Journal of Number Theory 131 (2011) 994–1019

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the zeta function associated with module classes of a number field

Xia Gao

School of Mathematical Science, Peking University, Beijing 100871, PR China

ARTICLE INFO

Article history:
Received 16 September 2007
Revised 5 January 2010
Accepted 19 November 2010
Available online 12 February 2011
Communicated by D. Zagier

MSC:
11R
11E
11M

Keywords:
Orders
Conductors
Binary cubic forms
Zeta functions

ABSTRACT

Text. The goal of this note is to generalize a formula of Datskovsky and Wright on the zeta function associated with integral binary cubic forms. We show that for a fixed number field K of degree d, the zeta function associated with decomposable forms belonging to K in $d-1$ variables can be factored into a product of Riemann and Dedekind zeta functions in a similar fashion. We establish a one-to-one correspondence between the pure module classes of rank $d-1$ of K and the integral ideals of width $< d-1$. This reduces the problem to counting integral ideals of a special type, which can be solved using a tailored Moebius inversion argument. As a by-product, we obtain a characterization of the conductor ideals for orders of number fields.

Video. For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=RePyaF8vDnE.

1. Introduction

Let K be a cubic extension of $\mathbb{Q}$. We say a binary cubic form $f(x,y) \in \mathbb{Z}[x,y]$ belongs to K if $f(\theta,1)=0$ for some irrational $\theta \in K$. Let $S_{2,K}$ denote the set of binary cubic forms belonging to K. The group $\Gamma = \mathrm{SL}(2,\mathbb{Z})$ acts on $S_{2,K}$ by

$$\gamma f(x,y) = f\big((x,y)\gamma\big) = f(ax+cy, bx+dy),$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $f \in S_{2,K}$. We denote by $D(f)$ the discriminant of f and by

$$\Gamma_f = \{\gamma \in \Gamma \mid \gamma f = f\}$$

E-mail addresses: xia@math.pku.edu.cn, gaomxia@yahoo.cn.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.11.010

the isotropic subgroup of f in Γ. The cardinality $|\Gamma_f|$ is finite and is an invariant of the Γ-orbit of f. We define

$$\xi_K(s) = \sum_f \frac{1}{|\Gamma_f|} \big|D(f)\big|^{-s}, \quad s \in \mathbb{C} \tag{1}$$

where the sum is taken over a set of Γ-orbit representatives of $S_{2,K}$.

In the course of adelizing Shintani's work [19] on binary cubic forms, Datskovsky and Wright [5] discovered the following formula

$$\xi_K(s) = 2m_K^{-1}|\Delta_K|^{-s}\zeta(4s)\zeta(6s-1)\frac{\zeta_K(2s)}{\zeta_K(4s)}. \tag{2}$$

Here $m_K = 3$ if K is Galois and 1 otherwise, Δ_K denotes the discriminant of K, $\zeta(s)$ and $\zeta_K(s)$ denote respectively the Riemann zeta function and the Dedekind zeta function of K.

Such a beautiful relation could not hold only in the case of cubic fields. Since there is a discriminant-preserving bijection between the $\mathrm{GL}(2,\mathbb{Z})$-classes of integral binary cubic forms belonging to a cubic field K and the isomorphism classes of orders of K [6], one way to generalize this formula is to count the orders of a fixed number field by index. This difficult task is accomplished by Nakagawa [15] in the quartic case. However, the formula he obtained is somewhat complicated; for example it is not clear at present whether his zeta function can be continued meromorphically to the whole complex plane.

The goal of this note is to give a direct generalization of (2) in arbitrary number fields. As a natural candidate for binary cubic forms, we consider decomposable forms belonging to a degree d number field K in $d-1$ variables. After introducing the concept of semi-discriminants and module indexes, we obtain an analogous zeta function (8) for $\xi_K(s)$. We show that this zeta function can be factored into a product of Riemann and Dedekind zeta functions in a similar fashion (see Theorems 2.1, 2.5). As it turns out, our counting result can also be formulated in terms of orders. But here, instead of counting the index of orders, we count the module index of the incomplete canonical module of orders (Theorem 2.3).

As a by-product, we obtain a characterization of the fractional ideals generated by subsets of a dimension $d-1$ subspace of K and the conductor ideals of orders in K (Theorems 5.2, 5.8). We also compute the conductor ideals of some widely used orders and discuss their Gorenstein properties. Considering the vast literature on the subject, it is somewhat surprising that these results have not been discovered before.

In Sections 2 and 3 we develop the concept of module index and formulate the main results in terms of module classes and decomposable forms belonging to a number field K. In Section 4 we establish a one-to-one correspondence between pure module classes of rank $d-1$ of K and integral ideals of width $< d-1$. Some of its consequences and applications to orders are discussed in Section 5. In Section 6 we show that our zeta function has an Euler product and compute these factors using a tailored Moebius inversion argument.

Much of the theory developed in this note can be stated for a finite dimensional associative algebra over a Dedekind domain, and this will be given in [9]. The recent proof of Ohno's conjecture on Shintani zeta functions associated with the space of binary cubic forms [16] suggests that in this area interesting structures can still be dug out.

2. Definitions and results

Let K be a number field of degree d over $\mathbb{Q}$. Let δ_K denote the different, Δ_K the discriminant, and $\mathcal{O}_K$ the ring of integers of K. The field K has d distinct embeddings $\sigma_1, \sigma_2, \ldots, \sigma_d$ into an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $\mathbb{M}_n$ $(1 \leqslant n \leqslant d)$ denote the set of free $\mathbb{Z}$-submodules of K of rank n. We call two modules M and $M' \in \mathbb{M}_n$ equivalent if there is a $\gamma \neq 0$ in K such that $\gamma M = \{\gamma\alpha \mid \alpha \in M\} = M'$. We denote by $[M]$ the module class of M and by $\mathbb{M}_n^{\sim}$ the quotient of $\mathbb{M}_n$ modulo the action of K^*.

Let $M \in \mathbb{M}_n$. We define the semi-discriminant of M, denoted by $\operatorname{dis} M$, as follows. Choose a $\mathbb{Z}$-basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ for M, write $\mathfrak{a}$ for the fractional ideal of $\mathcal{O}_K$ generated by M and $\mathbf{N}\mathfrak{a}$ for the absolute norm of $\mathfrak{a}$. Then

$$\operatorname{dis} M = \mathbf{N}\mathfrak{a}^{-2\binom{d-1}{n-1}} \prod_{1 \leqslant i_1 < \cdots < i_n \leqslant d} \det\bigl(\sigma_{i_v}(\alpha_j)\bigr)^2_{1 \leqslant v, j \leqslant n}.$$

Note that $\operatorname{dis} M$ is well defined and depends only on the module class of M. Moreover, as we shall see in Lemma 3.1 below, there is a unique integer $m \geqslant 0$ such that

$$\operatorname{dis} M = \Delta_K^{\binom{d-2}{n-2}} m^2. \tag{3}$$

This integer m is called the index of M, and denoted by $\operatorname{ind} M$. It depends only on the module class of M.

We call M and its module class $[M]$ degenerate if $\operatorname{ind} M = 0$. When $n = 1, d-1$ or d, every $M \in \mathbb{M}_n$ is non-degenerate. In the case $n = 2$, M is degenerate if and only if M is equivalent to a module contained in a proper subfield of K. In the general case, however, M can be degenerate even if K does not contain any non-trivial subfield. For instance, let ζ be a primitive 23rd root of unity, $\theta_i = \zeta^i + \zeta^{-i}$ for $1 \leqslant i \leqslant 11$, and $K = \mathbb{Q}(\theta_1)$. Let $M \in \mathbb{M}_3$ be the $\mathbb{Z}$-submodule of K generated by 1, θ_1, $h(\theta_1)$, where $h(x) = x^7 + x^6 - 7x^5 - 5x^4 + 14x^3 + 6x^2$. Then M is degenerate since

$$\det \begin{bmatrix} 1 & \theta_1 & h(\theta_1) \\ 1 & \theta_3 & h(\theta_3) \\ 1 & \theta_5 & h(\theta_5) \end{bmatrix} = 0.$$

In this note we are mostly interested in the case $n = d - 1$. We attach to each number field K a zeta function

$$\eta_K(s) = \sum_{[M] \in \mathbb{M}^{\sim}_{d-1}} \operatorname{ind} M^{-s}, \quad s \in \mathbb{C}. \tag{4}$$

Our main result is the following.

Theorem 2.1. *Let K be a number field of degree $d \geqslant 3$. Let $\zeta(s)$ denote the Riemann zeta function and $\zeta_K(s)$ the Dedekind zeta function of K. Then*

$$\eta_K(s) = \zeta(ds-1)\zeta(ds-2)\cdots\zeta(ds-d+2)\frac{\zeta_K(s)}{\zeta_K((d-1)s)}. \tag{5}$$

In particular, $\eta_K(s)$ converges absolutely for $\operatorname{Re} s > 1$ and has a meromorphic extension to the whole complex plane.

The proof of Theorem 2.1 is broken up into a sequence of lemmas and is given in Sections 4 and 6.

Corollary 2.2. *Let $N(K, X)$ denote the number of module classes in $\mathbb{M}^{\sim}_{d-1}$ whose module index is $< X$, and let ρ_K be the residue of $\zeta_K(s)$ at $s = 1$. Then, for any $\epsilon > 0$,*

$$N(K, X) = \frac{\zeta(d-1)\zeta(d-2)\cdots\zeta(2)}{\zeta_K(d-1)}\rho_K X + O\bigl(X^{1-\frac{1}{d}+\epsilon}\bigr).$$

Proof. We use the classical theorem

$$\sum_{n<X} a_n = \rho_K X + O\big(X^{1-\frac{1}{d}}\big), \quad \text{where } \zeta_K(s) = \sum_{n\geqslant 1} \frac{a_n}{n^s}.$$

Observe that the Dirichlet series

$$\frac{\zeta(ds-1)\zeta(ds-2)\cdots\zeta(ds-d+2)}{\zeta_K((d-1)s)} = \sum_{m\geqslant 1} \frac{b_m}{m^s}$$

converges absolutely for $\operatorname{Re} s > 1 - 1/d$. It follows that

$$\begin{aligned} N(K,X) &= \sum_{km<X} a_k b_m = \sum_{m<X} b_m \sum_{k<X/m} a_k \\ &= \rho_K X \sum_{m<X} \frac{b_m}{m} + O\left(X^{1-\frac{1}{d}+\epsilon} \sum_{m<X} \frac{|b_m|}{m^{1-\frac{1}{d}+\epsilon}}\right) \\ &= \rho_K X \sum_{m=1}^{\infty} \frac{b_m}{m} - \rho_K X \sum_{m\geqslant X} \frac{b_m}{m} + O\big(X^{1-\frac{1}{d}+\epsilon}\big). \end{aligned}$$

Clearly

$$\left| X \sum_{m\geqslant X} \frac{b_m}{m} \right| \leqslant \sum_{m\geqslant X} \frac{|b_m|}{m^{1-\frac{1}{d}+\epsilon}} \frac{X}{X^{\frac{1}{d}-\epsilon}} = O\big(X^{1-\frac{1}{d}+\epsilon}\big)$$

and this gives the result. □

Theorem 2.1 can also be formulated in terms of orders.

Let $V_0 = \{\alpha \in K \mid \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = 0\}$ denote the trace zero hyperplane of K. If $\mathcal{O}$ is an order of K, write $\mathcal{O}^\vee = \{\beta \in K \mid \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z},\ \forall \alpha \in \mathcal{O}\}$ for its dual module. We call the $\mathbb{Z}$-module $\mathcal{O}^\vee \cap V_0 \in \mathbb{M}_{d-1}$ the incomplete canonical module of $\mathcal{O}$. It can be shown that the map

$$\begin{aligned} \psi : \{\text{primitive orders of } K\} &\to \widetilde{\mathbb{M}_{d-1}}, \\ \mathcal{O} &\mapsto \big[\mathcal{O}^\vee \cap V_0\big] \end{aligned}$$

is a bijection (cf. Theorem 5.9). Moreover, the incomplete canonical module of $\mathcal{O}$ has module index

$$g(\mathcal{O}) = \frac{[\mathcal{O} : \mathfrak{f}_{\mathcal{O}}]^{d-1}}{[\mathcal{O}_K : \mathcal{O}]},$$

where $\mathfrak{f}_{\mathcal{O}}$ denotes the conductor of $\mathcal{O}$. Note that $g(\mathcal{O})$ is an integer dividing $[\mathcal{O}_K : \mathcal{O}]^{d-2}$. It is equal to $[\mathcal{O}_K : \mathcal{O}]^{d-2}$ if and only if $\mathcal{O}$ is a Gorenstein order (Lemma 5.11). Since primitive cubic orders are always Gorenstein, we have in this case $g(\mathcal{O}) = [\mathcal{O}_K : \mathcal{O}]$.

To each number field K we define a zeta function

$$\varsigma_K(s) = \sum_{\mathcal{O}\subseteq\mathcal{O}_K} g(\mathcal{O})^{-s},$$

where the sum extends over all primitive orders $\mathcal{O}$ of K. Combining Theorem 2.1, we immediately have the following result.

Theorem 2.3. *With the notations above,*

$$\varsigma_K(s) = \zeta(ds-1)\zeta(ds-2)\cdots\zeta(ds-d+2)\frac{\zeta_K(s)}{\zeta_K((d-1)s)}. \tag{6}$$

We next translate Theorem 2.1 into the context of decomposable forms. Assume that $1 < n \leqslant d$. Let $S_{n,K}$ denote the set of n-ary degree d homogeneous polynomials $f(x_1,\dots,x_n) \in \mathbb{Z}[x_1,\dots,x_n]$ belonging to K, that is, f has a linear factor $l(x_1,\dots,x_n) = \alpha_1 x_1 + \cdots + \alpha_n x_n$ with $\alpha_j \in \mathbb{C}$ for $1 \leqslant j \leqslant n$ such that

$$\mathbb{Q}(\alpha_i/\alpha_j \mid \alpha_j \neq 0,\ 1 \leqslant i, j \leqslant n) = K.$$

The group $\mathrm{GL}(n,\mathbb{Z})$ acts on $S_{n,K}$ by

$$Uf(x_1,\dots,x_n) = f\big((x_1,\dots,x_n)U\big), \quad \forall U \in \mathrm{GL}(n,\mathbb{Z}),\ f \in S_{n,K}.$$

For each $f \in S_{n,K}$, let

$$f(x_1,\dots,x_n) = \prod_{i=1}^{d}(\alpha_{i1}x_1 + \cdots + \alpha_{in}x_n), \quad \alpha_{ij} \in \mathbb{C}$$

be a factorization into linear forms and define

$$D(f) = \prod_{1\leqslant i_1<\cdots<i_n\leqslant d} \det(\alpha_{i_\nu j})^2_{1\leqslant \nu, j\leqslant n}.$$

Clearly $D(f)$ does not depend on the factorization of f and satisfies

$$D(Uf) = D(f), \quad \forall U \in \mathrm{GL}(n,\mathbb{Z}).$$

Put

$$\overline{S}_{n,K} = \big\{ f \in S_{n,K} \;\big|\; f \text{ is primitive and } D(f) \neq 0\big\}/\{\pm 1\}$$

and $G = \mathrm{GL}(n,\mathbb{Z})/\{\pm 1\}$. The action of $\mathrm{GL}(n,\mathbb{Z})$ on $S_{n,K}$ induces a G-action on $\overline{S}_{n,K}$. We define the discriminant of $\bar{f} = \{\pm f\} \in \overline{S}_{n,K}$ by $D(\bar{f}) = D(f)$. Clearly $D(\bar{f})$ is an invariant of the G-orbit of $\bar{f}$.

Let $M \in \mathbb{M}_n$ be a non-degenerate module with a $\mathbb{Z}$-basis $\alpha_1,\dots,\alpha_n$, and let $\mathfrak{a}$ be the fractional ideal generated by M. Observe that

$$f(x_1,\dots,x_n) = \frac{1}{\mathbf{N}\mathfrak{a}}\prod_{i=1}^{d}\big(\sigma_i(\alpha_1)x_1 + \cdots + \sigma_i(\alpha_n)x_n\big)$$

is a primitive irreducible homogeneous polynomial in $\mathbb{Z}[x_1,\dots,x_n]$. Moreover, multiplying $\alpha_1,\dots,\alpha_n$ by a non-zero element of K changes f at most by a sign, choosing a different $\mathbb{Z}$-basis for M amounts to a $\mathrm{GL}(n,\mathbb{Z})$ action on f. Thus we have a well-defined map

$$\Phi : [M] \mapsto G\text{-orbit of } \bar{f} \tag{7}$$

from the set of non-degenerate classes in $\mathbb{M}_n^{\sim}$ onto $\overline{S}_{n,K}/G$. Note that Φ preserves discriminants, i.e., $D(\bar{f}) = \operatorname{dis} M$ for $\bar{f} \in \Phi([M])$.

Let $G_{\bar{f}}$ denote the isotropic subgroup of $\bar{f}$ in G and $\mathrm{Aut}(K)$ the automorphic group of K. Put $m_{\bar{f}} = |G_{\bar{f}}|$ and $m_K = |\mathrm{Aut}(K)|$. Note that $m_{\bar{f}}$ is an invariant for the G-orbit of $\bar{f}$.

Lemma 2.4. *For $1 < n < d$ and $\bar{f} \in \overline{S}_{n,K}$, the isotropic group $G_{\bar{f}}$ is isomorphic to a subgroup of* $\mathrm{Aut}(K)$. *Furthermore, the G-orbit of $\bar{f}$ has precisely $m_K/m_{\bar{f}}$ inverse images under Φ.*

Proof. Let $\bar{f} = \{\pm f\} \in \overline{S}_{n,K}$ and let $l(\underline{x}) = \alpha_1 x_1 + \cdots + \alpha_n x_n$ be a linear factor of f with $\mathbb{Q}(\alpha_j \mid 1 \leqslant j \leqslant n) = K$. For each $U \in \mathrm{GL}(n,\mathbb{Z})$ satisfying $Uf = \pm f$, there is a unique $\sigma \in \mathrm{Aut}(K)$ such that

$$Ul(\underline{x}) = l(\underline{x}U) = \gamma\big(\sigma(\alpha_1)x_1 + \cdots + \sigma(\alpha_n)x_n\big)$$

for some $0 \neq \gamma \in K$. It is easy to check that the map $\{\pm U\} \mapsto \sigma^{-1}$ is a monomorphism from $G_{\bar{f}}$ into $\mathrm{Aut}(K)$. The second statement follows from the fact that the $G_{\bar{f}}$-action on $\{\sigma l(\underline{x}) \mid \sigma \in \mathrm{Aut}(K)\}$ has $m_K/m_{\bar{f}}$ distinct orbits. □

In the case $n = d-1$, we define an analogue of (2) as

$$\xi_K^*(s) = \sum_{\bar{f}} m_{\bar{f}}^{-1} \big|D(\bar{f})\big|^{-s}, \quad s \in \mathbb{C} \tag{8}$$

where the sum is taken over a set of G-orbit representatives in $\overline{S}_{d-1,K}$.

Theorem 2.5. *Let K be a number field of degree $d \geqslant 3$ with discriminant Δ_K. Then*

$$\xi_K^*(s) = m_K^{-1} |\Delta_K|^{-(d-2)s} \eta_K(2s). \tag{9}$$

In the case where K is a cubic field, we may identify G-orbits in $\overline{S}_{2,K}$ with primitive $\mathrm{GL}(2,\mathbb{Z})$-orbits in $S_{2,K}$ defined in the introduction. To include non-primitive $\mathrm{GL}(2,\mathbb{Z})$-orbits, we have to multiply $\xi_K^*(s)$ by the factor $\zeta(4s)$. Finally, each $\mathrm{GL}(2,\mathbb{Z})$-orbit in $S_{2,K}$ splits into two Γ-orbits, we get

$$\xi_K(s) = 2\zeta(4s)\xi_K^*(s)$$

which is exactly (2) by Theorem 2.1.

3. Preliminaries

Throughout this note, K denotes a number field of degree d over $\mathbb{Q}$, $\mathbb{M}_n$ denotes the set of free $\mathbb{Z}$-submodules of K of rank n. If M, N are $\mathbb{Z}$-submodules of K, MN will be the $\mathbb{Z}$-submodule of K generated by elements $\alpha\beta$ with $\alpha \in M$ and $\beta \in N$. If N is a submodule of M, we write M/N for the quotient module of M modulo N. We use $\mathrm{N}_{K/\mathbb{Q}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}$ to denote respectively the norm and trace map from K to $\mathbb{Q}$. Write

$$V_0 = \big\{\alpha \in K \;\big|\; \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0\big\}$$

for the trace zero hyperplane of K. For each $M \in \mathbb{M}_d$, we define its dual module by

$$M^{\vee} = \big\{\beta \in K \;\big|\; \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z} \text{ for all } \alpha \in M\big\} \cong \mathrm{Hom}(M,\mathbb{Z}).$$

Let δ_{ij} denote the Kronecker delta symbol, i.e., $\delta_{ij}=1$ if $i=j$ and $\delta_{ij}=0$ otherwise. If S is a finite set, we use $|S|$ and $\#S$ to denote its cardinality. If $U=(u_{ij})$ is a $k\times l$ matrix, $I=\{i_1,\dots,i_r\}$ $(1\leqslant i_1<\cdots<i_r\leqslant k)$ and $J=\{j_1,\dots,j_r\}$ $(1\leqslant j_1<\cdots<j_r\leqslant l)$, we denote by

$$U_{I,J}=\det(u_{ij})_{i\in I,\,j\in J}$$

the minor of U obtained from the corresponding $r\times r$ sub-matrix. In the case $r=l\leqslant k$, we also write

$$U_I=U_{I,J}=\det(u_{ij})_{i\in I,\,1\leqslant j\leqslant l}.$$

Furthermore, we denote by

$$\Lambda_r(U)=(U_{I,J})_{|I|=|J|=r}$$

the r-th compound matrix of U [12, §7.2, p. 417].

Lemma 3.1. *For $M\in\mathbb{M}_n$, the index of M defined by* (3) *is a rational integer.*

Proof. Let $\omega_1,\dots,\omega_d$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and $\alpha_1,\dots,\alpha_n$ a $\mathbb{Z}$-basis for M. Put

$$\mathfrak{a}=\mathcal{O}_K M\quad\text{and}\quad A=\big(\sigma_i(\alpha_j)\big)_{1\leqslant i\leqslant d,\,1\leqslant j\leqslant n}.$$

We claim that

$$\beta=\mathbf{N}\mathfrak{a}^{-\binom{d-1}{n-1}}\big(\det\big(\sigma_i(\omega_j)\big)_{1\leqslant i,j\leqslant d}\big)^{-\binom{d-2}{d-n}}\prod_{|I|=n}A_I$$

is a rational integer.

Let L be the Galois closure of K. Note that each $\tau\in\mathrm{Gal}(L/\mathbb{Q})$ induces a permutation $\sigma\mapsto\tau\sigma$ on the set of embeddings $\sigma_1,\dots,\sigma_d$. It is easy to check that $\tau(\beta)=\beta$, $\forall\tau\in\mathrm{Gal}(L/\mathbb{Q})$. Thus $\beta\in\mathbb{Q}$.

To show that β is an integer, we argue locally. Let p be a rational prime, $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ at p. Since multiplying M by a non-zero element of K changes β at most by a sign, we may assume that $\mathfrak{a}$ is integral and coprime to p.

Let $\mathfrak{P}_1,\dots,\mathfrak{P}_r$ be the prime ideals of $\mathcal{O}_K$ lying above p. For $1\leqslant v\leqslant r$, let $K_{\mathfrak{P}_v}$ denote the completion of K at $\mathfrak{P}_v$, $\mathcal{O}_{\mathfrak{P}_v}$ the valuation ring of $K_{\mathfrak{P}_v}$. Then $\mathcal{O}_{\mathfrak{P}_v}=\mathbb{Z}_p[\gamma_v]$ for some $\gamma_v\in\mathcal{O}_{\mathfrak{P}_v}$. Moreover, set $d_v=[K_{\mathfrak{P}_v}:\mathbb{Q}_p]$, $s_0=0$ and $s_v=\sum_{1\leqslant i\leqslant v}d_i$ for $1\leqslant v\leqslant r$.

Regarding $\sigma_1,\dots,\sigma_d$ as embeddings of K into an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, we may index them so that $\sigma_i(K)$ $(s_{v-1}<i\leqslant s_v)$ and $K_{\mathfrak{P}_v}$ are conjugate over $\mathbb{Q}_p$. Let $\gamma_{v,k}$ $(1\leqslant k\leqslant d_v)$ denote the corresponding conjugate of γ_v in $\sigma_{s_{v-1}+k}(K)$. Thus

$$1,\gamma_{v,k},\dots,\gamma_{v,k}^{d_v-1}$$

form a $\mathbb{Z}_p$-basis for the valuation ring of $\sigma_{s_{v-1}+k}(K)$. Write

$$B_v=\big(\gamma_{v,k}^{l}\big)_{1\leqslant k\leqslant d_v,\,0\leqslant l<d_v}$$

for the Vandermonde matrix and $B=\mathrm{diag}_{1\leqslant v\leqslant r}(B_v)$ for the $d\times d$ matrix with B_v's in the diagonal. Then there exists a $d\times n$ matrix C with entries in $\mathbb{Z}_p$ such that $A=BC$. Taking the n-th compound matrix on both sides, we obtain

$$\Lambda_n(A)=\Lambda_n(B)\Lambda_n(C),$$

where $\Lambda_n(C)=(C_I)_{|I|=n}$ is a column vector with entries in $\mathbb{Z}_p$.

Let v_p denote the unique non-archimedean valuation on $\overline{\mathbb{Q}}_p$ extending the usual one on $\mathbb{Q}_p$, i.e., $\mathrm{v}_p(p) = 1$. We have

$$\begin{aligned}\sum_{|I|=n} \mathrm{v}_p(A_I) &\geqslant \sum_{|I|=n} \min_{|J|=n} \{\mathrm{v}_p(B_{I,J})\} \\ &= \sum_{\substack{n_1,\dots,n_r\geqslant 0 \\ n_1+\cdots+n_r=n}} \sum_{1\leqslant v\leqslant r} \sum_{|I_v|=n_v} \min_{|J_v|=n_v} \{\mathrm{v}_p((B_v)_{I_v,J_v})\}. \end{aligned} \tag{10}$$

It is clear that for subsets $I_v, J_v \subseteq \{1, 2, \dots, d_v\}$ of n_v elements,

$$\begin{aligned}\mathrm{v}_p((B_v)_{I_v,J_v}) &\geqslant \mathrm{v}_p(\det(\gamma_{v,k}^{l})_{k\in I_v,\, 0\leqslant l<n_v}) \\ &= \begin{cases} \sum_{k,k'\in I_v,\, k<k'} \mathrm{v}_p(\gamma_{v,k} - \gamma_{v,k'}) & \text{if } n_v \geqslant 2, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Let $\Delta_{\mathfrak{P}_v}$ denote the discriminant of $K_{\mathfrak{P}_v}$ over $\mathbb{Q}_p$. The right-hand side of (10) now becomes

$$\begin{aligned}&= \binom{d-2}{n-2} \sum_{1\leqslant v\leqslant r} \sum_{1\leqslant k<k'\leqslant d_v} \mathrm{v}_p(\gamma_{v,k} - \gamma_{v,k'}) \\ &= \frac{1}{2}\binom{d-2}{n-2} \sum_{v=1}^{r} \mathrm{v}_p(\Delta_{\mathfrak{P}_v}) \\ &= \frac{1}{2}\binom{d-2}{n-2} \mathrm{v}_p(\Delta_K).\end{aligned}$$

This proves that $\mathrm{v}_p(\beta) \geqslant 0$ for any prime $p \in \mathbb{Z}$. Hence $\operatorname{ind} M = |\beta|$ is a rational integer. □

4. Pure modules and the width of complementary ideals

In this section we assume $1 \leqslant n < d$. Let $M \in \mathbb{M}_n$ and $\mathfrak{a}$ the fractional ideal generated by M. We say that M is pure if M is a direct summand of $\mathfrak{a}$. Equivalent modules must share the same pureness property. We call a module class pure if it consists of only pure modules.

If $M \in \mathbb{M}_n$ is a pure module, its complementary module is defined as follows. Choose a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ for M and extend it to a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n, \dots, \alpha_d$ for $\mathfrak{a}$. Let $\{\beta_j\}_{1\leqslant j\leqslant d}$ be the dual basis of $\{\alpha_i\}_{1\leqslant i\leqslant d}$, i.e.,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\beta_j) = \delta_{ij}, \quad \forall i, j.$$

Thus $\beta_1, \dots, \beta_d$ form a $\mathbb{Z}$-basis for the fractional ideal $\mathfrak{a}^\vee = (\delta_K\mathfrak{a})^{-1}$. The $\mathbb{Z}$-module generated by $\beta_{n+1}, \dots, \beta_d$ is a pure module in $\mathbb{M}_{d-n}$, which does not depend on the choice of bases for M and $\mathfrak{a}$. It is called the complementary module of M, and denoted by $M^\wedge$. Moreover, let $\mathfrak{b}$ be the unique integral ideal of $\mathcal{O}_K$ satisfying

$$(\beta_{n+1}, \dots, \beta_d) = \mathfrak{a}^\vee\mathfrak{b}.$$

Then $\mathfrak{b}$ depends only on the module class of M. It is called the complementary ideal associated with $[M]$.

Lemma 4.1. *With M and $\mathfrak{b}$ as above, we have*

$$\operatorname{ind} M = \mathbf{N}\mathfrak{b}^{\binom{d-1}{n}} \operatorname{ind} M^{\wedge}.$$

Proof. Let $A = (\sigma_i(\alpha_j))_{1\leqslant i,j\leqslant d}$ and $B = (\sigma_i(\beta_j))_{1\leqslant i,j\leqslant d}$. Thus

$$A^T = B^{-1} \quad \text{and} \quad \det A^2 = \mathbf{N}\mathfrak{a}^2 \Delta_K.$$

If U is a $d\times d$ matrix, we write $\Lambda_r^*(U) = (U_{I,J}^*)$ for the matrix obtained from the r-th compound matrix $\Lambda_r(U) = (U_{I,J})$ by replacing $U_{I,J}$ in each entry with its cofactor $U_{I,J}^*$ in U (see [12, p. 417]). Using Laplace's expansion formula and the properties of compound matrix, we have

$$\Lambda_{d-n}^*(A) = \det A\big(\Lambda_{d-n}(A)^T\big)^{-1} = \det A\,\Lambda_{d-n}(B).$$

In particular, for $J = \{1,2,\dots,n\}$, $J' = \{n+1,\dots,d\}$, $I = \{i_1,\dots,i_n\}$ and $I' = \{i_{n+1},\dots,i_d\}$ such that $\{i_1,\dots,i_d\}$ is a permutation of $\{1,2,\dots,d\}$, we have

$$A_{I,J} = \pm \det A B_{I',J'}.$$

Therefore

$$\begin{aligned}
\operatorname{ind}^2 M &= \Delta_K^{-\binom{d-2}{n-2}} \mathbf{N}\mathfrak{a}^{-2\binom{d-1}{n-1}} \prod_{|I|=n} A_{I,J}^2 \\
&= \Delta_K^{\binom{d}{n}-\binom{d-2}{n-2}} \mathbf{N}\mathfrak{a}^{2\binom{d-1}{n}} \prod_{|I'|=d-n} B_{I',J'}^2 \quad \left(\binom{d}{n} = \binom{d-1}{n} + \binom{d-1}{n-1}\right) \\
&= \Delta_K^{\binom{d-1}{n}+\binom{d-2}{n-1}} \mathbf{N}\mathfrak{a}^{2\binom{d-1}{n}} \mathbf{N}\big(\delta_K^{-1}\mathfrak{a}^{-1}\mathfrak{b}\big)^{2\binom{d-1}{n}} \operatorname{dis} M^{\wedge} \\
&= \mathbf{N}\mathfrak{b}^{2\binom{d-1}{n}} \operatorname{ind}^2 M^{\wedge}.
\end{aligned}$$

Taking square roots gives the desired result. □

Corollary 4.2. *If $M \in \mathbb{M}_{d-1}$ is a pure module, $\mathfrak{b}$ is its complementary ideal. Then* $\operatorname{ind} M = \mathbf{N}\mathfrak{b}$.

Let $\mathfrak{b}$ be a non-zero integral ideal of $\mathcal{O}_K$. By the elementary divisor theorem for torsion free modules, there exists a $\mathbb{Z}$-basis $\omega_1,\dots,\omega_d$ for $\mathcal{O}_K$ and positive integers $b_1,\dots,b_d$ such that

$$\mathfrak{b} = \mathbb{Z}b_1\omega_1 \oplus \cdots \oplus \mathbb{Z}b_d\omega_d$$

with $b_i \mid b_{i-1}$ for $1 < i \leqslant d$. The integers $b_1,\dots,b_d$ are uniquely determined by $\mathfrak{b}$. The largest subscript l with $b_l \neq 1$ (in the case $b_1 = 1$, put $l = 0$) is called the width of $\mathfrak{b}$ in $\mathcal{O}_K$, denoted by $\operatorname{width}(\mathfrak{b})$. It is the minimal number of cyclic components of the finite abelian group $\mathcal{O}_K/\mathfrak{b}$.

Lemma 4.3. *If M is a pure module in $\mathbb{M}_n$ with $1 \leqslant n < d$ and $\mathfrak{b}$ the complementary ideal associated with M. Then* $\operatorname{width}(\mathfrak{b}) < n$.

Proof. Suppose $\operatorname{width}(\mathfrak{b}) = l \geqslant n$. Then there exists a rational prime p such that $\mathbf{N}(\mathfrak{b} + p\mathcal{O}_K) = p^l$. Thus the integral ideal $\mathfrak{c} = (\mathfrak{b} + p\mathcal{O}_K)^{-1}p\mathcal{O}_K$ has norm p^{d-l}. As before, let $\alpha_1,\dots,\alpha_n$ be a $\mathbb{Z}$-basis for M and $\alpha_1,\dots,\alpha_n,\dots,\alpha_d$ a $\mathbb{Z}$-basis for $\mathfrak{a} = \mathcal{O}_K M$. Let $\{\beta_j\}_{1\leqslant j\leqslant d}$ denote the dual basis

of $\{\alpha_i\}_{1\leqslant i\leqslant d}$. Then $(\beta_{n+1},\dots,\beta_d)=\mathfrak{a}^\vee\mathfrak{b}$. By the elementary divisor theorem, there exists a $\mathbb{Z}$-basis $\omega_1,\dots,\omega_d$ for $\mathfrak{a}$ such that $\omega_1,\dots,\omega_l\in\mathfrak{ca}$. Thus, for $1\leqslant i\leqslant l$, $n<j\leqslant d$, we have

$$\omega_i\beta_j\in\mathfrak{ca}\mathfrak{a}^\vee\mathfrak{b}=\mathfrak{c}\mathfrak{b}\delta_K^{-1}\subseteq p\delta_K^{-1}\quad\text{and so}\quad \operatorname{Tr}_{K/\mathbb{Q}}(\omega_i\beta_j)\in p\mathbb{Z}. \tag{11}$$

Put $\mathbb{F}=\mathbb{Z}/p\mathbb{Z}$. Note that $\operatorname{Tr}_{K/\mathbb{Q}}(xy)$ $(x\in\mathfrak{a},\ y\in\mathfrak{a}^\vee)$ induces a non-degenerate $\mathbb{F}$-bilinear pairing between the $\mathbb{F}$-vector spaces $\mathfrak{a}/p\mathfrak{a}$ and $\mathfrak{a}^\vee/p\mathfrak{a}^\vee$. Let V denote the subspace of $\mathfrak{a}/p\mathfrak{a}$ generated by the images of $\alpha_1,\dots,\alpha_n$, and N the subspace of $\mathfrak{a}^\vee/p\mathfrak{a}^\vee$ generated by the images of $\beta_{n+1},\dots,\beta_d$. Clearly V is the orthogonal complement of N with respect to the above pairing. Moreover, let W be the subspace of $\mathfrak{a}/p\mathfrak{a}$ generated by the images of $\omega_1,\dots,\omega_l$. Then by (11), $W\subseteq V$. Since $\dim_{\mathbb{F}}W\geqslant\dim_{\mathbb{F}}V$, we have $W=V$, $l=n$. But this would imply

$$\mathfrak{a}=(\alpha_1,\dots,\alpha_n)\subseteq(\omega_1,\dots,\omega_n)+p\mathfrak{a}\subseteq\mathfrak{ca}+p\mathfrak{a}$$

which is impossible. □

Let $I_{K,l}$ denote the set of integral ideals of $\mathcal{O}_K$ of width $<d-l$. We have now constructed a map Ψ_n from the set of pure module classes in $\mathbb{M}_n^\sim$ into $I_{K,d-n}$ by sending $[M]$ to the complementary ideal associated with M. Such maps are in general difficult to deal with. But in the case $n=d-1$, we have:

Lemma 4.4. *The map Ψ_{d-1} is a bijection.*

Proof. Suppose first that $M,M'\in\mathbb{M}_{d-1}$ are pure modules with

$$\Psi_{d-1}\big([M]\big)=\Psi_{d-1}\big(\big[M'\big]\big)=\mathfrak{b}.$$

We claim that M and M' lie in the same module class. Let $\mathfrak{a}=\mathcal{O}_KM$ and $\mathfrak{a}'=\mathcal{O}_KM'$. Clearly $\mathfrak{a}$ and $\mathfrak{a}'$ lie in the same ideal class. Multiplying M by a suitable non-zero element of K if necessary, we may assume that $\mathfrak{a}=\mathfrak{a}'$. Now M and M' both have the form

$$\big\{\alpha\in\mathfrak{a}\ \big|\ \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\beta)=0\big\}$$

for some $\beta\in K$ determined by the condition $(\beta)=\delta_K^{-1}\mathfrak{a}^{-1}\mathfrak{b}$. Hence M and M' differ by at most a unit factor and thus are equivalent.

To prove that Ψ_{d-1} is surjective, take any $\mathfrak{b}\in I_{K,1}$. We can always extend $\beta_d=1$ to a $\mathbb{Z}$-basis $\beta_1,\dots,\beta_{d-1},\beta_d$ for $\mathfrak{b}^{-1}$. Let $\{\alpha_i\}_{1\leqslant i\leqslant d}$ denote the corresponding dual basis of $\{\beta_j\}_{1\leqslant j\leqslant d}$, i.e., $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\beta_j)=\delta_{ij}$, $\forall i,j$. Thus $\alpha_1,\dots,\alpha_d$ form a basis for $\mathfrak{a}=\delta_K^{-1}\mathfrak{b}$. Let M denote the $\mathbb{Z}$-module generated by $\alpha_1,\dots,\alpha_{d-1}$, and $\mathfrak{c}$ the integral ideal satisfying $(\alpha_1,\dots,\alpha_{d-1})=\mathfrak{ac}$. Note that M is pure and

$$\alpha_1,\dots,\alpha_{d-1},(\mathbf{N}\mathfrak{c})\alpha_d$$

is a $\mathbb{Z}$-basis for $\mathfrak{ac}$. Thus

$$\beta_1,\dots,\beta_{d-1},(\mathbf{N}\mathfrak{c})^{-1}\beta_d$$

forms a basis for $(\mathfrak{ac})^\vee=(\mathfrak{bc})^{-1}$. In particular, $(\mathbf{N}\mathfrak{c})^{-1}\in(\mathfrak{bc})^{-1}$, or $\mathbf{N}\mathfrak{c}\mid\mathfrak{bc}$. If $\mathfrak{c}$ is divisible by any prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$, we would have

$$\mathfrak{P}^{-1}\mathbf{N}\mathfrak{P}\mid\mathfrak{b},$$

contradicting our assumption that $\operatorname{width}(\mathfrak{b})<d-1$. Thus $\mathfrak{c}=\mathcal{O}_K$ and $\Psi_{d-1}([M])=\mathfrak{b}$. □

Corollary 4.5. *For $\mathfrak{b}\in I_{K,1}$, let $M_\mathfrak{b}=\delta_K^{-1}\mathfrak{b}\cap V_0$. Then $\mathcal{O}_KM_\mathfrak{b}=\delta_K^{-1}\mathfrak{b}$ and $\Psi_{d-1}([M_\mathfrak{b}])=\mathfrak{b}$.*

5. Applications to orders

Lemma 4.4 clearly has an interest of its own. We give some applications below.

For each $\mathbb{Q}$-subspace V of K, we let $I(V)$ denote the set of fractional ideals of $\mathcal{O}_K$ generated by subsets of V. Note that a fractional ideal $\mathfrak{a}$ belongs to $I(V)$ if and only if $\mathcal{O}_K(\mathfrak{a}\cap V)=\mathfrak{a}$.

Lemma 5.1. *With the notation above, we have*:

(1) *If U is a subspace of V, then $I(U)\subseteq I(V)$;*
(2) *For $0\neq\beta\in K$, $\beta I(V)=I(\beta V)$;*
(3) *If $\mathfrak{a}_1,\mathfrak{a}_2\in I(V)$, then $\mathfrak{a}_1+\mathfrak{a}_2\in I(V)$;*
(4) *If $\mathfrak{a}$ is a fractional ideal, then $M=\mathfrak{a}\cap V$ is a pure module and $\mathfrak{b}=\mathcal{O}_K M$ is the largest fractional ideal of $I(V)$ contained in $\mathfrak{a}$. Moreover, the integral ideal $\mathfrak{a}^{-1}\mathfrak{b}$ has width $\leqslant d-\dim V$.*

Proof. (1), (2) and (3) are clear. (4) Note that $M\subseteq\mathfrak{b}\cap V\subseteq\mathfrak{a}\cap V=M$, so $M=\mathfrak{b}\cap V$ is pure. If $\mathfrak{b}'\in I(V)$ is contained in $\mathfrak{a}$, then $M\subseteq(\mathfrak{b}+\mathfrak{b}')\cap V\subseteq\mathfrak{a}\cap V=M$. By (3), $\mathfrak{b}+\mathfrak{b}'\in I(V)$, so $\mathfrak{b}+\mathfrak{b}'=\mathcal{O}_K M=\mathfrak{b}$. Thus $\mathfrak{b}'\subseteq\mathfrak{b}$.

For the last statement, observe that as finite abelian groups, $\mathcal{O}_K/(\mathfrak{a}^{-1}\mathfrak{b})\cong\mathfrak{a}/\mathfrak{b}$. The group $\mathfrak{a}/\mathfrak{b}$ can clearly be written as a product of at most $d-\dim V$ cyclic groups. □

In the case $\dim V=d-1$, $I(V)$ has a particularly simple form. For the rest of the sequel, we write

$$I_{K,1}^{*}=\left\{\gamma\mathfrak{b}\;\middle|\;\gamma\in\mathbb{Q}^{*},\ \mathfrak{b}\in I_{K,1}\right\}. \tag{12}$$

Theorem 5.2. *For any $\beta\in K^{*}$, we have $I(\beta V_0)=\beta\delta_K^{-1}I_{K,1}^{*}$.*

Proof. It is enough to prove the case $\beta=1$. By Corollary 4.5, $I(V_0)\supseteq\delta_K^{-1}I_{K,1}^{*}$. Conversely, given $\mathfrak{a}\in I(V_0)$, let $\mathfrak{b}\in I_{K,1}$ be the complementary ideal associated with $M=\mathfrak{a}\cap V_0$. Then $\mathfrak{a}=\gamma\mathfrak{b}\delta_K^{-1}$ for some $\gamma\in\mathbb{Q}^{*}$. Thus $I(V_0)\subseteq\delta_K^{-1}I_{K,1}^{*}$. □

For the rest of the section we will apply Theorem 5.2 to study orders of a number field. We adopt the following convention. If $\alpha_1,\dots,\alpha_m$ are elements of K, we write

$$\{\alpha_1,\dots,\alpha_m\}_{\mathbb{Z}}$$

for the $\mathbb{Z}$-module generated by $\alpha_1,\dots,\alpha_m$. If $M,N\in\mathbb{M}_d$, we let

$$(M:N)=\{\alpha\in K\mid\alpha N\subseteq M\}.$$

Our treatment of orders is based on the following simple observation.

Lemma 5.3. *Let $M,N\in\mathbb{M}_d$, then $(M:N)=(M^{\vee}N)^{\vee}$.*

Proof. Note that for $\alpha\in K$, $\alpha N\subseteq M$ if and only if $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha NM^{\vee})\subseteq\mathbb{Z}$, or equivalently, $\alpha\in(M^{\vee}N)^{\vee}$. □

We next summarize some basic definitions on orders of number fields. For a classical treatment on this subject, see [16,17,4].

Let K be a number field of degree d and $\mathbb{M}_n$ the set of free $\mathbb{Z}$-submodules of K of rank n. We call a subring $\mathcal{O}$ of K containing 1 an order if $\mathcal{O}\in\mathbb{M}_d$. For example, $(M:M)$ is an order of K whenever $M\in\mathbb{M}_d$. All orders of K are contained in the maximal order $\mathcal{O}_K$ and thus have a finite index in $\mathcal{O}_K$.

Let $\mathcal{O}$ be an order of K and $\mathfrak{a} \in \mathbb{M}_d$. We call $\mathfrak{a}$ a (fractional) $\mathcal{O}$-ideal if $\mathcal{O}\mathfrak{a} \subseteq \mathfrak{a}$, or equivalently, $\mathcal{O} \subseteq (\mathfrak{a} : \mathfrak{a})$. When $\mathcal{O} = (\mathfrak{a} : \mathfrak{a})$, we say that $\mathfrak{a}$ is $\mathcal{O}$-proper. Moreover, we say that a fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is $\mathcal{O}$-invertible if $\mathfrak{a}(\mathcal{O} : \mathfrak{a}) = \mathcal{O}$. An invertible $\mathcal{O}$-ideal is always $\mathcal{O}$-proper. But the converse is not true in general.

Lemma 5.4. *Let $\mathcal{O}$ be an order of K and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then*:

(1) *$\mathfrak{a}$ is $\mathcal{O}$-proper if and only if $\mathfrak{a}^\vee\mathfrak{a} = \mathcal{O}^\vee$;*
(2) *$\mathfrak{a}\mathcal{O}^\vee$ is $\mathcal{O}$-proper if and only if $\mathfrak{a}$ is $\mathcal{O}$-invertible*;
(3) *For non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}$, we have $(\mathcal{O} : (\mathcal{O} : \mathfrak{p})) = \mathfrak{p}$.*
In particular, $\mathfrak{p}$ is $\mathcal{O}$-proper if and only if $\mathfrak{p}$ is $\mathcal{O}$-invertible.

Proof. (1) follows directly from Lemma 5.3. (2) By (1), $\mathcal{O}^\vee$ is always $\mathcal{O}$-proper, thus $\mathfrak{a}\mathcal{O}^\vee$ is $\mathcal{O}$-proper for any $\mathcal{O}$-invertible ideal $\mathfrak{a}$. Conversely, suppose that $\mathfrak{a}\mathcal{O}^\vee$ is $\mathcal{O}$-proper, then $\mathfrak{a}\mathcal{O}^\vee(\mathfrak{a}\mathcal{O}^\vee)^\vee = O^\vee$, thus $\mathfrak{a}(\mathfrak{a}\mathcal{O}^\vee)^\vee\mathcal{O}_K = \mathcal{O}_K$. Since $\mathfrak{a}(\mathfrak{a}\mathcal{O}^\vee)^\vee = \mathfrak{a}(\mathcal{O} : \mathfrak{a}) \subseteq \mathcal{O}$, we have $\mathfrak{a}(\mathfrak{a}\mathcal{O}^\vee)^\vee = \mathcal{O}$ by Nakayama's lemma. (3) Since $\mathfrak{p}(\mathcal{O} : \mathfrak{p}) \subseteq \mathcal{O}$ and $1 \in (\mathcal{O} : \mathfrak{p})$, we have

$$\mathfrak{p} \subseteq \big(\mathcal{O} : (\mathcal{O} : \mathfrak{p})\big) \subseteq \mathcal{O}.$$

If $(\mathcal{O} : (\mathcal{O} : \mathfrak{p})) = \mathcal{O}$, then $\mathcal{O}^\vee(\mathcal{O} : \mathfrak{p}) = \mathcal{O}^\vee$, so we have $\mathcal{O} \subseteq (\mathcal{O} : \mathfrak{p}) \subseteq (\mathcal{O}^\vee : \mathcal{O}^\vee) = \mathcal{O}$. Thus $(\mathcal{O} : \mathfrak{p}) = \mathcal{O}$, or $\mathcal{O}^\vee\mathfrak{p} = \mathcal{O}^\vee$, which is impossible by Nakayama's lemma. Hence $\mathfrak{p} = (\mathcal{O} : (\mathcal{O} : \mathfrak{p}))$. For the second statement, suppose $\mathfrak{p}$ is $\mathcal{O}$-proper but not $\mathcal{O}$-invertible. Then, by (2), $\mathcal{O}^\vee\mathfrak{p}$ and so $(\mathcal{O} : \mathfrak{p})$ cannot be $\mathcal{O}$-proper. This contradicts our assumption that $\mathfrak{p} = (\mathcal{O} : (\mathcal{O} : \mathfrak{p}))$ is $\mathcal{O}$-proper. □

Remark 5.5. It is a basic fact in algebraic number theory that ideals in a maximal order factor uniquely into prime ideals. Lemma 5.4 (2) can be used to give a simple proof of this theorem.

We call an order $\mathcal{O}$ of K Gorenstein if $\mathcal{O}^\vee$ is $\mathcal{O}$-invertible. By Lemma 5.4, Gorenstein orders $\mathcal{O}$ of K are characterized by the property that all proper $\mathcal{O}$-ideals are $\mathcal{O}$-invertible.

Let $\mathcal{O}$ be an order of K and $\mathfrak{f} = (\mathcal{O} : \mathcal{O}_K)$. Note that $\mathfrak{f}$ is the largest integral ideal of $\mathcal{O}_K$ contained in $\mathcal{O}$. It is called the conductor of $\mathcal{O}$. The conductor ideal is the most important invariant of an order. It measures the extent of failure of unique factorization for $\mathcal{O}$-ideals. For example, a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ is $\mathcal{O}$-invertible if and only if $\mathfrak{p} \not\supseteq \mathfrak{f}$ (cf. [17, p. 84]). For, if $\mathfrak{p} \supseteq \mathfrak{f}$ is $\mathcal{O}$-invertible, then $\mathcal{O} = \mathfrak{p}^{-1}\mathfrak{p} \supseteq \mathfrak{p}^{-1}\mathfrak{f} \supsetneq \mathfrak{f}$, contradicting the maximality of $\mathfrak{f}$. Conversely, by a lemma of Dedekind [16, Lemma 1.4], every ideal of $\mathcal{O}$ coprime to $\mathfrak{f}$ is $\mathcal{O}$-invertible.

On the quantitative side of the conductor, we have:

Theorem 5.6. *Let $\mathcal{O}$ be an order of K with conductor $\mathfrak{f}$. Then $[\mathcal{O} : \mathfrak{f}]$ divides $[\mathcal{O}_K : \mathcal{O}]$ and the two invariants are equal if and only if $\mathcal{O}$ is Gorenstein.*

This important result is a direct consequence of [7] (see [18, Theorem 11.8]). The analogous result of Theorem 5.6 in the context of one-dimensional Cohen–Macaulay ring is well known [11, p. 29]. For the convenience of the reader, we sketch a proof at the end of the section.

As we shall see, the $\mathbb{Z}$-module $\mathcal{O}^\vee \cap V_0 \in \mathbb{M}_{d-1}$ also plays an important role in the arithmetic of an order. We call $\mathcal{O}^\vee \cap V_0$ the incomplete canonical module of $\mathcal{O}$.

Lemma 5.7. *Let $\mathcal{O}$ be an order of K with conductor $\mathfrak{f}$ and incomplete canonical module M. Then*

$$(1)\quad \mathcal{O}M = \mathcal{O}^\vee; \qquad (2)\quad \mathfrak{f} = (\mathcal{O}_K M)^\vee.$$

Proof. (1) Clearly $M \subseteq \mathcal{O}M \cap V_0 \subseteq \mathcal{O}^\vee \cap V_0 = M$, so $M = \mathcal{O}M \cap V_0$. Let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_d$ be a $\mathbb{Z}$-basis for $\mathcal{O}$ and $\beta_1, \beta_2, \ldots, \beta_d$ its dual basis. Put $m = [\mathcal{O}^\vee : \mathcal{O}M]$. Then $m\beta_1, \beta_2, \ldots, \beta_d$ form a

$\mathbb{Z}$-basis for $\mathcal{O}M$. Thus $m^{-1}, \alpha_2, \ldots, \alpha_d$ is a $\mathbb{Z}$-basis for $(\mathcal{O}M)^\vee$. Since $\mathcal{O}\cdot 1 \subseteq m(\mathcal{O}M)^\vee \subseteq \mathcal{O}$, we have $m = 1$ and $\mathcal{O}M = \mathcal{O}^\vee$. (2) By Lemma 5.3, $\mathfrak{f} = (\mathcal{O} : \mathcal{O}_K) = (\mathcal{O}^\vee \mathcal{O}_K)^\vee = (\mathcal{O}_K M)^\vee$. □

Theorem 5.8. *An integral ideal $\mathfrak{f}$ of $\mathcal{O}_K$ is the conductor of an order of K if and only if $\mathfrak{f} \in I_{K,1}^\dagger$. Here we put*

$$I_{K,1}^\dagger = \left\{ m\mathfrak{b}^{-1} \;\middle|\; \mathfrak{b} \in I_{K,1} \text{ and } m \in \mathbb{Z} \cap \mathfrak{b},\ m \neq 0 \right\}.$$

Proof. If $\mathfrak{f}$ is the conductor of an order $\mathcal{O}$ with incomplete canonical module M, then $\mathfrak{f}^\vee = \mathcal{O}_K M \in I(V_0)$. By Theorem 5.2, $\mathfrak{f}^\vee = m^{-1}\delta_K^{-1}\mathfrak{b}$ for some $\mathfrak{b} \in I_{K,1}$ and $0 \neq m \in \mathbb{Q}$. Thus $\mathfrak{f} = m\mathfrak{b}^{-1}$ and so m is an integer contained in $\mathfrak{b}$. Hence $\mathfrak{f} \in I_{K,1}^\dagger$. Conversely, given $\mathfrak{f} \in I_{K,1}^\dagger$, thus $\mathfrak{f}^\vee \in I(V_0)$, it is easy to check that

$$\mathbb{Z} + \mathfrak{f} = \{a + \alpha \mid a \in \mathbb{Z},\ \alpha \in \mathfrak{f}\}$$

is an order of K having incomplete canonical module $M = \mathfrak{f}^\vee \cap V_0$ and conductor $(\mathcal{O}_K M)^\vee = \mathfrak{f}$. □

We call an order $\mathcal{O}$ pure if $\mathcal{O} = \mathbb{Z} + \mathfrak{c}$ for some integral ideal $\mathfrak{c}$ of $\mathcal{O}_K$. In this case we can always replace $\mathfrak{c}$ by the conductor $\mathfrak{f}$ of $\mathcal{O}$ and write $\mathcal{O} = \mathbb{Z} + \mathfrak{f}$. Note that the conductor $\mathfrak{f}$ is the unique smallest ideal in $I_{K,1}^\dagger$ containing $\mathfrak{c}$. By Theorem 5.6, a pure order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}$ is Gorenstein if and only if $\mathbf{N}\mathfrak{f} = m^2$, where m denotes the smallest positive integer contained in the conductor $\mathfrak{f}$. Writing out explicitly, we have the factorization

$$\mathfrak{f} = \prod_p \mathfrak{f}_p,$$

where $\mathfrak{f}_p$ are integral ideals of the following three types

(1) $\mathfrak{f}_p = (\mathfrak{P}_1\mathfrak{P}_2)^k$, where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are distinct prime ideals of $\mathcal{O}_K$ of norm p (with ramification index $e(\mathfrak{P}_1 \mid p) = e(\mathfrak{P}_2 \mid p) = 1$ if $k > 1$);
(2) $\mathfrak{f}_p = \mathfrak{P}^{2k}$, where $\mathfrak{P}$ is a prime of $\mathcal{O}_K$ of norm p and $e(\mathfrak{P} \mid p) > 1$ (in the case $k > 1$ we require that $e(\mathfrak{P} \mid p) = 2$);
(3) $\mathfrak{f}_p = \mathfrak{P}^k$, where $\mathfrak{P}$ is a prime of $\mathcal{O}_K$ of norm p^2 (with $e(\mathfrak{P} \mid p) = 1$ if $k > 1$).

We call an order $\mathcal{O}$ Bass if every order $\mathcal{O}'$ with $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$ is Gorenstein. It is easy to see that pure Gorenstein orders are Bass orders.

An order $\mathcal{O}$ is called primitive if $\mathcal{O} \neq \mathbb{Z} + m\mathcal{O}'$ for any integer $m > 1$ and any order $\mathcal{O}'$. For example, a pure order $\mathcal{O} = \mathbb{Z} + \mathfrak{f}$ is primitive when its conductor $\mathfrak{f}$ is a primitive integral ideal of $\mathcal{O}_K$, i.e., $m\mathcal{O}_K \nmid \mathfrak{f}$ for any integer $m > 1$. Every order $\mathcal{O}$ of K can be written uniquely as $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_1$, where $\mathcal{O}_1$ is a primitive order and m is a positive integer called the content of $\mathcal{O}$. In fact, we have the following correspondence.

Theorem 5.9. *The mapping $\psi : \mathcal{O} \mapsto [\mathcal{O}^\vee \cap V_0]$ is a surjection from the set of orders of K onto $\mathbb{M}_{d-1}^{\sim}$. Moreover, for each class $[M] \in \mathbb{M}_{d-1}^{\sim}$, there is a unique primitive order $\mathcal{O}_1$ such that $\psi(\mathcal{O}_1) = [M]$. All orders in the fiber $\psi^{-1}([M])$ have the form $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_1$ for some positive integer m.*

Proof. We first fix in each class $[M] \in \mathbb{M}_{d-1}^{\sim}$ a unique representative $M \subset V_0$ such that $(\mathcal{O}_K M)^\vee$ is a primitive integral ideal of $\mathcal{O}_K$. We may choose basis for M and $\mathcal{O}_K M$ so that

$$M = \{\beta_1, \beta_2, \ldots, \beta_{d-1}\}_{\mathbb{Z}} \subset \mathcal{O}_K M = \left\{\beta_0, c_1^{-1}\beta_1, c_2^{-1}\beta_2, \ldots, c_{d-1}^{-1}\beta_{d-1}\right\}_{\mathbb{Z}}.$$

Here $c_1, c_2, \ldots, c_{d-1}$ are positive integers satisfying $c_i \mid c_{i-1}$ for $1 < i \leqslant d-1$. Let $\alpha_0 = c_0, \alpha_1, \ldots, \alpha_{d-1}$ be the dual basis of $\beta_0, \beta_1, \ldots, \beta_{d-1}$. Note that c_0 is an integer in $(\mathcal{O}_K M)^\vee$.

Now let c_{ij}^k denote the rational numbers such that

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{d-1} c_{ij}^k \alpha_k, \quad \forall 1 \leqslant i, j \leqslant d-1.$$

Let ρ be the smallest positive integer such that

$$c_{ij}^0 \rho^2 \quad \text{and} \quad c_{ij}^k \rho \in \mathbb{Z}, \quad \forall 1 \leqslant i, j, k \leqslant d-1.$$

Then

$$\mathcal{O}_1 = \{1, \rho\alpha_1, \ldots, \rho\alpha_{d-1}\}_{\mathbb{Z}}$$

is an order of K with $\psi(\mathcal{O}_1) = [M]$.

Next suppose there exists an order $\mathcal{O}$ of K such that $\psi(\mathcal{O}) = [M]$, that is, $\mathcal{O}^\vee \cap V_0 = c^{-1}M$ for some $c \in \mathbb{Q}$, $c > 0$. By Lemma 5.7, $\mathcal{O}$ has conductor $c(\mathcal{O}_K M)^\vee$. So c is a positive integer. Moreover, we may write

$$\mathcal{O}^\vee = \mathbb{Z}\beta \oplus c^{-1}M,$$

for some $\beta \in c^{-1}\mathcal{O}M \subseteq c^{-1}\mathcal{O}_K M$ with $\mathrm{Tr}_{K/\mathbb{Q}}(\beta) = 1$. Thus

$$\beta = c_0\beta_0 + c^{-1}\beta',$$

where $\beta' \in \mathcal{O}_K M \cap V_0$. On the other hand, we have $c_0\mathcal{O} \subseteq (\mathcal{O}_K M)^\vee$, so $c_0\mathcal{O}_K M \subseteq \mathcal{O}^\vee$. In particular, $c_0\beta_0 = \beta - c^{-1}\beta' \in \mathcal{O}^\vee$, or $\beta' \in M$. Thus we may choose at the beginning that $\beta = c_0\beta_0$ and write

$$\mathcal{O} = \left(\mathbb{Z}c_0\beta_0 \oplus c^{-1}M\right)^\vee = \{1, c\alpha_1, \ldots, c\alpha_{d-1}\}_{\mathbb{Z}}.$$

By our choice of ρ, we have $c = m\rho$ and $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_1$ for some positive integer m. This also implies that $\mathcal{O}_1$ is a primitive order. □

Remark 5.10. In the above proof ρ is a positive integer dividing c_1^2 such that $c_1 \mid c_0\rho$. Moreover, by Theorem 5.6, we have

$$(c_0 c_1 \cdots c_{d-1})^2 \mid \left[\mathcal{O}_K : (\mathcal{O}_K M)^\vee\right]\rho^{d-2}$$

with equality holding if and only if $\mathcal{O}_1$ is Gorenstein. In the case where K is a cubic field, we have $\rho = c_1^2$ (see Theorem 5.13).

It is easy to see that the restriction of ψ induces a bijection between the set of primitive pure orders of K and the set of pure module classes in $\mathbb{M}_{d-1}^{\sim}$.

Given an order $\mathcal{O}$ of a number field K, there are several interesting invariants we can consider. For example, the index $[\mathcal{O}_K : \mathcal{O}]$, the norm of the conductor $[\mathcal{O}_K : \mathfrak{f}]$ (or simply $[\mathcal{O} : \mathfrak{f}]$), and the module index of the incomplete canonical module.

Lemma 5.11. *Let $\mathcal{O}$ be an order of K with conductor $\mathfrak{f}$ and incomplete canonical module M. Then*

$$\operatorname{ind} M = \frac{[\mathcal{O} : \mathfrak{f}]^{d-1}}{[\mathcal{O}_K : \mathcal{O}]}.$$

Moreover, $\operatorname{ind} M$ *is a factor of* $[\mathcal{O}_K : \mathcal{O}]^{d-2}$ *and the two invariants are equal if and only if* $\mathcal{O}$ *is Gorenstein.*

Proof. We may write $\mathcal{O}_K M = (m\delta_K)^{-1}\mathfrak{b}$ with $\mathfrak{b} \in I_{K,1}$ and $m \in \mathfrak{b} \cap \mathbb{Z}$ so that $\mathfrak{f} = m\mathfrak{b}^{-1}$. Note that the pure module $M' = \mathcal{O}_K M \cap V_0$ has complementary ideal $\mathfrak{b}$ and $[\mathcal{O} : \mathfrak{f}] = [\mathcal{O}_K M : \mathcal{O}^\vee] = m[M' : M]$. Thus we have

$$\operatorname{ind} M = \big[M' : M\big]^d \operatorname{ind} M' = m^{-d}[\mathcal{O} : \mathfrak{f}]^d \mathbf{N}\mathfrak{b} = \frac{[\mathcal{O} : \mathfrak{f}]^d}{[\mathcal{O}_K : \mathfrak{f}]}.$$

The rest of the lemma follows from Theorem 5.6 and the observation that

$$\operatorname{ind} M = [\mathcal{O}_K : \mathcal{O}]^{d-2}\left(\frac{[\mathcal{O} : \mathfrak{f}]}{[\mathcal{O}_K : \mathcal{O}]}\right)^{d-1}. \qquad \square$$

Besides the pure orders, we examine another class of widely used orders. Let θ be a generator of K and put $N = \mathbb{Z}1 + \mathbb{Z}\theta \in \mathbb{M}_2$. Then $N^{d-1} = \{1, \theta, \ldots, \theta^{d-1}\}_{\mathbb{Z}} \in \mathbb{M}_d$. We compute explicitly a basis for the order

$$\mathcal{O} = \big(N^{d-1} : N^{d-1}\big) = \big(\big(N^{d-1}\big)^\vee N^{d-1}\big)^\vee.$$

By [13, §3.1], the dual basis of $1, \theta, \ldots, \theta^{d-1}$ is given by

$$\frac{\beta_{d-1}}{f'(\theta)}, \ldots, \frac{\beta_0}{f'(\theta)},$$

where

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{Z}[x]$$

is a primitive polynomial such that $f(\theta) = 0$, and

$$\beta_i = a_0\theta^i + a_1\theta^{i-1} + \cdots + a_i, \quad 0 \leqslant i \leqslant d. \tag{13}$$

Since $\theta\beta_{i-1} = \beta_i - a_i$ for $1 \leqslant i \leqslant d$, we have

$$\begin{aligned}\big(N^{d-1}\big)^\vee N &= \frac{1}{f'(\theta)}\{\beta_0, \beta_1, \ldots, \beta_{d-1}, \theta\beta_0, \ldots, \theta\beta_{d-1}\}_{\mathbb{Z}} \\ &= \frac{1}{f'(\theta)}\{\beta_0 = a_0, a_1, \ldots, a_d, \beta_1, \ldots, \beta_{d-1}\}_{\mathbb{Z}} \\ &= \frac{1}{f'(\theta)}\{1, \beta_1, \ldots, \beta_{d-1}\}_{\mathbb{Z}}. \end{aligned} \tag{14}$$

In general we can prove by induction that for $1 \leqslant k \leqslant d$,

$$\big(N^{d-1}\big)^\vee N^k = \frac{1}{f'(\theta)}\big\{1, \theta, \ldots, \theta^{k-1}, \beta_k, \ldots, \beta_{d-1}\big\}_{\mathbb{Z}}.$$

In particular,

$$\mathcal{O}^\vee = \left(N^{d-1}\right)^\vee N^{d-1} = \frac{1}{f'(\theta)}\left\{1, \theta, \ldots, \theta^{d-2}, a_0\theta^{d-1}\right\}_{\mathbb{Z}} \tag{15}$$

and so

$$\mathcal{O} = \{1, \beta_1, \beta_2, \ldots, \beta_{d-1}\}_{\mathbb{Z}}. \tag{16}$$

This is the order used by [14,3,1] and many other authors. Note that $\mathcal{O}$ depends only on the module class $[N]$ of N and has incomplete canonical module

$$\mathcal{O}^\vee \cap V_0 = \frac{1}{f'(\theta)}\left\{1, \theta, \ldots, \theta^{d-2}\right\}_{\mathbb{Z}}$$

and conductor

$$\mathfrak{f} = f'(\theta)\delta_K^{-1}(\mathcal{O}_K N)^{-(d-2)}. \tag{17}$$

In the case that f is not primitive, say $f = mf_1$ where f_1 is a primitive polynomial and $m > 1$ is an integer, one can still use (16) and (13) to define an order, namely, $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_1$ with $\mathcal{O}_1$ the order defined by f_1.

Theorem 5.12. *Let $f(x)$ be an integral polynomial of degree $d > 2$ with a root θ that generates K, and let $\mathcal{O}$ be the order of f given by* (16) *and* (13)*. Let $\mathfrak{a}$ denote the $\mathcal{O}$-ideal generated by* 1 *and θ. Then*

$$\mathfrak{a}^k = \left\{1, \theta, \ldots, \theta^k, \beta_{k+1}, \ldots, \beta_{d-1}\right\}_{\mathbb{Z}}, \quad 0 \leqslant k \leqslant d-1,$$

and $\mathcal{O}^\vee = \mathfrak{a}^{d-2}/f'(\theta)$. Furthermore, the following three conditions are equivalent:

(1) *f is primitive*; (2) *$\mathcal{O}$ is Gorenstein*; (3) *$\mathcal{O}$ is primitive*.

Proof. We need only to prove the equivalence of the last three conditions. The rest can be argued as above. (1) $\Rightarrow$ (2) If f is primitive, then $\mathfrak{a}$ is $\mathcal{O}$-invertible with inverse

$$\mathfrak{a}^{-1} = \{\beta_0, \beta_1, \ldots, \beta_{d-1}\}_{\mathbb{Z}}.$$

Thus $\mathcal{O}$ is Gorenstein as $\mathcal{O}^\vee = \mathfrak{a}^{d-2}/f'(\theta)$ is $\mathcal{O}$-invertible. (2) $\Rightarrow$ (3) By an observation of Bhargava [2, §3.6], any Gorenstein order of rank greater than 2 must be primitive. This is also an easy consequence of Theorem 5.6. (3) $\Rightarrow$ (1) This follows directly from above. □

The restriction of the map ψ in Theorem 5.9 gives a bijection between the set of orders of primitive polynomials f and the set of module classes of the form $[N^{d-2}]$ with $N \in \mathbb{M}_2$.

We now restrict our attention to the case where K is a cubic field. Let $\mathcal{O}$ be an arbitrary primitive order of K. Suppose the incomplete canonical module of $\mathcal{O}$ is equivalent to $N = \mathbb{Z}1 + \mathbb{Z}\theta$ for some $\theta \in K$. Then, by Theorem 5.12,

$$\mathcal{O}^\vee \cap V_0 = N/f'(\theta),$$

where $f(x) = a_0x^3 + a_1x^2 + a_2x + a_3 \in \mathbb{Z}[x]$ is the primitive minimal polynomial of θ. Thus

$$\mathcal{O} = \left(N^2 : N^2\right) = \left\{1, a_0\theta, a_0\theta^2 + a_1\theta\right\}. \tag{18}$$

We associate to $\mathcal{O}$ a system of pure orders. Let u_0 be the smallest positive integer in the conductor $\mathfrak{f}$ of $\mathcal{O}$. Choose a $\mathbb{Z}$-basis γ_0, γ_1, γ_2 for $\mathcal{O}_K N$ so that

$$\begin{pmatrix} a_0\theta^2 \\ \theta \\ 1 \end{pmatrix} = \begin{pmatrix} u_0 & v_0 & v_1 \\ 0 & u_1 & v_2 \\ 0 & 0 & u_2 \end{pmatrix} \begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \end{pmatrix}.$$

Here $u_1, u_2, v_0, v_1, v_2 \in \mathbb{Z}$ and $u_1, u_2 \geqslant 1$. Then by (17),

$$\mathfrak{f} = f'(\theta)(\delta_K N)^{-1} = \{u_0, u_1\beta_1 + v_0, u_2\beta_2 + v_2\beta_1 + v_1\}_{\mathbb{Z}}$$

with $\beta_1 = a_0\theta + a_1$ and $\beta_2 = a_0\theta^2 + a_1\theta + a_2$. Let N' denote the pure module $\mathcal{O}_K N \cap \mathbb{Q}N = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$. Then $\mathcal{O}_0 = (N'^2 : N'^2)$ is a primitive pure order. Put $\alpha = \gamma_1/\gamma_2 = (u_2\theta - v_2)/u_1$. Then $(1, \alpha) = u_2(\gamma_1, \gamma_2) = u_2(1, \theta)$. By Gauss's lemma [10, Theorem 87], α has primitive minimal polynomial

$$g(x) = \frac{\mathrm{N}_{K/\mathbb{Q}}(x - \alpha)}{\mathbf{N}(1, \alpha)} = \frac{|a_0|}{u_2^3}x^3 + \cdots.$$

Thus $\mathcal{O}_0$ has conductor

$$g'(\alpha)\big(\delta_K(1, \alpha)\big)^{-1} = \frac{f'(\theta)}{u_1^2 u_2}\big(\delta_K u_2(1, \theta)\big)^{-1} = \frac{\mathfrak{f}}{c^2}.$$

Here $c = [N' : N] = u_1u_2$. Moreover, note that $cN' \subseteq N$ and $u_0\mathcal{O} \subseteq \mathfrak{f}$, so we have

$$\{u_0\gamma_0, c\gamma_1, c\gamma_2\}_{\mathbb{Z}} \subseteq \big\{a_0\theta^2, \theta, 1\big\}_{\mathbb{Z}} = f'(\theta)\mathcal{O}^{\vee}.$$

Hence $\mathcal{O} \subseteq \mathcal{O}_1 = \mathbb{Z} + c^{-1}\mathfrak{f}$. It can be shown that $\mathcal{O}_1$ is the smallest pure order containing $\mathcal{O}$.

Theorem 5.13. *Let $\mathcal{O}$ be a primitive order of a cubic field K with conductor $\mathfrak{f}$ and incomplete canonical module M. Put*

$$M' = \mathcal{O}_K M \cap \mathbb{Q}M \quad \textit{and} \quad c = \big[M' : M\big].$$

Then $c^{-2}\mathfrak{f}$ is a primitive integral ideal in $I_{K,1}^{\dagger}$ and

$$\mathbb{Z} + \mathfrak{f} \subseteq \mathcal{O} \subseteq \mathcal{O}_1 = \mathbb{Z} + \frac{\mathfrak{f}}{c} \subseteq \mathcal{O}_0 = \mathbb{Z} + \frac{\mathfrak{f}}{c^2} \subseteq \mathcal{O}_K. \tag{19}$$

Corollary 5.14. *Each primitive order of a cubic field K has conductor of the form $c^2c_0\mathfrak{b}^{-1}$, where $\mathfrak{b} \in I_{K,1}$, c_0 is the smallest positive integer in $\mathfrak{b}$, and c is any positive integer. Moreover, the number of primitive cubic orders of conductor $\mathfrak{f} = c^2c_0\mathfrak{b}^{-1}$ is given by*

$$a(\mathfrak{f}) = c\prod_{p|c}\lambda_p, \tag{20}$$

where

$$\lambda_p = \begin{cases} 1 - \frac{t_p - 1}{p}, & \text{if } p \nmid c_0; \\ 1 - \frac{1}{p}, & \text{if } p \mid c_0 \text{ and } \mathfrak{b} + p\mathcal{O}_K \text{ is a prime unramified over } p; \\ 1, & \text{otherwise}. \end{cases}$$

Here t_p denotes the number of prime ideals $\mathfrak{P}$ with $\mathbf{N}\mathfrak{P} = p$.

Proof. We need only to prove (20). Note that $I(V_0) = \delta_K^{-1} I_{K,1}^*$. For $\mathfrak{a} \in I_{K,1}^*$, we write $M_{\mathfrak{a}} = \delta_K^{-1}\mathfrak{a} \cap V_0$. Then, by Theorem 5.13,

$$a(\mathfrak{f}) = \#\big\{M \subseteq M_{\mathfrak{b}} \;\big|\; [M_{\mathfrak{b}} : M] = c,\ \mathcal{O}_K M = \delta_K^{-1}\mathfrak{b}\big\}. \tag{21}$$

Let $M_K = \delta_K^{-1} \cap V_0$. By using the argument at the beginning of Section 6, we may reduce the proof to the case where both M and $M_{\mathfrak{b}}$ are submodules of M_K of prime power indexes. Let p be a rational prime. If a is a non-zero integer, we let $a^{(p)} = p^{v_p(a)}$, where v_p denotes the p-valuation normalized so that $v_p(p) = 1$. Similarly, if $\mathfrak{a}$ is a non-zero integral ideal, we write $\mathfrak{a}^{(p)} = \prod_{\mathfrak{P}|p} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{a})}$ for the p-component of $\mathfrak{a}$. Here $v_{\mathfrak{P}}$ denotes the $\mathfrak{P}$-valuation so that $v_{\mathfrak{P}}(\mathfrak{P}) = 1$. Moreover, if $M \in \mathbb{M}_2$ is a submodule of M_K, we let $M^{(p)}$ denote the unique submodule of M_K containing M such that

$$\big[M_K : M^{(p)}\big] \text{ is a power of } p \text{ and } p \nmid \big[M^{(p)} : M\big].$$

Then $M^{(p)} = M_K$ for all but finitely many p and $[M_K : M] = \prod_p [M_K : M^{(p)}]$. Moreover, we have $(\delta_K M)^{(p)} = \delta_K M^{(p)}$ and $(M_{\mathfrak{a}})^{(p)} = M_{\mathfrak{a}^{(p)}}$, $\forall \mathfrak{a} \in I_{K,1}$. Using the bijection (25), we obtain

$$\begin{aligned} a(\mathfrak{f}) &= \prod_p \#\big\{M \subseteq M_{\mathfrak{b}^{(p)}} \;\big|\; [M_{\mathfrak{b}^{(p)}} : M] = c^{(p)},\ \mathcal{O}_K M = \delta_K^{-1}\mathfrak{b}^{(p)}\big\} \\ &= \prod_p a\big(\mathfrak{f}^{(p)}\big). \end{aligned}$$

In the following we assume that $\mathbf{N}\mathfrak{f} = c^6 c_0^2$ is a power of p. Then we have $\mathfrak{b} = \mathfrak{P}^l$ and $c_0 = p^l$ for some integer $l \geqslant 0$ and prime ideal $\mathfrak{P}$ with $\mathbf{N}\mathfrak{P} = p$. In the case $l > 1$, $\mathfrak{P}$ must also be unramified over p.

If $c = 1$, then clearly $a(\mathfrak{f}) = 1$. So we assume henceforth that $c = p^k$, $k \geqslant 1$. Observe that for each integral ideal $\mathfrak{a} \in I_{K,1}^*$, the number of submodules of $M_{\mathfrak{a}}$ of index $p^m (m \geqslant 0)$ is given by

$$a\big(p^m, \mathfrak{a}\big) = 1 + p + \cdots + p^m.$$

To count the submodules M with $\mathcal{O}_K M = \mathcal{O}_K M_{\mathfrak{a}}$, we apply the inclusion–exclusion principle. We consider three cases.

Case 1: $\mathfrak{b} = \mathcal{O}_K$. Then

$$\begin{aligned} a(\mathfrak{f}) &= a(c, \mathcal{O}_K) - \sum_{\mathbf{N}\mathfrak{P}'=p} a\left(\frac{c}{p}, \mathfrak{P}'\right) + (t_p - 1)a\left(\frac{c}{p^2}, p\mathcal{O}_K\right) \\ &= p^k\left(1 - \frac{t_p - 1}{p}\right). \end{aligned}$$

Case 2: $\mathfrak{b} = \mathfrak{P}^l$ with $l \geqslant 1$ and $\mathfrak{P}$ is unramified over p. Then

$$\begin{aligned} a(\mathfrak{f}) &= a\big(c, \mathfrak{P}^l\big) - a\left(\frac{c}{p}, \mathfrak{P}^{l+1}\right) - a\left(\frac{c}{p}, p\mathfrak{P}^{l-1}\right) + a\left(\frac{c}{p^2}, p\mathfrak{P}^l\right) \\ &= p^k\left(1 - \frac{1}{p}\right). \end{aligned}$$

Case 3: $\mathfrak{b} = \mathfrak{P}$ and $\mathfrak{P}$ is ramified over p. Then

$$a(\mathfrak{f}) = a(c, \mathfrak{P}) - a\left(\frac{c}{p}, p\mathcal{O}_K\right) = p^k.$$

Putting all these cases together, we obtain (20). □

There is another way to construct primitive cubic orders which is easier to generalize in a wider context.

Corollary 5.15. *Let K be a cubic field and $\mathfrak{f}_0$ a primitive integral ideal in $I_{K,1}^{\dagger}$. Let c be any positive integer and $\mathfrak{f} = c^2\mathfrak{f}_0$. Define $\mathcal{O}_0 = \mathbb{Z} + \mathfrak{f}_0$ and $\mathcal{O}_1 = \mathbb{Z} + c\mathfrak{f}_0$ as in Theorem* 5.12. *Let $S(\mathfrak{f})$ denote the set of $\mathcal{O}_1$-proper ideals $\mathfrak{c}$ with $\mathcal{O}_1 \subseteq \mathfrak{c} \subseteq \mathcal{O}_0$ and $[\mathcal{O}_0 : \mathfrak{c}] = c$. Then we have the following bijection*

$$\varphi : S(\mathfrak{f}) \to \{\textit{primitive orders of conductor } \mathfrak{f}\},$$
$$\mathfrak{c} \mapsto \mathcal{O} = \mathbb{Z} + c\mathfrak{c}.$$

The inverse map is given by $\varphi^{-1}(\mathcal{O}) = c^{-1}(\mathcal{O} : \mathcal{O}_1) = \mathcal{O}_0 \cap c^{-1}\mathcal{O}$.

Proof. We first let $\mathcal{O}$ be a primitive cubic order of conductor $\mathfrak{f}$ and write $\mathfrak{c}_1 = (\mathcal{O} : \mathcal{O}_1)$. Then $\mathfrak{c}_1^{\vee} = \mathcal{O}^{\vee}\mathcal{O}_1$, or equivalently, $\mathcal{O}_1^{\vee} = \mathcal{O}^{\vee}\mathfrak{c}_1$, as $\mathcal{O}^{\vee}$ is $\mathcal{O}$-invertible. Thus $\mathfrak{c}_1^{\vee}$ is $\mathcal{O}_1$-invertible and $(\mathcal{O} : \mathfrak{c}_1) = \mathcal{O}_1$. Moreover, from $\mathcal{O}_1^{\vee}\mathcal{O}_K = \mathcal{O}^{\vee}\mathcal{O}_K\mathfrak{c}_1$, or $(c^{-1}\mathfrak{f})^{\vee} = \mathfrak{f}^{\vee}\mathfrak{c}_1$, we deduce that $\mathfrak{c}_1\mathcal{O}_K = (c^{-1}\mathfrak{f})^{-1}\mathfrak{f} = c\mathcal{O}_K$. Thus

$$\mathfrak{c}_1 \subseteq \mathcal{O} \cap c\mathcal{O}_K = \mathcal{O} \cap (\mathcal{O}_1 \cap c\mathcal{O}_K) = \mathcal{O} \cap c\mathcal{O}_0.$$

We claim that $\mathfrak{c}_1 = \mathcal{O} \cap c\mathcal{O}_0$ and $\mathcal{O} = \mathbb{Z} + \mathfrak{c}_1$. Let c_0 denote the smallest positive integer in $\mathfrak{f}_0$. Observe that

$$[\mathfrak{c}_1 : \mathfrak{f}] = \left[\mathcal{O}^{\vee}\mathfrak{c}_1 : \mathcal{O}^{\vee}\mathfrak{f}\right] = \left[\mathcal{O}_1^{\vee} : \mathcal{O}_K^{\vee}\right] = [\mathcal{O}_K : \mathcal{O}_1] = c^2c_0$$

and $[\mathcal{O} : \mathfrak{f}] = (\mathbf{N}\mathfrak{f})^{1/2} = c^3c_0$. So we have $[\mathcal{O} : \mathfrak{c}_1] = c$. On the other hand, $[\mathcal{O} : \mathcal{O} \cap c\mathcal{O}_0] \geqslant c$. This forces $\mathfrak{c}_1 = \mathcal{O} \cap c\mathcal{O}_0$. Similarly, we have $\mathcal{O} = \mathbb{Z} + \mathfrak{c}_1$ as $[\mathbb{Z} + \mathfrak{c}_1 : \mathfrak{c}_1] = c$. Moreover, from $c\mathcal{O}_1 \subseteq \mathfrak{c}_1 \subseteq c\mathcal{O}_0$, we see that $\mathfrak{c}_1 = c\mathfrak{c}$ for some $\mathcal{O}_1$-ideal $\mathfrak{c}$ with $\mathcal{O}_1 \subseteq \mathfrak{c} \subseteq \mathcal{O}_0$ such that $\mathfrak{c}^{\vee}$ is $\mathcal{O}_1$-invertible. By Corollary 5.17, the last condition can be replaced by

$$\mathfrak{c} \text{ is } \mathcal{O}_1\text{-proper} \quad \text{and} \quad [\mathcal{O}_0 : \mathfrak{c}] = c.$$

In this way we associate to each primitive cubic order $\mathcal{O}$ a unique $\mathcal{O}_1$-ideal $\mathfrak{c} = c^{-1}(\mathcal{O} : \mathcal{O}_1) = \mathcal{O}_0 \cap c^{-1}\mathcal{O} \in S(\mathfrak{f})$.

It remains to show that for each $\mathfrak{c} \in S(\mathfrak{f})$, $\mathcal{O} = \mathbb{Z} + c\mathfrak{c}$ is primitive order of conductor $\mathfrak{f}$ and $\mathcal{O} \cap c\mathcal{O}_0 = c\mathfrak{c}$. Let $\mathfrak{c} \in S(\mathfrak{f})$ and $\mathcal{O} = \mathbb{Z} + c\mathfrak{c}$. Notice that

$$\mathcal{O}_0\mathfrak{c}^{\vee} = \mathcal{O}_0\mathfrak{c}\mathfrak{c}^{\vee} = \mathcal{O}_0\mathcal{O}_1^{\vee} = (\mathcal{O}_1 : \mathcal{O}_0)^{\vee} = c^{-1}\mathcal{O}_0^{\vee}.$$

Write $M' = \mathfrak{f}_0^{\vee} \cap V_0$. Then

$$\mathcal{O}_0^{\vee} = \mathbb{Z}\gamma \oplus M' \quad \text{and} \quad \mathcal{O}_1^{\vee} = \mathbb{Z}\gamma \oplus c^{-1}M'$$

for some $\gamma \in \mathcal{O}_0^{\vee} = \mathcal{O}_0M'$. Since $\mathcal{O}_0^{\vee} \subseteq \mathfrak{c}^{\vee} \subseteq \mathcal{O}_1^{\vee}$, we have $\mathfrak{c}^{\vee} = \mathbb{Z}\gamma \oplus M$, where $M = \mathfrak{c}^{\vee} \cap V_0$ is a $\mathbb{Z}$-module such that $M' \subseteq M \subseteq c^{-1}M'$. Then

$$\mathcal{O}_0\mathfrak{c}^{\vee} = \gamma\mathcal{O}_0 + \mathcal{O}_0M \subseteq \mathcal{O}_0M' + \mathcal{O}_0M = \mathcal{O}_0M \subseteq \mathcal{O}_0\mathfrak{c}^{\vee}.$$

So $\mathcal{O}_0 M = \mathcal{O}_0 \mathfrak{c}^\vee = c^{-1}\mathcal{O}_0^\vee$. Hence $\mathcal{O} = \mathbb{Z} + c\mathfrak{c}$ has incomplete canonical module $(c\mathfrak{c})^\vee \cap V_0 = c^{-1}M$ and conductor $(c^{-1}\mathcal{O}_K M)^\vee = c^2(\mathcal{O}_K \mathcal{O}_0^\vee)^\vee = \mathfrak{f}$. It is easy to check that $\mathcal{O}$ is primitive and $\mathcal{O} \cap c\mathcal{O}_0 = c\mathfrak{c}$. □

In the case where K is a cubic field, the restriction of ψ in Theorem 5.9 establishes a bijection ψ_3 between the set of primitive orders of K and $\mathbb{M}_2^\sim$. Observe that the module classes in $\mathbb{M}_2^\sim$ with $\mathrm{GL}(2,\mathbb{Z})$-equivalent norm forms correspond to isomorphic orders of K. Composing ψ_3 with the map

$$\Phi : \mathbb{M}_2^\sim \to \overline{S}_{2,K}/G$$

defined in (7), and extending the bijection trivially to the non-primitive forms and orders, we obtain the classical correspondence of Delone and Faddeev [2,6,8] stated in the introduction. For the parametrization of quartic orders using pairs of ternary quadratic forms, see the celebrated paper [2].

In the rest of this section we outline a proof of Theorem 5.6.

Lemma 5.16. *Let $\mathfrak{o}$ be a one-dimensional Noetherian local domain with field of fraction K. Suppose the integral closure $\tilde{\mathfrak{o}}$ of $\mathfrak{o}$ in K is a finitely generated $\mathfrak{o}$-module. Then for any $\mathfrak{o}$-submodule $\mathfrak{b}$ of $\tilde{\mathfrak{o}}$,*

$$l_{\mathfrak{o}}(\tilde{\mathfrak{o}}/\mathfrak{o}) \geqslant l_{\mathfrak{o}}(\mathfrak{b}\tilde{\mathfrak{o}}/\mathfrak{b}\mathfrak{o})$$

with equality holding if and only if $\mathfrak{b}$ is a principal $\mathfrak{o}$-ideal. Here $l_{\mathfrak{o}}(\mathfrak{a})$ denotes the length of an $\mathfrak{o}$-module, i.e., the maximal length of a strictly decreasing chain

$$\mathfrak{a} = \mathfrak{a}_0 \supsetneqq \mathfrak{a}_1 \supsetneqq \cdots \supsetneqq \mathfrak{a}_l = 0$$

of $\mathfrak{o}$-submodules.

Proof. By [17, §12], $\tilde{\mathfrak{o}}$ is a Dedekind domain with finitely many prime ideals and is thus a principal ideal domain. There exists an $\alpha \in K$ such that $\mathfrak{b}\tilde{\mathfrak{o}} = \alpha\tilde{\mathfrak{o}}$. Since $l_{\mathfrak{o}}(\mathfrak{b}\tilde{\mathfrak{o}}/\mathfrak{b}\mathfrak{o})$ is unchanged if we replace $\mathfrak{b}$ by $\alpha^{-1}\mathfrak{b}$, we may assume in the following that $\mathfrak{b}\tilde{\mathfrak{o}} = \tilde{\mathfrak{o}}$.

Let $\mathfrak{f} = (\mathfrak{o} : \tilde{\mathfrak{o}})$ denote the conductor of $\mathfrak{o}$ in $\tilde{\mathfrak{o}}$. Note that $\mathfrak{b} = \mathfrak{o}\mathfrak{b} \supseteq \mathfrak{f}\tilde{\mathfrak{o}}\mathfrak{b} = \mathfrak{f}$ and $\mathfrak{f} \neq 0$. Write $R = \tilde{\mathfrak{o}}/\mathfrak{f}$, $A = \mathfrak{o}/\mathfrak{f}$ and $B = \mathfrak{b}/\mathfrak{f}$. Then A is a subring of the Artin ring R with unique maximal ideal, B is an A-submodule of R with $RB = R$. We claim that

$$l_A(R/A) \geqslant l_A(R/B) \tag{22}$$

with equality holding if and only if $B = \varepsilon A$ for some unit ε of R. This will imply our lemma. Let $\mathfrak{f} = \prod_{i=1}^s \mathfrak{p}_i^{e_i}$ denote the prime factorization of $\mathfrak{f}$ in $\tilde{\mathfrak{o}}$. Then

$$R = \prod_{i=1}^s R_i \quad \text{with } R_i = \tilde{\mathfrak{o}}/\mathfrak{p}_i^{e_i}.$$

Let m_i denote the unique maximal ideal of R_i and let

$$m_{R,i} = (R_1, \ldots, R_{i-1}, m_i, R_{i+1}, \ldots, R_s), \quad 1 \leqslant i \leqslant s$$

denote the maximal ideals of R. Since A has a unique maximal ideal, it can be written as

$$m_{R,i} \cap A = (m_1, \ldots, m_s) \cap A, \quad \forall 1 \leqslant i \leqslant s. \tag{23}$$

We prove inequality (22) by induction on s. In the case $s = 1$, R is a local ring. Since $RB = R$, there exists in B a unit ε of R. Thus $\varepsilon A \subseteq B$ and so

$$l_A(R/A) = l_A(R/\varepsilon A) \geqslant l_A(R/B).$$

Moreover, we have $l_A(R/A) = l_A(R/B)$ if and only if $B = \varepsilon A$.

Now suppose $s > 1$ and assume the claim holds when R is a product of $s-1$ local rings. Let

$$\mathrm{pr} : R \to R' = \prod_{i=1}^{s-1} R_i$$

denote the canonical projection. Write $A' = \mathrm{pr}(A)$, $B' = \mathrm{pr}(B)$, and put

$$A_s = \{\alpha \in A \mid \mathrm{pr}(\alpha) = 0\} \quad \text{and} \quad B_s = \{\alpha \in B \mid \mathrm{pr}(\alpha) = 0\}.$$

Note that A' is a subring of R' with unique maximal ideal and B' is an A'-submodule of R' with $R'B' = R'$. By the induction hypothesis,

$$l_{A'}(R'/A') \geqslant l_{A'}(R'/B'). \tag{24}$$

Since $RB = R = R' \oplus R_s$, there exists an element $\epsilon = \epsilon' + \epsilon_s \in B$ such that $\epsilon' \in R'$ and ϵ_s is a unit of R_s. Thus $\epsilon A_s = \epsilon_s A_s \subseteq B_s$ and so

$$l_A(R_s/A_s) \geqslant l_A(R_s/B_s).$$

Combining this with (24), we have

$$l_A(R/A) = l_A(R'/A') + l_A(R_s/A_s) \geqslant l_A(R'/B') + l_A(R_s/B_s) = l_A(R/B).$$

Next suppose that $l_A(R/A) = l_A(R/B)$. Then $l_A(R_s/A_s) = l_A(R_s/B_s)$ and $l_{A'}(R'/A') = l_{A'}(R'/B')$. Thus $\epsilon_s A_s = B_s$. Moreover, by the induction hypothesis, there exists a unit ε' of R' such that $B' = \varepsilon' A'$. Since $\varepsilon' \in B'$, there exists an element $\varepsilon \in B$ such that $\mathrm{pr}(\varepsilon) = \varepsilon'$. Now

$$B = \varepsilon A + B_s = \varepsilon A + \epsilon_s A_s \quad \text{and so} \quad R = RB = \varepsilon R + R_s A_s.$$

But by (23), $A_s \subseteq m_{R,1} \cap A \subseteq m_{R,s}$. This shows that ε is a unit of R and by our assumption that $l_A(R/A) = l_A(R/B)$, we must have $B = \varepsilon A$. The proof of the converse direction is straightforward. □

Corollary 5.17. *Let $\mathcal{O}$ be an order of K with conductor $\mathfrak{f}$, $\mathfrak{a}$ a fractional ideal of $\mathcal{O}$. Then*:

(1) $[\mathcal{O}_K\mathfrak{a} : \mathfrak{a}]$ *is an integer dividing* $[\mathcal{O}_K : \mathcal{O}]$. *It is equal to* $[\mathcal{O}_K : \mathcal{O}]$ *if and only if* $\mathfrak{a}$ *is* $\mathcal{O}$*-invertible*;
(2) *In the case* $\mathfrak{a}$ *is* $\mathcal{O}$*-proper,* $[\mathcal{O} : \mathfrak{f}]$ *divides* $[\mathcal{O}_K\mathfrak{a} : \mathfrak{a}]$ *and with equality holding if and only if* $\mathfrak{a}^\vee$ *is* $\mathcal{O}$*-invertible.*

Proof. (1) Localize the $\mathcal{O}$-ideals $\mathcal{O}_K$, $\mathcal{O}$ and $\mathfrak{a}$ with respect to the multiplicative set $\mathcal{O}\backslash\mathfrak{p}$ for each maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ and apply Lemma 5.16. For the second statement, use the fact that $\mathfrak{a}$ is $\mathcal{O}$-invertible if and only if its localization $\mathfrak{a}_\mathfrak{p}$ is a principal $\mathcal{O}_\mathfrak{p}$-ideal at every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ [17, §12]. (2) Observe that

$$\left[\mathcal{O}_K\mathfrak{a}^\vee : \mathfrak{a}^\vee\right] = \left[(\mathcal{O}_K\mathfrak{a})^{-1}\mathcal{O}_K\mathcal{O}^\vee : \mathfrak{a}^\vee\right] = \left[(\mathfrak{a}\mathfrak{f})^\vee : \mathfrak{a}^\vee\right] = [\mathfrak{a} : \mathfrak{a}\mathfrak{f}],$$

so $[\mathcal{O}_K\mathfrak{a} : \mathfrak{a}][\mathcal{O}_K\mathfrak{a}^\vee : \mathfrak{a}^\vee] = [\mathcal{O}_K\mathfrak{a} : \mathfrak{a}\mathfrak{f}] = [\mathcal{O}_K : \mathfrak{f}] = [\mathcal{O}_K : \mathcal{O}][\mathcal{O} : \mathfrak{f}]$. Now (2) is a direct consequence of (1). □

Applying Corollary 5.17 to $[\mathcal{O} : \mathfrak{f}] = [\mathcal{O}_K\mathcal{O}^\vee : \mathcal{O}^\vee]$, we obtain Theorem 5.6.

6. The Euler product and the Moebius inversion

From now on, we let $M_K = \{\alpha \in \delta_K^{-1} \mid \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0\}$ denote the incomplete canonical module of the maximal order $\mathcal{O}_K$. Put

$$\mathcal{L} = \{M \in \mathbb{M}_{d-1} \mid M \subseteq M_K\}$$

and

$$\mathcal{L}_p = \left\{M \in \mathcal{L} \;\middle|\; [M_K : M] = p^v \text{ for some } v \in \mathbb{Z},\ v \geqslant 0\right\}$$

for each rational prime p. Moreover, let $\prod_p \mathcal{L}_p$ denote the restricted product of $\mathcal{L}_p$ over all primes p. The elements in $\prod_p \mathcal{L}_p$ are of the form $(M^{(p)})_p$ with each p-component $M^{(p)} \in \mathcal{L}_p$ and $M^{(p)} = M_K$ for all but finitely many p.

There is a natural bijection $\mathcal{E}$ between $\mathcal{L}$ and $\prod_p \mathcal{L}_p$ defined as follows (cf. [15]). Given $M \in \mathcal{L}$, there is a unique module $M^{(p)} \in \mathcal{L}_p$ with $M \subseteq M^{(p)} \subseteq M_K$ such that $[M^{(p)} : M]$ is coprime to p. In fact, $M^{(p)} = (M \otimes \mathbb{Z}_p) \cap M_K$, where we identify $M \otimes \mathbb{Z}_p$ and M_K with their images in $M_K \otimes \mathbb{Z}_p$ via the canonical embedding. Then we define

$$\mathcal{E}(M) = \left(M^{(p)}\right)_p \in \prod_p \mathcal{L}_p. \tag{25}$$

We show next that the bijection $\mathcal{E}$ preserves module indexes. Let $M \in \mathcal{L}$ with $\mathcal{E}(M) = (M^{(p)})_p$. Then $[M_K : M] = \prod_p [M_K : M^{(p)}]$. Moreover, let $\mathfrak{c}$ and $\mathfrak{c}^{(p)}$ denote respectively the integral ideals of $\mathcal{O}_K$ such that $\mathcal{O}_K M = \delta_K^{-1}\mathfrak{c}$ and $\mathcal{O}_K M^{(p)} = \delta_K^{-1}\mathfrak{c}^{(p)}$. Then $\mathfrak{c}^{(p)} = \mathcal{O}_K$ for all but finitely many p and $\mathfrak{c} = \prod_p \mathfrak{c}^{(p)}$. Since $\mathrm{ind}\, M_K = 1$, we have

$$\mathrm{ind}\, M = \mathbf{N}\mathfrak{c}^{-(d-1)}[M_K : M]^d \,\mathrm{ind}\, M_K = \prod_p \mathrm{ind}\, M^{(p)}.$$

Now put

$$\mathcal{L}^* = \left\{M^* \in \mathcal{L} \;\middle|\; M^* \neq kM \text{ for any } M \in \mathcal{L} \text{ and } k \in \mathbb{Z},\ k > 1\right\}$$

and $\mathcal{L}_p^* = \mathcal{L}_p \cap \mathcal{L}^*$. The restriction of $\mathcal{E}$ to $\mathcal{L}^*$ induces a bijection between $\mathcal{L}^*$ and the restricted product $\prod_p \mathcal{L}_p^*$ preserving module indexes. Since each module class of $\mathbb{M}_{d-1}^{\sim}$ contains exactly one representative in $\mathcal{L}^*$, we obtain:

Lemma 6.1.

$$\eta_K(s) = \sum_{M \in \mathcal{L}^*} (\mathrm{ind}\, M)^{-s} = \prod_p \eta_p(s), \tag{26}$$

where

$$\eta_p(s) = \sum_{M \in \mathcal{L}_p^*} (\mathrm{ind}\, M)^{-s}.$$

For the rest of the section, we compute the Euler factor $\eta_p(s)$ for a fixed rational prime p. Let $\mathcal{I}_p$ denote the set of integral ideals of $\mathcal{O}_K$ whose norms are powers of p. Put $\mathcal{I}_{p,1} = \mathcal{I}_p \cap I_{K,1}$ and

$$\mathcal{I}_{p,1}^* = \{ p^m \mathfrak{b} \mid \mathfrak{b} \in \mathcal{I}_{p,1} \text{ and } m \in \mathbb{Z},\ m \geqslant 0 \}.$$

For $\mathfrak{b} \in \mathcal{I}_{p,1}^*$, we write $M_{\mathfrak{b}} = \delta_K^{-1}\mathfrak{b} \cap V_0$ as in Corollary 4.5. Moreover, for $M \in \mathcal{L}$, let $M^\dagger = \mathcal{O}_K M \cap V_0$ denote the smallest pure module in $\mathbb{M}_{d-1}$ containing M. In the case $M \in \mathcal{L}_p^*$, we have $M^\dagger = M_{\mathfrak{b}}$ with $\mathfrak{b} = \delta_K M \in \mathcal{I}_{p,1}$. By Corollary 4.2, M has module index

$$\operatorname{ind} M = \big[M^\dagger : M\big]^d \operatorname{ind} M^\dagger = \big[M^\dagger : M\big]^d \mathbf{N}\mathfrak{b}.$$

Plug this into Lemma 6.1, we obtain:

Lemma 6.2.

$$\eta_p(s) = \sum_{\mathfrak{b} \in \mathcal{I}_{p,1}} \lambda(ds, \mathfrak{b}) \mathbf{N}\mathfrak{b}^{-s}, \tag{27}$$

where we put

$$\lambda(s, \mathfrak{b}) = \sum_{\substack{M \in \mathcal{L}_p \\ M^\dagger = M_{\mathfrak{b}}}} [M_{\mathfrak{b}} : M]^{-s}, \quad \forall \mathfrak{b} \in \mathcal{I}_{p,1}^*.$$

To compute $\lambda(s, \mathfrak{b})$ $(\mathfrak{b} \in \mathcal{I}_{p,1}^*)$, we invoke the following well-known identity [20, p. 175]:

$$\sum_{\substack{\mathfrak{b}' \in \mathcal{I}_{p,1}^* \\ \mathfrak{b} \mid \mathfrak{b}'}} \lambda\big(s, \mathfrak{b}'\big)[M_{\mathfrak{b}} : M_{\mathfrak{b}'}]^{-s} = \sum_{\substack{M \in \mathcal{L}_p \\ M \subseteq M_{\mathfrak{b}}}} [M_{\mathfrak{b}} : M]^{-s} = \zeta_{d,p}(s)$$

where

$$\zeta_{d,p}(s) = \zeta_p(s)\zeta_p(s-1)\cdots\zeta_p(s-d+2) \quad \text{and} \quad \zeta_p(s) = \big(1 - p^{-s}\big)^{-1}.$$

Let μ denote the Moebius function on non-zero integral ideals of $\mathcal{O}_K$, i.e., $\mu(\mathcal{O}_K) = 1$, $\mu(\mathfrak{P}) = -1$, $\mu(\mathfrak{P}^l) = 0$ for any prime ideal $\mathfrak{P}$ and integer $l > 1$ and $\mu(\mathfrak{a})\mu(\mathfrak{b}) = \mu(\mathfrak{a}\mathfrak{b})$ for coprime integral ideals $\mathfrak{a}$ and $\mathfrak{b}$.

Lemma 6.3. *For each $\mathfrak{b} \in \mathcal{I}_{p,1}^*$, there exist coprime integral ideals $\mathfrak{b}_1, \mathfrak{b}_2 \in \mathcal{I}_p$ with $\mathfrak{b}_2 \mid p$ and $\mathbf{N}\mathfrak{b}_2 > p$ such that*

$$\mathfrak{b} = p^m \frac{\mathfrak{b}_1}{\mathfrak{b}_2} \quad \textit{for some integer } m > 0.$$

In this notation, we have

$$\lambda(s, \mathfrak{b}) = \zeta_{d,p}(s)\zeta_{K,p}^{-1}(s)\left(1 + \big(p^s - 1\big)\frac{\mu(\mathfrak{b}_2)}{\mathbf{N}\mathfrak{b}_2{}^s} \prod_{\mathfrak{P} \mid \mathfrak{b}_2} \left(1 - \frac{1}{\mathbf{N}\mathfrak{P}^s}\right)^{-1}\right),$$

where $\zeta_{K,p}(s) = \prod_{\mathfrak{P} \mid p}(1 - \mathbf{N}\mathfrak{P}^{-s})^{-1}$.

Proof. We need to define a special Moebius function reflecting the inclusion relation on $\mathcal{I}_{p,1}^*$ (cf. [12, p. 482]). Let $\mathfrak{b}' \in \mathcal{I}_{p,1}^*$. If $\mathfrak{b} \nmid \mathfrak{b}'$, we put $\mu(\mathfrak{b}', \mathfrak{b}) = 0$. Otherwise there exist integral ideals $\mathfrak{c}_1, \mathfrak{c}_2 \in \mathcal{I}_p$ uniquely determined by $\mathfrak{b}$ and $\mathfrak{b}'$ such that $\mathfrak{c}_1\mathfrak{c}_2 = \mathfrak{b}^{-1}\mathfrak{b}'$, $\mathfrak{c}_1 + \mathfrak{b}_2 = \mathcal{O}_K$, and $\mathfrak{c}_2 \mid \mathfrak{b}_2^{\nu}$ for sufficiently large $\nu \in \mathbb{Z}$. In this case we define

$$\mu\big(\mathfrak{b}', \mathfrak{b}\big) = \begin{cases} \mu(\mathfrak{c}_1)\big(\mu(\mathfrak{c}_2) + \sum_{\mathfrak{P}\mid\mathfrak{b}_2,\, \mathbf{N}\mathfrak{P}=p} \mu(\mathfrak{b}_2\mathfrak{P}^{-1})\big) & \text{if } \mathfrak{c}_2 = \mathfrak{b}_2; \\ \mu(\mathfrak{c}_1)\mu(\mathfrak{c}_2) & \text{if } \mathfrak{c}_2 \neq \mathfrak{b}_2. \end{cases}$$

Note that $\mu(\mathfrak{c}_2) = 0$ if $\mathfrak{c}_2 \nmid \mathfrak{b}_2$, and $\mathfrak{c}_2 \neq \mathfrak{b}_2\mathfrak{P}^{-1}$ for any prime $\mathfrak{P} \mid \mathfrak{b}_2$ with $\mathbf{N}\mathfrak{P} = p$. It is easy to check that for $\mathfrak{b}'' \in \mathcal{I}_{p,1}^*$,

$$\sum_{\substack{\mathfrak{b}' \in \mathcal{I}_{p,1}^* \\ \mathfrak{b}\mid\mathfrak{b}',\, \mathfrak{b}'\mid\mathfrak{b}''}} \mu\big(\mathfrak{b}', \mathfrak{b}\big) = \begin{cases} 1, & \text{if } \mathfrak{b}'' = \mathfrak{b}; \\ 0, & \text{otherwise.} \end{cases}$$

Now we have

$$\begin{aligned} \lambda(s, \mathfrak{b}) &= \sum_{\substack{\mathfrak{b}'' \in \mathcal{I}_{p,1}^* \\ \mathfrak{b}\mid\mathfrak{b}''}} \Bigg(\sum_{\substack{\mathfrak{b}' \in \mathcal{I}_{p,1}^* \\ \mathfrak{b}\mid\mathfrak{b}',\, \mathfrak{b}'\mid\mathfrak{b}''}} \mu\big(\mathfrak{b}', \mathfrak{b}\big) \Bigg) \lambda\big(s, \mathfrak{b}''\big)[M_{\mathfrak{b}} : M_{\mathfrak{b}''}]^{-s} \\ &= \sum_{\substack{\mathfrak{b}' \in \mathcal{I}_{p,1}^* \\ \mathfrak{b}\mid\mathfrak{b}'}} \mu\big(\mathfrak{b}', \mathfrak{b}\big)[M_{\mathfrak{b}} : M_{\mathfrak{b}'}]^{-s} \sum_{\substack{\mathfrak{b}'' \in \mathcal{I}_{p,1}^* \\ \mathfrak{b}'\mid\mathfrak{b}''}} \lambda\big(s, \mathfrak{b}''\big)[M_{\mathfrak{b}'} : M_{\mathfrak{b}''}]^{-s} \\ &= \zeta_{d,p}(s) \sum_{\substack{\mathfrak{b}' \in \mathcal{I}_{p,1}^* \\ \mathfrak{b}\mid\mathfrak{b}'}} \mu\big(\mathfrak{b}', \mathfrak{b}\big)[M_{\mathfrak{b}} : M_{\mathfrak{b}'}]^{-s}. \end{aligned}$$

Observe that $\mu(\mathfrak{b}', \mathfrak{b}) = 0$ unless $\mathfrak{c}_2 \mid \mathfrak{b}_2$, and

$$[M_{\mathfrak{b}} : M_{\mathfrak{b}'}] = \begin{cases} \mathbf{N}\mathfrak{b}'/\mathbf{N}\mathfrak{b} = \mathbf{N}(\mathfrak{c}_1\mathfrak{c}_2), & \text{if } \mathfrak{c}_2 \mid \mathfrak{b}_2 \text{ but } \mathfrak{c}_2 \neq \mathfrak{b}_2; \\ \mathbf{N}(\mathfrak{c}_1\mathfrak{c}_2)/p, & \text{if } \mathfrak{c}_2 = \mathfrak{b}_2. \end{cases}$$

We have

$$\begin{aligned} \zeta_{d,p}(s)^{-1}\lambda(s, \mathfrak{b}) = \sum_{\substack{\mathfrak{c}_1 \in \mathcal{I}_p \\ (\mathfrak{c}_1, \mathfrak{b}_2) = \mathcal{O}_K}} \mu(\mathfrak{c}_1)\mathbf{N}\mathfrak{c}_1^{-s} \Bigg(& \sum_{\mathfrak{c}_2 \mid \mathfrak{b}_2} \mu(\mathfrak{c}_2)\mathbf{N}\mathfrak{c}_2^{-s} - \sum_{\substack{\mathfrak{P}\mid\mathfrak{b}_2 \\ \mathbf{N}\mathfrak{P}=p}} \mu\big(\mathfrak{b}_2\mathfrak{P}^{-1}\big)\mathbf{N}\big(\mathfrak{b}_2\mathfrak{P}^{-1}\big)^{-s} \\ & - \mu(\mathfrak{b}_2)\mathbf{N}\mathfrak{b}_2^{-s} + \Bigg(\mu(\mathfrak{b}_2) + \sum_{\substack{\mathfrak{P}\mid\mathfrak{b}_2 \\ \mathbf{N}\mathfrak{P}=p}} \mu\big(\mathfrak{b}_2\mathfrak{P}^{-1}\big)\Bigg)\big(p^{-1}\mathbf{N}\mathfrak{b}_2\big)^{-s} \Bigg) \\ = \prod_{\mathfrak{P}\mid p,\, \mathfrak{P}\nmid\mathfrak{b}_2} \big(1 - \mathbf{N}\mathfrak{P}^{-s}\big) & \Bigg(\prod_{\mathfrak{P}\mid\mathfrak{b}_2} \big(1 - \mathbf{N}\mathfrak{P}^{-s}\big) + \big(p^s - 1\big)\mu(\mathfrak{b}_2)\mathbf{N}\mathfrak{b}_2^{-s} \Bigg) \\ = \zeta_{K,p}^{-1}(s) & \Bigg(1 + \big(p^s - 1\big)\mu(\mathfrak{b}_2)\mathbf{N}\mathfrak{b}_2^{-s} \prod_{\mathfrak{P}\mid\mathfrak{b}_2} \big(1 - \mathbf{N}\mathfrak{P}^{-s}\big)^{-1}\Bigg). \end{aligned}$$

□

We conclude the proof of Theorem 2.1 with the following lemma.

Lemma 6.4.

$$\eta_p(s) = \zeta_p(ds-1)\zeta_p(ds-2)\cdots\zeta_p(ds-d+2)\frac{\zeta_{K,p}(s)}{\zeta_{K,p}((d-1)s)}.$$

Proof. By applying Lemma 6.3 to (27), we have

$$\begin{aligned}\zeta_{d,p}^{-1}(ds)\zeta_{K,p}(ds)\eta_p(s) &= \sum_{\mathfrak{b}\in\mathcal{I}_{p,1}} \mathbf{N}\mathfrak{b}^{-s} + \big(1-p^{-ds}\big)\sum_{\mathfrak{b}\in\mathcal{I}_{p,1}} \mu(\mathfrak{b}_2)\mathbf{N}(\mathfrak{b}/p)^{-s}\mathbf{N}\mathfrak{b}_2^{-ds}\prod_{\mathfrak{P}\mid\mathfrak{b}_2}\big(1-\mathbf{N}\mathfrak{P}^{-ds}\big)^{-1}\\ &= A_1 + \big(1-p^{-ds}\big)A_2.\end{aligned}$$

It is clear that

$$\begin{aligned}A_1 &= \big(1-p^{-ds}\big)\sum_{\mathfrak{b}\in\mathcal{I}_p}\mathbf{N}\mathfrak{b}^{-s} - \sum_{\substack{\mathfrak{P}\mid p\\ \mathbf{N}\mathfrak{P}=p}}\mathbf{N}\big(p\mathfrak{P}^{-1}\big)^{-s}\prod_{\substack{\mathfrak{P}'\mid p\\ \mathfrak{P}'\neq\mathfrak{P}}}\big(1-\mathbf{N}\mathfrak{P}'^{-s}\big)^{-1}\\ &= \zeta_{K,p}(s)\big(1-p^{-ds}+t_p\big(1-p^s\big)p^{-ds}\big),\end{aligned}$$

where t_p denotes the number of prime ideals $\mathfrak{P}$ with $\mathbf{N}\mathfrak{P}=p$.

As $\mathfrak{b}_2$ goes through integral ideals with $\mathfrak{b}_2 \mid p$ and $\mathbf{N}\mathfrak{b}_2 > p$, $\mathfrak{b}_1$ ranges over ideals in $\mathcal{I}_p$ coprime to $\mathfrak{b}_2$, $\mathfrak{b} = p\mathfrak{b}_1\mathfrak{b}_2^{-1}$ would go through $\mathcal{I}_{p,1}$. This enables us to write

$$\begin{aligned}A_2 &= \sum_{\substack{\mathfrak{b}_2\mid p\\ \mathbf{N}\mathfrak{b}_2>p}}\mu(\mathfrak{b}_2)\mathbf{N}\mathfrak{b}_2^{-(d-1)s}\Bigg(\sum_{\substack{\mathfrak{b}_1\in\mathcal{I}_p\\ (\mathfrak{b}_1,\mathfrak{b}_2)=\mathcal{O}_K}}\mathbf{N}\mathfrak{b}_1^{-s}\Bigg)\prod_{\mathfrak{P}\mid\mathfrak{b}_2}\big(1-\mathbf{N}\mathfrak{P}^{-ds}\big)^{-1}\\ &= \zeta_{K,p}(s)\sum_{\substack{\mathfrak{b}_2\mid p\\ \mathbf{N}\mathfrak{b}_2>p}}\mu(\mathfrak{b}_2)\mathbf{N}\mathfrak{b}_2^{-(d-1)s}\prod_{\mathfrak{P}\mid\mathfrak{b}_2}\big(1-\mathbf{N}\mathfrak{P}^{-s}\big)\big(1-\mathbf{N}\mathfrak{P}^{-ds}\big)^{-1}\\ &= \zeta_{K,p}(s)\Bigg(\prod_{\mathfrak{P}\mid p}\big(1-\mathbf{N}\mathfrak{P}^{-(d-1)s}\big(1-\mathbf{N}\mathfrak{P}^{-s}\big)\big(1-\mathbf{N}\mathfrak{P}^{-ds}\big)^{-1}\big)\\ &\quad -1+\sum_{\substack{\mathfrak{P}\mid p\\ \mathbf{N}\mathfrak{P}=p}}p^{-(d-1)s}\big(1-p^{-s}\big)\big(1-p^{-ds}\big)^{-1}\Bigg)\\ &= \zeta_{K,p}(s)\big(\zeta_{K,p}(ds)\zeta_{K,p}^{-1}\big((d-1)s\big)-1+t_pp^{-ds}\big(p^s-1\big)\big(1-p^{-ds}\big)^{-1}\big).\end{aligned}$$

Putting the above two parts together gives the stated result. □

Acknowledgment

The author wishes to thank the referee for helpful comments.

Supplementary material

The online version of this article contains additional supplementary material.
Please visit doi:10.1016/j.jnt.2010.11.010.

References

[1] A. Berczes, J.H. Evertse, K. Gyory, On the number of equivalence classes of binary forms of given degree and given discriminant, Acta Arith. 113 (2004) 363–399.
[2] M. Bhargava, Higher composition laws III: The parametrization of quartic rings, Ann. of Math. 159 (2004) 1329–1360.
[3] B.J. Birch, J.R. Merriman, Finiteness theorems for binary forms with given discriminant, Proc. Lond. Math. Soc. 24 (1972) 385–394.
[4] J.A. Buchmann, H.W. Lenstra Jr., Approximating rings of integers in number fields, J. Theor. Nombres Bordeaux 6 (1994) 221–260.
[5] B. Datskovsky, D.J. Wright, The adelic zeta function associated with the space of binary cubic forms, II: Local theory, J. Reine Angew. Math. 367 (1986) 27–75.
[6] B.N. Delone, D.K. Faddeev, The Theory of Irrationalities of the Third Degree, Transl. Math. Monogr., vol. 10, Amer. Math. Soc., Providence, RI, 1964.
[7] A. Fröhlich, Invariants for modules over commutative separable orders, Quart. J. Math. Oxford Ser. (2) 16 (1965) 193–232.
[8] W.T. Gan, B.H. Gross, G. Savin, Fourier coefficients of modular forms on G_2, Duke Math. J. 115 (2002) 105–169.
[9] X. Gao, On the zeta function associated with decomposable forms, in preparation.
[10] E. Hecke, Lectures on the Theory of Algebraic Numbers, Springer-Verlag, 1981.
[11] J. Herzog, E. Kunz, Der kanonische Modul eines Cohen–Macaulay-Rings, Lecture Notes in Math., vol. 238, Springer-Verlag, 1971.
[12] N. Jacobson, Basic Algebra I, second ed., W.H. Freeman and Company, New York, 1985.
[13] S. Lang, Algebraic Number Theory, second ed., Springer-Verlag, New York, 1994.
[14] J. Nakagawa, Binary forms and orders of algebraic number fields, Invent. Math. 97 (1989) 219–235.
[15] J. Nakagawa, Orders of a quartic field, Mem. Amer. Math. Soc. 583 (1996).
[16] J. Nakagawa, On the relations among the class numbers of binary cubic forms, Invent. Math. 134 (1998) 101–138.
[17] J. Neukirch, Algebraic Number Theory, Springer-Verlag, 1999.
[18] I. Reiner, A survey of integral representation theory, Recent progress in the theory of integral representations, 1969.
[19] T. Shintani, On Dirichlet series whose coefficients are class numbers of integral binary cubic forms, J. Math. Soc. Japan 24 (1972) 132–188.
[20] A. Terras, Harmonic Analysis on Symmetric Spaces and Applications II, Springer-Verlag, New York, 1988.