ACTA ARITHMETICA
112.3 (2004)

Congruence monoids

by

Alfred Geroldinger and Franz Halter-Koch (Graz)

1. Introduction. The simplest examples of congruence monoids are the multiplicative monoids $1 + 4\mathbb{N}_0$, $1 + p\mathbb{N}_0$ for some prime number p, and $2\mathbb{N} \cup \{1\}$. They are multiplicative submonoids of $\mathbb{N}$, and they appear in the literature as examples for non-unique factorizations (see [19, Sect. 3.3], [28] and [29]). A first systematic treatment of congruence monoids (defined by residue classes coprime to the module) was given in [20] and in [21], where it was proved that these congruence monoids are Krull monoids. Congruence monoids defined by residue classes which are not necessarily coprime to the module were introduced in [18] as a tool to describe the analytic theory of non-unique factorizations in orders of global fields.

In this paper, we investigate the arithmetic of congruence monoids in Dedekind domains satisfying some natural finiteness conditions (finiteness of the ideal class group and of the residue class rings). The main examples we have in mind are

- multiplicative submonoids of the naturals defined by congruences (called *Hilbert semigroups*);
- (non-principal) orders in algebraic number fields.

The crucial new idea is to use divisor-theoretic methods. As usual in algebraic number theory, the global arithmetical behavior is determined by the structure of the semilocal components and the class group. The class groups of congruence monoids in Dedekind domains are essentially ray class groups (and thus they are well studied objects in algebraic number theory). The semilocal components are congruence monoids in semilocal principal ideal domains. For their arithmetical investigation we construct abstract models which are easier to handle than the concrete arithmetical objects. These abstract models, called AC- and C_0-monoids, are built in a similar way to the finitely primary monoids which turned out to be useful in the investigation of the multiplicative structure of one-dimensional noetherian

2000 *Mathematics Subject Classification*: 11R27, 13F05, 20M14.

domains (see [23]). AC- and C_0-monoids are defined as submonoids of factorial monoids, and their deviation from the factorial overmonoid is measured by class semigroups, a new concept generalizing the usual class groups. In recent investigations by W. Hassler [27], C_0-monoids also proved to be useful as abstract models for the multiplicative arithmetic of noetherian integral domains D satisfying the following finiteness conditions: the divisor class group of the integral closure $\overline{D}$ of D is finite, and if $\mathfrak{f} = (D : \overline{D})$, then the residue class ring $\overline{D}/\mathfrak{f}$ is also finite.

Congruence monoids are atomic (every non-unit is a product of irreducible elements), but in general they do not have unique factorization. A systematic investigation of phenomena of non-unique factorization in rings of integers of algebraic number fields was initiated by W. Narkiewicz (see [30, Ch. 9] for a survey on classical results). In recent years there has been an increasing interest in phenomena of non-unique factorizations in integral domains, initiated by the work of D. D. Anderson, D. F. Anderson and others (see for example [2], [3] and [5]). For an overwiew concerning recent results on non-unique factorizations in monoids and integral domains the interested reader should consult the survey articles in [1] and [9], in particular [4], [6], [7], [8], [12] and [24].

We shall prove that congruence monoids in Dedekind domains show the same phenomena of non-unique factorizations as the rings of integers of algebraic number fields. They are locally tame, have finite catenary degree, and their sets of lengths of factorizations are almost arithmetical multiprogressions. Making allowance for the fact that phenomena of non-unique factorizations are purely multiplicative, most of the arithmetical investigations of this paper are carried out in the language of monoids. An essential tool is the theory of tame and complete ideals of monoids developed in [16].

This paper is organized as follows. In Section 2 we fix the notations concerning the algebraic and arithmetical theory of monoids and recall the basic concepts of non-unique factorizations. In Section 3 we introduce congruence monoids in Dedekind domains and give several different examples. We establish the divisor theory of these monoids and formulate the main result of the paper (Theorem 3.6).

In Sections 4 and 5 we develop the essential tools for the proof. For the reason mentioned above they are formulated in the language of monoids. In Section 4 we introduce the concept of class semigroups. It is an appropriate refinement of the usual notion of a class group in algebraic number theory. Its finiteness allows the transfer of arithmetical properties from a (simple) monoid to a (more complicated) submonoid. In Section 5 we define AC-monoids and C_0-monoids which are suitable models for the arithmetically interesting congruence monoids. In this paper we confine ourselves to the investigation of the arithmetical properties of these monoids (a system-

atical theory from an algebraic point of view will be presented in a forthcoming paper). Finally, in Section 5 we apply the abstract results to congruence monoids in Dedekind domains.

2. Notations and preliminaries on monoids. Let $\mathbb{N}$ denote the set of positive integers, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $m, n \in \mathbb{Z}$, we set

$$[m, n] = \{x \in \mathbb{Z} \mid m \le x \le n\}.$$

For a set X, we denote by $|X| \in \mathbb{N}_0 \cup \{\infty\}$ its cardinality. Our terminology is consistent with that of the survey articles [8], [12] and [24]. For convenience and to fix notations, we recall some key notions and the basic results of the theory of non-unique factorizations which we use in this paper.

Basic notions. By a *semigroup* we mean a non-empty set with a commutative and associative law of composition having a unit element. By a *monoid* we mean a cancellative semigroup. Subsemigroups and submonoids are always assumed to contain the unit element. Usually, we use multiplicative notation and denote the unit element by 1. For subsets A, B of a monoid H, we set $AB = \{ab \mid a \in A,\, b \in B\}$, and for $n \in \mathbb{N}$, we define $A^n = \{a_1 \cdot \ldots \cdot a_n \mid a_1, \ldots, a_n \in A\}$ and $A^{[n]} = \{a^n \mid a \in A\}$.

Additive notation will only be used for the submonoids of $\mathbb{R}^I$.

Concerning the notions of ideal theory and elementary divisibility theory in a monoid, we use the terminology of [25] (but note that there all monoids have an additional zero element which has to be neglected in our context). In particular, by an *s-ideal* of a monoid H we mean a subset $\mathfrak{a} \subset H$ satisfying $\mathfrak{a}H = \mathfrak{a}$.

For each monoid H, we fix a quotient group $\mathsf{q}(H)$ of H. For any subset $E \subset H$, we denote by $[E]$ the submonoid of H generated by E and by $\langle E \rangle$ the subgroup of $\mathsf{q}(H)$ generated by E. For a submonoid $T \subset H$ and any subset $\mathfrak{a} \subset \mathsf{q}(H)$, we set $T^{-1}\mathfrak{a} = \{t^{-1}a \mid t \in T,\, a \in \mathfrak{a}\} \subset \mathsf{q}(H)$. We denote by $H^\times$ the group of invertible elements of H and by $H_{\mathrm{red}} = \{aH^\times \mid a \in H\}$ the associated reduced monoid of H. We call H *reduced* if $H^\times = \{1\}$ (and then $H_{\mathrm{red}} = H$).

Let H be a monoid and $a, b \in H$. We call a a *divisor* of b and write $a \,|\, b$ (or more precisely $a \,|_H\, b$) if $b \in aH$. We call a and b *associated* if $aH = bH$ (or, equivalently, if $aH^\times = bH^\times$). An element $u \in H$ is called an *atom* if $u \notin H^\times$, and for all $a, b \in H$, $u = ab$ implies $a \in H^\times$ or $b \in H^\times$. We denote by $\mathcal{A}(H)$ the set of all atoms of H, and we call the monoid H *atomic* if every $a \in H \setminus H^\times$ is a product of atoms. An element $p \in H$ is called a *prime* if $H \setminus pH$ is a submonoid of H, and H is called *factorial* if every $a \in H \setminus H^\times$ is a product of primes. Every prime is an atom, and a monoid is factorial if and only if it is atomic, and every atom is a prime. If H is atomic and

$p \in H$ is a prime, then every $a \in \mathsf{q}(H)$ has a representation $a = p^n bc^{-1}$, where $b, c \in H$, $p \nmid bc$ and $n \in \mathbb{Z}$. The exponent n is uniquely determined by the classes $aH^\times$ and $pH^\times$ in $H_{\red}$, and we call $n = \mathsf{v}_p(a)$ the *p-adic value* of a. The map $\mathsf{v}_p \colon \mathsf{q}(H) \to \mathbb{Z}$ is a surjective group homomorphism, called the *p-adic valuation*.

For an integral domain R, we denote by $R^\bullet = R \setminus \{0\}$ its multiplicative monoid. Then $(R^\bullet)_{\red}$ is isomorphic to the monoid of non-zero principal ideals of R.

Free monoids and coproducts. For a set P, we denote by $\mathcal{F}(P)$ the free abelian monoid with basis P. Then $\mathcal{F}(P)$ is a reduced factorial monoid and P is the set of primes of $\mathcal{F}(P)$. Every subset X of $\mathcal{F}(P)$ has a unique greatest common divisor, denoted by $\gcd(X) \in \mathcal{F}(P)$. Every $a \in \mathcal{F}(P)$ has a unique representation in the form

$$a = \prod_{p \in P} p^{\nu_p}, \quad \text{where } \nu_p \in \mathbb{N}_0 \text{ and } \nu_p = 0 \text{ for all but finitely many } p \in P,$$

and then $\nu_p = \mathsf{v}_p(a)$ for all $p \in P$. For $a, b \in \mathcal{F}(P)$, we set

$$|a| = \sum_{p \in P} \mathsf{v}_p(a), \quad \mathsf{d}(a,b) = \max\left\{ \left| \frac{a}{\gcd(a,b)} \right|, \left| \frac{b}{\gcd(a,b)} \right| \right\}.$$

We call $|a|$ the *size* of a and $\mathsf{d}(a,b)$ the *distance* between a and b. Note that $|\cdot| \colon \mathcal{F}(P) \to \mathbb{N}_0$ is a homomorphism, and $\mathsf{d} \colon \mathcal{F}(P) \times \mathcal{F}(P) \to \mathbb{N}_0$ is a metric.

For $s \in \mathbb{N}$, the additive monoid $\mathbb{N}_0^s$ is free abelian with the canonical basis consisting of the unit vectors. For $\mathbf{m} = (m_1, \ldots, m_s), \mathbf{n} = (n_1, \ldots, n_s) \in \mathbb{N}_0^s$ we define $\mathbf{m} \le \mathbf{n}$ if $m_i \le n_i$ for all $i \in [1, s]$, and, conforming with the above definition, $|\mathbf{n}| = n_1 + \ldots + n_s$. Note that $\mathbf{m} \le \mathbf{n}$ if and only if $\mathbf{m} \,|\, \mathbf{n}$.

For a family of reduced monoids $(D_p)_{p \in P}$, we define the *coproduct* by

$$D = \coprod_{p \in P} D_p = \Big\{ (a_p)_{p \in P} \in \prod_{p \in P} D_p \;\Big|\; a_p = 1 \text{ for all but finitely many } p \in P \Big\}.$$

We view the components D_p as submonoids of D. Consequently, every $a \in D$ has a unique representation in the form

$$a = \prod_{p \in P} a_p, \quad \text{where } a_p \in D_p \text{ for all } p \in P, \text{ and } a_p = 1 \text{ for all but finitely many } p \in P.$$

If all D_p are equal, say $D_p = D_0$ for all $p \in P$, we set $D = D_0^{(P)}$. In particular, $\mathbb{N}_0^{(P)}$ is free abelian with the unit vectors as a basis. We shall henceforth identify this monoid with $\mathcal{F}(P)$. As usual, we set

$$\coprod_{i=1}^{n} H_i = H_1 \times \ldots \times H_n.$$

If $H_1, \ldots, H_n$ are submonoids of a monoid H, then $H = H_1 \times \ldots \times H_n$ if and only if every $a \in H$ has a unique representation $a = a_1 \cdot \ldots \cdot a_n$, where $a_i \in H_i$ for all $i \in [1, n]$.

A monoid H is factorial if and only if $H = H^\times \times \mathcal{F}(P)$ for some set P. More precisely, if H is factorial and P is any maximal set of pairwise non-associated prime elements of H, then $H = H^\times \times \mathcal{F}(P)$.

Divisor homomorphisms and Krull monoids. Semigroup and monoid homomorphisms are always assumed to respect the unit element. A monoid homomorphism $\varphi\colon H \to D$ is called

- a *divisor homomorphism* if, for all $u, v \in H$, $\varphi(u) \,|\, \varphi(v)$ implies $u \,|\, v$;
- *cofinal* if for every $a \in D$ there exists some $u \in H$ such that $a \,|\, \varphi(u)$.

A submonoid $H \subset D$ is called

- *cofinal* if the inclusion map $H \hookrightarrow D$ is cofinal;
- *saturated* if the inclusion map $H \hookrightarrow D$ is a divisor homomorphism (equivalently, $H = D \cap \mathsf{q}(H)$);
- *divisor-closed* if for all $a \in D$ and $b \in H$, $a \,|\, b$ implies $a \in H$.

For any subset $E \subset H$, we denote by $[\![E]\!]$ the smallest divisor-closed submonoid of H containing E. Explicitly, $[\![E]\!]$ consists of all $x \in H$ such that $x \,|\, u$ for some $u \in [E]$.

Every monoid homomorphism $\varphi\colon H \to D$ extends uniquely to a homomorphism of the quotient groups, denoted by $\mathsf{q}(\varphi)\colon \mathsf{q}(H) \to \mathsf{q}(D)$. Its cokernel $\mathcal{C}(\varphi) = \mathsf{q}(D)/\operatorname{Im}\mathsf{q}(\varphi)$ is called the *class group* of φ. We write $\mathcal{C}(\varphi)$ additively, and for $a \in \mathsf{q}(D)$, we denote by $[a]_\varphi \in \mathcal{C}(\varphi)$ the class of a. If $a, b \in D$, then $[a]_\varphi = [b]_\varphi$ if and only if there exist elements $u, v \in H$ such that $a\varphi(u) = b\varphi(v)$. If φ is a divisor homomorphism, then $\varphi(H) = \{a \in D \mid [a]_\varphi = [1]_\varphi\}$. If φ is cofinal, then $\mathcal{C}(\varphi) = \{[a]_\varphi \mid a \in D\}$.

If $H \subset D$ is a submonoid and $\varphi = (H \hookrightarrow D)$, then we define $D/H = \mathcal{C}(\varphi) = \mathsf{q}(D)/\mathsf{q}(H)$, and for $a \in D$ we set $[a]_{D/H} = [a]_\varphi$. We shall mainly apply this notion if $H \subset D$ is saturated. In this case, $\mathsf{q}(H) \cap D = H$, and if $|D/H| = \beta \in \mathbb{N}$, then $a^\beta \in H$ for all $a \in D$.

A monoid homomorphism $\varphi\colon H \to D$ is called a *divisor theory* if D is a free abelian monoid, and for every $a \in D$ there exists a finite subset $X \subset H$ such that $a = \gcd(\varphi(X))$. If $\varphi\colon H \to D$ and $\varphi'\colon H \to D'$ are divisor theories, then there exists a unique isomorphism $\Phi\colon D \to D'$ such that $\Phi \circ \varphi = \varphi'$. A monoid H is called a *Krull monoid* if there exists a divisor theory $\varphi\colon H \to D$. Its class group $\mathcal{C}(\varphi)$ is (up to canonical isomorphism) uniquely determined by H, and we call $\mathcal{C}(H) = \mathcal{C}(\varphi)$ the *class group* of H.

The most important case arises when $H = R^\bullet$ for some Dedekind domain R. If $\mathcal{I}(R)$ denotes the set of all non-zero ideals of R, then the map $\partial\colon R^\bullet \to \mathcal{I}(R)$ defined by $\partial(a) = aR$ is a divisor theory. Let $\mathcal{C}(R)$ denote

the ideal class group of R, and for $\mathfrak{a} \in \mathcal{I}(R)$ let $[\mathfrak{a}] \in \mathcal{I}(R)$ denote the ideal class of $\mathfrak{a}$. Then the assignment $[\mathfrak{a}]_\varphi \mapsto [\mathfrak{a}]$ defines an isomorphism $\mathcal{C}(R^\bullet) = \mathcal{C}(\partial) \xrightarrow{\sim} \mathcal{C}(R)$, and we shall henceforth not distinguish between these groups.

Next we review and supplement some divisor-theoretic results from [15]. Let $(D_p)_{p\in P}$ be a family of reduced monoids and

$$\varphi = (\varphi_p)_{p\in P} \colon H \to D = \coprod_{p\in P} D_p$$

a divisor homomorphism. φ is said to have the *approximation property* if for any distinct $p_1, \dots, p_n \in P$ and elements $a_i \in D_{p_i}$ there exists some $u \in H$ such that $\varphi_{p_i}(u) = a_i$ for all $i \in [1, n]$.

Assume now that φ has the approximation property. Then φ is cofinal, and for every finite subset $E \subset P$ and every class $g \in \mathcal{C}(\varphi)$, there exists some $a \in D$ such that $a_p = 1$ for all $p \in E$ and $g = [a]_\varphi$. Moreover, if $D_p \cong \mathbb{N}_0$ for all $p \in P$, then φ is a divisor theory, hence H is a Krull monoid and $\mathcal{C}(H) = \mathcal{C}(\varphi)$. We shall use the following more precise result.

PROPOSITION 2.1. *Let $(D_p)_{p\in P}$ be a family of reduced monoids and*

$$\varphi = (\varphi_p)_{p\in P} \colon H \to D = \coprod_{p\in P} D_p$$

a divisor homomorphism having the approximation property. Let $E \subset P$ be a finite subset, and set

$$D^{(E)} = \coprod_{p\in P\setminus E} D_p, \quad H^{(E)} = \varphi^{-1}(D^{(E)}), \quad \varphi^{(E)} = \varphi | H^{(E)} \colon H^{(E)} \to D^{(E)}.$$

(1) *$\varphi^{(E)}$ is a divisor homomorphism having the approximation property, and there exists an isomorphism $\Phi \colon \mathcal{C}(\varphi^{(E)}) \xrightarrow{\sim} \mathcal{C}(\varphi)$ satisfying*

$$\Phi([a]_{\varphi^{(E)}}) = [a]_\varphi \quad \text{for all } a \in D^{(E)}.$$

(2) *If $D_p \cong \mathbb{N}_0$ for all $p \in P \setminus E$, then $H^{(E)}$ is a Krull monoid, and $\varphi^{(E)}$ is a divisor theory having the approximation property. In particular, $\mathcal{C}(\varphi) \cong \mathcal{C}(H^{(E)})$.*

Proof. (1) It is easily checked that $\varphi^{(E)}$ is a divisor homomorphism.

Suppose now that $p_1, \dots, p_n \in P \setminus E$ are distinct, and let $a_i \in D_{p_i}$ be given. Since φ has the approximation property, there exists some $u \in H$ such that $\varphi_{p_i}(u) = 1$ for all $i \in [1, n]$ and $\varphi_p(u) = 1$ for all $p \in E$, whence $u \in H^{(E)}$. Since $\varphi^{(E)} = \varphi | H^{(E)}$, it follows that $\varphi^{(E)}$ has the approximation property, and hence it is cofinal. Thus we obtain $\mathcal{C}(\varphi^{(E)}) = \{[a]_{\varphi^{(E)}} \mid a \in D^{(E)}\}$. If $a, b \in D^{(E)}$, then $[a]_{\varphi^{(E)}} = [b]_{\varphi^{(E)}}$ implies $[a]_\varphi = [b]_\varphi$. Therefore there exists a homomorphism $\Phi \colon \mathcal{C}(\varphi^{(E)}) \to \mathcal{C}(\varphi)$ satisfying $\Phi([a]_{\varphi^{(E)}}) = [a]_\varphi$

for all $a \in D^{(E)}$. Since φ has the approximation property, Φ is surjective. If $a \in D^{(E)}$ and $[a]_{\varphi^{(E)}} \in \mathrm{Ker}(\Phi)$, then $[a]_\varphi = 0$ implies $a \in \varphi(H) \cap D^{(E)} = \varphi^{(E)}(H^{(E)})$ and therefore $[a]_{\varphi^{(E)}} = 0$. Consequently, Φ is an isomorphism.

(2) Obvious by (1) and the remarks preceding this proposition. ∎

Factorizations and sets of lengths. Let H be a monoid. The monoid $\mathsf{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\mathrm{red}}))$ is called the *factorization monoid* of H. The unique homomorphism $\pi\colon \mathsf{Z}(H) \to H_{\mathrm{red}}$ satisfying $\pi|\mathcal{A}(H_{\mathrm{red}}) = \mathrm{id}$ is called the *factorization homomorphism* of H. It is surjective if and only if H is atomic, and it is an isomorphism if and only if H is factorial. For $a \in H$, the elements in $\mathsf{Z}(a) = \pi^{-1}(aH^\times) \subset \mathsf{Z}(H)$ are called the *factorizations* of a, and $\mathsf{L}(a) = \{|z| \mid z \in \mathsf{Z}(a)\} \subset \mathbb{N}_0$ is called the *set of lengths* of a. If $m \in \mathsf{L}(a)$ and $d \in \mathbb{N}$ is such that $[m, m+d] \cap \mathsf{L}(a) = \{m, m+d\}$, then d is called a *distance* of a, and we denote by $\Delta(a)$ the set of all distances of a. Among the best investigated invariants of non-unique factorizations are the system of sets of lengths and the set of distances of a monoid H, defined by

$$\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}, \quad \Delta(H) = \bigcup_{a \in H} \Delta(a).$$

H is called a *BF-monoid* (a monoid with bounded factorizations), if all sets $L \in \mathcal{L}(H)$ are finite.

For a finite subset $A \subset \mathbb{Z}$ the *pattern ideal* $\Phi(A) \subset H$ is the set of all $a \in H$ such that $y + A \subset \mathsf{L}(a)$ for some $y \in \mathbb{Z}$. It is an s-ideal of H.

A finite set $L \subset \mathbb{Z}$ is called an *almost arithmetical multiprogression with bound* $M \in \mathbb{N}$ if there exists some $d \in [1, M]$ and some subset $D \subset [0, d]$ with $\{0, d\} \subset D$ such that $L = L' \cup L^* \cup L''$, where

$$L' \subset \min L^* + [-M, -1], \quad L'' \subset \max L^* + [1, M],$$
$$L^* = [\min L^*, \max L^*] \cap (\min L^* + D + d\mathbb{Z}).$$

We say that the *Structure Theorem for Sets of Lengths* holds for a monoid H if H is a BF-monoid and there exists some $M \in \mathbb{N}$ such that every $L \in \mathcal{L}(H)$ is an almost arithmetical multiprogression with bound M.

The main result of this paper asserts that the Structure Theorem for Sets of Lengths holds for AC-monoids and hence for congruence monoids in Dedekind domains satisfying some natural finiteness conditions. The proof will be done by verifying the assumptions in the following abstract result, which is proved in [14, Proposition 4.8] (see also in [16, Theorem 3.4 and Remark 3.5]), and whose assumptions will be explained below.

THEOREM 2.2. *Let H be a BF-monoid such that $\Delta(H)$ is finite and all pattern ideals in H are tamely generated. Then the Structure Theorem for Sets of Lengths holds for H.*

A homomorphism $\beta\colon H \to D$ of reduced monoids is called a *transfer homomorphism* if β is surjective, $\beta^{-1}(1) = \{1\}$, and for all $u \in H$ and $y, z \in D$, the following condition is satisfied: If $\beta(u) = yz$, then there exist $v, w \in H$ such that $u = vw$, $\beta(v) = y$ and $\beta(w) = z$.

If $\beta\colon H \to D$ is a transfer homomorphism, then the Structure Theorem for Sets of Lengths holds for H if and only if it holds for D (see [24, Lemma 5.4]).

We continue with an explanation of the notions used in the formulation of Theorem 2.2.

The catenary degree. Let H be an atomic monoid. For $a \in H$, we denote by $\mathsf{c}(a)$ the minimal $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property: For any two factorizations $z, z' \in \mathsf{Z}(a)$, there exists a finite sequence $(z_0, z_1, \ldots, z_k)$ in $\mathsf{Z}(a)$ such that $z_0 = z$, $z_k = z'$ and $\mathsf{d}(z_{i-1}, z_i) \le N$ for all $i \in [1, k]$. Then $\mathsf{c}(a) \le \sup \mathsf{L}(a)$, and we call

$$\mathsf{c}(H) = \sup\{\mathsf{c}(a) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}$$

the *catenary degree of* H. If $a \in H$, then $\max \Delta(a) \le \max\{0, \mathsf{c}(H) - 2\}$. Consequently, if $\mathsf{c}(H) < \infty$, then $\Delta(H)$ is finite.

Tameness. Let H be an atomic monoid. For $a \in H$ and $x \in \mathsf{Z}(H)$, we denote by $\mathsf{t}(a, x)$ the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property: If $\mathsf{Z}(a) \cap x\mathsf{Z}(H) \ne \emptyset$ and $z \in \mathsf{Z}(a)$, then there exists some $z' \in \mathsf{Z}(a) \cap x\mathsf{Z}(H)$ such that $\mathsf{d}(z, z') \le N$ (note that, if $c \in H$ and $x \in \mathsf{Z}(c)$, then the condition $\mathsf{Z}(a) \cap x\mathsf{Z}(H) \ne \emptyset$ is equivalent to $c \mid a$). For subsets $H' \subset H$ and $X \subset \mathsf{Z}(H)$, we define

$$\mathsf{t}(H', X) = \sup\{\mathsf{t}(a, x) \mid a \in H',\, x \in X\} \in \mathbb{N}_0 \cup \{\infty\}.$$

For $a \in H$ and $x \in \mathsf{Z}(H)$, we set $\mathsf{t}(a, X) = \mathsf{t}(\{a\}, X)$ and $\mathsf{t}(H', x) = \mathsf{t}(H', \{x\})$. We shall write t_H instead of t if it is necessary to refer to H.

H is called *locally tame* if $\mathsf{t}(H, u) < \infty$ for all $u \in \mathcal{A}(H_{\mathrm{red}})$.

Let $\mathfrak{a} \subset H$ be an s-ideal. A subset $E \subset \mathfrak{a}$ is called a *tame generating set* of $\mathfrak{a}$ if there exists some $\gamma \in \mathbb{N}$ such that, for every $a \in \mathfrak{a}$, there is some $e \in E$ satisfying $e \mid a$, $\sup \mathsf{L}(e) \le \gamma$ and $\mathsf{t}(a, \mathsf{Z}(e)) \le \gamma$. If $\mathfrak{a}$ has a tame generating set, then $\mathfrak{a}$ is called *tamely generated*. Our notion of a tame generating set is stronger than that used in [14], but it is consistent with that of [16]. For a detailed discussion we refer the reader to [16, Remark 3.5].

Finitary monoids and complete s-ideals. Let H be a monoid. A subset $U \subset H \setminus H^\times$ is called an *almost generating set* of H if there exists some $n \in \mathbb{N}$ such that $(H \setminus H^\times)^n \subset UH$. An s-ideal $\mathfrak{a} \subset H$ is called *complete* over U if there exists some $n \in \mathbb{N}$ such that

$$[\![u]\!]^{-1}\mathfrak{a} \cap H \subset u^{-n}\mathfrak{a} \quad \text{for all } u \in U.$$

The monoid H is called *finitary* if it is a BF-monoid and has a finite almost generating set. Finitary monoids are investigated in [17], and the theory of complete and tamely generated ideals is developed in [16]. We recall some notions of this theory which will be used in Section 5.

Let H be a finitary monoid and $U \subset H \setminus H^\times$ a finite almost generating set. For $u \in U$, we denote by H_u the set of all $a \in H$ without a divisor in $[\![u]\!] \setminus H^\times$. For an s-ideal $\mathfrak{a} \subset H$, we denote by $\mathfrak{a}(U,u)$ the set of all $a \in \mathfrak{a} \cap u^2H$ such that $[\![u]\!]$ is maximal in the set $\{[\![v]\!] \mid v \in U,\ a \in v^2H\}$, and we set

$$\mathfrak{a}[U,u] = H_u \cap (u[\![u]\!])^{-1}\mathfrak{a}(U,u).$$

By definition, we have $\mathfrak{a}(U,u) \subset H(U,u)$ and $\mathfrak{a}[U,u] \subset H[U,u]$. The s-ideal $\mathfrak{a}$ is called *U-generated* if

$$\mathfrak{a} = \Big(\bigcup_{u \in U} u[\![u]\!]\, \mathfrak{a}[U,u]\Big) \cup (\mathfrak{a} \setminus U^{[2]}H).$$

An almost generating set U is called *full* if there exists some $m \in \mathbb{N}$ such that $H[U,u] \subset H \setminus U^{[m]}H$ for all $u \in U$. If U is full, then there exists some $M \in \mathbb{N}$ such that $\max \mathsf{L}(a) \le M$ whenever $a \in H[U,u]$ for some $u \in U$.

Restriction to reduced monoids. All factorization properties explained hitherto apply for a monoid H if and only if they apply for the associated reduced monoid H_{red}. Hence we may without restriction assume that H is reduced, and we will do this whenever it is convenient.

3. Congruence monoids in Dedekind domains. We start with some preliminaries concerning congruences which regard signatures.

Definition 3.1. Let R be an integral domain and $m \in \mathbb{N}_0$.

(1) A map

$$\sigma = (\sigma_1, \dots, \sigma_m)\colon R^\bullet \to \{\pm 1\}^m$$

is called a *sign vector* of R if there exist distinct ring monomorphisms $w_1, \dots, w_m\colon R \to \mathbb{R}$ such that $\sigma_j(a) = \operatorname{sign}\{w_j(a)\}$ for all $a \in R^\bullet$ and all $j \in [1,m]$. We call $m = |\sigma|$ the *dimension* of σ. For $m = 0$, the empty sequence will also be considered as a sign vector.

(2) Let $\{0\} \ne \mathfrak{f} \lhd R$ be an ideal and $\sigma = (\sigma_1, \dots, \sigma_m)$ a sign vector of R. Two elements $a, b \in R^\bullet$ are called *congruent modulo* $\mathfrak{f}\sigma$, in symbols $a \equiv b \bmod \mathfrak{f}\sigma$, if $a \equiv b \bmod \mathfrak{f}$ and $\sigma(a) = \sigma(b)$. Obviously, congruence modulo $\mathfrak{f}\sigma$ is a congruence relation on the monoid $R^\bullet$. We denote by $R/\mathfrak{f}\sigma$ the semigroup of congruence classes, and for $a \in R^\bullet$, we denote by $[a]_{\mathfrak{f}\sigma} \in R/\mathfrak{f}\sigma$ the congruence class containing a. For $m = 0$, the congruence modulo $\mathfrak{f}\sigma$ is just the ordinary congruence modulo $\mathfrak{f}$, and we write $\mathfrak{f}$ instead of $\mathfrak{f}\sigma$.

(3) Let $\{0\} \neq \mathfrak{f} \lhd R$ be an ideal of R, let σ be a sign vector of R and $\emptyset \neq \Gamma \subset R/\mathfrak{f}\sigma$ a multiplicatively closed subset (not necessarily containing the unit element $[1]_{\mathfrak{f}\sigma}$). Then the (multiplicative) monoid

$$H = H_\Gamma = \{a \in R^\bullet \mid [a]_{\mathfrak{f}\sigma} \in \Gamma\} \cup \{1\} \subset R^\bullet$$

is called the *congruence monoid defined in R modulo $\mathfrak{f}\sigma$ by Γ*. It is called

- *regular modulo* $\mathfrak{f}$ if $aR + \mathfrak{f} = R$ for all $a \in H$;
- *singular modulo* $\mathfrak{f}$ if $aR + \mathfrak{f} \neq R$ for all $a \in H \setminus \{1\}$.

(4) A submonoid $H \subset R^\bullet$ is called a *congruence monoid in R* if there exists an ideal $\mathfrak{f} \neq \{0\}$ of R, a sign vector σ of R and a multiplicatively closed subset $\emptyset \neq \Gamma \subset R/\mathfrak{f}\sigma$ such that H is the congruence monoid defined in R modulo $\mathfrak{f}\sigma$ by Γ. Every such ideal $\mathfrak{f}$ is called an *ideal of definition for H*.

We summarize the properties of congruences regarding signatures in the following

LEMMA 3.2. *Let R be an integral domain, $\{0\} \neq \mathfrak{f} \lhd R$ an ideal and $\sigma = (\sigma_1, \ldots, \sigma_m)$ a sign vector of R.*

(1) *Let $\emptyset \neq \Gamma \subset R/\mathfrak{f}\sigma$ be a multiplicatively closed subset, $\{0\} \neq \mathfrak{f}' \subset \mathfrak{f}$ another ideal of R, $m' \in \mathbb{N}$ and $\sigma' = (\sigma'_1, \ldots, \sigma'_{m'})$ a sign vector of R such that $\{\sigma_1, \ldots, \sigma_m\} \subset \{\sigma'_1, \ldots, \sigma'_{m'}\}$. Then there is a unique monoid homomorphism $\psi\colon R/\mathfrak{f}'\sigma' \to R/\mathfrak{f}\sigma$ satisfying*

$$\psi([a]_{\mathfrak{f}'\sigma'}) = [a]_{\mathfrak{f}\sigma}.$$

ψ is surjective, and if $\Gamma' = \psi^{-1}(\Gamma) \subset R/\mathfrak{f}'\sigma'$, then $H_\Gamma = H_{\Gamma'}$.

(2) *Suppose that $a \in R^\bullet$. For every $e \in \{\pm 1\}^{|\sigma|}$ there exists an element $a_e \in R^\bullet$ such that $\sigma(a_e) = e$ and $a_e \equiv a \bmod \mathfrak{f}$. If the elements a_e are chosen in this way, then*

$$a + \mathfrak{f} = \biguplus_{e \in \{\pm 1\}^{|\sigma|}} [a_e]_{\mathfrak{f}\sigma}.$$

(3) *$(R/\mathfrak{f}\sigma)^\times = \{[a]_{\mathfrak{f}\sigma} \mid a \in R^\bullet, a + \mathfrak{f} \in (R/\mathfrak{f})^\times\}$, and there is an exact sequence*

$$1 \to \{\pm 1\}^{|\sigma|} \xrightarrow{\nu} (R/\mathfrak{f}\sigma)^\times \xrightarrow{\theta} (R/\mathfrak{f})^\times \to 1,$$

where $\theta([a]_{\mathfrak{f}\sigma}) = a + \mathfrak{f}$, and $\nu(e) = [a]_{\mathfrak{f}\sigma}$ if $a \equiv 1 \bmod \mathfrak{f}$ and $\sigma(a) = e$.

(4) *Let $\emptyset \neq \Gamma \subset R/\mathfrak{f}\sigma$ be a multiplicatively closed subset. Then H_Γ is regular modulo $\mathfrak{f}$ if and only if $\Gamma \subset (R/\mathfrak{f}\sigma)^\times$, and H_Γ is singular modulo $\mathfrak{f}$ if and only if $\Gamma \cap (R/\mathfrak{f}\sigma)^\times = \emptyset$.*

Proof. (1) Observe that, for all $a, b \in R^\bullet$, $[a]_{\mathfrak{f}'\sigma'} = [b]_{\mathfrak{f}'\sigma'}$ implies $[a]_{\mathfrak{f}\sigma} = [b]_{\mathfrak{f}\sigma}$.

(2) and (3) are proved in [21, Hilfssatz 2, Satz 6 and Satz 7], and (4) is a simple consequence of (3). ∎

EXAMPLES 3.3. (1) Let R be an integral domain and $A \subset R$ an order in R (that means, $A \subset R$ is a subring and R/A is a finitely generated torsion A-module). Then $\mathfrak{f} = \{a \in R \mid aR \subset A\} \neq \{0\}$, $\mathfrak{f}$ is the largest ideal of R lying in A, and $A/\mathfrak{f} \subset R/\mathfrak{f}$ is a subring (hence multiplicatively closed). The multiplicative monoid

$$A^\bullet = \{a \in R^\bullet \mid a + \mathfrak{f} \in A/\mathfrak{f}\}$$

of A is the congruence monoid defined in R modulo $\mathfrak{f}$ by $A/\mathfrak{f}$. It is neither regular nor singular modulo $\mathfrak{f}$.

(2) Suppose that $f \in \mathbb{N}$, and let $\Lambda \subset \mathbb{Z}/f\mathbb{Z}$ be a multiplicatively closed subset. Then the *Hilbert semigroup defined modulo f by Λ* is the monoid

$$H_f(\Lambda) = \{a \in \mathbb{N} \mid a + f\mathbb{Z} \in \Lambda\} \cup \{1\}.$$

All examples of congruence monoids mentioned in the introduction are of this type. In order to view them as congruence monoids according to our definition, let $\sigma = \text{sign}\colon \mathbb{Z}^\bullet \to \{\pm 1\}$ be the ordinary sign function, and set

$$\Lambda^+ = \{[a]_{f\mathbb{Z}\sigma} \in \mathbb{Z}/f\mathbb{Z}\sigma \mid a \in \mathbb{N},\ a + f\mathbb{Z} \in \Lambda\}.$$

Then $\Lambda^+ \subset \mathbb{Z}/f\mathbb{Z}\sigma$ is a multiplicatively closed subset, and $H_f(\Lambda)$ is the congruence monoid defined in $\mathbb{Z}$ modulo $f\mathbb{Z}\sigma$ by Λ^+. Hilbert semigroups modulo f may by regular (as $1 + 4\mathbb{N}_0$), singular (as $\{1\} \cup 2\mathbb{N}$) or neither of them (as $\{a \in \mathbb{N} \mid a \not\equiv -1 \bmod 3\}$).

(3) Let R be the ring of integers of an algebraic number field K, $m \in \mathbb{N}_0$, and let $w_1, \dots, w_m\colon K \to \mathbb{R}$ be the real embeddings of K. Define $\sigma = (\sigma_1, \dots, \sigma_m)\colon R^\bullet \to \{\pm 1\}^m$ by $\sigma_j(a) = \text{sign}(w_j(a))$ for all $j \in [1, m]$. For an ideal $\{0\} \neq \mathfrak{f} \lhd R$, the principal ray modulo $\mathfrak{f}$ in R is defined by

$$S_\mathfrak{f} = \{a \in R^\bullet \mid a \equiv 1 \bmod \mathfrak{f},\ w_j(a) > 0 \text{ for all } j \in [1, m]\}.$$

According to our definition, $S_\mathfrak{f}$ is the congruence monoid defined in R modulo $\mathfrak{f}\sigma$ by $\{[1]_{\mathfrak{f}\sigma}\}$. It is regular modulo $\mathfrak{f}$.

PROPOSITION 3.4. *Let R be an integral domain and $H \subset R^\bullet$ a congruence monoid in R.*

(1) *Let $\{0\} \neq \mathfrak{f}' \subset \mathfrak{f} \subset R$ be ideals of R. If $\mathfrak{f}$ is an ideal of definition for H, then so is $\mathfrak{f}'$.*

(2) *If $\mathfrak{f}_1$ and $\mathfrak{f}_2$ are ideals of definition for H, then so is $\mathfrak{f}_1 + \mathfrak{f}_2$. In particular, if R is noetherian, then H has a largest ideal of definition.*

Proof. (1) Let σ be a sign vector of R and $\emptyset \neq \Gamma \subset R/\mathfrak{f}\sigma$ a multiplicatively closed subset such that $H = H_\Gamma$. If $\psi\colon R/\mathfrak{f}'\sigma \to R/\mathfrak{f}\sigma$ is the homomorphism defined in Lemma 3.2(1) and $\Gamma' = \psi^{-1}(\Gamma)$, then $H_{\Gamma'} = H_\Gamma$, and thus $\mathfrak{f}'$ is an ideal of definition for H.

(2) For $i \in \{1, 2\}$, let $\sigma^{(i)} = (\sigma_1^{(i)}, \dots, \sigma_{m_i}^{(i)})$ be a sign vector of R and $\emptyset \neq \Gamma_i' \subset R/\mathfrak{f}_i\sigma^{(i)}$ a multiplicatively closed subset such that $H = H_{\Gamma_i'}$.

Let $\sigma = (\sigma_1, \dots, \sigma_m)$ be a sign vector of R such that $\{\sigma_1, \dots, \sigma_m\} = \{\sigma_1^{(1)}, \dots, \sigma_{m_1}^{(1)}, \sigma_1^{(2)}, \dots, \sigma_{m_2}^{(2)}\}$. If $\psi_i\colon R/\mathfrak{f}_i\sigma \to R/\mathfrak{f}_i\sigma^{(i)}$ is the homomorphism defined in Lemma 3.2(1) and $\Gamma_i = \psi_i^{-1}(\Gamma_i')$, then $H = H_{\Gamma_1} = H_{\Gamma_2}$.

We set $\mathfrak{f} = \mathfrak{f}_1 + \mathfrak{f}_2$ and $\Gamma = \{[a]_{\mathfrak{f}\sigma} \mid a \in H \setminus \{1\}\} \subset R/\mathfrak{f}\sigma$. Then $\Gamma \ne \emptyset$ is a multiplicatively closed subset of $R/\mathfrak{f}\sigma$, $H \subset H_\Gamma$, and we assert that equality holds. If $b \in H_\Gamma \setminus \{1\}$, then there exists some $a \in H \setminus \{1\}$ such that $[b]_{\mathfrak{f}\sigma} = [a]_{\mathfrak{f}\sigma}$, that is, $b \equiv a \bmod \mathfrak{f}$ and $\sigma(b) = \sigma(a)$. Hence there exist elements $x_1 \in \mathfrak{f}_1$ and $x_2 \in \mathfrak{f}_2$ such that $b = a + x_1 + x_2$, and there exists some $c \in R^\bullet \setminus \{1\}$ such that $c \equiv a + x_1 \bmod (\mathfrak{f}_1 \cap \mathfrak{f}_2)$ and $\sigma(c) = \sigma(a)$. We set $c = a + x_1 + x_0$, where $x_0 \in \mathfrak{f}_1 \cap \mathfrak{f}_2$. Now $[c]_{\mathfrak{f}_1\sigma} = [a]_{\mathfrak{f}_1\sigma}$ implies $c \in H$. Since $b = c + (x_2 - x_0) \equiv c \bmod \mathfrak{f}_2$ and $\sigma(b) = \sigma(c)$, we obtain $[b]_{\mathfrak{f}_2\sigma} = [c]_{\mathfrak{f}_2\sigma}$, and thus finally $b \in H$. ∎

Our next result is the divisor-theoretic description of congruence monoids in Dedekind domains. We fix some notations and conventions.

Assumptions for congruence monoids in Dedekind domains. Let R be a Dedekind domain, $\{0\} \ne \mathfrak{f} \lhd R$, σ a sign vector of R, $\emptyset \ne \Gamma \subset R/\mathfrak{f}\sigma$ a multiplicatively closed subset and

$$H_\Gamma = \{a \in R^\bullet \mid [a]_{\mathfrak{f}\sigma} \in \Gamma\} \cup \{1\}$$

the congruence monoid defined in R modulo $\mathfrak{f}\sigma$ by Γ. We set $\mathcal{P} = \max(R)$, we denote by $\mathcal{I} = \mathcal{F}(\mathcal{P})$ the monoid of all non-zero ideals of R and, for $\mathfrak{p} \in \mathcal{P}$, by $\mathsf{v}_\mathfrak{p}$ the $\mathfrak{p}$-adic exponent. We set

$$\mathcal{P}_\mathfrak{f} = \{\mathfrak{p} \in \mathcal{P} \mid \mathfrak{p} + \mathfrak{f} = R\}, \quad T_\mathfrak{f} = R^\bullet \setminus \bigcup_{\mathfrak{p} \in \mathcal{P} \setminus \mathcal{P}_\mathfrak{f}} \mathfrak{p} = \{a \in R^\bullet \mid a + \mathfrak{f} \in (R/\mathfrak{f})^\times\},$$

we denote by $\mathcal{I}_\mathfrak{f} = \mathcal{F}(\mathcal{P}_\mathfrak{f}) \subset \mathcal{I}$ the monoid of all non-zero ideals of R which are coprime to $\mathfrak{f}$, and we consider the semilocal principal ideal domain $T_\mathfrak{f}^{-1}R$.

The embedding $R \hookrightarrow T_\mathfrak{f}^{-1}R$ induces an isomorphism

$$R/\mathfrak{f}\sigma \xrightarrow{\sim} T_\mathfrak{f}^{-1}R/T_\mathfrak{f}^{-1}\mathfrak{f}\sigma$$

by which we will identify these two semigroups. Then $[a]_{\mathfrak{f}\sigma} = [a]_{T_\mathfrak{f}^{-1}\mathfrak{f}\sigma}$ for all $a \in R^\bullet$. Let

$$H_{\Gamma,\mathfrak{f}} = \{z \in (T_\mathfrak{f}^{-1}R)^\bullet \mid [z]_{T_\mathfrak{f}^{-1}\mathfrak{f}\sigma} \in \Gamma\} \cup \{1\}$$

be the congruence monoid in the semilocal principal ideal domain $T_\mathfrak{f}^{-1}R$ defined modulo $T_\mathfrak{f}^{-1}\mathfrak{f}\sigma$ by Γ. Clearly, $H_\Gamma \subset H_{\Gamma,\mathfrak{f}}$. Now we define

$$\partial\colon H_\Gamma \to \mathcal{F}(\mathcal{P}_\mathfrak{f}) \times (H_{\Gamma,\mathfrak{f}})_{\mathrm{red}} \quad \text{by} \quad \partial(a) = \Big(\prod_{\mathfrak{p} \in \mathcal{P}_\mathfrak{f}} \mathfrak{p}^{\mathsf{v}_\mathfrak{p}(a)}, aH_{\Gamma,\mathfrak{f}}^\times\Big),$$

and we call ∂ the *canonical divisor homomorphism associated with* H_Γ (we shall prove in a moment that it is indeed a divisor homomorphism). We view ∂ as the family of its components

$$\partial = ((\partial_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{P}_{\mathfrak{f}}}, \partial_{\mathfrak{f}}), \quad \text{where} \quad \partial_{\mathfrak{p}}(a) = \mathfrak{p}^{\mathsf{v}_{\mathfrak{p}}(a)} \text{ for } \mathfrak{p} \in \mathcal{P}_{\mathfrak{f}} \text{ and } \partial_{\mathfrak{f}}(a) = aH_{\Gamma,\mathfrak{f}}^{\times}.$$

We define

$$H_{\Gamma}^{*} = \partial^{-1}\mathcal{F}(\mathcal{P}_{\mathfrak{f}}), \quad \partial^{*} = \partial | H_{\Gamma}^{*} \colon H_{\Gamma}^{*} \to \mathcal{F}(\mathcal{P}_{\mathfrak{f}}) = \mathcal{I}_{\mathfrak{f}}.$$

THEOREM 3.5. *Let R be a Dedekind domain, and let $H_{\Gamma} \subset R^{\bullet}$ be a congruence monoid as in the assumptions for congruence monoids in Dedekind domains.*

(1) $\partial \colon H_{\Gamma} \to \mathcal{F}(\mathcal{P}_{\mathfrak{f}}) \times (H_{\Gamma,\mathfrak{f}})_{\mathrm{red}}$ *is a divisor homomorphism.*

(2) *Suppose that $(R/\mathfrak{f}\sigma)^{\times} \cap \Gamma$ is a subgroup of $(R/\mathfrak{f}\sigma)^{\times}$. Then*:

(a) $H_{\Gamma,\mathfrak{f}} = (T_{\mathfrak{f}} \cap H_{\Gamma})^{-1} H_{\Gamma}$.

(b) *∂ has the approximation property.*

(c) *H_{Γ}^{*} is a Krull monoid, ∂^{*} is a divisor theory having the approximation property, and $\mathcal{C}(\partial) \cong \mathcal{C}(\partial^{*}) \cong \mathcal{C}(H_{\Gamma}^{*})$. Moreover,*

$$H_{\Gamma}^{*} = \{a \in H_{\Gamma} \mid aR + \mathfrak{f} = R\} = \{a \in R^{\bullet} \mid [a]_{\mathfrak{f}\sigma} \in (R/\mathfrak{f}\sigma)^{\times} \cap \Gamma\},$$

and there is a (canonical) exact sequence

$$1 \to (R/\mathfrak{f}\sigma)^{\times}/[R^{\times}]_{\mathfrak{f}\sigma}(\Gamma \cap (R/\mathfrak{f}\sigma)^{\times}) \to \mathcal{C}(H_{\Gamma}^{*}) \to \mathcal{C}(R) \to 0,$$

where $[R^{\times}]_{\mathfrak{f}\sigma} = \{[u]_{\mathfrak{f}\sigma} \mid u \in R^{\times}\}$, and $\mathcal{C}(R)$ denotes the ideal class group of R.

(3) *Let $\mathfrak{f}$ be the largest ideal of definition for H_{Γ} and suppose that $(R/\mathfrak{f}\sigma)^{\times} \cap \Gamma$ is a subgroup of $(R/\mathfrak{f}\sigma)^{\times}$. Then H_{Γ} is a Krull monoid if and only if H_{Γ} is regular modulo $\mathfrak{f}$.*

Proof. (1) If $a, b \in H_{\Gamma}$ and $\partial(a) \,|\, \partial(b)$, then $\mathsf{v}_{\mathfrak{p}}(a) \le \mathsf{v}_{\mathfrak{p}}(b)$ for all $\mathfrak{p} \in \mathcal{P}_{\mathfrak{f}}$ and $a^{-1}b \in H_{\Gamma,\mathfrak{f}} \subset T_{\mathfrak{f}}^{-1}R$. Hence also $\mathsf{v}_{\mathfrak{p}}(a) \le \mathsf{v}_{\mathfrak{p}}(b)$ for all $\mathfrak{p} \in \mathcal{P} \setminus \mathcal{P}_{\mathfrak{f}}$, and thus $c = a^{-1}b \in R$. If $c = 1$, there is nothing to do. If $c \ne 1$, then $[c]_{\mathfrak{f}\sigma} = [a^{-1}b]_{T^{-1}\mathfrak{f}\sigma} \in \Gamma$ implies $c \in H_{\Gamma}$ and thus $a \,|\, b$ (in H_{Γ}).

(2) If $(R/\mathfrak{f}\sigma)^{\times} \cap \Gamma$ is a subgroup of $(R/\mathfrak{f}\sigma)^{\times}$, then $[1]_{\mathfrak{f}\sigma} \in \Gamma$ and therefore $H_{\Gamma} = \{a \in R^{\bullet} \mid [a]_{\mathfrak{f}\sigma} \in \Gamma\}$.

(a) We show first that $T_{\mathfrak{f}} \cap H_{\Gamma} \subset H_{\Gamma,\mathfrak{f}}^{\times}$ (which implies that $H_{\Gamma,\mathfrak{f}} \supset (T_{\mathfrak{f}} \cap H_{\Gamma})^{-1} H_{\Gamma}$). If $s \in T_{\mathfrak{f}} \cap H_{\Gamma}$, then $[s]_{\mathfrak{f}\sigma} \in \Gamma \cap (R/\mathfrak{f}\sigma)^{\times}$, and since $\Gamma \cap (R/\mathfrak{f}\sigma)^{\times}$ is a group, we obtain $[s^{-1}]_{T^{-1}\mathfrak{f}\sigma} = [s]_{\mathfrak{f}\sigma}^{-1} \in \Gamma$. Hence $s^{-1} \in H_{\Gamma,\mathfrak{f}}$ and $s \in H_{\Gamma,\mathfrak{f}}^{\times}$.

For the reverse inclusion, suppose that $b = s^{-1}c \in H_{\Gamma,\mathfrak{f}}$, where $c \in R^{\bullet}$ and $s \in T_{\mathfrak{f}}$. By Lemma 3.2, there exists some $s' \in R^{\bullet}$ such that $ss' \equiv 1 \bmod \mathfrak{f}\sigma$ and therefore $[cs']_{\mathfrak{f}\sigma} = [(cs')(ss')^{-1}]_{T^{-1}\mathfrak{f}\sigma} \in \Gamma$. Since $cs' \in H_{\Gamma}$ and $ss' \in T_{\mathfrak{f}} \cap H_{\Gamma}$, we obtain $b \in (T_{\mathfrak{f}} \cap H_{\Gamma})^{-1} H_{\Gamma}$.

(b) Suppose that $n \in \mathbb{N}$, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathcal{P}_{\mathfrak{f}}$ be distinct, $e_1, \ldots, e_n \in \mathbb{N}_0$ and $b \in H_{\Gamma,\mathfrak{f}}$. We must prove that there exists some $a \in H_{\Gamma}$ such that $\mathsf{v}_{\mathfrak{p}_i}(a) = e_i$ for all $i \in [1, n]$, and $aH_{\Gamma,\mathfrak{f}}^{\times} = bH_{\Gamma,\mathfrak{f}}^{\times}$. By (a) there exists some $c \in H_{\Gamma}$ and $s \in T_{\mathfrak{f}} \cap H_{\Gamma}$ such that $b = s^{-1}c$. Let $q \in R^{\bullet}$ be such that $\mathsf{v}_{\mathfrak{q}}(q) =$

$\mathsf v_{\mathfrak q}(c)$ for all $\mathfrak q \in \mathcal P \setminus \mathcal P_{\mathfrak f}$ and $\mathsf v_{\mathfrak p_i}(q) = 0$ for all $i \in [1,n]$. Then $q^{-1}c \in (T_{\mathfrak f}^{-1}R)^\times$, and thus there exist elements $w, t \in T_{\mathfrak f}$ such that $q^{-1}c = w^{-1}t$. For $i \in [1,n]$, let $p_i \in \mathfrak p_i \setminus \mathfrak p_i^2$. By the Chinese Remainder Theorem and Lemma 3.2, there exists some $u \in R^\bullet$ satisfying

$$wu \equiv t \bmod \mathfrak f\sigma, \quad u \equiv p_i \bmod \mathfrak p_i^{e_i+1} \quad \text{for all } i \in [1,n].$$

Then $a = qu \in H$, $\mathsf v_{\mathfrak p_i}(a) = \mathsf v_{\mathfrak p_i}(u) = e_i$ for all $i \in [1,n]$, $[a]_{\mathfrak f\sigma} = [qw^{-1}t]_{T^{-1}\mathfrak f\sigma} = [c]_{\mathfrak f\sigma} \in \Gamma$ implies $a \in H_\Gamma$, and $b^{-1}a = sc^{-1}qu = swut^{-1} \equiv s \bmod T^{-1}\mathfrak f\sigma$ implies $ba^{-1} \in H_{\Gamma,\mathfrak f}^\times$.

(c) By definition, $H_\Gamma^* = \{a \in H_\Gamma \mid aR + \mathfrak f = R\} = \{a \in R^\bullet \mid [a]_{\mathfrak f\sigma} \in (R/\mathfrak f\sigma)^\times \cap \Gamma\}$. The remaining assertions except those concerning the exact sequence follow by Proposition 2.1.

We identify $\mathcal C(H_\Gamma^*)$ with $\mathcal C(\partial^*)$. For $\mathfrak a \in \mathcal I_{\mathfrak f}$, we denote by $[\mathfrak a] \in \mathcal C(R)$ the ideal class of $\mathfrak a$. Then $\mathcal C(R) = \{[\mathfrak a] \mid \mathfrak a \in \mathcal I_{\mathfrak f}\}$ and $\mathcal C(H_\Gamma^*) = \{[\mathfrak a]_{\partial^*} \mid \mathfrak a \in \mathcal I_{\mathfrak f}\}$. Since $[\mathfrak a]_{\partial^*} = [\mathfrak b]_{\partial^*}$ implies $[\mathfrak a] = [\mathfrak b]$ for all $\mathfrak a, \mathfrak b \in \mathcal I_{\mathfrak f}$, there is an epimorphism $\eta\colon \mathcal C(H_\Gamma^*) \to \mathcal C(R)$ satisfying $\eta([\mathfrak a]_{\partial^*}) = [\mathfrak a]$ for all $\mathfrak a \in \mathcal I_{\mathfrak f}$, and $\mathrm{Ker}(\eta) = \{[zR]_{\partial^*} \mid z \in T_{\mathfrak f}\}$. If $z, z' \in T_{\mathfrak f}$ and $z \equiv z' \bmod \mathfrak f\sigma$, then $[zR]_{\partial^*} = [z'R]_{\partial^*}$. Hence there exists an epimorphism $\theta\colon (R/\mathfrak f\sigma)^\times \to \mathrm{Ker}(\eta)$ satisfying $\theta([z]_{\mathfrak f\sigma}) = [zR]_{\partial^*}$ for all $z \in T_{\mathfrak f}$, and $\mathrm{Ker}(\theta)$ consists of all $[a]_{\mathfrak f\sigma} \in (R/\mathfrak f\sigma)^\times$ such that there exists some $\varepsilon \in R^\times$ satisfying $[\varepsilon a]_{\mathfrak f\sigma} \in \Gamma$. Hence $\mathrm{Ker}(\theta) = [R^\times]_{\mathfrak f\sigma}(\Gamma \cap (R/\mathfrak f\sigma)^\times)$.

(3) If H_Γ is regular modulo $\mathfrak f$, then $H_\Gamma = H_\Gamma^*$, and thus it is a Krull monoid by (2).

Suppose now that H_Γ is a Krull monoid, and set $\mathfrak f = \mathfrak p_1^{e_1} \cdot \ldots \cdot \mathfrak p_s^{e_s}$, where $s \in \mathbb N_0$, $\mathfrak p_1, \ldots, \mathfrak p_s \in \mathcal P$ are distinct and $e_1, \ldots, e_s \in \mathbb N$. We consider the decomposition $\mathfrak f = \mathfrak f_0\mathfrak f_1$, where

$$\mathfrak f_0 = \prod_{\substack{i=1 \\ \mathfrak p_i \cap H \ne \emptyset}}^{s} \mathfrak p_i^{e_i}, \quad \mathfrak f_1 = \prod_{\substack{i=1 \\ \mathfrak p_i \cap H = \emptyset}}^{s} \mathfrak p_i^{e_i}.$$

Then H_Γ is regular modulo $\mathfrak f$ if and only if $\mathfrak f_0 = R$. The set $\Gamma_1 = \{[a]_{\mathfrak f_1\sigma} \mid a \in H_\Gamma,\ a \ne 1\} \subset R/\mathfrak f_1\sigma$ is a non-empty multiplicatively closed subset, and $H_\Gamma \subset H_{\Gamma_1}$. We shall prove that $H_{\Gamma_1} \subset H_\Gamma$. Then equality holds, $\mathfrak f_1$ is an ideal of definition for H_Γ, and therefore $\mathfrak f_1 = \mathfrak f$, $\mathfrak f_0 = R$, and H is regular modulo $\mathfrak f$.

By the very definition of $\mathfrak f_0$, there exists an element $y \in \mathfrak f_0 \cap H_\Gamma$. If $x \in H_{\Gamma_1} \setminus \{1\}$, then there exists some $a \in H_\Gamma \setminus \{1\}$ such that $x \equiv a \bmod \mathfrak f_1\sigma$. For all $n \in \mathbb N$, this implies $x^n y \equiv a^n y \bmod \mathfrak f\sigma$, hence $x^n y \in H_\Gamma$, and the identity $(xy)^{n+1} = y^n(x^{n+1}y)$ implies $y^n \,|\, (xy)^{n+1}$ (in H_Γ). By [20, Lemma 2], we get $y \,|\, xy$ (in H_Γ), and thus $x \in H_\Gamma$. ∎

The following Theorem 3.6 is the main result of this paper. Its proof will be completed in Section 6.

THEOREM 3.6 (Main Theorem for congruence monoids in Dedekind domains). *Let R be a Dedekind domain, H a congruence monoid in R and $\mathfrak{f}$ an ideal of definition for H. If the residue class ring $R/\mathfrak{f}$ and the ideal class group $\mathcal{C}(R)$ are both finite, then H is locally tame, $\mathsf{c}(H) < \infty$, and the Structure Theorem for Sets of Lengths holds for H.*

4. Class semigroups. If $H \subset D$ is a submonoid, we defined the class group of D modulo H by $D/H = \mathsf{q}(D)/\mathsf{q}(H)$. This definition generalizes the usual notion of a class group in algebraic number theory. However, it does not describe the structure of H in D in a sufficiently precise way unless $H \subset D$ is saturated and cofinal. In the general case, we have to introduce the following more subtle construction.

DEFINITION 4.1. Let D be a monoid and $A \subset D$ a subset. Two elements $y, y' \in D$ are called *A-equivalent* (in D) if

$$y^{-1}A \cap D = y'^{-1}A \cap D.$$

It is easily checked that A-equivalence is a congruence relation on D. For $y \in D$, we denote by $[y]_A^D$ the *A-equivalence class of y*, and we define

$$\mathcal{C}(A, D) = \{[y]_A^D \mid y \in D\}, \quad \mathcal{C}^*(A, D) = \{[y]_A^D \mid y \in (D \setminus D^\times) \cup \{1\}\}.$$

The quotient law on $\mathcal{C}(A, D)$ is written additively, that is, $[xy]_A^D = [x]_A^D + [y]_A^D$ for all $x, y \in D$. Then $\mathcal{C}(A, D)$ is an (additive) semigroup, $\mathcal{C}^*(A, D) \subset \mathcal{C}(A, D)$ is a subsemigroup, and the assignment $y \mapsto [y]_A^D$ defines a surjective semigroup homomorphism $D \to \mathcal{C}(A, D)$.

If $T \subset D$ is any subset, then the map

$$\psi\colon \{[y]_A^D \mid y \in T\} \to \{y^{-1}A \cap D \mid y \in T\}, \quad [y]_A^D \mapsto y^{-1}A \cap D$$

is bijective by definition. Note that for all $y \in D$ we have either $[y]_A^D \cap A = \emptyset$ or $[y]_A^D \subset A$. Indeed, if $a \in [y]_A^D \cap A$ and $z \in [y]_A^D$, then $[a]_A^D = [z]_A^D$, hence $1 \in a^{-1}A \cap D = z^{-1}A \cap D$, and therefore $z \in A$.

Without giving details, we mention that there are examples of submonoids $H \subset D$ such that $D/H = \{0\}$ but $\mathcal{C}(H, D)$ is infinite. However, if $H \subset D$ is saturated and cofinal, and if $y, y' \in D$, then $[y]_{D/H} = [y']_{D/H}$ if and only if $[y]_H^D = [y']_H^D$, and thus $\mathcal{C}(H, D) \cong D/H$.

PROPOSITION 4.2. *Let D be a factorial monoid, and let $H \subset D$ be an atomic submonoid such that $H \cap D^\times = H^\times$ and $\mathcal{C}^*(H, D)$ is finite. Then $\mathcal{C}^*(\mathcal{A}(H), D)$ is also finite.*

Proof. We set $D^* = D \setminus D^\times$ and $H^* = H \setminus H^\times$. By assumption, the set $\{y^{-1}H \cap D \mid y \in D^*\}$ is finite, and we must prove that the set $\{y^{-1}\mathcal{A}(H) \cap D \mid y \in D^*\}$ is also finite.

If $y \in D^*$ and $a \in y^{-1}H \cap D$, then $ay = u \in H \setminus D^\times = H^*$. Hence $y^{-1}H \cap D = y^{-1}H^* \cap D$, and therefore the set $\{y^{-1}H^* \cap D \mid y \in D^*\}$ is also finite. Now we consider the partition $H^* = \mathcal{A}(H) \uplus H^*H^*$. If $y \in D$, then $y^{-1}H^* \cap D = (y^{-1}\mathcal{A}(H) \cap D) \uplus (y^{-1}H^*H^* \cap D)$. Hence it is sufficient to prove that the set $\{y^{-1}H^*H^* \cap D \mid y \in D^*\}$ is finite, and for this, we show that

$$y^{-1}H^*H^* \cap D = \bigcup_{\substack{y_1,y_2 \in D^* \cup \{1\} \\ y_1y_2 = y}} (y_1^{-1}H^* \cap D)(y_2^{-1}H^* \cap D).$$

If $a \in y^{-1}H^*H^* \cap D$, then $ay = a_1a_2$, where $a_1, a_2 \in H^*$. Since D is factorial, there exist elements $y_1, y_2 \in D^* \cup \{1\}$ such that $y = y_1y_2$, $y_1 \,|\, a_1$ and $y_2 \,|\, a_2$, and we obtain

$$a = (y_1^{-1}a_1)(y_2^{-1}a_2) \in (y_1^{-1}H^* \cap D)(y_2^{-1}H^* \cap D).$$

The reverse inclusion is obvious. ∎

Now we are going to explain in which way the class semigroup $\mathcal{C}^*(H, D)$ connects the arithmetic of H with that of D. We need the following notions.

Definition 4.3. (1) Let H be a monoid and $a, b \in H$. Then $\omega_H(a, b)$ denotes the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property: For any $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in H$, if $a = a_1 \cdot \ldots \cdot a_n$ and $b \,|\, a$, then there exists a subset $\Omega \subset [1, n]$ such that $|\Omega| \le N$ and

$$b \,\Big|\, \prod_{\nu \in \Omega} a_\nu.$$

By definition, $\omega_H(a, b) = 0$ if either $b \nmid a$ or $b \in H^\times$. If $m \in \mathbb{N}_0$, $p_1, \ldots, p_m$ are primes of H and $b = p_1 \cdot \ldots \cdot p_m$, then $\omega_H(a, b) \le m$.

(2) Let C be an additive abelian semigroup. We denote by $\mathsf{d}(C)$ the smallest $d \in \mathbb{N} \cup \{\infty\}$ with the following property: For any $m \in \mathbb{N}$ and $c_1, \ldots, c_m \in C$ there exists a subset $J \subset [1, m]$ such that $|J| \le d$ and

$$\sum_{j=1}^{m} c_j = \sum_{j \in J} c_j.$$

If C is an abelian group, then $\mathsf{D}(C) = \mathsf{d}(C) + 1$ is known as Davenport's constant and plays an important role in the theory of non-unique factorization (see [8] or [30, Section 9.1]).

Lemma 4.4. *If C is a finite additive abelian semigroup, then $\mathsf{d}(C) < \infty$.*

Proof. Suppose that $C = \{c_1, \ldots, c_k\}$. For every $c \in C$ we consider the set

$$X(c) = \Big\{(m_1, \ldots, m_k) \in \mathbb{N}_0^k \,\Big|\, \sum_{i=1}^{k} m_i c_i = c\Big\}.$$

The set $\mathrm{Min}(X(c))$ of minimal points of $X(c)$ is finite by Dickson's Theorem (see [25, Theorem 1.1]), and therefore the set

$$X = \bigcup_{c \in C} \mathrm{Min}(X(c)) \subset \mathbb{N}_0^k$$

is also finite. By construction, we obtain $\mathsf{d}(C) = \max\{|\mathbf{m}| \mid \mathbf{m} \in X\}$. ∎

Proposition 4.5. *Let $H \subset D$ be a submonoid, $H \cap D^\times = H^\times$ and $a, b \in H$. Then*

$$\omega_H(a,b) \le \omega_D(a,b) + \mathsf{d}(\mathcal{C}^*(H,D)).$$

Proof. Suppose that $n \in \mathbb{N}$, $a, b, a_1, \ldots, a_n \in H$, $a = a_1 \cdot \ldots \cdot a_n$ and $b \,|_H\, a$. We may assume that $a_1, \ldots, a_n$ do not lie in $H^\times$ and thus not in $D^\times$. Since $b \,|_D\, a$, it follows that (after renumbering, if necessary) there exists some $m \in [1,n]$ such that $m \le \omega_D(a,b)$ and $b \,|_D\, a_1 \cdot \ldots \cdot a_m$. Let $d \in D$ be such that $a_1 \cdot \ldots \cdot a_m = bd$. Then $b^{-1}a = a_{m+1} \cdot \ldots \cdot a_n d$, and (after renumbering again, if necessary), there exists some $t \in \mathbb{N}$ such that $m + t \le n$, $t \le \mathsf{d}(\mathcal{C}^*(H,D))$ and

$$\sum_{j=m+1}^{n} [a_j]_H^D = \sum_{j=m+1}^{m+t} [a_j]_H^D.$$

Then

$$[b^{-1}a]_H^D = \sum_{j=m+1}^{n} [a_j]_H^D + [d]_H^D = \sum_{j=m+1}^{m+t} [a_j]_H^D + [d]_H^D = [a_{m+1} \cdot \ldots \cdot a_{m+t} d]_H^D,$$

and $b^{-1}a \in H$ implies $b^{-1}a_1 \cdot \ldots \cdot a_{m+t} = a_{m+1} \cdot \ldots \cdot a_{m+t} d \in H$. Hence $b \,|\, a_1 \cdot \ldots \cdot a_{m+t}$, and since $m + t \le \omega_D(a,b) + \mathsf{d}(\mathcal{C}^*(H,D))$, we are done. ∎

Theorem 4.6 (Partition Theorem). *Let D be a factorial monoid, and let $S \subset H \subset D$ be submonoids such that $\mathcal{C}^*(\mathcal{A}(H), D)$ is finite. Let $\Omega \subset H$ be a subset such that $\Omega \cap D^\times \subset H^\times$ and*

$$\sup\{\omega_H(ab, b) \mid a \in S,\, b \in \Omega\} < \infty.$$

Then Ω has a finite decomposition $\Omega = \Omega_1 \cup \ldots \cup \Omega_t$ such that, for all $j \in [1,t]$, $a \in S$ and $b, b' \in \Omega_j$, we have $\mathsf{L}_H(ab) = \mathsf{L}_H(ab')$.

In particular, if $\mathfrak{a} \subset H$ is a pattern ideal, $j \in [1,t]$, $a \in S$ and $b, b' \in \Omega_j$, then $ab \in \mathfrak{a}$ if and only if $ab' \in \mathfrak{a}$.

Proof. Let $M \in \mathbb{N}$ be such that $\omega_H(ab, b) \le M$ for all $a \in S$ and $b \in \Omega$, and set

$$C = \{[a]_{\mathcal{A}(H)}^D \mid a \in (D \setminus D^\times) \cup H^\times\}.$$

Since $[\varepsilon]_{\mathcal{A}(H)}^D = [1]_{\mathcal{A}(H)}^D$ for all $\varepsilon \in H^\times$, we infer that $C = \mathcal{C}^*(\mathcal{A}(H), D)$ is finite. For $b \in \Omega \setminus H^\times$, we denote by $\mathbf{T}(b)$ the set of all $T \in \mathcal{F}(C)$ which arise in the following way: There exists some $m \in [1, M]$, and there exist elements $x_1, \ldots, x_m \in D$, $y_1, \ldots, y_m \in (D \setminus D^\times) \cup H^\times$ and $a_1 \in H$ such that

$b = y_1 \cdot \ldots \cdot y_m$, $a = a_1 x_1 \cdot \ldots \cdot x_m \in S$, the elements $x_j y_j$ are atoms of H for all $j \in [1, m]$, and

$$T = \prod_{j=1}^{m} [y_j]^D_{\mathcal{A}(H)}.$$

By assumption, the set $\mathcal{T} = \{\mathbf{T}(b) \mid b \in \Omega \setminus H^\times\}$ is finite. For $T \in \mathcal{T}$, we denote by Ω_T the set of all $b \in \Omega \setminus H^\times$ such that $\mathbf{T}(b) = T$, and we assert that

$$\Omega = (\Omega \cap H^\times) \cup \bigcup_{T \in \mathcal{T}} \Omega_T$$

is the desired decomposition. If $b, b' \in H^\times$, then clearly $\mathsf{L}_H(ab) = \mathsf{L}_H(ab')$ for all $a \in S$. Thus assume that $T \in \mathcal{T}$, $b, b' \in \Omega_T$, $a \in S$ and $n \in \mathsf{L}_H(ab)$. We must prove that $n \in \mathsf{L}_H(ab')$.

Let $u_1, \ldots, u_n \in \mathcal{A}(H)$ be such that $ab = u_1 \cdot \ldots \cdot u_n$. Since $\omega_H(ab, b) \le M$, we may renumber $u_1, \ldots, u_n$ in such a way that $b \,|_H\, u_1 \cdot \ldots \cdot u_m$ for some $m \in [1, M]$, say $u_1 \cdot \ldots \cdot u_m = bc$, where $c \in H$. Since D is factorial, there exist elements $x_1, \ldots, x_m, y_1, \ldots, y_m \in D$ such that $b = y_1 \cdot \ldots \cdot y_m$, $c = x_1 \cdot \ldots \cdot x_m$, and $u_j = x_j y_j$ for all $j \in [1, m]$. We may assume that $y_j \notin D^\times \setminus H^\times$ for all $j \in [1, m]$. Indeed, suppose that (after renumbering) there is some $l \in [1, m]$ such that $y_1, \ldots, y_l \in D^\times \setminus H^\times$ and $y_{l+1}, \ldots, y_m \notin D^\times \setminus H^\times$. Since $b \notin H^\times$, we infer $l < m$. Now we replace $y_1, \ldots, y_l$ by 1, y_m by $(y_1 \cdot \ldots \cdot y_l) y_m$, x_j by $y_j x_j$ for all $j \in [1, l]$ and x_m by $(y_1 \cdot \ldots \cdot y_l)^{-1} x_m$ to arrive at an appropriate choice.

If $a_1 = u_{m+1} \cdot \ldots \cdot u_n$, then $a = a_1 x_1 \cdot \ldots \cdot x_m$,

$$T = \prod_{j=1}^{m} [y_j]^D_{\mathcal{A}(H)} \in \mathbf{T}(b) = \mathbf{T}(b'),$$

and hence there exists a product decomposition $b' = y_1' \cdot \ldots \cdot y_m'$, where $y_j' \in (D \setminus D^\times) \cup H^\times$ and $[y_j']^D_{\mathcal{A}(H)} = [y_j]^D_{\mathcal{A}(H)}$ for all $j \in [1, m]$. For $j \in [1, m]$, we have $x_j = y_j^{-1} u_j \in y_j^{-1} \mathcal{A}(H) \cap D = y_j'^{-1} \mathcal{A}(H) \cap D$ and therefore $x_j y_j' \in \mathcal{A}(H)$. Since $ab' = (x_1 y_1') \cdot \ldots \cdot (x_m y_m')\, u_{m+1} \cdot \ldots \cdot u_n$, we obtain $n \in \mathsf{L}_H(ab')$.

If $\mathfrak{a} \subset H$ is a pattern ideal and $a, b, b' \in H$ are such that $\mathsf{L}_H(ab) = \mathsf{L}_H(ab')$, then (by the very definition of pattern ideals) we have $ab \in \mathfrak{a}$ if and only if $ab' \in \mathfrak{a}$. ∎

5. Abstract congruence monoids. In this section we introduce two types of monoids: Abstract congruence monoids (AC-monoids for short) and C_0-monoids. Abstract congruence monoids form a common generalization of singular congruence monoids in Dedekind domains, of congruence monoids

in semilocal Dedekind domains and of certain finitely primary monoids. C_0-monoids are special abstract congruence monoids satisfying a finiteness condition. They seem to be the appropriate tool to settle arithmetical questions in various contexts. In this paper we use them to investigate the arithmetic of congruence monoids in Dedekind domains. W. Hassler [27] used them only recently to obtain a multiplicative model for all finitely generated domains satisfying certain (natural) finiteness conditions.

DEFINITION 5.1. (1) Let F be a monoid, $Y \subset F$ a submonoid, $s \in \mathbb{N}$ and $p_1, \ldots, p_s$ pairwise non-associated prime elements of F such that $F = Y \times [p_1, \ldots, p_s]$. Then every $x \in F$ has a unique representation in the form

$$x = u \prod_{i=1}^{s} p_i^{n_i}, \quad \text{where} \quad u \in Y \text{ and } (n_1, \ldots, n_s) \in \mathbb{N}_0^s.$$

We call $\mathrm{supp}(x) = \{i \in [1,s] \mid \mathsf{v}_{p_i}(x) \ne 0\}$ the *support* of x, and we set $u = \mathsf{E}(x)$.

(2) Let $F = Y \times [p_1, \ldots, p_s]$ be as above and $H \subset F$ a submonoid. A subset $I \subset [1,s]$ is called *H-essential* if there exists some $a \in H$ such that $I = \mathrm{supp}(a)$. By definition, $\emptyset$ is always H-essential. We denote by $\mathfrak{E}_H$ the set of all non-empty H-essential subsets of $[1,s]$. A congruence relation $\equiv$ on Y is called *H-admissible* with respect to $p_1, \ldots, p_s$ if for all $u, v \in Y$,

$$u \equiv v \quad \text{implies} \quad u^{-1}H \cap ([p_1, \ldots, p_s] \setminus \{1\}) = v^{-1}H \cap ([p_1, \ldots, p_s] \setminus \{1\})$$

(equivalently, if $x \in [p_1, \ldots, p_s] \setminus \{1\}$, then $ux \in H$ implies $vx \in H$).

(3) Let $F = Y \times [p_1, \ldots, p_s]$ be as above. A submonoid $H \subset F$ is called an *AC-monoid* defined in F by $p_1, \ldots, p_s$ and a congruence relation $\equiv$ on Y with parameter $\alpha \in \mathbb{N}$ if the following conditions are satisfied:

(AC 1) $Y \cap H = H^\times$.

(AC 2) For every $j \in [1,s]$ and $a \in p_j^\alpha F$, we have $a \in H$ if and only if $p_j^\alpha a \in H$.

(AC 3) $\equiv$ is H-admissible with respect to $p_1, \ldots, p_s$, $Y/\equiv$ is a finite group, and $|Y/\equiv| \,\big|\, \alpha$.

(4) A monoid H is called a *C_0-monoid* if there exists a monoid $F = Y \times [p_1, \ldots, p_s]$ as above with $Y = F^\times$ such that H is an AC-monoid defined in F by $p_1, \ldots, p_s$ and a congruence relation $\equiv$ on Y with some parameter α.

The concept of an AC-monoid is similar to that of a finitely primary monoid as introduced in [23] and investigated in detail in [11]. We recall the definition. A monoid H is called *finitely primary of rank s and exponent α* if there exists a factorial monoid $F = F^\times \times [p_1, \ldots, p_s]$ (with pairwise non-associated primes $p_1, \ldots, p_s$) such that $H \subset F$ is a submonoid satisfying

$$(p_1 \cdot \ldots \cdot p_s)^\alpha F \subset H, \quad H \setminus H^\times \subset p_1 \cdot \ldots \cdot p_s F.$$

In this case, F is uniquely determined by H (in fact, $F = \widehat{H}$ is the complete integral closure of H), $H \cap F^\times = H^\times$ and $\mathfrak{E}_H = \{[1, s]\}$.

In general, a finitely primary monoid need not be an AC-monoid inside some factorial monoid F. Without proof, we mention that the latter is always v-noetherian, while there exist finitely primary monoids which are not (see [26]). The precise connection between AC-monoids and finitely primary monoids is as follows.

PROPOSITION 5.2. *Let H be a finitely primary monoid of rank s and exponent α, and*

$$F = \widehat{H} = F^\times \times [p_1, \ldots, p_s]$$

with pairwise non-associated primes $p_1, \ldots, p_s$. Then H is an AC-monoid (and thus a C_0-monoid) defined in F by $p_1, \ldots, p_s$ and some congruence relation on $F^\times$ with parameter α if and only if the following two conditions are satisfied:

(1) *There exists a subgroup $V \subset F^\times$ with $(F^\times : V) \,|\, \alpha$ and $V(H \setminus H^\times) \subset H$.*

(2) *For every $j \in [1, s]$ and $a \in p_j^\alpha F$, we have $a \in H$ if and only if $p_j^\alpha a \in H$.*

Proof. It is sufficient to prove that (1) is equivalent to (AC 3).

Let $\equiv$ be a congruence relation of $F^\times$ which is H-admissible with respect to $p_1, \ldots, p_s$ such that $F^\times/\equiv$ is a finite group satisfying $|F^\times/\equiv| \;\big|\; \alpha$. Then $V = \{u \in F^\times \mid u \equiv 1\}$ is a subgroup of $F^\times$, and $F^\times/V = F^\times/\equiv$. If $v \in V$ and $a \in H \setminus H^\times$, then $a = uc$, where $u \in F^\times$ and $c \in [p_1, \ldots, p_s] \setminus \{1\}$. Since $vu \equiv u$ and $uc \in H$, it follows that $va = vuc \in H$.

If (1) is satisfied, let $\equiv$ be the congruence modulo V on $F^\times$, that is, $u \equiv v$ if and only if $u^{-1}v \in V$. Then $F^\times/V = F^\times/\equiv$, and we must prove that $\equiv$ is H-admissible with respect to $p_1, \ldots, p_s$. If $u, v \in F^\times$, $u \equiv v$, $x \in [p_1, \ldots, p_s] \setminus \{1\}$ and $ux \in H$, then $ux \notin H^\times$ and thus $vx = (u^{-1}v)(ux) \in V(H \setminus H^\times) \subset H$. ∎

The following lemma is quite elementary. It contains the main arguments used throughout the paper.

LEMMA 5.3. *Let $F = Y \times [p_1, \ldots, p_s]$ be as in Definition* 5.1 *and $H \subset F$ an AC-monoid defined by $p_1, \ldots, p_s$ and a congruence relation $\equiv$ on Y with parameter $\alpha \in \mathbb{N}$.*

(1) *If $u, v \in Y$, $a \in F \setminus Y$ and $u \equiv v$, then $ua \in H$ implies $va \in H$.*

(2) *If $u \in Y$ and $(n_1, \ldots, n_s), (n_1', \ldots, n_s') \in \mathbb{N}_0^s$ are such that, for all $i \in [1, s]$,*

$$\text{either} \quad n_i = n_i' \quad \text{or} \quad (n_i \equiv n_i' \bmod \alpha \text{ and } \min\{n_i, n_i'\} \ge \alpha),$$

then

$$up_1^{n_1} \cdot \ldots \cdot p_s^{n_s} \in H \quad \text{implies} \quad up_1^{n_1'} \cdot \ldots \cdot p_s^{n_s'} \in H.$$

(3) *If* $I \in \mathfrak{E}_H$, $(l_i)_{i\in I} \in \mathbb{N}^I$, $u \in Y$ *and* $u \equiv 1$, *then*

$$u \prod_{i\in I} p_i^{\alpha l_i} \in H.$$

Proof. (1) Let $u, v \in Y$ be such that $u \equiv v$, $a \in F \setminus Y$ and $ua \in H$. Then $a = wc$ for some $w \in Y$ and $c \in [p_1, \dots, p_s] \setminus \{1\}$. Now $u \equiv v$ implies $uw \equiv vw$, and therefore $ua = uwc \in H$ implies $va = vwc \in H$.

(2) Let $u \in Y$, $(n_1, \dots, n_s) \in \mathbb{N}_0^s$ and $up_1^{n_1} \cdot \ldots \cdot p_s^{n_s} \in H$. Let $(n_1', \dots, n_s') \in \mathbb{N}_0^s$ be such that, for all $i \in [1, s]$, either $n_i = n_i'$ or ($n_i \equiv n_i' \bmod \alpha$ and $\min\{n_i, n_i'\} \ge \alpha$). In order to prove that $up_1^{n_1'} \cdot \ldots \cdot p_s^{n_s'} \in H$ we proceed by induction on $l = |\{j \in [1, s] \mid n_j \ne n_j'\}|$. If $l = 0$, there is nothing to do. Thus suppose that $l \ge 1$, and let $j \in [1, s]$ be such that $n_j' = n_j + k\alpha$ for some $k \in \mathbb{Z}\setminus\{0\}$. By induction on $|k|$ we obtain $up_1^{n_1} \cdot \ldots \cdot p_{j-1}^{n_{j-1}} p_j^{n_j'} p_{j+1}^{n_{j+1}} \cdot \ldots \cdot p_s^{n_s} \in H$, and the induction hypothesis concerning l implies $up_1^{n_1'} \cdot \ldots \cdot p_s^{n_s'} \in H$.

(3) Since $I \in \mathfrak{E}_H$, there exists some $v \in Y$ and $(n_i)_{i\in I} \in \mathbb{N}^I$ such that

$$a = va_0 \in H, \quad \text{where} \quad a_0 = \prod_{i\in I} p_i^{n_i} \in F \setminus Y.$$

Hence $a^\alpha = v^\alpha a_0^\alpha \in H$ and $a_0^\alpha \in F \setminus Y$. Since $v^\alpha \equiv 1 \equiv u$ and $\equiv$ is H-admissible, (1) implies $ua_0^\alpha \in H$. Now the assertion follows by (2), since $\alpha n_i \equiv \alpha l_i \bmod \alpha$ and $\min\{\alpha l_i, \alpha n_i\} \ge \alpha$ for all $i \in I$. ∎

THEOREM 5.4. *Let* $F = Y \times [p_1, \dots, p_s]$ *be as in Definition* 5.1 *and* $H \subset F$ *an AC-monoid defined by* $p_1, \dots, p_s$ *and a congruence relation* $\equiv$ *on* Y *with parameter* $\alpha \in \mathbb{N}$.

(1) $\mathcal{C}^*(H, F)$ *is finite.*

(2) $H_{\mathrm{red}} \subset F/H^\times = Y/H^\times \times [p_1H^\times, \dots, p_sH^\times]$ *is an AC-monoid defined by* $p_1H^\times, \dots, p_sH^\times$ *and some congruence relation* $\equiv^*$ *on* $Y/H^\times$ *with parameter* α. *If* H *is a* C_0*-monoid, then so is* H_{red}.

(3) *If* F *is factorial and* H *is reduced, then there exists a transfer homomorphism* $\beta\colon H \to \overline{H}$ *into a reduced* C_0*-monoid* $\overline{H}$.

Proof. (1) For $\alpha \in \mathbb{N}$, we define a reduction map $\varrho_\alpha\colon F \to F$ as follows. If $x = up_1^{n_1} \cdot \ldots \cdot p_s^{n_s}$, where $u \in Y$ and $(n_1, \dots, n_s) \in \mathbb{N}_0^s$, then $\varrho_\alpha(x) = up_1^{n_1 - \alpha l_1} \cdot \ldots \cdot p_s^{n_s - \alpha l_s}$, where

$$l_i = \begin{cases} 0 & \text{if } n_i < 2\alpha, \\ \lfloor n_i/\alpha \rfloor - 1 & \text{if } n_i \ge 2\alpha. \end{cases}$$

If $l_i \ne 0$, then $\alpha \le n_i - \alpha l_i < 2\alpha$. Hence Lemma 5.3 implies that, for all $x, y \in F$, we have $xy \in H$ if and only if $\varrho_\alpha(x)y \in H$.

Let $\{u_1, \dots, u_t\} \subset Y$ be a set of representatives for $Y/\equiv$, chosen in such a way that $u_\tau \notin F^\times$ whenever there exists some $u \in Y \setminus F^\times$ such that

$u \equiv u_\tau$. Now we consider the finite set

$$B = \Big\{ u_\tau \prod_{i=1}^{s} p_i^{n_i} \;\Big|\; \tau \in [1,t],\ (n_1,\dots,n_s) \in [0, 2\alpha-1]^s \Big\},$$

and we define $\varphi\colon F \to B$ by $\varphi(uc) = u_\tau \varrho_\alpha(c)$ whenever $u \in Y$, $u \equiv u_\tau$ and $c \in [p_1,\dots,p_s]$. We assert that $[x]_H^F = [\varphi(x)]_H^F$ for all $x \in F \setminus F^\times$, which in particular implies that $\mathcal{C}^*(H,F)$ is finite.

To prove this assertion, assume that $x = uc \in F \setminus F^\times$, where $c \in [p_1,\dots,p_s]$, $u \in Y$ and $u \equiv u_\tau$ for some $\tau \in [1,t]$. Then $\varphi(x) = u_\tau \varrho_\alpha(c)$, and we must prove that, for all $y \in F$, we have $yx \in H$ if and only if $y\varphi(x) \in H$.

If $y \in F$, then $y = vb$, where $v \in Y$ and $b \in [p_1,\dots,p_s]$, $yx = uvbc$ and $y\varphi(x) = u_\tau v b \varrho_\alpha(c)$. If $bc \ne 1$, then also $\varrho_\alpha(bc) = \varrho_\alpha(b\varrho_\alpha(c)) \ne 1$, and since $uv \equiv u_\tau v$, we have $yx \in H$ if and only if $y\varphi(x) \in H$. If $bc = 1$, then $b = c = \varrho_\alpha(c) = 1$, $yx = uv$, $y\varphi(x) = u_\tau v$, and we argue that then $yx \notin H$ and $y\varphi(x) \notin H$. Indeed, $yx = uv \in H \cap Y = H^\times \subset F^\times$ implies $x \in F^\times$, a contradiction. If $y\varphi(x) = u_\tau v \in H \cap Y = H^\times \subset F^\times$, then $u_\tau \in F^\times$ implies $u \in F^\times$ by our special choice of representatives, whence again $yx = uv \in F^\times$, which leads to a contradiction as above.

(2) Clearly, $p_1H^\times, \dots, p_sH^\times$ are pairwise non-associated primes of $F/H^\times$, $H_{\red} \subset F/H^\times$ and $Y/H^\times \cap H_{\red} = \{1_{H_{\red}}\}$. Hence (AC 1) holds. If $a \in F$, then $aH^\times \in H_{\red}$ if and only if $a \in H$, and thus (AC 2) follows.

To prove (AC 3), we define $\equiv^*$ on $Y/H^\times$ by $uH^\times \equiv^* vH^\times$ if $u \equiv v\varepsilon$ for some $\varepsilon \in H^\times$. Then $\equiv^*$ is an $H_{\red}$-admissible congruence relation on $F/H^\times$ with respect to $p_1H^\times, \dots, p_sH^\times$, and the canonical map $Y \to (Y/H^\times)/{\equiv^*}$ induces an epimorphism $Y/{\equiv} \to (Y/H^\times)/{\equiv^*}$. Hence $(Y/H^\times)/{\equiv^*}$ is also a finite group of order dividing α.

If H is a C_0-monoid, we may assume that $Y = F^\times$, hence $Y/H^\times = (F/H^\times)^\times$, and $H_{\red}$ is also a C_0-monoid.

(3) If F is factorial, then so is Y, and thus $Y = F^\times \times \mathcal{F}(Q)$ for some set Q of pairwise non-associated primes of F. For $q \in Q$, we denote by $\overline{q} \in Y/{\equiv}$ the congruence class of q. Then the set $\overline{Q} = \{\overline{q} \mid q \in Q\}$ is finite, say $\overline{Q} = \{\overline{q}_1, \dots, \overline{q}_t\}$, where $t \in \mathbb{N}_0$ and $q_1, \dots, q_t \in Q$. We consider the factorial monoid

$$\overline{F} = F^\times \times [\overline{q}_1, \dots, \overline{q}_t, p_1, \dots, p_s].$$

Let $\overline{\beta}\colon F \to \overline{F}$ be the unique monoid homomorphism satisfying $\overline{\beta}|F^\times \times [p_1,\dots,p_s] = \mathrm{id}$ and $\overline{\beta}(q) = \overline{q}$ for all $q \in Q$. We set

$$\overline{H} = \overline{\beta}(H) \subset \overline{F}, \qquad \beta = \overline{\beta}|H\colon H \to \overline{H},$$

and we assert that β is the desired transfer homomorphism. For this, we shall prove the following assertions:

(1) If $x, y \in Y$, then $\overline{\beta}(x) = \overline{\beta}(y)$ implies $x \equiv y$.

(2) If $x \in F$ and $\overline{\beta}(x) \in \overline{H}$, then $x \in H$.

(3) β is a transfer homomorphism.

(4) $\overline{H} \cap F^\times = \{1\}$.

(5) If $i \in [1, t]$ and $\overline{a} \in \overline{q}_i^\alpha \overline{F}$, then $\overline{a} \in \overline{H}$ if and only if $\overline{q}_i^\alpha \overline{a} \in \overline{H}$.

(6) If $j \in [1, s]$ and $\overline{a} \in p_j^\alpha \overline{F}$, then $\overline{a} \in \overline{H}$ if and only if $p_j^\alpha \overline{a} \in \overline{H}$.

(7) If $u, v \in F^\times$, $u \equiv v$ and $\overline{x} \in [\overline{q}_1, \ldots, \overline{q}_t, p_1, \ldots, p_s] \setminus \{1\}$, then $u\overline{x} \in \overline{H}$ implies $v\overline{x} \in \overline{H}$.

By (4)–(7) it follows that $\overline{H}$ is a C_0-monoid, and we are done. Now we prove the assertions (1)–(7).

(1) If $x, y \in Y$ and $\overline{\beta}(x) = \overline{\beta}(y)$, then $x = \varepsilon q_1' \cdot \ldots \cdot q_m'$ and $y = \varepsilon q_1'' \cdot \ldots \cdot q_m''$, where $m \in \mathbb{N}_0$, $q_1', \ldots, q_m', q_1'', \ldots, q_m'' \in Q$ and $q_j' \equiv q_j''$ for all $j \in [1, m]$. Since $\equiv$ is a congruence relation, we get $x \equiv y$.

(2) Suppose $x \in F$ and $\overline{\beta}(x) \in \overline{H}$, say $\overline{\beta}(x) = \overline{\beta}(u)$, where $u \in H$. Then $x = ba$ and $u = ca$, where $b, c \in Y$ and $a \in [p_1, \ldots, p_s]$. Then $\overline{\beta}(b) = \overline{\beta}(c)$, and thus $b \equiv c$ by (1). If $a \neq 1$, then $u \in H$ implies $x \in H$, since $\equiv$ is H-admissible. If $a = 1$, then $u \in H \cap Y = \{1\}$ implies $u = 1$, whence also $x = 1 \in H$.

(3) Obviously, β is a surjective homomorphism satisfying $\beta^{-1}(1) = \{1\}$.

Assume now that $u = q_1' \cdot \ldots \cdot q_m' a \in H$, where $m \in \mathbb{N}_0$, $q_1', \ldots, q_m' \in Q$, $a \in F^\times \times [p_1, \ldots, p_s]$, and $\beta(u) = \overline{q_1'} \cdot \ldots \cdot \overline{q_m'}\, a = \overline{v}\,\overline{w}$ for some $\overline{v}, \overline{w} \in \overline{H}$. We may assume that $\overline{v} = \overline{q_1'} \cdot \ldots \cdot \overline{q_k'}\, a_1$ and $\overline{w} = \overline{q_{k+1}'} \cdot \ldots \cdot \overline{q_m'}\, a_2$, where $a_1, a_2 \in F^\times \times [p_1, \ldots, p_s]$ and $a = a_1 a_2$. If $v = q_1' \cdot \ldots \cdot q_k' a_1 \in F$ and $w = q_{k+1}' \cdot \ldots \cdot q_m' a_2 \in F$, then $u = vw$, $\overline{v} = \overline{\beta}(v) \in \overline{H}$, $\overline{w} = \overline{\beta}(w) \in \overline{H}$, and (2) implies $v, w \in H$.

(4) If $u \in \overline{H} \cap F^\times$, then $u = \beta(u) \in H \cap F^\times = H^\times = \{1\}$.

(5) If $\overline{a} \in \overline{q}_i^\alpha \overline{F}$, then $\overline{a} = \overline{\beta}(q^\alpha b)$, where $q \in Q$, $q \equiv q_i$ and $b \in F$. Then $\overline{q}_i^\alpha \overline{a} = \overline{\beta}(q^{2\alpha} b)$, and by (2) we must prove that $q^\alpha b \in H$ if and only if $q^{2\alpha} b \in H$.

If $b \in Y$, then $q^\alpha b \in H$ implies $q^\alpha b \in H \cap Y = \{1\}$, a contradiction. Hence $q^\alpha b \notin H$ and, for the same reason, $q^{2\alpha} b \notin H$. If $b \notin Y$, then the assertion follows by Lemma 5.3(1), since $q^\alpha \equiv q^{2\alpha}$.

(6) If $\overline{a} \in p_j^\alpha \overline{F}$, then $\overline{a} = \overline{\beta}(p_j^\alpha b)$ for some $b \in F$, and $p_j^\alpha \overline{a} = \overline{\beta}(p_j^{2\alpha} b)$. Hence the assertion follows by (2) and (AC 2).

(7) If $1 \neq \overline{x} = \overline{\beta}(x)$, where $x \in \mathcal{F}(Q) \times [p_1, \ldots, p_s]$, then $u\overline{x} = \overline{\beta}(ux)$ and $v\overline{x} = \overline{\beta}(vx)$. By (2), we must prove that $ux \in H$ implies $vx \in H$. If $x \notin \mathcal{F}(Q)$, this follows by Lemma 5.3(1). If $x \in \mathcal{F}(Q)$ and $ux \in H$, then $ux \in H \cap Y = \{1\}$, hence $x \in F^\times$ and therefore $x = 1$. However, we assumed that $\overline{x} \neq 1$. ∎

PROPOSITION 5.5. *Let $F = F^\times \times [p_1, \ldots, p_s]$ be a factorial monoid with pairwise non-associated prime elements $p_1, \ldots, p_s$, and let $H \subset F$ be a*

C_0*-monoid defined by* $p_1, \ldots, p_s$ *and some congruence relation* $\equiv$ *on* $F^\times$ *with parameter* α.

(1) *If* E *is a finite set and* $(F^\times : H^\times) < \infty$, *then* $\mathcal{F}(E) \times H$ *is also a* C_0*-monoid.*

(2) *If* $S \subset H$ *is a saturated submonoid such that* H/S *is finite, then* S *is also a* C_0*-monoid.*

Proof. (1) We may assume that $(F^\times : H^\times) \mid \alpha$, and we denote by $\equiv_H$ the congruence modulo $H^\times$ on $F^\times$. We set $E = \{p_{s+1}, \ldots, p_{s+t}\}$, where $t \in \mathbb{N}_0$ and

$$\overline{H} = H \times \mathcal{F}(E) = H \times [p_{s+1}, \ldots, p_{s+t}] \subset \overline{F} = F^\times \times [p_1, \ldots, p_{s+t}].$$

Clearly, $\equiv_H$ is an $\overline{H}$-admissible congruence relation on $F^\times$ with respect to $p_1, \ldots, p_{s+t}$, and $F^\times/\equiv_H = F^\times/H^\times$. Now it is easily checked that $\overline{H} \subset \overline{F}$ is an AC-monoid defined by $p_1, \ldots, p_{s+t}$ and the congruence relation $\equiv_H$ with parameter α.

(2) We set $\beta = |H/S|$, and we assert that S is an AC-monoid defined in F by $p_1, \ldots, p_s$ and some congruence relation $\equiv^*$ with parameter $\alpha\beta$. We verify the conditions of Definition 5.1.

(AC 1) $F^\times \cap S = F^\times \cap H \cap S = H^\times \cap S = S^\times$, since $S \subset H$ is saturated.

(AC 2) Suppose that $j \in [1, s]$, $a \in p_j^{\alpha\beta} F$, and use the identity $(p_j^{\alpha\beta} a)a^\beta = a(p_j^\alpha a)^\beta$. If $a \in S$, then $p_j^\alpha a \in H$, $p_j^{\alpha\beta} a \in H$ and $(p_j^\alpha a)^\beta \in S$. Hence $p_j^{\alpha\beta} a \in S$, since $S \subset H$ is saturated. Conversely, if $p_j^{\alpha\beta} a \in S$, then $a \in H$, $p_j^\alpha a \in H$, hence $a^\beta \in S$ and $(p_j^\alpha a)^\beta \in S$, and thus also $a \in S$, again since $S \subset H$ is saturated.

(AC 3) $V = \{u \in F^\times \mid u \equiv 1\} \subset F^\times$ is a subgroup, $(F^\times : V) \mid \alpha$, and we assert that $V \subset \mathsf{q}(H)$. Indeed, if $a \in H \setminus F^\times$ and $v \in V$, then $av \in H$ by Lemma 5.3(1) and thus $v \in \mathsf{q}(H)$. Hence $W = \mathsf{q}(S) \cap V \subset F^\times$ is a subgroup satisfying $(F^\times : W) \mid \alpha\beta$, and it is easily checked that the congruence modulo W on $F^\times$ is S-admissible with respect to $p_1, \ldots, p_s$. ∎

Now we are ready to proceed with the more subtle arithmetical statements concerning AC-monoids. Proposition 5.6 is the main step in proving that AC-monoids are locally tame, and Proposition 5.7 asserts that pattern ideals in C_0-monoids are complete.

Proposition 5.6. *Let* $F = Y \times [p_1, \ldots, p_s]$ *be as in Definition* 5.1 *and* $H \subset F$ *an AC-monoid defined by* $p_1, \ldots, p_s$ *and some congruence relation* $\equiv$ *on* Y *with parameter* $\alpha \in \mathbb{N}$.

(1) *If* $a \in H$, $I = \mathrm{supp}(a)$ *and* $I^* = \{i \in I \mid \{i\} \in \mathfrak{E}_H\}$, *then*

$$\frac{1}{2\alpha - 1} \max\{\mathsf{v}_{p_i}(a) \mid i \in I^*\} \le \min \mathsf{L}(a) \le \sum_{i \in I^*} \mathsf{v}_{p_i}(a) + |I|(3\alpha - 1).$$

(2) *If* $a, b \in H$, *then* $\mathsf{t}(a, \mathsf{Z}(b)) \le s(2\alpha-1)(\omega_H(a,b)+1)+s\alpha+\max \mathsf{L}(b)$.
(3) *For* $I \in \mathfrak{E}_H$, *we set*

$$u_I = \prod_{i \in I} p_i^{\alpha}.$$

Then $U = \{u_I \mid I \in \mathfrak{E}_H\}$ *is an almost generating set of* H.

Proof. (1) If $a \in H$, $i \in I^*$ and $\mathsf{v}_{p_i}(a) \ge 2\alpha$, then $p_i^{-\alpha} a \in H$ and thus $a \notin \mathcal{A}(H)$. Hence $\mathsf{v}_{p_i}(u) \le 2\alpha - 1$ for all $u \in \mathcal{A}(H)$ and $i \in I^*$, and therefore $\max\{\mathsf{v}_{p_i}(a) \mid i \in I^*\} \le (2\alpha-1) \min \mathsf{L}(a)$, whence the first inequality.

The second inequality is proved by induction on $|I|$. If $I = \{i\}$, then $I^* = I$, and we clearly have $\min \mathsf{L}(a) \le \mathsf{v}_{p_i}(a)$. Hence we assume that $|I| \ge 2$, we set $I' = \{i \in I \mid \mathsf{v}_{p_i}(a) < 3\alpha\}$, and we distinguish two cases.

Case 1: $I' = \emptyset$. There exists a partition $I \setminus I^* = I_1 \uplus \ldots \uplus I_t \uplus I''$ where $I_1, \ldots, I_t$ are minimial non-empty H-essential subsets of $I \setminus I^*$ and I'' has no non-empty H-essential subset. Clearly such a partition exists (but need not be unique), and we have

$$|I \setminus I^*| \ge |I''| + 2t, \quad \text{whence} \quad t \le |I|/2.$$

For every $i \in I$, we have $\mathsf{v}_{p_i}(a) \ge 3\alpha$ and therefore $\mathsf{v}_{p_i}(a) = \alpha k_i + l_i$, where $k_i \ge 2$ and $\alpha \le l_i < 2\alpha$. This supplies us with a decomposition $a = a^* a_1 \cdot \ldots \cdot a_t a''$, where

$$a_j = \prod_{i \in I_j} p_i^{\alpha k_i} \quad \text{for all } j \in [1,t],$$

$$a^* = \prod_{i \in I^*} p_i^{\alpha k_i}, \quad a'' = \mathsf{E}(a) \prod_{i \in I''} p_i^{\mathsf{v}_{p_i}(a)} \prod_{i \in I \setminus I''} p_i^{l_i}.$$

By Lemma 5.3(3) we have $a^*, a_1, \ldots, a_t \in H$, and Lemma 5.3(2) implies $a'' \in H$. Thus we obtain

$$\min \mathsf{L}(a) \le \min \mathsf{L}(a^*) + \sum_{j=1}^{t} \min \mathsf{L}(a_j) + \min \mathsf{L}(a''),$$

and we estimate the individual summands. We obviously have

$$\min \mathsf{L}(a^*) \le \sum_{i \in I^*} \alpha k_i \le \sum_{i \in I^*} \mathsf{v}_{p_i}(a).$$

Since I'' has no non-empty H-essential subset, every atom u dividing a'' satisfies $\mathsf{v}_{p_i}(u) \ge 1$ for some $i \in I \setminus I''$. Hence

$$\min \mathsf{L}(a'') \le \sum_{i \in I \setminus I''} l_i \le |I|(2\alpha - 1).$$

For every $j \in [1,t]$, we fix some $i_j \in I_j$, and we consider the elements

$$a_j' = p_{i_j}^{\alpha(k_{i_j}-1)} \prod_{i \in I_j \setminus \{i_j\}} p_i^{\alpha} \in H, \quad a_j'' = p_{i_j}^{\alpha} \prod_{i \in I_j \setminus \{i_j\}} p_i^{\alpha(k_i-1)} \in H.$$

Since I_j is a minimal non-empty H-essential set, it follows that

$$\min \mathsf L(a_j) \le \min \mathsf L(a_j') + \min \mathsf L(a_j'') \le 2\alpha.$$

Putting all information together, we obtain

$$\min \mathsf L(a) \le \sum_{i \in I^*} \mathsf v_{p_i}(a) + |I|\,(2\alpha - 1) + 2\alpha t \le \sum_{i \in I^*} \mathsf v_{p_i}(a) + |I|\,(3\alpha - 1).$$

Case 2: $I' \ne \emptyset$. Let a_1 be a maximal divisor of a such that $\mathrm{supp}(a_1) \cap I' = \emptyset$, and set $a = a_1 a_2$, where $a_2 \in H$. Every atom u dividing a_2 satisfies $\mathsf v_{p_i}(u) \ge 1$ for some $i \in I'$, which implies

$$\min \mathsf L(a_2) \le \sum_{i \in I'} \mathsf v_{p_i}(a) \le |I'|\,(3\alpha - 1).$$

By induction hypothesis, we obtain

$$\min \mathsf L(a_1) \le \sum_{i \in I^*} \mathsf v_{p_i}(a_1) + |I \setminus I'|\,(3\alpha - 1) \le \sum_{i \in I^*} \mathsf v_{p_i}(a) + |I \setminus I'|\,(3\alpha - 1),$$

and therefore

$$\min \mathsf L(a) \le \min \mathsf L(a_1) + \min \mathsf L(a_2) \le \sum_{i \in I^*} \mathsf v_{p_i}(a) + |I|\,(3\alpha - 1).$$

(2) We may assume that H is reduced. Suppose that $x \in \mathsf Z(b)$, $z = u_1 \cdot \ldots \cdot u_n \in \mathsf Z(a)$, where $u_1, \ldots, u_n \in \mathcal A(H)$, and $b \,|\, a$. We prove that there exists a factorization $z' \in \mathsf Z(a) \cap x\mathsf Z(H)$ such that $\mathsf d(z, z')$ admits the asserted bound.

After renumbering if necessary, we may assume that there exists some $m \in [0, n]$ such that $b \,|\, u_1 \cdot \ldots \cdot u_m$, say $u_1 \cdot \ldots \cdot u_m = bc$, where $c \in H$. Let $y \in \mathsf Z(c)$ be a factorization with $|y| = \min \mathsf L(c)$. Then $z' = xyu_{m+1} \cdot \ldots \cdot u_n \in \mathsf Z(a)$, and if $I^* = \{i \in \mathrm{supp}(c) \mid \{i\} \in \mathfrak E_H\}$, then (1) implies

$$\begin{aligned} \mathsf d(z, z') &\le \max\{m, |x| + |y|\} \\ &\le \max\Big\{\omega_H(a, b), \max \mathsf L(b) + \sum_{i \in I^*} \mathsf v_{p_i}(c) + s(3\alpha - 1)\Big\}. \end{aligned}$$

For $i \in I^*$, again (1) implies $\mathsf v_{p_i}(c) \le \mathsf v_{p_i}(bc) \le m(2\alpha - 1) \le \omega_H(a, b)\,(2\alpha - 1)$, and therefore

$$\begin{aligned} \mathsf d(z, z') &\le \max\{m, \max \mathsf L(b) + s(2\alpha - 1)\omega_H(a, b) + s(3\alpha - 1)\} \\ &\le s(2\alpha - 1)(\omega_H(a, b) + 1) + s\alpha + \max \mathsf L(b). \end{aligned}$$

(3) We set $n = 2^{s+1}\alpha$, and we assert that $(H \setminus H^\times)^n \subset UH$. Suppose that $a = a_1 \cdot \ldots \cdot a_n \in (H \setminus H^\times)^n$, where $a_1, \ldots, a_n \in H \setminus H^\times$. Then $\mathrm{supp}(a_i) \ne \emptyset$ for all $i \in [1, n]$ and $|\mathfrak E_H| < 2^s$, and therefore there exists some $I \in \mathfrak E_H$ such that $|\{\nu \in [1, n] \mid \mathrm{supp}(a_\nu) = I\}| > 2\alpha$. Hence Lemma 5.3 implies $u_I^{-1} a \in H$, and thus $a \in UH$. ∎

PROPOSITION 5.7. *Let $F = F^\times \times [p_1, \dots, p_s]$ be a factorial monoid with pairwise non-associated prime elements $p_1, \dots, p_s$, and let $H \subset F$ be a C_0-monoid defined by $p_1, \dots, p_s$ and some congruence relation $\equiv$ on $F^\times$ with parameter α. For $I \in \mathfrak{E}_H$, we define*

$$w_I = \prod_{i \in I} p_i^{\alpha(s+1-|I|)},$$

and we set $W = \{w_I \mid I \in \mathfrak{E}_H\}$.

(1) *For every $\theta \in \mathbb{N}$, the set $W^{[\theta]}$ is a full almost generating set of H.*

(2) *Every pattern ideal is complete over W.*

(3) *If $\mathfrak{a} \subset H$ is an s-ideal which is complete over W, then there exists some $\theta_0 \in \mathbb{N}$ such that for every $\theta \ge \theta_0$ the set*

$$E_\theta = \bigcup_{w \in W} w^\theta \mathfrak{a}[W^{[\theta]}, w^\theta] \cup (\mathfrak{a} \setminus W^{[2\theta]} H) \subset \mathfrak{a}$$

is a tame generating set of $\mathfrak{a}$.

The proof of Proposition 5.7 depends on the following technical Lemma 5.8.

LEMMA 5.8. *Let all assumptions and notations be as in Proposition* 5.7, *$I, J \in \mathfrak{E}_H$ and $\theta \in \mathbb{N}$.*

(1) *If $J \subset I$, then $w_J \mid w_I^{s+1}$.*

(2) *$[\![w_J]\!] \subset [\![w_I]\!]$ if and only if $J \subset I$.*

(3) *If $a \in H$, $w_I^\theta \mid a$ and $w_J^\theta \mid a$, then $w_{I \cup J}^\theta \mid a$.*

(4) *If $\mathfrak{a} \subset H$ is an s-ideal and $\theta \ge 2$, then there exists a subset $\Omega \subset \mathfrak{a}[W^{[\theta]}, w_I^\theta]$ such that $\mathsf{v}_{p_i}(b) \le 2\alpha - 1$ for all $b \in \Omega$ and $i \in I$, and $\mathfrak{a}(W^{[\theta]}, w_I^\theta) \subset w_I^\theta [\![w_I]\!]\, \Omega$.*

(5) *If $a \in [\![w_I]\!]^{-1} [\![w_I]\!] H(W^{[\theta]}, w_I^\theta) \cap H$ and $b \in H$, then*

$$\omega_H(a, b) \le 2^s \alpha(\theta s + 1) + \sum_{i \in I} \mathsf{v}_{p_i}(b) + \mathsf{d}(\mathcal{C}^*(H, F)).$$

Proof. (1) and (3) follow by a painstaking application of Lemma 5.3, and (2) holds by (1) and the very definitions.

(4) For every $a \in \mathfrak{a}(W^{[\theta]}, w_I^\theta)$, we construct an element $a^* \in \mathfrak{a}[W^{[\theta]}, w_I^\theta]$ as follows. If $a \in \mathfrak{a}(W^{[\theta]}, w_I^\theta)$ and $i \in I$, then $\mathsf{v}_{p_i}(a) \ge \mathsf{v}_{p_i}(w_I^{2\theta}) = 2\theta\alpha(s + 1 - |I|)$ $\ge \theta\alpha(s - |I| + 1) + 2\alpha$. Hence there exist integers $l_i \in \mathbb{N}$ and $r_i \in [0, \alpha - 1]$ such that $\mathsf{v}_{p_i}(a) = \mathsf{v}_{p_i}(w_I^\theta) + \alpha l_i + r_i + \alpha$, and we obtain

$$a = \Big(w_I^\theta \prod_{i \in I} p_i^{\alpha l_i} \Big) a',$$

where $\alpha \le \mathsf{v}_{p_i}(a') \le 2\alpha - 1$ for all $i \in I$, and thus $a' \in H$ by Lemma 5.3. Let now $a'' \in [\![w_I]\!]$ be a maximal divisor of a', and set $a^* = a''^{-1} a'$. By this

construction, we obtain

$$a^* \in H_{w_I} \cap w_I^{-\theta}[\![w_I]\!]^{-1}\mathfrak{a}(W^{[\theta]}, w_I^\theta) = \mathfrak{a}[W^{[\theta]}, w_I^\theta],$$

$\alpha \le \mathsf{v}_{p_i}(a^*) \le \mathsf{v}_{p_i}(a') \le 2\alpha - 1$ for all $i \in I$ and $a \in a' w_I^\theta [\![w_I]\!] \subset a^* w_I^\theta [\![w_I]\!]$.

For every $a \in \mathfrak{a}(W^{[\theta]}, w_I^\theta)$, we fix an element $a^* \in \mathfrak{a}[W^{[\theta]}, w_I^\theta]$ as above. Then the set Ω of all these elements a^* has the required properties.

(5) Suppose that $a = c_1^{-1}c_2a' \in H$, where $c_1, c_2 \in [\![w_I]\!]$ and $a' \in H(W^{[\theta]}, w_I^\theta)$. Then $w_I^{2\theta} \,|\, a'$ and $w_J^{2\theta} \nmid a'$ for all $J \in \mathfrak{E}_H$ satisfying $J \supsetneq I$. For $b \in H$, we estimate $\omega_H(a, b)$ by means of Proposition 4.5. It suffices to prove that for any $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in H$ such that $a = a_1 \cdot \ldots \cdot a_n$ and $b \,|_H\, a$, there exists a subset $\Omega \subset [1, n]$ satisfying

$$|\Omega| \le 2^s\alpha(\theta s + 1) + \sum_{i \in I} \mathsf{v}_{p_i}(b), \qquad b \,\Big|_F \prod_{\nu \in \Omega} a_\nu.$$

Suppose that $n \in \mathbb{N}$, $a_1, \ldots, a_n \in H$, $a = a_1 \cdot \ldots \cdot a_n$ and $b \,|_H\, a$. If $\Omega_1 = \{\nu \in [1, n] \mid \mathrm{supp}(a_\nu) \not\subset I\}$, then

$$\prod_{i \in [1,s] \setminus I} p_i^{\mathsf{v}_{p_i}(b)} \,\Big|_F \prod_{\nu \in \Omega_1} a_\nu,$$

and there exists a subset $\Omega_2 \subset [1, n]$ such that

$$|\Omega_2| \le \sum_{i \in I} \mathsf{v}_{p_i}(b), \qquad \prod_{i \in I} p_i^{\mathsf{v}_{p_i}(b)} \,\Big|_F \prod_{\nu \in \Omega_2} a_\nu.$$

Hence it is sufficient to prove that $|\Omega_1| \le 2^s\alpha(\theta s + 1)$.

For every subset $\emptyset \ne L \subset [1, s] \setminus I$, we set $l_L = |\{\nu \in [1, n] \mid \mathrm{supp}(a_\nu) \setminus I = L\}|$, and we assert that $l_L < (2\theta s + 1)\alpha$. Once this is proved, we are done since there are less than 2^{s-1} such sets L and hence

$$|\Omega_1| = \sum_{\emptyset \ne L \subset [1,s] \setminus I} l_L < 2^{s-1}(2\theta s + 1)\alpha < 2^s\alpha(\theta s + 1).$$

Assume to the contrary that $l_L \ge (2\theta s+1)\alpha$ for some subset $\emptyset \ne L \subset [1, s]\setminus I$. Then $I \cup L \in \mathfrak{E}_H$, and we assert that $w_{I\cup L}^{2\theta} \,|\, a'$, which gives the desired contradiction.

In fact, if $i \in I$, then $\mathsf{v}_{p_i}(a') \ge \mathsf{v}_{p_i}(w_I^{2\theta}) = 2\theta\alpha(s + 1 - |I|)$, and if $i \in L$, then $\mathsf{v}_{p_i}(a') = \mathsf{v}_{p_i}(a) \ge l_L \ge (2\theta s + 1)\alpha$. Hence

$$\mathsf{v}_{p_i}(a') \ge 2\theta\alpha(s + 1 - |I \cup L|) + \alpha = \mathsf{v}_{p_i}(w_{I\cup L}^{2\theta}) + \alpha \quad \text{for all } i \in I \cup L,$$

and thus $w_{I\cup L}^{2\theta} \,|\, a'$ by Lemma 5.3. ∎

Proof of Proposition 5.7. (1) We set $n = 2^s\theta\alpha(s+1)$, and we assert that $(H \setminus H^\times)^n \subset W^{[\theta]}H$. Suppose that $a_1, \ldots, a_n \in H \setminus H^\times$ and $a = a_1 \cdot \ldots \cdot a_n$. Since $|\mathfrak{E}_H| < 2^s$ and $\mathrm{supp}(a_i) \ne \emptyset$ for all $i \in [1, n]$, there exists some $I \in \mathfrak{E}_H$ such that $|\{\nu \in [1, n] \mid \mathrm{supp}(a_\nu) = I\}| > \theta\alpha(s + 1)$. Hence $\mathsf{v}_{p_i}(a) > \theta\alpha(s + 1) \ge \mathsf{v}_{p_i}(w_I^\theta) + \alpha$ for all $i \in I$, and thus $w_I^\theta \,|\, a$ by Lemma 5.3(2).

It remains to prove that $W^{[\theta]}$ is full, and for this we use [16, Lemma 5.9.2]. We must prove that, for any $I', I'' \in \mathfrak{E}_H$ and $a \in w_{I'}^{2\theta} H \cap w_{I''}^{2\theta} H$, there exists some $I \in \mathfrak{E}_H$ such that $a \in w_I^{2\theta} H$ and $w_{I'}^{2\theta}, w_{I''}^{2\theta} \in [\![w_I^{2\theta}]\!]$. By Lemma 5.8(3), the set $I = I' \cup I''$ has the required properties.

(2) Let $\mathfrak{a} \subset H$ be a pattern ideal. By [16, Theorem 5.7], it is sufficient to prove that for every $w \in W$ and every $\theta \in \mathbb{N}$ with $\theta \ge 2$, there exists some subset $\Omega \subset H[W^{[\theta]}, w^\theta]$ such that $H(W^{[\theta]}, w^\theta) \subset w^\theta [\![w]\!] \, \Omega$, and there exists a decomposition $\Omega = \Omega_1 \cup \ldots \cup \Omega_t$ with the following property: For all $\nu \in [1, t]$, $a \in [\![w]\!]$ and $b, b' \in \Omega_\nu$, we have $ab \in \mathfrak{a}$ if and only if $ab' \in \mathfrak{a}$.

Suppose that $w = w_I$ for some $I \in \mathfrak{E}_H$ and $\theta \in \mathbb{N}$ with $\theta \ge 2$. By Lemma 5.8(4) there exists a subset $\Omega \subset H[W^{[\theta]}, w_I^\theta]$ such that $H(W^{[\theta]}, w_I^\theta) \subset w_I^\theta [\![w_I]\!] \, \Omega$ and $\mathsf{v}_{p_i}(b) \le 2\alpha - 1$ for all $i \in I$ and $b \in \Omega$. The desired decomposition of Ω is furnished by Theorem 4.6 with $S = [\![w_I]\!]$. By Theorem 5.4(1) and Proposition 4.2 it follows that $\mathcal{C}^*(\mathcal{A}(H), F)$ is finite, and thus we must prove that

$$\sup\{\omega_H(ab, b) \mid a \in [\![w_I]\!], \, b \in \Omega\} < \infty.$$

If $a \in [\![w_I]\!]$ and $b \in \Omega \subset H[W^{[\theta]}, w_I^\theta]$, then $ab \in [\![w_I]\!] H[W^{[\theta]}, w_I^\theta] \subset [\![w_I]\!]^{-1} [\![w_I]\!] H(W^{[\theta]}, w_I^\theta) \cap H$, and Lemma 5.8(5) implies

$$\begin{aligned} \omega_H(ab, b) &\le 2^s \alpha(\theta s + 1) + \sum_{i \in I} \mathsf{v}_{p_i}(b) + \mathsf{d}(\mathcal{C}^*(H, F)) \\ &\le 2^s \alpha(\theta s + 1) + (2\alpha - 1)s + \mathsf{d}(\mathcal{C}^*(H, F)). \end{aligned}$$

(3) By [16, Theorem 5.6], there exists some $\theta_0 \ge 2$ such that $\mathfrak{a}$ is $W^{[\theta]}$-generated for all $\theta \in \mathbb{N}$ with $\theta \ge \theta_0$. Let $\theta \ge \theta_0$ be given. By [16, Lemma 5.9.1], there exists some $M_0 \in \mathbb{N}$ such that $\max \mathsf{L}(b) \le M_0$ for all $w \in W$ and $b \in H[W^{[\theta]}, w^\theta]$. We shall use [16, Theorem 5.10] to prove that E_θ is a tame generating set of $\mathfrak{a}$, and therefore we must establish the existence of some bound $M \in \mathbb{N}$ with the following property: For every $w \in W$ and $a \in \mathfrak{a}(W^{[\theta]}, w^\theta)$, there exists some $b \in \mathfrak{a}[W^{[\theta]}, w^\theta]$ such that $w^\theta b \,|\, a$ and $\mathsf{t}(a, \mathsf{Z}(b)) \le M$.

Suppose that $w = w_I$ for some $I \in \mathfrak{E}_H$ and $a \in \mathfrak{a}(W^{[\theta]}, w_I^\theta)$. By Lemma 5.8(4) there exists some $b \in \mathfrak{a}[W^{[\theta]}, w_I^\theta]$ such that $w_I^\theta b \,|\, a$ and $\mathsf{v}_{p_i}(b) \le 2\alpha - 1$ for all $i \in I$. Since $\mathfrak{a}(W^{[\theta]}, w_I^\theta) \subset H(W^{[\theta]}, w_I^\theta) \subset [\![w_I]\!]^{-1} [\![w_I]\!] H(W^{[\theta]}, w_I^\theta) \cap H$, Lemma 5.8(5) implies

$$\omega_H(a, b) \le 2^s \alpha(\theta s + 1) + (2\alpha - 1)s + \mathsf{d}(\mathcal{C}^*(H, F)) = M_1 \quad \text{(say)}.$$

By Proposition 5.6(2) it follows that $\mathsf{t}(a, \mathsf{Z}(b)) \le s(2\alpha - 1)(M_1 + 1) + s\alpha + M_0$, giving the asserted bound. ∎

THEOREM 5.9 (Main Theorem on AC-monoids). *If H is an AC-monoid defined in some factorial monoid F, then H is finitary, locally tame, $\mathsf{c}(H) < \infty$, and the Structure Theorem for Sets of Lengths holds for H.*

Proof. Let F be a factorial monoid, $Y \subset F$ a submonoid, $s \in \mathbb{N}$ and $p_1, \ldots, p_s$ pairwise non-associated prime elements of F such that $F = Y \times [p_1, \ldots, p_s]$, and assume that $H \subset F$ is an AC-monoid defined by $p_1, \ldots, p_s$ and a congruence relation $\equiv$ on Y with parameter α. Since F is a BF-monoid and $F^\times \cap H = H^\times$, it follows by [22, Theorem 3] that H is a BF-monoid, and thus it is finitary by Proposition 5.6(3).

By Theorem 5.4(1), the semigroup $C = \mathcal{C}^*(H, F)$ is finite. If $a \in H$, and $u \in \mathcal{A}(H)$ is a product of $\tau(u)$ primes of F, then Proposition 4.5 implies $\omega_H(a, u) \le \omega_F(a, u) + \mathsf{d}(C) \le \tau(u) + \mathsf{d}(C)$ for all $a \in H$. Using Proposition 5.6(2) we deduce that $\mathsf{t}(a, \mathsf{Z}(u)) \le s(2\alpha - 1)[\tau(u) + \mathsf{d}(C) + 1] + s\alpha + 1$. Since the right hand side is independent of a, it is a bound for $\mathsf{t}(H, u)$, and therefore H is locally tame. By [17, Theorem 3.10] we have $\mathsf{c}(H) < \infty$, and therefore $\Delta(H)$ is finite.

It remains to prove that the Structure Theorem for Sets of Lengths holds for H. By Theorem 5.4(3) it suffices to do this for a C_0-monoid, and by Theorem 2.2 it suffices to prove that in a C_0-monoid pattern ideals are tamely generated. But this was proved in Proposition 5.7. ∎

6. Proof of the Main Theorem for congruence monoids in Dedekind domains

THEOREM 6.1. *Let R be a Dedekind domain and $\mathfrak{f}$ an ideal of R such that $R/\mathfrak{f}$ is finite. Let σ be a sign vector of R, $\emptyset \ne \Gamma \subset R/\mathfrak{f}\sigma$ a multiplicatively closed subset and $H = H_\Gamma \subset R^\bullet$ the congruence monoid defined in R modulo $\mathfrak{f}\sigma$ by Γ.*

(1) *If R is semilocal, $\mathfrak{f}$ is contained in all maximal ideals of R and $\Gamma \cap (R/\mathfrak{f}\sigma)^\times \ne \emptyset$, then H is a C_0-monoid defined in some factorial monoid F such that $(F^\times : H^\times) < \infty$.*

(2) *If $\Gamma \cap (R/\mathfrak{f}\sigma)^\times = \emptyset$ and the ideal class group of R is finite, then H is an AC-monoid.*

Proof. We set $\mathcal{P} = \max(R)$ and $\mathfrak{f} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in \mathcal{P}$ are distinct and $e_1, \ldots, e_s \in \mathbb{N}$. We denote by $\mathcal{P}_\mathfrak{f} = \mathcal{P} \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ the set of all maximal ideals of R which are coprime to $\mathfrak{f}$, by $\mathcal{I} = \mathcal{F}(\mathcal{P})$ the monoid of non-zero ideals of R and by $\mathcal{I}_\mathfrak{f} = \mathcal{F}(\mathcal{P}_\mathfrak{f}) \subset \mathcal{I}$ the submonoid of all ideals coprime to $\mathfrak{f}$. By [10, Theorem 6.28], we have $\mathcal{C}(R) = \{[\mathfrak{a}] \mid \mathfrak{a} \in \mathcal{I}_\mathfrak{f}\}$. If R is semilocal, then R is a principal ideal domain and $\mathcal{P}_\mathfrak{f} = \emptyset$.

Being a Krull monoid, $R^\bullet$ splits in the form $R^\bullet = R^\times \times S$, where S is a submonoid of a free monoid D such that the inclusion map $S \hookrightarrow D$ is a divisor theory (see [25, Theorem 23.4]). The canonical map $R^\bullet \to \mathcal{I}$, defined by $a \mapsto aR$, is also a divisor theory. By the uniqueness of divisor theories, there exists an isomorphism

$$\Phi\colon \mathcal{I} \xrightarrow{\sim} D, \quad \text{written in the form} \quad \mathfrak{a} \mapsto \mathfrak{a}^{\Phi},$$

such that $(aR)^{\Phi} = a$ for all $a \in S$. Then $D = \mathcal{F}(\mathcal{P}^{\Phi})$, and we set $p_i = \mathfrak{p}_i^{\Phi}$ for all $i \in [1, s]$. Then Φ induces an isomorphism $\mathcal{C}(R) \xrightarrow{\sim} D/S$ given by the assignment $[\mathfrak{a}] \mapsto [\mathfrak{a}^{\Phi}]_{D/S}$.

We consider the factorial monoid

$$F = R^{\times} \times D = Y \times [p_1, \ldots, p_s], \quad \text{where} \quad Y = R^{\times} \times \mathcal{I}_{\mathfrak{f}}^{\Phi} = R^{\times} \times \mathcal{F}(\mathcal{P}_{\mathfrak{f}}^{\Phi}).$$

Then $H \subset R^{\bullet} \subset F$ are submonoids, and $T_{\mathfrak{f}} = Y \cap R^{\bullet}$ is the monoid of all $a \in R^{\bullet}$ which are coprime to $\mathfrak{f}$. If $u \in Y$, then $u = \varepsilon \mathfrak{u}^{\Phi}$ with (uniquely determined) $\varepsilon \in R^{\times}$ and $\mathfrak{u} \in \mathcal{I}_{\mathfrak{f}}$, and we have $u \in R^{\bullet}$ if and only if $\mathfrak{u}$ is a principal ideal.

We shall prove that $H \subset F$ is an AC-monoid defined by $p_1, \ldots, p_s$ and some congruence relation $\equiv$ on Y with parameter

$$\alpha = 2 \max\{e_1, \ldots, e_s\} |\mathcal{C}(R)| \, |(R/\mathfrak{f})^{\times}|.$$

If R is semilocal, then $Y = R^{\times}$, $F = R^{\bullet}$, and H is a C_0-monoid. If R is semilocal and $\Gamma \cap (R/\mathfrak{f}\sigma)^{\times} \neq \emptyset$, then $V = \{a \in R \mid a \equiv 1 \bmod \mathfrak{f}\sigma\} \subset H^{\times}$, and since $R^{\times}/V \cong (R/\mathfrak{f}\sigma)^{\times}$ is finite, it follows that $F^{\times}/H^{\times}$ is finite.

We check the conditions of Definition 5.1.

(AC 1) The inclusion $H^{\times} \subset Y \cap H$ is obvious. If $\Gamma \cap (R/\mathfrak{f})^{\times} = \emptyset$, then $Y \cap H = \{1\} = H^{\times}$. If R is semilocal and $\Gamma \cap (R/\mathfrak{f})^{\times} \neq \emptyset$, then $Y = R^{\times}$ and $\Gamma \cap (R/\mathfrak{f}\sigma)^{\times}$ is a group. If $u \in Y \cap H \subset R^{\times}$, then $[u^{-1}]_{\mathfrak{f}\sigma} = [u]_{\mathfrak{f}\sigma}^{-1} \in \Gamma$, hence $u^{-1} \in Y \cap H$, and thus $u \in H^{\times}$.

(AC 2) Suppose that $j \in [1, s]$ and $a \in p_j^{\alpha} F$. Then $p_j^{\alpha} \in R^{\bullet}$, and thus $a \in R^{\bullet}$ if and only if $p_j^{\alpha} a \in R^{\bullet}$. Since $p_j^{\alpha} a \equiv a \equiv 0 \bmod \mathfrak{p}_j^{e_j}$, $p_j^{\alpha} \equiv 1 \bmod \mathfrak{p}_i^{e_i}$ for all $i \in [1, s] \setminus \{j\}$ and $2 \mid \alpha$, we get $p_j^{\alpha} a \equiv a \bmod \mathfrak{f}\sigma$. Since $a \neq 1$, it follows that $p_j^{\alpha} a \in H$ if and only if $a \in H$.

(AC 3) For $u, v \in Y$, we define $u \equiv v$ if and only if there exists some $c \in Y$ such that $uc, vc \in R^{\bullet}$ and $uc \equiv vc \bmod \mathfrak{f}\sigma$. We must prove that $\equiv$ is transitive, compatible with multiplication, $Y/\equiv$ is a finite group, and $\equiv$ is H-admissible.

First of all, if $u, v, c \in Y$, say $u = \varepsilon \mathfrak{u}^{\Phi}$, $v = \eta \mathfrak{v}^{\Phi}$ and $c = \gamma \mathfrak{c}^{\Phi}$, where $\varepsilon, \eta, \gamma \in R^{\times}$ and $\mathfrak{u}, \mathfrak{v}, \mathfrak{c} \in \mathcal{I}_{\mathfrak{f}}$, then we have $uc = \varepsilon\gamma(\mathfrak{u}\mathfrak{c})^{\Phi} \in R$ if and only if $\mathfrak{c} \in -[\mathfrak{u}]$. Hence $u \equiv v$ implies $[\mathfrak{u}] = [\mathfrak{v}]$, and if $c' \in Y$, then $c'u \in R^{\bullet}$ implies $c'v \in R^{\bullet}$. We assert that even $uc' \equiv vc' \bmod \mathfrak{f}\sigma$. Indeed, if $c \in Y$ is such that $uc, vc \in R^{\bullet}$ and $uc \equiv vc \bmod \mathfrak{f}\sigma$, then $(uc')(uc) \equiv (vc')(uc) \bmod \mathfrak{f}\sigma$, and $uc \in T_{\mathfrak{f}}$ implies $uc' \equiv vc' \bmod \mathfrak{f}\sigma$.

If $u, v, w \in Y$, $u \equiv v$ and $v \equiv w$, then there exists some $c \in Y$ such that $uc, vc \in R^{\bullet}$ and $uc \equiv vc \bmod \mathfrak{f}\sigma$, and by the above, we also have $wc \in R^{\bullet}$ and $vc \equiv wc \bmod \mathfrak{f}\sigma$, whence $u \equiv w$.

If $u, v, w \in Y$ and $u \equiv v$, let $c, d \in Y$ be such that $uc, vc, wd \in R^\bullet$ and $uc \equiv vc \bmod \mathfrak{f}\sigma$. Then $(uw)(cd), (vw)(cd) \in R^\bullet$ and $(uw)(cd) \equiv (vw)(cd) \bmod \mathfrak{f}\sigma$ implies $uw \equiv vw$.

If $u = \varepsilon \mathfrak{u}^\Phi \in Y$, where $\varepsilon \in R^\times$ and $\mathfrak{u} \in \mathcal{I}_\mathfrak{f}$, let $\mathfrak{c} \in (-[\mathfrak{u}]) \cap \mathcal{I}_\mathfrak{f}$ be arbitrary, and set $c = \mathfrak{c}^\Phi \in Y$. Then $uc \in T_\mathfrak{f}$, and there exists some $w \in T_\mathfrak{f}$ such that $ucw \equiv 1 \bmod \mathfrak{f}\sigma$. Then $cw \in Y$ and $u(cw) \equiv 1$. Hence $Y/\equiv$ is a group.

Let $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\} \subset \mathcal{I}_\mathfrak{f}$ be a set of representatives for $\mathcal{C}(R)$, and let $\{x_1, \ldots, x_m\} \subset T_\mathfrak{f}$ be a set of representatives for $(R/\mathfrak{f}\sigma)^\times$. Then $\{\mathfrak{a}_i^\Phi x_j \mid i \in [1,h],\ j \in [1,m]\} \subset Y$ is a set of representatives for $Y/\equiv$, and thus $|Y/\equiv| = |\mathcal{C}(R)|\,|(R/\mathfrak{f}\sigma)^\times|$ divides α.

We finally prove that $\equiv$ is H-admissible. Suppose that $u, v \in Y$, $u \equiv v$, $a \in [p_1, \ldots, p_s] \setminus \{1\}$ and $au \in H \subset R^\bullet$. Let $c \in Y$ be such that $cu, cv \in R^\bullet$ and $cu \equiv cv \bmod \mathfrak{f}\sigma$. Since $(cv)(au) = (cu)(av)$ and $cu \in T_\mathfrak{f}$, we obtain $au \equiv av \bmod \mathfrak{f}\sigma$ and therefore also $av \in H$, since $au \neq 1$. ∎

Proof of Theorem 3.6. If $\Gamma \cap (R/\mathfrak{f}\sigma)^\times = \emptyset$, or if R is semilocal and $\mathfrak{f}$ is contained in every maximal ideal of R, then H is an AC-monoid by Theorem 6.1, and the assertions follow by Theorem 5.9.

Assume now that $\Gamma \cap (R/\mathfrak{f}\sigma)^\times \neq \emptyset$. We set $T_\mathfrak{f} = \{a \in R^\bullet \mid a + \mathfrak{f} \in (R/\mathfrak{f})^\times\}$, and we consider (as in Section 3) the congruence monoid $H_{\Gamma,\mathfrak{f}}$, defined in the semilocal Dedekind domain $T_\mathfrak{f}^{-1}R$ modulo $T_\mathfrak{f}^{-1}\mathfrak{f}$ by $\Gamma \subset R/\mathfrak{f}\sigma = T_\mathfrak{f}^{-1}R/T_\mathfrak{f}^{-1}\mathfrak{f}\sigma$. Note that $T_\mathfrak{f}^{-1}\mathfrak{f}$ is contained in every maximal ideal of $T_\mathfrak{f}^{-1}R$. By Theorem 6.1(1), $H_{\Gamma,\mathfrak{f}}$ is a C_0-monoid defined in some factorial monoid F such that $(F^\times : H_{\Gamma,\mathfrak{f}}^\times) < \infty$, and Theorem 5.4(2) implies that then $(H_{\Gamma,\mathfrak{f}})_{\mathrm{red}}$ is a C_0-monoid defined in the factorial monoid $\overline{F} = F/H_{\Gamma,\mathfrak{f}}^\times$ for which $\overline{F}^\times$ is finite. By Theorem 3.5, there exists a divisor homomorphism $\partial\colon H \to \mathcal{F}(\mathcal{P}_\mathfrak{f}) \times (H_{\Gamma,\mathfrak{f}})_{\mathrm{red}}$ whose class group $\mathcal{C}(\partial)$ fits into an exact sequence

$$(R/\mathfrak{f}\sigma)^\times \to \mathcal{C}(\partial) \to \mathcal{C}(R) \to 0.$$

By assumption, the groups $\mathcal{C}(R)$ and $(R/\mathfrak{f})^\times$ are finite, and by Lemma 3.2(3) the group $(R/\mathfrak{f}\sigma)^\times$ is finite as well. Hence $\mathcal{C}(\partial)$ is finite.

To finish the proof, we need the block monoid $\mathcal{B}$ associated with the divisor homomorphism ∂. We recall its definition and basic properties from [24, Section 5]. Let $\mathcal{C}_0 = \{[\mathfrak{p}]_\partial \mid \mathfrak{p} \in \mathcal{P}_\mathfrak{f}\} \subset \mathcal{C}(\partial)$ be the set of all classes containing primes, and let

$$\overline{\beta}\colon \mathcal{F}(\mathcal{P}_\mathfrak{f}) \times (H_{\Gamma,\mathfrak{f}})_{\mathrm{red}} \to \mathcal{F}(\mathcal{C}_0) \times (H_{\Gamma,\mathfrak{f}})_{\mathrm{red}}$$

be the unique monoid homomorphism satisfying $\overline{\beta}(\mathfrak{p}) = [\mathfrak{p}]_\partial$ for all $\mathfrak{p} \in \mathcal{P}_\mathfrak{f}$ and $\beta|(H_{\Gamma,\mathfrak{f}})_{\mathrm{red}} = \mathrm{id}$. Then the monoid $\mathcal{B} = \overline{\beta} \circ \partial(H)$ is called the block monoid and the homomorphism $\beta = \overline{\beta} \circ \partial\colon H \to \mathcal{B}$ is called the block homomorphism associated with ∂. Furthermore, β is a transfer homomorphism, $\mathcal{B} \subset \mathcal{F}(\mathcal{C}_0) \times (H_{\Gamma,\mathfrak{f}})_{\mathrm{red}}$ is a saturated submonoid, and the class group

$\mathcal{F}(\mathcal{C}_0)\times(H_{\Gamma,\mathrm{f}})_{\mathrm{red}}/\mathcal{B}$ is isomorphic to $\mathcal{C}(\partial)$. By Proposition 5.5(1), the monoid $\mathcal{F}(\mathcal{C}_0)\times(H_{\Gamma,\mathrm{f}})_{\mathrm{red}}$ is a C_0-monoid, and therefore $\mathcal{B}$ is a C_0-monoid by Proposition 5.5(2). In particular, $\mathcal{B}$ is locally tame, $\mathsf{c}(\mathcal{B}) < \infty$, and the Structure Theorem for Sets of Lengths holds for $\mathcal{B}$ by Theorem 5.9. Hence the Structure Theorem for Sets of Lengths also holds for H.

By [13, Propositon 4.2], $\mathsf{c}(H) < \infty$, and by [12, Proposition 3.7], H is locally tame (however, see the remark below). ∎

Remark 6.2. The second inequality in [12, Proposition 3.7] is not correct as it stands. It must read

$$\mathsf{t}_H(H', u) \le \mathsf{t}_{\mathcal{B}}(\beta(H'), \beta(u)) + \mathcal{D}(G_0) + \delta.$$

Since $\mathcal{A}(\mathcal{B}) = \{\beta(u) \mid u \in \mathcal{A}(H)\}$, this inequality shows that the local tameness of $\mathcal{B}$ implies that of H.

We indicate the necessary modifications in the proof of [12, Proposition 3.7]. Let $a \in H' \cap uH$ and $z \in \mathsf{Z}(a)$ be given. Set $U = \beta(u) \in \mathcal{A}(\mathcal{B})$ and $Z = \beta(z) \in \mathsf{Z}(\mathcal{B})$. If $U \mid Z$ one can argue as in [12] (there it is Case 2) to obtain a factorization $z' \in \mathsf{Z}(a) \cap u\mathsf{Z}(H)$ such that $\mathsf{d}(z, z') \le \mathcal{D}(G_0) + \delta$. If $U \nmid Z$, there exists a factorization $Z_1 \in \mathsf{Z}(\beta(a)) \cap U\mathsf{Z}(\mathcal{B})$ such that $\mathsf{d}(Z, Z_1) \le \mathsf{d}_{\mathcal{B}}(\beta(H'), U)$. As in the proof of Proposition 4.2 in [13], we find a factorization $z_1 \in \mathsf{Z}(a)$ such that $\beta(z_1) = Z_1$ and $\mathsf{d}(z, z_1) = \mathsf{d}(Z, Z_1)$. Since $U \mid Z_1$, we can apply the case already done and obtain a factorization $z' \in \mathsf{Z}(a) \cap u\mathsf{Z}(H)$ satisfying $\mathsf{d}(z', z_1) \le \mathcal{D}(G_0) + \delta$. Now the assertion follows by the inequality $\mathsf{d}(z, z') \le \mathsf{d}(z, z_1) + \mathsf{d}(z_1, z')$.

References

[1] D. D. Anderson (ed.), *Factorization in Integral Domains* (*Iowa City, IA, 1996*), Lecture Notes in Pure and Appl. Math. 189, Marcel Dekker, 1997.

[2] D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Factorization in integral domains*, J. Pure Appl. Algebra 69 (1990), 1–19.

[3] —, —, —, *Factorization in integral domains. II*, J. Algebra 152 (1992), 78–93.

[4] D. F. Anderson, *Elasticity of factorizations in integral domains: a survey*, in: [1], 1–29.

[5] D. F. Anderson and D. N. El Abidine, *Factorization in integral domains. III*, J. Pure Appl. Algebra 135 (1999), 107–127.

[6] S. T. Chapman and J. Coykendall, *Half-factorial domains, a survey*, in: [9], 97–115.

[7] S. T. Chapman, M. Freeze, and W. W. Smith, *On generalized lengths of factorizations in Dedekind and Krull domains*, in: [9], 117–137.

[8] S. T. Chapman and A. Geroldinger, *Krull domains and monoids, their sets of lengths, and associated combinatorial problems*, in: [1], 73–112.

[9] S. T. Chapman and S. Glaz (eds.), *Non-Noetherian Commutative Ring Theory*, Math. Appl. 520, Kluwer, 2000.

[10] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer, 1978.

[11] A. Geroldinger, *On the structure and arithmetic of finitely primary monoids*, Czechoslovak Math. J. 46 (1996), 677–695.
[12] —, *The catenary degree and tameness of factorizations in weakly Krull domains*, in: [1], 113–153.
[13] —, *Chains of factorizations in weakly Krull domains*, Colloq. Math. 72 (1997), 53–81.
[14] —, *A structure theorem for sets of lengths*, ibid. 78 (1998), 225–259.
[15] A. Geroldinger and F. Halter-Koch, *Arithmetical theory of monoid homomorphisms*, Semigroup Forum 48 (1994), 333–362.
[16] —, —, *Tamely generated ideals in finitary monoids*, JP J. Algebra Number Theory Appl. 2 (2002), 205–239.
[17] A. Geroldinger, F. Halter-Koch, W. Hassler, and F. Kainrath, *Finitary monoids*, Semigroup Forum 67 (2003), 1–21.
[18] A. Geroldinger, F. Halter-Koch, and J. Kaczorowski, *Non-unique factorizations in orders of global fields*, J. Reine Angew. Math. 459 (1995), 89–118.
[19] E. Grosswald, *Topics from the Theory of Numbers*, Birkhäuser, 1984.
[20] F. Halter-Koch, *Arithmetical semigroups defined by congruences*, Semigroup Forum 42 (1991), 59–62.
[21] —, *Ein Approximationssatz für Halbgruppen mit Divisorentheorie*, Result. Math. 19 (1991), 74–82.
[22] —, *Finiteness theorems for factorizations*, Semigroup Forum 44 (1992), 112–117.
[23] —, *Elasticity of factorizations in atomic monoids and integral domains*, J. Théor. Nombres Bordeaux 7 (1995), 367–385.
[24] —, *Finitely generated monoids, finitely primary monoids, and factorization properties of integral domains*, in: [1], 31–72.
[25] —, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.
[26] F. Halter-Koch, W. Hassler, and F. Kainrath, *Remarks on the multiplicative structure of one-dimensional integral domains*, in: Proc. Algebra Conf. in Venezia, 2002, to appear.
[27] W. Hassler, *Factorization in finitely generated domains*, J. Pure Appl. Algebra 186 (2004), 151–168.
[28] B. Jacobson, *Matrix number theory: An example of non-unique factorization*, Amer. Math. Monthly 72 (1965), 399–402.
[29] —, *Factorizations with unequal numbers of primes*, ibid. 73 (1966), 1110.
[30] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., PWN and Springer, 1990.

Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36
8010 Graz, Austria
E-mail: alfred.geroldinger@uni-graz.at
franz.halterkoch@uni-graz.at

Received on 17.9.2002
and in revised form on 18.11.2003 (4374)