Sets of lengths in maximal orders in central simple algebras

Daniel Smertnig

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstraße 36, 8010 Graz, Austria

ARTICLE INFO

Article history:
Received 6 December 2012
Available online 14 June 2013
Communicated by Michel Broué

MSC:
16H10
16U30
20M12
20M13
11R54

Keywords:
Sets of lengths
Maximal orders
Global fields
Brandt groupoid
Divisorial ideals
Krull monoids

ABSTRACT

Let \( \mathcal{O} \) be a holomorphy ring in a global field \( K \), and \( R \) a classical maximal \( \mathcal{O} \)-order in a central simple algebra over \( K \). We study sets of lengths of factorizations of cancellative elements of \( R \) into atoms (irreducibles). In a large majority of cases there exists a transfer homomorphism to a monoid of zero-sum sequences over a ray class group of \( \mathcal{O} \), which implies that all the structural finiteness results for sets of lengths—valid for commutative Krull monoids with finite class group—hold also true for \( R \). If \( \mathcal{O} \) is the ring of algebraic integers of a number field \( K \), we prove that in the remaining cases no such transfer homomorphism can exist and that several invariants dealing with sets of lengths are infinite.

© 2013 The Author. Published by Elsevier Inc. All rights reserved.

1. Introduction

Let \( H \) be a (left- and right-) cancellative semigroup and \( H^\times \) its group of units. An element \( u \in H \setminus H^\times \) is called irreducible (or an atom) if \( u = ab \) with \( a, b \in H \) implies that \( a \in H^\times \) or \( b \in H^\times \). If \( a \in H \setminus H^\times \), then \( l \in \mathbb{N} \) is a length of \( a \) if there exist atoms \( u_1, \ldots, u_l \in H \) with \( a = u_1 \cdots u_l \), and the set of lengths of \( a \), written as \( L(a) \), consists of all such lengths. If there is a non-unit \( a \in H \) with
This gives rise to the construction of a transfer homomorphism \( \theta : H \rightarrow B(G_P) \), where \( B(G_P) \) is the monoid of zero-sum sequences over a subset \( G_P \) of the class group \( G \) of \( H \). Transfer homomorphisms preserve sets of lengths, and if \( G_P \) is finite, then \( B(G_P) \) is a finitely generated commutative Krull monoid, whose sets of lengths can be studied with methods from combinatorial number theory. This approach has lead to a large variety of structural results for sets of lengths in commutative Krull monoids (see [27,24] for an overview).

Only first hesitant steps were taken so far to study factorization properties in a non-commutative setting (for example, quaternion orders are investigated in [19,18,16], semifirs in [14,15], semigroup algebras in [37]). The present paper provides an in-depth study of sets of lengths in classical maximal orders over holomorphy rings in global fields.

Let \( \mathcal{O} \) be a commutative Krull domain with quotient field \( K \), \( A \) a central simple algebra over \( K \), \( R \) a maximal order in \( A \), and \( R^* \) the semigroup of cancellative elements (equivalently, \( R \) is a PI Krull ring). Any approach to study sets of lengths, which runs as described above and involves divisorial two-sided ideals, is restricted to normalizing Krull monoids [25, Theorem 4.13]. For this reason we develop the theory of divisorial one-sided ideals. In Section 3 we fix our terminology in the setting of cancellative small categories. Following ideas of Asano and Murata [5] and partly of Rehm [45,46], we provide in Section 4 a factorization theory of integral elements in arithmetical groupoids, and introduce an abstract transfer homomorphism for a subcategory of such a groupoid (Theorem 4.15). In Section 5 the divisorial one-sided ideal theory of maximal orders in quotient semigroups is given, and Proposition 5.16 establishes the relationship with arithmetical groupoids. Theorem 5.23 is a main result in the abstract setting of arithmetical maximal orders (Remarks 5.17.2 and 5.24.1 reveal how the well-known transfer homomorphisms for normalizing Krull monoids fit into our abstract theory).

For maximal orders over commutative Krull domains, we see that all sets of lengths are finite and non-empty (Corollary 5.30). In Section 6 we demonstrate that classical maximal orders over holomorphy rings in global fields fulfill the abstract assumptions of Theorem 5.23, which implies the following structural finiteness results on sets of lengths.

**Theorem 1.1.** Let \( \mathcal{O} \) be a holomorphy ring in a global field \( K \), \( A \) a central simple algebra over \( K \), and \( R \) a classical maximal \( \mathcal{O} \)-order of \( A \). Suppose that every stably free left \( R \)-ideal is free. Then there exists a transfer homomorphism \( \theta : R^* \rightarrow B(C_A(\mathcal{O})) \), where

\[
C_A(\mathcal{O}) = F^x(\mathcal{O}) \backslash \{ a\mathcal{O} \mid a \in K^x, a_v > 0 \text{ for all archimedean places } v \text{ of } K \text{ where } A \text{ is ramified} \}
\]

is a ray class group of \( \mathcal{O} \), and \( B(C_A(\mathcal{O})) \) is the monoid of zero-sum sequences over \( C_A(\mathcal{O}) \). In particular,

1. The set of distances \( \Delta(R^*) \) is a finite interval, and if it is non-empty, then \( \min \Delta(R^*) = 1 \).
2. For every \( k \in \mathbb{N} \), the union of sets of lengths containing \( k \), denoted by \( l_k(R^*) \), is a finite interval.
3. There is an \( M \in \mathbb{N}_0 \) such that for every \( a \in R^* \) the set of lengths \( L(a) \) is an AAMP with difference \( d \in \Delta(R^*) \) and bound \( M \).

Thus, under the additional hypothesis that every stably free left \( R \)-ideal is free, we obtain a transfer homomorphism to a monoid of zero-sum sequences over a finite abelian group. Therefore, sets of lengths in \( R \) are the same as sets of lengths in a commutative Krull monoid with finite class group.
If $A$ satisfies the Eichler condition relative to $O$, then every stably free left $R$-ideal is free by Eichler’s Theorem. In particular, if $K$ is a number field and $O$ is its ring of algebraic integers, then $A$ satisfies the Eichler condition relative to $O$ unless $A$ is a totally definite quaternion algebra. Thus in this setting Theorem 1.1 covers the large majority of cases, and the following complementary theorem shows that the condition that every stably free left $R$-ideal is free is indeed necessary.

**Theorem 1.2.** Let $O$ be the ring of algebraic integers in a number field $K$, $A$ a central simple algebra over $K$, and $R$ a classical maximal $O$-order of $A$. If there exists a stably free left $R$-ideal that is not free, then there exists no transfer homomorphism $\theta : R^* \to B(G_P)$, where $G_P$ is any subset of an abelian group. Moreover,

1. $\Delta(R^*) = \mathbb{N}$.
2. For every $k \geq 3$, we have $\mathbb{N}_{\geq 3} \subset U_k(R^*) \subset \mathbb{N}_{\geq 2}$.

The proof of Theorem 1.2 is based on recent work of Kirschmer and Voight [39,40], and will be given in Section 7. If $H$ is a commutative Krull monoid with an infinite class group such that every class contains a prime divisor, then Kainrath showed that every finite subset of $\mathbb{N}_{\geq 2}$ can be realized as a set of lengths ([38], or [27, Section 7.4]), whence $\Delta(H) = \mathbb{N}$ and $U_k(H) = \mathbb{N}_{\geq 2}$ for all $k \geq 2$. However, we explicitly show that in the above situation no transfer homomorphism is possible, implying that the factorization of $R^*$ cannot be modeled by a monoid of zero-sum sequences. A similar statement about sets of lengths in the integer-valued polynomials, as well as the impossibility of a transfer homomorphism to a monoid of zero-sum sequences, was recently shown by Frisch [21].

2. Preliminaries

Let $\mathbb{N}$ denote the set of positive integers and put $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$. For integers $a, b \in \mathbb{Z}$, let $[a, b] = \{x \in \mathbb{Z} | a \leq x \leq b\}$ denote the discrete interval. All semigroups and rings are assumed to have an identity element, and all homomorphisms respect the identity. By a factorization we always mean a factorization of a cancellative element into irreducible elements (a formal definition follows in Section 3). In order to study factorizations in semigroups we will have to investigate their divisorial one-sided ideal theory, in which the multiplication of ideals only gains sufficiently nice properties if one considers it as a partial operation that is only defined for certain pairs of ideals. This is the reason why we introduce our concepts in the setting of groupoids and consider subcategories of these groupoids.

Throughout the paper there will be many statements that can be either formulated “from the left” or “from the right”, and most of the time it is obvious how the symmetric statement should look like. Therefore often just one variant is formulated and it is left to the reader to fill in the symmetric definition or statement if required.

2.1. Small categories as generalizations of semigroups

Let $H$ be a small category. In the sequel the objects of $H$ play no role, and therefore we shall identify $H$ with the set of morphisms of $H$. We denote by $H_0$ the set of identity morphisms (representing the objects of the category). There are two maps $s, t : H \to H_0$ such that two elements $a, b \in H$ are composable to a (uniquely determined) element $ab \in H$ if and only if $t(a) = s(b)$. For $e, f \in H_0$ we set $H(e, f) = \{a \in H | s(a) = e, t(a) = f\}$, $H(e) = H(e, e)$, $H(e, \cdot) = \bigcup f \in H_0 H(e, f')$ and $H(\cdot, f) = \bigcup e \in H_0 H(e', f)$. Note that an element $e \in H$ lies in $H_0$ if and only if $s(e) = t(e) = e, ea = a$ for all $a \in H(e, \cdot)$ and $ae = a$ for all $a \in H(\cdot, e)$.

A semigroup may be viewed as a category with a single object (corresponding to its identity element), and elements of the semigroup as morphisms with source and target this unique object. In this way the notion of a small category generalizes the usual notion of a semigroup ($H$ is a semigroup

---

$\cdot$ This choice of $t$ and $s$ is compatible with the usual convention for groupoids, but unfortunately opposite to the usual convention for categories.
if and only if $|H_0| = 1$. We will consider a semigroup to be a small category in this sense whenever this is convenient, without explicitly stating this anymore. For $A, B \subset H$ we write $AB = \{ab \in H \mid a \in A, b \in B \}$ for the set of all possible products, and if $b \in H$, then $Ab = A\{b\}$ and $bA = \{b\}A$.

An element $a \in H$ is called left-cancellative if it is an epimorphism ($ab = ac$ implies $b = c$ for all $b, c \in H(t(a), \ldots)$), and it is called right-cancellative if it is a monomorphism ($ba = ca$ implies $b = c$ for all $b, c \in H(\ldots, s(a))$, and cancellative if it is both. The set of all cancellative elements is denoted by $H^*$, and $H$ is called cancellative if $H = H^*$. The set of isomorphisms of $H$ will also be called the set of units, and we denote it by $H^\times$. A subcategory $D \subset H$ is wide if $D_0 = H_0$.

In line with the multiplicative notation, if $H$ and $D$ are two small categories, we call a functor $f : H \to D$ a homomorphism (of small categories). Explicitly, a map $f : H \to D$ is a homomorphism if $f(H_0) \subset D_0$ and whenever $a, b \in H$ with $t(a) = s(b)$ then also $f(a) \cdot f(b)$ is defined (i.e., $t(f(a)) = s(f(b))$) and $f(ab) = f(a)f(b)$.

If $H$ is a commutative semigroup, and $D \subset H$ is a subsemigroup, then a localization $\sim^{-1}H$ with an embedding $H \hookrightarrow \sim^{-1}H$ exists whenever all elements of $D$ are cancellative, and in particular $H$ has a group of fractions if and only if $H$ is cancellative. If $H$ is a non-commutative semigroup and $D \subset H$, then a semigroup of right fractions with respect to $D$, $HD^{-1}$, in which every element can be represented as a fraction $ad^{-1}$ with $a \in H, d \in D$, together with an embedding $H \hookrightarrow HD^{-1}$, exists if and only if $D$ is cancellative and $D$ satisfies the right Ore condition, meaning $aD \cap bD \neq \emptyset$ for all $a \in H$ and $d \in D$. For a semigroup of left fractions, $D^{-1}H$, one gets the analogous left Ore condition, and if $D$ satisfies both, the left and the right Ore condition, then every semigroup of right fractions is a semigroup of left fractions and conversely. In this case we write $\sim^{-1}H = HD^{-1}$. If $H^*$ satisfies the left and right Ore condition, we also write $\mathfrak{q}(H) = H(H^*)^{-1} = (H^*)^{-1}H$ for the corresponding semigroup of fractions.

The notion of semigroups of fractions generalizes to categories of fractions with analogous conditions [23]. Let $H$ be a small category, and $D \subset H^*$ a subset of the cancellative elements. Then $D$ admits a calculus of right fractions if $D$ is a wide subcategory of $H$ and it satisfies the right Ore condition, i.e., $aD \cap bD \neq \emptyset$ for all $a \in H$ and $d \in D$ with $s(a) = s(d)$. In that case there exists a small category $HD^{-1}$ with $(HD^{-1})_0 = H_0$ and an embedding $j : H \to HD^{-1}$ (i.e., $j$ is a faithful functor) with $j | H_0 = \text{id}$ and such that every element of $HD^{-1}$ can be represented in the form $j(a)j(d)^{-1}$ with $a \in H, d \in D$ and $t(a) = t(d), j(D) \subset H^\times$ and it is universal with respect to that property, i.e., if $f : H \to S$ is any homomorphism with $f(D) \subset S^\times$, then there exists a unique $D^{-1}f : HD^{-1} \to S$ such that $D^{-1}f \circ j = f$. We can assume $H \subset HD^{-1}$ and take $j$ to be the inclusion map, and we call $HD^{-1}$ the category of right fractions of $H$ with respect to $D$. If $D$ also admits a left calculus of fractions, then $HD^{-1}$ is also a category of left fractions, and we write $HD^{-1} = D^{-1}H$.

A monoid is a cancellative semigroup satisfying the left and right Ore condition (following the convention of [25]). Every monoid has a (left and right) group of fractions which is unique up to isomorphism. A semigroup $H$ is called normalizing if $aH = Ha$ for all $a \in H$. It is easily checked that a normalizing cancellative semigroup is already a normalizing monoid.

Let $M$ be a directed multigraph (i.e., a quiver). For every edge $a$ of $M$ we write $s(a)$ for the vertex that is its source and $t(a)$ for the vertex that is its target. The path category on $M$, denoted by $\mathcal{F}(M)$, is defined as follows: It consists of all tuples $(e, a_1, \ldots, a_k, f)$ with $k \in \mathbb{N}_0$, $e, f$ vertices of $M$ and $a_1, \ldots, a_k$ edges of $M$ with either $k = 0$ and $e = f$ or $k > 0$, $s(a_1) = e$, $t(a_1) = s(a_{k+1})$ for all $i \in [1, k - 1]$ and $t(a_k) = f$. The set of identities $\mathcal{F}(M)_0$ is the set of all tuples with $k = 0$, and given any tuple $y$ as above, $s(y) = (e, e)$ and $t(y) = (f, f)$. Composition is defined in the obvious manner by concatenating tuples and removing the two vertices in the middle. We identify the set of vertices of $M$ with $\mathcal{F}(M)_0$ so that $(e, e) = e$. Every subset $M$ of a small category $H$ will be viewed as a quiver, with vertices $\{s(a) \mid a \in M\} \cup \{t(a) \mid a \in M\}$ and for each $a \in M$ a directed edge (again called $a$) from $s(a)$ to $t(a)$.

2.2. Groupoids

A groupoid $G$ is a small category in which every element is a unit (i.e., every morphism is an isomorphism). If $e, f, e', f' \in G_0$ and there exist $a \in G(e, f)$ and $b \in G(e', f')$, then
is a bijection.

For all $e \in G_0$ the set $G(e)$ is a group, called the vertex group or isotropy group of $G$ at $e$. If $f \in G_0$ and $a \in G(e, f)$, then, taking $b = a$, the map in (1) is a group isomorphism from $G(e)$ to $G(f)$. If $G(e)$ is abelian, it can be easily checked that this isomorphism does not depend on the choice of $a$: If $a, a' \in G(e, f)$, then

$$a'(a^{-1}xa')^{-1} = (a'a^{-1})x(aa'^{-1}) = (a'a^{-1})(aa'^{-1})x = x.$$  

In particular, if $G$ is connected (meaning $G(e, e') \neq \emptyset$ for all $e, e' \in G_0$) and one vertex group is abelian, then all vertex groups are abelian, and they are canonically isomorphic.

In this case we define for $e \in G_0$ and $x \in G(e)$ the set $(x) = \{a^{-1}xa \mid a \in G(e, \cdot)\}$, and the universal vertex group as

$$\mathbb{G} = \{(x) \mid x \in G(e), e \in G_0\}.$$  

$\mathbb{G}$ indeed has a natural abelian group structure: For every $e \in G_0$ there is a bijection $j_e : G(e) \to \mathbb{G}$, $x \mapsto (x)$ inducing the structure of an abelian group on $\mathbb{G}$, and because the diagrams

$$\begin{array}{c}
G(e) \\
\downarrow j_e \\
\mathbb{G}
\end{array}
\xrightarrow{x \mapsto a^{-1}xa} 
\begin{array}{c}
G(f) \\
\downarrow j_f \\
\mathbb{G}
\end{array}
$$  

commute for every choice of $e, f \in G_0$ and $a \in G(e, f)$, this group structure is independent of the choice of $e$, yielding a canonical group isomorphism $j_e : G(e) \to \mathbb{G}$ for every $e \in G_0$. We will use calligraphic letters to denote elements of $\mathbb{G}$. If $\mathcal{X} \in \mathbb{G}$, then the unique representative of $\mathcal{X}$ in $G(e)$, $j_e^{-1}(\mathcal{X})$, will be denoted by $\mathcal{X}_e$.

If $G$ is a groupoid, and $H \subset G$ is a subcategory, then $HH^{-1}$ denotes the set of all right fractions of elements of $H$. Furthermore, $HH^{-1} \subset G$ is a subgroupoid if and only if $H$ satisfies the right Ore condition.

2.3. Krull monoids and Krull rings

A monoid $H$ is called a Krull monoid if it is completely integrally closed (in other words, a maximal order) and satisfies the ACC on divisorial two-sided ideals. A prime Goldie ring $R$ is a Krull ring if it is completely integrally closed and satisfies the ACC on divisorial two-sided ideals (equivalently, its monoid $R^\star$ of cancellative elements is a Krull monoid; see [25]). The theory of commutative Krull monoids is presented in [32,27]. The simplest examples of non-commutative Krull rings are classical maximal orders in central simple algebras over Dedekind domains (see Section 5.2). We discuss monoids of zero-sum sequences.

Let $G = (G, 0, +)$ be an additively written abelian group, $G_P \subset G$ a subset and let $\mathcal{F}_{ab}(G_P)$ be the (multiplicatively written) free abelian monoid with basis $G_P$. Elements $S \in \mathcal{F}_{ab}(G_P)$ are called sequences over $G_P$, and are written in the form $S = g_1 \cdot \cdots \cdot g_l$ where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G_P$. We denote by $|S| = l$ the length of $S$. Such a sequence $S$ is said to be a zero-sum sequence if $\sigma(S) = g_1 + \cdots + g_l = 0_G$. The submonoid

$$B(G_P) = \{ S \in \mathcal{F}_{ab}(G_P) \mid \sigma(S) = 0 \} \subset \mathcal{F}_{ab}(G_P)$$

is a bijection.

For all $e \in G_0$ the set $G(e)$ is a group, called the vertex group or isotropy group of $G$ at $e$. If $f \in G_0$ and $a \in G(e, f)$, then, taking $b = a$, the map in (1) is a group isomorphism from $G(e)$ to $G(f)$. If $G(e)$ is abelian, it can be easily checked that this isomorphism does not depend on the choice of $a$: If $a, a' \in G(e, f)$, then

$$a'(a^{-1}xa')^{-1} = (a'a^{-1})x(aa'^{-1}) = (a'a^{-1})(aa'^{-1})x = x.$$  

In particular, if $G$ is connected (meaning $G(e, e') \neq \emptyset$ for all $e, e' \in G_0$) and one vertex group is abelian, then all vertex groups are abelian, and they are canonically isomorphic.

In this case we define for $e \in G_0$ and $x \in G(e)$ the set $(x) = \{a^{-1}xa \mid a \in G(e, \cdot)\}$, and the universal vertex group as

$$\mathbb{G} = \{(x) \mid x \in G(e), e \in G_0\}.$$  

$\mathbb{G}$ indeed has a natural abelian group structure: For every $e \in G_0$ there is a bijection $j_e : G(e) \to \mathbb{G}$, $x \mapsto (x)$ inducing the structure of an abelian group on $\mathbb{G}$, and because the diagrams

$$\begin{array}{c}
G(e) \\
\downarrow j_e \\
\mathbb{G}
\end{array}
\xrightarrow{x \mapsto a^{-1}xa} 
\begin{array}{c}
G(f) \\
\downarrow j_f \\
\mathbb{G}
\end{array}
$$  

commute for every choice of $e, f \in G_0$ and $a \in G(e, f)$, this group structure is independent of the choice of $e$, yielding a canonical group isomorphism $j_e : G(e) \to \mathbb{G}$ for every $e \in G_0$. We will use calligraphic letters to denote elements of $\mathbb{G}$. If $\mathcal{X} \in \mathbb{G}$, then the unique representative of $\mathcal{X}$ in $G(e)$, $j_e^{-1}(\mathcal{X})$, will be denoted by $\mathcal{X}_e$.

If $G$ is a groupoid, and $H \subset G$ is a subcategory, then $HH^{-1}$ denotes the set of all right fractions of elements of $H$. Furthermore, $HH^{-1} \subset G$ is a subgroupoid if and only if $H$ satisfies the right Ore condition.

2.3. Krull monoids and Krull rings

A monoid $H$ is called a Krull monoid if it is completely integrally closed (in other words, a maximal order) and satisfies the ACC on divisorial two-sided ideals. A prime Goldie ring $R$ is a Krull ring if it is completely integrally closed and satisfies the ACC on divisorial two-sided ideals (equivalently, its monoid $R^\star$ of cancellative elements is a Krull monoid; see [25]). The theory of commutative Krull monoids is presented in [32,27]. The simplest examples of non-commutative Krull rings are classical maximal orders in central simple algebras over Dedekind domains (see Section 5.2). We discuss monoids of zero-sum sequences.

Let $G = (G, 0_G, +)$ be an additively written abelian group, $G_P \subset G$ a subset and let $\mathcal{F}_{ab}(G_P)$ be the (multiplicatively written) free abelian monoid with basis $G_P$. Elements $S \in \mathcal{F}_{ab}(G_P)$ are called sequences over $G_P$, and are written in the form $S = g_1 \cdot \cdots \cdot g_l$ where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G_P$. We denote by $|S| = l$ the length of $S$. Such a sequence $S$ is said to be a zero-sum sequence if $\sigma(S) = g_1 + \cdots + g_l = 0_G$. The submonoid

$$B(G_P) = \{ S \in \mathcal{F}_{ab}(G_P) \mid \sigma(S) = 0 \} \subset \mathcal{F}_{ab}(G_P)$$
is called the monoid of zero-sum sequences over $G_P$. It is a reduced commutative Krull monoid, which is finitely generated whenever $G_P$ is finite [27, Theorem 3.4.2]. Moreover, every commutative Krull monoid possesses a transfer homomorphism onto a monoid of zero-sum sequences, and thus $B(G_P)$ provides a model for the factorization behavior of commutative Krull monoids [27, Section 3.4].

### 3. Arithmetical invariants

In this section we introduce our main arithmetical invariants (rigid factorizations, sets of lengths, sets of distances) and transfer homomorphisms in the setting of cancellative small categories.

Throughout this section, let $H$ be a cancellative small category.

**Proposition 3.1.** If $H$ satisfies the ACC on principal left and right ideals, then $H$ is atomic.

**Proof.** We first note that if $a, b \in H$ then $aH = bH$ if and only if $a = b\varepsilon$ with $\varepsilon \in H^\times$, and similarly $Ha = Hb$ if and only if $a = \varepsilon b$ with $\varepsilon \in H^\times$. [We only show the statement for the right ideals. The non-trivial direction is showing that $aH = bH$ implies $a = b\varepsilon$. Since $aH = bH$ implies $a = bx$ and $b = ay$ with $x, y \in H$, we get $a = a(ay)$ and $b = b(xy)$. Since $H$ is cancellative, this implies $xy = t(b) = s(x)$ and $yx = t(a) = s(y)$, hence $y = x^{-1}$ and therefore $x, y \in H^\times$.]

**Claim A.** If $a \in H \setminus H^\times$, then there exist $u \in \mathcal{A}(H)$ and $a_0 \in H$ such that $a = ua_0$.

**Proof of Claim A.** Assume the contrary. Then the set

$$
\Omega = \{a' \mid a' \in H \setminus H^\times \text{ such that there are no } u \in \mathcal{A}(H), \ a_0 \in H \text{ with } a' = ua_0\}
$$

is non-empty, and hence, using the ascending chain condition on the principal right ideals, possesses a maximal element $aH$ with $a \in H \setminus H^\times$. Then $a \notin \mathcal{A}(H)$, and therefore $a = bc$ with $b, c \in H \setminus H^\times$. But $aH \subseteq bH$ since $c \notin H^\times$, and thus maximality of $aH$ in $\Omega$ implies $b = ub_0$ with $u \in \mathcal{A}(H)$ and $b_0 \in H$. But then $a = u(b_0c)$, a contradiction. \(\square\)

We proceed to show that every $a \in H \setminus H^\times$ is a product of atoms. Again, assume that this is not the case. Then

$$
\Omega' = \{Ha' \mid a' \in H \setminus H^\times \text{ such that } a' \text{ is not a product of atoms}\}
$$

is non-empty, and hence possesses a maximal element $Ha$ with $a \in H \setminus H^\times$ (this time using the ascending chain condition on principal left ideals). Again $a \notin \mathcal{A}(H)$ as otherwise it would be a product of atoms. By **Claim A**, $a = ua_0$ with $u \in \mathcal{A}(H)$ and $a_0 \in H$. Since $a \notin \mathcal{A}(H)$, $a_0 \notin H^\times$. Moreover, $Ha \subsetneq Ha_0$ since $u \notin H^\times$ and therefore $a_0 = u_1 \cdots u_l$ with $l \in \mathbb{N}$ and $u_1, \ldots, u_l \in \mathcal{A}(H)$. Thus $a = uu_1 \cdots u_l$ is a product of atoms, a contradiction. \(\square\)

The following definition provides a natural notion of an ordered factorization (called a rigid factorization) in a cancellative small category. It is modeled after a terminology by Cohn [14,15].
Let $\mathcal{F}(\mathcal{A}(H))$ denote the path category on atoms of $H$. We define

$$H^\times \times_r \mathcal{F}(\mathcal{A}(H)) = \left\{ (\varepsilon, y) \in H^\times \times \mathcal{F}(\mathcal{A}(H)) \mid t(\varepsilon) = s(y) \right\},$$

and define an associative partial operation on $H^\times \times_r \mathcal{F}(\mathcal{A}(H))$ as follows: If $(\varepsilon, y), (\varepsilon', y') \in H^\times \times_r \mathcal{F}(\mathcal{A}(H))$ with $\varepsilon, \varepsilon' \in H^\times$,

$$y = (\varepsilon, u_1, u_2, \ldots, u_k, f) \in \mathcal{F}(\mathcal{A}(H)) \quad \text{and} \quad y' = (\varepsilon', v_1, v_2, \ldots, v_l, f') \in \mathcal{F}(\mathcal{A}(H)),$$

then the operation is defined if $t(y) = s(\varepsilon')$, and

$$(\varepsilon, y) \cdot (\varepsilon', y') = (\varepsilon, (\varepsilon, u_1, \ldots, u_k \varepsilon', v_1, v_2, \ldots, v_l, f')) \quad \text{if } k > 0,$$

while $(\varepsilon, y) \cdot (\varepsilon', y') = (\varepsilon \varepsilon', y')$ if $k = 0$. In this way $H^\times \times_r \mathcal{F}(\mathcal{A}(H))$ is again a cancellative small category (with identities $\{(\varepsilon, (\varepsilon, e)) \mid e \in H_0\}$ that we identify with $H_0$ again, $s(\varepsilon, y) = s(\varepsilon)$ and $t(\varepsilon, y) = t(y)$). We define a congruence relation $\sim$ on it as follows: If $(\varepsilon, y), (\varepsilon', y') \in H^\times \times_r \mathcal{F}(\mathcal{A}(H))$ with $y, y'$ as before, then $(\varepsilon, y) \sim (\varepsilon', y')$ if $k = l, \varepsilon u_1 \cdot \cdot \cdot u_k = \varepsilon' v_1 \cdot \cdot \cdot v_l \in H$ and either $k = 0$ or there exist $\delta_2, \ldots, \delta_k \in H^\times$ and $\delta_{k+1} = t(u_k)$ such that

$$\varepsilon' v_1 = \varepsilon u_1 \delta_2^{-1}$$

and $v_i = \delta_i u_i \delta_{i+1}^{-1}$ for all $i \in [2, k]$.

**Definition 3.2.** The category of rigid factorizations of $H$ is defined as

$$Z^*(H) = \left( H^\times \times_r \mathcal{F}(\mathcal{A}(H)) \right)/\sim.$$

For $z \in Z^*(H)$ with $z = [(\varepsilon, (\varepsilon, u_1, u_2, \ldots, u_k, f))]_\sim$ we write $z = \varepsilon u_1 \ast \cdots \ast u_k$ and the operation on $Z^*(H)$ is also denoted by $\ast$. The length of $z$ is $|z| = k$. There is a surjective homomorphism $\pi : Z^*(H) \to H$, induced by multiplying out the elements of the factorization in $H$, explicitly $\pi(z) = \varepsilon u_1 u_2 \cdots u_k \in H$. For $a \in H$, we define $Z^*(a) = Z^*_H(a) = \pi^{-1}(\{a\})$ to be the set of rigid factorization of $a$.

To simplify the notation, we make the following conventions:

- If, for a rigid factorization $z = \varepsilon u_1 \ast \cdots \ast u_k \in Z^*(H)$, we have $k > 0$ (i.e., $\pi(z) \notin H^\times$), then the unit $\varepsilon$ can be absorbed into the first factor $u_1$ (replacing it by $\varepsilon u_1$), and we can essentially just work in $\mathcal{F}(\mathcal{A}(H))/\sim$, with $\sim$ defined to match the equivalence relation on $H^\times \times_r \mathcal{F}(\mathcal{A}(H))$.
- If $H$ is reduced but $|H_0| > 1$, we often still write $s(u_1) u_1 \ast \cdots \ast u_k$ instead of the shorter $u_1 \ast \cdots \ast u_k$, as $k = 0$ is allowed and in the path category there is a different empty path for every $e \in H_0$.

**Remark 3.3.**

1. If $H$ is reduced, then $Z^*(H) = \mathcal{F}(\mathcal{A}(H))$.
2. If $H$ is not reduced, the $H^\times$ factor allows us to represent trivial factorizations of units, and the equivalence relation $\sim$ allows us to deal with trivial insertion of units. In the commutative setting these technicalities can easily be avoided by identifying associated elements and passing to the reduced monoid $H_{\text{red}} = \{aH^\times \mid a \in H\}$. Unfortunately, associativity (left, right or two-sided) is in general no congruence relation in the non-commutative case.
ordered while rigid factorizations are ordered. The homomorphism $\pi : \mathbb{Z}^+(H_{\text{red}}) \to H_{\text{red}}$ obviously factors through the multiplication homomorphism $\mathbb{Z}(H_{\text{red}}) \to H_{\text{red}}$, and the fibers consist of the different permutations of a factorization.

In the following we will only be concerned with invariants related to the lengths of factorizations, which may as well be defined using rigid factorizations.

**Definition 3.4.** Let $a \in H$.

1. We call

$$L(a) = L_H(a) = \{ |z| \in \mathbb{N}_0 \mid z \in \mathbb{Z}^+(a) \}$$

the set of lengths of $a$.

2. The system of sets of lengths of $H$ is defined as $L(H) = \{ L(a) \subset \mathbb{N}_0 \mid a \in H \}$.

3. A positive integer $d \in \mathbb{N}$ is a distance of $a$ if there exists an $l \in L(a)$ such that $(l, l + d) \in L(a)$ and $L(a) \cap (l + 1, l + d - 1) = \emptyset$. The set of distances of $a$ is the set consisting of all such distances and is denoted by $\Delta(a) = \Delta_H(a)$. The set of distances of $H$ is defined as

$$\Delta(H) = \bigcup_{a \in H} \Delta(a).$$

4. We define $L_k(H) = \bigcup_{L \in L(H), k \in \mathbb{N}_0} L$ for $k \in \mathbb{N}_0$.

5. $H$ is half-factorial if $|L(a)| = 1$ for all $a \in H$ (equivalently, $H$ is atomic and $\Delta(H) = \emptyset$).

We write $b \mid_H^r a$ if $a \in Hb$ and similarly $b \mid_H^l a$ if $a \in bH$.

**Definition & Lemma 3.5.** Let $H \subset D$ be subcategories of a groupoid. The following are equivalent:

(a) For all $a, b \in H$, $b \mid_D^r a$ implies $b \mid_H^r a$.

(b) $HH^{-1} \cap D = H$.

$H \subset D$ is called right-saturated if these equivalent conditions are fulfilled.

**Proof.** (a) $\Rightarrow$ (b): Let $c = ab^{-1}$ with $a, b \in H$, $t(a) = t(b)$ and $c \in D$. Then $cb = a$, i.e., $b \mid_D^r a$ and hence also $b \mid_H^r a$. Since the left factor is uniquely determined as $c = ab^{-1}$, it follows that $c \in H$.

(b) $\Rightarrow$ (a): Let $b \mid_D^r a$. There exists $c \in D$ with $cb = a$, and thus $c = ab^{-1}$. Therefore $c \in HH^{-1} \cap D = H$, hence $b \mid_H^r a$. □

**Definition 3.6.** Let $B$ be a reduced cancellative small category. A homomorphism $\theta : H \to B$ is called a transfer homomorphism if it has the following properties:

(T1) $B = \theta(H)$ and $\theta^{-1}(B_0) = H^\times$.

(T2) If $a \in H$, $b_1, b_2 \in B$ and $\theta(a) = b_1b_2$, then there exist $a_1, a_2 \in H$ such that $a = a_1a_2$, $\theta(a_1) = b_1$ and $\theta(a_2) = b_2$.

The notion of a transfer homomorphism plays a central role in studying sets of lengths. It is easily checked that the following still holds in our generalized setting (cf. [27, §3.2] for the commutative case, [25, Proposition 6.4] for the non-commutative monoid case).

**Proposition 3.7.** If $\theta : H \to B$ is a transfer homomorphism, then $L_H(a) = L_B(\theta(a))$ for all $a \in H$ and hence all invariants defined in terms of lengths coincide for $H$ and $B$. In particular,
• \( \mathcal{L}(H) = \mathcal{L}(B) \),
• \( \mathcal{U}_k(H) = \mathcal{U}_k(B) \) for all \( k \in \mathbb{N}_0 \),
• \( \Delta_H(a) = \Delta_B(\theta(a)) \) for all \( a \in H \), and \( \Delta(H) = \Delta(B) \).

**Proposition 3.8.** Let \( H \) be a cancellative small category, \( G \) a finite abelian group and \( \theta : H \to \mathcal{B}(G) \) a transfer homomorphism. Then \( H \) is half-factorial if and only if \( |G| \leq 2 \). If \( |G| \geq 3 \), then we have

1. \( \Delta(H) \) is a finite interval, and if it is non-empty, then \( \min \Delta(H) = 1 \),
2. for every \( k \geq 2 \), the set \( \mathcal{U}_k(H) \) is a finite interval,
3. there exists an \( M \in \mathbb{N}_0 \) such that for every \( a \in H \) the set of lengths \( \mathcal{L}(a) \) is an almost arithmetical multiprogression (AAMP) with difference \( d \in \Delta(H) \) and bound \( M \).

**Proof.** By the previous lemma it is sufficient to show these statements for the monoid of zero-sum sequences \( \mathcal{B}(G) \) over a finite abelian group \( G \). \( \mathcal{B}(G) \) is half-factorial if and only if \( |G| \leq 2 \) by [27, Proposition 2.5.6]. The first statement is proven in [29], the second can be found in [24, Theorem 3.1.3]. For the definition of AAMPs and a proof of 3 see [27, Chapter 4].

The description in 3 is sharp by a realization theorem of W.A. Schmid [49].

### 4. Factorization of integral elements in arithmetical groupoids

In this section we introduce arithmetical groupoids and study the factorization behavior of integral elements. In Section 5 we will see that the divisorial fractional one-sided ideals of suitable semigroups form such groupoids. Thus in non-commutative semigroups arithmetical groupoids generalize the free abelian group of divisorial fractional two-sided ideals familiar from the commutative setting (see Proposition 4.6 and Remark 4.16). This abstract approach to factorizations was first used by Asano and Murata in [5]. We follow their ideas and also those of Rehm in [45,46], who studies factorizations of ideals in rings in a different abstract framework. The notation and terminology for lattices follows [30], a reference for l-groups is [51]. Proposition 4.12 is the main result on factorizations of integral elements in a lattice-ordered groupoid (due to Asano and Murata). We introduce an abstract norm homomorphism \( \eta \), and as the main result in this section, we present a transfer homomorphism to a monoid of zero-sum sequences in Theorem 4.15.

**Definition 4.1.** A lattice-ordered groupoid \((G, \leq)\) is a groupoid \( G \) together with a relation \( \leq \) on \( G \) such that for all \( e, f \in G_0 \)

1. \((G(e, \cdot), \leq_{G(e, \cdot)})\) is a lattice (we write \( \land_{e}^{\prime} \) and \( \lor_{e}^{\prime} \) for the meet and join),
2. \((G(\cdot, f), \leq_{G(\cdot, f)})\) is a lattice (we write \( \land_{f}^{\prime} \) and \( \lor_{f}^{\prime} \) for the meet and join),
3. \((G(e, f), \leq_{G(e,f)})\) is a sublattice of both \( G(e, \cdot) \) and \( G(\cdot, f) \). Explicitly: For all \( a, b \in G(e, f) \) it holds that \( a \land_{e}^{\prime} b = a \land_{f}^{\prime} b \in G(e, f) \) and \( a \lor_{e}^{\prime} b = a \lor_{f}^{\prime} b \in G(e, f) \).

If \( a, b \in G \) and \( s(a) = s(b) \) we write \( a \land b = a \land_{s(a)}^{\prime} b \) and \( a \lor b = a \lor_{s(a)}^{\prime} b \). If \( t(a) = t(b) \) we write \( a \land b = a \land_{t(a)}^{\prime} b \) and \( a \lor b = a \lor_{t(a)}^{\prime} b \). By 3 this is unambiguous if \( s(a) = s(b) \) and \( t(a) = t(b) \) both hold. The restriction of \( \leq \) to any of \( G(e, \cdot), G(\cdot, f) \) or \( G(e, f) \) will in the following simply be denoted by \( \leq \) again. (Keep in mind however that \( \leq \) need not be a partial order on the entire set \( G \), and \( \land \) and \( \lor \) do not represent meet and join operations on the entire set \( G \) in the order-theoretic sense.)

An element \( a \) of a lattice-ordered groupoid is called integral if \( a \leq s(a) \) and \( a \leq t(a) \), and we write \( G_+ \) for the subset of all integral elements of \( G \).

**Definition 4.2.** A lattice-ordered groupoid \( G \) is called an arithmetical groupoid if it has the following properties for all \( e, f \in G_0 \):

\((P_1)\) For \( a \in G \), \( a \leq s(a) \) if and only if \( a \leq t(a) \).
(P₂) \( G(e, \cdot) \) and \( G(\cdot, f) \) are modular lattices.

(P₃) If \( a \leq b \) for \( a, b \in G(e, \cdot) \) and \( c \in G(\cdot, e) \), then \( ca \leq cb \). Analogously, if \( a, b \in G(\cdot, f) \) and \( c \in G(f, \cdot) \), then \( ac \leq bc \).

(P₄) For every non-empty subset \( M \subset G(\cdot, e) \cap G_+ \), \( \text{sup}(M) \in G(\cdot, \cdot) \) exists, and similarly for \( M \subset G(\cdot, f) \cap G_+ \). If moreover \( M \subset G(e, f) \) then \( \text{sup}_{G(\cdot, e)}(M) = \text{sup}_{G(\cdot, f)}(M) \).

(P₅) \( G(e, f) \) contains an integral element.

(P₆) \( G(e, \cdot) \) and \( G(\cdot, f) \) satisfy the ACC on integral elements.

For the remainder of this section, let \( G \) be an arithmetical groupoid.

P₃ implies in particular \( G(e, f) \neq \emptyset \) for all \( e, f \in G_0 \), i.e., \( G \) is connected. If \( e, e' \in G_0 \) and \( c \in G(e', e) \), then \( G(e, \cdot) \to G(e', \cdot), x \mapsto cx \) is an order isomorphism by P₃, and similarly every \( d \in G(f, f') \) induces an order isomorphism from \( G(\cdot, f) \) to \( G(\cdot, f') \). P₂ could therefore equivalently be required for a single \( e \) and a single \( f \in G_0 \). Moreover, since the map \( (G(e, \cdot), \leq) \to (G(\cdot, e), \geq), x \mapsto x^{-1} \) is also an order isomorphism (Lemma 4.3.1) and the property of being modular is self-dual, it is in fact sufficient that one of \( G(e, \cdot) \) and \( G(\cdot, e) \) is modular for one \( e \in G_0 \).

Using P₃ we also observe that it is sufficient to have the ACC on integral elements on one \( G(e, \cdot) \) and one \( G(\cdot, f) \): If, say, \( a_1 \leq a_2 \leq a_3 \leq \cdots \) is an ascending chain of integral elements in \( G(e', \cdot) \) and \( c \in G(e, e') \) is integral, then \( ca_1 \leq ca_2 \leq ca_3 \leq \cdots \) is an ascending chain of integral elements in \( G(e', \cdot) \) (Lemma 4.3.2), hence becomes stationary, and multiplying by \( c^{-1} \) from the left again shows that the original chain also becomes stationary.

We summarize some basic properties that follow immediately from the definitions.

**Lemma 4.3.** Let \( e, f \in G_0 \).

1. \( a \leq x \iff a^{-1} \geq x^{-1} \) holds if either \( a, x \in G(\cdot, \cdot) \) or \( a, x \in G(\cdot, f) \). In particular, for \( a \in G \) the following are equivalent: (a) \( a \leq s(a) \); (b) \( a \leq t(a) \); (c) \( a^{-1} \geq s(a) \); (d) \( a^{-1} \geq t(a) \).

2. Let \( a \in G(e, f) \), \( x \in G(\cdot, e) \) and \( y \in G(f, \cdot) \) are conditionally complete as lattices.

3. If \( a \in G(e, f) \), \( x \in G(\cdot, e) \) and \( y \in G(f, \cdot) \), then
   (i) \( x(a \lor b) = xa \lor xb \) and \( x(a \land b) = xa \land xb \)
   if \( b \in G(\cdot, \cdot) \),
   (ii) \( (a \lor b)y = ay \lor by \) and \( (a \land b)y = ay \land by \)
   if \( b \in G(\cdot, f) \).

4. Let \( \emptyset \neq M \subset G(\cdot, \cdot) \) and \( x \in G(\cdot, e) \). If \( \text{sup}_{G(\cdot, \cdot)}(M) \) exists, then also \( \text{sup}_{G(x \cdot (\cdot))}(xM) \) exists, and \( \text{sup}(xM) = x \text{sup}(M) \). Moreover, then also \( \text{inf}_{G(\cdot, \cdot)}(M^{-1}) \) exists and \( \text{inf}(M^{-1}) = \text{sup}(M)^{-1} \). Analogous statements hold for \( \emptyset \neq M \subset G(\cdot, f) \) and \( x \in G(f, \cdot) \).

5. \( G(\cdot, e) \), \( G(\cdot, f) \), \( G(e, f) \) and in particular \( G(e) \) are conditionally complete as lattices.

6. The set \( G_+ \) of all integral elements forms a reduced wide subcategory of \( G \), and \( G = \mathbf{q}(G_+) \) is the groupoid of (left and right) fractions of this subcategory.

7. For every \( a \in G(e, f) \), there exist \( b \in G(e) \) and \( c \in G(f) \) with \( b \leq a \) and \( c \leq a \).

**Proof.** 1. Assume first \( s(x) = s(a) \). By P₃, \( a \leq x \) if and only if \( x^{-1}a \leq t(x) \). By P₁ this is equivalent to \( x^{-1}a \leq t(a) \). Again by P₃ this is equivalent to \( x^{-1}a \leq a^{-1} \). The case \( t(x) = t(a) \) is proven similarly.

2. Since \( x \leq t(x) = s(a) \), we have \( xa \leq s(a)a = a \) by P₃. Similarly, by \( y \).

3. We show (i), (ii) is similar. Since \( a \leq a \lor b \) and \( b \leq a \lor b \), P₃ implies \( xa \leq x(a \lor b) \) and \( xb \leq x(a \lor b) \), thus \( xa \lor xb \leq x(a \lor b) \). Therefore

\[
a \lor b = (x^{-1}xa) \lor (x^{-1}xb) \leq x^{-1}(xa \lor xb),
\]

and multiplying by \( x \) from the left gives \( x(a \lor b) \leq xa \lor xb \). Dually, \( x(a \land b) = xa \land xb \).

4. Let \( c = \text{sup}(M) \). Then for all \( m \in M \), \( xm \leq xc \), hence \( xc \) is an upper bound for \( xM \). If \( d \in G(s(x), \cdot) \) is another upper bound for \( xM \), then \( m \leq x^{-1}d \) for all \( m \in M \), hence \( c \leq x^{-1}d \) and thus \( xc \leq d \). Therefore \( xc = \text{sup}(xM) \).
For \( d \in G(e, \cdot) \) we have \( m \leq d \) for all \( m \in M \) if and only if \( m^{-1} \geq d^{-1} \) (in \( G(\cdot, e) \)), and \( \inf(M^{-1}) = \sup(M)^{-1} \) follows.

5. We show the claim for \( G(e, \cdot) \), for \( G(\cdot, f) \) the proof is similar. Let \( \emptyset \neq M \subset G(e, \cdot) \) be bounded, say \( x \leq m \leq y \) for some \( x, y \in G(e, \cdot) \) and all \( m \in M \). Then \( y^{-1}M \subset G(t(y), \cdot) \) is integral, hence \( \sup(y^{-1}M) \) exists by \( P_4 \), and \( \sup(M) = y \sup(y^{-1}M) \) by 4. Similarly, \( M^{-1}x \subset G(\cdot, t(x)) \) is integral, and therefore \( \sup(M^{-1}x) \) exists, implying \( \inf(M) = \sup(M^{-1})^{-1} = x \sup(M^{-1}x)^{-1} \).

The proof for \( G(e, f) \) is similar but uses in addition \( \sup_{G(t(y), \cdot)}(y^{-1}M) = \sup_{G(\cdot, f)}(y^{-1}M) \) (from \( P_4 \)), to ensure that the supremum lies in \( G(e, f) \) again.

6. By 2 and the fact that every \( e \in G_0 \) is integral by definition, \( G_+ \) forms a wide subcategory of \( G \). If \( a \in G_+ \setminus G_0 \), then \( a < s(a) \), thus \( a^{-1} > s(a) \) and therefore \( a^{-1} \) is not integral. Hence the subcategory of integral elements is reduced. Let \( x \in G \) and \( e = s(x) \). Then \( a = x \land e \leq e \), hence \( a \) is integral. Since \( a \leq x \), also \( x^{-1}a \leq t(x) \) is integral. Set \( b = x^{-1}a \). Then \( x = ab^{-1} \) with \( a, b \in G_+ \). Similarly one can find \( c, d \in G_+ \) with \( x = d^{-1}c \).

7. By \( P_5 \) there exist integral \( b' \in G(f, e) \) and \( c' \in G(e, f) \). Set \( b = ab' \) and \( c = c'a \). Then \( b \leq a, c \leq a \) and \( b \in G(e), c \in G(f) \). □

For \( e, f \in G \) it is immediate from the definitions that \( G_+(e, \cdot) = G(e, \cdot) \cap G_+ \), \( G_+(\cdot, f) = G(\cdot, f) \cap G_+ \) and \( G_+(e, f) = G(e, f) \cap G_+ \). Moreover, \( G_+(e, \cdot) \) is a sublattice of \( G(e, \cdot) \), \( G_+(\cdot, f) \) is a sublattice of \( G(\cdot, f) \).

If \( a, b \in G_+(e, \cdot) \), then \( a \leq b \) if and only if \( b \upharpoonright_{G_+} a = a \) if and only if \( b^{-1}a \) is integral if and only if \( a \leq b \). Similarly, if \( a, b \in G_+(\cdot, f) \), then \( a \leq b \) if and only if \( b \upharpoonright_{G_+} a \). Correspondingly, for integral elements with the same left (right) identity, we may view the join and meet operations as left (right) gcd and lcm.

**Definition & Lemma 4.4.** For \( u \in G \) the following are equivalent:

(a) \( u \) is maximal in \( G_+(s(u), \cdot) \setminus \{s(u)\} \).
(b) \( u \) is maximal in \( G_+(\cdot, t(u)) \setminus \{t(u)\} \).
(c) \( u \in \mathcal{A}(G_+) \).

An element \( u \in G \) satisfying these equivalent conditions is called maximal integral.

**Proof.** (a) ⇒ (b): By definition, \( u \) is maximal in \( G(s(u), \cdot) \) with \( u < s(u) \). If \( u < y < t(u) \) with \( y \in G(\cdot, t(u)) \), then \( uy^{-1} \leq yy^{-1} = s(y) \), hence \( uy^{-1} \in G(s(u), \cdot) \) is integral, and therefore \( u < uy^{-1} \leq s(u) \). By maximality of \( u \) in the first set, therefore \( uy^{-1} = s(u) \), whence \( y = u \) and \( u \) is maximal in the second set.

(b) ⇒ (c): Assume \( u = vw \) with \( v, w \in G_+ \setminus G_0 \). Then \( u < w < t(u) \), contradicting the maximality of \( u \) in \( G_+(\cdot, t(u)) \).

(c) ⇒ (a): Let \( v \in G_+(s(u), \cdot) \) with \( u \leq v < s(u) \). Then \( u = v(v^{-1}u) \) with \( v \) and \( v^{-1}u \) integral, and since \( v \not\in G_0 \) necessarily \( v^{-1}u \in G_0 \), i.e., \( u = v \). □

**Lemma 4.5.** Let \( U \) be an \( l \)-group. For \( p \in U \) the following are equivalent:

(a) \( p \) is maximal integral,
(b) \( p \) is a prime element in \( U_+ \),
(c) \( p \in \mathcal{A}(U_+) \).

**Proof.** (a) ⇔ (c) is shown as in **Definition & Lemma 4.4**. It suffices to show (a) ⇒ (b) and (b) ⇒ (c). Let \( e \) be the identity of \( U \).

(a) ⇒ (b): Let \( p \) be maximal in \( U_+ \) with \( p \neq e \). Assume \( p | ab \) for \( a, b \leq e \). That means \( ab \leq p \). Assume \( a \not\leq p \). Then \( b = (a \lor p)b = ab \lor pb \leq p \lor pb = p \), i.e., \( p | b \).

(b) ⇒ (c): Let \( p \) be a prime, \( p = ab \) with \( a, b \leq e \). Say \( p | a \), i.e., \( a \leq p \). Then \( a \leq p \leq a \) implies \( p = a \) and therefore \( b = e \). □
Proposition 4.6.

1. If G is a group (i.e., |G₀| = 1), then G is the free abelian group with basis Α(G₊), and G₊ is the free abelian monoid with basis A(G₊). Moreover gcd(a, b) = a ∨ b and lcm(a, b) = a ∧ b.

2. Let M be a set, F the free abelian group with basis M, and H ⊆ F the free abelian monoid with the same basis. A lattice order is defined on F by a ≤ b if a = cb with c ∈ H, and (F, ≤) is an arithmetical groupoid with F₊ = H and M = A(F₊).

3. For every e ∈ G₀, the group isomorphism je : G(e) → G induces the structure of an arithmetical groupoid on G, and the induced structure on G is independent of the choice of e. G₊(G(e)) is a free abelian group and G₊(G(e)₊) is a free abelian monoid with basis A(G₊)(A(G(e)₊)). Moreover, je(A(G(e)₊)) = A(G₊).

Proof. 1. G is an l-group, and by Lemma 4.3.5 it is conditionally complete. Therefore G is commutative [51, Theorems 2.3.1(d) and 2.3.9]. Since it satisfies the ACC on integral elements, G₊ is atomic (Proposition 3.1). By the previous lemma, every atom of G₊ is a prime element, and therefore G₊ is factorial. Because it is also reduced, G₊ is the free abelian monoid with basis A(G₊). Now G = q(G₊) implies that G is the free abelian group with basis A(G₊). Finally, gcd(a, b) = a ∨ b and gcd(a, b) = a ∧ b for a, b ∈ G₊ follow because c ≤ d if and only if d | c for all c, d ∈ G₊.

2. Clearly ≤ defines a lattice order on F, and the properties of an arithmetical groupoid are, except for P₂, either trivial, or easily checked. For P₂ recall that every l-group is distributive, hence modular, as a lattice [51, Theorem 2.1.3(a)]. Now F₊ = H and A(F₊) = M are immediate from the definitions.

3. For every e ∈ G₀ the vertex group G(e) is an arithmetical groupoid, as is easily checked. Via the group isomorphism je : G(e) → G therefore G gains the structure of an arithmetical groupoid. If f ∈ G₀ and c ∈ G(e, f), then for all x, y ∈ G(e) we have x ≤ y ⇔ c⁻¹xc ≤ c⁻¹yc, and since j⁻¹f ∩ je(x) = c⁻¹xc, the induced order on G is independent of the choice of e.

By 1, applied to G, respectively G(e), the remaining claims follow (for je(A(G₊)) = A(G(e)₊) use the characterization of atoms as maximal integral elements from Lemma 4.5). □

Let [a, b], [c, d] be intervals in a lattice. Recall that [a, b] is down-perspective to [c, d] if c = a ∧ d and b = a ∨ d. Moreover, [a, b] is perspective to [c, d] if either [a, b] is down-perspective to [c, d], or [c, d] is down-perspective to [a, b]. [a, b], [c, d] are projective if there exists a finite sequence of intervals [a, b] = [a₀, b₀], [a₁, b₁], ..., [aₖ, bₖ] = [c, d] such that [aᵢ₋₁, bᵢ₋₁] is perspective to [ai, bi] for all i ∈ [1, k]. (See [30, Chapter I.3.5].)

Definition 4.7.

1. An element a ∈ G₊(e, f) is transposable to an element b ∈ G₊(e', f') if there exists an element c ∈ G₊(e, e') such that [a, e] is down-perspective to [cb, c]. Explicitly: b = c⁻¹(c ∧ a) and c ∨ a = e.

2. An element a ∈ G₊ is projective to an element b ∈ G₊ if there exists a sequence of integral elements a = c₀, c₁, ..., cₙ, cₙ₊₁ = b, such that for any pair of successive elements (cᵢ, cᵢ₊₁) either cᵢ is transposable to cᵢ₊₁ or cᵢ₊₁ is transposable to cᵢ.

It is easily checked that being transposable is a transitive and reflexive relation (but not symmetric), and projectivity is an equivalence relation. Note that in a modular lattice perspective intervals are isomorphic [30, p. 308, Theorem 348], and therefore in particular the lengths of [a, s(a)] and [b, s(b)] coincide if a is projective to b.

Lemma 4.8. If a, b, c are as in the definition of transposability, then cb = c ∧ a = ad for some d ∈ G₊ and c is transposable to d.

Proof. Since c ∧ a ≤ a, there exists an integral d with ad = c ∧ a, and cb = c ∧ a by definition of transposability. The claim follows from d = a⁻¹(c ∧ a) and c ∨ a = e. □
Lemma 4.11. If two lattice intervals \([a, b]\) and \([c, d]\) of \(G(e, \cdot)\) are projective, then the integral elements \(b^{-1}a\) and \(d^{-1}c\) are projective to each other in the sense of the previous definition.

**Proof.** It suffices to show that if the lattice interval \([a, b]\) is down-perspective to \([c, d]\), then \(b^{-1}a\) is transposable to \(d^{-1}c\). Then \(a = bx, d = by\) and \(c = dz = byz\) with \(x, y, z \in G_+\).

We have:

\[
\begin{align*}
\Phi(b) &= b \\
\Phi(d) &= d = by \\
\Phi(bx) &= bx = a \\
\Phi(c) &= c = byz
\end{align*}
\]

Since \([a, b]\) is down-perspective to \([c, d]\), we get

\[
\begin{align*}
b &= a \lor d = bx \lor by = b(x \lor y) \quad \text{and therefore} \quad x \lor y = s(x) = t(b), \quad \text{and} \\
c &= a \land d = bx \land by = b(x \land y) \quad \text{and therefore} \quad x \land y = b^{-1}c = yz.
\end{align*}
\]

Thus \(d^{-1}c = z = y^{-1}(x \land y)\) with \(y \in G(t(b), t(d))\), and hence \(x = b^{-1}a\) is transposable to \(d^{-1}c\). \(\square\)

**Definition & Lemma 4.10.** For every \(a \in G\),

\[
\{X \in G \mid \mathcal{X}_{t(a)} \leq a\} = \{X \in G \mid \mathcal{X}_{s(a)} \leq a\},
\]

and we write \(G_{\leq a}\) for this set. The lower bound \(\Phi : G \to G\) is defined by \(\Phi(a) = \sup(G_{\leq a})\).

**Proof.** Let \(X \in G\). Recall from Section 2.2 that \(\mathcal{X}_{s(a)} = j^{-1}_{s(a)}(X)\) denotes the unique representative of \(X\) in \(G(s(a))\), and that \(\mathcal{X}_{t(a)} = a^{-1}\mathcal{X}_{s(a)}a\). We have to show that \(\mathcal{X}_{t(a)} \leq a\) if and only if \(\mathcal{X}_{s(a)} \leq a\), but this follows from \(\mathcal{X}_{s(a)} \leq a \Leftrightarrow a^{-1}\mathcal{X}_{s(a)}a \leq a^{-1}aa = a\). \(\square\)

With the definition of \(\Phi\) and the notation of Section 2.2 we have: If \(a \in G(e, f)\), then \(\Phi(a)_e = \sup\{x \in G(e) \mid x \leq a\} \in G(e), \Phi(a)_f = \sup\{x \in G(f) \mid x \leq a\} \in G(f), \Phi(a)_f = a^{-1}\Phi(a)_a = b^{-1}\Phi(a)_b\) for all \(b \in G(e, f)\) and \(\Phi(a) = j_e(\Phi(a)_e) = j_f(\Phi(a)_f)\).

**Lemma 4.11.** Let \(e, f \in G_0\).

1. If \(a, b \in G(e, \cdot)\) or \(a, b \in G(\cdot, f)\) with \(a \leq b\), then \(\Phi(a) \leq \Phi(b)\). In particular, if \(a \in G_+\), then \(\Phi(a) \in G_+\).
2. If \(a \in G(e, f)\), \(b \in G(f, \cdot)\) then \(\Phi(a) \Phi(b) \leq \Phi(ab)\). If moreover \(a, b \in G_+\), then \(\Phi(ab) \leq \Phi(a) \land \Phi(b)\), and if furthermore \(\Phi(a)\) and \(\Phi(b)\) are coprime, then \(\Phi(ab) = \Phi(a)\Phi(b)\).
3. If \(u \in A(G_+)\), then \(\Phi(u) \in G_+\) is prime.
4. Let \(u, v \in G_+\) be projective elements. If \(u \in A(G_+)\), then \(v \in A(G_+)\), and \(\Phi(u) = \Phi(v)\).

**Proof.** 1. Immediate from the definition of \(\Phi\).
2. Observe that \(c = a^{-1}\Phi(a)_e \in G(f, e)\) is integral. Therefore

\[
\Phi(a)_e \Phi(b)_e = ac \Phi(b)_e = acc^{-1} \Phi(b)_f c = a \Phi(b)_f c \leq a \Phi(b)_f \leq ab,
\]

and hence \(\Phi(a) \Phi(b) \leq \Phi(ab)\).

Let now \(a, b\) be integral. Then 1 implies \(\Phi(ab) \leq \Phi(a)\) and \(\Phi(ab) \leq \Phi(b)\), so \(\Phi(ab) \leq \Phi(a) \land \Phi(b)\). The last statement follows because \(\Phi(a) \land \Phi(b) = \text{lcm}(\Phi(a), \Phi(b))\) in \(G_+\).
3. By Lemma 4.5 it suffices to show $\Phi(u) \in \mathcal{A}(G_+)$. If $e = s(u)$, then it suffices to prove $\Phi(u)_e \in \mathcal{A}(G(e)_+)$ (by Proposition 4.6.3). Assume that $\Phi(u)_e = ab$ with $a, b \in G(e)$ such that $a < e$ and $b < e$. Then $b \cup e = e$, since $b > ab = \Phi(u)_e$, and therefore

$$u \geq ab \vee au = a(b \cup e) = a,$$

a contradiction to $a > ab = \Phi(u)_e$.

4. We first show that $v$ is maximal integral, and may assume that either $u$ is transposable to $v$ or $v$ is transposable to $u$. Let $e = s(u)$ and $f = s(v)$. Assume first that $u$ is transposable to $v$ via $c \in G(e, f)$. Then $[u, e]$ is down-perspective to $[cv, c]$, and since $G(e, \cdot)$ is modular, the intervals are isomorphic, hence have the same length (namely 1). Multiplying from the left by $c^{-1}$ therefore also $[v, f]$ has length 1, and thus $v$ is maximal integral. If $v$ is transposable to $u$, one argues along similar lines.

For the remainder of the claim we may now assume that $u$ is transposable to $v$ (since we already know that $v$ is also maximal integral). Let again $c \in G(e, f)$ be such that $cv = c \land u$ and $e = c \lor u$. If $p = \Phi(u)_e$, then $c^{-1}pc = \Phi(u)_f$. Since $pc \leq c \land p \leq c \land u = cv$, we get $c^{-1}pc \leq v$ and therefore $\Phi(v) \geq \Phi(c^{-1}pc) = \Phi(\Phi(u)_f) = \Phi(u)$. By 3, $\Phi(u)$ is prime and thus maximal integral in $G_+$, which implies $\Phi(u) = \Phi(v)$. \qed

The converse of Lemma 4.11.3 is false in general: A non-maximal integral element can have a prime lower bound.

**Proposition 4.12.**

1. The category $G_+$ is half-factorial. Explicitly: Every $a \in G_+$ possesses a rigid factorization

$$s(a)u_1 \ast \cdots \ast u_k \in \mathbb{Z}^+(a)$$

with $k \in \mathbb{N}_0$ and $u_1, \ldots, u_k \in \mathcal{A}(G_+)$ and the number of factors, $k \in \mathbb{N}_0$, is uniquely determined by $a$. Moreover, if $s(a)v_1 \ast \cdots \ast v_k \in \mathbb{Z}^+(a)$ is another rigid factorization with $v_1, \ldots, v_k \in \mathcal{A}(G_+)$, then there exists a permutation $\tau \in S_k$ such that $u_{\tau(i)}$ is projective to $v_i$ for all $i \in [1, k]$. In particular, $\Phi(u_{\tau(i)}) = \Phi(v_i)$ for all $i \in [1, k]$.

2. Any two rigid factorizations of $a \in G_+$ can be transformed into each other by a number of steps, each of which only involves replacing two successive elements by two new ones.

3. (Transposition.) If $a = uv$ with $u, v \in \mathcal{A}(G_+)$ and $\Phi(u) = P$, $\Phi(v) = Q$, $Q \neq P$, then there exist uniquely determined $v', u' \in \mathcal{A}(G_+)$ such that $\Phi(v') = Q$, $\Phi(u') = P$ and $uv = v'u'$. Explicitly,

$$u' = a \lor \mathcal{P}_{t(a)}, \quad u' \land v = a, \quad u' \lor v = t(a),$$

$$v' = a \lor \mathcal{Q}_{s(a)}, \quad u \land v' = a, \quad u \lor v' = s(a).$$

So $u$ is transposable to $u'$ and $v'$ is transposable to $v$.

4. Given any permutation $\tau' \in S_k$, there exist $w_1, \ldots, w_k \in \mathcal{A}(G_+)$, such that

$$s(a)w_1 \ast \cdots \ast w_k \in \mathbb{Z}^+(a)$$

and $\Phi(w_i) = \Phi(u_{\tau'(i)})$ for all $i \in [1, k]$.

**Proof.** 1, 2. We observe that rigid factorizations of $a$ correspond bijectively to maximal chains of the sublattice $[a, s(a)]$ of $\mathcal{G}(s(a), \cdot)$: If $s(a)w_1 \ast \cdots \ast w_k \in \mathbb{Z}^+(a)$, then $s(a) > u_1 > u_1u_2 > \cdots > u_1 \cdots u_k = a$ is a chain in $[a, s(a)]$ and since $u_1, \ldots, u_k$ are maximal integral, it is in fact a maximal chain of $[a, s(a)]$. Conversely, if $s(a) = x_0 > x_1 > x_2 > \cdots > x_k = a$ is a maximal chain of $[a, s(a)]$ then we set
\[ u_i = x_i^{-1} x_i \] for all \( i \in [1, k] \). These elements are maximal integral, i.e., atoms of \( G_+ \), and \( a = x_k = s(a)x_1(x_1^{-1} x_2)\cdots(x_{k-2}^{-1} x_{k-1})(x_{k-1}^{-1} x_k) = s(a)u_1 \cdots u_k \).

By \( P_6 \), \([a, s(a)]\) satisfies the ACC, but also the DCC because if \( s(a) = x_0 \geq x_1 \geq \cdots \geq a \) is a descending chain in \([a, s(a)]\), then \( x_0^{-1} a \leq x_1^{-1} a \leq \cdots \leq a^{-1} a = t(a) \) is an ascending chain in \( G_+ (t(a)) \) and therefore becomes stationary again by \( P_6 \). Being a modular lattice, \([a, s(a)]\) is therefore of finite length.

The claims now follow from the Jordan–Hölder Theorem for modular lattices (see e.g., [30, p. 333, Theorem 3.77]). The existence of maximal chains implies that \( G_+ \) is atomic (alternatively, use Proposition 3.1 together with the ACC on integral elements). For half-factoriality, and projectivity of the factors, assume that \( u = uv \) for \( i \). By Lemma 4.9, this implies that \( \tau_i \) is maximal integral, i.e., atoms of \( \mathcal{Q} \times \mathcal{Q} \). The equalities \( a = uv \cdot v \) for all \( i \) are derived. Then the uniqueness part of the Jordan–Hölder Theorem implies that \( \tau_i \) is projective to \( v_i \) for all \( i \). By Lemma 4.9, this implies that \( \tau_i \cdot \) is projective to \( v_i \) for all \( i \).

Finally, \( 2 \) follows in a similar manner by induction on the length of \( a \). Fix a composition series of \([u_1 \wedge v_1, a]\). This gives rise to refinements of \( s(a) > u_1 \wedge v_1 \geq a \) and \( s(a) > v_1 \wedge u_1 \geq a \) to composition series of \([a, s(a)]\). Applying the induction hypothesis to \( u_2 \cdots u_k \) (respectively \( v_2 \cdots v_k \)), and the rigid factorization derived from the refined chain \( t(u_1) > u_i^{-1} (u_1 \wedge v_1) \cdots > u_1^{-1} a \) (respectively \( t(v_1) > v_i^{-1} (u_1 \wedge v_1) \cdots > v_1^{-1} a) \) one proves the claim.

3. Let \( e = s(u), q = \mathcal{Q}_e \) and set \( v' = u v \vee q \). We first show:

\textbf{Claim A.} \( q \nleq u \).

\textbf{Claim B.} \( v' \wedge u = u v \).

\textbf{Claim C.} \( v' \) is maximal integral.

\textbf{Proof of Claim A.} Suppose \( q \leq u \). Then \( \mathcal{Q} \leq \Phi(u) = \mathcal{P} \), a contradiction to \( \mathcal{P} \) and \( \mathcal{Q} \) being distinct prime elements of \( G_+ \) (Lemma 4.4). \( \square \)

\textbf{Proof of Claim B.} Since \( G(e, \cdot) \) is modular and \( u v \leq u \),

\[ v' \wedge u = (u v \vee q) \wedge u = u v \vee (q \wedge u). \]

Because \( q \nleq u \) (Claim A), we have \( q \leq q \wedge u \geq qu \) and thus, by maximality of \( u \), \( qu = q \wedge u \). Therefore

\[ u v \vee (q \wedge u) = u v \vee qu = u v \vee u \mathcal{Q}_{\tau(i)}(u) = u (v \vee \mathcal{Q}_{\tau(i)}(u)) = u v. \] \( \square \)

\textbf{Proof of Claim C.} Since \( u v \) is a product of two atoms and \( G_+ \) is half-factorial, it suffices to show \( u v < v' < e \). Suppose first \( u v = v' \). Then \( q \leq u v \leq u \), contradicting Claim A. Assume now \( v' = e \). Then \( u = e \wedge u = v' \wedge u \), and by Claim B therefore \( u = u v \), contradicting \( v < s(v) \). \( \square \)

\textbf{Existence.} We have \( u v = v'u' \) with \( v' \in \mathcal{A}(G_+) \) (by Claim C) and \( u' = v'^{-1} u v \in G_+ \). Since \( G_+ \) is half-factorial, this necessarily implies \( u' \in \mathcal{A}(G_+) \). By definition of \( v' \), \( \mathcal{Q} \leq \Phi(v') < 1_{G_+} \), where the latter inequality is strict because \( v' < e \). Thus \( \Phi(v') = \mathcal{Q} \) and 1 implies \( \Phi(u') = \mathcal{P} \).

\textbf{Uniqueness.} If \( v''u'' = u v \) with \( \Phi(v'') = \mathcal{Q} \), then \( v'' < e \) and \( v'' \geq u v \vee q = v' \). By Claim C, \( v' \) is maximal integral and thus \( v'' = v' \), and then also \( u'' = u' \).

\textbf{Explicit formulas.} Since \( e \geq u \vee v' \geq \Phi(u) e \vee \Phi(v') e = \mathcal{P} e \vee \mathcal{Q}_e = (\mathcal{P} \vee \mathcal{Q})_e = (1_{G_+})_e = e \), it follows that \( u \vee v' = e \). By Claim B, \( u \wedge v' = u v = a \).

The equalities \( u' = a \vee \mathcal{P}_{\tau(i)}(u) \), \( u' \wedge v = a \) and \( u' \vee v = t(a) \) are shown similarly.

4. Write \( \tau' \) as a product of transpositions and use 3. \( \square \)
Proposition 4.12.3 gives an explicit and complete description of the possible relations between two maximal integral elements with coprime lower bound. The case where the lower bounds coincide is more complicated (there can be no relations, or many), but in the case where we will need it, it is quite simple (see Section 7.2).

Corollary 4.13. If \( H \subseteq G_{+} \) is a subcategory, then \( \mathcal{L}_{H}(a) \) is finite and non-empty for all \( a \in H \). If for every prime \( \mathcal{P} \in \mathcal{G}_{+} \) and all (equivalently, one) \( e \in G_{0} \) the set \( \{ u \in \mathcal{A}(G_{+}) \mid \Phi(u) = \mathcal{P} \text{ and } s(u) = e \} \) is finite, then \( \mathcal{Z}_{H}(a) \) is finite for all \( a \in H \).

Proof. Using that \( G_{+} \) is reduced, it follows from \( P_{6} \) that \( H \) satisfies the ACC on principal left and right ideals, and hence \( \mathcal{Z}_{H}(a) \neq \emptyset \). If \( s(a)u_{1} \cdots u_{k} \in \mathcal{Z}_{H}(a) \) with \( k \in \mathbb{N}_{0} \) and \( u_{1}, \ldots, u_{k} \in \mathcal{A}(H) \), then in particular \( u_{i} \prec s(u_{i}) \) for all \( i \in [1, k] \), and therefore \( k \) is bounded by the length of the factorization of \( a \) in \( G_{+} \). A similar argument shows the second claim. \( \Box \)

The properties that all sets of lengths, respectively that all sets of factorizations, are finite have been studied a lot in the commutative setting. Note, if \( H \) is a commutative monoid and \( a \in H \), then \( \mathcal{Z}_{H}(a) \) is finite if and only if \( \mathcal{Z}_{H}(a) \) is finite.

Definition & Lemma 4.14. There exists a unique groupoid epimorphism \( \eta : G \to \mathcal{G} \) such that \( \eta(u) = \Phi(u) \) for all \( u \in \mathcal{A}(G_{+}) \). We call \( \eta \) the abstract norm of \( G \).

Proof. We need to show existence and uniqueness of such a homomorphism. Let \( a \in G_{+} \), and let \( s(a)u_{1} \cdots u_{k} \in \mathcal{Z}^{*}(a) \) with \( u_{1}, \ldots, u_{k} \in \mathcal{A}(G_{+}) \). Since the sequence of \( \Phi(u_{1}), \ldots, \Phi(u_{k}) \) is, up to order, uniquely determined by \( a \) (Proposition 4.12), it follows that we can define \( \eta(a) = \Phi(u_{1}) \cdots \Phi(u_{k}) \), and this is a homomorphism \( G_{+} \to \mathcal{G}_{+} \) with \( \eta(u) = \Phi(u) \) for all \( u \in \mathcal{A}(G_{+}) \). \( G \) is the category of (left and right) fractions of \( G_{+} \), and hence \( \eta \) extends to a unique groupoid homomorphism \( \eta : G \to \mathcal{G} \).

To verify that \( \eta \) is surjective, let first \( \mathcal{P} \in \mathcal{G} \) be a prime element of \( \mathcal{G}_{+} \), and let \( e \in G_{0} \). Let \( u \in G_{+}(e, \cdot) \) be a maximal integral element with \( \mathcal{P}_{u} \leq u \). Then \( \Phi(u) = \mathcal{P} \), and therefore \( \eta(u) = \mathcal{P} \). The claim follows since \( G \) is the free abelian group with basis \( \mathcal{A}(G_{+}) \). \( \Box \)

In general \( \eta \neq \Phi \), since \( \Phi \) need not be a homomorphism, but from Lemma 4.11.2 it follows that for integral \( a \) the prime factorizations of \( \Phi(a) \) and \( \eta(a) \) have the same support and \( v_{\mathcal{P}}(\eta(a)) \geq v_{\mathcal{P}}(\Phi(a)) \) for all primes \( \mathcal{P} \) of \( G_{+} \).

Theorem 4.15. Let \( G \) be an arithmetical groupoid, \( \eta : G \to \mathcal{G} \) the abstract norm, \( H \) a right-saturated subcategory of \( G_{+} \), and \( C = \mathcal{G}/\mathcal{Q}(\eta(H)) \). For \( \mathcal{G} \to C \) set \( [\mathcal{G}] = \mathcal{G}/\mathcal{Q}(\eta(H)) \in \mathcal{C} \), and \( \mathcal{C}_{M} = \{ [\eta(u)] \in \mathcal{C} \mid u \in \mathcal{A}(G_{+}) \} \). Assume that

1. for \( a \in G \) with \( s(a) \in H_{0}, a \in HH^{-1} \) if and only if \( \eta(a) \in \mathcal{Q}(\eta(H)) \),
2. for every \( e \in G_{0} \) and \( g \in \mathcal{C}_{M} \), there exists an element \( u \in \mathcal{A}(G_{+}) \) such that \( s(u) = e \) and \( [\eta(u)] = g \).

Then there exists a transfer homomorphism \( \theta : H \to \mathcal{B}(\mathcal{C}_{M}) \).

Proof. Let \( \theta : H \to \mathcal{B}(\mathcal{C}_{M}) \) be defined as follows: For \( a \in H \) and \( s(a)u_{1} \cdots u_{k} \in \mathcal{Z}_{G_{+}}^{*}(a) \) with \( u_{1}, \ldots, u_{k} \in \mathcal{A}(G_{+}) \), set \( \theta(a) = [\eta(u_{1})] \cdot \cdots \cdot [\eta(u_{k})] \in \mathcal{B}(\mathcal{C}_{M}) \) (in particular, identities are mapped to the empty sequence). We have to show that this definition depends only on \( a \), and not on the particular rigid factorization into maximal integral elements chosen. Let \( s(a)v_{1} \cdots v_{k} \in \mathcal{Z}_{G_{+}}^{*}(a) \) be another such rigid factorization. Then there exists a permutation \( \tau \in \mathcal{S}_{k} \) with \( \eta(u_{i}) = \Phi(u_{i}) = \Phi(v_{\tau(i)}) = \eta(v_{\tau(i)}) \) (due to Proposition 4.12.1 and by definition of \( \eta \)). Therefore \( [\eta(u_{1})] \cdot \cdots \cdot [\eta(u_{k})] = [\eta(v_{1})] \cdot \cdots \cdot [\eta(v_{k})] \).
With this definition \( \theta \) is a homomorphism: Obviously \( \theta(e) = 1_{B(C_M)} \) for all \( e \in H_0 \), and if \( b \in H \) with \( t(a) = s(b) \) and \( s(b)w_1 \cdots w_l \in \mathbb{Z}^*(b) \) is a rigid factorization of \( b \) into maximal integral elements, then \( s(a)u_1 \cdots u_k \cdot w_1 \cdots w_l \) is a rigid factorization of \( ab \). Thus

\[
\theta(ab) = [\eta(u_1)] \cdots [\eta(u_k)] [\eta(w_1)] \cdots [\eta(w_l)] = \theta(a)\theta(b).
\]

We still have to check that \( \theta \) has properties T1 and T2.

If \( \theta(a) = 1_{B(C_M)} \), then \( a \) possesses an empty factorization into maximal elements, hence \( a \in G_0 \cap H = H_0 = H^* \).

\( \theta \) is surjective: \( \theta(e) = 1_{B(C_M)} \) for any \( e \in H_0 \). Let \( k \in \mathbb{N} \) and \( g_1 \cdots g_k \in B(C_M) \). By definition of \( C_M \) and our second assumption, there exists an element \( u_1 \in A(G_+ \mathfrak{h}) \) with \( [\eta(u_1)] = g_1 \) and \( s(u_1) \in H_0 \). Again by our second assumption, for all \( i \in [2, k] \), there exist \( u_i \in A(G_+ \mathfrak{h}) \) with \( s(u_i) = t(u_{i-1}) \) and \( [\eta(u_i)] = g_i \). With \( a = u_1 \cdots u_k \in G \) we get \( [\eta(a)] = [\eta(u_1)] \cdots [\eta(u_k)] = [\eta(u_1)] + \cdots + [\eta(u_k)] = 0 \in C \) and \( s(a) \in H_0 \), and hence \( \eta(a) \in q(\eta(H)) \). By our first assumption, therefore \( a \in H \), and since moreover \( a \) is integral in \( G \) and \( H \) is right-saturated in \( G_+ \), we get \( a \in H \) and \( \theta(a) = g_1 \cdots g_k \).

\( \theta \) satisfies T2: Let \( a \in H \), \( \theta(a) = ST \) with \( S, T \in B(C_M) \) and \( S = g_1 \cdots g_k, T = g_{k+1} \cdots g_l \), where \( k \in \mathbb{N}_0 \) and \( l \in \mathbb{N}_{\geq 2} \). By Proposition 4.12.4, we can find a rigid factorization \( s(a)u_1 \cdots u_l \in \mathbb{Z}^*(a) \) with \( u_i \in A(G_+ \mathfrak{h}) \) and \( [\eta(u_i)] = g_i \) for all \( i \in [1, l] \). Let \( b = s(a)u_1 \cdots u_k \) and \( c = t(b)u_{k+1} \cdots u_l \). Then \( a = bc \). Since \( s(b) \in H_0 \) and \( [\eta(b)] = \sigma(S) = \sigma(H) \), the first assumption implies \( b \in H \), \( H^* \). Then \( s(c) \in H_0 \) and \( c \in H \) follows similarly. Finally, \( \theta(b) = S \) and \( \theta(c) = T \).

The theorem remains true if \( H \) is a left-saturated subcategory of \( G_+ \), and in the first condition the set \( HH^{-1} \) is replaced by \( H^{-1}H \), and the condition \( s(a) \in H_0 \) is replaced by \( t(a) \in H_0 \). Similarly, one can replace the second condition by a symmetrical one, requiring \( t(u) = e \) instead of \( s(u) = e \) (in the proof of the surjectivity of \( \theta \) one then first chooses \( u_k \), followed by \( u_{k-1} \) and so on).

**Remark 4.16.** If \( G \) is a group, then \( G_+ \) is the free abelian monoid with basis \( A(G_+ \mathfrak{h}) \) (Proposition 4.6). As a saturated submonoid of this free abelian monoid, \( H \) is therefore a reduced commutative Krull monoid \([27, \text{Theorem 2.4.8}]) \). Since \( \eta = \text{id}_G \) and \( HH^{-1} = \eta(H)\eta(H)^{-1} \), the first condition is trivially satisfied, and because of \( G_0 = \{1\} \), the second condition is also trivially satisfied.

Conversely, let \( H \) be a normalizing Krull monoid. Then \( H_{\text{red}} = \{ah \mid a \in H \} \) is a reduced commutative Krull monoid, isomorphic to the monoid of its non-zero principal ideals \([25, \text{Corollary 4.14}]) \). The latter is a submonoid of the divisorial fractional ideals of \( H \), which form the free abelian monoid of integral elements in the free abelian group of divisorial ideals of \( H \). In this way we recover the well-known transfer homomorphism for Krull monoids as given for example in \([27, \text{Proposition 3.4.8}]) \) for commutative Krull monoids, and in \([25, \text{Theorem 6.5}]) \) for normalizing Krull monoids.

We continue the discussion of normalizing Krull monoids in Remarks 5.17.2 and 5.24.1, where the divisorial two-sided ideal theory appears as a special case of the divisorial one-sided ideal theory.

### 5. Divisorial ideal theory in semigroups

In this section we develop a divisorial one-sided ideal theory in semigroups. This follows again original ideas of Asano and Murata and generalizes the corresponding theory in rings and the theory of divisorial two-sided ideals in cancellative semigroups (see \([2,3,4,6,5,17]) \) for classical treatments, and \([42,32,33,25,36]) \) for more modern treatments in this area). In particular, the one-sided ideal theory of classical maximal orders over Dedekind domains is a special case of the theory presented here.

The divisorial fractional one-sided ideals with left- and right-orders maximal in a fixed equivalence class of orders form a groupoid as studied in the previous section (this was in fact the motivation for Brandt to introduce the notion of a groupoid, see \([9,10]) \). We connect the factorization theory of elements of a maximal order \( H \) with the one for the cancellative small category of integral principal ideals with left- and right-order conjugate to \( H \), and apply results from the previous section to the factorization of elements in \( H^* \). The main result in this section is Theorem 5.23. After having
derived it we discuss in detail the case of rings, and of classical maximal orders (Section 5.1 and Section 5.2).

A semigroup Q is called a quotient semigroup if every cancellative element is invertible in Q, in short \( Q^* = Q \times \). A subsemigroup \( H \subset Q \) is a right order in Q if \( H(H \cap Q^*)^{-1} = Q \), and \( H \) is a left order in Q if \( (H \cap Q^*)^{-1}H = Q \). \( H \) is an order in Q if it is a left and a right order. We summarize the connection between a subsemigroup \( H \subset Q \) being an order, and \( Q \) being a semigroup of (left and right) fractions of \( H \).

**Lemma 5.1.** Let \( Q \) be a quotient semigroup, and \( H \subset Q \) a subsemigroup.

1. If \( H \) is an order in \( Q \), then \( H^* = H \cap Q^* \) and \( Q = q(H) \).
2. If \( q(H) = Q \), then \( H^* = H \cap Q^* \) and \( H \) is an order in \( Q \).
3. If \( H \) is an order in \( Q \), \( H' \) is a subsemigroup of \( Q \) and there exist \( a, b \in Q^* \) with \( aHb \subset H' \), then \( H' \) is an order in \( Q \).

**Proof.** 1. It suffices to show \( H^* = H \cap Q^* \), and the inclusion \( H \cap Q^* \subset H^* \) is clear. Let \( a \in H^* \), and \( q, q' \in Q \) with \( aq = aq' \). Since \( H \) is a right order in \( Q \), there exist \( c, d \in H \) and \( s \in H \cap Q^* \) with \( q = cs^{-1} \) and \( q' = ds^{-1} \), where we can choose a common denominator because \( H \cap Q^* \) satisfies the right Ore condition in \( H \). Then \( ac = ad \), and, because \( a \in H^* \), also \( c = d \), showing \( q = q' \). Since \( H \) is a left order it follows in the same way that \( a \) is right-cancellative in \( Q^* \), and hence \( a \in H \cap Q^* \).

2. It again suffices to show \( H^* = H \cap Q^* \), and this follows in the same way as in 1.

3. It suffices to show that every \( q \in Q \) has representations of the form \( q = cs^{-1} = t^{-1}d \) with \( c, d \in H' \) and \( s, t \in H' \cap Q^* \). Since \( H \) is an order in \( Q \), there exist \( c', d' \in H \) and \( s', t' \in H \cap Q^* \) with \( a^{-1}qa = c's'^{-1} \) and \( bqb^{-1} = t'^{-1}d' \). Setting \( c = ac'b, d = ad'b, s = as'b \) and \( t = at'b \), the claim follows. ∎

For the remainder of this section, let \( Q \) be a quotient semigroup.

If \( H \) and \( H' \) are orders in \( Q \), then \( H \) is (Asano-)equivalent to \( H' \), written \( H \sim H' \), if there exist \( a, b, c, d \in Q^* \) with \( aHb \subset H' \) and \( cH'd \subset H \). This is an equivalence relation on the set of orders in \( Q \). An order \( H \) is maximal if it is maximal within its equivalence class with respect to set inclusion.

A feature of the non-commutative theory is that often there is no unique maximal order in a given equivalence class, and in fact in the most important cases we study there are usually infinitely many, but only finitely many conjugacy classes of them. In studying the divisorial one-sided ideal theory of a maximal order \( H \), one has to study the ideal theory of all maximal orders in its equivalence class at the same time.

Let \( H, H' \subset Q \) be subsemigroups (not necessarily orders), and let \( X, Y \subset Q \). As in the previous sections \( XY = \{xy \mid x \in X, \ y \in Y \} \). \( X \) is a left \( H \)-module if \( HX \subset X \), and a right \( H' \)-module if \( XH' \subset X \). It is an \( (H, H') \)-module if it is a left \( H \) and a right \( H' \)-module, i.e., \( HXH' \subset X \). We define

\[
(Y;_2 X) = \{q \in Q \mid Xq \subset Y \} \quad \text{and} \quad (Y;_1 X) = \{q \in Q \mid qX \subset Y \}.
\]

Every left \( H \)-module is an \( (H, \{1\}) \)-module, and similarly every right \( H' \)-module is a \( \{1\}, H' \)-module. We set \( O_l(X) = (X;_1 X) \) and \( O_r(X) = (X;_2 X) \).

**Lemma 5.2.** Let \( H, H' \) be subsemigroups of \( Q \) and let \( X \) be an \( (H, H') \)-module.

1. \( (H;_2 X) \) and \( (H;_1 X) \) are \( (H', H) \)-modules.
2. \( X \subset (H;_2 (H;_2 X)) \) and \( X \subset (H;_1 (H;_1 X)) \).
3. \( O_l(X) \) and \( O_r(X) \) are subsemigroups of \( Q \).
4. \( (O_l(X);_2 X) = (O_r(X);_2 X) = \{q \in Q \mid XqX \subset X \} \).
5. \( X \subset O_l(X) \) if and only if \( X \subset O_r(X) \) if and only if \( X^2 \subset X \).
Lemma 5.5. \( H \) is a fractional left (right) \( H \)-ideal, or \( \bigcap \mathcal{O}_r(X) = \{ q \in Q \mid Xq \subset X \} \). Let \( q \in Q \). Then \( Xq \subset X \) is equivalent to \( Xq \subset \mathcal{O}_r(X) \), which in turn is equivalent to \( q \in (\mathcal{O}_r(X))_rX \).

Proof. Let \( \mathcal{O}_r(X) = \{ \mathcal{O}_r(X) \} \) and \( \mathcal{O}_r(X) \subset X \subset X \), which implies \( \mathcal{O}_r(X) \subset \mathcal{O}_r(X) \). The claim for \( \mathcal{O}_r(X) \) is shown similarly.

We show \( (\mathcal{O}_r(X))_rX = \{ q \in Q \mid Xq \subset X \} \). Let \( q \in Q \). Then \( Xq \subset X \) is equivalent to \( Xq \subset \mathcal{O}_r(X) \), which in turn is equivalent to \( q \in (\mathcal{O}_r(X))_rX \).

Immediate from the definitions of \( \mathcal{O}_r(X) \) and \( \mathcal{O}_r(X) \).  

Definition 5.3. For \( X \in Q \) as in Lemma 5.2, we define

\[
X^{-1} = (\mathcal{O}_r(X))_rX = (\mathcal{O}_l(X))_rX = \{ q \in Q \mid Xq \subset X \} \quad \text{and} \quad X_y = (X^{-1})^{-1}.
\]

Definition 5.4. Let \( H \) and \( H' \) be orders in \( Q \).

1. A fractional left \( H \)-ideal is a left \( H \)-module \( I \) such that \( I \cap Q^* \neq \emptyset \) and \( (H'_I) \cap Q^* \neq \emptyset \).
2. A fractional right \( H' \)-ideal is a right \( H' \)-module \( I \) such that \( I \cap Q^* \neq \emptyset \) and \( (H'_I) \cap Q^* \neq \emptyset \).
3. If \( I \) is a fractional left \( H \)-ideal and \( \mathcal{O}_r(X)_rX \) is a fractional right \( H' \)-ideal, then \( I \) is a fractional \( (H, H') \)-ideal.
4. A fractional \( H \)-ideal is a fractional \( (H, H') \)-ideal.
5. \( I \) is a left \( H \)-ideal if it is a fractional left \( H \)-ideal and \( I \subset H \). A right \( H' \)-ideal is defined analogously.
6. If \( I \) is a left \( H \)-ideal and \( \mathcal{O}_r(X)_rX \) is an \( (H, H') \)-ideal, then \( I \) is an \( (H, H') \)-ideal.
7. An \( H \)-ideal is an \( (H, H') \)-ideal.
8. A fractional left \( H \)-ideal \( I \) is integral if \( I \subset \mathcal{O}_r(I) \) (equivalently, \( I \subset \mathcal{O}_r(I) \)). The same definition is made for fractional right \( H' \)-ideals.

If \( H \) is a maximal order, then the notions of a left \( H \)-ideal and that of an integral fractional left \( H \)-ideal coincide (this will follow from Lemma 5.6.1 and Lemma 5.6.2). We will sometimes call a fractional left (right) \( H \)-ideal one-sided to emphasize that it need not be a fractional right (left) \( H \)-ideal, or two-sided to emphasize that it is indeed a fractional \( H \)-ideal.

We recall some properties of fractional left \( H \)-ideals and first observe the following.

Lemma 5.5. If \( H \) is an order in \( Q \) and \( I \) is a fractional left \( H \)-ideal, then \( \mathcal{O}_r(I) \) and \( \mathcal{O}_r(I) \) are orders. \( I \) is a fractional \( \mathcal{O}_r(I) \), \( \mathcal{O}_r(I) \)-ideal.

Proof. Let \( a \in I \cap Q^* \), and let \( b \in (H_I) \cap Q^* \). By definition, \( H \subset \mathcal{O}_r(I) \) and since \( H \) is an order and \( \mathcal{O}_r(I) \) a semigroup, it is also an order. \( \mathcal{O}_r(I) I \subset I \) and \( b \in (\mathcal{O}_r(I))_rI \) imply that \( I \) is a fractional left \( \mathcal{O}_r(I) \)-ideal. Since \( b \in (\mathcal{O}_r(I))_rI \), \( (\mathcal{O}_r(I))_rI \) holds that \( b \mathcal{O}_r(I) a \subset bI \subset \mathcal{O}_r(I) \), and since \( \mathcal{O}_r(I) \) is a semigroup and \( \mathcal{O}_r(I) \) an order, \( \mathcal{O}_r(I) \) is also an order. Therefore \( I \) is also a fractional right \( \mathcal{O}_r(I) \)-ideal.  

The previous lemma implies that it is no restriction to require \( I \) to be a fractional \( (H, H') \)-ideal over it, say, being a fractional left \( H \)-ideal (set \( H' = \mathcal{O}_r(I) \)).

Lemma 5.6. Let \( H \) and \( H' \) be orders in \( Q \), and let \( I \) be a fractional \( (H, H') \)-ideal.

1. The orders \( H \), \( H' \), \( \mathcal{O}_r(I) \), and \( \mathcal{O}_r(I) \) are all equivalent.
2. If \( H \) is maximal, then \( \mathcal{O}_r(I) = H \), and similarly, if \( H' \) is maximal, then \( \mathcal{O}_r(I) = H' \).
3. \( (H_I) \) is a fractional right \( H \)-ideal, and \( (H'_I) \) is a fractional left \( H' \)-ideal.
4. If \( I \) is a fractional left \( H \)-ideal, then \( I \cap J \) and \( I \cup J \) are fractional left \( H \)-ideals.
5. If \( \{ I_m \}_{m \in M} \) is a non-empty family of left \( H \)-ideals for some index set \( M \), then \( \bigcup_{m \in M} I_m \) is a left \( H \)-ideal.
6. If \( H'' \) is an order, and \( K \) is a fractional \( (H', H'') \)-ideal, then \( IK \) is a fractional \( (H, H'') \)-ideal.
Lemma 5.7. Let \( H \) and \( H' \) be orders in \( Q \).

1. If \( H \sim H' \), then there exist \( a, b \in H' \) with \( ah'b \subset H \). If moreover \( H \subset H' \), then we can even take \( a, b \in H' \).

2. If \( H \sim H' \) and \( H \subset H' \), then there exists an order \( H'' \) and \( a, b \in H'' \) such that \( H \subset H'' \subset H' \) and \( ah' \subset H'' \) and \( ah'' \subset H'' \).

3. The following statements are equivalent:
   (a) \( H \sim H' \).
   (b) There exists a fractional \((H, H')\)-ideal.
   (c) There exists a fractional \((H'', H'')\)-ideal.

Proof. 1. There exist \( x, y \in Q' \) with \( xH' y \subset H \). Since \( H' \) is an order in \( Q \), \( x = ac \) and \( y = d^{-1}b \) with \( a, b \in H' \) and \( c, d \in H' \cap Q' \). If \( H \subset H' \) we even take \( a, b, c, d \) in \( H \). Then \( ah'b \subset c^{-1}H' d^{-1}b \subset H \).

2. Using 1 choose \( a, b \in H' \) with \( ah'b \subset H \). Let \( H'' = H \cup ah' \cup HaH' \). Then it is easily checked that \( H'' \cap H'' \subset H'' \) and obviously \( H \subset H'' \), thus \( H'' \) is an order. Moreover, \( H'' \subset H' \), \( H''b \subset H \) and \( ah' \subset H'' \), as claimed.

3. (a) \(\Rightarrow\) (b): By 1 there exist \( a, b \in H' \) with \( ah'b \subset H' \) and \( c, d \in H' \) with \( ch'd \subset H \). Define \( I = HbcH' \). Clearly \( I \) is an \((H', H')\)-module with \( bc \in I \cap Q' \). Since \( 1 = ahbcH' \subset H'ch' \subset H' \) and \( I = HbcH'\subset HbH \subset H \), \( I \) is a fractional \((H, H')\)-ideal.

(b) \(\Rightarrow\) (a): By Lemma 5.6.1.

(a) \(\Leftrightarrow\) (c) follows by symmetry, swapping the roles of \( H \) and \( H' \). \(\square\)

Lemma 5.8. Let \( H \) be an order in \( Q \). The following statements are equivalent.

(a) \( H \) is a maximal order.
(b) If \( I \) is a fractional left \( H \)-ideal, then \( \mathcal{O}_I(l) = H \) and if \( J \) is a fractional right \( H \)-ideal, then \( \mathcal{O}_J(l) = H \).
(c) If \( I \) is a fractional \( H \)-ideal, then \( \mathcal{O}_I(l) = \mathcal{O}_I(l) = H \).
(d) If \( I \) is an \( H \)-ideal, then \( \mathcal{O}_I(l) = \mathcal{O}_I(l) = H \).

Proof. (a) \(\Rightarrow\) (b): By Lemma 5.6.2, \( \mathcal{O}_I(l) = H \) and \( \mathcal{O}_J(l) = H \).
(b) \(\Rightarrow\) (c) \(\Rightarrow\) (d): Trivial.
(d) \(\Rightarrow\) (a): Assume \( H' \) is an order equivalent to \( H \) and \( H \subset H' \). Applying Lemma 5.7.2 we find an equivalent order \( H'' \) with \( H \subset H'' \subset H' \) and \( a, b \in Q' \) with \( ah' \subset H'' \) and \( ah'b \subset H \). Let \( I = \{x \in Q \mid \ldots\} \).
\(H' \subset H\). Then \(I\) is an \(H\)-ideal, and \(H'' \subset O_I(1)\), implying \(H'' = H\) by (d). Set \(J = \{x \in Q \mid xH' \subset H\}\). Then \(J\) is again an \(H\)-ideal (we use \(a \in J\) since \(H'' = H\)), and \(H' \subset O_I(J)\) implies \(H' = H\). \(\Box\)

**Lemma 5.9.** Let \(H\) be a maximal order in \(Q\), let \(I\) and \(J\) be fractional left \(H\)-ideals, and let \(K\) be a fractional left \(O_I(I)\)-ideal.

1. \(O_I(I) = H\), \(I^{-1}\) is a fractional right \(H\)-ideal with \(O_I(I^{-1}) = H\) and \(I^v\) is a fractional left \(H\)-ideal with \(O_I(I^v) = H\) and \(I \subset I^v\). Moreover, \(O_I(I^v) = H^v\).
2. If \(a \in Q^*\), then \(Ha\) is a fractional left \(H\)-ideal with \(O_I(Ha) = a^{-1}(Ha) = a^{-1}H\) and \((Ha)_v = Ha\).
3. If \(I \subset J\) then \(J^{-1} \subset I^{-1}\) and \(J^v \subset I^v\).
4. \(I \subset I^v = (I^v)_v\), \((I^{-1})^v = I^{-1}\) and \(O_I(I^v) = O_I(I)\).
5. \((I_v \cap J_v)_v = I_v \cap J_v\).
6. \((I \cup J)_v = (I_v \cup J_v)_v\).
7. If \(O_I(I)\) and \(O_I(K)\) are also maximal, then \((IK)_v = (IK)_v\).

**Proof.** 1. By **Lemma 5.6.2**, \(O_I(I) = H\), and thus **Lemma 5.6.3** implies that \(I^{-1} = (H;1)\) is a right \(H\)-ideal. By the symmetric statement of what we just showed for fractional right \(H\)-ideals, therefore \(O_I(I^{-1}) = H\) and \(I^v\) is a fractional left \(H\)-ideal. Applying the first part of the statement to \(I^v\), we get \(O_I(I^v) = H\). Now \(I \subset I^v\) follows from **Lemma 5.2.2**, and \(H^v = H\) from \(H^v = (H;1) = H\).

2. Since \(a \in H \cap Q^*\) and \(a^{-1} \in (H;1)\), \(Ha\) is a fractional left \(H\)-ideal. Certainly \(a^{-1}Ha \subset O_I(Ha)\). Conversely, if \(x \in O_I(Ha)\), then \(ax \in Ha\) and thus \(x \in a^{-1}Ha\), so that altogether \(O_I(Ha) = a^{-1}Ha\).

3. If \(a \in H \cap Q^*\), then \(Ha \subset H\) if \(ax \in a^{-1}H\), and \(Hax \subset H\), hence \(J^{-1} \subset I^{-1}\). By 1, \(J^{-1}\) and \(I^{-1}\) are fractional right \(H\)-ideals with \(O_I(J^{-1}) = O_I(I^{-1}) = H\), and the symmetric statement for right fractional \(H\)-ideals obtained \(I^v \subset J^v\).

4. By 1, \(I^{-1}\) is a fractional right \(H\)-ideal with \(O_I(I^{-1}) = H\), and \(I^v\) is a fractional left \(H\)-ideal with \(O_I(I^v) = H\). Moreover, also by 1, \(I \subset I^v\) and \(I^{-1} \subset (I^v)_v = (I^{-1})^{-1} = I^{-1}\). It follows from 3, that \(I^v \subset (I^{-1})_v\) and \(I^{-1} = (I^v)_v\). Therefore \((I^{-1})^v = (I^{-1})^{-1} \subset (I^{-1})^{-1} = I^{-1}\), whence \(I^v = (I^{-1})_v\).

5. \(I \cup J \subset I \cup J \subset I \cup J \subset (I \cup J)_v\) and by taking divisorial closures, and 4, the claim follows.

6. We use \(O_I(I^v) = O_I(I)\) and \(O_I(K) = O_I(K_v)\) from (1). We have \(I \subset I^v \subset I^v \subset I^v\), and similarly \(IK \subset IK \subset IK \subset IK\). By (1), this implies \((IK)_v \subset (IK)_v \subset (IK)_v \subset (IK)_v\).

7. To prove the claim it suffices to show \((I^v)_v \subset (IK)_v\), which will follow from 3 and 4 if we show \((I^v)_v \subset (IK)_v\). Since \(IK_1 \subset O_I(I)\), we have \(K(IK) \subset O_I(I)_v\). The last equality is due to 4. Multiplying by \(I\) from the right gives \(K(IK)I \subset I^{v^2}I_v\). By definition, \(I^{v^2}I_v \subset O_I(I_v)\). Since \(O_I(I^v) = O_I(I)\), and \(O_I(K)\), therefore \(K(IK)I \subset O_I(K)\). Finally \((IK)^{-1}I \subset (IK)^{-1}\), as \(IK_1^{-1}I \subset (IK)_v\). (Using 4 again). Multiplying by \(K\) from the right and using \(O_I(K_v) = O_I(K)\), we obtain \((IK)^{-1}I \subset (IK)^{-1}\). Since \(O_I((IK)^{-1}) = O_I(K)\), this implies \(I^v \subset (IK)^{-1}\).

**Definition 5.10.** Let \(H\) be an order in \(Q\). A fractional left or right \(H\)-ideal \(I\) is called **divisorial** if \(I = I^v\).

If \(I\) is a fractional left \(H\)-ideal for a maximal order \(H\), then it is not necessarily true that \(O_I(I)\) is again a maximal order. The next proposition shows that for divisorial fractional left or right \(H\)-ideals with \(H\) maximal, both \(O_I(I)\) and \(O_I(I)\) are maximal. We can define an associative partial operation, the \(v\)-product, by \(I \cdot v = (IJ)_v\) when \(J\) is a divisorial fractional left \(O_I(I)\)-ideal. Moreover it shows that every divisorial fractional left or right ideal is \(v\)-invertible, i.e., invertible with respect to this operation.

**Proposition 5.11.** Let \(H\) be a maximal order in \(Q\). Let \(I\) be a fractional left \(H\)-ideal. Then:

1. \(O_I(I^{-1})\) is a maximal order. In particular, \(O_I(I^v)\) is a maximal order.
2. \((I^{-1})_v = \mathcal{O}_I(I)\) and if \(\mathcal{O}_I(I)\) is also maximal, then \((I^{-1})_v = \mathcal{O}_I(I)\).
3. If \(I\) is a divisorial fractional left \(H\)-ideal, \(J\) a divisorial fractional left \(\mathcal{O}_H(I)\)-ideal and \(K\) a divisorial fractional left \(\mathcal{O}_F(J)\)-ideal, then

\[
(I \cdot_v J) \cdot_v K = I \cdot_v (J \cdot_v K).
\]

**Proof.** 1. Because \(H\) is maximal, \(\mathcal{O}_H(I) = H\). Trivially, \(\mathcal{O}_I(I) \subset \mathcal{O}_I(I^{-1})\). Let \(H' \supset \mathcal{O}_I(I^{-1})\) be an order with \(H' \sim \mathcal{O}_I(I^{-1})\). Then \(J = IH'I^{-1}\) is an \((H, H)\)-module and if \(a \in I \cap Q^*\) and \(b \in I^{-1} \cap Q^*\), then \(ab \in J\) and moreover

\[
J^2 = IH'I^{-1}IH'I^{-1} \subset IH'\mathcal{O}_I(I^{-1})H'I^{-1} = IH'I^{-1} = J,
\]

showing that \(J\) is an integral left \(\mathcal{O}_H(I)\)-ideal.

We claim \(H = \mathcal{O}_I(J)\). Since \(H = \mathcal{O}_I(I) \subset \mathcal{O}_I(J)\) and \(H\) is maximal, it suffices to show \(\mathcal{O}_I(J) \sim H\). To this end we first show \(bJa \subset H'\):

\[
bJa = bIH'I^{-1}a \subset I^{-1}IHI^{-1}I \subset \mathcal{O}_I(I)H'\mathcal{O}_I(I) = H'.
\]

Since \(H' \sim H\), there exist \(c, d \in Q^*\) with \(cH'd \subset H\). Since \(ab \in J \cap Q^*\) therefore \(cb(\mathcal{O}_I(J)ab)ad \subset cbJa\), proving the claim.

Therefore, from the definition of \(J\), \(H'I^{-1} \subset (J; I) \subset (\mathcal{O}_I(J)\mathcal{I}) = (H; I) = I^{-1}\) and thus \(H' \subset \mathcal{O}_I(I^{-1})\), and, because we started out with the converse inclusion, also \(H' = \mathcal{O}_I(I^{-1})\).

Now \(\mathcal{O}_I(I_v) = \mathcal{O}_I(I^{-1})\) implies the “in particular” statement.

2. We have to show \((I^{-1})_v = \mathcal{O}_I(I)\) and \((I^{-1})_v = \mathcal{O}_I(I)\), and we check the first equality as the second one then follows analogously. The inclusion \(I^{-1} \subset \mathcal{O}_I(I)\) implies \((I^{-1})_v \subset \mathcal{O}_I(I)_v = \mathcal{O}_I(I)\). It remains to prove \(\mathcal{O}_I(I) \subset (I^{-1})_v\). Due to maximality of \(\mathcal{O}_I(I)\), it holds that \(\mathcal{O}_I(I^{-1}) = \mathcal{O}_I(I)\), and therefore \(I^{-1}I(I^{-1})^{-1} \subset \mathcal{O}_I(I)\). Thus \(I^{-1}I(I^{-1})^{-1} \subset I^{-1}\), and \((I^{-1})^{-1} \subset \mathcal{O}_I(I^{-1}) = \mathcal{O}_I(I)\). By Lemma 5.9.3, therefore \(\mathcal{O}_I(I) \subset (I^{-1})_v\).

3. Using Lemma 5.9.7, which can be applied due to 1. \(((I J) \mathcal{K})_v = (I J K)_v = (I(J K)_v)\).

**Corollary 5.12.** If \(H\) is a maximal order, then every order \(H'\) with \(H' \sim H\) is contained in a maximal order equivalent to \(H\).

**Proof.** By Lemma 5.7.3, there exists a fractional \((H, H')\)-ideal \(I\). Then \(I_v\) is divisorial, \(\mathcal{O}_H(I_v) \sim \mathcal{O}_I(I_v) = H\), \(H' \subset \mathcal{O}_I(I_v)\) and by Proposition 5.11.1 \(\mathcal{O}_I(I_v)\) is maximal.

**Corollary 5.13.** Let \(\alpha\) denote an equivalence class of maximal orders of \(Q\). Let

\[
\mathcal{F}_v(\alpha) = \{I \mid I\text{ is a divisorial fractional left (or right) }H\text{-ideal with }H \in \alpha\}
\]

and

\[
\mathcal{I}_v(\alpha) = \{I \mid I\text{ is a divisorial left (or right) }H\text{-ideal with }H \in \alpha\}.
\]

Then \((\mathcal{F}_v(\alpha), \cdot_v, \subset)\) is a lattice-ordered groupoid, with identity elements the maximal orders in \(\alpha\). If \(I, J\) are in \(\mathcal{F}_v(\alpha)\) with \(\mathcal{O}_H(I) = \mathcal{O}_H(J)\) or \(\mathcal{O}_I(I) = \mathcal{O}_I(J)\), then \(I \wedge J = I \cap J\) and \(I \vee J = I \cup J\). Moreover, \(\mathcal{I}_v(\alpha)\) is the subcategory of integral elements.

**Proof.** For \(I \in \mathcal{F}_v(\alpha)\) we have \(\mathcal{O}_H(I) \cdot_v I = I \cdot_v \mathcal{O}_H(I)\). If \(J \in \mathcal{F}_v(\alpha)\), then the \(v\)-product \(I \cdot_v J\) is defined whenever \(\mathcal{O}_H(I) = \mathcal{O}_H(J)\), and then \(I \cdot_v J\) is a divisorial fractional \((\mathcal{O}_H(I), \mathcal{O}_H(J))\)-ideal. The \(v\)-product is associative when it is defined (Proposition 5.11.3). Therefore \(\mathcal{F}_v(\alpha)\) with \(\cdot_v\) as composi-
tion is a category where the set of identities is the set of maximal orders, \( \alpha, \) and for \( I \in \mathcal{F}_v(\alpha) \) we have \( s(I) = \mathcal{O}_I(I) \) and \( t(I) = \mathcal{O}_I(I) \). This category is a groupoid due to Proposition 5.11.2.

On \( \mathcal{F}_v(\alpha) \) set inclusion defines a partial order, and obviously also the restrictions to \( \{ I \in \mathcal{F}_v(\alpha) \mid \mathcal{O}_I(I) = H \} \) and \( \{ I \in \mathcal{F}_v(\alpha) \mid \mathcal{O}_I(I) = H \} \) for \( H \in \alpha \), given by set inclusion in these subsets, are partial orders. Let \( I, J \in \mathcal{F}_v(\alpha) \) with \( \mathcal{O}_I(I) = \mathcal{O}_J(J) \). Then \( I \cap J \in \mathcal{F}_v(\alpha) \) and \( I \cup J \in \mathcal{F}_v(\alpha) \) (by Lemmas 5.6 and 5.9), and clearly they are the infimum respectively supremum of \( \{ I, J \} \) in \( \{ I \in \mathcal{F}_v(\alpha) \mid \mathcal{O}_I(I) = H \} \), making this set lattice-ordered. Symmetric statements hold if \( \mathcal{O}_I(I) = \mathcal{O}_J(J) \). If \( \mathcal{O}_I(I) = \mathcal{O}_J(J) \) and \( \mathcal{O}_I(I) = \mathcal{O}_J(J) \) both hold, then also \( \mathcal{O}_I(I \cap J) = \mathcal{O}_J(I \cup J) = \mathcal{O}_I(I) \) and \( \mathcal{O}_J(I \cap J) = \mathcal{O}_I(I \cup J) = \mathcal{O}_J(J) \) both hold. Therefore \( (\mathcal{F}_v(\alpha), \subseteq) \) is a lattice-ordered groupoid with the claimed meet and join. It is immediate from the definitions that \( \mathcal{F}_v(\alpha) \) is the subcategory of integral elements of this lattice-ordered groupoid.

**Definition & Lemma 5.14.** An order \( H \) is bounded if it satisfies the following equivalent conditions:

(a) Every fractional left \( H \)-ideal and every fractional right \( H \)-ideal contains a fractional (two-sided) \( H \)-ideal.

(b) Every left \( H \)-ideal and every right \( H \)-ideal contains a (two-sided) \( H \)-ideal.

(c) For all \( a \in Q^* \) there exist \( b, c \in Q^* \) such that \( bH \subseteq Ha \) and \( Hc \subseteq aH \).

(d) For all \( a \in Q^* \) there exist \( b, c \in Q^* \) such that \( Ha \subseteq bH \) and \( aH \subseteq Hc \).

(e) For all \( a \in Q^* \), \( HaH \) is a fractional (two-sided) \( H \)-ideal.

(f) For all \( a \in Q^* \) there exists a fractional (two-sided) \( H \)-ideal \( I \) with \( a \in I \).

(g) If \( M \subseteq Q \) and \( a, b \in Q^* \) with \( aMb \subseteq H \), then there exist \( c, d \in Q^* \) with \( cM \subseteq H \) and \( Md \subseteq H \).

**Proof.** (a) \( \Rightarrow \) (b): Trivial.

(b) \( \Rightarrow \) (c): Let \( a \in Q^* \). Then \( a = d^{-1}c \) with \( d, c \in H \cap Q^* \), and \( Ha = Hd^{-1}c \subseteq Hc \). By (b), \( Hc \) contains an \( H \)-ideal \( J \). If \( b \in J \), then \( bH \subseteq J \subseteq Hc \). The symmetric claim follows similarly.

(c) \( \Rightarrow \) (d): By (c) applied to \( a^{-1} \), there exist \( c, d \in Q^* \) with \( bH \subseteq Ha^{-1}c \) and \( Hc \subseteq a^{-1}H \). Then \( Ha \subseteq bH \) and \( Ha \subseteq Hc \).

(d) \( \Rightarrow \) (e): \( HaH \) is an \((H, H)\)-module and contains the element \( a \in Q^* \). Let \( b, c \in Q^* \) with \( Ha \subseteq bH \) and \( aH \subseteq Hc \). Then \( HaH \subseteq bH \) and \( HaH \subseteq Hc \), hence \( b^{-1} \in (H; HaH) \) and \( c^{-1} \in (H; HaH) \).

(e) \( \Rightarrow \) (f): Trivial.

(f) \( \Rightarrow \) (g): \( aM \subseteq Hb^{-1} \subseteq Hb^{-1}H \), and the latter being contained in a fractional \( H \)-ideal, there exists \( a' \in Q^* \cap (Hb^{-1}H) \) and thus \( a' \in H \subseteq H \). Similarly, \( Mb \subseteq a^{-1}H \subseteq Ha^{-1}H \), and there exists a \( a'' \in Q^* \cap (H; Ha^{-1}H) \). Thus \( b'' \in Hb^{-1} \subseteq Hb^{-1}H \).

(g) \( \Rightarrow \) (a): Let \( I \) be a fractional left \( H \)-ideal and \( a \in I \). Then \( (Ha^{-1})a \subseteq H \) and so there exists \( a \in Q^* \) such that \( Ha^{-1} \subseteq H \), and thus \( Hb \subseteq Ha \). Therefore \( Hb \subseteq Ha \subseteq I \) and \( Hb \subseteq H \) is a fractional \( H \)-ideal contained in \( I \) as \( b \in Hb \), \( a^{-1} \in (Hb; Hb) \) and, by (g) again, there exists \( c \in Q^* \) with \( c(Hb) \subseteq H \), whence \( c \in (Hb; Hb) \). The case where \( I \) is a fractional right \( H \)-ideal is similar.

**Lemma 5.15.**

1. Let \( H \) and \( H' \) be orders in \( Q \). If \( H \) is bounded and \( H \sim H' \), then \( H' \) is also bounded.

2. Let \( H \) and \( H' \) be bounded equivalent maximal orders of \( Q \). Then there exists an \((H, H')\)-ideal \( I \).

**Proof.** 1. Because \( H \sim H' \) and \( H \) is bounded, there exist \( c, d \in Q^* \) with \( cH \subseteq H' \subseteq dH \) (using (c) and (d)) of the equivalent characterizations of boundedness). We verify condition (c) for \( H' \). Let \( a \in Q^* \). Then \( cHa \subseteq HA \), and there exists \( x \in Q^* \) with \( xH \subseteq Ha \). Then \( cxH \subseteq Ha \) and finally \( cxd^{-1}H' \subseteq cxH \subseteq H'a \). Similarly, one finds \( z \in Q^* \) with \( H'z \subseteq aH' \).

2. We show: If \( H \) and \( H' \) are bounded equivalent maximal orders, then \( H' \) is a fractional \((H, H)\)-ideal. Then \( (H')^{-1} \) is an \((H, H)\)-ideal (since \( \mathcal{O}_I(H') = H \) by maximality of \( H \) and \( H \subseteq H' \), Lemma 5.9.3 implies \( (H')^{-1} \subseteq H \); similarly, one shows \( (H')^{-1} \subseteq H' \).

Clearly \( H' \) is an \((H, H)\)-module and \( 1 \in H' \). We need to show that there exist \( a, b \in Q^* \) with \( H'a \subseteq H' \) and \( bH' \subseteq H \). Since \( H \) and \( H' \) are bounded and equivalent there exist \( a, b \in Q^* \) with \( Ha \subseteq H' \) and \( bH' \subseteq H \), and the claim follows.
**Proposition 5.16.** Let $\alpha$ be an equivalence class of maximal orders in $Q$. $(F_\nu(\alpha), \cdot_\nu, \subseteq)$ is an arithmetical groupoid if and only if all $H \in \alpha$ (equivalently, one $H \in \alpha$) satisfy the following three conditions:

1. $H$ satisfies the ACC on divisorial left $H$-ideals and the ACC on divisorial right $H$-ideals,
2. $H$ is bounded,
3. the lattice of divisorial fractional left $H$-ideals is modular, and the lattice of divisorial right $H$-ideals is modular.

**Proof.** From Corollary 5.13 we already know that $F_\nu(\alpha)$ is a lattice-ordered groupoid. As in the discussion after Definition 4.2 and from Lemma 5.15, we see that if one representative $H \in \alpha$ satisfies $A_1$–$A_3$, then the same is true for all $H' \in \alpha$.

Assume first that $A_1$–$A_3$ hold. Then $P_1$ holds due to Lemma 5.2.5, property $P_2$ is just $A_3$ in the present setting. $P_3$ follows easily: If $I \subseteq J$ are divisorial fractional left $H$-ideals, and $K$ is a divisorial fractional right $H$-ideal, then $KI \subseteq KJ$ and therefore $K \cdot_\nu I = (KI)_\nu \subseteq (KJ)_\nu = K \cdot_\nu J$, and similarly for the symmetric statement. $P_4$ also holds: Let $(I_m)_{m \in M}$ be a non-empty family of divisorial left $H$-ideals. Then $(\bigcup_{m \in M} I_m)_\nu \subseteq H$ is also a divisorial left $H$-ideal, and if $(I_m)_{m \in M}$ is a family of $(H, H')$-ideals with $H' \in \alpha$, then the divisorial closure of the union is again an $(H, H')$-ideal. $P_5$ is just $A_1$. $A_2$ implies $P_6$: If $H, H' \in \alpha$, then there exists an $(H, H')$-ideal $I$ by Lemma 5.15.2. Then $I_\nu$ is as required in $P_5$.

Assume now that $(F_\nu(\alpha), \cdot_\nu, \subseteq)$ is an arithmetical groupoid, and $H \in \alpha$. Then $P_2$ implies $A_3$, and $P_6$ implies $A_3$. From $P_5$ we can derive $A_2$: Let $I$ be a fractional left $H$-ideal, and $x \in I \cap Q^*$. Then $Hx \in F_\nu(\alpha)$. By $P_5$, there exists $J \in \mathcal{I}_\nu(\alpha)$ with $O_x(J) = O_x(Hx)$ and $O_x(J) = H$. Thus $HxJ$ is a fractional $H$-ideal, and $HxJ \subseteq I$. We proceed similarly if $I$ is a fractional right $H$-ideal. 

**Remark 5.17.**

1. From the discussion after Definition 4.2, we also see that we can equivalently formulate $A_3$ as “the lattice of divisorial fractional left (right) $H$-ideals is modular”, as the property for the other side then holds automatically.
2. Let $H$ be a normalizing monoid. By definition of a monoid, $H$ satisfies the left and right Ore condition, hence it is an order in its quotient group. Lemma 5.9.2 shows that every fractional left or right $H$-ideal is in fact already a two-sided $H$-ideal, and thus $H$ is bounded.

Assume that $H$ is a normalizing Krull monoid. Then $\alpha = \{H\}$, and the lattice-ordered groupoid $F_\nu(\alpha)$ is in fact a group. The lattice of divisorial fractional $H$-ideals is then modular, even distributive [51, Theorem 2.1.3(a)], and hence by the previous theorem an arithmetical groupoid.

**Definition 5.18.** We call a maximal order $H$ satisfying $A_1$–$A_3$ an *arithmetical maximal order*. If $\alpha$ is its equivalence class of arithmetical maximal orders, then we denote by $\mathcal{M}_\nu(\alpha) \subseteq \mathcal{I}_\nu(\alpha)$ the (quiver of) maximal integral elements.

Let from here on $H$ be an arithmetical maximal order in $Q$, and let $\alpha$ be its equivalence class of arithmetical maximal orders.

By Lemma 5.9.2, every principal left ideal $Ha$ with $a \in H^*$ is a divisorial left $H$-ideal with inverse $a^{-1}H \in F_\nu(\alpha)$. Let

$$\mathcal{H}(\alpha) = \{H'a \in \mathcal{I}_\nu(\alpha) \mid H' \in \alpha, a \in H^*\}.$$ 

The $\nu$-product coincides with the usual proper product on $\mathcal{H}(\alpha)$. Thus $(\mathcal{H}(\alpha), \cdot) \subseteq (\mathcal{I}_\nu(\alpha), \cdot_\nu)$ is a wide subcategory, with the product $IJ = I \cdot_\nu J$ for $I, J \in \mathcal{H}(\alpha)$ defined whenever $O_x(I) = O_x(J)$, and then $O_x(IJ) = O_x(I)$ and $O_x(JI) = O_x(J)$. The inclusion $(\mathcal{H}(\alpha), \cdot) \subseteq (\mathcal{I}_\nu(\alpha), \cdot_\nu)$ is left- and right-saturated. By $\mathcal{H}_H(\alpha)$ (or shorter, $\mathcal{H}_H$, since $H$ determines $\alpha$) we denote the subcategory of $\mathcal{H}(\alpha)$
where the left and right orders of every element are not only equivalent but in fact conjugate to \( H \).
Explicitly,
\[
\mathcal{H}_H = \mathcal{H}_H(\alpha) = \{ d(Ha)d^{-1} \in \mathcal{I}_v(\alpha) \mid a \in H^\bullet, \ d \in Q^\bullet \}.
\]
If \( H' \in \alpha \), then \( \mathcal{H}_H = \mathcal{H}_{H'} \) if and only if \( H' \) and \( H \) are conjugate. Again the inclusion \( (\mathcal{H}_H, \cdot) \subset (\mathcal{H}(\alpha), \cdot) \) is left- and right-saturated, and thus so is the inclusion \( (\mathcal{H}_H, \cdot) \subset (\mathcal{I}_v(\alpha), \cdot) \).

The following simple lemma gives a correspondence between \( H \) and \( \mathcal{H}_H \).

Lemma 5.19. Let \( d \in Q^\bullet \).

1. If \( a, a_1, a_2 \in H^\bullet \) with \( a = a_1a_2 \), then \( d^{-1}(Ha)d = d^{-1}(Ha_2)d \cdot d^{-1}a_2^{-1}(Ha_1)a_2d \in \mathcal{H}_H \) with \( d^{-1}(Ha_2)d \).
2. If \( a \in H^\bullet \) and \( d^{-1}(Ha)d = I_2 \cdot I_1 \) with \( I_1, I_2 \in \mathcal{H}_H \), then there exist \( a_1, a_2 \in H^\bullet \) with \( I_2 = d^{-1}(Ha_2)d \).
3. If \( a_1, a_2, b_1, b_2 \in H^\bullet \) with \( Ha_2 = Hb_2 \) and \( a_2^{-1}(Ha_1)a_2 = b_2^{-1}(Hb_1)b_2 \), then there exist \( \varepsilon_1, \varepsilon_2 \in H^\times \) with \( b_1 = \varepsilon_1a_1\varepsilon_1^{-1} \) and \( b_2 = \varepsilon_2a_2 \).

In particular, for \( a \in H^\bullet \) we have \( a \in \mathcal{A}(H^\bullet) \) if and only if \( d^{-1}(Ha)d \in \mathcal{A}(\mathcal{H}_H) \).

Proof. 1. The multiplication is defined because \( C_r(d^{-1}(Ha_2)d) = d^{-1}a_2^{-1}Ha_2d = C_r(d^{-1}a_2^{-1}(Ha_1)a_2d). \) The remaining statements are then clear.

2. Since \( C_r(I_2) = d^{-1}Hd \) we have \( I_2 = d^{-1}Hda'_2 \) with \( a'_2 \in (d^{-1}Hd)^\bullet \), and hence, with \( a_2 = da'_2d^{-1} \in H^\bullet \), \( I_2 = d^{-1}(Ha)d \).

3. Since \( Ha_2 = Hb_2 \), there exists an \( \varepsilon_2 \in H^\times \) with \( b_2 = \varepsilon_2a_2 \). Then

\[
a_2^{-1}(Ha_1)a_2 = b_2^{-1}(Hb_1)b_2 = a_2^{-1}\varepsilon_2^{-1}(Hb_1)\varepsilon_2a_2 = a_2^{-1}(Hb_1\varepsilon_2)a_2,
\]

and thus there exists \( \varepsilon_1 \in H^\times \) with \( b_1 = \varepsilon_1a_1\varepsilon_2^{-1} \).

Observe that we may view a rigid factorization \( Ha_2 \ast a_2^{-1}(Ha_1)a_2 \in Z^\bullet(\mathcal{H}_H) \) as a multiplicative way of writing the chain \( H \supset Ha_2 \supset Ha_1a_2 \).

Proposition 5.20. Let \( a \in H^\bullet \). For every \( d \in Q^\bullet \) there is a bijection \( Z^\bullet_H(a) \rightarrow Z^\bullet_{H^\bullet}(d^{-1}(Ha)d) \), given by

\[
u_1 \ast u_2 \ast \cdots \ast u_k \mapsto d^{-1}(Hu_k)d \ast (d^{-1}u_k^{-1}(H_{u_{k-1}})u_k)d \ast \cdots \ast (d^{-1}u_1^{-1}u_2 \cdots \cdot u_k)d.
\]

If \( \tilde{\beta} : \mathcal{H}_H \rightarrow B \) is a transfer homomorphism to a reduced cancellative small category \( B \) and having the additional property that \( \tilde{\beta}(d^{-1}(Ha)d) = \tilde{\beta}(Ha) \) for all \( a \in H^\bullet \) and \( d \in Q^\bullet \), then it induces a transfer homomorphism \( \tilde{\beta} : H^\bullet \rightarrow B^{op} \) given by \( \tilde{\beta}(a) = \tilde{\beta}(Ha) \).

Proof. The claimed bijection follows by iterating the previous lemma.

We need to verify that \( \tilde{\beta} \) is a transfer homomorphism and first check that \( \tilde{\beta} \) is a homomorphism: For \( a, b \in H^\bullet \)

\[
\tilde{\beta}(ab) = \tilde{\beta}(Hab) = \tilde{\beta}(Hb \cdot b^{-1}(Ha)b) = \tilde{\beta}(Hb) \cdot \tilde{\beta}(b^{-1}(Ha)b) = \tilde{\beta}(Hb) \cdot \tilde{\beta}(Ha) = \tilde{\beta}(a) \cdot \tilde{\beta}(b),
\]

D. Smertnig / Journal of Algebra 390 (2013) 1–43
and if \( a \in H^\times \) then \( Ha = H \), whence \( \theta(a) = \overline{\theta}(H) \in B_0 \). We verify T1: Let \( b \in B \). Then there exist \( d \in Q^\ast \) and \( a \in H^\ast \) with \( \overline{\theta}(d^{-1}(Ha)d) = b \), hence \( \theta(a) = b \). If \( a \in H^\ast \) with \( \theta(a) \in B_0 \), then \( \overline{\theta}(Ha) \in B_0 \), hence \( Ha \in \langle H_H \rangle_0 \), i.e., \( Ha = H \) and \( a \in H^\times \). It remains to check T2: Let \( a \in H^\ast \) and \( b_1, b_2 \in B \) with \( \theta(a) = b_1 \prec_0 b_2 \). Then \( \overline{\theta}(Ha) = b_2b_1 \), hence there exist \( a_1, a_2 \in H^\ast \) with \( Ha = Ha_2 \cdot a_2^{-1}(Ha_1)a_2 \) and \( \overline{\theta}(Ha_2) = b_2, \overline{\theta}(a_2^{-1}(Ha_1)a_2) = b_1 \). This implies \( a = \varepsilon a_1a_2 \) with \( \varepsilon \in H^\times \), and \( \theta(\varepsilon a_1) = b_1, \theta(a_2) = b_2 \). □

**Remark 5.21.** The condition \( \overline{\theta}(d^{-1}(Ha)d) = \overline{\theta}(Ha) \) implies in particular \( |\overline{\theta}(H_H)_0| = 1 \). Thus in fact \( B \) is necessarily a semigroup.

Let \( G \) be the universal vertex group of \( \mathcal{F}_v(\alpha) \), and let \( \eta: \mathcal{F}_v(\alpha) \to G \) be the abstract norm, as defined in the previous section.

**Lemma 5.22.**

1. If \( I \in \mathcal{I}_v(\alpha) \) and \( d \in Q^\ast \), then \( \eta(d^{-1}Id) = \eta(I) \).
2. \( q(\eta(H\alpha)) = q(\eta(Ha) \mid a \in H^\ast) = q(\eta(Hq) \mid q \in Q^\ast) \).

**Proof.** 1. It suffices to verify the claim for maximal integral \( I \in \mathcal{I}_v(\alpha) \). If \( P \in \mathcal{I}_v(\alpha) \) is the maximal divisorial two-sided \( O_I \)-ideal contained in \( I \), then \( d^{-1}Pd \) is the maximal divisorial two-sided ideal contained in \( d^{-1}Id \), and since \( d^{-1}Pd = (O_I(d^{-1}Id)d^{-1}O_I(I)) \cdot v \) \( \prec_v (O_I(d)O_I(d^{-1}Id)) \) we have \( \eta(I) = (P) = (d^{-1}Pd) = \eta(d^{-1}Id) \in G \).

2. The first equality is immediate from 1. For the second equality, note that if \( q = ab^{-1} \) with \( a, b \in H^\ast \), then (using 1 multiple times and the fact that \( \eta \) is a homomorphism)

\[
\eta(Hq) = \eta(Hab^{-1}) = \eta(Hb^{-1} \cdot b(Ha)b^{-1}) = \eta(Hb^{-1})\eta(b(Ha)b^{-1}) = \eta(bH)^{-1}\eta(Ha)
\]

\[
= \eta(b^{-1}(bH)b^{-1})^{-1}\eta(Ha) = \eta(Ha)\eta(Hb)^{-1}.
\]

Applying Theorem 4.15 to the present situation, we obtain a transfer homomorphism \( H_H \to B(C_M) \) if we impose some additional crucial conditions on \( H \).

**Theorem 5.23.** Let \( Q \) be a quotient semigroup, \( H \) an arithmetical maximal order in \( Q \), and \( \alpha \) its equivalence class of arithmetical maximal orders.

1. For all \( a \in H^\ast, L_H(\alpha) \) is finite and non-empty. If, for every maximal divisorial \( H \)-ideal \( P \) with \( P \subseteq I \) is finite, then \( Z_{H^\ast}(\alpha) \) is finite for all \( a \in H^\ast \).
2. Let \( P_{H^\ast} = \{ \eta(Hq) \mid q \in Q^\ast \} \subseteq G, C = G/P_{H^\ast}, \) and \( C_M = \{ \eta(I) \} \subseteq C \mid I \in \mathcal{I}_v(\alpha) \) maximal integral.

Assume:

(i) A divisorial fractional left \( H \)-ideal \( I \) is principal if and only if \( \eta(I) \in P_{H} \).

(ii) For all \( H^\prime \in \alpha \) and all \( g \in C_M \) there exists a maximal divisorial left \( H^\prime \)-ideal with \( [\eta(I)] = g \). Then there exists a transfer homomorphism \( \theta : H^\ast \to B(C_M) \).

**Proof.** By Proposition 5.16, \( (\mathcal{F}_v(\alpha), \prec_v, \subset) \) is an arithmetical groupoid, and \( \mathcal{I}_v(\alpha) \) is its subcategory of integral elements. \( (H_H, \cdot) \) is a left- and right-saturated subcategory of \( (\mathcal{I}_v, \cdot_v) \).

1. This follows immediately from Corollary 4.13 and Proposition 5.20.

2. Let \( I \) be a fractional left \( H^\prime \)-ideal with \( H^\prime = dHd^{-1} \). Then \( I \) is principal if and only if the fractional left \( H \)-ideal \( d^{-1}Id \) is, and this is the case if and only if \( \eta(I) = \eta(d^{-1}Id) \in P_{H^\ast} = q(\eta(H_H)) \) (where the last equality is due to the previous lemma). Therefore the first condition of Theorem 4.15 is satisfied. Condition (ii) of the present theorem is equivalent to the second condition of Theorem 4.15. Thus there exists a transfer homomorphism \( \overline{\theta} : H_H \to B(C_M) \) as in Theorem 4.15. By Proposition 5.20, there exists a transfer homomorphism \( \theta : H^\ast \to B(C_M) \). □
Remark 5.24.

1. We continue our discussion from Remark 5.17. Let $H$ be a normalizing Krull monoid. Then $\alpha = \{H\}$, $Ha = HaH = aH$ for all $a \in \mathbb{Q}^*$ and associativity is a congruence relation [25, Lemma 4.4.1], thus $H_{\text{red}} = \{H \cdot a \mid a \in H\}$ with the induced operation is also a monoid. Therefore $\mathcal{H} = \mathcal{H}_H = \{HaH \mid a \in H\} \cong H_{\text{red}}$ and $G = F_v(\alpha)$ is the free abelian group on the maximal divisorial (two-sided) $H$-ideals, while $I_v(\alpha)$ is the free abelian monoid on the same basis. In the previous theorem we therefore have $\mathbb{G} = G$, $\eta = \text{id}$, $P_{H^\bullet} = \{Hq \mid q \in \mathbb{Q}^*\}$, and hence $C$ is the divisorial class group of $H$, and $C_M$ is the set of divisorial ideal classes that contain a maximal divisorial $H$-ideal. The second condition of the theorem is trivially true by virtue of $|G_0| = 1$ and the definition of $C_M$, and the first condition is trivially true because $\eta = \text{id}$. We thus get a transfer homomorphism $H \to B(C_M)$ (induced from the transfer homomorphism $H_{\text{red}} \cong \mathcal{H}_H \to B(C_M)$), which is the same one as in [25, Theorem 6.5].

2. If $H$ is a maximal order satisfying only $A_1$ and $A_3$, then $L_{H^\bullet}(a)$ is finite and non-empty for all $a \in H^\bullet$. In Section 4 one may drop $P_5$ and $P_6$, and still obtain Proposition 4.12.1 in the weaker form that, for each $a \in G_+$, either $Z_{G_+}(a) = \emptyset$ or $|L_{G_+}(a)| = 1$ (and of course without any statement about $\Phi$, which can only be defined in the presence of $P_5$). This is possible because $P_6$ is only used to show existence of a rigid factorization of $a$. A sufficient condition for $Z_{G_+}(a) = \emptyset$ is that $G_+(s(a), \cdot)$ and $G_+(-t(a))$ satisfy the ACC. If $H$ satisfies $A_1$, then $G_+(e, \cdot)$ and $G_+(-e, e)$ with $e \in (\mathcal{H}_H)_0$ (corresponding to conjugate orders of $H$) satisfy the ACC, and as in Corollary 4.13 one shows that $L_{H^\bullet}(a)$ is finite and non-empty for all $a \in \mathcal{H}_H$. Hence the same is true for $H^\bullet$.

5.1. Rings

Suppose that $Q = (\mathbb{Q}, +, \cdot)$ is a quotient ring in the sense of [42, Chapter 3] (but recall that we in addition require it to be unital, as we do for all rings). Then $(\mathbb{Q}, \cdot)$ is a quotient semigroup. In the remainder of this section we show that the ring-theoretic divisorial one-sided ideal theory for maximal orders in $(\mathbb{Q}, +, \cdot)$ coincides with the semigroup-theoretic one.\(^3\) If $R$ is a ring-theoretic order in $Q$, then a fractional left $R$-ideal $I$ in the semigroup-theoretic sense is a fractional left $R$-ideal in the ring-theoretic sense if and only if $I - I \subseteq I$ (see [42, §3.1.11] for the usual definition).

Let for the remainder of this subsection $Q = (\mathbb{Q}, +, \cdot)$ be a quotient ring.

Lemma 5.25. Let $H$ be an order in the multiplicative semigroup $(\mathbb{Q}, \cdot)$ and $I$ a fractional left $H$-ideal (in the semigroup-theoretic sense). Consider the following statements:

(a) $I - I \subseteq I$.
(b) $O_l(I)$ is a subring of $Q$.
(c) $O_r(I)$ is a subring of $Q$.

Then (a) $\Rightarrow$ (b) and (a) $\Rightarrow$ (c). If $H$ is a maximal order and $I$ is divisorial, then (a) $\iff$ (b) $\iff$ (c).

Proof. Assume that (a) holds. We show (b): Let $a, b \in O_l(I)$. Then $aI \subseteq I$ and $bI \subseteq I$ and hence $(a - b)I \subseteq aI - bI \subseteq I - I \subseteq I$, thus $a - b \in O_l(I)$.

Assume now that $H$ is maximal, $I = I_v$ and (b) holds. We show (a). Let $a, b \in I = I_v = (I^{-1})^{-1}$. Then $aI^{-1} \subseteq O_l(I)$, and $bI^{-1} \subseteq O_l(I)$, whence $(a - b)I^{-1} \subseteq aI^{-1} - bI^{-1} \subseteq O_l(I) - O_l(I) = O_l(I)$ and thus $a - b \in (I^{-1})^{-1} = I$. □

Lemma 5.26. A ring-theoretic order $R$ in $Q$ is maximal in the ring-theoretic sense if and only if it is maximal in the semigroup-theoretic sense.

\(^3\) In [42, Chapter 5] the terminology “reflexive” is used in place of “divisorial”.
Proof. We show that if $R$ is maximal in the ring-theoretic sense, then it is maximal in the semigroup-theoretic sense, as the other direction is trivial. Let $I$ be a fractional left $R$-ideal in the semigroup-theoretic sense. Then $R(I)$ is a fractional left $R$-ideal in the ring-theoretic sense, and using $R \subseteq O_l(I)$, it follows that $O_l(I) \subseteq O_l(R(I))$. Maximality of $R$ in the ring-theoretic sense implies $R = O_l(R(I))$, hence also $R = O_l(I)$. Similarly, if $J$ is a fractional right $R$-ideal in the ring-theoretic sense then $O_r(J) = R$. Therefore Lemma 5.8 implies that $R$ is maximal in the semigroup-theoretic sense.

As before let $\alpha$ be an equivalence class of maximal orders of $(Q, \cdot)$ in the semigroup-theoretic sense.

Lemma 5.27. Let $H \in \alpha$ and assume that $H$ is a subring of $Q$ (i.e., an order in $Q$ in the ring-theoretic sense).

1. Every $H' \in \alpha$ is a subring of $Q$ (and therefore an order in $Q$ in the ring-theoretic sense).
2. If $I$ is a divisorial fractional left $H$-ideal and $J$ is a divisorial fractional left $O_l(I)$-ideal, then

\[ \{ab \mid a \in I, b \in J\} = \{H[\{ab \mid a \in I, b \in J\}]\}, \]

i.e., the semigroup-theoretic $v$-product coincides with the ring-theoretic one.
3. If $I$ and $J$ are divisorial fractional left $H$-ideals, then $(I \cup J)_v = (I + J)_v$.

Proof. 1. By Lemma 5.7.3 there exists a fractional $(H, H')$-ideal $I$. By maximality of $H$ and $H'$, also $O_l(I_v) = H$ and $O_l(I_v) = H'$ and the claim follows from Lemma 5.25 applied to $I_v$.

2. Write $I \cdot S J = \{ab \mid a \in I, b \in J\}$ for the semigroup-theoretic ideal product and $I \cdot_R J = H[\{ab \mid a \in I, b \in J\}]$ for the ring-theoretic one. Then $I \cdot_S J \subseteq I \cdot_R J$, and both of these sets are fractional left $H$-ideals (in the semigroup-theoretic sense). Therefore $(I \cdot_S J)_v \subseteq (I \cdot_R J)_v$. For the converse inclusion, it suffices to show $I \cdot_R J \subseteq (I \cdot_S J)_v$, but this is true because by Lemma 5.25 $(I \cdot_S J)_v$ is additively closed.

3. Clearly $I \cup J \subseteq I + J$ and both sets are fractional left $H$-ideals (for $I + J$ proceed as in the proof of Lemma 5.6.4; in particular observe $(H, I \cup J) \subseteq (H, I + J)$). As before it therefore suffices to show $I + J \subseteq (I \cup J)_v$. This again holds due to Lemma 5.25.

 Altogether, if $R$ is a maximal order in $Q$ in the ring-theoretic sense, then it does not matter whether we form $F_v(\alpha)$ by using the ring-theoretic or the semigroup-theoretic notions. We use the same notion of boundedness for ring-theoretic orders as in Definition & Lemma 5.14; for semiprime Goldie rings this coincides with the notion in [42].

Theorem 5.28. Let $R$ be a maximal order in a quotient ring $Q$, $\alpha$ its equivalence class of maximal orders in the semigroup-theoretic sense, and $\beta$ its equivalence class of maximal orders in the ring-theoretic sense. Then $\alpha = \beta$ and $F_v(\alpha) = F_v(\beta)$, where the latter is the ring-theoretic analogue of $F_v(\alpha)$.

If $R$ is bounded, satisfies the ACC on divisorial left $R$-ideals and on divisorial right $R$-ideals, and the lattice of divisorial fractional left (right) $R$-modules is modular, then $(R, \cdot)$ is an arithmetical maximal order in $(Q, \cdot)$ in the semigroup-theoretic sense. In particular, the conclusions of Theorem 5.23 hold for $R$.

Proof. By Lemma 5.27.1, $\alpha = \beta$, and by Lemma 5.25, $F_v(\alpha) = F_v(\beta)$ as sets. By Lemma 5.27, the $v$-product, meet and join coincide, and hence $F_v(\alpha) = F_v(\beta)$ as lattice-ordered groupoids. The remaining claims follow from this.

In [46, §5(d)], Rehm gives examples for bounded maximal orders $E$, that are prime and satisfy the ACC on divisorial two-sided $E$-ideals, but do not satisfy the ACC on divisorial left $E$-ideals or the ACC on divisorial right $E$-ideals. In fact (unless one takes the special case where $E$ itself is a quotient ring), the orders $E$ are not even atomic. However, these orders are not Goldie, as they are not of finite left or right uniform dimension, and do not satisfy the ACC on left or right annihilator ideals.

Before going to maximal orders in central simple algebras, we discuss principal ideal rings.
Example 5.29 (Principal ideal rings). Let \( R \) be a bounded order in a quotient ring \( Q \). Assume that every left \( R \)-ideal and every right \( R \)-ideal is principal. By the characterization in Lemma 5.8, \( R \) is then already a maximal order, and it satisfies \( A_1-A_2 \). Thus \( \mathcal{H}_R = \mathcal{I}_R(\alpha) \), and facts about the rigid factorizations in \( \mathcal{I}_R(\alpha) \) trivially descend to facts about rigid factorizations of \( R^* \). Examples we have in mind include bounded skew polynomial rings \( D[X, \sigma] \), where \( D \) is a division ring and \( \sigma : D \rightarrow D \) is an automorphism, and the Hurwitz quaternions \( \mathbb{Z}[i, j, k, i^{2}+j^{2}+k^{2}+1] \) with \( i^2 = -1 \), \( j^2 = -1 \) and \( ij = -ji \). Both of these examples are left- and right-euclidean domains, and hence principal ideal rings. In this way we can for example rediscover Theorem 2 in [16, §5].

Let \( Q \) be a quaternion algebra over a field \( K \) with \( \text{char}(K) \neq 2 \), and \( a \in Q^* \setminus K^* \). Then \( \text{nr}(a) = a\overline{a} \in K^\times \) and \( \text{tr}(a) = a + a \in K \). For the polynomial ring \( Q[X] \) in the central variable \( X \), therefore

\[
f = X^2 - \text{tr}(a)X + \text{nr}(a) = (X - cac^{-1})(X - \overline{c}c^{-1}) \quad \text{for all} \ c \in Q^*,
\]

and thus \( |Z^*_Q[X](f)| = \infty \) if \( K \) is infinite. (But these rigid factorizations are usually considered to be identical factorizations, and \( Q[X] \), being left- and right-euclidean, is even a UFD with suitable definitions, see for example [8, Chapter 3.2] and [14, Chapter 3].) In terms of ideal theory, every element \( X - cac^{-1} \) with \( c \in Q^* \) generates a maximal left \( Q[X] \)-ideal lying above the maximal two-sided \( Q[X] \)-ideal \( Q[X]f \). If also \( d \in Q^* \), then \( Q[X](X - cac^{-1}) = Q[X](X -dad^{-1}) \) if and only if \( cac^{-1} = dad^{-1} \), i.e., \( d^{-1}c \in K(a) \).

5.2. Classical maximal orders over Dedekind domains in CSAs

Let \( \mathcal{O} \) be a commutative domain with quotient field \( K \). By a central simple algebra \( A \) over \( K \), we mean a \( K \)-algebra with \( \dim_K(A) < \infty \), which is simple as a ring, and has center \( K \). Then \( A \) is artinian because it is a finite-dimensional \( K \)-algebra, and hence it is a quotient ring (in an artinian ring, every non-zero-divisor is invertible [42, §3.1.1], hence it is a quotient ring and an element is left-cancellative if and only if it is right-cancellative if and only if it is cancellative). By Posner’s Theorem [42, §13.6.6], a ring \( R \) is a prime \( \mathcal{P} \)-ring if and only if it is an order in a central simple algebra, and hence in particular, prime \( \mathcal{P} \)-rings are bounded Goldie rings. Furthermore, \( \mathcal{P} \)-Krull rings are characterized as those maximal orders in central simple algebras whose center is a commutative Krull domain [35, Theorem 2.4]. We start with a simple corollary of Theorem 5.28.

Corollary 5.30. If \( R \) is a \( \mathcal{P} \)-Krull ring, then \( L_{R^*}(\alpha) \) is finite and non-empty for all \( \alpha \in R^* \).

Proof. We only have to verify the conditions of Theorem 5.28. By [35, Theorem 2.4] the various notions of Krull rings coincide for prime \( \mathcal{P} \)-rings. Thus \( R \) is a bounded Chamarie–Krull ring. The ACC on divisorial left \( \mathcal{P} \)-ideals and divisorial right \( \mathcal{P} \)-ideals follows from [11] or [31, Corollary 3.11]. Moreover, for every divisorial prime \( \mathcal{P} \)-ideal \( P \), the set of regular elements modulo \( P \), denoted \( C(P) \), is cancellative, satisfies the left and right Ore condition, and for the localization \( R_{C(P)} = C(P) R \subset Q \) every left (right) \( R_{C(P)} \)-ideal is principal [11, Proposition 2.5]. The lattice of divisorial fractional left (right) \( R_{C(P)} \)-ideals is hence modular. Using the ACC on divisorial left and right \( \mathcal{P} \)-ideals, one checks as in the commutative case that \( I \cap R_{C(P)} = (IR_{C(P)})_\nu \) for a fractional right \( \mathcal{P} \)-ideal \( I \).

Suppose now \( I, J, K \) are divisorial fractional right \( \mathcal{P} \)-ideals, and \( K \subset I \). We have to check \( I \cap (J + K)_\nu = ((I \cap J) + K)_\nu \). But \( (I \cap (J + K))_\nu R_{C(P)} = IR_{C(P)} \cap (JR_{C(P)} + KR_{C(P)})_\nu \) and \( ((I \cap J) + K)_\nu R_{C(P)} = (IR_{C(P)} \cap JR_{C(P)} + KR_{C(P)})_\nu \), and thus, by modularity in the localizations, they are equal for every divisorial prime \( \mathcal{P} \)-ideal \( P \). The claim now follows from [11, Lemme 2.7], by which the global divisorial fractional right \( \mathcal{P} \)-ideals can be recovered as intersections from the local ones. □

Using Remark 5.24.2, we get the above result even for more general classes of rings, namely for Dedekind prime rings and bounded Chamarie–Krull rings (cf. [11]).

But the aim of this subsection is to restrict to the situation where the base ring \( \mathcal{O} \) is a Dedekind domain, as a preparation for the structural results on sets of lengths in the setting of holomorphy rings. Suppose that \( \mathcal{O} \) is a Dedekind domain. A ring \( R \) is a classical \( \mathcal{O} \)-order of \( A \) if \( \mathcal{O} \subset R \), \( R \) is finitely
Lemma 5.31. Let $I \subset A$ and let $T$ be a classical $O$-order in $A$. The following are equivalent:

(a) $I$ is a fractional left $T$-ideal in the ring-theoretic sense (i.e., as in [42, §3.1.11]).
(b) $I$ is a finitely generated $O$-module with $KI = A$ and $T I \subset I$.4

If $T$ is maximal, then in addition the following statements are equivalent to the previous ones:

(c) $I$ is a divisorial fractional left $T$-ideal in the semigroup-theoretic sense (Definitions 5.4 and 5.10).
(d) $I$ is a divisorial fractional left $T$-ideal in the ring-theoretic sense (i.e., a reflexive fractional left $T$-ideal as in [42, §5.1]).

Proof. (a) $\Rightarrow$ (b): Recall that $I$ is a fractional left $T$-ideal in the ring-theoretic sense if $TI \subset I$, $I+I \subset I$ and there exist $x, y \in A^\times$ with $x \in I$ and $ly \subset T$. $O$ is the center of $T$, and $T$ is finitely generated over the noetherian $O$. Since $ly \subset T$, therefore also $I$ is a finitely generated $O$-module. Writing $x^{-1} = rc^{-1}$ with $r \in T^\times$ and $c \in O^\times$ we see that $c = rx \in I \cap O^\times$. If $a \in A$ is arbitrary, then $a = r'd^{-1}$ with $r' \in T$, $d \in O^\times$ and therefore $a = (r'c)(c^{-1}d^{-1}) \in KI$.

(b) $\Rightarrow$ (a): Certainly $TI \subset I$ and $I+I \subset I$. We have to find $x, y \in A^\times$ with $x \in I$ and $ly \subset T$. Since $KI = A$, there exist $\lambda \in K^\times$ and $x \in I \cap A^\times$ with $1 = \lambda x$ (in fact even $x \in K^\times$). If $I = O\langle y_1, \ldots, y_l \rangle$ with $y_1, \ldots, y_l \in I$, then due to $KT = A$ there exists a common denominator $y \in O^\times$ with $y_1y \in T$, hence $ly \subset T$.

Let now $T$ be maximal. (d) $\Rightarrow$ (a) is trivial, and (a) $\Rightarrow$ (d) follows because $T$ is a Dedekind prime ring, and hence every fractional left $T$-ideal (in the ring-theoretic sense) is invertible (see [42, §5.2.14] or [47, §22, §23] for the more specific case where $R$ is a maximal order in a CSA), and therefore divisorial.

(c) $\Leftrightarrow$ (d) follows from Lemma 5.25.

A subset $I \subset A$ satisfying the second condition of the previous lemma and additionally $O_I(I) = T$ is considered to be a left $T$-ideal in [47] and [53]. Thus, a left $T$-ideal in the sense of [47,53] is (in our terms) a fractional left $T$-ideal in the ring-theoretic sense with $O_I(I) = T$. If $T$ is maximal, then the extra condition $O_I(I) = T$ is trivially satisfied, and the definitions are equivalent, but for a non-maximal order the definitions do not entirely agree (we will only need to work with ideals of maximal orders).

Since all $I \in F_r(\alpha)$ are invertible (i.e., $II^{-1} = O_I(I)$ and $I^{-1}I = O_I(I)$ for the ring-theoretic products), the $v$-product coincides with the usual proper product of ideals: $I \cdot v J = I \cdot J$ whenever $I, J \in F_r(\alpha)$ with $O_I(I) = O_J(J)$. Therefore, $F_r(\alpha)$ is the groupoid of all normal ideals of $A$ in Reiner’s terminology ($O$ is fixed implicitly).

4 Here $KI = \{\lambda a \mid \lambda \in K \ , \ a \in I\} = \{\sum_{i=1}^{n} \lambda_i a_i \mid \lambda_i \in K \ , \ a_i \in I\} = K \otimes_O I$. 

generated as $O$-module and $KR = A$. $R$ is a classical maximal $O$-order if it is maximal with respect to set inclusion within the set of all classical $O$-orders. Such classical maximal $O$-orders as well as their ideal theory are well-studied, in particular Reiner’s book [47] provides a thorough description of them. If $R$ is a classical $O$-order, then it is a ring-theoretic order in $A$ in the sense we discussed, and it is a maximal order if and only if it is a classical maximal $O$-order (for this see [42, §5.3]). The set of all classical maximal $O$-orders forms an equivalence class of (ring-theoretic) maximal orders, call it $b$ for a moment. If we write $\alpha$ for the same semigroup-theoretic equivalence class of maximal orders (i.e., $\alpha = b$ as sets, but we view the elements of $b$ as rings and those of $\alpha$ just as semigroups), then $F_r(\alpha) = F_r(b)$ by Theorem 5.28. Next, we recall that our notion of ideals coincides with that of [47] and [53] in the case of maximal orders, thereby seeing how the one-sided ideal theory of classical maximal $O$-orders is a special case of the semigroup-theoretic divisorial one-sided ideal theory developed in this section. We also recognize the abstract norm homomorphism $\eta$ of Section 4 as a generalization of the reduced norm of ideals (in the sense of [47, §24]).
To be able to apply our abstract results we still have to check that A1 through A3 are true for \( \alpha \): A1 follows because every \( R \in \alpha \) is noetherian, while A2 is true because every fractional left \( R \)-ideal with \( R \in \alpha \) in fact even contains a non-zero element of the center (cf. \([42, \text{Prop. 5.3.8(i) and (ii)}]\) or see “(b) \( \Rightarrow \) (a)” of the last proof). Since every fractional left (right) \( R \)-ideal is divisorial, A3 follows from the modularity of the lattice of left (right) \( R \)-modules.

Writing \( \mathcal{F}_*(\mathcal{O}) \) for the non-zero fractional ideals of the commutative Dedekind domain \( \mathcal{O} \), and \( \mathcal{G} \) for the universal vertex group of \( \mathcal{F}_*(\alpha) \), we have the following.

**Lemma 5.32.** If \( R, R' \in \alpha \) and \( \mathcal{P} \in \mathcal{G} \), then \( \mathcal{P}_R \cap \mathcal{O} = \mathcal{P}_{R'} \cap \mathcal{O} \in \text{max}(\mathcal{O}) \) and there is a canonical bijection

\[
\{ \mathcal{P} \mid \mathcal{P} \in \mathcal{G} \text{ maximal integral} \} \to \text{max}(\mathcal{O}),
\]

inducing an isomorphism of free abelian groups \( r : \mathcal{G} \cong \mathcal{F}_*(\mathcal{O}) \). The inverse map is given by \( \mathcal{P} \mapsto (\mathcal{P}) \) where \( \mathcal{P} \) is the unique maximal (two-sided) \( R \)-ideal lying over \( \mathcal{P} \). If \( R \) is unramified at \( \mathcal{P} \), then \( \mathcal{P} = \mathcal{R}_\mathcal{P} \).

If all residue fields of \( \mathcal{O} \) are finite, and \( \eta : \mathcal{F}_*(\alpha) \to \mathcal{G} \) is the abstract norm homomorphism, then \( r \circ \eta = \text{nr}_{\mathcal{A}/\mathcal{K}} \).

**Proof.** All but the last statement follow from \([47, \text{Theorem 22.4}]\). Since \( r \circ \eta \) and \( \text{nr}_{\mathcal{A}/\mathcal{K}} \) are both homomorphisms \( \mathcal{F}_*(\alpha) \to \mathcal{F}_*(\mathcal{O}) \), it suffices to verify equality for \( \mathcal{M} \) a maximal integral left \( R' \)-ideal with \( R' \in \alpha \), where it holds due to \([47, \text{Theorem 24.13}]\). \( \square \)

6. Proof of Theorem 1.1

Throughout this section, let \( \mathcal{K} \) be a global field and \( \mathcal{O} \) be a holomorphy ring in \( \mathcal{K} \).\(^5\) Furthermore, let \( \mathcal{A} \) be a central simple algebra over \( \mathcal{K} \), and \( \mathcal{R} \) a classical maximal \( \mathcal{O} \)-order.

Setting \( \mathcal{P}_A = \{ a \mathcal{O} \mid a \in \mathcal{K}^\times, a_\nu > 0 \text{ for all archimedean places } \nu \text{ of } \mathcal{K} \text{ where } \mathcal{A} \text{ is ramified} \} \), and denoting by \( \mathcal{C}_\mathcal{A}(\mathcal{O}) = \mathcal{F}_*(\mathcal{O})/\mathcal{P}_A \) the corresponding ray class group, we have the following.

**Lemma 6.1.** Let \( r \) be as in Lemma 5.32. Then \( r \) induces an isomorphism

\[
\mathcal{G}/\mathcal{P}_{R^\circ} \cong \mathcal{C}_\mathcal{A}(\mathcal{O}),
\]

where \( \mathcal{P}_{R^\circ} = \{ \eta(Rx) \mid x \in \mathcal{A}^\times \} \subset \mathcal{G} \).

**Proof.** By Lemma 5.32, \( r \circ \eta = \text{nr}_{\mathcal{A}/\mathcal{K}} \). The isomorphism follows because \( \text{nr}(Rx) = \mathcal{O} \text{nr}(x) \) for all \( x \in \mathcal{A}^\times \), and \( \text{nr}(\mathcal{A}^\times) = \{ a \in \mathcal{K}^\times \mid a_\nu > 0 \text{ for all archimedean places } \nu \text{ of } \mathcal{K} \text{ where } \mathcal{A} \text{ is ramified} \} \) by the Hasse–Schilling–Mass theorem on norms \([47, \text{Theorem 33.15}]\). \( \square \)

**Lemma 6.2.** For all classical maximal \( \mathcal{O} \)-orders \( \mathcal{R}' \), and all \( g \in \mathcal{C}_\mathcal{A}(\mathcal{O}) \), there exist infinitely many maximal left \( \mathcal{R}' \)-ideals \( I \) with \( [\text{nr}(I)] = g \).

**Proof.** Let \( g \in \mathcal{C}_\mathcal{A}(\mathcal{O}) \). Then there exist infinitely many distinct maximal ideals \( \mathcal{P} \) of \( \mathcal{O} \) with \([\mathcal{P}] = g\); the number field case for \( \mathcal{O} = \mathcal{O}_K \), the ring of algebraic integers, can be found in \([27, \text{Corollary 2.11.16}]\) or \([43, \text{Corollary 7 to Proposition 7.9}]\). The general case then follows because \( \mathcal{O} \) is obtained from \( \mathcal{O}_K \) by localizing at finitely many maximal ideals, hence the induced epimorphism \( \mathcal{C}_\mathcal{A}(\mathcal{O}_K) \to \mathcal{C}_\mathcal{A}(\mathcal{O}) \) yields the statement. For the function field case see \([27, \text{Proposition 8.9.7}]\).

For each \( \mathcal{P} \in \text{max}(\mathcal{O}) \) with \([\mathcal{P}] = g \) and every maximal left \( \mathcal{R}' \)-ideal \( M \) with \( \mathcal{P} \subset M \), we have \([\text{nr}(M)] = [\mathcal{P}] = g \) \([47, \text{Theorem 24.13}]\), or use Lemma 5.32). \( \square \)

---

\(^5\) For us, \( \mathcal{O} \) is a holomorphy ring if it is an intersection of all but finitely many of the valuation domains associated to valuations of \( \mathcal{K} \).
In the following equivalent characterizations of the first condition of Theorem 1.1, “left” may be replaced by “right” in each statement; this follows easily from the first statement. We write \( LC(R) \) for the finite set of isomorphism classes of fractional left \( R \)-ideals, i.e., \([I] = [J]\) in \( LC(R) \) if and only if \( J = xI \) with \( x \in A^\times \). The reduced norm induces a surjective map of finite sets \( \mu_R : LC(R) \to C_A(O) \), given by \([I] \mapsto [\text{nr}(I)]\).

**Lemma 6.3.** The following are equivalent.

(a) A fractional left \( R' \)-ideal with \( R' \) conjugate to \( R \) is principal if and only if \( \text{nr}(I) \in P_A \).

(b) A fractional left \( R \)-ideal is principal if and only if \( \text{nr}(I) \in P_A \).

(c) Every fractional left \( R \)-ideal \( I \) with \( [\text{nr}(I)] = 0 \) is principal.

(d) For the map of finite sets \( \mu_R : LC(R) \to C_A(O) \) it holds that \( |\mu_R^{-1}(0)| = 1 \).

(e) Every stably free left \( R \)-ideal is free.

(f) Every finitely generated projective \( R \)-module that is stably free is free.

**Proof.** The equivalence of (a), (b), (c) and (d) is trivial. The remaining equivalences follow from standard literature: (f) ⇒ (e) is true because \( R \) is hereditary noetherian.

(e) ⇒ (f): Let \( M \neq 0 \) be a stably free finitely generated projective \( R \)-module. Then \( M \cong R^n \oplus I \) for some left \( R \)-ideal \( I \) and \( n \in \mathbb{N}_0 \) ([47, Theorem 27.8] or [42, §5.7.8]). \( I \) is stably free and hence free by (e), but then so is \( M \).

To see (d) ⇔ (e) it suffices to recall that \( C_A(O) \) is isomorphic to the projective class group \( C(R) \) (see e.g. [52, Corollary 9.5]) and that \( LC(R) \) is just the set of isomorphism classes of locally free \( R \)-modules of rank one, i.e., the map \( \mu_R \) corresponds to \( \text{LF}_1 \to C(R) \). \([I] \mapsto [I] - [R] \) in the notation of [52]. (See also [47, Theorem 35.14] or [22] for the number field case.) □

**Proof of Theorem 1.1.** By Theorem 5.28, \( R \) is an arithmetical maximal order in \( Q \). We verify conditions (i) and (ii) of Theorem 5.23. Let \( I \) be a fractional left \( R \)-ideal. By Lemma 6.1, \( \eta(I) \in P_R \) if and only if \( \text{nr}(I) \in P_A \). By Lemma 6.3, and the fact that every stably free left \( R \)-ideal is free, this is the case if and only if \( I \) is principal, thus condition (i) holds. Condition (ii) holds due to Lemma 6.2. By Lemma 6.1, \( C \cong C_A(O) \), and by Lemma 6.2, therefore \( C = C_M \). Hence there exists a transfer homomorphism \( \theta : R^* \to B(C_A(O)) \). The remaining claims in the theorem follow from this by Proposition 3.8. □

**Remark 6.4.** If more generally \( O' \) is an arbitrary Dedekind domain with quotient field the global field \( K \), then there is a transfer homomorphism to either \( B(C_A(O')) \) or \( B(C_A(O') \setminus \{0\}) \), depending on whether or not \( O' \) contains prime elements. Only Lemma 6.2 has to be adapted: \( O' \) is a localization of a holomorphy ring \( O \), and hence there is an epimorphism \( C_A(O) \to C_A(O') \). This implies that every class \( g \in C_A(O') \setminus \{0\} \) contains a maximal ideal (see [13] for details). Therefore, for all classical maximal \( O' \)-orders \( R' \) and all \( g \in C_A(O') \setminus \{0\} \), there exists a maximal left \( R' \)-ideal \( I \) with \( [\text{nr}(I)] = g \).

The trivial class however may or may not contain a maximal ideal. In either case, the statements 1–3 of Theorem 1.1 hold true. Thanks to Kainrath for pointing this out.

**7. Proof of Theorem 1.2**

Throughout this section, let \( O_K \) be the ring of algebraic integers in a number field \( K \), \( A \) a central simple algebra over \( K \), and \( R \) a classical maximal \( O_K \)-order in \( A \) having a stably free left \( R \)-ideal that is not free. Furthermore, the discriminant of \( A \) is denoted by

\[
\Delta = \prod_{\substack{p \in \max(O_K) \
A \text{ is ramified at } p}} p \cdot A \cap O_K.
\]

The aim of this section is to prove Theorem 1.2. The existence of a stably free left \( R \)-ideal that is not free implies that \( A \) is a totally definite quaternion algebra and that \( K \) is totally real. (Note,
that conversely, for all but finitely many isomorphism classes of such classical maximal \(O_K\)-orders in totally definite quaternion algebras there exist stably free left \(R\)-ideals that are non-free.) We proceed in three subsections.

7.1. Reduction

We state two propositions and show how they imply Theorem 1.2. The proofs of these two propositions will then be given in Section 7.3.

**Proposition 7.1.** There exists a totally positive prime element \(p \in O_K\), a non-empty subset \(E \subset \{2, 3, 4\}\) and for every \(l \in \mathbb{N}_0\) an atom \(y_l \in A(R^*)\) such that

\[
L_{R^*}(y_l p) = \{3\} \cup (l + E).
\]

(We emphasize that \(E\) does not depend on \(l\).)

**Proposition 7.2.** If \(L \in \mathcal{L}(R^*)\) and \(n \in \mathbb{N}\), then \(n + L = \{n + l \mid l \in L\} \in \mathcal{L}(R^*)\).

**Proof of Theorem 1.2 (based on Proposition 7.1 and Proposition 7.2).** We first show that there is no transfer homomorphism \(R^* \to B(G_P)\) for any subset \(G_P\) of an abelian group. Assume to the contrary that \(\theta : R^* \to B(G_P)\) is such a transfer homomorphism.

**Claim A.** If \(S \in B(G_P)\) and \(U \in A(B(G_P))\), then \(\max_{\mathcal{L}(B(G_P))}(SU) \leq |S| + 1\).

**Proof.** Let \(S = g_1 \cdots g_l\), with \(l = |S|\) and \(g_1, \ldots, g_l \in G_P\), and suppose that \(SU = T_1 \cdots T_k\) with \(k \in \mathbb{N}\) and \(T_1, \ldots, T_k \in \mathcal{A}(B(G_P))\). Then for every \(i \in [1, k]\) either \(T_i \mid U\), but then already \(T_i = U\), or \(g_j \mid T_i\) for some \(j \in [1, l]\). This shows \(k \leq |S| + 1\).

By Proposition 7.1, there exists a totally positive prime element \(p \in O_K\), and for every \(l \in \mathbb{N}_0\) an atom \(y_l \in A(R^*)\) with \(\max_{\mathcal{L}(R^*)}(y_l p) \geq l + 2\). But, if \(l \geq |\theta(p)|\), then

\[
l + 2 \leq \max_{\mathcal{L}(R^*)}(y_l p) = \max_{\mathcal{L}(B(G_P))}(\theta(y_l)\theta(p)) \leq |\theta(p)| + 1 \leq l + 1,
\]

a contradiction.

In order to show \(\Delta(R^*) = \mathbb{N}\), we choose \(d \in \mathbb{N}\). Let \(p\) and \(E\) be as in Proposition 7.1 and set \(\epsilon = \min E\). If \(l = d + 3 - \epsilon\) and \(y_l\) as in Proposition 7.1, then we find \(d = (l + \epsilon) - 3 \in \Delta_{R^*}(y_l p)\).

Let \(k \in \mathbb{N}_{\geq 3}\). By definition, we have \(L_k(R^*) \subset \mathbb{N}_{\geq 2}\). Thus it remains to show that for every \(k' \geq 3\) there exists an element \(a \in R^*\) with \(\{k, k'\} \subset L(a)\). Assume without restriction that \(k \leq k'\) and let \(k = 3 + n\) with \(n \in \mathbb{N}_0\). Using Proposition 7.1, we find an element \(a' \in R^*\) with \(\{3 = k - n, k' - n\} \in L(a')\), and hence by Proposition 7.2 there exists an element \(a \in R^*\) with \(\{k, k'\} \subset L(a)\).

7.2. Preliminaries

**Algebraic number theory.** Our notation mainly follows Narkiewicz [43]. Let \(L/K\) be an extension of number fields. Then \(D_{L/K}\) is the relative discriminant, \(N_{L/K}\) the relative field norm, \(d_{L/K} = N_{L/K}(D_{L/K})\) is the relative discriminant and \(d_K = d_{K/Q}\) the absolute discriminant (we tacitly identify ideals of \(\mathbb{Z}\) with their positive generators for the absolute discriminant and norm). If \(O \subset O_K\) is an order, then \(\Gamma_O\) is the conductor of \(O\) in \(O_K\) and \(h(O) = |\Gamma_O(O)|\) is the class number of \(O\). Given \(a \in L\) with minimal polynomial \(f \in K[X]\) over \(K\), \(\delta_{L/K}(a) = f'(a)\) is the different of \(a\). Completion at a prime \(p \in \max(O_K)\) is denoted by a subscript \(p\), e.g., \(O_{K,p}\), \(K_p\), and so on. If \(m \in O_K\) is a squarefree ideal, then

\[
C_m^+(O_K) = \{a \in \mathcal{O}_K^+ \mid (a, m) = O_K\}/\{aO_K \mid a \in K^*\text{ is totally positive, } a \equiv 1 \mod m\}.
\]
denotes the corresponding ray class group. We will repeatedly make use of the fact that every class in \( C_{\text{nr}}^\mu(\mathcal{O}_K) \) contains infinitely many maximal ideals of \( \mathcal{O}_K \) [43, Corollary 7 to Proposition 7.9].

**Quaternion algebras.** We follow [53,41], and [39,40] for computational aspects. Denote by \( \sim : A \xrightarrow{\sim} A^{\text{op}} \) the anti-involution given by conjugation of elements. Then

\[
\text{nr}_{A/K}(x) = \text{nr}(x) = x\bar{x} = \bar{x}x \quad \text{and} \quad \text{tr}_{A/K}(x) = \text{tr}(x) = x + \bar{x} \quad \text{for all } x \in A.
\]

Every element \( x \in A \) satisfies an equation of the form

\[
x^2 - \text{tr}(x)x + \text{nr}(x) = 0,
\]

and if \( x \in A \setminus K \), then \( K(x)/K \) is a quadratic field extension. From the equation above we see that \( N_{K(x)/K} = \text{nr}_{A/K} | K(x) \) and \( \text{Tr}_{K(x)/K} = \text{tr}_{A/K} | K(x) \).

A classical \( \mathcal{O}_K \)-order \( T \) of \( A \) is called a classical Eichler \( (\mathcal{O}_K) \)-order if it is the intersection of two classical maximal \( \mathcal{O}_K \)-orders.\(^6\) The reduced discriminant of a classical \( \mathcal{O}_K \)-order \( T \) takes the form \( D\mathfrak{N} \) where \( \mathfrak{N} < \mathcal{O}_K \) is the level of \( T \). Furthermore, because \( A \) is totally definite, we have \( [T^\times : \mathcal{O}_K^\times] < \infty \) for the unit group, and \( C_A(\mathcal{O}_K) = C^+(\mathcal{O}_K) \) is the narrow class group of \( \mathcal{O}_K \).

As in the previous section, \( \mathcal{L}(R) \) is the set of isomorphism classes of left \( R \)-ideals, and \( \mu_R : \mathcal{L}(R) \to C^+(\mathcal{O}_K) \), \([I] \mapsto [\text{nr}(I)]\). \(^{[43, \text{Corollary 7 to Proposition 7.9}]}\)

**Proposition 7.3.** Let \( \mathcal{C} \in \mathbb{N} \). Let \( p \in \text{max}(\mathcal{O}_K) \) with \( p \mid d_K \mathcal{D} \), and such that

\[
\frac{h^+}{M\mathcal{W}_2}(N_{K/Q}(p) + 1) - 2w\sqrt{N_{K/Q}(p)} \geq C.
\]

Then, for every \( c \in \mathcal{L}(R) \) with \( \mu_R(c) = [p] \), there exist at least \( C \) maximal left (right) \( R \)-ideals of reduced norm \( p \) and class \( c \). Here \( h^+ = |C^+(\mathcal{O}_K)| \) is the narrow class number, and \( w \) and \( M \) are constants depending on \( \mathcal{D} \) (see [39,40]).

**Proof.** Although not explicitly stated in this way, this is proved by Kirschmer and Voight in [39,40]: In the proof of [39, Proposition 7.7], a lower bound on the entries of a matrix \( T \) (in their notation) is derived, which immediately gives a lower bound on the entries of a matrix \( T(p) \) (in their notation). This is exactly what we need, as is clear from their definition of \( T(p) \). \( \square \)

**Optimal embeddings.** Let \( L/K \) be a quadratic field extension, and \( T \) a classical Eichler \( \mathcal{O}_K \)-order in \( A \) of squarefree level \( \mathfrak{M} \ll \mathcal{O}_K \). If \( \mathcal{O} \) is an order in \( L \), every embedding \( \iota : \mathcal{O} \to T \) gives rise to a unique embedding \( \iota : L \to A \), and \( \iota \) is an optimal embedding if \( \iota(L) \cap T = \mathcal{O} \). For \( a \in T^\times \), \( \mathcal{O} \to T \), \( x \mapsto a(x)\bar{a}^{-1} \) is then another such embedding. The number of optimal embeddings up to conjugation by units is bounded above by a constant (depending only on \( \mathcal{D} \) and \( \mathfrak{M} \)) times \( h(\mathcal{O}) \) (see [53, Corollaire III.5.12]). Since \( [T^\times : \mathcal{O}_K^\times] \) is finite, the total number of optimal embeddings of \( \mathcal{O} \) into \( T \) is still bounded by a constant times \( h(\mathcal{O}) \).

**Quadratic forms.** We use a theorem about representation numbers of totally positive definite quadratic forms over totally real fields. Let \( V \) be an \( n \)-dimensional \( K \)-vector space. An \( \mathcal{O}_K \)-lattice \( L \) of rank \( n \) is a finitely generated \( \mathcal{O}_K \)-submodule of \( V \) that generates \( V \) (over \( K \)). Together with a quadratic form \( q : V \to K \) with \( q(L) \subset \mathcal{O}_K \), \((L,q)\) it is a quadratic lattice. For \( a \in \mathcal{O}_K \) we set

\[
r(L,a) = \left| \left\{ x \in L \mid q(x) = a \right\} \right|.
\]

An element \( a \in \mathcal{O}_K \) is locally represented everywhere by \((L,q)\) if it is represented by the completion \( L_v = L \otimes_{\mathcal{O}_K} \mathcal{O}_{K,v} \) for all places \( v \) of \( K \). The following result is a special case of Theorem 5.1 in [50].

---

\(^6\) Though unconventional, we keep the qualifier “classical” for consistency with the earlier sections.
Proposition 7.4. Let $(L, q)$ be a quadratic $O_K$-lattice of rank four and suppose that $q$ is totally positive definite. Then, for every $\eta > 0$ and $s \in \mathbb{N}_0$, there exists a constant $C_{\eta, s} > 0$, such that for all $a \in O_K$ that are locally represented everywhere by $L$, with $|N_{K/Q}(a)|$ sufficiently large and $p^s \mid \mathfrak{a}O_K$ if $L_p$ is anisotropic, the asymptotic formula

$$r(L, a) = r(\text{gen} L, a) + O\left(\left|N_{K/Q}(a)\right|^{13\over 15 + \varepsilon}\right)$$

holds with

$$r(\text{gen} L, a) \geq C_{\eta, s} \cdot N_{K/Q}(a)\left(Q_{(\mathfrak{a}(q(L)))^{-1}}\right)^{-1} - \eta.$$

In particular, $r(L, a)$ is of order of magnitude $|N_{K/Q}(a)|^{1-\eta}$. If $T$ is any classical $O_K$-order and $l$ any left $T$-ideal (in particular if $l = T$), then the restriction of the reduced norm to $l$ makes $(l, nr | l)$ into a quadratic $O_K$-lattice of rank four and this is the situation that we will apply this result to.

Ideal theory in $R$. Let $\alpha$ be the set of all classical maximal $O_K$-orders in $A$ (i.e., the equivalence class of the maximal order $R$). Conjugation extends to ideals: For $I \in \mathcal{F}_\nu(\alpha)$ define $I = \{x \mid x \in I\}$. Then $I$ is a fractional $(\mathcal{O}_\nu(1), \mathcal{O}_\nu(1))$-ideal, $I \cdot \bar{I} = \mathcal{O}_\nu(1) nr(I)$, and $\bar{I} \cdot I = \mathcal{O}_\nu(1) nr(I)$, and hence $I^{-1} = \bar{I} \cdot (\mathcal{O}_\nu(1) nr(\bar{I}))^{-1} = (nr(1)\mathcal{O}_\nu(1))^{-1} \cdot \bar{I}$.

$\mathcal{F}_\nu(\alpha)$ takes a particularly simple form: If $p \not\mid \mathfrak{D}$ then there exists a maximal two-sided $R$-ideal $\mathfrak{P}$ with $\mathfrak{P}^2 = p$, $nr(\mathfrak{P}) = p$ and if $I$ is a left or right $R$-ideal with $nr(I) = p^k$, then $I = \mathfrak{P}^k$.

If $p \not\mid \mathfrak{D}$, then $\mathfrak{P} = pR$ is the maximal two-sided $R$-ideal lying above $p$, and $R_p/\mathfrak{P}_p \cong M_2(O_{K,p}/p) \cong M_2(F_{\mathfrak{N}_K/Q}(p))$. In particular there are $N_{K/Q}(p) + 1$ maximal left $R$-ideals (respectively maximal right $R$-ideals) with reduced norm $p$. If $M, N$ are two distinct maximal left $R$-ideals with $nr(M) = nr(N) = p$, then $M \cap N = \mathfrak{P}$ (since the composition length of $M_2(F_{\mathfrak{N}_K/Q}(p))$ is two). This implies that if $M \cdot M' = N \cdot N'$ with maximal integral $M', N' \in \mathcal{F}_\nu(\alpha)$, then $M \cdot M' = N \cdot N'$ and this necessarily $M' = \bar{M}$, $N' = \bar{N}$.

We therefore explicitly know all relations between maximal integral elements of $\mathcal{F}_\nu(\alpha)$: From Proposition 4.12 we know that all relations are generated from those between pairs of products of two elements and it also characterizes the only relation between maximal integral elements of coprime reduced norm. With the discussion above we now also know the relations between two maximal integral elements of the same reduced norm: Either there are none, or the product is $\mathfrak{P}$.

A left $R$-ideal $l$ is primitive if it is not contained in an ideal of the form $Ra$ with $a \subset O_K$. If $nr(l) = p^k$ with $p \in \text{max}(O_K)$ and $l$ is primitive, then it has a unique rigid factorization in $\mathcal{I}_\nu(\alpha)$.

7.3. Proofs of Proposition 7.1 and Proposition 7.2

We start with some lemmas.

Lemma 7.5. Let $T$ be a classical $O_K$-order in $A$. For all but finitely many associativity classes of totally positive prime elements $q \in O_K$ we have: If $x \in T$ with $nr(x) = q$ and $x^2 = \varepsilon q$ for some $\varepsilon \in T^\times$, then $\varepsilon = -1$.

Proof. $x$ satisfies the polynomial equation $x^2 - tr(x)x + nr(x) = 0$. Substituting $x^2 = \varepsilon q$ and $nr(x) = q$ yields

$$tr(x)x = (1 + \varepsilon)q.$$  

(2)

It will thus suffice to show that for all but finitely many $O_K q$, we have $tr(x) = 0$.

Assume that $q \in O_K$ is a totally positive prime element, $x \in T$ with $x^2 = \varepsilon q$ and $tr(x) \neq 0$. Then $K(x) = K(\varepsilon)$ by (2). Let $L = K(\varepsilon)$. Since $\varepsilon \in L \cap T^\times \subset O_L^\times$,

$$O_L q = O_L \varepsilon q = (O_L x)^2,$$
and therefore \( q \) ramifies in \( \mathcal{O}_L \), implying \( \mathcal{O}_K q\mid d_{L/K} \). Hence, for fixed \( L \) there are only finitely many possibilities for \( \mathcal{O}_K q \), and moreover there are only finitely many possibilities for \( L = K(\varepsilon) \) because \( \left[T^*_K : \mathcal{O}_K^* \right] \) is finite since \( A \) is totally definite.\(^7\) Thus there are, up to associativity, only finitely many such \( q \). \( \square \)

**Lemma 7.6.** Let \( T \) be a classical \( \mathcal{O}_K \)-order in \( A \). For every \( M \in \mathbb{N} \) there exists a \( C \in \mathbb{N} \) such that for all totally positive prime elements \( q \in \mathcal{O}_K \) with \( n_r a_p / K_p(\mathfrak{P}_p) \) for all \( p \in \max(\mathcal{O}_K) \) and \( N_{K/Q}(q) > C \)

\[
\left| \left\{ a \in T \left| n_r(a) = q \text{ and } a^2 \neq -q \right. \right\} \right| \geq M.
\]

**Proof.** Let \( q \) be a totally positive prime element of \( \mathcal{O}_K \). We derive an upper bound with order of magnitude \( \sqrt{N_{K/Q}(q)} \log(N_{K/Q}(q))^{2|K:Q|-1} \) on the number of elements \( a \in T \) with \( a^2 = -q \) (based on counting optimal embeddings). Comparing this to the lower bound of order of magnitude \( N_{K/Q}(q)^{1-\eta} \) for the number of elements \( a \in T \) with \( n_r(a) = q \) obtained from Proposition 7.4 will give the result.

If \( a \in T \) with \( n_r(a) = q \) and \( a^2 = -q \), then \( \mathcal{O}_K[a] \subseteq T \) is isomorphic to the order \( \mathcal{O}_K[\sqrt{-q}] \) in the relative quadratic extension \( K(\sqrt{-q}) \). We determine an upper bound the number of embeddings of \( \mathcal{O}_K[\sqrt{-q}] \) into \( T \). For this we may without loss of generality assume that \( T \) is a classical Eichler order of squarefree level, for otherwise we may replace it by a classical Eichler order of squarefree level in which it is contained (e.g., a classical maximal order), and bound the number of embeddings there.

Let \( L = K(\sqrt{-q}) \). Since \( f = X^2 + q \) is the minimal polynomial of \( \sqrt{-q} \) over \( K \), we get for the different \( \delta_{L/K}(\sqrt{-q}) = f'(\sqrt{-q}) = 2\sqrt{-q} \). Therefore, we find for the conductor of \( \mathcal{O}_K[\sqrt{-q}] \) in \( \mathcal{O}_L \),

\[
f_{\mathcal{O}_K[\sqrt{-q}]} = \delta_{L/K}(\sqrt{-q})D_{L/K}^{-1} | 2\mathcal{O}_L
\]

(cf. [43, Proposition 4.12 and Theorem 4.8]). Since \( 2\mathcal{O}_L \subseteq \mathcal{O}_K[\sqrt{-q}] \subseteq \mathcal{O}_L \) and \( \mathcal{O}_{L/2\mathcal{O}_L} = 2^{[L:Q]} \), there are at most \( 2^{2[L:Q]} \) orders in \( \mathcal{O}_L \) that contain \( \mathcal{O}_K[\sqrt{-q}] \). For any such order \( \mathcal{O} \) with \( \mathcal{O}_K[\sqrt{-q}] \subseteq \mathcal{O} \subseteq \mathcal{O}_L \), we have

\[
h(\mathcal{O}) = h(\mathcal{O}_L) \frac{|(\mathcal{O}_L/\mathcal{O})|^{-X}}{|(\mathcal{O}/\mathcal{O}_L)|^{-X}} \leq h(\mathcal{O}_L)2^{[L:Q]}
\]

(cf. [44, 1.12.9 and 1.12.11]). The number of optimal embeddings of \( \mathcal{O} \) into \( T \) is bounded by a constant times \( h(\mathcal{O}) \), and hence the total number of embeddings of \( \mathcal{O}_K[\sqrt{-q}] \) into \( T \) is bounded by a constant times \( h(\mathcal{O}_L) \), where the constant does not depend on \( q \). Combining the upper bound

\[
h(\mathcal{O}_L) \ll \sqrt{|d_L|} \log(|d_L|)^{[L:Q]-1}
\]

(cf. [43, Theorem 4.4]), with

\[
d_L = N_{L/Q}(D_{L/Q}) = N_{L/Q}(D_{K/Q})N_{L/Q}(D_{L/K}) \leq d_K^2 2^{[L:Q]} |N_{L/Q}(\sqrt{-q})| = d_K^2 2^{[L:Q]} N_{K/Q}(q)
\]

(here \( D_{L/K} | 2\sqrt{-q} \mathcal{O}_L \) was used), we obtain

\(^7\) It should be pointed out that an even stronger statement is true. For any fixed totally real field \( K \), there are only finitely many totally imaginary quadratic extensions that have larger unit group (i.e., weak unit defect), while all other totally imaginary quadratic extensions \( L/K \) have \( \mathcal{O}_K^* = \mathcal{O}_L^* \) (i.e., strong unit defect). This follows from \( [\mathcal{O}_K^* : \mu(L)\mathcal{O}_K^*] \in \{1, 2\} \) [54, Theorem 4.12]: For \( \varepsilon \in \mathcal{O}_K^* \) we have \( \varepsilon^2 = \eta \chi \) with \( \zeta \in \mu(L) \) and \( \eta \in \mathcal{O}_L^* \). But ord(\( \chi \)) \( [L : Q] = 2[K : Q] \) and if \( \gamma \in \mathcal{O}_K^* \), then \( \eta \gamma \chi \) yields the same extension. Since \( [\mathcal{O}_K^* : \mathcal{O}_L^*] = \infty \) there are therefore only finitely many such extensions. This argument is due to Remak in [48, 3.3].
and thus an upper bound of the same order for \(||a \in T | nr(a) = q \rangle = q^2 = -q\)|.

By Proposition 7.4, for every \( \eta > 0 \) and sufficiently large (in norm) \( q \) with \( q \) being locally represented everywhere by the norm form, \(||a \in T | nr(a) = q\rangle|\) grows with order of magnitude \( N_{K/Q}(q)^{1-\eta} \), and the claim follows, by choosing \( \eta \) small enough, say \( \eta < \frac{1}{4} \). \( \Box \)

**Remark 7.7.** For any classical \( O_K \)-order \( T \) of \( A \) there are infinitely many pairwise non-associated totally positive primes \( q \in O_K \) that are locally represented everywhere by \( nr_{A/K} \) on \( T \). This can easily be seen as follows: Let \( \mathfrak{D} \cap O_K \) be the discriminant of \( T \). If \( p \in \text{max}(O_K) \) with \( p \nmid \mathfrak{D} \), then \( T_p \cong M_2(O_{K_p}) \) and thus \( nr_{A_p/K_p}(T_p) = O_{K_p} \). If \( p \nmid \mathfrak{D} \), since center \( (T_p) = O_{K_p} \), certainly still every square of \( O_{K,p} \) is represented by \( nr_{A_p/K_p} \) on \( T_p \) (in fact, if \( p \nmid \mathfrak{D} \) but \( p \nmid \mathfrak{A} \) then \( T_p \) is isomorphic to the unique classical maximal \( O_{K,p} \)-order in the unique quaternion division algebra over \( K_p \), for which \( nr(T_p) = O_{K,p} \) also holds). By Hensel's Lemma therefore every totally positive prime element \( q \in O_K \) with \( q \equiv 1 \mod 4\mathfrak{D} \) is locally represented everywhere by \( nr_{A/K} \) on \( T \). But there are infinitely many pairwise non-associated such primes, because every class of the ray class group \( C^+_{4\mathfrak{D}\mathfrak{A}}(O_K) \) contains infinitely many pairwise distinct maximal ideals, and primes \( q \) of the required form correspond exactly to the trivial class in \( C^+_{4\mathfrak{D}\mathfrak{A}}(O_K) \).

**Lemma 7.8.** Let \( q \) be a totally positive prime element of \( O_K \). Let \( I \) be a non-principal right \( R \)-ideal with \( nr(I) = q^m O_K \) for some \( m \in \mathbb{N} \), and \( J \) be a left \( \mathfrak{S}(I) \)-ideal with \( nr(J) = q^o O_K \) for some \( n \in \mathbb{N} \) such that: \( I \cong J \) (as left \( S \)-ideals) and \( I \) (respectively \( J \)) is not contained in any principal left \( S \)-ideal except \( S \) itself, and not contained in any principal right \( O_r(I) \)-ideal (respectively right \( O_r(J) \)-ideal) except \( O_r(I) \) (respectively \( O_r(J) \)) itself.

Assume further that \( a \in S \) with \( nr(a) = q \) and \( a^2 S \neq q S \).

1. For all \( l \in \mathbb{N} \), \((a^l \overline{\alpha}^{-1})a^l I \) is a principal right \( R \)-ideal and an atom of \( \mathcal{H}_R^* \). In particular, \( a^m q^m \in \mathcal{A}(R^*) \) for all \( l \in \mathbb{N} \).
2. \( \overline{J} I \in \mathcal{A}(\mathcal{H}_R^*) \) if it is primitive. In particular if \( m = n = 1 \) and \( I \neq J \), then \( \overline{J} I \in \mathcal{A}(\mathcal{H}_R^*) \).

**Proof.** Since \( I \) is not contained in any principal right \( R \)-ideal, it is in particular not contained in \( q R \), hence primitive. Similarly, \( J \) is primitive. Let \( M_1 \ast \cdots \ast M_m \in \mathbb{Z}_{\overline{x}(\alpha)}(1) \) and \( N_1 \ast \cdots \ast N_n \in \mathbb{Z}_{\overline{x}(\alpha)}(J) \), with \( M_1, \ldots, M_m, N_1, \ldots, N_n \in \mathcal{M}_r(\alpha) \), be the unique rigid factorizations of \( I \) and \( J \).

1. Since \( I \cong J \) as left \( S \)-ideals, \((a^l \overline{\alpha}^{-1})a^l I = a^l \overline{J} I \) is principal. A rigid factorization of it is given by

\[
(a^l \overline{N}_i a^{-1}) \ast \cdots \ast (a^l \overline{N}_i a^{-1}) \ast (a^l S a^{-1}) a \ast (a^l^{-1} S a^{-l-1}) a \ast \cdots \ast (a S a^{-1}) a \ast M_1 \ast \cdots \ast M_m
\]

with \( M_1, a^l \overline{N}_i a^{-1}, (a^l \overline{N}_i a^{-1}) a \in \mathcal{M}_r(\alpha) \) for \( i \in [1, m], j \in [1, n] \) and \( k \in [0, l-1] \). By the restrictions imposed on \( I \), \( J \), and \( a \), this is the only rigid factorization of \( a^l \overline{J} I \). Since any non-empty proper subproduct starting from the left (or the right) is non-principal, it is an atom in \( \mathcal{H}_R^* \). The “in particular” statement follows by setting \( J = I \), as then \( a^l \overline{J} I = a^m q^m R \in \mathcal{A}(\mathcal{H}_R^*) \) and because of Proposition 5.20, therefore \( a^m q^m \in \mathcal{A}(R^*) \).

2. By primitivity,

\[
\overline{N}_n \ast \cdots \ast \overline{N}_1 \ast M_1 \ast \cdots \ast M_m \in \mathbb{Z}_{\overline{x}(\alpha)}(\overline{J} I)
\]

is the unique rigid factorization of \( \overline{J} I \), and since as before no non-empty proper subproduct from the left (or the right) is principal, it is an atom in \( \mathcal{H}_R^* \). For the “in particular” statement, note that if \( m = n = 1 \) (i.e., \( I \) and \( J \) are both maximal left \( S \)-ideals), then \( \overline{J} I = q R \) if and only if \( I = J \), and otherwise \( \overline{J} I \) is necessarily primitive. \( \Box \)
Lemma 7.9. Let \( I \) be a left \( R \)-ideal, \( S = \mathcal{O}_l(I) \), and \( a \in R \cap S \). Then
\[
\prod_{i=1}^{l} (a^{l-i+1}Ra^{-(l-i+1)})a \cdot I = a^l I = (a^l Ia^{-l})a^l = (a^l Ia^{-l}) \cdot \prod_{i=1}^{l} (a^{l-i+1}Sa^{-(l-i+1)})a
\]
with the left-most and the right-most expressions being proper products of
\[
(a^{l-i+1}Ra^{-(l-i+1)})a, I, (a^{l-i+1}Sa^{-(l-i+1)})a, a^l Ia^{-l} \in \mathcal{I}_v(\alpha).
\]
(The products have to be read in ascending order with “\( i = 1 \)” to the very left.)

Proof. The formulas are clear, and so is that the products are proper ones. The key point is that these one-sided ideals are indeed integral. But this is so because \( a \in S \), hence \( a \in d^kSa^{-k} \) for all \( k \in \mathbb{N}_0 \), implying that \( (a^kS) \in \mathcal{I}_v(\alpha) \), and similarly \( a \in R \), thus \( (a^kR) \in \mathcal{I}_v(\alpha) \). \( \Box \)

Lemma 7.10. Let \( M \) be a maximal left \( R \)-ideal, and \( N \) a maximal left \( O_l(M) \)-ideal. If \( M \cdot N = N' \cdot M' \), then \( \mathcal{M} \cdot N' = N \cdot \mathcal{M}' \).

Proof. Since \( \mathcal{O}_l(\mathcal{M}) = \mathcal{O}_l(M) = \mathcal{O}_l(N') \) and \( \mathcal{O}_l(T) = \mathcal{O}_l(M') = \mathcal{O}_l(\mathcal{M}') \) the product is proper. We have
\[
\mathcal{M} \cdot N' \cdot M' = \mathcal{M} \cdot M \cdot N = \text{nr}(M)\mathcal{O}_l(N) \cdot N = N \cdot \mathcal{O}_l(N) \text{nr}(M) = N \cdot \mathcal{M}' \cdot M',
\]
and thus \( \mathcal{M} \cdot N' = N \cdot \mathcal{M}' \). \( \Box \)

Proof of Proposition 7.1. Let \( p \in \mathcal{O}_K \) be a totally positive prime element with \( p\mathcal{O}_K \uparrow d_K \mathcal{D}_M \) and with \( \text{nr}(p) \) satisfying the bound of Proposition 7.3 for the classical maximal order \( R \) (with \( C = 1 \)). Then there exists a maximal right \( R \)-ideal \( U \) with \( \text{nr}(U) = p\mathcal{O}_K \) that is non-free (i.e., non-principal) but is stably free (i.e., \( \{\text{nr}(U)\} = 0 \) in \( C^+(\mathcal{O}_K) \)). Let \( U = U_0, \ldots, U_r \) be the maximal left \( \mathcal{O}_l(U) \)-ideals of reduced norm \( p\mathcal{O}_K \) (of which there are \( r + 1 = N_{K/Q}(p) + 1 \)). By Lemma 7.6, there exists a totally positive prime element \( q \in \mathcal{O}_K \), \( q\mathcal{O}_K \uparrow pd_K \mathcal{D}_M \), and an element
\[
a \in \mathcal{O}_l(U) \cap \bigcap_{j=0}^{r} \mathcal{O}_l(U_j) \text{ with } \text{nr}(a) = q \text{ and } a^2 \neq -q,
\]
and in fact, by Lemma 7.5, we may make this choice such that \( a^2 \neq \varepsilon q \) for any \( \varepsilon \in R^\times \). In addition, we may take \( N_{K/Q}(q) \) to be sufficiently large to satisfy the bound of Proposition 7.3 for \( \mathcal{O}_l(U) \) (with \( C = 2 \)). Then there exist distinct left \( \mathcal{O}_l(U) \)-ideals \( I \) and \( J \) such that \( I \uparrow J \subseteq U \) and \( \text{nr}(I) = \text{nr}(J) = q\mathcal{O}_K \).

Set \( S = \mathcal{O}_l(I) \), and observe that \( S \subseteq R \), because \( U \subseteq I \). By Lemma 7.8, \( (a^lJa^{-l})a \in \mathcal{A}(\mathcal{H}_S^*) \) for all \( l \in \mathbb{N}_0 \), say \( (a^lJa^{-l})a \in \mathcal{O}_l(\mathcal{H}_s) \). We consider the principal right \( S \)-ideal \( X_l = (a^lJa^{-l})a \uparrow S \), say \( X_l = X_lS \) with \( X_l \in S^* \). We will first determine all possible rigid factorizations of \( X_l \) in \( \mathcal{I}_v(\alpha) \). As in Lemma 7.8, the right \( S \)-ideal \( a^lJa^{-l}a \) has reduced norm \( q^{l+2}\mathcal{O}_K \), is primitive, and thus possesses a unique rigid factorization,
\[
(a^lJa^{-l})a \ast (a\mathcal{O}_l(I)a^{-l})a \ast (a^{-l-1}Ia^{-l-1})a \ast \cdots \ast (a\mathcal{O}_l(I)a^{-l})a \ast I \in \mathcal{Z}_{X_v(\alpha)}((a^lJa^{-l})a) \mathcal{I}_v(\alpha).
\]
with the \( l + 2 \) factors \( a^lJa^{-l} \), \( (a^lJa^{-l})a \) for \( k \in \{0, l-1\} \) and \( I \) all in \( \mathcal{M}_v(\alpha) \).

For an element with a unique rigid factorization we make the convention of identifying the element and its factorization when this is notationally convenient. For principal ideals we omit the order
and only write the generator if it is clear from the neighboring elements in the factorization what the order must be. For example, we can write the previous rigid factorization as $a^dJa^{-l} * a^d * I$.

$X_l$ has $(r + 1)^{l+4}$ rigid factorizations: They arise from the different rigid factorizations $U_l * \overline{U}_l \in Z_{\mathcal{I}_p(\alpha)}(\mathcal{O}_l(U)p)$ for $i \in [0, r]$ and the possible transpositions of $U_l$ and $\overline{U}_l$. We denote the rigid factorization of $X_l$ that arises from $a^dJa^{-l} * a^d * U_l * \overline{U}_l * I$ by transposing the one-sided ideals of norm $p$ to the positions $m \in [-l, l + 1]$ and $n \in [m, l + 1]$ in the factorization by $F_{i,m,n}$: Here, the left-most position in the rigid factorization is denoted by $-1$, the right-most by $l + 1$. So, by “the rigid factorization obtained by transposing $U_l$ to the position $-1$ and $\overline{U}_l$ to $l + 1”$ we mean the unique rigid factorization of $X_l$ that has a factor of norm $p\mathcal{O}_l$ as the first factor and as the last factor, and that can be transformed into $a^dJa^{-l} * a^d * U_l * \overline{U}_l * I$ by transposition of maximal integral elements with coprime norm.

For $i \in [0, r]$ let $V_i \in \mathcal{M}_p(\alpha)$ and $M_i \in \mathcal{M}_v(\alpha)$ be defined by $\overline{U}_lI = M_lV_i$ under transposition, and let $W_i \in \mathcal{M}_v(\alpha)$ and $N_i \in \mathcal{M}_v(\alpha)$ be defined by $W_iN_i = JU_l$ under transposition. ([$V_i | i \in [0, r]$] is then the set of all $r + 1$ left $S = \mathcal{O}_l(l)$-ideals of reduced norm $p$. Similarly [$W_i | i \in [0, r]$] is then the set of all $r + 1$ left $\mathcal{O}_l(J)$-ideals of reduced norm $p$, and since $\mathcal{O}_l(l) \cong \mathcal{O}_l(J)$ the sets are actually conjugate under conjugation by an element of $\mathcal{A}_r^*$. By Lemma 7.10 we then also have $U_lM_i = IV_i$ and $W_iJ = N_i\overline{U}_l$ under transposition. Using Lemma 7.9 to see that $a$ transposes “nicely” with $U_l$ and $\overline{U}_l$, we can explicitly describe all $F_{i,m,n}$ as follows:

**Case 1.** If $m = n = -1$:

$$F_{i,m,n} = a^dW_l a^{-l} * a^d\overline{W}_l a^{-l} * a^dJa^{-l} * a^d * I.$$

**Case 2.** If $m = -1$ and $0 \leq n \leq l$:

$$F_{i,m,n} = a^dW_l a^{-l} * a^d\overline{N}_l a^{-l} * a^n * a^{l-n}U_l a^{-(l-n)} * a^{l-n} * I.$$

**Case 3.** If $0 \leq m \leq n \leq l$:

$$F_{i,m,n} = a^dJa^{-l} * a^m * a^{l-m}U_l a^{-(l-m)} * a^n * a^{l-n}U_l a^{-(l-n)} * a^{l-n} * I.$$

**Case 4.** If $m = -1$ and $n = l + 1$:

$$F_{i,m,n} = a^dW_l a^{-l} * a^d\overline{N}_l a^{-l} * a^d * M_i * \overline{V}_l.$$

**Case 5.** If $0 \leq m \leq l$ and $n = l + 1$:

$$F_{i,m,n} = a^dJa^{-l} * a^m * a^{l-m}U_l a^{-(l-m)} * a^{l-m} * M_i * \overline{V}_l.$$

**Case 6.** If $m = n = l + 1$:

$$F_{i,m,n} = a^dJa^{-l} * a^d * I * V_l * \overline{V}_l.$$

For each of these rigid factorizations of the ideal $X_l$ in $\mathcal{I}_p(\alpha)$ we can form minimal subproducts of principal one-sided ideals (starting from the left or the right) to obtain a representation of $X_l$ as a product in $\mathcal{H}_{\mathcal{S}}$ (and hence a representation of $x_l$ as a product of elements of $S^\bullet$). But only when each of these minimal principal subproducts is an atom of $\mathcal{H}_{\mathcal{S}}$, this gives rise to an actual rigid factorization of $x_l$ into atoms. We discuss the individual cases one-by-one:
Case 1. If \( m = n = -1 \): If \( W_i \) is non-principal, then this does not give rise to a rigid factorization into atoms, as \( m = n = -1 \) implies that the first principal factor is \( d'(W_i W_{i-1})a^{l_1} = d'(pC_\ell(I))a^{l_1} \), and this is not an atom (since there is at least one element in \( \{W_i \mid i \in \{0, r\}\} \) that is principal by Proposition 7.3). If on the other hand \( W_i \) is principal, then this gives rise to a rigid factorization of \( X_i \) in \( H_{S^*} \) of length 3, with atomic factors \( d'W_i a^{-l_1} \), \( d'W_{i-1} a^{-l_1} \) and \( d' \bar{a} a^{-l_1} \), which in turn gives rise to a rigid factorization of length 3 of \( x_i \in S \).

Case 2. If \( m = -1 \) and \( 0 \leq n \leq l \):

Case 2a. If \( U_i \equiv I \): Then the last principal factor is necessarily \( (d^{-n-1}U_i a^{-(l-n)}d)^{-n}I \). If \( n < l \), then transposing \( U_i \) to the right shows that this is not an atom in \( H_{S^*} \). If \( n = l \) then \( U_i \) is an atom if and only if \( V_i \) is non-principal. Since also \( U_i \equiv J \), the factor \( W_i Ni_i = \bar{J} U_i \) is principal, and, because \( \bar{J} \) and \( U_i \) are non-principal, this is either an atom (if \( W_i \) is non-principal), or a product of two atoms (if \( W_i \) is principal). So if \( V_i \) is non-principal we get a rigid factorization of length either \( l + 2 \) or \( l + 3 \), and if \( V_i \) is principal we get no rigid factorization into atoms.

Case 2b. If \( U_i \not\equiv I \): Then either there are no non-trivial principal factors (if \( W_i \) is non-principal), or the first factor is \( W_i \) and the remaining product does not factor into non-trivial principal factors. But then this second factor is not an atom, because after transposition of \( U_i \) to the very left of the second factor (i.e., position 0), we have a principal factor \( \bar{W}_i \). So in any case, this does not give rise to a rigid factorization into atoms.

Case 3. If \( 0 \leq m \leq n \leq l \): If \( l \not\equiv U_i \), then there are no non-trivial principal factors, and hence no rigid factorization into atoms is obtained.

If \( l \equiv U_i \), then the first principal factor is \( (d^1 \bar{J} a^{-1})a^m(d^{-m}U_i a^{-l-n}) \), and the last one is \( (d^{-n-1}U_i a^{-(l-n)}d)^{-n}I \). If \( m > 0 \) (or \( n < l \)), then by transposing \( U_i \) to the left in the first factor (or \( U_i \) to the right in the second factor) once, we see that this does not give rise to a rigid factorization into atoms. Consider now \( m = 0 \) and \( n = l \). If \( V_i \) is principal, then \( \bar{J} U_i = V_i \bar{W}_i \) implies that the first factor \( d^1 \bar{J} U_i a^{-1} \) is not an atom, and hence again we get no rigid factorization into atoms. Analogously we get no rigid factorization into atoms if \( W_i \) is principal. If on the other hand \( V_i \) and \( W_i \) are both non-principal then \( \bar{J} U_i \) is an atom, and so \( U_i \bar{J} \). Thus we obtain a rigid factorization of \( X_i \) (and hence of \( x_i \)) of length \( l + 2 \). (It is then in fact the same one as the one obtained from Case 2 in the same situation.)

Case 4. If \( m = -1 \) and \( n = l + 1 \):

Case 4a. If \( U_i \equiv I \): Then \( W_i Ni_i \) and \( M_i \bar{W}_i \) are both principal. If \( W_i \) is non-principal, then \( W_i Ni_i = \bar{J} U_i \) is an atom since \( J \) is non-principal. If \( W_i \) is principal, then \( W_i Ni_i \) is a product of two atoms. Similarly, \( M_i \bar{W}_i \) is either an atom or a product of two atoms. So in this case we get a rigid factorization of length \( l + 2 \), \( l + 3 \) or \( l + 4 \). (In the case that \( V_i \) is non-principal, it is the same as in Case 2. In the case that \( V_i \) and \( W_i \) are both non-principal it is the same as in Case 3 in the same situation.)

Case 4b. If \( U_i \not\equiv I \): Then \( W_i Ni_i \) and \( M_i \bar{W}_i \) are both non-principal. If \( W_i \) is principal, but \( \bar{W}_i \) is not, then the second principal factor is necessarily \( (d^{-1} Ni_i a^{-1})d^1 M_i \bar{W}_i \), and this cannot be split as a non-trivial product of principal factors. But transposing \( \bar{W}_i \) to the very left in this factor gives a principal factor \( W_i \), hence \( (d^{-1} Ni_i a^{-1})d^1 M_i \bar{W}_i \) is not an atom. Arguing analogously, if \( \bar{W}_i \) is principal but \( W_i \) is not, no rigid factorization into atoms is obtained.

Finally, if \( W_i \) and \( V_i \) are both principal, we get a rigid factorization into 3 atoms.

Case 5. If \( 0 \leq m \leq l \) and \( n = l + 1 \): This is analogous to Case 2.

Case 6. If \( m = n = l + 1 \): This is analogous to Case 1.

Since there is at least one \( i \in \{0, r\} \) for which \( W_i \) is principal, we get at least one rigid factorization of \( x_i \) of length 3 from Case 1. For \( i = 0 \), \( U_i \equiv I \), so Case 4 gives at least one factorization with length in \( \{l + 2, l + 4\} \). Note that which of the lengths in \( \{l + 2, l + 4\} \) occur in Case 2, Case 3, and Case 4 depends only on the principle of certain one-sided ideals, and not on \( l \). Thus we have shown that there exists a set \( \emptyset \neq E \subset \{2, 3, 4\} \) such that, for any choice of \( l \in \mathbb{N}_0 \),
Remark 7.11.

1. In the proof, the classical $\mathcal{O}_K$-order

$$T = \mathcal{O}_l(U) \cap \bigcap_{j=0}^r \mathcal{O}_r(U_j)$$

is maximal at every prime $r \in \text{max}(\mathcal{O}_K)$ with $r \neq p\mathcal{O}_K$ (thus $T_r \cong M_2(\mathcal{O}_{K,r})$ if $r \mid p\mathcal{D}$ and $T_r$ is isomorphic to the unique classical maximal $\mathcal{O}_{K,r}$-order in the unique quaternion division algebra over $K$ if $r \mid \mathcal{D}$). At $p = p\mathcal{O}_K$, it is not hard to see by local calculations that

$$T_p \cong \left\{ \begin{pmatrix} a & b \\ p^2c & a + pd \end{pmatrix} \mid a, b, c, d \in \mathcal{O}_{K,p} \right\}.$$ 

But $T_p$ is not a classical Eichler order, and so neither is $T$.

2. If $r \in \text{max}(\mathcal{O}_K)$ we can find infinitely many pairwise non-associated totally positive prime elements $q \in \mathcal{O}_K$ such that $r$ splits in $K(\sqrt{-q})$, and infinitely many pairwise non-associated totally positive prime elements $q \in \mathcal{O}_K$ such that $r$ is inert in $K(\sqrt{-q})$: We may restrict ourselves to $q$ with $N_{K/Q}(q)$ odd, and $q\mathcal{O}_K \neq \mathcal{O}_r$. Let $\nu' = \nu + \nu_1$. If $-q \equiv 1 \mod \nu'$, then $-q$ is a square in $\mathcal{O}_K/\mathcal{O}'$ and hence $r$ splits in $K(\sqrt{-q})$. If $-q \equiv a \mod \nu'$, with $a$ a non-square in $\mathcal{O}_K/\mathcal{O}'$, then $r$ is inert in $K(\sqrt{-q})$. It therefore suffices to show that in every class of $(\mathcal{O}_K/\mathcal{O}')^\times$ there are infinitely many pairwise non-associated totally positive prime elements of $\mathcal{O}_K$. Since we have the exact sequence

$$1 \to \mathcal{O}_K^{\times, +}/\{x \in \mathcal{O}_K^{\times, +} \mid x \equiv_1 1\} \to (\mathcal{O}_K/\mathcal{O}')^\times \to \mathcal{C}_r^+(\mathcal{O}_K) \to \mathcal{C}^+(\mathcal{O}_K) \to 1$$

(cf. [43, Lemma 3.2], [44, Exercises VI.1.12, VI.1.13]), it suffices that every class in the kernel of $\mathcal{C}_r^+(\mathcal{O}_K) \to \mathcal{C}^+(\mathcal{O}_K)$ contains infinitely many pairwise non-associated prime elements. But this is so, because in fact every class of $\mathcal{C}_r^+(\mathcal{O}_K)$ contains infinitely many pairwise distinct maximal ideals (cf. [43, Corollary 7 to Proposition 7.9]).

3. Using the previous observation to find a suitable element $a$ in the proof, we can replace Lemma 7.6 by a simpler one if $\mathcal{D} \neq \mathcal{O}_K$: Choosing the totally positive prime element $q \in \mathcal{O}_K$ such that a prime divisor $r \mid \mathcal{D}$ splits in $K(\sqrt{-q})$, the field $K(\sqrt{-q})$ does not embed into $A$ at all (see e.g. [53, Theoreme III.3.8] or [41, Theorem 7.3.3]).

If $\mathcal{D} = \mathcal{O}_K$, we may make use of the fact that the particular classical order $T$ in the proof is contained in a classical Eichler order of squarefree level $p$. Taking $q$ such that $p$ is inert in $K(\sqrt{-q})$, the formulas for counting optimal embeddings [53, Corollaire III.5.12] show that no order of $K(\sqrt{-q})$ embeds into $T$.

For this approach we only need the qualitative statement of Proposition 7.4, but not the order of magnitude.

Proof of Proposition 7.2. It suffices to prove the claim for $n = 1$. Let $a \in \mathcal{R}_v^*$, and let

$$\left\{ I_1^{(1)} \cdots I_k^{(1)}, \ldots, I_1^{(l)} \cdots I_k^{(l)} \right\} = \mathbb{Z}_{\mathcal{L}_v}(\alpha)(Ra) \subset \mathcal{F}(\mathcal{M}_v(\alpha))$$
be the set of all rigid factorizations of \( Ra \) in \( I_\nu(\alpha) \). Using Proposition 7.4, we can choose a totally positive prime element \( q \in \mathcal{O}_K \) with \( q \mid nr(a) \) and such that there exists an \( x \in A^\times \) with \( nr(x) = q \) and

\[
x \in T = \bigcap_{i=1}^l \bigcap_{j=1}^k \mathcal{O}_I(I^{(i)}_j) \cap \mathcal{O}_R(I^{(i)}_j).
\]

We claim \( L(xa) = 1 + L(a) \). The rigid factorizations of \( Rxa \) in \( I_\nu(\alpha) \) are given by all possible transpositions of \( x \) to any position in

\[
I^{(i)}_1 \ast \cdots \ast I^{(i)}_m \ast x,
\]

for all \( i \in [1, l] \). But, since \( x \in T \), it follows from Lemma 7.9 that any such rigid factorization is of the form

\[
I^{(i)}_1 \ast \cdots \ast I^{(i)}_m \ast x \ast x^{-1}I^{(i)}_{m+1} \ast \cdots \ast x^{-1}I^{(i)}_{k} \ast x,
\]

for \( m \in [0, k] \). We see that for the principal subproducts this does not change anything except insert one additional factor (corresponding to \( x \)) at some position. Thus, for each \( i \in [1, l] \), \( I^{(i)}_1 \ast \cdots \ast I^{(i)}_m \ast x \ast x^{-1}I^{(i)}_{m+1} \ast \cdots \ast x^{-1}I^{(i)}_{k} \ast x \) gives rise to a rigid factorization of \( \alpha x \) in \( R^\times \) of length \( l + 1 \) if and only if \( I^{(i)}_1 \ast \cdots \ast I^{(i)}_m \ast x \ast x^{-1}I^{(i)}_{m+1} \ast \cdots \ast x^{-1}I^{(i)}_{k} \ast x \) gives rise to a rigid factorization of \( a \) of length \( l \). \( \square \)

Acknowledgments

I thank Alfred Geroldinger for suggesting the topic, and him and Franz Halter-Koch for reading preliminary versions of this manuscript and providing many valuable comments.

References


