathbb{Z}$-线性无关集 $\Leftrightarrow D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n)\neq 0$.

Proposition 2.6. 设 $L\supseteq K$ 是域的 n 次有限可分扩张, $\{\alpha_1,...,\alpha_n\},\{\beta_1,...,\beta_n\}\subseteq L$ 满足存在 $C\in\mathrm{M}_n(K)$ 使得 $(\beta_1,...,\beta_n)=(\alpha_1,...,\alpha_n)C$, 那么 $D_{L/K}(\beta_1,...,\beta_n)=D_{L/K}(\alpha_1,...,\alpha_n)(\det C)^2$.

Proof. 记 A,B 分别为如下的 K 上 n 阶方阵, 那么 $B=AC$.

$$A=\begin{pmatrix}\sigma_1(\alpha_1)&\sigma_1(\alpha_2)&\cdots&\sigma_1(\alpha_n)\\ \sigma_2(\alpha_1)&\sigma_2(\alpha_2)&\cdots&\sigma_2(\alpha_n)\\ \vdots&\vdots&&\vdots\\ \sigma_n(\alpha_1)&\sigma_n(\alpha_2)&\cdots&\sigma_n(\alpha_n)\end{pmatrix},B=\begin{pmatrix}\sigma_1(\beta_1)&\sigma_1(\beta_2)&\cdots&\sigma_1(\beta_n)\\ \sigma_2(\beta_1)&\sigma_2(\beta_2)&\cdots&\sigma_2(\beta_n)\\ \vdots&\vdots&&\vdots\\ \sigma_n(\beta_1)&\sigma_n(\beta_2)&\cdots&\sigma_n(\beta_n)\end{pmatrix}$$

根据前面的讨论, $\mathrm{tr}_{L/K}(\alpha_i\alpha_j))_{n\times n}=A^TA$ 且 $\mathrm{tr}_{L/K}(\beta_i\beta_j))_{n\times n}=B^TB$, 故由 $B^TB=C^TA^TAC$ 即得. □

下面我们来说明代数数域的整数环作为 $\mathbb{Z}$-模总是有限生成自由模, 首先我们需要

Lemma 2.7. 设 R 是整闭整区, 有商域 K, $L\supseteq K$ 是域的 n 次有限可分扩张, R 在 L 中整闭包记作 $\mathcal{O}$. 并设 $\{\alpha_1,...,\alpha_n\}\subseteq\mathcal{O}$ 是 ${}_KL$ 的基 (对 L 的 K-基乘上 R 中适当的元素总可调整在 $\mathcal{O}$ 中). 那么对每个 $\beta\in\mathcal{O}$, 其关于 $\{\alpha_1,...,\alpha_n\}$ 的 K-线性表示 $\beta=k_1\alpha_1+\cdots+k_n\alpha_n$ 满足

$$D_{L/K}(\alpha_1,...,\alpha_n)k_i\in R,\forall 1\leq i\leq n.$$

Proof. 设 $\{\sigma_1,...,\sigma_n\}$ 是 [命题1.6] 中的嵌入, 那么

$$\begin{pmatrix}\sigma_1(\beta)\\ \sigma_2(\beta)\\ \vdots\\ \sigma_n(\beta)\end{pmatrix}=\begin{pmatrix}\sigma_1(\alpha_1)&\sigma_1(\alpha_2)&\cdots&\sigma_1(\alpha_n)\\ \sigma_2(\alpha_1)&\sigma_2(\alpha_2)&\cdots&\sigma_2(\alpha_n)\\ \vdots&\vdots&&\vdots\\ \sigma_n(\alpha_1)&\sigma_n(\alpha_2)&\cdots&\sigma_n(\alpha_n)\end{pmatrix}\begin{pmatrix}k_1\\ k_2\\ \vdots\\ k_n\end{pmatrix}.$$

记 $A=(\sigma_i(\alpha_j))_{n\times n}\in\overline{K}^{n\times n}$, 那么 $D_{L/K}(\alpha_1,...,\alpha_n)=(\det A)^2$, 故 $\det A\neq 0$. 对上式两边同乘 A^{-1} 得

$$\begin{pmatrix}k_1\\k_2\\\vdots\\k_n\end{pmatrix}=A^{-1}\begin{pmatrix}\sigma_1(\beta)\\\sigma_2(\beta)\\\vdots\\\sigma_n(\beta)\end{pmatrix}=\frac{A^*}{\det A}\begin{pmatrix}\sigma_1(\beta)\\\sigma_2(\beta)\\\vdots\\\sigma_n(\beta)\end{pmatrix}=(\det A)^{-1}\begin{pmatrix}\delta_1\\\delta_2\\\vdots\\\delta_n\end{pmatrix}.$$

根据 [推论1.9] 这里每个 δ_i 都满足 $(\det A)\delta_i\in R$. 所以对上式两边同乘上 $D_{L/K}(\alpha_1,...,\alpha_n)$ 便得结论. □

Corollary 2.8. 设 L 是代数数域, 那么 $\mathcal{O}_L$ 作为 $\mathbb{Z}$-模是有限生成自由模.

Proof. 设 L 是 $\mathbb{Q}$ 的 n 次扩张, 并取 L 的一个由 $\mathcal{O}_L$ 中元素构成的 K-基 $\{\alpha_1,...,\alpha_n\}$. 那么利用 [引理2.7] 得到 $D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n)\mathcal{O}_L\subseteq\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$. 通过 [例1.10] 知 $D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n)$ 是非零整数, 所以 $\mathcal{O}_L$ 作为 $\mathbb{Z}$-模同构于有限生成自由 $\mathbb{Z}$-模 $\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$ 的子模. 因为 P.I.D. 上自由模的子模仍自由, 故结论明显成立. □

回忆 **Dedekind 整区**是指 1 维 Noether 整闭整区. 下面我们说明代数数域的整数环是 Dedekind 整区.

Corollary 2.9. 代数数域的整数环是 Dedekind 整区.

Proof. 设 L 是 $\mathbb{Q}$ 的有限扩张, 那么 [推论2.8] 表明 $\mathcal{O}_L$ 是交换 Noether 环. 因为 $\mathbb{Z}\subseteq\mathcal{O}_L$ 是整扩张, 所以 $\mathrm{k.dim}\mathcal{O}_L=\mathrm{k.dim}\mathbb{Z}=1$. 由 $\mathcal{O}_L\subseteq L$ 是整闭扩张立即得到 $\mathcal{O}_L$ 是整闭整区. □

Definition 2.10. 设 L 是代数数域, 称 $\mathcal{O}_L$ 作为有限生成自由 $\mathbb{Z}$-模的基 $\{\alpha_1,...,\alpha_n\}$ 为 $\mathcal{O}_L$ 的**整基**.

Proposition 2.11. 设 L 是代数数域, $\{\alpha_1,...,\alpha_n\}$ 是其整基, $\{\beta_1,...,\beta_n\}\subseteq\mathcal{O}_L$. 那么存在 $t\in\mathbb{Z}$ 使得

$$D_{L/\mathbb{Q}}(\beta_1,...,\beta_n)=t^2D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n).$$

并且 $\{\beta_1,...,\beta_n\}$ 是 $\mathcal{O}_L$ 的整基当且仅当 $t^2=1$.

Proof. 首先存在整数矩阵 $C\in\mathrm{M}_n(\mathbb{Z})$ 使得 $(\beta_1,...,\beta_n)=(\alpha_1,...,\alpha_n)C$. 取 $t=\det C$, 由 [命题2.6] 便知

$$D_{L/\mathbb{Q}}(\beta_1,...,\beta_n)=t^2D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n).$$

如果 $t^2=1$, 那么由 $D_{L/\mathbb{Q}}(\beta_1,...,\beta_n)\neq 0$ 便知 $\{\beta_1,...,\beta_n\}$ 是整基. 反之, 如果 $\{\beta_1,...,\beta_n\}$ 是整基, 那么同样存在整数 s 使得 $D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n)=s^2D_{L/\mathbb{Q}}(\beta_1,...,\beta_n)$. 于是 $s^2t^2=1$. 这迫使 $t^2=1$. □

由代数数域的整数环的任意两个整基的判别式相同这一观察, 自然产生了代数数域的一个数值不变量——代数数域的判别式. 它是由 R. Dedekind(德国, 1831-1916) 于 1871 年给出的.

Definition 2.12. 设 L 是代数数域, $\{\alpha_1,...,\alpha_n\}$ 为 $\mathcal{O}_L$ 的整基. 称 $D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n)$ 是 L 的**判别式**.

Remark 2.13. 设 $\{\sigma_1,...,\sigma_n\}$ 是 [命题1.6] 中的嵌入, 那么 L 的判别式 $D_{L/\mathbb{Q}}(\alpha_1,...,\alpha_n)=(\det A)^2$, 其中

$$A=\begin{pmatrix}\sigma_1(\alpha_1)&\sigma_1(\alpha_2)&\cdots&\sigma_1(\alpha_n)\\\sigma_2(\alpha_1)&\sigma_2(\alpha_2)&\cdots&\sigma_2(\alpha_n)\\\vdots&\vdots&&\vdots\\\sigma_n(\alpha_1)&\sigma_n(\alpha_2)&\cdots&\sigma_n(\alpha_n)\end{pmatrix}$$

参考文献

[Cay48] A. Cayley. On the theory of elimination. *Cambridge Dublin Math J*, 3:116–120, 1848.

[Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[Syl51] J. J. Sylvester. On a remarkable discovery in the theory of canonical forms and of hyperdeterminants. *Philos Magazine*, 2:391–410, 1851.

[WZ18] Y.H. Wang and J.J. Zhang. Discriminants of noncommutative algebras and their applications. *Sci. China Math*, 48:1615–1630, 2018.

[Yic] Tian Yichao. Lectures on algebraic number theory.