PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 11, November 2013, Pages 3709–3722
S 0002-9939(2013)11651-5
Article electronically published on July 15, 2013

EXPLICIT COMPUTATIONS IN HECKE ALGEBRAS OF GL_2 OVER DEDEKIND DOMAINS

MARC ENSENBACH

(Communicated by Kathrin Bringmann)

Dedicated to the memory of Fritz Grunewald

Abstract. In this paper, a formula for the number of right cosets contained in a double coset with respect to the unimodular group of invertible (2×2)-matrices over a Dedekind domain is developed. As applications we derive an index formula for congruence subgroups and an algorithm for the explicit calculation of products in Hecke algebras.

1. Introduction and statement of results

Since the first implicit appearance of Hecke operators in the context of modular forms ([1]), Hecke operators and thus Hecke algebras have become an indispensable instrument in the theory of automorphic forms (see e.g. [2] and [3]). Thus the structure of abstract Hecke algebras has been investigated in a variety of settings (see e.g. [4] for an overview and [5] as well as [6] for the analysis of special cases). Following the traditional approach for matrix groups (as depicted e.g. in [4], Chapter V), this article first focuses on the structure of the elements themselves, namely the decomposition of double cosets into right cosets. It will later turn out that the gained insight into these building blocks of a Hecke algebra can be used as a means to further investigate the multiplicative structure both computationally and theoretically.

In the development of Hecke theory, the first abstract Hecke algebras to appear were constructed with respect to unimodular groups over the rational integers. Later, generalisations to other underlying rings became of interest for the theory of modular forms (see e.g. [7]). In order to provide means for the theory of automorphic forms over number fields, the present paper deals with Hecke algebras over norm-finite Dedekind domains, i.e. Dedekind domains in which every principal ideal has a finite norm. In this setting, the first main results are obtained by adapting the considerations for the analogous results for matrices over $\mathbb{Z}$ (see Example 3.1) to Dedekind domains, where right cosets with respect to unimodular groups no longer need to have a triangular representative. To begin with, a formula for the number of special right cosets contained in a double coset is derived.

1.1. **Theorem.** *Let $\mathfrak{o}$ be a norm-finite Dedekind domain, $A \in \mathfrak{o}^{2\times 2}$ with nonzero determinant and $\mathfrak{a}$ an ideal in $\mathfrak{o}$. Denote by $\mathfrak{d}_1(A)$ and $\mathfrak{d}_2(A)$ the ideals generated by*

Received by the editors November 17, 2011 and, in revised form, January 11, 2012.
2010 *Mathematics Subject Classification.* Primary 20G30, 20H05, 20C08.
Key words and phrases. Unimodular group, Dedekind domain, congruence subgroup, index formula, Hecke algebra.

the entries of A and by the determinant, respectively, and let $\mathrm{N}(\cdot)$ denote the norm of an ideal. Then, if $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}$, the double coset $\mathrm{GL}_2(\mathfrak{o})A\,\mathrm{GL}_2(\mathfrak{o})$ contains exactly

$$\frac{\mathrm{N}(\mathfrak{d}_2(A))}{\mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{d}_1(A))} \prod_{\substack{\mathfrak{p}\ \textit{prime ideal}\\ \mathfrak{p}\mid \mathfrak{a}\mathfrak{d}_1(A)^{-1}+\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}}} (1-\mathrm{N}(\mathfrak{p})^{-1})$$

cosets $\mathrm{GL}_2(\mathfrak{o})B$, where the first column entries of B generate the ideal $\mathfrak{a}$. Otherwise, the double coset of A does not contain any such right coset. □

Theorem 1.1 is a main step towards an algorithmic approach to Hecke algebras: If we want to carry out computations in abstract Hecke algebras, we need an algorithm that allows us to multiply two elements. Since the product can be calculated by a multiplication of representatives of right cosets, the task of multiplying elements of an abstract Hecke algebra can essentially be reduced to the search for decompositions of double cosets into right cosets. Knowing how many cosets we have to find allows us to state a randomised algorithm which carries out the decomposition. In order to obtain a formula for this quantity, we sum over all ideals $\mathfrak{a}$ in Theorem 1.1, which yields the following.

1.2. **Theorem.** *In Theorem* 1.1*, the coset system $\mathrm{GL}_2(\mathfrak{o})\backslash \mathrm{GL}_2(\mathfrak{o})A\,\mathrm{GL}_2(\mathfrak{o})$ contains exactly*

$$\frac{\mathrm{N}(\mathfrak{d}_2(A))}{\mathrm{N}(\mathfrak{d}_1(A))^2} \prod_{\substack{\mathfrak{p}\ \textit{prime ideal}\\ \mathfrak{p}\mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}}} (1+\mathrm{N}(\mathfrak{p})^{-1})$$

elements. □

Since there exist algorithms for the calculation of all data that occur in this formula, programmes for the computation of products in the Hecke algebra can now be stated.

As has already been mentioned, this article will not only focus on algorithmic questions, but will also deal with theoretical results that can be derived from Theorem 1.1: A principal question in the theory of abstract Hecke algebras is whether a certain formal power series over this algebra can be written as a quotient of two polynomials (see e.g. the rationality theorem in [4] on page 123). To this end, in the "classic" Hecke algebra H_n related to $\mathrm{GL}_n(\mathbb{Z})$, the reduction of certain products in H_n to products in H_{n-1} is analysed. We are currently not able to give the full proof for a generalised rationality theorem, but a first step can be taken: By counting right cosets with representatives whose first column entries are coprime, a general reduction theorem can be proved for $n = 2$. This result is sketched in the following; after the required notation has been introduced in Section 5, the Theorem is rendered more precisely as Theorem 5.6.

Theorem. *Let $a, b, c \in \mathfrak{o}$ for a norm-finite Dedekind domain $\mathfrak{o}$, and let $A = \left(\begin{smallmatrix}1 & 0\\ 0 & a\end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix}1 & 0\\ 0 & b\end{smallmatrix}\right)$ as well as $C = \left(\begin{smallmatrix}1 & 0\\ 0 & c\end{smallmatrix}\right)$. Then the double coset of C has a nonzero coefficient in the Hecke product of the double cosets of A and B, if and only if abc^{-1} is a unit in $\mathfrak{o}$; moreover, the nonzero coefficient is always equal to* 1.

Another theoretical result can be derived from the coset counting formulae via a relation between representatives in a double coset and elements of certain right transversals (a set of representatives of right cosets) of GL_2. For special choices

of the double coset an index formula for congruence subgroups is obtained from Theorem 1.2.

1.3. **Corollary.** *Let $m \in \mathfrak{o}$ with $m \neq 0$ for a Dedekind domain $\mathfrak{o}$, and define the subgroup $U^0[m] = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathfrak{o}) \mid b \in m\mathfrak{o}\}$ of $\mathrm{GL}_2(\mathfrak{o})$. Then the index of $U^0[m]$ in $\mathrm{GL}_2(\mathfrak{o})$ can be calculated by*

$$[U : U^0[m]] = \mathrm{N}(m\mathfrak{o}) \prod_{\substack{\mathfrak{p} \text{ prime ideal} \\ \mathfrak{p} \mid m}} (1 + \mathrm{N}(\mathfrak{p})^{-1}).$$

□

The main content of this article is organised as follows: In the following section, the notation is fixed and some basic facts which are used throughout this article are assembled. After that, the two already discussed formulae for numbers of right cosets contained in a double coset are proved in Section 3. The application of these formulae to congruence subgroups will shortly be dealt with in Section 4, and the already mentioned applications to Hecke algebras are finally depicted in Section 5.

2. Preliminaries and notation

Denote by $\mathfrak{o}$ a norm-finite Dedekind domain, i.e. a Dedekind domain in which $|\mathfrak{o}/a\mathfrak{o}| < \infty$ holds for every $a \in \mathfrak{o}$ (where $|M|$ is the cardinality of the set M). Furthermore, denote by K the field of fractions of $\mathfrak{o}$, and by $\mathfrak{o}^*$ the group of units of $\mathfrak{o}$. Then denote by $\mathrm{v}_\mathfrak{p}(\mathfrak{a})$ the multiplicity of a prime ideal $\mathfrak{p}$ in the ideal $\mathfrak{a}$ of $\mathfrak{o}$ (fundamental properties of Dedekind domains and multiplicities can be found for example in [8], Chapter II).

Let I be the set of (2×2) matrices with entries in $\mathfrak{o}$ and with nonzero determinant; furthermore, denote by U the set of matrices in I with determinant in $\mathfrak{o}^*$ (in other words, $U = \mathrm{GL}_2(\mathfrak{o})$ and $I = \mathrm{GL}_2(K) \cap \mathfrak{o}^{2\times2}$). For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathfrak{o}^{2\times2}$ one defines the first and second determinantal divisor of A by $\mathfrak{d}_1(A) = a\mathfrak{o} + b\mathfrak{o} + c\mathfrak{o} + d\mathfrak{o}$ and $\mathfrak{d}_2(A) = (\det A)\mathfrak{o}$, respectively. Furthermore, one introduces the notation $\mathfrak{g}(A)$ for the g.c.d. of the first column of A, i.e. $\mathfrak{g}(A) = a\mathfrak{o} + c\mathfrak{o}$. By $\mu(A)$ denote the number of right cosets UA' contained in UAU, and let $\mu_\mathfrak{a}(A)$ for an ideal $\mathfrak{a}$ of $\mathfrak{o}$ count such right cosets in UAU with $\mathfrak{g}(A') = \mathfrak{a}$.

The relation between determinantal divisors and double cosets of U is given in the following theorem, which goes back to Steinitz ([9]; see also [10], Theorem 2.2).

2.1. **Theorem.** *Let $A, B \in \mathfrak{o}^{2\times2}$.*

a) If A and B have rank 2 (i.e., if $A, B \in I$), the following assertions are equivalent: (i) $UAU = UBU$, (ii) $\mathfrak{d}_1(A) = \mathfrak{d}_1(B)$ and $\mathfrak{d}_2(A) = \mathfrak{d}_2(B)$.

b) If A and B have rank 1 and the first columns of A and B both contain at least one nonzero element, the following assertions are equivalent: (i) $UAU = UBU$, (ii) $\mathfrak{d}_1(A) = \mathfrak{d}_1(B)$ and $\mathfrak{g}(A) = \mathfrak{g}(B)$. □

This theorem can not only be used to characterise the equality of double cosets, but also has an application in the proof of the following corollary which allows us to state a relation between different generators of the same ideal in $\mathfrak{o}$.

2.2. **Corollary.** *Let $a, b, c, d \in \mathfrak{o}$ be such that $a\mathfrak{o} + b\mathfrak{o} = c\mathfrak{o} + d\mathfrak{o}$. Then there exists an $R \in U$ satisfying $R\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$.* □

Proof. In the case $c = d = 0$ we also have $a = b = 0$ and can choose $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. For the remaining part of the proof assume $c \neq 0$ (without loss of generality). Let $A = \left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} c & 0 \\ d & 0 \end{smallmatrix}\right)$. Since A and B both have rank 1 and satisfy $\mathfrak{d}_1(A) = \mathfrak{d}_1(B)$ as well as $\mathfrak{g}(A) = \mathfrak{g}(B)$, Theorem 2.1 yields the existence of $P, Q \in U$ such that $PAQ = B$ and thus $PA = BQ^{-1}$. Writing $P = \left(\begin{smallmatrix} p_1 & p_2 \\ p_3 & p_4 \end{smallmatrix}\right)$ and $Q^{-1} = \left(\begin{smallmatrix} q_1 & q_2 \\ q_3 & q_4 \end{smallmatrix}\right)$ and calculating PA as well as BQ^{-1}, we obtain

$$\begin{pmatrix} p_1a + p_2b & 0 \\ p_3a + p_4b & 0 \end{pmatrix} = \begin{pmatrix} cq_1 & cq_2 \\ dq_1 & dq_2 \end{pmatrix}.$$

In particular, we have $cq_2 = 0$, and since $c \neq 0$, this implies $q_2 = 0$. Thus $\det Q^{-1} = q_1q_4$, which implies $q_1 \in \mathfrak{o}^*$. If we define $R = q_1^{-1}P$, we thus have $R \in U$. Furthermore,

$$R\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = q_1^{-1}PA = q_1^{-1}\begin{pmatrix} p_1a + p_2b & 0 \\ p_3a + p_4b & 0 \end{pmatrix} = q_1^{-1}\begin{pmatrix} cq_1 & 0 \\ dq_1 & 0 \end{pmatrix} = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix},$$

which proves $R\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$ and completes the proof. □

2.3. *Remark.* Since there exists a version of Theorem 2.1 for $A, B \in \mathfrak{o}^{n\times n}$ for arbitrary $n \in \mathbb{N}$ (see e.g. [10], Theorem 2.2), Corollary 2.2 can easily be generalised from two generators to an arbitrary number of generators of an ideal as long as the number of generators on both sides of the equation is the same. □

3. Counting right cosets

In this section a formula for the number of right cosets in a given double coset of U is derived. To begin with, a short example shows how coset counting is carried out in the classic case $\mathfrak{o} = \mathbb{Z}$. This will serve as a guideline for the subsequent analysis of the general case.

3.1. **Example.** Let $\mathfrak{o} = \mathbb{Z}$. Since $\mathfrak{o}$ is a principal ideal domain, every right coset UB for $B \in I$ has a unique representative

$$B' = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad \text{with } a, d > 0 \text{ and } 0 \leq b < d,$$

known as the Hermite normal form of B. Given this normal form, the number of right cosets in a given double coset UAU can be obtained by generating all possible normal forms (in a sensible way) and deciding whether they belong to UAU. The latter can be carried out using Theorem 2.1 to test for $UB'U = UAU$, so it has to be checked whether $\mathfrak{d}_1(B') = \mathfrak{d}_1(A)$ and $\mathfrak{d}_2(B') = \mathfrak{d}_2(A)$ hold.

As a concrete example construct every right coset representative B' as above contained in UAU, where $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$. Since $\mathfrak{d}_2(A) = \mathfrak{d}_2(B')$ is a necessary condition for $UB'U = UAU$, the equation $(\det A)\mathbb{Z} = (\det B')\mathbb{Z}$ and thus $4 = ad$ has to be satisfied. So there are three possible cases: (i) $a = 4$ and $d = 1$, (ii) $a = 2$ and $d = 2$, and (iii) $a = 1$ and $d = 4$. For these cases determine for which values of b the equation $UB'U = UAU$ is fulfilled. To this end, it suffices to test whether $\mathfrak{d}_1(B') = \mathfrak{d}_1(A)$ holds since a and d have already been constructed to satisfy $\mathfrak{d}_2(B') = \mathfrak{d}_2(A)$.

Case (i). Since $d = 1$ and $0 \leq b < d = 1$, only the case $b = 0$ has to be analysed. Then we have $\mathfrak{d}_1(B') = a\mathbb{Z} + b\mathbb{Z} + d\mathbb{Z} = 4\mathbb{Z} + 0\mathbb{Z} + 1\mathbb{Z} = 1\mathbb{Z} = 1\mathbb{Z} + 4\mathbb{Z} = \mathfrak{d}_1(A)$, so $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is a right coset representative in UAU.

Case (ii). Since $d = 2$ and $0 \le b < d = 2$, the cases $b = 0$ and $b = 1$ have to be considered. For $b = 0$ we have $\mathfrak{d}_1(B') = 2\mathbb{Z} \neq 1\mathbb{Z} = \mathfrak{d}_1(A)$, so $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ is not an element of UAU. For $b = 1$, however, we have $\mathfrak{d}_1(B') = 1\mathbb{Z} = \mathfrak{d}_1(A)$, so $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)$ belongs to UAU.

Case (iii). Since $d = 4$ and $0 \le b < d = 4$, the cases $b \in \{0, 1, 2, 3\}$ have to be analysed. Due to $a = 1$ we have $\mathfrak{d}_1(B') = 1\mathbb{Z} = \mathfrak{d}_1(A)$ in any of these cases, so $\left(\begin{smallmatrix} 1 & b \\ 0 & 4 \end{smallmatrix}\right)$ belongs to UAU for every $b \in \{0, 1, 2, 3\}$.

Summarising, in UAU we have found the 6 right coset representatives $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 4 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 3 \\ 0 & 4 \end{smallmatrix}\right)$.

Generalising these considerations, a formula for the number $\mu(A)$ of right cosets contained in UAU can be stated:

$$\mu(A) = \sum_{\substack{d \in \mathbb{N} \\ d \mid \det A}} |\{b \in \mathbb{N}_0 \mid b < d \text{ and } \tfrac{\det A}{d}\mathbb{Z} + b\mathbb{Z} + d\mathbb{Z} = \mathfrak{d}_1(A)\}|$$

(where $\mathbb{N} = \{1, 2, 3, \dots, \}$ and $\mathbb{N}_0 = \{0, 1, 2, \dots\}$). The cardinality of a set $\{b \in \mathbb{N}_0 \mid b < d \text{ and } a\mathbb{Z} + b\mathbb{Z} + d\mathbb{Z} = \mathfrak{d}_1(A)\}$ can be calculated explicitly, which finally leads to a product formula for $\mu(A)$ (not presented in detail since the same steps are to be done for the general case in the following). □

The first main ingredient of the approach taken in Example 3.1 in the classic case is the Hermite normal form. In the general case, another normal form can be constructed – not as "nice" as in the classic case, but nevertheless solving the issue of a uniquely determined representative.

3.2. **Lemma.** *Let $\mathfrak{a}$ be an ideal in $\mathfrak{o}$ and $b \in \mathfrak{a}$. Choose an $a \in \mathfrak{a}$ satisfying $a \neq 0$ and $a\mathfrak{o} + b\mathfrak{o} = \mathfrak{a}$ (always possible since $\mathfrak{o}$ is a Dedekind domain) and a transversal T of $(\mathfrak{o} \cap ab^{-1}\mathfrak{o})/(ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o})$. This transversal is finite, and for every $A \in I$ satisfying $\mathfrak{g}(A) = \mathfrak{a}$ and $\mathfrak{d}_2(A) = b\mathfrak{o}$ there exists a uniquely determined $c \in T$ such that*

$$U \begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix} = UA.$$

□

Proof. The finiteness of T follows from the norm-finiteness of $\mathfrak{o}$ since $ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$ is an ideal in $\mathfrak{o}$.

To prove the uniqueness of c, assume

$$U \begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix} = U \begin{pmatrix} a & d-1 \\ b & ba^{-1}d \end{pmatrix}$$

for $c, d \in T$. Since

$$\begin{pmatrix} a & d-1 \\ b & ba^{-1}d \end{pmatrix} \begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix}^{-1} = \begin{pmatrix} c-d+1 & ab^{-1}(d-c) \\ ba^{-1}(c-d) & 1-c+d \end{pmatrix}$$

then has to be an element of U, we obtain in particular that $ab^{-1}(d-c) \in \mathfrak{o}$ and $ba^{-1}(c-d) \in \mathfrak{o}$, which yields $d-c \in ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$. Since T is a transversal modulo $ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$ and $c, d \in T$, this shows $c = d$ and thus proves the uniqueness of the representative.

In the remaining part of the proof the existence of the desired representative is shown. Let $A \in I$ satisfying $\mathfrak{g}(A) = \mathfrak{a}$ and $\mathfrak{d}_2(A) = b\mathfrak{o}$. Since $a\mathfrak{o} + b\mathfrak{o} = \mathfrak{g}(A)$,

by Corollary 2.2 there exists a $P_1 \in U$ such that $P_1 A = \left(\begin{smallmatrix} a & * \\ b & * \end{smallmatrix}\right)$. Then let $\varepsilon = b(\det(P_1 A))^{-1} \in \mathfrak{o}^*$ and $P_2 = \left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & 1 \end{smallmatrix}\right) \in U$ such that $\det(P_2 P_1 A) = b$. Furthermore, the Chinese Remainder Theorem allows us to choose a $p \in \mathfrak{o}$ satisfying $p \in (\mathfrak{o} \cap ba^{-1}\mathfrak{o}) + \varepsilon^{-1}$ and $p \in (\mathfrak{o} \cap ab^{-1}\mathfrak{o}) + 1$ since $\mathfrak{o} \cap ba^{-1}$ and $\mathfrak{o} \cap ab^{-1}\mathfrak{o}$ are relatively prime. The matrix

$$P_3 = \begin{pmatrix} p & ab^{-1}(1-\varepsilon p) \\ ba^{-1}(p-1) & \varepsilon + 1 - \varepsilon p \end{pmatrix}$$

is then an element of $\mathfrak{o}^{2\times 2}$ with $\det P_3 = 1$, and we have

$$P_3 P_2 P_1 A = P_3 P_2 \begin{pmatrix} a & * \\ b & * \end{pmatrix} = P_3 \begin{pmatrix} \varepsilon a & * \\ b & * \end{pmatrix} = \begin{pmatrix} a & * \\ b & * \end{pmatrix}$$

with $\det(P_3 P_2 P_1 A) = b$, so if the second column of $P_3 P_2 P_1 A$ is denoted by $\left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right)$, we have $as - br = b$ and thus $1 + r = ab^{-1}s \in ab^{-1}\mathfrak{o}$. Since furthermore $1 + r \in \mathfrak{o}$, by the choice of T there exists a $c \in T$ satisfying $1 + r \in c + (ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o})$. Now let

$$P_4 = \begin{pmatrix} ab^{-1}s - c + 1 & ab^{-1}(c - r - 1) \\ s - ba^{-1}c & c - r \end{pmatrix}.$$

Then $P_4 \in \mathfrak{o}^{2\times 2}$ and $\det P_4 = 1$ (since $ab^{-1}s = 1 + r$ and $c - r - 1 \in ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$), and putting everything together we have $P_4 P_3 P_2 P_1 \in U$ and

$$P_4 P_3 P_2 P_1 A = P_4 \begin{pmatrix} a & r \\ b & s \end{pmatrix} = \begin{pmatrix} a(ab^{-1}s - r) & ab^{-1}s(c-1) - cr + r \\ as - br & ba^{-1}c(ab^{-1}s - r) \end{pmatrix} = \begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix},$$

which shows the existence of a representative with the desired form and thus completes the proof. □

With this normal form, a first elementary formula for the number of right cosets with a prescribed g.c.d. of the first column can be given. (All elements of a right coset with respect to U have the same g.c.d. of the first column, so it is possible to talk about the g.c.d. of the first column of a right coset.)

3.3. **Corollary.** *Let $A \in I$ and $\mathfrak{a}$ an ideal of $\mathfrak{o}$ such that $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)$. Choose an $a \in \mathfrak{a}$ satisfying $a\mathfrak{o} + \mathfrak{d}_2(A) = \mathfrak{a}$ (possible since $\mathfrak{a} \mid \mathfrak{d}_2(A)$ and $\mathfrak{o}$ is a Dedekind domain), let $\mathfrak{q} = \mathfrak{a}^{-1}a$ as well as $\mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{d}_2(A)$, and choose a transversal T of $\mathfrak{q}/\mathfrak{q}\mathfrak{b}$. Then the number $\mu_{\mathfrak{a}}(A)$ of right cosets in UAU with $\mathfrak{a}$ as a g.c.d. of the first column can be calculated by*

$$\mu_{\mathfrak{a}}(A) = |\{c \in T \mid \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)\}|. \qquad \square$$

Proof. Since $\mathfrak{a} = a\mathfrak{o} + \mathfrak{d}_2(A) = \mathfrak{a}\mathfrak{q} + \mathfrak{a}\mathfrak{b}$, the ideals $\mathfrak{q}$ and $\mathfrak{b}$ are relatively prime, which yields $\mathfrak{o} \cap a\mathfrak{d}_2(A)^{-1} = \mathfrak{o} \cap \mathfrak{q}\mathfrak{b}^{-1} = \mathfrak{q}$ as well as $\mathfrak{d}_2(A)a^{-1} \cap a\mathfrak{d}_2(A)^{-1} = \mathfrak{b}\mathfrak{q}^{-1} \cap \mathfrak{q}\mathfrak{b}^{-1} = \mathfrak{b}\mathfrak{q}$. Thus T is a transversal of $(\mathfrak{o} \cap a\mathfrak{d}_2(A)^{-1})/(\mathfrak{d}_2(A)a^{-1} \cap a\mathfrak{d}_2(A)^{-1})$.

If UB for some $B \in I$ is a right coset in UAU satisfying $\mathfrak{g}(B) = \mathfrak{a}$, then in particular $\mathfrak{d}_2(B) = \mathfrak{d}_2(A)$, and according to Lemma 3.2 there exists a uniquely determined representative C of UB of the form described in that lemma (with $b = \det A$ and $c \in T$, the latter according to the first paragraph of this proof). Thus

$$\begin{aligned} &\{UB \mid B \in I \text{ with } \mathfrak{g}(B) = \mathfrak{a} \text{ and } UB \subseteq UAU\} \\ &= \left\{ UB \;\middle|\; B = \begin{pmatrix} a & c-1 \\ \det A & (\det A)a^{-1}c \end{pmatrix} \text{ for some } c \in T \text{ and } B \in UAU \right\}, \end{aligned}$$

and since $\mathfrak{d}_2(B) = \mathfrak{d}_2(A)$ for those B, Theorem 2.1 and $a\mathfrak{o} + \mathfrak{d}_2(A) = \mathfrak{a}$ yield

$$\begin{aligned}\mu_{\mathfrak{a}}(A) &= \left|\left\{c \in T \;\middle|\; \mathfrak{d}_1\left(\begin{pmatrix} a & c-1 \\ \det A & (\det A)a^{-1}c \end{pmatrix}\right) = \mathfrak{d}_1(A)\right\}\right| \\ &= |\{c \in T \mid \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)\}|. \qquad \square\end{aligned}$$

The formula presented in Corollary 3.3 is only a first step, since it is not very far from a mere enumeration of right cosets. The next step is the establishment of a product formula for the cardinality on the right-hand side. To achieve this, we first need some auxiliary results.

3.4. **Lemma.** *In the setting of Corollary* 3.3 *the following assertions are equivalent:*

(i) $\mathfrak{c} \mid \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b}$.

(ii) $\mathfrak{c} \mid \mathfrak{a}$ *and* $\mathfrak{ac} \mid \mathfrak{d}_2(A)$ *and* $\mathfrak{c} \mid c-1$. $\square$

Proof. First assume that (i) is satisfied and show that (ii) is fulfilled. Since (i) implies $\mathfrak{c} \mid (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b}$ and c and $c-1$ are relatively prime, we have $\mathfrak{c} \mid \mathfrak{q}^{-1}\mathfrak{b}$ and thus $\mathfrak{ac} \mid \mathfrak{aq}^{-1}\mathfrak{b} = a^{-1}\mathfrak{a}\mathfrak{d}_2(A)$, which implies $\mathfrak{ac} \mid \mathfrak{d}_2(A)$ since $a \in \mathfrak{a}$. The remaining parts of (ii) follow obviously.

Now assume that (ii) is fulfilled. For the proof of (i) it remains to show $\mathfrak{c} \mid c\mathfrak{q}^{-1}\mathfrak{b}$. But this follows from $\mathfrak{ac} \mid \mathfrak{d}_2(A)$ and $c \in \mathfrak{q}$, since the latter implies $\mathfrak{c} \mid \mathfrak{a}^{-1}\mathfrak{d}_2(A) = \mathfrak{b}$ and $c\mathfrak{q}^{-1} \subseteq \mathfrak{o}$, so the proof is complete. $\square$

The second auxiliary result gives an explicit formula for the cardinality of a certain subset of T needed in the calculation of $\mu_{\mathfrak{a}}(A)$.

3.5. **Lemma.** *In the setting of Corollary* 3.3 *we have*

$$|\{c \in T \mid c-1 \in \mathfrak{c}\}| = \mathrm{N}(\mathfrak{b})\,\mathrm{N}(\mathfrak{c})^{-1}$$

for every ideal $\mathfrak{c}$ *of* $\mathfrak{o}$ *satisfying* $\mathfrak{c} \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{c}^{-1}$. $\square$

Proof. In the given setting we have $\mathfrak{c} \mid \mathfrak{b}$, and $\mathfrak{b}$ and $\mathfrak{q}$ are relatively prime, so $\mathfrak{c}$ and $\mathfrak{q}$ are relatively prime. By the Chinese Remainder Theorem there exists a $d \in \mathfrak{q} \cap (\mathfrak{c}+1)$. Then $\{c-d \mid c \in T,\ c-1 \in \mathfrak{c}\}$ is a transversal of $\mathfrak{cq}/\mathfrak{bq}$: All those $c-d$ are elements of $\mathfrak{c} \cap \mathfrak{q} = \mathfrak{cq}$, the $(c-d) + \mathfrak{bq}$ are pairwise different since T is a transversal of $\mathfrak{q}/\mathfrak{bq}$, and for every $x \in \mathfrak{cq}$ there exists a $c \in T$ satisfying $x \in (c-d) + \mathfrak{bq}$, namely the one satisfying $x + d \in c + \mathfrak{bq}$, which exists in T since $x + d \in \mathfrak{q}$, and is an element of $\{c \in T \mid c-1 \in \mathfrak{c}\}$ since $x + d \in c + \mathfrak{bq} \subseteq c + \mathfrak{c}$ and thus $c - 1 \in x + (d-1) + \mathfrak{c} = \mathfrak{c}$. Now the definition and the multiplicativity of the norm yield $|\{c \in T \mid c-1 \in \mathfrak{c}\}| = |\mathfrak{cq}/\mathfrak{bq}| = \mathrm{N}(\mathfrak{b})\,\mathrm{N}(\mathfrak{c})^{-1}$. $\square$

Now we are prepared to prove the product formula for $\mu_{\mathfrak{a}}(A)$, which has been stated as Theorem 1.1.

Proof of Theorem 1.1. If $\mu_{\mathfrak{a}}(A) > 0$, then there exists a $B \in UAU$ having $\mathfrak{a}$ as a g.c.d. of the first column. Then $\mathfrak{d}_1(A) = \mathfrak{d}_1(B) \mid \mathfrak{a}$ and $\mathfrak{a} \mid \mathfrak{d}_2(B) = \mathfrak{d}_2(A)$, so Corollary 3.3 is applicable. Thus, using the notation introduced in Corollary 3.3, there exists a $c \in T$ satisfying $\mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)$. So Lemma 3.4 implies $\mathfrak{a}\mathfrak{d}_1(A) \mid \mathfrak{d}_2(A)$, which shows that $\mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}$ is necessary for $\mu_{\mathfrak{a}}(A) > 0$. Thus it is proved that $\mu_{\mathfrak{a}}(A) = 0$ if $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}$ does not hold.

In the following assume $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}$. Denote by $\mathfrak{Q}$ the set of all prime ideals of $\mathfrak{o}$ dividing $\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}$, let $M = \{c \in T \mid \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)\}$ and $M(\mathfrak{c}) = \{c \in T \mid \mathfrak{c} \text{ divides } \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b}\}$ for all ideals $\mathfrak{c}$ of $\mathfrak{o}$. By the inclusion-exclusion principle we then have

$$|M| = \sum_{\mathfrak{M} \subseteq \mathfrak{Q}} (-1)^{|\mathfrak{M}|} \left| M\left(\mathfrak{d}_1(A) \prod_{\mathfrak{q} \in \mathfrak{M}} \mathfrak{q}\right)\right|.$$

If for a product $\mathfrak{q}'$ of pairwise distinct prime ideals $\mathfrak{d}_1(A)\mathfrak{q}' \mid \mathfrak{a} \mid \mathfrak{d}_2(A)(\mathfrak{d}_1(A)\mathfrak{q}')^{-1}$ does not hold, then for $\mathfrak{c} = \mathfrak{d}_1(A)\mathfrak{q}'$ the first or second condition in Lemma 3.4 (ii) is violated, which implies $|M(\mathfrak{c})| = 0$. Since $\mathfrak{d}_1(A)\mathfrak{q}' \mid \mathfrak{a} \mid \mathfrak{d}_2(A)(\mathfrak{d}_1(A)\mathfrak{q}')^{-1}$ is equivalent to $\mathfrak{q}' \mid \mathfrak{a}\mathfrak{d}_1(A)^{-1}$ and $\mathfrak{q}' \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}$, in the above formula $\mathfrak{Q}$ can be replaced by $\mathfrak{Q}'$, where $\mathfrak{Q}'$ denotes the set of all prime ideals of $\mathfrak{o}$ dividing $\mathfrak{a}\mathfrak{d}_1(A)^{-1} + \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}$. In the case where $\mathfrak{q}'$ is a product of pairwise distinct prime ideals in $\mathfrak{Q}'$, the condition $\mathfrak{d}_1(A)\mathfrak{q}' \mid \mathfrak{a} \mid \mathfrak{d}_2(A)(\mathfrak{d}_1(A)\mathfrak{q}')^{-1}$ is satisfied, and Lemma 3.4 and Lemma 3.5 yield $M(\mathfrak{d}_1(A)\mathfrak{q}') = |\{c \in T \mid \mathfrak{d}_1(A)\mathfrak{q}' \text{ divides } c-1\}| = \mathrm{N}(\mathfrak{b})\,\mathrm{N}(\mathfrak{d}_1(A)\mathfrak{q}')^{-1}$. Plugging this into the above formula and using the multiplicativity of the norm and the distributive law, we obtain

$$\begin{aligned} |M| &= \frac{\mathrm{N}(\mathfrak{b})}{\mathrm{N}(\mathfrak{d}_1(A))} \sum_{\mathfrak{M} \subseteq \mathfrak{Q}'} (-1)^{|\mathfrak{M}|}\,\mathrm{N}\left(\prod_{\mathfrak{q} \in \mathfrak{M}} \mathfrak{q}\right)^{-1} = \frac{\mathrm{N}(\mathfrak{b})}{\mathrm{N}(\mathfrak{d}_1(A))} \sum_{\mathfrak{M} \subseteq \mathfrak{Q}'} \prod_{\mathfrak{q} \in \mathfrak{M}} (-\mathrm{N}(\mathfrak{q})^{-1}) \\ &= \frac{\mathrm{N}(\mathfrak{b})}{\mathrm{N}(\mathfrak{d}_1(A))} \prod_{\mathfrak{q} \in \mathfrak{Q}'} (1 - \mathrm{N}(\mathfrak{q})^{-1}). \end{aligned}$$

Since $|M| = \mu_{\mathfrak{a}}(A)$ according to Corollary 3.3 and $\mathfrak{b} = \mathfrak{d}_2(A)\mathfrak{a}^{-1}$, the proof is complete. □

The just-proved formula will be applied in the following.

3.6. **Example.** Let $\mathfrak{o} = \mathbb{Z}$ and $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ as well as $\mathfrak{a} = 2\mathbb{Z}$. Theorem 1.1 then yields

$$\mu_{\mathfrak{a}}(A) = \frac{\mathrm{N}(4\mathbb{Z})}{\mathrm{N}(2\mathbb{Z})\,\mathrm{N}(\mathbb{Z})} \prod_{\substack{\mathfrak{p} \text{ prime ideal} \\ \mathfrak{p} \mid 2\mathbb{Z}}} (1 - \mathrm{N}(\mathfrak{p})^{-1}) = \frac{4}{2 \cdot 1}\left(1 - \frac{1}{2}\right) = 1,$$

which corresponds to the results of Example 3.1, where we had exactly one representative of type $\left(\begin{smallmatrix} 2 & * \\ 0 & * \end{smallmatrix}\right)$, namely $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)$. □

Since Theorem 1.1 is just an intermediate result, more interesting cases than $\mathfrak{o} = \mathbb{Z}$ will not be discussed at this point.

The formula for $\mu_{\mathfrak{a}}(A)$ given in Theorem 1.1 has several applications. Later we will see how it can be used to prove a reduction theorem in the context of Hecke algebras, but for now we will stick to the already announced goal of a formula for the number of right cosets contained in a given double coset. The desired result has already been stated as Theorem 1.2.

Proof of Theorem 1.2. To calculate the number $\mu(A)$ of right cosets with respect to U contained in UAU, we have to sum over all $\mu_{\mathfrak{a}}(A)$. Then we use Theorem 1.1 and rewrite the obtained sum to use $\mathfrak{a}' = \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}$ as a summation index:

$$\begin{aligned}\mu(A) &= \sum_{\mathfrak{a} \text{ ideal in } \mathfrak{o}} \mu_{\mathfrak{a}}(A)\\ &= \sum_{\mathfrak{d}_1(A)|\mathfrak{a}|\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}} \frac{\mathrm{N}(\mathfrak{d}_2(A))}{\mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{d}_1(A))} \prod_{\substack{\mathfrak{p} \text{ prime ideal}\\ \mathfrak{p}|\mathfrak{a}\mathfrak{d}_1(A)^{-1}+\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}}} (1-\mathrm{N}(\mathfrak{p})^{-1})\\ &= \sum_{\mathfrak{o}|\mathfrak{a}'|\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}} \mathrm{N}(\mathfrak{a}') \prod_{\substack{\mathfrak{q} \text{ prime ideal}\\ \mathfrak{q}|(\mathfrak{a}')^{-1}\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}+\mathfrak{a}'}} (1-\mathrm{N}(\mathfrak{q})^{-1}).\end{aligned}$$

Using this equality, we can prove the theorem by showing that

$$S(\mathfrak{b}) := \sum_{\mathfrak{o}|\mathfrak{a}|\mathfrak{b}} \mathrm{N}(\mathfrak{a}) \prod_{\substack{\mathfrak{q} \text{ prime ideal}\\ \mathfrak{q}|\mathfrak{a}^{-1}\mathfrak{b}+\mathfrak{a}}} (1-\mathrm{N}(\mathfrak{q})^{-1}) = \mathrm{N}(\mathfrak{b}) \prod_{\substack{\mathfrak{q} \text{ prime ideal}\\ \mathfrak{q}|\mathfrak{b}}} (1+\mathrm{N}(\mathfrak{q})^{-1})$$

holds for every ideal $\mathfrak{b}$ in $\mathfrak{o}$ (since $\mathfrak{b} = \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}$ yields the assertion). We carry out an induction on the number of prime ideals dividing $\mathfrak{b}$. The initial case $\mathfrak{b} = \mathfrak{o}$ is obvious, so we now assume that there exists a prime ideal $\mathfrak{p}$ which divides $\mathfrak{b}$. Write $\mathfrak{b} = \mathfrak{p}^m\mathfrak{r}$ with $\mathfrak{p} \nmid \mathfrak{r}$. Analogously split up every $\mathfrak{a}$ as the product of a power of $\mathfrak{p}$ and the rest not divided by $\mathfrak{p}$. Introducing the set $\mathfrak{Q}_{\mathfrak{c}}$ of prime ideals dividing $\mathfrak{c}^{-1}\mathfrak{b}+\mathfrak{c}$, we then have

$$S(\mathfrak{b}) = \sum_{\mathfrak{o}|\mathfrak{a}|\mathfrak{b}} \mathrm{N}(\mathfrak{a}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{a}}} (1-\mathrm{N}(\mathfrak{q})^{-1}) = \sum_{k=0}^{m} \sum_{\mathfrak{o}|\mathfrak{c}|\mathfrak{r}} \mathrm{N}(\mathfrak{p}^k\mathfrak{c}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{p}^k\mathfrak{c}}} (1-\mathrm{N}(\mathfrak{q})^{-1}).$$

If $\mathfrak{p} \nmid \mathfrak{c}$ and $\mathfrak{q}$ is a prime ideal in $\mathfrak{o}$, the definition of $\mathfrak{Q}_{\mathfrak{p}^k\mathfrak{c}}$ yields

$$\mathfrak{q} \in \mathfrak{Q}_{\mathfrak{p}^k\mathfrak{c}} \quad \Leftrightarrow \quad (\mathfrak{q} = \mathfrak{p} \text{ and } 1 \le k < m) \text{ or } (\mathfrak{q} \ne \mathfrak{p} \text{ and } \mathfrak{q} \in \mathfrak{Q}_c).$$

Using this equivalence in the above expression for $S(\mathfrak{b})$, by splitting up the outer sum we obtain

$$\begin{aligned}S(\mathfrak{b}) = &\sum_{k=1}^{m-1} \sum_{\mathfrak{o}|\mathfrak{c}|\mathfrak{r}} \mathrm{N}(\mathfrak{p})^k\,\mathrm{N}(\mathfrak{c})(1-\mathrm{N}(\mathfrak{p})^{-1}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{c}}} (1-\mathrm{N}(\mathfrak{q})^{-1})\\ &+ \sum_{\mathfrak{o}|\mathfrak{c}|\mathfrak{r}} \mathrm{N}(\mathfrak{c}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{c}}} (1-\mathrm{N}(\mathfrak{q})^{-1}) + \sum_{\mathfrak{o}|\mathfrak{c}|\mathfrak{r}} \mathrm{N}(\mathfrak{p})^m\,\mathrm{N}(\mathfrak{c}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{c}}} (1-\mathrm{N}(\mathfrak{q})^{-1}).\end{aligned}$$

Since the double sum on the right-hand side is a telescoping sum, the equation simplifies to

$$\begin{aligned}S(\mathfrak{b}) &= \sum_{\mathfrak{o}|\mathfrak{c}|\mathfrak{r}} \mathrm{N}(\mathfrak{p})^{m-1}\,\mathrm{N}(\mathfrak{c}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{c}}} (1-\mathrm{N}(\mathfrak{q})^{-1}) + \sum_{\mathfrak{o}|\mathfrak{c}|\mathfrak{r}} \mathrm{N}(\mathfrak{p})^m\,\mathrm{N}(\mathfrak{c}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{c}}} (1-\mathrm{N}(\mathfrak{q})^{-1})\\ &= \mathrm{N}(\mathfrak{p})^m(1+\mathrm{N}(\mathfrak{p})^{-1}) \sum_{\mathfrak{o}|\mathfrak{c}|\mathfrak{r}} \mathrm{N}(\mathfrak{c}) \prod_{\mathfrak{q}\in\mathfrak{Q}_{\mathfrak{c}}} (1-\mathrm{N}(\mathfrak{q})^{-1})\\ &= \mathrm{N}(\mathfrak{p})^m(1+\mathrm{N}(\mathfrak{p})^{-1})S(\mathfrak{r}).\end{aligned}$$

Applying the induction hypothesis, we have

$$S(\mathfrak{b}) = \mathrm{N}(\mathfrak{p})^m(1+\mathrm{N}(\mathfrak{p})^{-1})S(\mathfrak{r}) = \mathrm{N}(\mathfrak{p})^m(1+\mathrm{N}(\mathfrak{p})^{-1})\,\mathrm{N}(\mathfrak{r}) \prod_{\substack{\mathfrak{q}\text{ prime ideal}\\ \mathfrak{q}\mid\mathfrak{r}}} (1+\mathrm{N}(\mathfrak{q})^{-1})$$

$$= \mathrm{N}(\mathfrak{b}) \prod_{\substack{\mathfrak{q}\text{ prime ideal}\\ \mathfrak{q}\mid\mathfrak{b}}} (1+\mathrm{N}(\mathfrak{q})^{-1}),$$

which completes the proof. □

In the following examples Theorem 1.2 is applied in a case where $\mathfrak{o}$ is not a principal ideal domain.

3.7. **Examples.** Let $\mathfrak{o} = \mathbb{Z}+\mathbb{Z}\omega$, where $\omega = \sqrt{-5}$ and $A = \left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)$. Since $3\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 = 3\mathfrak{o}+(\omega+1)\mathfrak{o}$ and $\mathfrak{p}_2 = 3\mathfrak{o}+(\omega+2)\mathfrak{o}$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of norm 3 in $\mathfrak{o}$, Theorem 1.2 yields

$$\mu(A) = \mathrm{N}(3\mathfrak{o}) \prod_{\substack{\mathfrak{p}\text{ prime ideal}\\ \mathfrak{p}\mid 3\mathfrak{o}}} (1+\mathrm{N}(\mathfrak{p})^{-1}) = 9\left(1+\frac{1}{3}\right)\left(1+\frac{1}{3}\right) = 16.$$

Since $2\mathfrak{o}$ has the prime ideal decomposition $(2\mathfrak{o}+(\omega+1)\mathfrak{o})^2$, one similarly obtains $\mu(\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)) = 6$. Possible choices for the six representatives are calculated in Example 5.4.

The above examples can be generalised: If $\mathfrak{o}$ is a quadratic number field and p a rational prime, we have $\mu(\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)) = (p+1)^2$ if p is split and $\mu(\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)) = p(p+1)$ otherwise. □

To complete this section, already existing results similar to Theorem 1.2 are shortly reviewed in the following.

3.8. *Remark.* In the case $\mathfrak{o} = \mathbb{Z}$ we have a so-called rationality theorem for abstract Hecke algebras with respect to unimodular groups (see e.g. [4], Theorem V (9.3)). The proof of this theorem uses the fact that the double coset $\mathrm{GL}_n(\mathbb{Z})P_j\,\mathrm{GL}_n(\mathbb{Z})$, where P_j is a diagonal matrix with j diagonal entries equal to p (for a fixed rational prime p) and the other diagonal entries equal to 1, decomposes into exactly

$$p^{-\frac{j(j+1)}{2}} \sum_{1\le v_1<\cdots<v_j\le n} p^{v_1+\cdots+v_j}$$

right cosets with respect to $\mathrm{GL}_n(\mathbb{Z})$. (One easily checks that for $n=2$ and $j\in\{0,1,2\}$, this yields the same values for $\mu(P_j)$ as Theorem 1.2.)

Another similar theorem does not count right cosets in double cosets but right cosets in the set of all matrices with the same determinant (modulo units). According to [11], Theorem II.4, the set $\{A\in\mathfrak{o}^{n\times n} \mid \det A \in d\mathfrak{o}^*\}$ decomposes into exactly

$$\prod_{\substack{p\in P\\ p\mid d}} \prod_{j=1}^{n-1} \frac{\mathrm{N}(p)^{\mathrm{v}_{p\mathfrak{o}}(d)+j}-1}{\mathrm{N}(p)^j-1}$$

right cosets with respect to $\mathrm{GL}_n(\mathfrak{o})$ (where P denotes a system of representatives of prime elements in $\mathfrak{o}$ modulo $\mathfrak{o}^*$). □

4. Applications to congruence subgroups

In this short section, an application of Theorem 1.2 to the calculation of indexes of certain congruence subgroups is presented. The result has already been stated as Corollary 1.3.

Proof of Corollary 1.3. Let $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right)$. A simple calculation using $A\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)A^{-1} = \left(\begin{smallmatrix} a & m^{-1}b \\ mc & d \end{smallmatrix}\right)$ shows that $U \cap A^{-1}UA = U^0[m]$. Since $[U : U \cap A^{-1}UA] = \mu(A)$ (see e.g. [12], Lemma 3.1.2), the assertion immediately follows from Theorem 1.2. □

4.1. *Remark.* Corollary 1.3 generalises a similar formula for the index of congruence subgroups in $\mathrm{SL}_2(\mathbb{Z})$ which is of interest in the theory of modular forms (see e.g. [13], Section 1.2). However, such index formulae are also studied in other contexts (see e.g. [14]). □

5. Applications to Hecke algebras

As has already been mentioned, Theorem 1.2 has been developed with the theory of Hecke algebras in mind. The applications in this field will be presented here.

Denote by H the complex vector space spanned by $\{1_{UAU} \mid A \in I\}$ where $1_M : G \to \{0,1\}$ is the characteristic function of the set M. For $A, A_1, \ldots, A_k, B, B_1, \ldots, B_m \in I$ with $UAU = UA_1 \cup \cdots \cup UA_k$ and $UBU = UB_1 \cup \cdots \cup UB_m$, where the unions are pairwise disjoint, define

$$1_{UAU} * 1_{UBU} = \sum_{k=1}^{k} \sum_{j=1}^{m} 1_{UA_iB_j}$$

and extend this operation bilinearly to a (well-defined(!)) operation on H. The obtained algebra is called an (abstract) Hecke algebra; for details see e.g. [4]. The formula

$$(1_{UAU} * 1_{UBU})(C) = |\{(i,j) \mid A_iB_j \in UC,\ 1 \le i \le k,\ 1 \le j \le m\}|,$$

which can be found in [4], I.4.4, immediately yields an algorithm for the calculation of $1_{UAU} * 1_{UBU}$.

5.1. **Algorithm.** *Input: $A, B \in I$; output: $D \subseteq I$ and $c_C \in \mathbb{N}$ for every $C \in D$ such that*

$$1_{UAU} * 1_{UBU} = \sum_{C \in D} c_C 1_{UCU}.$$

(1) Decompose UAU and UBU into pairwise disjoint right cosets $UA_1, \ldots, UA_k$ and $UB_1, \ldots, UB_m$, respectively.
(2) Let $D = \emptyset$.
(3) For every pair (i,j) with $1 \le i \le k$ and $1 \le j \le m$, test whether there exists a $C' \in D$ with $UA_iB_jU = UC'U$. If this is not the case, add the element A_iB_j to D and set $c_{A_iB_j} = 1$; otherwise, if additionally $UC' = UA_iB_j$ is fulfilled, increase $c_{C'}$ by 1. □

For the execution of this algorithm, a right coset decomposition of UAU and UBU has to be constructed explicitly in step (1). Using Theorem 1.2 we can give an algorithm that carries out this task.

5.2. **Algorithm.** *Input: $A \in I$ and an enumeration $(Q_n)_{n \in \mathbb{N}}$ of U; output: right transversal R of $U \setminus UAU$.*

(1) Calculate $k = \mu(A)$ (using Theorem 1.2).
(2) Set $R = \{A\}$ and $n = 1$.
(3) If there exists no $B \in R$ with $UAQ_n = UB$, add the element AQ_n to R.
(4) If $|R| < k$, increase n by 1 and go back to (3); otherwise stop. □

5.3. *Remark.* In order to implement Algorithm 5.2, we have to enumerate all elements of U, which might not be feasible. To avoid this problem, one can use random elements instead of enumerated elements for Q_n. Then Algorithm 5.2 is turned into a probabilistic algorithm which produces the desired output if it terminates. The remaining problem of the generation of random unimodular matrices will not be discussed here but is delegated to Sage ([15]).

Another idea for the implementation of an algorithm for the construction of a right transversal is to use Lemma 3.2: With the notation of Lemma 3.2, run over all possible $\mathfrak{a}$ and $c \in T$ and verify whether the given representative is an element of UAU by checking the determinantal divisors. However, Algorithm 5.2 seems to be easier to implement. □

Using Algorithm 5.2 and Remark 5.3, we can calculate some

5.4. **Examples.** Let $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\omega$ for $\omega = \sqrt{-5}$. For $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ the probabilistic decomposition algorithm terminates after an average of 14 loop cycles and yields for example

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & \omega \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1+\omega \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1+\omega & 1 \end{pmatrix} \right\}$$

as a system of representatives of $U\backslash UAU$ (with 6 elements according to Examples 3.7). With this transversal it is then possible to use Algorithm 5.1 to calculate $1_{UAU} * 1_{UAU}$; one obtains

$$1_{UAU} * 1_{UAU} = 1_{UA_1U} + 6 \cdot 1_{UA_2U} + 1_{UA_3U},$$

with $A_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ and $A_2 = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ as well as $A_3 = \left(\begin{smallmatrix} 2 & 1+\omega \\ 0 & 2 \end{smallmatrix}\right)$.

In order to get a feeling for the complexity of the decomposition algorithm (a detailed analysis has to take into account the strategy for choosing the elements of U and will not be carried out in this paper), we execute this algorithm for some more A and obtain the following table:

A	$\mathfrak{d}_1(A)$	$\mathfrak{d}_2(A)$	$\mu(A)$	avg. loop cycles
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$	$\mathfrak{o}$	$2\mathfrak{o}$	6	14
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1+\omega \end{smallmatrix}\right)$	$\mathfrak{o}$	$(\omega+1)\mathfrak{o}$	12	39
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right)$	$\mathfrak{o}$	$3\mathfrak{o}$	16	53
$\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)$	$\mathfrak{o}$	$4\mathfrak{o}$	24	110
$\left(\begin{smallmatrix} \omega & 1 \\ 0 & \omega \end{smallmatrix}\right)$	$\mathfrak{o}$	$5\mathfrak{o}$	30	130
$\left(\begin{smallmatrix} \omega & 1 \\ 1 & 2 \end{smallmatrix}\right)$	$\mathfrak{o}$	$(1+2\omega)\mathfrak{o}$	32	124
$\left(\begin{smallmatrix} \omega & 0 \\ 0 & 2 \end{smallmatrix}\right)$	$\mathfrak{o}$	$2\omega\mathfrak{o}$	36	171

□

After these algorithmic applications, the remaining part of this article will deal with the reduction theorem announced in the introduction. First, an auxiliary result has to be proved.

5.5. **Lemma.** *For all $f \in H$ define $\mu_{\mathfrak{o}}(f) = \sum_{A\in R} f(A)\cdot\mu_{\mathfrak{o}}(A)$, where R is a system of representatives of $U\backslash I/U$. Then $\mu_{\mathfrak{o}}(f * g) = \mu_{\mathfrak{o}}(f)\mu_{\mathfrak{o}}(g)$ for all $f, g \in H$.* □

Proof. By the definition of $\mu_{\mathfrak{o}}$ and $*$ it suffices to prove the assertion for $f = 1_{UAU}$ and $g = 1_{UBU}$, where $A, B \in I$. For $C \in I$ with $(1_{UAU} * 1_{UBU})(C) \neq 0$ we have $C \in UAUBU$ by the definition of $*$, and [10], Theorem 3.1 yields $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{d}_1(C)$ and thus $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{g}(C)$. This implies that in the case $\mathfrak{d}_1(A) \neq \mathfrak{o}$ or $\mathfrak{d}_1(B) \neq \mathfrak{o}$ both sides of the equation $\mu_{\mathfrak{o}}(1_{UAU} * 1_{UBU}) = \mu_{\mathfrak{o}}(1_{UAU})\mu_{\mathfrak{o}}(1_{UBU})$ evaluate to zero, so it remains to analyse the case $\mathfrak{d}_1(A) = \mathfrak{o} = \mathfrak{d}_1(B)$. In this case let $A_1, \dots, A_k$ and $B_1, \dots, B_m$ be systems of representatives of $U\backslash UAU$ and $U\backslash UBU$, respectively, where the B_j with $\mathfrak{g}(B_j) = \mathfrak{o}$ have the form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ (without loss of generality due to Corollary 2.2). Let $1 \leq i \leq k$ and $1 \leq j \leq m$. If $\mathfrak{g}(B_j) \neq \mathfrak{o}$, then $\mathfrak{g}(A_iB_j) \neq \mathfrak{o}$ since the first column of A_iB_j consists of linear combinations of entries of the first column of B_j. If $\mathfrak{g}(B_j) = \mathfrak{o}$, then the special structure of B_j yields that the first column of A_iB_j equals the first column of A_i. So we have $\mathfrak{g}(A_iB_j) = \mathfrak{o}$ if and only if $\mathfrak{g}(A_i) = \mathfrak{o}$ and $\mathfrak{g}(B_j) = \mathfrak{o}$. Since according to the definition of $\mu_{\mathfrak{o}}$ and $*$ we have

$$\mu_{\mathfrak{o}}(1_{UAU} * 1_{UBU}) = |\{(i,j) \mid \mathfrak{g}(A_iB_j) = \mathfrak{o},\ 1 \leq i \leq k,\ 1 \leq j \leq m\}|,$$

the just-proved characterisation of $\mathfrak{g}(A_iB_j) = \mathfrak{o}$ used to split up the right-hand side as a product of two cardinalities yields the assertion. □

Now the desired reduction theorem can be stated and proved.

5.6. **Theorem.** *Let $a, b, c \in \mathfrak{o}$ and $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right)$ as well as $C = \left(\begin{smallmatrix} 1 & 0 \\ 0 & c \end{smallmatrix}\right)$. Then $(1_{UAU} * 1_{UBU})(C) = 1$ if $c \in ab\mathfrak{o}^*$, and $(1_{UAU} * 1_{UBU})(C) = 0$ otherwise.* □

Proof. With R as in Lemma 5.5 write

$$\begin{aligned}\mu_{\mathfrak{o}}(1_{UAU} * 1_{UBU}) &= \sum_{D\in R} (1_{UAU} * 1_{UBU})(D) \cdot \mu_{\mathfrak{o}}(D) \\ &= \sum_{\substack{D\in R \\ D\notin UABU}} (1_{UAU} * 1_{UBU})(D) \cdot \mu_{\mathfrak{o}}(D) \\ &\quad + (1_{UAU} * 1_{UBU})(AB) \cdot \mu_{\mathfrak{o}}(AB).\end{aligned}$$

Using Lemma 5.5, Theorem 1.1 and the multiplicativity of the norm, we have

$$\begin{aligned}\mu_{\mathfrak{o}}(1_{UAU} * 1_{UBU}) &= \mu_{\mathfrak{o}}(1_{UAU})\mu_{\mathfrak{o}}(1_{UBU}) \\ &= \mathrm{N}(\mathfrak{d}_2(A))\,\mathrm{N}(\mathfrak{d}_2(B)) = \mathrm{N}(\mathfrak{d}_2(AB)) = \mu_{\mathfrak{o}}(AB),\end{aligned}$$

so

$$\sum_{\substack{D\in R \\ D\notin UABU}} (1_{UAU} * 1_{UBU})(D) \cdot \mu_{\mathfrak{o}}(D) + (1_{UAU} * 1_{UBU})(AB) \cdot \mu_{\mathfrak{o}}(AB) = \mu_{\mathfrak{o}}(AB).$$

Since all numbers in this equation are nonnegative integers and $(1_{UAU} * 1_{UBU})(AB) \geq 1$ by the definition of $*$, we have $(1_{UAU} * 1_{UBU})(AB) = 1$ and $(1_{UAU} * 1_{UBU})(D) \cdot \mu_{\mathfrak{o}}(D) = 0$ for all $D \in R$ with $D \notin UABU$. Since $\mu_{\mathfrak{o}}(C) \geq 1$ as $\mathfrak{g}(C) = \mathfrak{o}$, these equations imply $(1_{UAU} * 1_{UBU})(C) = 0$ if $C \notin UABU$ and $(1_{UAU} * 1_{UBU})(C) = 1$ if $C \in UABU$, where the latter condition is equivalent to $c \in ab\mathfrak{o}^*$, which proves the assertion. □

References

[1] L. J. Mordell. On Mr. Ramanujan's Empirical Expansions of Modular Functions. *Proc. Cambridge Phil. Soc.*, 19:117–124, 1917.

[2] Ken Ono. Hecke operators and the q-expansion of modular forms. In *CRM Proceedings & Lecture Notes*, volume 36, pages 229–235. American Mathematical Society (AMS), Providence, RI, 2004. MR2076599 (2005d:11063)

[3] Suzanne Caulk and Lynne H. Walling. Hecke operators on Hilbert-Siegel modular forms. *Int. J. Number Theory*, 3(3):391–420, 2007. MR2352827 (2009b:11083)

[4] Aloys Krieg. Hecke algebras. *Mem. Am. Math. Soc.*, 435:158, 1990. MR1027069 (90m:16024)

[5] Aloys Krieg. The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions. *Proc. Indian Acad. Sci., Math. Sci. (Ramanujan Birth Centenary Volume)*, 97(1-3):201–229, 1987. MR983615 (90b:11048)

[6] Martin Raum. Hecke algebras related to the unimodular and modular groups over quadratic field extensions and quaternion algebras. *Proc. Am. Math. Soc.*, 139(4):1321–1331, 2011. MR2748425 (2011k:11067)

[7] Aloys Krieg. *Modular forms on half-spaces of quaternions.* Lecture Notes in Mathematics. 1143. Berlin: Springer-Verlag. XIII, 203 pp., 1985. MR807947 (87f:11033)

[8] A. Fröhlich and M.J. Taylor. *Algebraic number theory.* Cambridge Studies in Advanced Mathematics. 27. Cambridge (UK): Cambridge University Press. xiv, 355 pp., 1990. MR1215934 (94d:11078)

[9] E. Steinitz. Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. I. *Math. Ann.*, 71:328–354, 1912. MR1511661

[10] Marc Ensenbach. Determinantal divisors of products of matrices over Dedekind domains. *Linear Algebra Appl.*, 432(11):2739–2744, 2010. MR2639239 (2011h:15009)

[11] Morris Newman. *Integral matrices.* Pure and Applied Mathematics, 45. New York-London: Academic Press. XVII, 224 pp., 1972. MR0340283 (49:5038)

[12] Anatolij N. Andrianov. *Quadratic forms and Hecke operators.* Grundlehren der Mathematischen Wissenschaften, 286. Berlin: Springer-Verlag. XII, 374 pp., 1987. MR884891 (88g:11028)

[13] Fred Diamond and Jerry Shurman. *A first course in modular forms.* Graduate Texts in Mathematics 228. Berlin: Springer. xv, 436 pp., 2005. MR2112196 (2006f:11045)

[14] Daniel Appel and Evija Ribnere. On the index of congruence subgroups of $\mathrm{Aut}(F_n)$. *J. Algebra*, 321(10):2875–2889, 2009. MR2512632 (2010d:20039)

[15] W. A. Stein et al. *Sage Mathematics Software (Version 4.6).* The Sage Development Team, 2010. `http://www.sagemath.org`.

Department of Mathematics, University of Siegen, 57068 Siegen, Germany
E-mail address: `ensenbach@mathematik.uni-siegen.de`