Selected Topics from Algebra: Multiplicative Ideal Theory and Factorization Theory

Izbrana poglavja iz algebre: Multiplikativna teorija idealov in teorija faktorizacij

Daniel Smertnig

Spring Semester 2026

Version from
June 3, 2026

Contents

Preface

These are lecture notes for a semester-long PhD course *Selected Topics from Algebra: Multiplicative Ideal Theory and Factorization Theory* at the Faculty of Mathematics and Physics of the University of Ljubljana, held in the summer semester 2026.

The course meets for 15 weeks, two hours per week. Students are expected to have taken the standard undergraduate courses in algebra. Additional knowledge of commutative algebra or algebraic number theory is helpful but not required. Students are expected to pick up some basic knowledge of localization and integral extensions along the way, when needed. When non-trivial results from commutative algebra or number theory are used, this is in an ancillary role, and they can be taken as black boxes.

The notes provide an introduction to non-unique factorizations rather than a comprehensive treatment of the theory. Since knowledge of commutative algebra is not strictly assumed, significant space is devoted to a discussion of Dedekind domains as a suitable starting point for factorization theory.

My thanks to Jan Pantner for carefully reading earlier versions of the notes and pointing out mistakes.

Notation and Conventions

In these notes $\mathbb{N} = \{1, 2, 3, \dots\}$ is the set of all positive integers, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We write $\mathbb{P} = \{2, 3, 5, \dots\} \subseteq \mathbb{N}$ for the set of all prime numbers. The symbols $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}$ denote the complex numbers, rational numbers, real numbers, and integers, respectively. We write $\mathbb{R}_{\geq 0}$ for the nonnegative reals, and $\mathbb{R}_{>0}$ for the positive reals. Analogous notation applies to other ordered sets. For $a, b \in \mathbb{R}$, we write $[a, b] = \{ x \in \mathbb{Z} : a \leq x \leq b \}$ for the discrete interval between a and b.

A **monoid** is a set H together with an associative binary operation (usually written multiplicatively) and a neutral element 1. A monoid H is **cancellative** if $ab = ac$ implies $b = c$ for all $a, b, c \in H$ and similarly $ba = ca$ implies $b = c$. We denote by $H^\times$ the unit group (that is, the group of invertible elements) of H. Unless stated otherwise, we only consider cancellative commutative monoids. We write $a \mid b$ if $b = ac$ for some $c \in H$, and we say that a divides b.

Similarly, **rings** are commutative and unital, unless stated otherwise. Ring homomorphisms are assumed to preserve the multiplicative identity. A **domain** is a (nonzero) ring in which 0 is the only zero-divisor. For a domain R, we denote by $R^\bullet = R \setminus \{0\}$ the multiplicative monoid of nonzero elements. For a ring R, we denote by $R^\times$ the group of units (that is, the group of invertible elements).

1 Introduction and Basic Concepts

1.1 Motivating Examples

We will study factorizations of elements in (commutative) domains. To do so, it is convenient to work in the more general setting of (commutative, cancellative) monoids: if R is a domain, then $R^\bullet = R \setminus \{0\}$ is such a monoid under multiplication.

Given some monoid H, an element $a \in H$ is an **atom** if it is a nonunit and whenever $a = bc$ with $b, c \in H$, then b or c is a unit. By a factorization of an element $a \in H$ we mean an expression of the form $a = u_1 \cdots u_n$ with u_i atoms (a more precise definition will be given below). It is only interesting to study factorizations up to order and associates, where u and u' are associates if $u = u'\varepsilon$ for some unit ε (equivalently $uH = u'H$; we then write $u \simeq u'$).

We already know that rings such as $\mathbb{Z}$ and the polynomial ring $K[x]$ over a field K are factorial: every nonzero nonunit can be written as a product of atoms, and this factorization is unique up to order and associates. The usual proof proceeds by first showing that these domains are Euclidean, that is, there exists a function $\delta\colon R^\bullet \to \mathbb{N}_0$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\delta(r) < \delta(b)$. Then one shows that Euclidean domains are principal ideal domains (PIDs), and that PIDs are factorial:

$$\text{Euclidean} \implies \text{PID} \implies \text{factorial}.$$

There are other factorial domains that are not PIDs, for instance the polynomial rings $\mathbb{Z}[x]$, $\mathbb{Z}[x_1, \ldots, x_n]$ and $K[x_1, \ldots, x_n]$ with $n \geq 2$.

There are however many interesting domains, in which each element has a factorization into atoms, but this factorization is not unique. Studying the structure of factorizations in such domains is the main topic of factorization theory, or more precisely, the theory of non-unique factorizations. To motivate these questions, let us start with some examples.

Consider the following three domains:

$$\begin{aligned} R_1 &:= \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}, \\ R_2 &:= \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}, \\ R_3 &:= \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right] = \left\{a + b\frac{1+\sqrt{-23}}{2} : a, b \in \mathbb{Z}\right\}. \end{aligned}$$

They are subrings of the fields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-5})$, and $\mathbb{Q}(\sqrt{-23})$, respectively, and are called **rings of integers** in these fields. To say something about factorizations in these rings, it is helpful to first introduce the field norm.

On each field $\mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z}$ a non-square, there is an automorphism σ, defined by $x \coloneqq \alpha + \beta\sqrt{d} \mapsto \alpha - \beta\sqrt{d}$ for $\alpha, \beta \in \mathbb{Q}$ (for $d = -1$ this is just complex conjugation). The field norm $N\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ is defined by $N(x) = x\sigma(x) = \alpha^2 - d\beta^2$. It is easy to check the following:

(1) The map N is multiplicative, meaning $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Q}(\sqrt{d})$.

(2) The restriction $N|_{R_i}$ takes values in $\mathbb{N}_0$ for $i = 1, 2, 3$.

(3) For $x \in R_i$, we have $x \in R_i^\times$ if and only if $N(x) = 1$.

The last property gives $R_1^\times = \{\pm 1, \pm i\}$ and $R_2^\times = R_3^\times = \{\pm 1\}$. Now we find the following.

(1) The ring R_1 is Euclidean with respect to its norm (Exercise 1.33), and hence factorial. For instance $2 = (1+i)(1-i)$ is a factorization of 2 into atoms (since $N(1 \pm i) = 2$ is prime, these elements are necessarily atoms).

(2) In the ring R_2, the number 6 factors as:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

To check that 2, 3, $1 \pm \sqrt{-5}$ are atoms, note that their norms are 4, 9, and 6, respectively, and that $N(a + b\sqrt{-5}) = a^2 + 5b^2$ is never 2 or 3 for $a, b \in \mathbb{Z}$.

Since $R_2^\times = \{\pm 1\}$, the four atoms are not associates, so these are two distinct factorizations of 6 into atoms. Hence, the ring R_2 is not factorial. However, both factorizations of 6 have the same length (namely two). Computing more examples in R_2, we would start to suspect that all factorizations of a given element have the same length.

(3) In R_3, the number 8 factors as

$$8 = 2 \cdot 2 \cdot 2 = \left(\frac{3 + \sqrt{-23}}{2}\right) \cdot \left(\frac{3 - \sqrt{-23}}{2}\right).$$

Here $N(a + b(1 + \sqrt{-23})/2) = a^2 + ab + 6b^2$. Now $N(2) = 4$ and $N((3 \pm \sqrt{-23})/2) = 8$, and one can check $2 \notin N(R_3)$, so the factors are again atoms. Observe that one factorization has length three, while the other one has length two.

We will introduce invariants and notions describing the different possible structures of factorizations. For instance, a domain is **half-factorial** if all factorizations of a given element have the same length (and every nonzero nonunit has a factorization). Then R_2 is half-factorial, but R_3 is not. The problem then becomes how to determine these invariants and properties: while it is easy to see that R_3 is not half-factorial, at this point, it is not clear how to prove that R_2 is indeed half-factorial.

The rings we have seen here (rings of integers in number fields) are prototypical examples where this theory works well. But there are other such rings. As an example, if K is a field, then the subring $K[x^2, x^3]$ of the polynomial ring $K[x]$ is clearly not factorial, since x^6 has two distinct factorizations into atoms, namely $x^6 = (x^2) \cdot (x^2) \cdot (x^2) = (x^3) \cdot (x^3)$.

In the next chapter, we will introduce Dedekind domains as a suitable abstraction to cover such rings. Later, we will meet Krull monoids and domains as a further generalization, and we will see that the theory of non-unique factorizations also works well in these domains. First we introduce some basic concepts and invariants.

1.2 Atomicity and Factoriality

Let H be a monoid.

Definition 1.1. (1) *An **atom** is a nonunit $a \in H$ such that $a = bc$ with $b, c \in H$ implies $b \in H^\times$ or $c \in H^\times$.*

(2) *A **prime element** is a nonunit $p \in H$ such that $p \mid ab$ implies $p \mid a$ or $p \mid b$ for all $a, b \in H$.*

(3) *The monoid H is **atomic** if every $a \in H \setminus H^\times$ can be written as $a = u_1 \cdots u_n$ with u_i atoms.*

(4) *The monoid H is **factorial** if every $a \in H \setminus H^\times$ can be written as $a = u_1 \cdots u_n$ with u_i prime elements.*

As a general convention, we say a domain R is atomic, factorial, etc., if the multiplicative monoid $H = R^\bullet$ has this property.

Lemma 1.2. *Every prime element is an atom.*

Proof. Let $p \in H$ be prime and suppose $p = ab$ with $a, b \in H$. Then $p \mid ab$, hence $p \mid a$ or $p \mid b$. Say $p \mid a$, then $a = pc$ for some $c \in H$, and thus $p = ab = pcb$. By cancellativity of H, we have $cb = 1$, and hence $b \in H^\times$. □

An **ideal**, or more precisely, **s-ideal** of H is a (possibly empty) subset $I \subseteq H$ such that $HI \subseteq I$. A **principal ideal** is an ideal of the form aH for some $a \in H$. Then $a \mid b$ if and only if $bH \subseteq aH$.

Definition 1.3. *The monoid H satisfies the **ascending chain condition on principal ideals** (**ACCP**) if every ascending chain of principal ideals $a_1H \subseteq a_2H \subseteq a_3H \subseteq \cdots$ stabilizes, that is, there exists n such that $a_nH = a_{n+m}H$ for all $m \geq 0$.*

Equivalently, every nonempty set of principal ideals has a maximal element with respect to inclusion. The ACCP provides the most useful sufficient condition for atomicity.

Proposition 1.4. *If H satisfies the ACCP, then H is atomic.*

Proof. Let $\Omega_0 \subseteq H$ be the set of all nonunits that cannot be written as a product of atoms. Suppose $\Omega_0 \neq \varnothing$. Let $\Omega = \{ aH : a \in \Omega_0 \}$. By the ACCP, the set Ω has a maximal element, say aH.

Then a cannot be an atom, so $a = bc$ with $b, c \in H \setminus H^\times$. But then $aH \subsetneq bH$ and $aH \subsetneq cH$. Thus, the elements b, c can be written as product of atoms, and therefore so can $a = bc$, contradicting $a \in \Omega_0$. □

The converse is false, but counterexamples are non-trivial to construct. The first such example was given by Grams [Gra74].

Example 1.5 (Grams's example). Fix a field K, let $(p_n)_{n\geq 0} = (3, 5, 7, 11, \dots)$ be the sequence of odd prime numbers, and let

$$A \coloneqq K[x^{\frac{1}{2^n p_n}} : n \geq 0].$$

So every element of A is of the form $f = \sum_{i=1}^{M} a_i x^{r_i}$ with $a_i \in K$ and $r_i \in \langle \frac{1}{2^n p_n} : n \geq 0 \rangle \subseteq (\mathbb{Q}_{\geq 0}, +)$ (where the angle brackets denote the submonoid generated by a set). Let $S \subseteq A$ consist of all elements with nonzero constant term, and let $B = S^{-1}A = \{ f/g : f \in A, g \in S \}$. Since $(x^{\frac{1}{2^{n+1}}})^2 = x^{\frac{1}{2^n}}$, the chain $(x^{\frac{1}{2^n}} B)_{n\geq 0}$ is an infinite ascending chain of principal ideals in B, so $B^\bullet$ does not satisfy the ACCP. One can show that B is atomic (Exercise 1.35). ◯

For domains, there is the following immediate corollary.

Corollary 1.6. *Every noetherian domain is atomic.*

Proof. Let R be a domain. The nonzero principal ideals of R are of the form aR with $a \in R$, and the principal ideals of the monoid $R^\bullet$ are of the form $aR^\bullet$ with $a \in R^\bullet$. Since $aR = aR^\bullet \cup \{0\}$, the partially ordered set of nonzero principal ideals of R is isomorphic to the poset of principal ideals of $R^\bullet$. Hence, the monoid $R^\bullet$ satisfies the ACCP, and is therefore atomic. □

Another sufficient condition for the ACCP is the existence of a length function.

Definition 1.7. *A **length function** is a function $\lambda\colon H \to \mathbb{N}_0$ such that $\lambda(a) > \lambda(b)$ whenever $a = bc$ with $c \in H \setminus H^\times$.*

Lemma 1.8. *If H has a length function, then H satisfies the ACCP.*

Proof. If $aH \subsetneq bH$, then $a = bc$ with $c \in H \setminus H^\times$, so $\lambda(a) > \lambda(b)$. Therefore, the length of any chain $a_1 H \subsetneq a_2 H \subsetneq a_3 H \subsetneq \cdots$ is bounded by $\lambda(a_1)$. □

Atomicity and factoriality are connected as follows.

Proposition 1.9. *The following statements are equivalent.*

(a) *H is factorial.*

(b) *Every $a \in H \setminus H^\times$ can be written uniquely as $a = u_1 \cdots u_n$ with u_i atoms, up to order and associates.*

(c) *H is atomic and every atom is prime.*

Proof. (a) $\Rightarrow$ (b) Only the uniqueness needs to be shown. By assumption $a = p_1 \cdots p_n$ with p_i prime elements. Suppose $a = u_1 \cdots u_m$ with u_j atoms. Since p_1 is prime, $p_1 \mid u_j$ for some j, say $j = 1$ after reordering. Because u_1 is an atom, then $u_1 \simeq p_1$. We can cancel p_1 to get $p_2 \cdots p_n \simeq u_2 \cdots u_m$. The claim follows by induction on n.

(b) $\Rightarrow$ (c) The first statement is immediate. It remains to show that every atom is prime. Let $u \in H$ be an atom and suppose $u \mid ab$ for some $a, b \in H$. Write $a \simeq u_1 \cdots u_r$ and $b \simeq v_1 \cdots v_s$ with u_i, v_j atoms. Now $ab = uc = u_1 \cdots u_r v_1 \cdots v_s$ for some $c \in H$. By uniqueness, we have $u \simeq u_i$ for some i, or $u \simeq v_j$ for some j. But then $u \mid a$ or $u \mid b$, as claimed.

(c) $\Rightarrow$ (a) Clear. □

The prototypical factorial monoid is the free abelian monoid.

Definition 1.10. *If P is a set, then the* ***free abelian monoid*** *$\mathcal{F}(P)$ over P is the set of all formal products $\prod_{p \in P} p^{v_p}$ with $v_p \in \mathbb{N}_0$ and $v_p = 0$ for all but finitely many p, together with the operation*

$$\Big(\prod_{p \in P} p^{v_p}\Big) \cdot \Big(\prod_{p \in P} p^{w_p}\Big) = \prod_{p \in P} p^{v_p + w_p}.$$

Here we are using multiplicative notation for $\mathcal{F}(P)$. In additive notation, the free abelian monoid is $\mathbb{N}_0^{(P)}$, with the isomorphism

$$(\mathbb{N}_0^{(P)}, +) \to (\mathcal{F}(P), \cdot), \quad (v_p)_{p \in P} \mapsto \prod_{p \in P} p^{v_p}.$$

After fixing a set of representatives for the prime elements (for instance, in $\mathbb{Z}$ we take the positive prime elements, in $K[x]$ it is customary to take monic irreducible polynomials, but in general there may not be a "natural" such set), the following is immediate from the uniqueness of the prime factorization.

Corollary 1.11. *If H is factorial and P is a set of representatives for the associativity classes of prime elements, then*

$$H = H^\times \times \mathcal{F}(P) \cong H^\times \times \mathbb{N}_0^{(P)}.$$

We should by now be convinced that in studying factorizations, the invertible elements do not play a role. A monoid H is **reduced** if $H^\times = \{1\}$. Given an arbitrary monoid H, we can form the associated **reduced monoid** $H_{\text{red}} = H/H^\times$, whose elements are the associativity classes of H, and whose operation is given by $[a][b] = [ab]$. Roughly speaking, the factorization theory of H is the same as that of H_{red}, and it is often convenient to work with the reduced monoid, without explicitly mentioning it. However, even if $H = R^\bullet$ then H_{red} is generally not the multiplicative monoid of a ring, so this is really a monoid-theoretical reduction.

1.3 Length Sets

Let H be a monoid.

Definition 1.12. (1) *The* ***length set*** *of* $a \in H \setminus H^\times$ *is*

$$\mathsf{L}(a) \coloneqq \{ k \in \mathbb{N} : a = u_1 \cdots u_k \text{ with } u_i \text{ atoms} \}.$$

One sets $\mathsf{L}(a) \coloneqq \{0\}$ *for* $a \in H^\times$.

(2) *The* ***system of sets of lengths*** *of* H *is* $\mathcal{L}(H) \coloneqq \{ \mathsf{L}(a) : a \in H \}$.

(3) *The monoid* H *is* ***half-factorial*** *if* $|\mathsf{L}(a)| = 1$ *for all* $a \in H$.

Observe that if H is half-factorial, then $\mathcal{L}(H)$ consists of singletons. Suppose H is not half factorial, say $a = u_1 \cdots u_k = v_1 \cdots v_l$ with $k > l$ and u_i, v_j atoms. Then $a^n = (u_1 \cdots u_k)^m (v_1 \cdots v_l)^{n-m}$ has a factorization of length $nl + m(k-l)$ for each $0 \le m \le n$. So $\mathsf{L}(a^n)$ contains an arithmetic progression of length $n+1$ and difference $k-l$. As soon as we leave the half-factorial case, length sets can therefore become arbitrarily large, and the system of sets of lengths can become quite complicated.

Several simpler invariants are derived from length sets.

Definition 1.13. *Let* H *be atomic.*

(1) *The* ***elasticity*** *of* $a \in H \setminus H^\times$ *is* $\rho(a) \coloneqq \sup \mathsf{L}(a) / \min \mathsf{L}(a) \in \mathbb{Q}_{\ge 1} \cup \{\infty\}$ *(set* $\rho(a) \coloneqq 1$ *for* $a \in H^\times$*), and the* ***elasticity*** *of* H *is* $\rho(H) \coloneqq \sup\{ \rho(a) : a \in H \} \in \mathbb{R}_{\ge 1} \cup \{\infty\}$.

(2) *The* ***union of sets of lengths*** *containing* $k \in \mathbb{N}$ *is* $\mathcal{U}_k(H) \coloneqq \bigcup_{k \in \mathsf{L}(a)} \mathsf{L}(a)$.

(3) *The* k***-th elasticity*** *of* H *is* $\rho_k(H) \coloneqq \sup \mathcal{U}_k(H)$.

Note that an atomic monoid H is half-factorial if and only if $\rho(H) = 1$. In our example, the ring R_3 has $\rho_2(R_3) \ge 3$ and $\rho(R_3) \ge 3/2$. (In fact, equality holds, but we do not yet have the tools to show this.)

Lemma 1.14. (1) *For all* k, $l \ge 1$, *we have* $\rho_{k+l}(H) \ge \rho_k(H) + \rho_l(H)$.

(2) *It holds that*

$$\sup_{k \ge 1} \frac{\rho_k(H)}{k} = \lim_{k \to \infty} \frac{\rho_k(H)}{k} = \rho(H).$$

Proof. (1) There exists $a \in H$ with $\mathsf{L}(a) = \{k, M\}$ with $M = \rho_k(H)$ if $\rho_k(H) < \infty$, and M arbitrarily large if $\rho_k(H) = \infty$. Similarly, there exists b with $\mathsf{L}(b) = \{l, N\}$ and $N = \rho_l(H)$ or N arbitrarily large. Now ab has a factorization of length $k+l$ and one of length $M+N$. Hence, we have $\rho_{k+l}(H) \ge M + N$.

(2) If $\rho_k(H)$ is infinite for some k, then the claims are clear. So suppose $\rho_k(H) < \infty$ for all k. Since the sequence $(\rho_k(H))_{k \ge 1}$ is superadditive by (1), Fekete's Lemma shows that $\lambda \coloneqq \lim_{k \to \infty} \frac{\rho_k(H)}{k}$ exists and equals $\sup_{k \ge 1} \frac{\rho_k(H)}{k}$.

It remains to show $\lambda = \rho(H)$. Since $\rho_k(H)/k \le \rho(H)$ by definition, we have $\lambda \le \rho(H)$. Suppose $\lambda < \rho(H)$. Then there exists $a \in H$ with $\rho(a) > \lambda$. Hence, there exist $l \ge k \ge 1$ with k, $l \in \mathsf{L}(a)$ such that $l/k > \lambda$. But then $\rho_k(H)/k \ge l/k > \lambda$, contradicting the definition of λ. □

Definition 1.15. *Let H be atomic and $a \in H$. The* ***set of distances*** *of a is*

$$\Delta(a) := \{ d \in \mathbb{N} : \mathsf{L}(a) \cap [k, k+d] = \{k, k+d\} \text{ for some } k \},$$

and the ***set of distances*** *of H is $\Delta(H) := \bigcup_{a \in H} \Delta(a)$.*

For instance, if $\mathsf{L}(a) = \{2, 3, 6\}$ then $\Delta(a) = \{1, 3\}$.

Lemma 1.16. (1) *We have $\Delta(a) = \varnothing$ if and only if $|\mathsf{L}(a)| \le 1$.*

(2) *If H is atomic, then $\Delta(H) = \varnothing$ if and only if H is half-factorial.*

(3) *We have $|\Delta(a)| = 1$ if and only if $\mathsf{L}(a)$ is a (non-trivial) arithmetic progression.*

Proof. Clear. □

The behavior of factorization-theoretic notions under natural ring constructions can be tricky. For instance, we know that a domain R is factorial if and only if $R[x]$ is factorial by Gauss's lemma. However, if R is atomic, then $R[x]$ need not be atomic (this is a difficult example of Roitman [Roi93]). Similarly, if R is half-factorial, then $R[x]$ need not be half-factorial. This leads to an open problem.

Open Problem 1.17. *Characterize half-factorial polynomial rings $R[x]$ in terms of properties of R. The following is known:*

- *If $R[x]$ is half-factorial, then R is half-factorial and integrally closed.*
- *If R is noetherian (or a Krull domain), a characterization is available [GH06, Proposition 3.7.10].*

1.4 BF-monoids

Having a suitable sufficient criterion for atomicity, it may still be the case that the length sets of elements are infinite.

Example 1.18. Let $R = K[x^{1/p} : p \in \mathbb{P}]$ with K a field. One can show that in R, each $x^{1/p}$ is an atom, so $\mathsf{L}(x) = \mathbb{P}$ is infinite. The ring R satisfies the ACCP, but is not noetherian (Exercise 1.36). ○

Definition 1.19. *The monoid H is a* ***BF-monoid*** *(or a* ***bounded factorization monoid****) if $\mathsf{L}(a)$ is nonempty and finite for all $a \in H$.*

Proposition 1.20. *Let $M = H \setminus H^\times$. Then the following statements are equivalent.*

(a) *H is a BF-monoid.*

(b) *$\bigcap_{n \ge 0} M^n = \varnothing$.*

(c) *H has a length function.*

Proof. (a) $\Rightarrow$ (b) Let $a \in H$. If $a \in M^n$, then $a = a_1 \cdots a_n$ with $a_i \in M$. Since H is atomic, we can replace each a_i by a product of atoms. Then $\max \mathsf{L}(a) \geq n$. Since $\mathsf{L}(a)$ is finite, there exists n such that $a \notin M^n$, and hence $\bigcap_{n \geq 0} M^n = \varnothing$.

(b) $\Rightarrow$ (c) Define $\lambda(a) \coloneqq \max\{ n \in \mathbb{N}_0 : a \in M^n \}$ for $a \in H$. By (b), this gives a function $\lambda \colon H \to \mathbb{N}_0$. If $a = bc$ with $c \in H \setminus H^\times = M$, then $\lambda(a) \geq \lambda(b) + 1$, so λ is a length function.

(c) $\Rightarrow$ (a) Because H has a length function, it satisfies the ACCP and is therefore atomic. Now suppose $a = u_1 \cdots u_k$ with u_i atoms. Then $\lambda(a) \geq k$, so $\max \mathsf{L}(a) \leq \lambda(a) < \infty$. □

Corollary 1.21. *If H is a BF-monoid and $S \subseteq H$ is a submonoid with $S^\times = S \cap H^\times$, then S is a BF-monoid.*

Proof. Let $\lambda \colon H \to \mathbb{N}_0$ be a length function. Suppose $a, b \in S$ are such that b properly divides a in S, that is $a = bc$ with $c \in S \setminus S^\times$. By assumption, then also $c \in H \setminus H^\times$, so $\lambda(a) > \lambda(b)$. Thus, the restriction $\lambda|_S$ is a length function on S, and S is a BF-monoid by Proposition 1.20. □

An ideal P of H is **prime** if $P \neq H$ and $ab \in P$ implies $a \in P$ or $b \in P$ for all $a, b \in H$. It is easy to see that an element $p \in H$ is prime if and only if the principal ideal pH is a prime ideal.

Theorem 1.22. *Suppose that there exists a set of prime ideals Ω of H with the following properties.*

(i) *It holds that $\bigcap_{n \geq 1} P^n = \varnothing$ for all $P \in \Omega$.*

(ii) *For every a in $H \setminus H^\times$, the set $\{ P \in \Omega : a \in P \}$ is finite and nonempty.*

Then H is a BF-monoid.

Proof. For $a \in H$, let

$$\lambda(a) = \max\{ n_1 + \cdots + n_r : a \in P_1^{n_1} \cap \cdots \cap P_r^{n_r} \text{ with } P_i \in \Omega \text{ pairwise distinct} \}.$$

By assumption, each $\lambda(a)$ is finite. Suppose $a = bc$ with $c \in H \setminus H^\times$. Let $P_1, \ldots, P_r \in \Omega$ and $n_1, \ldots, n_r \in \mathbb{N}_0$ be such that $b \in P_1^{n_1} \cap \cdots \cap P_r^{n_r}$ and $\lambda(b) = n_1 + \cdots + n_r$. Since $c \notin H^\times$, there exists $Q \in \Omega$ with $c \in Q$. Then $a = bc \in (P_1^{n_1} \cap \cdots \cap P_r^{n_r})Q$. If $Q = P_i$ for some i, then $a \in P_i^{n_i+1}$, showing $\lambda(a) > \lambda(b)$. If $Q \neq P_i$ for all i, then $a \in P_1^{n_1} \cap \cdots \cap P_r^{n_r} \cap Q$ similarly shows $\lambda(a) > \lambda(b)$. □

Corollary 1.23. *Every noetherian domain is a BF-domain.*

Proof. Non-trivial, but standard, results from commutative algebra show how to find a set Ω satisfying the assumptions of the previous theorem in this setting.

Let R be a noetherian domain, and let Ω be the set of minimal nonzero prime ideals. For each $P \in \Omega$, the set $P \setminus \{0\}$ is a prime ideal of the monoid $R^\bullet$. By Krull's Intersection Theorem, we have $\bigcap_{n \geq 1} P^n = \{0\}$ for each $P \in \Omega$. The set $\{ P \in \Omega : a \in P \}$ is the set of minimal prime ideals of the noetherian ring R/aR, and hence is finite for each $a \in R^\bullet$. By Krull's Principal Ideal Theorem, every prime ideal that is minimal over $a \in R^\bullet$, is a minimal nonzero prime ideal of R, so also $\{ P \in \Omega : a \in P \} \neq \varnothing$ for each $a \in R^\bullet$. □

While the result for commutative noetherian domains is straightforward, it is open whether the analogous conclusion holds for noncommutative noetherian domains.

Open Problem 1.24. *Is every noncommutative noetherian domain a BF-domain? (See [Bel+23].)*

1.5 Factorizations, Distances, and Catenary Degrees

So far we have only considered lengths of factorizations. For a monoid H, we denote by $\mathcal{A}(H)$ the set of all atoms of H.

Definition 1.25. *The free abelian monoid* $\mathsf{Z}(H) \coloneqq \mathcal{F}(\mathcal{A}(H_{\red}))$ *is the* ***factorization monoid*** *of* H. *It comes with a canonical epimorphism* $\pi\colon \mathsf{Z}(H) \to H_{\red}$ *given by* $\pi(u_1 \cdots u_n) = u_1 \cdots u_n$ *for* $u_i \in \mathcal{A}(H_{\red})$. *For* $a \in H$, *the set* $\mathsf{Z}(a) \coloneqq \pi^{-1}(aH^\times)$ *is the* ***set of factorizations*** *of* a.

If $\mathcal{F}(A)$ is a free abelian monoid over some set A, the length of an element $z = u_1^{n_1} \cdots u_r^{n_r}$ is simply $|z| \coloneqq n_1 + \cdots + n_r$. There is a natural distance function: if $z, z' \in \mathcal{F}(A)$, we can write $z = z_0 z_1$ and $z' = z_0 z_1'$ with $z_1, z_1' \in \mathcal{F}(A)$ having no common factor, and we set $\mathsf{d}(z, z') = \max\{|z_1|, |z_1'|\}$. Then $\mathsf{d}\colon \mathcal{F}(A) \times \mathcal{F}(A) \to \mathbb{N}_0$ is a translation-invariant metric: for all $z, z', z'' \in \mathcal{F}(A)$, we have

- $\mathsf{d}(z, z') = 0$ if and only if $z = z'$.
- $\mathsf{d}(z, z') = \mathsf{d}(z', z)$.
- $\mathsf{d}(z, z') \le \mathsf{d}(z, z'') + \mathsf{d}(z'', z')$.
- $\mathsf{d}(zz'', z'z'') = \mathsf{d}(z, z')$,
- and also $\mathsf{d}(z^k, (z')^k) = k\mathsf{d}(z, z')$ for all $k \in \mathbb{N}$.

The following is slightly less obvious, but useful.

Lemma 1.26. *If* $z \ne z' \in \mathsf{Z}(a)$, *then* $\mathsf{d}(z, z') \ge \big||z| - |z'|\big| + 2$.

Proof. Without restriction $|z| \le |z'|$. Write $z = z_0 z_1$ and $z' = z_0 z_1'$ with $z_1, z_1' \in \mathsf{Z}(H)$ having no common factor. Since $\pi(z) = \pi(z') = aH^\times$, we have $\pi(z_0)\pi(z_1) = \pi(z_0)\pi(z_1')$, and $\pi(z_1) = \pi(z_1')$ by cancellativity. Since $z_1 \ne z_1'$, necessarily $|z_1| \ge 2$. Then $\mathsf{d}(z, z') = |z_1'| \ge |z_1'| - |z_1| + 2 = |z'| - |z| + 2$. □

If $a \in H$ has two different factorizations $z, z' \in \mathsf{Z}(a)$, then a^k has factorizations:

$$z^k,\ z^{k-1}z',\ \ldots,\ z(z')^{k-1},\ (z')^k.$$

To measure how far apart factorizations of elements can be globally in H, it therefore does not make sense to simply look at distances between factorizations of a given element. Instead, the following invariant is used.

Definition 1.27. (1) *The* ***catenary degree*** $\mathsf{c}(a)$ *of* $a \in H$ *is the smallest* $N \in \mathbb{N}_0 \cup \{\infty\}$ *such that for all* $z, z' \in \mathsf{Z}(a)$, *there are* $z = z_0, \ldots, z_k = z'$ *in* $\mathsf{Z}(a)$ *with* $\mathsf{d}(z_{i-1}, z_i) \le N$ *for all* i.

(2) *The* ***catenary degree*** *of H is* $\mathsf{c}(H) \coloneqq \sup\{\, \mathsf{c}(a) : a \in H \,\} \in \mathbb{N}_0 \cup \{\infty\}$.

Lemma 1.28. *If $\Delta(a) \neq \emptyset$, then* $\sup \Delta(a) + 2 \le \mathsf{c}(a)$. *If H is atomic but not half-factorial, then* $\sup \Delta(H) + 2 \le \mathsf{c}(H)$.

Proof. It suffices to show the first claim. Let $d \in \Delta(a)$ and let $k \in \mathbb{N}$ be such that k, $k + d \in \mathsf{L}(a)$, but $\mathsf{L}(a)$ contains no element strictly between k and $k + d$. Let z, z' be factorizations of a with $|z| = k$ and $|z'| = k + d$. If $z = z_0, z_1, \ldots, z_m = z'$ is a chain of factorizations of a, there must exist some pair $(i-1, i)$ with $|z_{i-1}| \le k$ and $|z_i| \ge k + d$. Then $\mathsf{d}(z_{i-1}, z_i) \ge d + 2$ by Lemma 1.26, so $\mathsf{c}(a) \ge d + 2$. □

1.6 FF-monoids

Definition 1.29. *H is an* ***FF-monoid*** *(or* ***finite factorization monoid****) if $\mathsf{Z}(a)$ is finite and nonempty for all $a \in H$.*

On $\mathbb{N}_0^n$ there is a componentwise partial order, with $(a_1, \ldots, a_n) \le (b_1, \ldots, b_n)$ if $a_i \le b_i$ for all i. We will need the following basic lemma.

Lemma 1.30 (Dickson's lemma)**.** *If $M \subseteq \mathbb{N}_0^n$ is nonempty, then the set* $\mathrm{Min}(M)$ *of minimal elements with respect to the componentwise partial order is finite and nonempty.*

Proof. Given any $\mathbf{a} \in M$, the set of elements $\{\, \mathbf{b} \in M : \mathbf{b} \le \mathbf{a} \,\}$ is finite, so it contains a minimal element. Replacing M by the set of its minimal elements, we may now assume that M consists of pairwise incomparable elements.

We show $|M| < \infty$ by induction on n, the case $n \le 1$ being trivial. Let $\mathbf{a} = (a_1, \ldots, a_n) \in M$. For each $1 \le i \le n$ and $0 \le j \le a_i$ let $M_{i,j} = \{\, \mathbf{b} \in M : b_i = j \,\}$. By induction hypothesis each set $M_{i,j}$ is finite. Since $M = \bigcup_{i=1}^{n} \bigcup_{j=0}^{a_i} M_{i,j}$ by incomparability, the claim follows. □

Proposition 1.31. *The following statements are equivalent.*

(a) *H is an FF-monoid.*

(b) *Every $a \in H$ has only finitely many non-associated divisors.*

(c) *H is atomic and every $a \in H$ is divisible by only finitely many non-associated atoms.*

Proof. (a) ⇒ (b). If $b \mid a$ and z is a factorization of b, then there exists a factorization z' of a such that $z \mid z'$ in $\mathsf{Z}(H)$. Since $\mathsf{Z}(a)$ is finite, there are only finitely many possibilities for z', and hence only finitely many possibilities for z. Thus, there are finitely many possibilities for b up to associates.

(b) ⇒ (c). The non-trivial part of the statement is to show that H is atomic. For each $a \in H$, let $\lambda(a)$ denote the number of non-associated divisors of a. By assumption, the number $\lambda(a)$ is finite for each $a \in H$. Moreover, the map λ is a length function: if $a = bc$ with $c \in H \setminus H^\times$, then bc divides a, but bc does not divide b, so $\lambda(a) > \lambda(b)$. Thus, the monoid H is a BF-monoid, and in particular, atomic.

(c) $\Rightarrow$ (a). Let $a \in H$ and let $u_1, \ldots, u_s$ be a set of representatives for the associativity classes of atoms dividing a. Let $M = \{(n_1, \ldots, n_s) \in \mathbb{N}_0^s : u_1^{n_1} \cdots u_s^{n_s} \simeq a\}$. Since H is cancellative, $M = \mathrm{Min}(M)$, and hence M is finite by Lemma 1.30. □

Proposition 1.32. *Let H be an FF-monoid, let $S \subseteq H$ be a submonoid, and let $\rho: S \to S_{\mathrm{red}}$ be the canonical epimorphism.*

(1) *If $\rho(aH^\times \cap S)$ is finite for all $a \in S$, then S is an FF-monoid.*

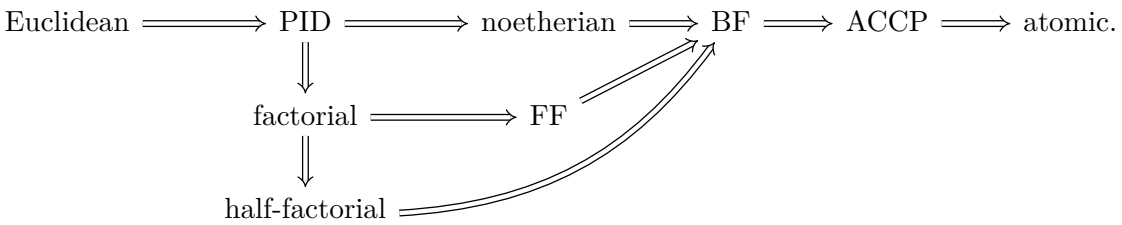
(2) *If $(H^\times : S^\times) < \infty$, then S is an FF-monoid.*

Proof. (1) Let $a \in S$. Using Proposition 1.31, we know that a has only finitely many non-associated divisors in H. It suffices to show that a has only finitely many non-associated divisors in S. Let $D \subseteq S$ be the set of all divisors of a in S. Then there exists a finite set $D_0 \subseteq D$ such that $D \subseteq D_0 H^\times \cap S$. By assumption, then also $\rho(D)$ is finite. This implies the claim.

(2) Let $D \subseteq H^\times$ be a set of representatives for $H^\times/S^\times$. If $a \in S$ then $\rho(aH^\times \cap S) = \rho(aD \cap S)$ is finite, and so (1) implies the claim. □

1.7 Summary of Implications

We can arrange the classes of domains we have introduced so far in the following diagram.



None of the implications in this diagram can be reversed.

- Grams's example (Example 1.5) is an atomic domain without ACCP.
- Example 1.18 gives an ACCP domain that is not a BF-domain.
- The ring of integer-valued polynomials $\mathrm{Int}(\mathbb{Z})$ is an FF-domain, and hence a BF-domain, that is not noetherian (Exercise 1.38). Another example of a non-noetherian FF-domain is a polynomial ring in infinitely many variables over a field. This one is even factorial, but not noetherian.
- $\mathbb{R} + x\mathbb{C}[x]$ is a noetherian domain (and hence a BF-domain) that is not an FF-domain (Exercise 1.37).
- $\mathbb{Z}[\sqrt{-5}]$ is half-factorial, but not factorial. [1]
- $\mathbb{Q}[x, y]$ is a noetherian factorial domain, but not a PID.

[1] We do not yet have the means to show that it is half-factorial.

- $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID but not Euclidean. We can show that it is non-Euclidean (Exercise 1.40). That it is nevertheless a PID follows from standard results in algebraic number theory, according to which it suffices to show that the class group is trivial (see also the next chapter).
- The notions of half-factoriality and FF-domains are also incomparable (Exercises 1.37 and 1.39): $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ and $\mathrm{Int}(\mathbb{Z})$ are FF-domains, but not half-factorial. On the other hand, the ring $\mathbb{R} + x\mathbb{C}[x]$ is half-factorial, but not an FF-domain.
- For incomparability of noetherianity and half-factoriality, note that $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ is noetherian but not half-factorial, while the polynomial ring $K[x_1, x_2, \dots]$ in countably many variables over a field K is half-factorial (even factorial), but not noetherian.

1.8 Exercises

Exercise 1.33. *Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers.*

(1) *The domain R is Euclidean with respect to the norm $N(a+bi) = a^2 + b^2$.*

(2) *Up to associates, the prime elements of R are the following elements:*

- $1 + i$,
- *p with $p \in \mathbb{P}$ and $p \equiv 3 \mod 4$,*
- *for every $p \in \mathbb{P}$ with $p \equiv 1 \mod 4$, two elements $a \pm bi$ with $a^2 + b^2 = p$.*

Exercise 1.34. *A domain R is a BF-domain if and only if $R[x]$ is a BF-domain.*

Exercise 1.35 (Grams's atomic non-ACCP domain)**.** *Let $(p_n)_{n\geq 0} = (3, 5, 7, \dots)$ be the sequence of odd prime numbers, define $t_n := \frac{1}{2^n p_n}$, and let $A = K[x^{t_n} : n \geq 0]$ with K a field. Let $S \subseteq A$ be the multiplicative set of all elements with nonzero constant term, and let $B := S^{-1}A := \{ f/g : f \in A, g \in S \}$.*

(1) *Every element r of the additive monoid generated by $(t_n)_{n\geq 0}$ has a unique representation of the form*

$$r = a + \sum_{i=0}^{N} a_n t_n$$

with $a = \frac{a'}{2^e}$ for some a', $e \in \mathbb{N}_0$ and $0 \leq a_n \leq p_n - 1$ for all n. Consequently, to r we can associate the unique element $\alpha(r) := a \in \mathbb{N}_0[\frac{1}{2}]$.

(2) *Suppose $f = \sum_{i=0}^{M} f_i x^{r_i} \in A^\bullet \setminus A^\times$, with pairwise distinct r_i and all $f_i \neq 0$, is such that $\alpha(r_i) = 0$ for some i. Let r_i be the smallest exponent with $\alpha(r_i) = 0$, and let $r_i = \sum_{n=0}^{N} a_n t_n$ be the unique representation of r_i as above. Show that any representation $f = g_1 \cdots g_k$ with $g_i \in A^\bullet \setminus A^\times$ satisfies $k \leq \sum_{n=0}^{N} a_n$.*

(3) *B is atomic.*

Exercise 1.36 (An ACCP non-BF domain)**.** *Let* $(p_n)_{n\geq 0} = (2, 3, 5, 7, \dots)$ *be the sequence of prime numbers, and let* $R = K[x^{1/p} : p \in \mathbb{P}]$ *with* K *a field.*

(1) *The exponent of every monomial has a unique representation of the form* $a_0 + \sum_{n=1}^{N} \frac{a_n}{p_n}$ *with* $a_0 \in \mathbb{N}_0$*, and* $0 \leq a_n \leq p_n - 1$ *for all* n*.*

(2) *Each* $x^{1/p}$ *is an atom in* R*.*

(3) *For* $f \in R^\bullet$*, let* $\beta(f)$ *be the exponent of the highest-degree monomial occurring in* f*. If* $g \mid f$*, then* $\beta(g) \leq \beta(f)$*, with equality only if* g *and* f *are associates. In particular, the domain* R *satisfies the ACCP.*

Exercise 1.37 (A noetherian non-FF domain)**.** *Let* $R = \mathbb{R} + x\mathbb{C}[x]$*.*

(1) *As* $\mathbb{R}$*-algebra, the ring* R *is generated by* x *and* ix*, so* R *is a noetherian domain by Hilbert's Basis Theorem.*

(2) R *is not an FF-domain, because* x^2 *has infinitely many essentially distinct factorizations.*

(3) *If* $f \in R$ *is an atom, then it is an atom in* $\mathbb{C}[x]$*. Thus, the ring* R *is half-factorial.*

Exercise 1.38 (A non-noetherian FF-domain)**.** *Let* $\mathrm{Int}(\mathbb{Z}) = \{ f \in \mathbb{Q}[x] : f(\mathbb{Z}) \subseteq \mathbb{Z} \}$ *denote the ring of integer-valued polynomials. For instance, for* $n \geq 2$ *we have* $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \in \mathrm{Int}(\mathbb{Z})$*, but* $\binom{x}{n} \notin \mathbb{Z}[x]$*.*

(1) $\mathrm{Int}(\mathbb{Z})$ *is an FF-domain.* (Hint*: write* $f \in \mathrm{Int}(\mathbb{Z})^\bullet$ *as* $f = g/d$ *with* $d \in \mathbb{N}$ *and* g *primitive.*)

(2) $\mathrm{Int}(\mathbb{Z})$ *is not noetherian.* (Hint*: the ideal generated by the family* $\left(\binom{x}{n}\right)_{n\geq 1}$ *is not finitely generated.*)

Exercise 1.39 (FF vs. half-factorial)**.** *In Exercise 1.37 we saw that* $\mathbb{R} + x\mathbb{C}[x]$ *is half-factorial but not an FF-domain. Show that* $\mathrm{Int}(\mathbb{Z})$ *and* $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$ *are FF-domains but not half-factorial.*

Exercise 1.40 (A non-Euclidean PID)**.** (1) *Suppose that* R *is a Euclidean domain with Euclidean norm function* $\delta : R^\bullet \to \mathbb{N}_0$*. If* q *minimizes* $\delta(q)$ *among all nonzero nonunits of* R*, then each* $r \in R$ *is congruent to* 0 *or a unit modulo* q*. In particular* $|R/qR| \leq |R^\times| + 1$*.*

(2) *The ring* $R := \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ *is not Euclidean.* (Hint*:* $|R/qR| \notin \{2, 3\}$ *for all* $q \in R$*. To see this, consider the minimal polynomial of* $(1 + \sqrt{-19})/2$ *modulo* 2 *and* 3*.*)

2 Dedekind Domains

We have seen that unique factorization of elements fails in many interesting domains. Dedekind domains are an important class of rings in which we can replace elements by ideals to recover unique factorization on a "higher level". In this chapter we give an introduction to Dedekind domains, in the spirit of a commutative algebra course.

2.1 Fractional Ideals

We need the notion of fractional ideals. Let R be a domain and K its field of fractions.

Definition 2.1. (1) *A* ***fractional*** R***-ideal*** *is a nonzero R-submodule I of K such that $dI \subseteq R$ for some nonzero $d \in R$. Let* $\mathrm{Frac}(R)$ *denote the set of fractional R-ideals.*

(2) *A fractional R-ideal I is* ***integral*** *if $I \subseteq R$. Let $\mathcal{I}(R)$ denote the set of integral R-ideals.*

(3) *A fractional R-ideal I is* ***invertible*** *if there exists a fractional R-ideal J such that $IJ = R$.*

(4) *A* ***principal fractional*** R***-ideal*** *is a fractional ideal of the form aR with $a \in K^\times$. The set of principal fractional R-ideals is denoted by* $\mathrm{FPrinc}(R)$.

The product IJ in (3) is understood to be the R-submodule of K generated by $\{ xy : x \in I, y \in J \}$. Integral R-ideals are precisely the nonzero ideals of R, and a fractional ideal is simply a set of the form $d^{-1}I$ with $d \in R^\bullet$ and I a nonzero ideal of R. For two fractional R-ideals I and J, the **colon ideal** is $(I{:}J) \coloneqq \{ a \in K : aJ \subseteq I \}$, and $I^{-1} \coloneqq (R{:}I)$.

Lemma 2.2. (1) *If I, J are fractional R-ideals, then IJ, $I \cap J$, $I + J$, and $(I : J)$ are also fractional R-ideals.*

(2) *The set* $\mathrm{Frac}(R)$ *is a monoid, with identity element R, and $\mathcal{I}(R)$ is a submonoid of* $\mathrm{Frac}(R)$.

(3) *If I is invertible, then I^{-1} is the unique inverse of I in* $\mathrm{Frac}(R)$. *In particular, the set of invertible fractional R-ideals is the unit group* $\mathrm{Frac}(R)^\times$.

Proof. (1) Let $0 \neq a \in I$, $0 \neq b \in J$, and let c, $d \in R^\bullet$ such that $cI \subseteq R$ and $dJ \subseteq R$. Then $ab \in IJ$ and $abcd \in I \cap J$, $a + b \in I + J$. Further $adJ \subseteq aR \subseteq I$, so $(I : J) \neq \mathbf{0}$. Next, we have $cdIJ \subseteq cIR \subseteq R$, $c(I \cap J) \subseteq R$, and $cd(I + J) \subseteq dR + cR \subseteq R$. Finally, also $cb(I{:}J) \subseteq cI \subseteq R$.

(2) Clear.

(3) Suppose $IJ = R$ for some $J \in \mathrm{Frac}(R)$. Then $J \subseteq I^{-1} = (R{:}I)$ by definition of the colon ideal. Conversely, multiplying $II^{-1} \subseteq R$ by J gives $I^{-1} = RI^{-1} = JII^{-1} \subseteq JR = J$. □

If $a \in K^\times$, then $(aR)^{-1} = a^{-1}R$ and $(aR)(a^{-1}R) = R$, so every principal fractional ideal is invertible. Note that if $IJ = aR$ for some $a \in K^\times$, then I and J are invertible, since $I(a^{-1}J) = R$ and $J(a^{-1}I) = R$.

The following lemma shows that, in noetherian rings, fractional ideals are just nonzero finitely generated R-submodules of K.

Lemma 2.3. (1) *If $0 \neq I \subseteq K$ is a finitely generated R-submodule, then I is a fractional R-ideal.*

(2) *If R is noetherian and $I \in \mathrm{Frac}(R)$, then I is a finitely generated R-submodule of K.*

(3) *If $I \in \mathrm{Frac}(R)$ is invertible, then I is a finitely generated R-submodule of K.*

Proof. (1) It suffices to show that $I^{-1} \neq \mathbf{0}$. Let $I = \langle a_1, \ldots, a_n \rangle_R$ with $a_i \in K$. Take $d \in R^\bullet$ such that $da_i \in R$ for all i. Then $dI \subseteq R$.

(2) Let $d \in R^\bullet$ be such that $dI \subseteq R$. Then $I \cong dI$, $x \mapsto dx$ is an R-module isomorphism. Since dI is an ideal of R, it is finitely generated, and hence so is I.

(3) We have $R = II^{-1}$, so there exist $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in I^{-1}$ such that $1 = a_1b_1 + \cdots + a_nb_n$. If $x \in I$, then $x = x \cdot 1 = x(a_1b_1 + \cdots + a_nb_n) = (xb_1)a_1 + \cdots + (xb_n)a_n$. Since $x \in I$ and $b_i \in I^{-1}$, we have $xb_i \in R$ for all i, and hence $x \in \langle a_1, \ldots, a_n \rangle_R$. □

2.2 A First Characterization

We recall the notions of integral elements and integral closure from commutative algebra. Given an extension of domains $R \subseteq S$, an element $s \in S$ is **integral** over R if there is a monic polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ such that $f(s) = 0$. Equivalently, there exists a finitely generated nonzero R-submodule M of S such that $sM \subseteq M$. Again equivalently, one can take $M = R[s] = \{ a_0 + a_1s + \cdots + a_ms^m : a_i \in R, m \geq 0 \}$. The **integral closure** of R in S is the set of all elements of S that are integral over R. One can show that this is a ring.

If R is a domain with field of fractions K, then the integral closure $\overline{R}$ of R is taken in K (unless otherwise specified). The domain R is **integrally closed** if $R = \overline{R}$.

Example 2.4. The ring $R = \mathbb{Z}[\sqrt{-23}]$ is not integrally closed in $\mathbb{Q}(\sqrt{-23})$, since $\frac{1+\sqrt{-23}}{2}$ satisfies the monic polynomial $x^2 - x + 6 \in \mathbb{Z}[x]$. In this example $\overline{R} = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$, and this is also the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-23})$ (Exercise 2.38). ○

We can give a first characterization and definition of Dedekind domains.

Theorem 2.5. *For a domain R, the following statements are equivalent.*

(a) *Every nonzero ideal of R is a product of prime ideals.*

(b) *Every fractional R-ideal is invertible.*

(c) *The ring R is noetherian, integrally closed, and every nonzero prime ideal is maximal.*

Definition 2.6. *A **Dedekind domain** is a domain that satisfies the equivalent conditions of Theorem 2.5.*

Remark 2.7. (1) The **Krull dimension** of a ring R, denoted by $\dim(R)$, is the supremum of the lengths n of chains $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ of prime ideals of R. Hence, in a domain, the condition that every nonzero prime ideal is maximal is equivalent to $\dim(R) \leq 1$.

(2) Fields are precisely the domains of Krull dimension 0. They are often excluded from the definition of Dedekind domains to avoid pathological examples.

Before proving the characterization, we need some preliminary lemmas. Let R be a domain.

Lemma 2.8. *If $P_1 \cdots P_m = Q_1 \cdots Q_n$ are two factorizations into invertible prime ideals, then $m = n$ and $P_i = Q_i$ after renumbering.*

Proof. By induction on m, the case $m = 0$ being clear. Without restriction, we assume that P_1 is minimal in $\{P_1, \ldots, P_m\}$ with respect to inclusion. Since $Q_1 \cdots Q_n \subseteq P_1$, we have $Q_j \subseteq P_1$ for some j, because P_1 is a prime ideal. After renumbering, we can assume $Q_1 \subseteq P_1$. Now $P_1 \cdots P_m \subseteq Q_1 \subseteq P_1$, and hence there is some i with $P_i \subseteq Q_1 \subseteq P_1$. By minimality of P_1, we have $P_i = P_1$, and hence $P_1 = Q_1$. Multiplying both sides by P_1^{-1} gives $P_2 \cdots P_m = Q_2 \cdots Q_n$, and the induction hypothesis implies the claim. □

Lemma 2.9. *If R is noetherian and integrally closed and $I \in \mathrm{Frac}(R)$, then $(I:I) = R$.*

Proof. Let $S \coloneqq (I:I)$. Note that S is an overring of R. Since R is noetherian and S is a fractional R-ideal, moreover S is a finitely generated R-module (Lemma 2.3). Therefore, the ring S is integral over R, and hence $S = R$, since R is integrally closed. □

Lemma 2.10. *Suppose R is noetherian and $I \in \mathcal{I}(R)$.*

(1) *The ideal I contains a product of nonzero prime ideals.*

(2) (*Jacobson*) *If R is at most one-dimensional and $I \neq R$, then $R \subsetneq I^{-1}$.*

Proof. (1) By noetherian induction. If this is not the case, then there exists a nonzero ideal I maximal with respect to not containing a product of nonzero prime ideals. Then I is not itself prime, and hence there exist $a, b \in R \setminus I$ such that $ab \in I$. Then there exist products of nonzero prime ideals $P_1 \cdots P_m \subseteq I + aR$ and $Q_1 \cdots Q_n \subseteq I + bR$. But then $P_1 \cdots P_m Q_1 \cdots Q_n \subseteq (I + aR)(I + bR) \subseteq I$, a contradiction.

(2) Let $0 \neq a \in I$. By (1) there exists a product of nonzero prime ideals $P_1 \cdots P_n \subseteq aR \subseteq I$. We can take such a product with n minimal (note $n \geq 1$ because $I \subsetneq R$). Let M be a maximal ideal containing I. Then $P_1 \cdots P_n \subseteq M$, and hence $P_i \subseteq M$ for some i, say $P_1 \subseteq M$ (recall that maximal ideals are prime). Since $\dim(R) \leq 1$, this means $P_1 = M$.

If $n = 1$, then $P_1 \subseteq aR \subseteq I \subseteq M$, and equality holds throughout. Hence, we have $I^{-1} = a^{-1}R \supsetneq R$.

If $n \geq 2$, then $P_2 \cdots P_n \nsubseteq aR$ by minimality of n. Let $b \in P_2 \cdots P_n \setminus aR$. Then $a^{-1}b \notin R$. However, we have $Ia^{-1}b \subseteq a^{-1}MP_2 \cdots P_n \subseteq a^{-1}aR \subseteq R$, so $a^{-1}b \in I^{-1} \setminus R$. □

Proof of Theorem 2.5. (a) ⇒ (b): (Matusita) It suffices to show that every nonzero prime ideal is invertible.

We first show that every invertible prime ideal is maximal. Suppose that P is an invertible prime ideal that is not maximal. Let $a \in R \setminus P$ be such that $P + aR \subsetneq R$. We can factor $P + aR = P_1 \cdots P_m$ and $P + a^2R = Q_1 \cdots Q_n$ into prime ideals with $m, n \geq 1$. Let $\pi\colon R \to R/P$ be the canonical epimorphism. Then

$$\pi(P + aR) = \pi(aR) = \pi(a)R/P = \pi(P_1) \cdots \pi(P_m),$$
$$\pi(P + a^2R) = \pi(a^2R) = \pi(a)^2R/P = \pi(Q_1) \cdots \pi(Q_n).$$

Each $\pi(P_i)$ and $\pi(Q_j)$ is a prime ideal of R/P and also invertible (since the products are nonzero and principal in R/P). Now $\pi(P_1)^2 \cdots \pi(P_m)^2 = \pi(Q_1) \cdots \pi(Q_n)$, and Lemma 2.8 shows uniqueness of this factorization.

Since the prime ideals of R/P bijectively correspond to prime ideals of R that contain P, we conclude $(P_1, P_1, P_2, P_2, \ldots, P_m, P_m) = (Q_1, Q_2, \ldots, Q_n)$ after renumbering. But then $P + a^2R = (P + aR)^2 \subseteq P^2 + aR$, and in particular $P \subseteq P^2 + aR$. Further $P \subseteq P^2 + aP = P(P + aR)$ (using that P is prime and $a \notin P$). The invertibility of P shows $R \subseteq P + aR$, a contradiction.

With the claim shown, let now P be a nonzero prime ideal of R. Let $0 \neq a \in P$ and factor $aR = P_1 \cdots P_n$ into prime ideals. Then each P_i is invertible. Since $P_1 \cdots P_n \subseteq P$, there exists some i with $P_i \subseteq P$. By the claim, the ideal P_i is maximal, and hence $P_i = P$. We conclude that P is invertible.

(b) ⇒ (c): By (3) of Lemma 2.3, every fractional ideal is finitely generated, and hence R is noetherian. Let now P be a nonzero prime ideal of R. Suppose that P is not maximal, and let $M \supsetneq P$ be a maximal ideal. Since $P = PM^{-1}M$ and P is prime, we find $PM^{-1} \subseteq P$. Then $M^{-1} = P^{-1}PM^{-1} \subseteq P^{-1}P = R$. But then $MM^{-1} \subseteq M$, contradicting $MM^{-1} = R$.

We still have to show that R is integrally closed. Let $s \in K$ be integral over R. Then the R-module $R[s]$ is finitely generated, and hence a fractional ideal (Lemma 2.3). By assumption, it is invertible, so $R[s]R[s]^{-1} = R$. Now

$$R[s] = R[s]R = R[s]R[s]R[s]^{-1} = R[s]R[s]^{-1} = R,$$

where we used $R[s]^2 = R[s]$, because $R[s]$ is a ring.

(c) ⇒ (a): We first show that every nonzero ideal is invertible. Let I be a nonzero ideal of R. Then II^{-1} also is a nonzero ideal of R, and $(II^{-1})(II^{-1})^{-1} \subseteq R$ implies $I^{-1}(II^{-1})^{-1} \subseteq I^{-1}$. This shows $(II^{-1})^{-1} \subseteq (I^{-1}\colon I^{-1}) = R$, with the last equality due to Lemma 2.9. By (2) of Lemma 2.10 applied to II^{-1}, this is only possible if $II^{-1} = R$, hence I is invertible.

Now suppose that not every nonzero ideal is a product of prime ideals. By noetherianity, there exists a nonzero ideal I that is maximal with respect to this property. Then I cannot be prime, and in particular not maximal. Let P be a maximal ideal with $I \subsetneq P$. Since P is

invertible, multiplying by P^{-1} gives $I \subsetneq IP^{-1} \subseteq PP^{-1} = R$. By maximal choice of I, the ideal IP^{-1} is a product of prime ideals, and hence so is $I = (IP^{-1})P$. □

Examples 2.11. (1) Every PID is a Dedekind domain: every nonzero (fractional) ideal is principal and hence invertible.

(2) A **number field** K is a finite field extension of $\mathbb{Q}$. The **ring of integers** $\mathcal{O}_K$ of K is the integral closure of $\mathbb{Z}$ in K. One can show that $\mathcal{O}_K$ is a Dedekind domain. (The non-trivial part is showing that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, from which it then follows that $\mathcal{O}_K$ is noetherian and one-dimensional.) For the special case of quadratic fields, see Exercises 2.38 and 2.39. In fact, rings of integers in number fields are the prototypical examples of Dedekind domains from which much of the theory was developed.

(3) The coordinate ring of a smooth affine irreducible algebraic curve is a Dedekind domain. For instance, if $y^2 = x^3 + ax + b$ is the Weierstrass equation of an elliptic curve E, then the coordinate ring $\mathbb{C}[E] = \mathbb{C}[x, y]/(y^2 - x^3 - ax - b)$ of E is a Dedekind domain. The nonzero prime ideals correspond precisely to points on E. Here, noetherianity is clear, one-dimensionality comes from E being a curve, and integral closure (that is, normality) follows from the smoothness of E. ○

2.3 Basic Properties

Now let R be a Dedekind domain. Combining Theorem 2.5 with Lemma 2.8, we see that every nonzero ideal of R can be *uniquely* factored into prime ideals. That is, each $I \in \mathcal{I}(R)$ can be written as $I = P_1^{n_1} \cdots P_m^{n_m}$ for some pairwise nonzero prime ideals $P_1, \ldots, P_m$ of R and some positive integers $n_1, \ldots, n_m$, and this factorization is unique up to renumbering of the prime ideals. Let $\mathcal{P}(R)$ denote the set of nonzero prime ideals of R.

Corollary 2.12. *The monoid $\mathcal{I}(R)$ is the free abelian monoid on the set $\mathcal{P}(R)$, and* $\mathrm{Frac}(R) = \mathrm{Frac}(R)^\times$ *is the free abelian group on $\mathcal{P}(R)$.*

Proof. Theorem 2.5 and Lemma 2.8 show the statement for $\mathcal{I}(R)$. Now $\mathrm{Frac}(R)$ is the group of fractions of $\mathcal{I}(R)$, and the free abelian group on a set is the group of fractions of the free abelian monoid on that set. □

Corollary 2.13. *Dedekind domains are FF-domains.*

Proof. It suffices to show that $(R^\bullet)_{\mathrm{red}}$ is an FF-monoid. For $a, b \in R^\bullet$, we have $aR = bR$ if and only if $aR^\times = bR^\times$, so $(R^\bullet)_{\mathrm{red}}$ is isomorphic the submonoid $\{ aR : a \in R^\bullet \}$ of the reduced FF-monoid $\mathcal{I}(R)$. Hence, the monoid $(R^\bullet)_{\mathrm{red}}$ is an FF-monoid by Proposition 1.32. □

Definition 2.14. *For $I \in \mathrm{Frac}(R)$ and P a nonzero prime ideal of R, let $\mathsf{v}_P(I) \in \mathbb{Z}$ denote the exponent of P in the unique factorization of I into prime ideals.*

More explicitly, every $I \in \mathrm{Frac}(R)$ can be written as $I = \prod_P P^{\mathsf{v}_P(I)}$, with the product taken over all nonzero prime ideals P of R (and $\mathsf{v}_P(I) = 0$ for all but finitely many P), and this representation is unique.

Lemma 2.15. *Let P be a nonzero prime ideal of R and I, $J \in \mathrm{Frac}(R)$.*

(1) *One has $\mathsf{v}_P(IJ) = \mathsf{v}_P(I) + \mathsf{v}_P(J)$.*

(2) *We have $I \subseteq J$ if and only if there exists $X \in \mathcal{I}(R)$ such that $I = JX$. Equivalently, we have $\mathsf{v}_P(I) \geq \mathsf{v}_P(J)$ for all $P \in \mathcal{P}(R)$.*

(3) *For I, $J \in \mathcal{I}(R)$, it holds that $I + J = \gcd(I, J)$ and $I \cap J = \mathrm{lcm}(I, J)$ in the free abelian monoid $\mathcal{I}(R)$.*

(4) *It holds that $\mathsf{v}_P(I + J) = \min\{\mathsf{v}_P(I), \mathsf{v}_P(J)\}$ and $\mathsf{v}_P(I \cap J) = \max\{\mathsf{v}_P(I), \mathsf{v}_P(J)\}$.*

Proof. (1) This is clear from the definition of $\mathsf{v}_P(I)$ and Corollary 2.12.

(2) If $I = JX$ for some $X \in \mathcal{I}(R)$, then clearly $I \subseteq J$. Conversely, if $I \subseteq J$, then $I = J(J^{-1}I)$, and $J^{-1}I$ is a fractional ideal of R. Since $I \subseteq J$, we have $J^{-1}I \subseteq J^{-1}J \subseteq R$, so $J^{-1}I \subseteq \mathcal{I}(R)$. Since $\mathrm{Frac}(R)$ is the free abelian group on $\mathcal{P}(R)$, clearly $I = JX$ with $X \in \mathcal{I}(R)$ if and only if $\mathsf{v}_P(I) \geq \mathsf{v}_P(J)$ for all $P \in \mathcal{P}(R)$.

(3) It is easy to see that $I + J$ is the least upper bound (supremum) of I and J in the partial order $\subseteq$ on $\mathrm{Frac}(R)$, and that $I \cap J$ is the greatest lower bound (infimum) of I and J in this partial order. By definition, the ideals $\gcd(I, J)$ and $\mathrm{lcm}(I, J)$ are the infimum, respectively, supremum of I and J with respect to the divisibility relation $\mid$ on $\mathcal{I}(R)$. Since $I \subseteq J$ if and only if $J \mid I$ by (2), the claim follows.

(4) Observing that $\mathrm{Frac}(R)$ is the free abelian group on $\mathcal{P}(R)$ and $\mathsf{v}_P(I)$ is simply the multiplicity of P in the factorization of I, the claim follows as in (3). □

Definition 2.16. *A **discrete valuation** on a field K is a surjective map $\mathsf{v}\colon K \to \mathbb{Z} \cup \{\infty\}$ with the following properties for all x, $y \in K$.*

(*i*) $\mathsf{v}(x) = \infty$ *if and only if* $x = 0$.

(*ii*) $\mathsf{v}(xy) = \mathsf{v}(x) + \mathsf{v}(y)$.

(*iii*) $\mathsf{v}(x + y) \geq \min\{\mathsf{v}(x), \mathsf{v}(y)\}$.

(*Here $\infty + n = \infty = \infty + \infty$ for all $n \in \mathbb{Z}$ and $\infty > n$ for all $n \in \mathbb{Z}$.*)

One easily sees $\mathsf{v}(1) = 0$ and $\mathsf{v}(x) = \mathsf{v}(-x)$ for $x \in K$. We also have the following important property.

Lemma 2.17. *If x, $y \in K$ and $\mathsf{v}(x) \neq \mathsf{v}(y)$, then $\mathsf{v}(x + y) = \min\{\mathsf{v}(x), \mathsf{v}(y)\}$.*

Proof. Without restriction assume $\mathsf{v}(x) < \mathsf{v}(y)$. Then

$$\mathsf{v}(x) = \mathsf{v}\big((x + y) - y\big) \geq \min\{\mathsf{v}(x + y), \mathsf{v}(y)\} \geq \min\{\mathsf{v}(x), \mathsf{v}(y)\} = \mathsf{v}(x).$$

We get $\min\{\mathsf{v}(x+y),\mathsf{v}(y)\} = \mathsf{v}(x)$, and since $\mathsf{v}(x) < \mathsf{v}(y)$, this means $\mathsf{v}(x+y) = \mathsf{v}(x) = \min\{\mathsf{v}(x),\mathsf{v}(y)\}$. □

Let K be the field of fractions of the Dedekind domain R. For each nonzero prime ideal P of R, we define $\mathsf{v}_P(a) \coloneqq \mathsf{v}_P(aR)$ for $a \in K^\times$ and $\mathsf{v}_P(0) = \infty$. (Note that v_P was previously defined on fractional ideals, but now we define a function with the same name on elements of K.) The map v_P is the **P-adic valuation** on K.

Lemma 2.18. *The P-adic valuation $\mathsf{v}_P\colon K \to \mathbb{Z}\cup\{\infty\}$ is a discrete valuation on K.*

Proof. The first property holds by definition. We check the remaining properties for $x, y \neq 0$, and leave the cases where one or both of x, y are zero to the reader. For the second property, we have $\mathsf{v}_P(xy) = \mathsf{v}_P(xyR) = \mathsf{v}_P(xRyR) = \mathsf{v}_P(xR) + \mathsf{v}_P(yR) = \mathsf{v}_P(x) + \mathsf{v}_P(y)$ by (1) of Lemma 2.15. Finally,

$$\mathsf{v}_P(x+y) = \mathsf{v}_P\big((x+y)R\big) \geq \mathsf{v}_P(xR+yR) = \min\{\mathsf{v}_P(xR),\mathsf{v}_P(yR)\} = \min\{\mathsf{v}_P(x),\mathsf{v}_P(y)\},$$

where we used $(x+y)R \subseteq xR+yR$ together with (2) of Lemma 2.15 for the inequality. □

We get a version of the Chinese Remainder Theorem for Dedekind domains.

Theorem 2.19 (Weak Approximation Theorem)**.** *Let $P_1, \ldots, P_n$ be pairwise distinct nonzero prime ideals of R and let $e_1, \ldots, e_n \in \mathbb{Z}$. Then there exists $x \in K^\times$ such that $\mathsf{v}_{P_i}(x) = e_i$ for all i, and $\mathsf{v}_P(x) \geq 0$ for all other nonzero prime ideals P of R.*

Proof. Let

$$J_i \coloneqq P_i^{e_i} \prod_{\substack{1\leq j\leq n\\ i\neq j}} P_j^{e_j+1}$$

for $1 \leq i \leq n$. Note that $P_iJ_i \subsetneq J_i$, with the inclusion being proper and minimal due to uniqueness of the factorization of ideals into prime ideals. Let $x_i \in J_i \smallsetminus P_iJ_i$. Then $\mathsf{v}_{P_i}(x_i) = e_i$ and $\mathsf{v}_{P_j}(x_i) \geq e_j + 1$ for $j \neq i$. Let $x \coloneqq x_1 + \cdots + x_n$. Then $\mathsf{v}_{P_i}(x) = e_i$ for all i by Lemma 2.17.

If $e_i \geq 0$ for all i, then we are done, since then $J_i \subseteq R$ and hence $x \in R$, so that $\mathsf{v}_P(x) \geq 0$ for all other nonzero prime ideals P of R.

Now let $e_i \in \mathbb{Z}$ be arbitrary. Let $\{Q_1,\ldots,Q_m\}$ be the set of nonzero prime ideals of R, different from $P_1, \ldots, P_n$, for which $f_j \coloneqq \mathsf{v}_{Q_j}(x) < 0$. Using the already established case of nonnegative valuations, we find $y \in R^\bullet$ such that $\mathsf{v}_{Q_j}(y) = -f_j$ for all j and $\mathsf{v}_{P_i}(y) = 0$ for all i. Then xy has the desired properties. □

2.4 The Class Group

Definition 2.20. *The **class group** (or **ideal class group**) of a Dedekind domain R is*

$$\mathrm{Cl}(R) \coloneqq \mathrm{Frac}(R)/\,\mathrm{FPrinc}(R).$$

Theorem 2.21. *For a Dedekind domain R, the following statements are equivalent.*
(a) *R is a PID.*
(b) *R is a factorial.*
(c) *The class group $\mathrm{Cl}(R)$ is trivial.*

Proof. (a) ⇒ (b) This is clear, because every PID is factorial.

(b) ⇒ (c) Since every nonzero ideal is a product of prime ideals, it suffices to show that every nonzero prime ideal is principal. Let $P \subseteq R$ be a nonzero prime ideal, and let $0 \neq a \in P$. Then $a = p_1 \cdots p_n$ for some prime elements $p_1, \ldots, p_n \in R$. Since P is prime, we have $p_i \in P$ for some i. Then $p_i R \subseteq P$. Because $\dim(R) \leq 1$, already $p_i R$ is maximal, and so $P = p_i R$.

(c) ⇒ (a) If I is a nonzero ideal of R, then triviality of the class group implies $I = ab^{-1}R$ for some $a, b \in R^\bullet$. But $ab^{-1} \in R$ implies that we can take $b = 1$, and hence $I = aR$ is principal. □

2.5 Discrete Valuation Rings

If K is a field and $\mathsf{v}\colon K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation on K, then the set $R_\mathsf{v} := \{\, x \in K : \mathsf{v}(x) \geq 0 \,\}$ is a ring, called the **valuation ring** of v.

Definition 2.22. *A **discrete valuation ring** (**DVR**) is a ring of the form R_v for some field K and some discrete valuation v on K.*

A ring R is **local** if it has a unique maximal ideal.

Proposition 2.23. *Let $R = R_\mathsf{v}$ be a DVR.*

(1) *We have $R^\times = \{\, x \in K : \mathsf{v}(x) = 0 \,\}$. If $\pi \in R$ is such that $\mathsf{v}(\pi) = 1$, then every element $x \in K^\times$ has a unique representation $x = \varepsilon\pi^n$ with $\varepsilon \in R^\times$ and $n \in \mathbb{Z}$. In particular, the ring R is factorial with a unique (up to associates) prime element π.*

(2) *The ring R is local with maximal ideal $M_\mathsf{v} := \{\, x \in K : \mathsf{v}(x) > 0 \,\}$.*

(3) *If I is a nonzero ideal of R and $x \in I$ is such that $\mathsf{v}(x) = \min\{\, \mathsf{v}(y) : y \in I \,\}$, then $I = xR$. In particular, the nonzero ideals of R are precisely the ideals*

$$M_\mathsf{v}^n = \{\, x \in K : \mathsf{v}(x) \geq n \,\} = \pi^n R \quad \text{for } n \geq 0.$$

Proof. (1) If $\varepsilon \in R^\times$, then $\varepsilon\varepsilon^{-1} = 1$, and hence $\mathsf{v}(\varepsilon) + \mathsf{v}(\varepsilon^{-1}) = 0$, so $\mathsf{v}(\varepsilon) = 0$. Conversely, if $\varepsilon \in K$ with $\mathsf{v}(\varepsilon) = 0$, then also $\mathsf{v}(\varepsilon^{-1}) = 0$, and hence $\varepsilon^{-1} \in R$.

Let $x \in K^\times$ and $n := \mathsf{v}(x)$. Then $\varepsilon := x\pi^{-n} \in R$ has valuation 0, hence $\varepsilon \in R^\times$, and the existence of the representation follows. Uniqueness follows because necessarily $n = \mathsf{v}(x)$, and then $\varepsilon = x\pi^{-n}$ is determined by x and n. Now clearly π is a prime element of R and factoriality follows.

(2) The properties of a discrete valuation imply that M_v is a proper ideal of R. Since $R \setminus M_\mathsf{v} = R^\times$, the ideal M_v is the unique maximal ideal, and hence R is local.

(3) If $z \in I$, then $\mathsf{v}(z) \geq \mathsf{v}(x)$, and hence $zx^{-1} \in R$, so $z = (zx^{-1}) \in xR$. Thus, we have $I = xR$. Since, up to associates, the nonzero elements of R are of the form π^n, it follows that the only ideals are $\pi^n R$ for $n \geq 0$, and that these are all distinct. □

Theorem 2.24. *For a domain R, the following statements are equivalent.*

(a) *R is a DVR.*

(b) *R is a local PID that is not a field.*

(c) *R is a local Dedekind domain that is not a field.*

(d) *R is a factorial domain with a unique (up to associates) prime element.*

Proof. (a) ⇒ (b) By Proposition 2.23, the ring R is a local PID. It is not a field, because $M_{\mathsf{v}} \neq \mathbf{0}$, since v is surjective.

(b) ⇒ (c) Every PID is a Dedekind domain.

(c) ⇒ (d) Let P be the unique maximal ideal of R. Since R is not a field, the ideal P is nonzero. Since R is a Dedekind domain, then $P \neq P^2$, and we can take $\pi \in P \smallsetminus P^2$ (or use Theorem 2.19 to find such a $\pi \in R$). Then $P = \pi R$, and this is the unique nonzero prime ideal of R. In particular, the element π is a prime element. If $0 \neq a \in R$, then $aR = P^n$ for some $n \geq 0$, and hence $aR = \pi^n R$, so $a = \pi^n \varepsilon$ for some $\varepsilon \in R^\times$. This shows that R is factorial with unique prime element π, up to associates.

(d) ⇒ (a) Let π be a prime element of R. Every $x \in K^\times$ has the form $x = \varepsilon\pi^n$ for some $\varepsilon \in R^\times$. It is easy to check that $\mathsf{v}\colon K \to \mathbb{Z} \cup \{\infty\}$ defined by $\mathsf{v}(x) = n$ if $x = \varepsilon\pi^n$ and $\mathsf{v}(0) = \infty$ is a discrete valuation on K, and that $R = R_{\mathsf{v}}$. □

2.6 A Local Characterization of Dedekind Domains

Let R be a domain with field of fractions K. Let $\operatorname{Spec}(R)$ denote the set of prime ideals of R, let $\mathcal{P}(R)$ denote the set of nonzero prime ideals of R, and let $\operatorname{Max}(R)$ denote the set of maximal ideals of R.

We recall basic facts about localizations of domains that are easy to check, see any text on commutative algebra for more details.

Remark 2.25. Let $S \subseteq R^\bullet$ be a multiplicative subset (meaning $1 \in S$ and $SS \subseteq S$).

(1) The **localization** of R by S is the ring

$$S^{-1}R = \left\{ \frac{r}{s} \in K : r \in R, s \in S \right\}.$$

The inclusion $R \hookrightarrow S^{-1}R$ is universal with respect to ring homomorphisms from R that send elements of S to units.

(2) If $I \in \operatorname{Frac}(R)$, then $S^{-1}I \coloneqq \{ \frac{x}{s} \in K : x \in I, s \in S \} = \langle I \rangle_{S^{-1}R} = I(S^{-1}R)$ and $S^{-1}I \in \operatorname{Frac}(S^{-1}R)$. Then $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$, $S^{-1}(I + J) = S^{-1}I + S^{-1}J$, and $S^{-1}(I \cap J) =$

$S^{-1}I \cap S^{-1}J$ for $I, J \in \mathrm{Frac}(R)$. In particular, the induced map $\mathrm{Frac}(R) \to \mathrm{Frac}(S^{-1}R)$ is a monoid homomorphism and hence maps $\mathrm{Frac}(R)^\times$ to $\mathrm{Frac}(S^{-1}R)^\times$.

(3) If I is an ideal of R, then $S^{-1}I$ is an ideal of $S^{-1}R$ and $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \varnothing$. If J is an ideal of $S^{-1}R$, then $J \cap R$ is an ideal of R and $S^{-1}(J \cap R) = J$. In particular, we have $\mathcal{F}(S^{-1}R) = \{ S^{-1}I : I \in \mathcal{F}(R) \}$ and $\mathcal{I}(S^{-1}R) = \{ S^{-1}I : I \in \mathcal{I}(R) \}$. Moreover, if R is noetherian then so is $S^{-1}R$.

(4) There is a bijection

$$\{ P \in \mathrm{Spec}(R) : P \cap S = \varnothing \} \to \mathrm{Spec}(S^{-1}R), \quad P \mapsto S^{-1}P.$$

The inverse map is given by $Q \mapsto Q \cap R$.

(5) If P is a prime ideal of R then $S \coloneqq R \setminus P$ is multiplicative subset, and we write R_P instead of $S^{-1}R$ (and analogously for ideals and fractional ideals). In this case, the ring R_P is local with maximal ideal PR_P.

There are two slightly less trivial properties that we will need.

Lemma 2.26. *If $I \in \mathrm{Frac}(R)$ is finitely generated, then $(S^{-1}I)^{-1} = S^{-1}(I^{-1})$.*

Proof. From $II^{-1} \subseteq R$, we get $S^{-1}I \cdot S^{-1}I^{-1} = S^{-1}(II^{-1}) \subseteq S^{-1}R$, so $S^{-1}I^{-1} \subseteq (S^{-1}I)^{-1}$. Conversely, if $I = \langle a_1, \ldots, a_n \rangle_R$, then $S^{-1}I = \langle a_1, \ldots, a_n \rangle_{S^{-1}R}$. If $x \in (S^{-1}I)^{-1}$, then $xa_i = b_i t^{-1}$ for all $1 \leq i \leq n$ some $b_i \in R$ and $t \in S$. Then $txa_i = b_i \in R$, and hence $tx \in I^{-1}$, so $x \in S^{-1}(I^{-1})$. □

Lemma 2.27. *If I is an R-submodule of K, then*

$$I = \bigcap_{P \in \mathrm{Spec}(R)} I_P = \bigcap_{M \in \mathrm{Max}(R)} I_M.$$

Proof. It suffices to show $\bigcap_{M \in \mathrm{Max}(R)} I_M \subseteq I$, as the inclusions $I \subseteq \bigcap_{P \in \mathrm{Spec}(R)} I_P \subseteq \bigcap_{M \in \mathrm{Max}(R)} I_M$ are clear. Let $x \in \bigcap_{M \in \mathrm{Max}(R)} I_M$ and let $J \coloneqq \{ r \in R : rx \in I \}$. Then J is an ideal of R. If $x \notin I$, then J is proper and there exists a maximal ideal M of R with $J \subseteq M$. However, since $x \in I_M$, we have $sx \in I$ for some $s \in R \setminus M$, so $J \notin M$, a contradiction. □

Lemma 2.28. *Let $I \in \mathrm{Frac}(R)$. Then I is invertible if and only if I is finitely generated and locally principal (meaning that I_P is a principal ideal of R_P for every prime ideal P of R).*

Proof. First suppose that I is invertible. Then I is finitely generated by (3) of Lemma 2.3, and we have to show it is locally principal. Localizing, we get $R_P = (II^{-1})_P = I_P(I^{-1})_P$, so I_P is invertible as a fractional ideal of R_P. Noting that $S \coloneqq R_P$ is a local ring, it now suffices to show that every invertible fractional ideal of a local ring is principal. Let $J \in \mathrm{Frac}(S)^\times$ and let M be the unique maximal ideal of S. Since J is invertible, then $J \notin JM$ (otherwise $R \subseteq M$). Let $x \in J \setminus JM$. Then xJ^{-1} is an ideal of R, and $xJ^{-1} \notin M$. Thus, necessarily $R = xJ^{-1}$, and so $J = xJ^{-1}J = xR$ is principal.

In the other direction, let I be finitely generated and locally principal. Lemma 2.26 implies $(I^{-1})_P = I_P^{-1}$ for every prime ideal P of R. Using that each I_P is principal, hence invertible,

$$(II^{-1})_P = I_P(I^{-1})_P = I_P(I_P)^{-1} = R_P,$$

and so Lemma 2.27 shows $II^{-1} = R$. □

Theorem 2.29. *A domain R is a Dedekind domain if and only if it is noetherian and R_P is a DVR for every nonzero prime ideal P of R.*

Proof. First suppose that R is a Dedekind domain. By Theorem 2.24, it suffices to show that R_P is a Dedekind domain for each $P \in \mathcal{P}(R)$. To do so, it suffices to show that every nonzero ideal I of R_P is invertible. Let I be a nonzero ideal of R_P and let $J \coloneqq I \cap R$. Then $I = J_P$ and J is a nonzero ideal of R. Since R is a Dedekind domain, we have $JJ^{-1} = R$. Localizing shows $R_P = (JJ^{-1})_P = J_P(J^{-1})_P = I(J^{-1})_P$, so I is invertible.

Now suppose that R is noetherian and R_P is a DVR for every $P \in \mathcal{P}(R)$. Let $I \in \operatorname{Frac}(R)$. Then I is finitely generated, and it is locally principal, since each R_P is a DVR, and hence a PID. Lemma 2.28 shows that I is invertible. □

2.7 A Module-Theoretic Characterization

We now give a module-theoretic (homological) characterization of Dedekind domains. We recall the notion of projective modules (it can be found in any text covering commutative algebra or homological algebra).

Proposition 2.30. *Let R be a ring. For an R-module P, the following statements are equivalent.*

(a) *The functor $\operatorname{Hom}_R(P, -)$ is exact, that is, for every short exact sequence of R-modules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

the sequence

$$0 \longrightarrow \operatorname{Hom}_R(P, A) \longrightarrow \operatorname{Hom}_R(P, B) \longrightarrow \operatorname{Hom}_R(P, C) \longrightarrow 0$$

is exact.

(b) *For every R-epimorphism $f\colon A \to B$ and every homomorphism $g\colon P \to B$, there exists a homomorphism $h\colon P \to A$ such that $f \circ h = g$.*

(c) *Every R-epimorphism $g\colon A \to P$ splits, that is, there exists a homomorphism $h\colon P \to A$ such $g \circ h = \mathrm{id}_P$.*

(d) *P is a direct summand of a free R-module. (Explicitly, there exists an R-module Q such that $P \oplus Q \cong R^{(X)}$ for some index set X.)*

Definition 2.31. *A module is **projective** if it satisfies the equivalent conditions of the previous proposition.*

We can characterize projective ideals in a domain.

Lemma 2.32. *If R is a domain and $I \in \mathrm{Frac}(R)$, then $I^{-1} \cong \mathrm{Hom}_R(I, R)$.*

Proof. If $y \in I^{-1}$, then $m_y : I \to R$, $x \mapsto xy$ is an R-module homomorphism. We claim that the homomorphism $\varphi : I^{-1} \to \mathrm{Hom}_R(I, R)$, $y \mapsto m_y$ is an isomorphism (it is straightforward to check that it is a homomorphism).

To show injectivity of φ, let $y \in I^{-1}$ with $m_y = 0$. Let $0 \neq x \in I$. Then $m_y(x) = yx = 0$, so $y = 0$ since R is a domain. We conclude that φ is injective.

To show surjectivity, let $f \in \mathrm{Hom}_R(I, R)$. Now fix $0 \neq x \in I$ and let $y := f(x)x^{-1}$. We claim $y \in I^{-1}$ and $f = m_y$. Indeed, let $0 \neq x' \in I$ and $d \in I^{-1}$. Then $x'df(x) = f(xx'd) = f(x')xd$. Cancelling d, we find $f(x')(x')^{-1} = f(x)x^{-1} = y$, so $f(x') = yx'$ for all $x' \in I$. Since $f(x') \in R$, this also shows $y \in I^{-1}$. □

Proposition 2.33. *Let R be a domain. If $I \in \mathrm{Frac}(R)$, then I is invertible if and only if it is projective as R-module.*

Proof. Suppose first that I is invertible. Then $II^{-1} = R$, so there exist $x_1, \ldots, x_n \in I$ and $y_1, \ldots, y_n \in I^{-1} = (R : I)$ such that $1 = x_1y_1 + \cdots + x_ny_n$. First note that $I = \langle x_1, \ldots, x_n \rangle_R$. Indeed, if $r \in I$, then $r = r \cdot 1 = (ry_1)x_1 + \cdots + (ry_n)x_n$ and $ry_i \in R$ since $y_i \in I^{-1}$. Thus, the map $f : R^n \to I$ defined by $f(r_1, \ldots, r_n) = r_1x_1 + \cdots + r_nx_n$, is an epimorphism of R-modules.

For every i, the assignment $r \mapsto ry_i$ defines a homomorphism $I \mapsto R$. Let $g : I \to R^n$ be defined by $g(r) = (ry_1, \ldots, ry_n)$. Then $f \circ g = \mathrm{id}_I$, so the epimorphism f splits. Therefore, the ideal $I \simeq g(I)$ is a direct summand of the free R-module R^n, and hence is projective.

Conversely, suppose that I is projective. Let $f : R^{(X)} \to I$ be an epimorphism of R-modules. It has the form $f\big((r_n)_{n\in X}\big) = \sum_{n\in X} r_nx_n$ with elements $x_n \in I$. Since I is projective, there exists a homomorphism $g : I \to R^{(X)}$ such that $f \circ g = \mathrm{id}_I$. Here g has the form $g(r) = (g_n(r))_{n\in X}$ with homomorphisms $g_n : I \to R$ and with the property that for each $r \in I$ only finitely many $g_n(r)$ are nonzero. By Lemma 2.32, each g_n has the form $g_n(r) = ry_n$ for some $y_n \in I^{-1}$. In particular, the set X is finite. Now let $0 \neq d \in I$. Then $d = f \circ g(d) = \sum_{n\in X} g_n(d)x_n = \sum_{n\in X} dy_nx_n$. Cancelling d, we find $1 \in I^{-1}I$. □

This gives an additional characterization of Dedekind domains.

Definition 2.34. *A ring R is **hereditary** if every ideal of R is projective as an R-module.*

Remark 2.35. By an inductive argument, one can show that a ring is hereditary of and only if every submodule of a projective module is projective, but we will not need this fact.

Corollary 2.36. *A domain R is a Dedekind domain if and only if it is hereditary.*

Proof. Immediate from the definitions and Proposition 2.33. □

Remark 2.37. Let M be an R-module. The **projective dimension** of M, denoted by $\mathrm{pd}(M) \in \mathbb{N}_0 \cup \{\infty\}$, is the smallest integer $n \geq 0$ such that there exists a projective resolution of M of length n, that is, an exact sequence

$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

with P_i projective R-modules. If no such n exists, then $\mathrm{pd}(M) \coloneqq \infty$. Then the **global dimension** of R is $\mathrm{gldim}(R) \coloneqq \sup\{\, \mathrm{pd}(M) : M \text{ is an } R\text{-module} \,\}$. A ring is hereditary if and only if $\mathrm{gldim}(R) \leq 1$, so Dedekind domains are the domains of global dimension at most 1. (The domains of global dimension 0 are precisely the fields.)

2.8 Exercises

Exercise 2.38. *Let $d \in \mathbb{Z}$ be a squarefree integer (this excludes $d = 1$ by definition). Let $K \coloneqq \mathbb{Q}(\sqrt{d})$ be the corresponding quadratic number field, and denote by $\mathcal{O}_K$ the integral closure of $\mathbb{Z}$ in K (this is called the **ring of integers** of K). Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Exercise 2.39. *The rings $\mathcal{O}_K$ from the Exercise 2.38 are Dedekind domains.*

Exercise 2.40. *A ring R is called semilocal if it has only finitely many maximal ideals. For a semilocal domain R, a fractional ideal $I \in \mathrm{Frac}(R)$ is invertible if and only if I is principal. In particular, semilocal Dedekind domains are PIDs. (An easier version of this exercise is to only show the final claim.)*

Exercise 2.41 ($1\frac{1}{2}$-generator property)**.** (1) *If R is a Dedekind domain, I is a nonzero ideal of R, and $0 \neq a \in I$, then there exists $b \in I$ such that $I = aR + bR$.*

(2) *The previous property characterizes Dedekind domains among domains.*

3 Divisor Theories and a Transfer Principle

Recall the example

$$8 = 2 \cdot 2 \cdot 2 = \frac{3+\sqrt{-23}}{2} \cdot \frac{3-\sqrt{-23}}{2} \tag{3.1}$$

in the Dedekind domain $D \coloneqq \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$. The principal ideals generated by the atoms can be factored into prime ideals as

$$(2) = PQ, \quad \left(\frac{3+\sqrt{-23}}{2}\right) = P^3, \quad \left(\frac{3-\sqrt{-23}}{2}\right) = Q^3,$$

where P and Q are two distinct non-principal prime ideals, namely $P = (2, \frac{1+\sqrt{-23}}{2})$ and $Q = (2, \frac{1-\sqrt{-23}}{2})$.[1] Then $(8) = P^3Q^3$. We can factor 8 by first factoring the ideal (8) into prime ideals and then grouping the prime ideals into products that are principal.

It turns out that PQ, P^3, and Q^3 are principal, while P^2 and Q^2 are not. A systematic way of understanding this is to use the class group: it is possible to compute that $\mathrm{Cl}(D) \cong \mathbb{Z}/3\mathbb{Z}$, with $[P]$ mapping to $\overline{1}$ and $[Q]$ mapping to $\overline{2}$. Then

$$[P^i] = i[P] = i\overline{1} = \overline{i} \in \mathbb{Z}/3\mathbb{Z},$$

so P^i is principal if and only if i is a multiple of 3, and the same applies to Q^i. Moreover, the product PQ is principal, since $[P] + [Q] = \overline{1} + \overline{2} = \overline{0}$.

From these considerations we see that the factors in (3.1) are indeed atoms and that these are (up to order and associates) the only factorizations of 8 in D.

In this chapter we develop these ideas in a more systematic fashion.

3.1 Divisor Homomorphisms

To be able to reuse the results in more generality later, we introduce the notion of a divisor theory as an abstraction of the situation we encounter in Dedekind domains.

Definition 3.1. *Let H and D be monoids.*

[1] The actual generators are not important. For the details of this computation, see any textbooks on algebraic number theory. It can be performed by hand or with a computer algebra system such as Magma, Pari/GP or SageMath.

(1) *A **divisor homomorphism** is a monoid homomorphism $\varphi\colon H \to D$ such that for all $a, b \in H$, if $\varphi(a) \mid \varphi(b)$ in D, then $a \mid b$ in H.*

(2) *A submonoid $H \subseteq D$ is **saturated** if the inclusion map is a divisor homomorphism.*

(3) *A **divisor theory** is a divisor homomorphism $\varphi\colon H \to D$ with $D = \mathcal{F}(P)$ a free abelian monoid and such that for every $p \in P$ there exists a finite nonempty subset $X \subseteq H$ such that $p = \gcd(\varphi(X))$.*

In Dedekind domains, the ideal theory gives a divisor theory.

Proposition 3.2. *If R is a Dedekind domain, then $\varphi\colon R^\bullet \to \mathcal{I}(R)$, $a \mapsto aR$ is a divisor theory.*

Proof. Let $a, b \in R^\bullet$. If aR divides bR in $\mathcal{I}(R)$, then there exists an ideal I such that $aR \cdot I = bR$. Then $I = a^{-1}bR$, showing that $a^{-1}b \in R^\bullet$. This means that a divides b in $R^\bullet$, and so φ is a divisor homomorphism.

To verify that φ is a divisor theory, let $P \in \mathcal{P}(R)$ (keep in mind $\mathcal{I}(R) = \mathcal{F}(\mathcal{P}(R))$). Since R is noetherian, there exist $a_1, \ldots, a_n \in R^\bullet$ such that $P = \langle a_1, \ldots, a_n \rangle_R$. Then $P = a_1R + \cdots + a_nR = \gcd(a_1R, \ldots, a_nR)$ in $\mathcal{I}(R)$ by Lemma 2.15. □

Given a monoid H, we can form the **group of fractions** (or **quotient group**) $\mathbf{q}(H) = \{ ab^{-1} : a, b \in H \}$ using the usual pair construction, which we know from the construction of the field of fractions of an integral domain: the elements of $\mathbf{q}(H)$ are equivalence classes of pairs of $H \times H$ with $(a, b) \sim (c, d)$ if $ad = bc$. We represent the equivalence class of (a, b) by the symbol ab^{-1} and identify H with the subset $a1^{-1}$, so that $H \subseteq \mathbf{q}(H)$.

Definition 3.3. *If $\varphi\colon H \to D$ is a divisor homomorphism, then its **class group** is*

$$\mathrm{Cl}(\varphi) \coloneqq \mathbf{q}(D)/\mathbf{q}(\varphi(H)).$$

Example 3.4. If R is a Dedekind domain, and φ is the natural divisor theory $\varphi\colon R^\bullet \to \mathcal{I}(R)$, then

$$\mathrm{Cl}(\varphi) = \mathbf{q}(\mathcal{I}(R))/\mathbf{q}(\{aR : a \in R^\bullet\}) = \mathrm{Frac}(R)/\mathrm{FPrinc}(R) = \mathrm{Cl}(R)$$

is just the class group that we encountered in the previous chapter. ○

We observe two basic properties.

Lemma 3.5. *Let $\varphi\colon H \to D$ be a divisor homomorphism. Then*

(1) *$\mathbf{q}(\varphi(H)) \cap D = \varphi(H)$; and*

(2) *if $d \in D$, then $d \in \varphi(H)$ if and only if $[d] = 0$ in $\mathrm{Cl}(\varphi)$.*

Proof. (1) We always have $\varphi(H) \subseteq \mathbf{q}(\varphi(H)) \cap D$, so we have to show $\mathbf{q}(\varphi(H)) \cap D \subseteq \varphi(H)$.

Let $\varphi(a)\varphi(b)^{-1} \in \mathbf{q}(\varphi(H)) \cap D$ with $a, b \in H$. Then $\varphi(a)\varphi(b)^{-1} = d$ for some $d \in D$, so $\varphi(a) = d\varphi(b)$. Since φ is a divisor homomorphism, also b divides a in H, that is $a = bc$ for some $c \in H$. Now $\varphi(a) = \varphi(b)\varphi(c) = \varphi(b)d$, and so $d = \varphi(c) \in \varphi(H)$.

(2) If $d \in H$, then clearly $[d] = 0$. Conversely, if $[d] = 0$, then $d \in \mathbf{q}(\varphi(H)) \cap D = \varphi(H)$ by the first part. □

3.2 Transfer Homomorphisms

A divisor theory allows us to reduce the study of the factorization of a given element to the factorization of its image into prime elements, together with an analysis of which products of the corresponding prime elements actually arise from H (using the class group). This is great if we care about the factorizations of a specific element, but not yet so helpful if we want to understand global arithmetic invariants of H.

This is where transfer homomorphism come into play: the idea is to substitute for H a simpler model T that preserves enough of the arithmetic of H to be able to deduce results about H from results about T.

Definition 3.6. *A **transfer homomorphism** is a monoid homomorphism $\theta\colon H \to T$ having the following properties.*

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

(T2) *If $a \in H$ and $s, t \in T$ are such that $\theta(a) = st$, then there exist $b, c \in H$ such that $a = bc$, $\theta(b) \simeq s$, and $\theta(c) \simeq t$.*

We gather the basic properties of transfer homomorphisms in the following proposition.

Proposition 3.7. *Let $\theta\colon H \to T$ be a transfer homomorphism and $a \in H$.*

(1) *If $\theta(a) \simeq s_1 \cdots s_n$ for some $n \ge 0$ and $s_1, \ldots, s_n \in T$, then there exist $b_1, \ldots, b_n \in H$ such that $a \simeq b_1 \cdots b_n$ and $\theta(b_i) \simeq s_i$ for all $1 \le i \le n$.*

(2) *The element a is an atom of H if and only if $\theta(a)$ is an atom of T.*

(3) *On the level of factorization monoids, there is a unique induced homomorphism $\overline{\theta}\colon \mathsf{Z}(H) \to \mathsf{Z}(T)$ such that $\overline{\theta}(uH^\times) = \theta(u)T^\times$ for all atoms $u \in H$. Moreover, the following hold.*

   (*i*) *The following commutative diagram commutes.*

$$\begin{array}{ccc} \mathsf{Z}(H) & \xrightarrow{\overline{\theta}} & \mathsf{Z}(T) \\ {\scriptstyle \pi_H}\downarrow & & \downarrow{\scriptstyle \pi_T} \\ H_{\mathrm{red}} & \xrightarrow{\theta_{\mathrm{red}}} & T_{\mathrm{red}} \end{array}$$

   (*ii*) $\overline{\theta}(\mathsf{Z}_H(a)) = \mathsf{Z}_T(\theta(a))$ *and $\overline{\theta}$ is surjective.*

   (*iii*) *H is atomic if and only T is atomic.*

   (*iv*) *For $z, z' \in \mathsf{Z}(H)$, we have $|\overline{\theta}(z)| = |z|$ and $\mathsf{d}(\overline{\theta}(z), \overline{\theta}(z')) \le \mathsf{d}(z, z')$.*

(v) *If* $z \in \mathsf{Z}_H(a)$ *and* $\overline{y} \in \mathsf{Z}_T(\theta(a))$, *then there exists* $y \in \mathsf{Z}_H(a)$ *such that* $\overline{\theta}(y) = \overline{y}$, *such that* $\overline{\theta}(\gcd(z,y)) = \gcd(\overline{\theta}(z), \overline{y})$, *and* $\mathsf{d}(z,y) = \mathsf{d}(\overline{\theta}(z), \overline{y})$.

(vi) $\mathsf{L}_T(\theta(a)) = \mathsf{L}_H(a)$ *and* $\mathcal{L}(H) = \mathcal{L}(T)$.

Proof. For $a \in H$ we denote by $[a] = aH^\times \in H_{\mathrm{red}}$ the associativity class, and similarly in T. If $\theta\colon H \to T$ is a monoid homomorphism, then it induces $\theta_{\mathrm{red}}\colon H_{\mathrm{red}} \to T_{\mathrm{red}}$, given by $\theta_{\mathrm{red}}([a]) = [\theta(a)]$ for all $a \in H$.

(1) For $n = 0$, the claim follows from (T1), as $a \in H^\times$ if and only if $\theta(a) \in T^\times$. For $n = 1$ it is trivial. For $n \ge 1$, the claim follows using (T2) and induction on n (replacing s_1 by an associate, we can without restriction assume $\theta(a) = s_1 \cdots s_n$).

(2) Let $a \in H$ be an atom. Then $\theta(a) \notin T^\times$ by (T1). If $\theta(a) = st$ for some $s, t \in T$, then $a = bc$ with $\theta(b) \simeq s$ and $\theta(c) \simeq t$ by (T2). Without restriction, then $b \in H^\times$, and so $s \in T^\times$.

Conversely, suppose $\theta(a)$ is an atom of T. Since $\theta(a) \notin T^\times$, we see $a \notin H^\times$. Let $a = bc$ with $b, c \in H$. Since $\theta(a) = \theta(b)\theta(c)$, without restriction $\theta(b) \in T^\times$. Using (T1), we see $b \in H^\times$.

(3) Existence and uniqueness of $\overline{\theta}$ follows from $\mathsf{Z}(H)$ being the free abelian monoid on $\mathcal{A}(H_{\mathrm{red}})$, and (i) is a simple consequence of θ being a homomorphism: if $z = [u_1] \cdots [u_k]$ with $u_i \in \mathcal{A}(H)$, then $\pi_T(\overline{\theta}(z)) = [\theta(u_1)] \cdots [\theta(u_k)] = [\theta(u_1 \cdots u_k)] = \theta_{\mathrm{red}}(\pi_H(z))$.

(ii) By commutativity of the diagram, the map $\overline{\theta}$ restricts to a map $\mathsf{Z}_H(a) \to \mathsf{Z}_T(\theta(a))$. Let $z = [s_1] \cdots [s_n] \in \mathsf{Z}_T(\theta(a))$ with $s_1, \ldots, s_n \in \mathcal{A}(T)$ and $n \ge 0$. Then $\theta(a) \simeq s_1 \cdots s_n$. By (1), there exist $b_1, \ldots, b_n \in H$ such that $a \simeq b_1 \cdots b_n$ and $\theta(b_i) \simeq s_i$ for all $1 \le i \le n$. Then $\overline{\theta}([b_1] \cdots [b_n]) = z$, so $\overline{\theta}(\mathsf{Z}_H(a)) = \mathsf{Z}_T(\theta(a))$.

Now if $[s] \in T_{\mathrm{red}}$ with $s \in T$ is arbitrary, then without restriction, we can choose $s \in \theta(H)$ by (T1). If $s = \theta(a)$, then $\mathsf{Z}_T(s) = \overline{\theta}(\mathsf{Z}_H(a))$ by the first part. Since $\mathsf{Z}(T) = \bigcup_{s \in T} \mathsf{Z}_T(s)$, we see that $\overline{\theta}$ is surjective.

(iii) Note that H is atomic if and only if $\mathsf{Z}_H(a) \ne \varnothing$ for all $a \in H$, and the same applies to T. The claim follows from (ii).

(iv) Preservation of length is clear by definition, because $\overline{\theta}$ acts on each atom of the factorization separately. Let $z = z_0 z_1$ and $z' = z_0 z_1'$ with $z_0 = \gcd(z, z')$. Then $\mathsf{d}(z, z') = \max\{|z_1|, |z_1'|\}$ and $\mathsf{d}(\overline{\theta}(z), \overline{\theta}(z')) \le \max\{|\overline{\theta}(z_1)|, |\overline{\theta}(z_1')|\} = \mathsf{d}(z, z')$.

(v) Let $z = [u_1] \cdots [u_n]$ with $u_1, \ldots, u_n \in \mathcal{A}(H)$. Then $\overline{\theta}(z) = [\theta(u_1)] \cdots [\theta(u_n)]$. After renumbering, without restriction, we can assume $\gcd(\overline{\theta}(z), \overline{y}) = [\theta(u_1)] \cdots [\theta(u_k)]$ for some $0 \le k \le n$, and $\overline{y} = [\theta(u_1)] \cdots [\theta(u_k)][s_{k+1}] \cdots [s_m]$ for some $m \ge k$ and $s_{k+1}, \ldots, s_m \in \mathcal{A}(T)$. Multiplying out the factorizations, in T we have $\theta(u_1) \ldots \theta(u_k)\theta(u_{k+1}) \cdots \theta(u_n) \simeq \theta(u_1) \cdots \theta(u_k) s_{k+1} \cdots s_m$, so $\theta(u_{k+1}) \cdots \theta(u_n) \simeq s_{k+1} \cdots s_m$. Letting $b \coloneqq u_{k+1} \cdots u_n$, therefore there exist $c_{k+1}, \ldots, c_m \in \mathcal{A}(H)$ such that $b \simeq c_{k+1} \cdots c_m$ and $\theta(c_i) \simeq s_i$ for all $k+1 \le i \le m$ by (1). Now $y \coloneqq [u_1] \cdots [u_k][c_{k+1}] \cdots [c_m] \in \mathsf{Z}_H(a)$ is the desired factorization.

(vi) Follows from (3), since $\mathsf{L}_H(a) = \{\, |z| : z \in \mathsf{Z}_H(a) \,\}$. □

As a consequence of the last property, clearly all invariants based solely on sets of lengths,

such as the elasticity and the refined elasticities, coincide for H and T. For instance, the monoid H is half-factorial if and only if T is half-factorial.

Other invariants may not be preserved perfectly. For the catenary degree, we have the following bounds.

Definition 3.8. *Let $\theta\colon H \to T$ be a transfer homomorphism and let $\overline{\theta}\colon \mathsf{Z}(H) \to \mathsf{Z}(T)$ be the induced homomorphism on factorization monoids.*

(1) *For $a \in H$, the **catenary degree in the fiber**, denoted by $\mathsf{c}(a,\theta)$ is the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property: if z, $z' \in \mathsf{Z}_H(a)$ with $\overline{\theta}(z) = \overline{\theta}(z')$, then there exist $z = z_0$, z_1, …, $z_n = z' \in \mathsf{Z}_H(a)$ such that $\overline{\theta}(z_i) = \overline{\theta}(z)$ and $\mathsf{d}(z_{i-1}, z_i) \le N$ for all $1 \le i \le n$.*

(2) *The **catenary degree in the fibers** of θ is $\mathsf{c}(H,\theta) = \sup\{\, \mathsf{c}(a,\theta) : a \in H \,\}$.*

Proposition 3.9. *If $\theta\colon H \to T$ is a transfer homomorphism and $a \in H$, then*

$$\mathsf{c}_T(\theta(a)) \le \mathsf{c}_H(a) \le \max\big\{\mathsf{c}_T(\theta(a)), \mathsf{c}(a,\theta)\big\}.$$

In particular, we have $\mathsf{c}(T) \le \mathsf{c}(H) \le \max\big\{\mathsf{c}(T), \mathsf{c}(H,\theta)\big\}$.

Proof. We first show $\mathsf{c}_T(\theta(a)) \le \mathsf{c}_H(a)$. Without restriction $\mathsf{c}_H(a) = N < \infty$. Let $\overline{z}$, $\overline{z}' \in \mathsf{Z}_T(\theta(a))$. Then there exist z, $z' \in \mathsf{Z}_H(a)$ such that $\overline{\theta}(z) = \overline{z}$ and $\overline{\theta}(z') = \overline{z}'$ by (ii) of Proposition 3.7. By definition of the catenary degree, we can find $z = z_0$, z_1, …, $z_n = z' \in \mathsf{Z}_H(a)$ such that $\mathsf{d}(z_{i-1}, z_i) \le N$ for all $1 \le i \le n$. Then $\overline{\theta}(z_i) \in \mathsf{Z}_T(\theta(a))$ and $\mathsf{d}(\overline{\theta}(z_{i-1}), \overline{\theta}(z_i)) \le \mathsf{d}(z_{i-1}, z_i) \le N$ for all $1 \le i \le n$, so $\mathsf{c}_T(\theta(a)) \le N$.

Let us now show $\mathsf{c}_H(a) \le \max\{\mathsf{c}_T(\theta(a)), \mathsf{c}(a,\theta)\}$. Without restriction, we can assume $N \coloneqq \max\{\mathsf{c}_T(\theta(a)), \mathsf{c}(a,\theta)\} < \infty$. Let z, $z' \in \mathsf{Z}_H(a)$. Then $\overline{\theta}(z)$, $\overline{\theta}(z') \in \mathsf{Z}_T(\theta(a))$, so there exist $\overline{z_0}$, …, $\overline{z_n} \in \mathsf{Z}_T(\theta(a))$ such that $\overline{z_0} = \overline{\theta}(z)$, $\overline{z_n} = \overline{\theta}(z')$, and $\mathsf{d}(\overline{z_{i-1}}, \overline{z_i}) \le N$ for all $1 \le i \le n$. Using (v) of Proposition 3.7 inductively, we can find $z = z_0$, z_1, …, $z_n \in \mathsf{Z}_H(a)$ such that $\overline{\theta}(z_i) = \overline{z_i}$ for all $0 \le i \le n$, and $\mathsf{d}(z_{i-1}, z_i) = \mathsf{d}(\overline{z_{i-1}}, \overline{z_i}) \le N$ for all $1 \le i \le n$. Noting that $\overline{z_n} = \overline{\theta}(z_n) = \overline{\theta}(z')$, the definition of $\mathsf{c}(a,\theta)$ shows that there further exist z_{n+1}, …, $z_m \in \mathsf{Z}_H(a)$ such that $z_m = z'$ and $\mathsf{d}(z_{i-1}, z_i) \le N$ for all $n+1 \le i \le m$. □

3.3 Monoids of Zero-Sum Sequences

To construct a transfer homomorphism from a Dedekind domain R, we need a target monoid T that provides a simplification but is rich enough to capture the arithmetic of R. We will be able to build such a monoid using a combinatorial construction over the class group.

Let $(G,+)$ be an abelian group and $G_0 \subseteq G$ a subset. A **sequence over** G_0 is an element of the free abelian monoid $\mathcal{F}(G_0)$ over G_0, that is, a formal product of elements of G_0. Thus, every sequence $S \in \mathcal{F}(G_0)$ can be written as $S = g_1 \cdots g_n$ with g_1, …, $g_n \in G_0$ and $n \ge 0$. The order of elements does not matter and repetition is allowed. Writing $\mathsf{v}_g(S) \in \mathbb{N}_0$ for the multiplicity of g in S, a concise notation is $S = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}$.

The **length** of a sequence $S = g_1 \cdots g_n = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}$ is $|S| := n = \sum_{g \in G_0} \mathsf{v}_g(S)$. The **sum** of S is $\sigma(S) = g_1 + \cdots + g_n = \sum_{g \in G_0} \mathsf{v}_g(S) g \in G$. Note that $\sigma : \mathcal{F}(G_0) \to G$ is a monoid homomorphism.

A **zero-sum sequence** is a sequence $S \in \mathcal{F}(G_0)$ with $\sigma(S) = 0$. Since $\sigma(ST) = \sigma(S) + \sigma(T)$ for all $S, T \in \mathcal{F}(G_0)$, the set of zero-sum sequences forms a submonoid of $\mathcal{F}(G_0)$.

Definition 3.10. *Let $(G, +)$ be an abelian group and $G_0 \subseteq G$ a subset. The **monoid of zero-sum sequences over** G_0 is*

$$\mathcal{B}(G_0) := \big\{ S \in \mathcal{F}(G_0) : \sigma(S) = 0 \big\}.$$

Example 3.11. Let $G = G_0 = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. An arbitrary sequence over G has the form $S = \overline{0}^k \overline{1}^l \overline{2}^m$ with $k, l, m \in \mathbb{N}_0$. Then $|S| = k + l + m$ and $\sigma(S) = \overline{0}k + \overline{1}l + \overline{2}m = \overline{l + 2m}$. It follows that S is a zero-sum sequence if and only if $l + 2m \equiv 0 \mod 3$, that is $l \equiv -2m \equiv m \mod 3$. In particular, the following sequences are zero-sum sequences (of lengths 1, 3, 3, and 2, respectively):

$$U = \overline{0}, \quad V_1 = \overline{1}^3, \quad V_2 = \overline{2}^3, \quad W = \overline{1}\,\overline{2}.$$

It is not hard to see that any other zero-sum sequence is a product of U, V_1, V_2, and W, and that these are precisely the atoms of $\mathcal{B}(G)$. Note that $V_1 V_2 = W^3$ is a non-trivial factorization in $\mathcal{B}(G)$, so $\mathcal{B}(G)$ is not half-factorial (compare this to the initial example of the chapter). ○

A **minimal zero-sum sequence** is a non-trivial zero-sum sequence that does not contain a non-trivial proper zero-sum subsequence.

Lemma 3.12. *Let G be an abelian group and $G_0 \subseteq G$ a subset.*

(1) *The monoid $\mathcal{B}(G_0)$ is a saturated submonoid of $\mathcal{F}(G_0)$.*

(2) *An $S \in \mathcal{B}(G_0)$ is an atom of $\mathcal{B}(G_0)$ if and only if S is a minimal zero-sum sequence.*

Proof. (1) Let $S, T \in \mathcal{B}(G_0)$. Suppose $S = TT'$ with $T' \in \mathcal{F}(G_0)$. Then $\sigma(T) + \sigma(T') = \sigma(S) = 0$, and since $\sigma(T) = 0$, also $\sigma(T') = 0$.

(2) If $S = T_1 T_2$ with $T_1, T_2 \in \mathcal{B}(G_0)$ both non-trivial, then clearly T_i is a non-trivial proper zero-sum subsequence of S. Conversely, if T is a non-trivial proper zero-sum subsequence of S, then $S = TT'$ with $T' \in \mathcal{F}(G_0)$, and (1) implies $T' \in \mathcal{B}(G_0)$, so S is not an atom. □

We will study the arithmetic of $\mathcal{B}(G_0)$ in more detail in the next chapter, we just observe one basic result here.

Proposition 3.13. *For an abelian group G, the following statements are equivalent.*

(a) *The group G has at most two elements.*

(b) *The monoid $\mathcal{B}(G)$ is factorial.*

(c) *The monoid $\mathcal{B}(G)$ is half-factorial.*

Proof. (a) ⇒ (b) If $|G| = 1$, then $\mathcal{B}(G) = \mathcal{F}(G) \cong (\mathbb{N}_0, +)$ is factorial. Suppose $G = \{0, g\}$ has two elements. Then $\mathcal{B}(G) = \{ 0^l g^{2k} : k \in \mathbb{N}_0 \}$, and 0 and g^2 are prime elements, so $\mathcal{B}(G) \cong (\mathbb{N}_0^2, +)$.

(b) ⇒ (c) Trivial.

(c) ⇒ (a) Suppose $|G| > 2$. We distinguish three cases: G contains an element g of finite order $n \geq 3$, or G contains two distinct elements g and h each of order 2, or G contains an element g of order at least 3.

Case $\operatorname{ord}(g) = n \geq 3$: Then $U := g^n$ and $V := (-g)^n$ are two minimal zero-sum sequences, and so is $W := g(-g)$. The factorization $UV = W^n$ shows that $\mathcal{B}(G)$ is not half-factorial.

Case $\operatorname{ord}(g) = \operatorname{ord}(h) = 2$ **and** $g \neq h$: Let $U := g^2$, $V := h^2$, and $W := (g + h)^2$. Let $X := gh(g + h)$. All of these are atoms and $UVW = X^2$.

Case $\operatorname{ord}(g) \geq 3$:[2] Let $U := g^2(-2g)$ and $-U := (-g)^2(2g)$. Let $V = g(-g)$ and $W = (2g)(-2g)$. These are atoms and $U(-U) = V^2W$. □

3.4 A Transfer Principle

We have all the ingredients to construct a transfer homomorphism for Dedekind domains.

Theorem 3.14. *Let $\varphi: H \to \mathcal{F}(P)$ be a divisor homomorphism with class group $G := \mathrm{Cl}(\varphi)$ and let $G_0 := \{ [p] : p \in P \} \subseteq G$ be the set of classes containing prime divisors. Then there exists a transfer homomorphism $\beta: H \to \mathcal{B}(G_0)$, with $\mathcal{B}(G_0)$ the monoid of zero-sum sequences over G_0.*

Proof. The universal property of the free abelian monoid $\mathcal{F}(P)$ implies that there is a homomorphism $\alpha_0: \mathcal{F}(P) \to \mathcal{F}(G_0)$ given by $\alpha_0(p) = [p]$ for all $p \in P$. Thus, if $A = p_1 \cdots p_n \in \mathcal{F}(P)$, then $\alpha_0(A) = [p_1] \cdots [p_n]$ is the sequence over G_0 consisting of the classes of the prime divisors in A.

Now $A \in \varphi(H)$ if and only if $[A] = [p_1] + \cdots + [p_n] = 0$ in G by Lemma 3.5. We get $\alpha_0(A) \in \mathcal{B}(G_0)$ if and only if $A \in \varphi(H)$. In particular, the homomorphism α_0 restricts to $\alpha: \varphi(H) \to \mathcal{B}(G_0)$, and we can define $\beta := \alpha \circ \varphi: H \to \mathcal{B}(G_0)$.

$$\begin{array}{ccccc} H & \xrightarrow{\varphi} & \varphi(H) & \hookrightarrow & \mathcal{F}(P) \\ & \searrow^{\beta} & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha_0} \\ & & \mathcal{B}(G_0) & \hookrightarrow & \mathcal{F}(G_0). \end{array}$$

Thus, if $a \in H$, then we first factor $\varphi(a) = p_1 \cdots p_n$ with $p_i \in P$, and then take the class of each p_i to get $\beta(a)$. It is important to note that this is very different from simply taking $[\varphi(a)] \in G$.

We verify that β is a transfer homomorphism.

(T1): Let $S \in \mathcal{B}(G_0)$. Then $S = g_1 \cdots g_n$ for some $g_1, \ldots, g_n \in G_0$ with $g_1 + \cdots + g_n = 0 \in G$. By definition of G_0, there exist $p_1, \ldots, p_n \in P$ such that $[p_1] = g_1, \ldots, [p_n] = g_n$. Define $A = p_1 \cdots p_n \in \mathcal{F}(P)$. Since $[A] = [p_1] + \cdots + [p_n] = 0$ in G, we have $A = \varphi(a)$ for some $a \in H$ by Lemma 3.5. Then $\beta(a) = \alpha_0(A) = S$, so φ is surjective.

[2] This case also covers the first one.

Suppose $\beta(a) \in \mathcal{B}(G_0)^\times = \{1\}$, in other words, the sequence $\beta(a) = 1$ is trivial. Then also $\varphi(a) = 1 = \varphi(1)$ in $\mathcal{F}(P)$. Since φ is a divisor homomorphism, this implies $a \mid 1$ in H, so $a \in H^\times$.

(T2): Let $a \in H$ and $S, T \in \mathcal{B}(G_0)$ be such that $\beta(a) = ST$. We show that there exist $b, c \in H$ such that $a = bc$ and such that $\beta(b) = S$ and $\beta(c) = T$. We have $\varphi(a) = p_1 \cdots p_n$ for some $p_1, \ldots, p_n \in P$ with $\alpha_0(\varphi(a)) = \beta(a) = ST$. After renumbering, we can assume $[p_1] \cdots [p_k] = S$ and $[p_{k+1}] \cdots [p_n] = T$ for some $0 \le k \le n$. Since $[p_1] + \cdots + [p_k] = 0$, there exists $b \in H$ with $\varphi(b) = p_1 \cdots p_k$ by Lemma 3.5. In particular, we have $\beta(b) = S$.

By construction, the element $\varphi(b) = p_1 \cdots p_k$ divides $\varphi(a)$ in $\mathcal{F}(P)$. Since φ is a divisor homomorphism, we see that b divides a in H, so $a = bc$ with $c \in H$. From $\varphi(a) = \varphi(b)\varphi(c)$ we see $\varphi(c) = p_{k+1} \cdots p_n$, so $\beta(c) = T$. □

For this particular transfer homomorphism, also catenary degrees are almost preserved.

Proposition 3.15. *For β as in Theorem 3.14, we have $\mathsf{c}(H, \beta) \le 2$. In particular, unless H is half-factorial with $\mathsf{c}(H) = 2$, we have $\mathsf{c}(H) = \mathsf{c}(\mathcal{B}(G_0))$.*

Proof. Denote by $\overline{\beta} : \mathsf{Z}(H) \to \mathsf{Z}(\mathcal{B}(G_0))$ the extension of β to the factorization monoids. Let $a \in H$ and $z, z' \in \mathsf{Z}_H(a)$ with $\overline{\beta}(z) = \overline{\beta}(z')$. We have to show that there exist $z = z_0, z_1, \ldots, z_n = z' \in \mathsf{Z}_H(a)$ such that $\overline{\beta}(z_i) = \overline{\beta}(z)$ for all i, and $\mathsf{d}(z_{i-1}, z_i) \le 2$ for all $1 \le i \le n$.

Let $z = (u_1 H^\times) \cdots (u_k H^\times)$ and $z' = (v_1 H^\times) \cdots (v_k H^\times)$ with $u_1, \ldots, u_k, v_1, \ldots, v_k \in \mathcal{A}(H)$. We can assume $\beta(u_i) = \beta(v_i)$ for all $1 \le i \le k$. We also assume $k \ge 2$, as the claim is trivial otherwise.

The proof is by induction on k and $\mathsf{d}_{\mathcal{F}(P)}(\varphi(u_1), \varphi(v_1))$ (lexicographically). First suppose $\varphi(u_1) = \varphi(v_1)$. Then u_1 and v_1 are associates in H and without restriction $u_1 = v_1$. Applying the induction hypothesis to the factorization $(u_2 H^\times) \cdots (u_k H^\times)$ and $(v_2 H^\times) \cdots (v_k H^\times)$ of $u_1^{-1} a$, we get the desired chain of factorizations.

So now suppose $\varphi(u_1) \ne \varphi(v_1) \in \mathcal{F}(P)$. Let $y \coloneqq \gcd_{\mathcal{F}(P)}(\varphi(u_1), \varphi(v_1))$. Then there exists a prime $p \in P$ with $p \mid \varphi(u_1) y^{-1}$ and $p \nmid \varphi(v_1) y^{-1}$. Since $\varphi(a) = \varphi(u_1) \cdots \varphi(u_k) = \varphi(v_1) \cdots \varphi(v_k)$, there exists $2 \le j \le k$ such that $p \mid \varphi(v_j)$. After renumbering, we can take $p \mid \varphi(v_2)$.

Since $\beta(u_1) = \beta(v_1)$, there exists $q \in P$ such that $[q] = [p]$ in G, and $q \mid \varphi(v_1)$. Now let $V_1' \coloneqq p q^{-1} \varphi(v_1)$ and $V_2' \coloneqq q p^{-1} \varphi(v_2)$. Now $V_1' V_2' = \varphi(v_1 v_2)$, and using that φ is a divisor homomorphism, we can find $v_1', v_2' \in H$ such that $v_1 v_2 = v_1' v_2'$ and moreover $\varphi(v_1') = V_1'$ and $\varphi(v_2') = V_2'$. The factorization $z'' \coloneqq (v_1' H^\times)(v_2' H^\times)(v_3 H^\times) \cdots (v_k H^\times)$ of a satisfies $\overline{\beta}(z'') = \overline{\beta}(z')$, and $\mathsf{d}(z', z'') \le 2$. Since also $\mathsf{d}_{\mathcal{F}(P)}(\varphi(u_1), \varphi(v_1')) < \mathsf{d}_{\mathcal{F}(P)}(\varphi(u_1), \varphi(v_1))$, the induction hypothesis applies to z and z'', giving the desired chain of factorizations.

For the final claim, note that if H is not half-factorial, then $\mathsf{c}(H) \ge 2$ and $\mathsf{c}(\mathcal{B}(G_0)) \ge 2$ by Lemma 1.28. Proposition 3.9 therefore implies $\mathsf{c}(H) = \mathsf{c}(\mathcal{B}(G_0))$. □

In the specific setting of Dedekind domains, we immediately get the following consequence.

Corollary 3.16. *Let R be a Dedekind domain with class group $G \coloneqq \mathrm{Cl}(R)$ and let $G_0 \subseteq G$ be the set of classes containing prime ideals. Then there exists a transfer homomorphism $\beta : R^\bullet \to \mathcal{B}(G_0)$ with catenary degree in the fibers at most 2.*

The motto is: to understand the arithmetic of a Dedekind domain R, we need to know its class group, G, and the distribution of prime ideals in the classes, G_0.

If R is a ring of integers in a number field, then there are two important (non-trivial) facts about G coming from algebraic and analytic number theory:

(1) the group G is finite abelian, and

(2) every class in G contains infinitely many prime ideals (Chebotarev's density theorem). See, for instance, [GH06, Corollary 2.11.16].

We summarize this in the following corollary.

Corollary 3.17. *Let R be a ring of integers in a number field. Then its class group $G = \mathrm{Cl}(R)$ is a finite abelian group and there exists a transfer homomorphism $\beta: R^\bullet \to \mathcal{B}(G)$ with catenary degree in the fibers at most 2.*

Given any such R, there are moreover algorithms to compute G (and also to find prime ideals in each class), so in this case this machinery works very well to reduce questions about factorizations in R to questions about $\mathcal{B}(G)$ with G finite abelian. A similar situation occurs when R is more generally a holomorphy ring in a global field (in particular, this includes coordinate rings of smooth affine curves over *finite* fields) [GH06, Proposition 8.9.7 and Example 8.10.2].

From Proposition 3.13 we immediately obtain the following result. It was first proven by Carlitz [Car60], without the machinery of transfer homomorphism or monoids of zero-sum sequences. Carlitz's result is usually considered to be the starting point of the systematic study of non-unique factorizations.

Corollary 3.18. *A ring of integers R in a number field is half-factorial if and only if $|\mathrm{Cl}(R)| \le 2$.*

See Exercise 3.25 for a discussion of $|\mathrm{Cl}(R)| = 3$.

3.5 The Distribution of Prime Divisors

For rings of algebraic integers the class group is always finite, and every class contains infinitely many prime ideals. For general Dedekind domains there are no such restrictions.

Theorem 3.19 (Claborn)**.** *If G is an abelian group, then there exists a Dedekind domain R with $\mathrm{Cl}(R) \cong G$.*

We skip the proof of this result, which is originally due to Claborn [Cla66] [Fos73, §14]. There are many refinements and generalizations [Lee72; Ros73; Ros76; Cla09; Sme17; Cha22; Per23; CG24; Pom26].

While every abelian group G can be realized as the class group of a Dedekind domain, the distribution of prime ideals in the classes is not completely arbitrary. There is an obstruction coming from the Weak Approximation Theorem.

Proposition 3.20. *Let R be a Dedekind domain with class group $G = \mathrm{Cl}(R)$, for each $g \in G$ let*

$$m_g \coloneqq |\{\, P \in \mathcal{P}(R) : [P] = g \,\}| \in \mathbb{N}_0 \cup \{\infty\},$$

and let $G_0 \coloneqq \{\, g \in G : m_g > 0 \,\}$. If $G' \subseteq G_0$ is any subset with $\sum_{g \in G'} m_g < \infty$, then the set $G_0 \setminus G'$ generates G as monoid.

Proof. Let K be the field of fractions of R. Let $g \in G$. By definition of the class group, there exists $I \in \mathrm{Frac}(R)$ such that $[I] = g$. Let $I = \prod_{P \in \mathcal{P}(R)} P^{\mathsf{v}_P(I)}$ be the prime ideal factorization of I. Note that $\mathcal{P}' \coloneqq \{\, P \in \mathcal{P}(R) : [P] \in G' \,\}$ is finite, so Theorem 2.19 allows us to choose $a \in K^\times$ with $\mathsf{v}_P(a) = -\mathsf{v}_P(I)$ for all $P \in \mathcal{P}' \cup \{P : \mathsf{v}_P(I) \neq 0\}$ and $\mathsf{v}_P(a) \geq 0$ for all other P. Then

$$g = [aI] = \sum_{P \in \mathcal{P}(R) \setminus \mathcal{P}'} (\mathsf{v}_P(I) + \mathsf{v}_P(a))[P] = \sum_{h \in G_0 \setminus G'} n_h h,$$

for some $n_h \in \mathbb{N}_0$, only finitely many of which are nonzero. □

However, for countable groups, this is the only obstruction.

Theorem 3.21. *Let G be a countable abelian group, let $(m_g)_{g \in G}$ be a family in $\mathbb{N}_0 \cup \{\infty\}$, and let $G_0 = \{\, g \in G : m_g > 0 \,\}$. Suppose that whenever G' is a subset of G with $\sum_{g \in G'} m_g < \infty$, then $G_0 \setminus G'$ generates G as monoid. Then there exists a Dedekind domain R with $\mathrm{Cl}(R) \cong G$ with the property that $|\{P \in \mathcal{P}(R) : [P] = g\}| = m_g$ for each $g \in G$ (after identifying G with $\mathrm{Cl}(R)$).*

Again, we skip the proof, see Gilmer, Heinzer, and Smith [GHS96, Theorem 8]. The heavy lifting is again done by a result of Claborn [Cla68]. In the uncountable case, an analogous characterization exists, but there are additional obstructions coming from a stronger form of the Approximation Theorem that involves infinite cardinalities [Fos73, §15][GH06, §3.7c].

The arithmetic of $\mathcal{B}(G_0)$ depends heavily on G_0 and not just the group G. Compare the following open problem to Proposition 3.13.

Open Problem 3.22. *Given an abelian group G, does there always exist a half-factorial Dedekind domain R such that $\mathrm{Cl}(R) \cong G$?*

This is equivalent to asking whether, for every abelian group G, there exists a subset $G_0 \subseteq G$ that generates G as a monoid and such that $\mathcal{B}(G_0)$ is half-factorial.

The question, originally due to Zaks, was first studied by Michel and Steffan [MS86]. See [GH06, §3.7c]. The problem has a positive answer for Warfield groups and some other groups [GG03b]. It is also known that for every abelian group G, there exists a subset $G_0 \subseteq G$ such that $\mathcal{B}(G_0)$ is half-factorial [GG98, Propositon 3.4] (without the extra property that G_0 generates G as a monoid).

3.6 Exercises

Exercise 3.23. *Let* $R \coloneqq \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$.

(1) *The ideals* $P = (2, \frac{1+\sqrt{-23}}{2})$ *and* $Q = (2, \frac{1-\sqrt{-23}}{2})$ *are maximal ideals of* R.

(2) *We have* $PQ = (2)$, $P^3 = (\frac{3+\sqrt{-23}}{2})$, *and* $Q^3 = (\frac{3-\sqrt{-23}}{2})$.

(3) *The ideals* P, Q, P^2, *and* Q^2 *are not principal.*

Exercise 3.24. *A monoid* H *is half-factorial if and only if there exists a transfer homomorphism* $H \to \mathbb{N}_0$.

Exercise 3.25. *Let* R *be a Dedekind domain with class group* $G \cong \mathbb{Z}/3\mathbb{Z}$ *and such that* $G_0 = G$. *For instance, let* R *be a ring of algebraic integers with class number* 3, *such as* $R = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$.

Then $\mathsf{c}(R) = 3$ *and* $\Delta(R) = \{1\}$. *In particular, every length set is a discrete interval. Furthermore, we have* $\rho(R) = 3/2$.

Exercise 3.26 (Skula and Sliwa)**.** *Let* G *be a torsion abelian group and* $G_0 \subseteq G$ *a subset. For* $S = g_1 \cdots g_n \in \mathcal{B}(G_0)$, *let* $\mathsf{k}(S) = \sum_{i=1}^{n} \operatorname{ord}(g_i)$ *be the* ***cross number*** *of* S. *Then* $\mathcal{B}(G_0)$ *is half-factorial if and only if* $\mathsf{k}(U) = 1$ *for all atoms* U *of* $\mathcal{B}(G_0)$.

Exercise 3.27. *Let* $R \subseteq D$ *be domains with the same field of fractions* Q. *Suppose that* $D = RD^\times$, *that* $D^\times \cap R = R^\times$, *and that* $(R : D) \coloneqq \{ x \in Q : xD \subseteq R \}$ *is a maximal ideal of* R. *Then the inclusion* $R^\bullet \hookrightarrow D^\bullet$ *is a transfer homomorphism. A typical example of this occurs when* $K \subseteq L$ *is field extension, and we set* $R = L[X]$ *and* $D = K + XL[X]$.

4 The Arithmetic of Monoids of Zero-Sum Sequences

The transfer homomorphism to a monoid of zero-sum sequences motivates the study of the arithmetic of monoids of zero-sum sequences. In this chapter, we discuss some of the basic results, though the area is too vast to be covered in any depth here. Some additional starting points are [Ger09; Gry13; Ger16; Sch16; GZ20] and [GH06, Chapter 5].

Throughout the chapter, let G be an abelian group and $G_0 \subseteq G$ a subset. Given any arithmetic invariant $*$ we tacitly write $*(G_0)$ as shorthand for $*(\mathcal{B}(G_0))$. For instance, we write $\mathcal{A}(G_0) \coloneqq \mathcal{A}(\mathcal{B}(G_0))$ and $\mathcal{L}(G_0) \coloneqq \mathcal{L}(\mathcal{B}(G_0))$.

4.1 Basic Finiteness Results

The following invariant is central in the theory.

Definition 4.1. *The **Davenport constant** of G_0 is*

$$\mathsf{D}(G_0) \coloneqq \sup\{\, |S| : S \in \mathcal{A}(G_0) \,\} \in \mathbb{N}_0 \cup \{\infty\}.$$

For easy of notation, by convention, we set $\mathsf{D}(G_0) = \sup \varnothing = 0$ if $\mathcal{A}(G_0) = \varnothing$, but this case will be largely irrelevant. We collect some basic finiteness results.

Proposition 4.2. (1) *The monoid of zero-sum sequences $\mathcal{B}(G_0)$ is a reduced FF-monoid.*

(2) *If $|G| \neq 2$, the inclusion $\iota\colon \mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory with class group isomorphic to G. Every class contains exactly one prime divisor.*

(3) *If $|G_0| < \infty$, then $|\mathcal{A}(G_0)| < \infty$, the monoid $\mathcal{B}(G_0)$ is finitely generated, and $\mathsf{D}(G_0) < \infty$.*

Proof. (1) Since $\mathcal{F}(G_0)$ is a reduced FF-monoid, so is $\mathcal{B}(G_0)$ by Proposition 1.32.

(2) If $|G| = 1$, then $\mathcal{B}(G) = \mathcal{F}(G) \cong (\mathbb{N}_0, +)$ and the claim is trivial. Suppose $|G| \geq 3$. Lemma 3.12 shows that the inclusion is a divisor homomorphism. To show that it is a divisor theory, let $g \in G$. We have to show $g = \gcd_{\mathcal{F}(G)}(S_1, \ldots, S_k)$ for some $S_1, \ldots, S_k \in \mathcal{B}(G)$. For $g = 0$ we can take $S_1 = 0$ and $k = 1$. Let $n \coloneqq \mathsf{ord}(g) \in \mathbb{N}_{\geq 2} \cup \{\infty\}$. If $3 \leq n \leq \infty$, we take $S_1 = g^2(-2g)$ and $S_2 = g(-g)$. Finally, if $n = 2$, by assumption, there exists $h \in G \setminus \{0, g\}$. We take $S_1 = g^2$ and $S_2 = gh(-g-h)$.

To determine the class group, note that the homomorphism $\sigma : \mathcal{F}(G) \to G$ extends to a group epimorphism $\overline{\sigma}\colon \mathbf{q}(\mathcal{F}(G)) \to G$. Clearly $\mathbf{q}(\mathcal{B}(G)) \subseteq \ker(\overline{\sigma})$, so there is an induced epimorphism

$\varphi\colon \mathrm{Cl}(\iota) \to G$. To see that it is injective, let $S, T \in \mathcal{F}(G)$ with $g := \sigma(S) = \sigma(T)$. Then $ST^{-1} = (S(-g)) \cdot (T(-g))^{-1} \in \mathbf{q}(\mathcal{B}(G))$. Therefore, the map φ is an isomorphism.

For the final claim, note $\{ g \in G : \varphi([g]) = g \} = \{g\}$ for all $g \in G$.

(3) If $s := |G_0|$, then $\mathcal{F}(G_0) \cong (\mathbb{N}_0^s, +)$. We can therefore identify $\mathcal{B}(G_0)$ with a saturated submonoid of $\mathbb{N}_0^s$. Saturation implies that the atoms of $\mathcal{B}(G_0)$ are the minimal nonzero elements of $\mathbb{N}_0^s$ with respect to the componentwise partial order. Dickson's Lemma (Lemma 1.30) implies that this set is finite, so $\mathcal{A}(G_0)$ is finite. Since $\mathcal{B}(G_0)$ is atomic and reduced, it is therefore a finitely generated monoid. Since $\mathcal{A}(G_0)$ is finite, clearly $\mathsf{D}(G_0) < \infty$. □

Note that $\mathsf{D}(G_0) = 0$ is equivalent to $\mathcal{B}(G_0) = \{1\}$, and $\mathsf{D}(G_0) = 1$ is equivalent to $\mathcal{B}(G_0) = \mathcal{F}(\{0\})$.

Analogous to the refined elasticities ρ_k, we define $\lambda_k(G_0) := \inf \mathcal{U}_k(G_0)$. Then we have the following.

Proposition 4.3. *Suppose* $1 < \mathsf{D}(G_0) < \infty$.

(1) *For all* $k \in \mathbb{N}$,

$$\rho(G_0) \le \frac{\mathsf{D}(G_0)}{2}, \qquad 1 \le \frac{\rho_k(G_0)}{k} \le \rho(G_0), \qquad \frac{1}{\rho(G_0)} \le \frac{\lambda_k(G_0)}{k} \le 1.$$

(2) *If* $G_0 = -G_0$, *then* $\rho_2(G_0) = \mathsf{D}(G_0)$.

(3) *If* $\rho_2(G_0) = \mathsf{D}(G_0)$, *then*

$$\rho_{2k}(G_0) = k\mathsf{D}(G_0), \qquad k\mathsf{D}(G_0) + 1 \le \rho_{2k+1}(G_0) \le k\mathsf{D}(G_0) + \frac{\mathsf{D}(G_0)}{2}$$

for all $k \in \mathbb{N}$. *If* $l, r \in \mathbb{N}_0$ *are such that* $l\mathsf{D}(G_0) + r \ge 1$, *then*

$$2l + \frac{2r}{\mathsf{D}(G_0)} \le \lambda_{l\mathsf{D}(G_0)+r}(G_0) \le 2l + r.$$

In particular, we have $\lambda_{lD(G_0)}(G_0) = 2l$ *for all* $l \in \mathbb{N}$ *and* $\rho(G_0) = \frac{\mathsf{D}(G_0)}{2}$.

Proof. (1) We show the first inequality, the others follow straight from the definitions (see also Lemma 1.14). Let $U_1, \ldots, U_k$ and $V_1, \ldots, V_l \in \mathcal{A}(G_0)$ be such that $S := U_1 \cdots U_k = V_1 \cdots V_l$ and $l \ge k \ge 1$. We have to show $\frac{l}{k} \le \frac{\mathsf{D}(G_0)}{2}$.

We can assume $|U_i|, |V_j| \ge 2$ for all i, j: if, say $|U_1| = 1$, then $U_1 = 0$ is a prime element, and hence there must be a V_j with $V_j = U_1$. In this case we cancel the factors (without decreasing the ratio $\frac{l}{k}$). Now $2l \le |S| \le k\mathsf{D}(G_0)$, so $\frac{l}{k} \le \frac{\mathsf{D}(G_0)}{2}$.

(2) We have $\rho_2(G_0) \le \mathsf{D}(G_0)$ by (1). Let $U \in \mathcal{A}(G_0)$ with $|U| = \mathsf{D}(G_0)$, say $U = g_1 \cdots g_l$ with $l = \mathsf{D}(G_0)$. Then $-U = (-g_1) \cdot (-g_l) \in \mathcal{A}(G_0)$ and $U(-U) = (g_1(-g_1)) \cdots (g_l(-g_l))$ shows $\rho_2(G_0) \ge l$.

(3) By (1), we have $\rho_{2k}(G_0) \le 2k\rho(G_0) \le k\mathsf{D}(G_0)$ and $\rho_{2k+1}(G_0) \le (2k+1)\rho(G_0) \le k\mathsf{D}(G_0) + \frac{\mathsf{D}(G_0)}{2}$. For the lower bounds, recall $\rho_k(G_0) + \rho_l(G_0) \le \rho_{k+l}(G_0)$, so

$$k\mathsf{D}(G_0) = k\rho_2(G_0) \le \rho_{2k}(G_0) \qquad \text{and} \qquad k\mathsf{D}(G_0) + 1 = k\rho_2(G_0) + 1 \le \rho_{2k+1}(G_0).$$

This implies $\rho(G_0) = \frac{\mathsf{D}(G_0)}{2}$ using Lemma 1.14.

We set $\rho_0(G_0) = \lambda_0(G_0) = 0$ for notational convenience. Now

$$\lambda_{l\mathsf{D}(G_0)}(G_0) \ge \frac{2}{\mathsf{D}(G_0)} l\mathsf{D}(G_0) = 2l \qquad \text{and} \qquad \rho_{2l}(G_0) = l\mathsf{D}(G_0)$$

show $\lambda_{l\mathsf{D}(G_0)}(G_0) = 2l$. Finally, for $l, r \ge 0$ with $l\mathsf{D}(G_0) + r \ge 1$,

$$\begin{aligned} 2l + \frac{2r}{\mathsf{D}(G_0)} = \frac{2}{\mathsf{D}(G_0)}(l\mathsf{D}(G_0) + r) = \frac{1}{\rho(G_0)}(l\mathsf{D}(G_0) + r) \\ \le \lambda_{l\mathsf{D}(G_0)+r}(G_0) \le \lambda_{l\mathsf{D}(G_0)}(G_0) + \lambda_r(G_0) \le 2l + r. \end{aligned}$$

□

There is also a structure theorem for the unions of sets of lengths.

Proposition 4.4. *Let $G = G_0$ be a finite abelian group. Then each $\mathcal{U}_k(G)$ is a finite (discrete) interval, namely $\mathcal{U}_k(G) = [\lambda_k(G), \rho_k(G)]$ for all $k \in \mathbb{N}$.*

Proof. We may assume $|G| \ge 3$, as otherwise $\mathcal{B}(G)$ is half-factorial, all $\mathcal{U}_k(G)$ are singletons, and the claim is trivial. First we observe that it suffices to show $[k, \rho_k(G)] \subseteq \mathcal{U}_k(G)$ for all $k \in \mathbb{N}$. Indeed, suppose this is the case, and let $l \in [\lambda_k(G), k]$. Then $\rho_l(G) \ge \rho_{l-\lambda_k(G)}(G) + \rho_{\lambda_k(G)}(G) \ge k$. We get $k \in [l, \rho_l(G)] \subseteq \mathcal{U}_l(G)$, so also $l \in \mathcal{U}_k(G)$.

Now let $l \in \mathcal{U}_k(G)$ be minimal such that $[l, \rho_k(G)] \subseteq \mathcal{U}_k(G)$. For sake of contradiction, assume $l > k$. Consider

$$\big\{ S \in \mathcal{B}(G) : \{k, j\} \subseteq \mathsf{L}(S) \text{ for some } j \ge l \big\}.$$

Choose S with $|S|$ minimal in this set. Let $S = U_1 \cdots U_k = V_1 \cdots V_j$ with $j \ge l$ and $U_1, \ldots, U_k, V_1, \ldots, V_j \in \mathcal{A}(G)$. Since $j \ne k$, clearly $S \ne 0^{|S|}$, so without restriction $U_1 = g_1 g_2 U'$ with $g_1, g_2 \in G$ and $U' \in \mathcal{F}(G)$. We can assume $V_1 V_2 = g_1 g_2 V'$ with $V' \in \mathcal{F}(G)$. Define $U_1' \coloneqq (g_1 + g_2)U'$ and $V_1' \coloneqq (g_1 + g_2)V'$. Then $U_1' \in \mathcal{A}(G)$ and $V_1' = W_1 \cdots W_t$ with $t \ge 1$ and $W_1, \ldots, W_t \in \mathcal{A}(G)$. Consider

$$S' \coloneqq U_1' U_2 \cdots U_k = W_1 \cdots W_t V_3 \cdots V_j,$$

with $\{k, j + t - 2\} \subseteq \mathsf{L}(S')$. Since $|S'| < |S|$, the minimal choice of $|S|$ implies $j + t - 2 < l$. This is only possible if $t = 1$ and $j = l$, so $l - 1 \in \mathcal{U}_k(G)$, contradicting the minimality of l. □

Proposition 4.5. *We have $\mathsf{c}(G_0) \le \mathsf{D}(G_0)$. In particular, if $\mathsf{D}(G_0) < \infty$, then $\mathsf{c}(G_0)$ and the set $\Delta(G_0)$ are finite.*

Proof. By Lemma 1.28 it suffices to show $\mathsf{c}(G_0) \le \mathsf{D}(G_0)$. We may assume $d \coloneqq \mathsf{D}(G_0) < \infty$. Let $S \in \mathcal{B}(G_0)$. We show $\mathsf{c}(S) \le d$ by induction on $|S|$.

Let $z, z' \in \mathsf{Z}(S)$. Let $z = U_1 \cdots U_k$ and $z' = V_1 \cdots V_l$ with $U_i, V_j \in \mathcal{A}(G_0)$. Without restriction $l \ge k \ge 2$ and $l > d$, as the claim is trivial otherwise. Since $|U_1| \le d$, we can assume $U_1 \mid V_1 \cdots V_r$ with $r \le d < l$. Write $V_1 \cdots V_r = U_1 W_1 \cdots W_s$ with $W_i \in \mathcal{A}(G_0)$.

Observe that $U_2 \cdots U_k = W_1 \cdots W_s V_{r+1} \cdots V_l \in \mathcal{B}(G_0)$. By induction hypothesis, there exist $z_0, \ldots, z_n \in \mathsf{Z}(G_0)$ with $\mathsf{d}(z_{i-1}, z_i) \le d$ that connect the factorizations $z_0 = U_2 \cdots U_k$ and $z_n = W_1 \cdots W_s V_{r+1} \cdots V_l$. Similarly, we find $y_0, \ldots, y_m \in \mathsf{Z}(G_0)$ with $\mathsf{d}(y_{i-1}, y_i) \le d$ that connect $U_1 W_1 \cdots W_s$ and $V_1 \cdots V_r$. Connecting the chains,

$$U_1 U_2 \cdots U_k = U_1 z_0,\ U_1 z_1,\ \ldots,\ U_1 z_n = y_0 V_{r+1} \cdots V_l,\ y_1 V_{r+1} \cdots V_l,\ \ldots,\ y_m V_{r+1} \cdots V_l = V_1 \cdots V_l$$

shows $\mathsf{c}(S) \le d$. □

Remark 4.6. (1) A structure theorem for union of sets of lengths also holds in much more generality [Tri19].

(2) If G is infinite, then $\Delta(G) = \mathbb{N}$. If G is finite, then $\Delta(G)$ is empty if $|G| \le 2$, and it is a finite interval with $\min \Delta(G) = 1$ otherwise [GY12].

(3) Again if $G = G_0$ is finite, it is possible to express $\lambda_k(G)$ in terms of $\rho_k(G)$ and $\mathsf{D}(G)$, see Exercise 4.35. It therefore suffices to study $\mathsf{D}(G)$ and $\rho_k(G)$.

4.2 The Davenport Constant of a Finite Abelian Group

We have seen that the Davenport constant controls much of the arithmetic of $\mathcal{B}(G_0)$. Unfortunately, its determination is a notoriously difficult problem, which is still open even when $G = G_0$ is a finite abelian group. We gather some known results.

Let G be an additive finite abelian group. We can assume $G = \mathsf{C}_{n_1} \oplus \cdots \oplus \mathsf{C}_{n_r}$ with $1 < n_1 \mid \cdots \mid n_r$, where $\mathsf{C}_{n_i} = \langle e_i \rangle$ is a cyclic group of order n_i, and $n_r = \exp(G)$ is the exponent of G.

There are some elementary bounds for $\mathsf{D}(G)$.

Definition 4.7. *Let* $\mathsf{D}^*(G) := 1 + \sum_{i=1}^r (n_i - 1)$.

Lemma 4.8. *We have* $\mathsf{D}^*(G) \le \mathsf{D}(G) \le |G|$.

Proof. Consider $S := e_1^{n_1 - 1} \cdots e_r^{n_r - 1}$. Then S is zero-sum free (there is no non-trivial subsequence T of S with $\sigma(T) = 0$). Let $g := e_1 + \cdots + e_r = -\sigma(S)$. Then $Sg \in \mathcal{A}(G)$ has length $\mathsf{D}^*(G)$, so $\mathsf{D}(G) \ge \mathsf{D}^*(G)$.

For the upper bound, let $S = g_1 \cdots g_l \in \mathcal{B}(G)$ with $l > |G|$. Consider the set $\{g_1, g_1 + g_2, \ldots, g_1 + \cdots + g_l\} \subseteq G$. By the pigeonhole principle, there exist $i < j$ such that $g_1 + \cdots + g_i = g_1 + \cdots + g_j$. Then $g_{i+1} + \cdots + g_j = 0$, and so $g_{i+1} \cdots g_j$ is a proper non-trivial zero-sum subsequence of S. □

Example 4.9. For a cyclic group C_n, we have $\mathsf{D}^*(\mathsf{C}_n) = n = \mathsf{D}(\mathsf{C}_n)$. ○

The general upper bound can be improved using group algebras and characters. Let K be a field. The **group algebra** $K[G]$ is the K-algebra that has, as K-vector space, a basis of symbols X^g for $g \in G$, equipped with the multiplication induced by K-linear extension of $X^g X^h = X^{g+h}$ for $g, h \in G$. Explicitly,

$$K[G] = \Big\{ \sum_{g\in G} a_g X^g : a_g \in K \Big\},$$

and

$$\Big(\sum_{g\in G} a_g X^g \Big)\Big(\sum_{g\in G} b_g X^g \Big) = \sum_{g\in G} \Big(\sum_{h\in G} a_h b_{g-h} \Big) X^g.$$

A **character** is a group homomorphism $\chi\colon G \to K^\times$. The characters form a group $\widehat{G} = \mathrm{Hom}(G, K^\times)$ under pointwise multiplication. The trivial character χ_0, given by $\chi_0(g) = 1$ for all $g \in G$, is the identity element of $\widehat{G}$.

Each character χ extends uniquely to a K-algebra homomorphism $\chi\colon K[G] \to K$, given by

$$\chi\Big(\sum_{g\in G} a_g X^g \Big) := \sum_{g\in G} a_g \chi(g).$$

Let $n := \exp(G)$. Then clearly $\mathrm{Hom}(G, K^\times) = \mathrm{Hom}(G, \mu_n(K))$, where $\mu_n(K)$ is the group of n-th roots of unity in K. The field K is a **splitting field** for G if $|\mu_n(K)| = n$. Note that in this case $|G| = n_1 \cdots n_r \neq 0$ in K, so $|G| \in K^\times$. For instance, the field of complex numbers $\mathbb{C}$ is a splitting field for every finite abelian group.

We need some basic results from character theory.

Lemma 4.10. *Let K be a splitting field for G.*

(1) *There is a (non-canonical) isomorphism $G \mapsto \widehat{G}$.*

(2) *The map*

$$\mathrm{Hom}(G, K^\times) \times G \to K^\times, \qquad (\chi, g) \mapsto \chi(g)$$

is a non-degenerate pairing. In particular, therefore $G \cong \widehat{\widehat{G}}$, via $g \mapsto (\chi \mapsto \chi(g))$.

Proof. (1) For each e_i, fix $\zeta_i \in K^\times$ a primitive n_i-th root of unity. Define $\chi_i\colon G \to K^\times$ by $\chi_i(e_i) = \zeta_i$ and $\chi_i(e_j) = 1$ for $j \neq 1$. Then it is easy to check that $\sum_{i=1}^r a_i e_i \mapsto \prod_{i=1}^r \chi_i^{a_i}$ defines an isomorphism $G \to \widehat{G}$.

(2) Non-degeneracy of the pairing means: if $\chi \in \widehat{G}$ and $\chi(g) = 1$ for all $g \in G$, then $\chi = \chi_0$, and similarly if $g \in G$ and $\chi(g) = 1$ for all $\chi \in \widehat{G}$, then $g = 0$.

The first of these is clear by definition of $\widehat{G}$, so we show the second. Let $0 \neq g \in G$. Then $g = \sum_{i=1}^r a_i e_i$ with $0 \le a_i < n_i$ and $a_j \neq 0$ for some j. Taking χ_j as in (1), we have $\chi_j(g) = \zeta_j^{a_j} \neq 1$.

By non-degeneracy of the pairing, the map $G \to \widehat{\widehat{G}}$ is injective. Since $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$ by (1), it is an isomorphism. □

Proposition 4.11 (Orthogonality of Characters)**.** *Let K be a splitting field for G.*

(1) For $\chi \in \widehat{G}$,

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases}$$

(2) For $\chi, \psi \in \widehat{G}$,

$$\sum_{g \in G} \chi(g)\psi^{-1}(g) = \begin{cases} |G| & \text{if } \chi = \psi, \\ 0 & \text{otherwise.} \end{cases}$$

(1') For $g \in G$,

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 0, \\ 0 & \text{otherwise.} \end{cases}$$

(2') For $g, h \in G$,

$$\sum_{\chi \in \widehat{G}} \chi(g)\chi(h)^{-1} = \begin{cases} |G| & \text{if } g = h, \\ 0 & \text{otherwise.} \end{cases}$$

(3) If $f = \sum_{g \in G} a_g X^g \in K[G]$ and $h \in G$, then

$$a_h = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(f)\chi(-h).$$

In particular, if $\chi(f) = 0$ for all $\chi \in \widehat{G}$, then $f = 0$.

Proof. (1): If $\chi = \chi_0$ this is clear. Suppose $\sum_{g \in G} \chi(g) \neq 0$ and let $h \in G$. Then

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g + h) = \chi(h) \sum_{g \in G} \chi(g).$$

Cancelling the sum shows $\chi(h) = 1$, so $\chi = \chi_0$.

(2): Apply (1) to $\chi\psi^{-1}$.

(1') and (2'): Apply (1) and (2) to the dual group $\widehat{G}$, using the canonical isomorphism $G \to \widehat{\widehat{G}}$ from Lemma 4.10.

(3): Using (2), we compute

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(f)\chi(-h) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \sum_{g \in G} a_g \chi(g)\chi(-h) = \frac{1}{|G|} \sum_{g \in G} a_g \sum_{\chi \in \widehat{G}} \chi(g)\chi(h)^{-1} = a_h. \qquad \square$$

The following constant is sometimes called the **group algebra Davenport constant**.

Definition 4.12. *Let $\mathsf{D}(G, K)$ be the smallest $l \in \mathbb{N}_0 \cup \{\infty\}$ such that for all $g_1, \ldots, g_n \in G$ with $n \geq l$, there exist $a_1, \ldots, a_n \in K^\times$, such that*

$$(X^{g_1} - a_1) \cdots (X^{g_n} - a_n) = 0 \in K[G].$$

Lemma 4.13. *It holds that* $\mathsf{D}(G) \le \mathsf{D}(G,K)$ *for every field* K.

Proof. Let $S = g_1 \cdots g_n \in \mathcal{F}(G)$ with $n \ge \mathsf{D}(G,K)$. We show that S contains a non-trivial zero-sum subsequence. By definition of $\mathsf{D}(G,K)$, there exist $a_1, \ldots, a_n \in K^\times$ such that

$$(X^{g_1} - a_1) \cdots (X^{g_n} - a_n) = 0 \in K[G].$$

If S does not contain a non-trivial zero-sum subsequence, then the constant term of this element is $(-1)^n a_1 \cdots a_n \neq 0$, a contradiction. □

We now work towards an upper bound for $\mathsf{D}(G,K)$.

Lemma 4.14. *Let* $M \subseteq \widehat{G}$. *If* $g_1, \ldots, g_n \in G$, *then there exist* $a_1, \ldots, a_n \in K^\times$ *such that*

$$|\{\, \chi \in M : \chi(g_i) \neq a_i \text{ for all } 1 \le i \le n \,\}| \le |M| \prod_{i=1}^{n} \Big(1 - \frac{1}{\operatorname{ord} g_i}\Big).$$

Proof. We proceed by induction on n, the case $n = 0$ being trivial. Suppose $a_1, \ldots, a_{n-1} \in K^\times$ have been chosen such that, for $M' \coloneqq \{\, \chi \in M : \chi(g_i) \neq a_i \text{ for all } 1 \le i \le n-1 \,\}$, we have

$$|M'| \le |M| \prod_{i=1}^{n-1} \Big(1 - \frac{1}{\operatorname{ord} g_i}\Big).$$

The set $\{\, \chi(g_n) \in K^\times : \chi \in M' \,\}$ is a subset of $\mu_l(K)$ with $l \coloneqq \operatorname{ord}(g_n)$, and therefore has cardinality at most l. By the pigeonhole principle, there exists some $a_n \in K^\times$ such that $\chi(g_n) = a_n$ for at least $\frac{|M'|}{l} = \frac{|M'|}{\operatorname{ord}(g_n)}$ characters $\chi \in M$. With this choice of a_n, we have

$$|\{\chi \in M' : \chi(g_n) \neq a_n\}| \le |M'|\Big(1 - \frac{1}{\operatorname{ord} g_n}\Big) \le |M| \prod_{i=1}^{n-1} \Big(1 - \frac{1}{\operatorname{ord} g_i}\Big).$$ □

Theorem 4.15. *If* $n \coloneqq \exp(G)$ *and* K *is a splitting field for* G, *then*

$$\mathsf{D}(G) \le \mathsf{D}(G,K) \le n\Big(1 + \log \frac{|G|}{n}\Big).$$

Proof. We only have to show the second inequality. We shall show that whenever $l \ge n\Big(1 + \log \frac{|G|}{n}\Big)$, then for all $g_1, \ldots, g_l \in G$ there exist $a_1, \ldots, a_l \in K^\times$ such that

$$(X^{g_1} - a_1) \cdots (X^{g_l} - a_l) = 0 \in K[G].$$

By (3) of Proposition 4.11, it suffices to show that there exist such $a_1, \ldots, a_l$ such that for each $\chi \in \widehat{G}$ there exists $1 \le i \le l$ with $\chi(g_i) = a_i$.

For each $0 \le k \le l$, using Lemma 4.14, we can ensure

$$s(k) \coloneqq |\{\chi \in \widehat{G} : \chi(g_i) \ne a_i \text{ for all } i\}| \le |G| \prod_{i=1}^{k} \Big(1 - \frac{1}{\operatorname{ord} g_i}\Big) \le \underbrace{|G|\Big(1 - \frac{1}{n}\Big)^k}_{=:c(k)}.$$

We show that we can choose k with $s(k) \le l - k$. Then we can simply choose $a_{k+1}, \ldots, a_l$ such that $\chi_j(g_{k+j}) = a_{k+j}$ for each of the remaining characters χ_j in the set.

Since $\log(1-y) < -y$ for $0 < y < 1$, we have

$$\log c(k) = \log|G| + k \log\Big(1 - \frac{1}{n}\Big) \le \log|G| - \frac{k}{n}.$$

Setting $k \coloneqq l - n + 1$, therefore

$$\begin{aligned} c(k) &\le \exp\Big(\log|G| - \frac{k}{n}\Big) = \exp\Big(\log|G| - \frac{l}{n} + \frac{n-1}{n}\Big) \\ &\le \exp\Big(\log|G| - \log\frac{|G|}{n} - 1 + \frac{n-1}{n}\Big) < n = l - k + 1, \end{aligned}$$

therefore $s(k) \le l - k$, as claimed (since $s(k) \in \mathbb{N}_0$). □

Another nice case that can be obtained using group algebras is that of p-groups with p a prime number, that is, groups G in which every cyclic factor of G has order a power of a fixed prime p. Here, we work over the finite field $\mathbb{F}_p$ (or more generally, a field of characteristic p).

The **augmentation homomorphism** of a group algebra is the homomorphism $\varepsilon\colon K[G] \to K$ given by $\varepsilon(\sum_{g\in G} a_g X^g) = \sum_{g\in G} a_g$. Its kernel $\operatorname{Aug} K[G] \coloneqq \ker\varepsilon$ is the **augmentation ideal** of $K[G]$.

Proposition 4.16. *Let p be a prime number and let $G = \langle e_1\rangle \oplus \cdots \oplus \langle e_r\rangle$ be a p-group. Suppose* $\operatorname{char} K = p$.

(1) *If $g \in G$ and $m = \operatorname{ord}(g)$, then*

$$(X^g - 1)^m = 0 \in K[G].$$

(2) *As a K-vector space, the augmentation ideal is generated by*

$$B \coloneqq \big\{ (X^{e_1} - 1)^{a_1} \cdots (X^{e_r} - 1)^{a_r} : a_i \in \mathbb{N}_0,\ a_1 + \cdots + a_r \ge 1 \big\}.$$

(3) *With $d \coloneqq \mathsf{D}^*(G)$, we have* $\operatorname{Aug}(K[G])^d = 0$.

Proof. (1) Since m is a power of p, we have $(X^g - 1)^m = X^{mg} - 1 = 0$.

(2) First observe that $\{ X^g - 1 : g \in G \setminus \{0\} \}$ is a K-basis of $\operatorname{Aug}(K[G])$: clearly these linearly independent elements are contained in $\operatorname{Aug}(K[G])$. Since $\dim_K \operatorname{Aug}(K[G]) = |G| - 1$, they form a basis.

For $g \in G$ with $g = c_1e_1 + \cdots + c_re_r$ and $0 \le c_i < \mathrm{ord}(e_i)$, define $\ell(g) = c_1 + \cdots + c_r$. Observing that

$$X^{g+h} - 1 = X^gX^h - 1 = (X^g - 1)(X^h - 1) + (X^g - 1) + (X^h - 1)$$

for all $g, h \in G$, the claim follows by induction on $\ell(g)$.

(3) A generating set for $\mathrm{Aug}(K[G])^d$ is given by elements of the form $(X^{e_1}-1)^{a_1}\cdots(X^{e_r}-1)^{a_r}$ with $a_1 + \cdots + a_r \ge d$, so it suffices to show that any such element is zero. Indeed, since $d > \sum_{i=1}^r(\mathrm{ord}(e_i) - 1)$, there exists some i with $a_i \ge \mathrm{ord}(e_i)$. But then (1) implies $(X^{e_i} - 1)^{a_i} = (X^{e_i} - 1)^{\mathrm{ord}(e_i)}(X^{e_i} - 1)^{a_i - \mathrm{ord}(e_i)} = 0$, so the entire product is zero. □

Theorem 4.17. *If G is a p-group and K has characteristic p, then $\mathsf{D}(G, K) = \mathsf{D}(G) = \mathsf{D}^*(G)$.*

Proof. Let $l \ge \mathsf{D}^*(G)$. If $g_1, \ldots, g_l \in G$, then $(X^{g_1} - 1)\cdots(X^{g_l} - 1) \in \mathrm{Aug}(K[G])^l$, and $\mathrm{Aug}(K[G])^l = 0$ by Proposition 4.16, so $\mathsf{D}(G, K) \le \mathsf{D}^*(G)$. □

Remark 4.18. (1) One can also show $\mathsf{D}(G) = \mathsf{D}^*(G)$ for groups of rank 2, that is, when $G = \mathsf{C}_{n_1} \oplus \mathsf{C}_{n_2}$ with $1 < n_1 \mid n_2$. The proof is very different though, relying on inductive arguments [GH06, Chapter 5.8].

(2) For each $r \ge 4$, an infinite family of groups G of rank r is known for which $\mathsf{D}(G) > \mathsf{D}^*(G)$ [GS92].

The following is one of the main open problems in the area.

Open Problem 4.19. *What is $\mathsf{D}(G)$ for a finite abelian group G? In particular,*

(1) *For groups of rank 3, is $\mathsf{D}(G) = \mathsf{D}^*(G)$? This is known for the special case of groups of the form $\mathsf{C}_p \oplus \mathsf{C}_p \oplus \mathsf{C}_{pn}$ with $p \in \{2, 3\}$ and $n \in \mathbb{N}$.*

(2) *Is $\mathsf{D}(\mathsf{C}_n^r) = \mathsf{D}^*(G) = 1 + r(n-1)$ for all $n, r \in \mathbb{N}$? For C_p^r this follows from Theorem 4.17 and other proofs are known: it can be related to a covering problem [GG03a] that can be solved using the polynomial method [LS08; Sze07][Gry13, Corollary 22.1].*

4.3 Inverse Zero-Sum Problems

We have already seen, for instance, in the proof of Proposition 4.3, that the atoms of maximal length play an important role. One would expect such atoms to have a special form.

Example 4.20. (1) Let $G = \mathsf{C}_n$ be cyclic. Using a variation of the pigeonhole principle proof of Lemma 4.8, it is not hard to show that every atom of maximal length is of the form g^n for some generator g of G. See Exercise 4.33.

(2) Let $G = \mathsf{C}_p^r$ with p a prime number. In this case G is really a $\mathbb{F}_p$-vector space. For every atom U of maximal length, there exists a basis $e_1, \ldots, e_r$ of G such that

$$U = e_1^{p-1}\cdots e_r^{p-1}(e_1 + \cdots + e_r).$$

See [GH06, Corollary 5.6.9] and Exercise 4.34. ○

Remark 4.21. For groups of rank two, an inverse result is known, based on work of Gao, Geroldinger, and Reiher. A full write-up of the general proof, spanning about 150 pages, will appear in the forthcoming monograph by Geroldinger, Grynkiewicz, and Zhong [GGZ26, Chapter 4]. In the special case $G = \mathsf{C}_n \oplus \mathsf{C}_n$, every $U \in \mathcal{A}(G)$ with $|U| = \mathsf{D}(G) = 2n-1$ is of the form

$$U = e_1^{n-1} \prod_{i=1}^{n} (x_i e_1 + e_2)$$

where (e_1, e_2) is a basis of G and $x_i \in [0, n-1]$ with $\sum_{i=1}^{n} x_i \equiv 1 \mod n$. In the general case, of $C_{n_1} \oplus C_{n_2}$, a second type of sequence can occur.

Going beyond minimal zero-sum sequences of maximal length, one can ask about the structure of *long* minimal zero-sum sequences. This becomes non-trivial already for cyclic groups. We need some definitions.

Definition 4.22. *Let $G = \mathsf{C}_n$ and let $S \in \mathcal{F}(G)$.*

(1) *For $g \in G$ with $\mathrm{ord}(g) = n$ and a sequence $S = (n_1 g) \cdots (n_l g)$, let $\|S\|_g \coloneqq \frac{n_1 + \cdots + n_l}{n}$.*

(2) *The **index** of S is $\mathrm{ind}(S) \coloneqq \min\{ \|S\|_g : g \in G, G = \langle g \rangle \}$.*

(3) *The sequence S is g-**smooth** for $g \in G$ if $S = (n_1 g) \cdots (n_l g)$ with $n_i \in [1, \mathrm{ord}(g) - 1]$ and $l = |S|$ such that $m \coloneqq n_1 + \cdots + n_l < \mathrm{ord}(g)$ and $\{ \sigma(T) : 1 \neq T \mid S \} = \{g, 2g, \ldots, mg\}$.*

(4) *The sequence S is a **splittable atom** if $S = (g_1 + g_2)T$ with some $g_1, g_2 \in G$ and $T \in \mathcal{F}(G)$ such that $S \in \mathcal{A}(G)$ and $g_1 g_2 T \in \mathcal{A}(G)$.*

Theorem 4.23 (Savchev–Chen)**.** *Let G be cyclic of order $n \geq 3$.*

(1) *If S is zero-sum free and $|S| \geq \frac{n+1}{2}$, then S is g-smooth for some $g \in G$ with $\mathrm{ord}(g) = n$.*

(2) *If $U \in \mathcal{A}(G)$ has length $|U| \geq \lfloor \frac{n}{2} \rfloor + 2$, then $\mathrm{ind}(U) = 1$ and if U is not splittable, then $U = g^n$ for some $g \in G$.*

We again omit the proof (see [SC07][Ger09, Theorem 5.1.8]) and instead show how this result can be applied to study $\rho_{2k+1}(\mathsf{C}_n)$.

Theorem 4.24. *For $k \in \mathbb{N}_0$ and $n \in \mathbb{N}$ with $n \geq 3$, we have $\rho_{2k+1}(\mathsf{C}_n) = kn + 1$.*

Proof. Suppose that this is not the case, and that k is minimal with $\rho_{2k+1}(\mathsf{C}_n) \geq kn + 2$. Thus, there exist $U_1, \ldots, U_{2k+1}$ and $V_1, \ldots, V_r \in \mathcal{A}(\mathsf{C}_n)$ with $r \geq kn + 2$ such that

$$S \coloneqq U_1 \cdots U_{2k+1} = V_1 \cdots V_r. \tag{4.1}$$

Since $\rho_{2k}(C_n) = kn$, necessarily $0 \nmid S$, so that $|U_i|, |V_j| \geq 2$ for all i, j. We choose the notation so that $2 = |V_1| = \cdots = |V_l| < |V_{l+1}| \leq \cdots \leq |V_r|$ for some $l \in [0, r]$ and $|U_1| \geq |U_2| \geq \cdots \geq |U_{2k+1}| \geq 2$.

Among sequences of the form as in 4.1, consider those with $|S|$ maximal. Among those, we consider one with l maximal. Then we can observe $h(-h) \nmid V_{l+1} \cdots V_r$ for all $h \in \mathsf{C}_n$, as otherwise there would be V_i, V_j with $i \neq j \geq l+1$ such that $h \mid V_i$ and $-h \mid V_j$. Consequently, then $V_i V_j = h(-h)V'$ for some $V' \in \mathcal{B}(G)$, which contradicts the maximal choice of l.

We now observe the following:

- *We have* $l \geq 1$. Otherwise, if $l = 0$, then $3r \leq |S| \leq (2k+1)\mathsf{D}(C_n) = (2k+1)n$, so $r \leq \frac{n}{3}(2k+1) < kn+2$, a contradiction.
- *We have* $|U_1| \geq \cdots \geq |U_{2k}| \geq \lfloor \frac{n}{2} \rfloor + 2$. Otherwise, we have $|U_{2k+1}| \leq |U_{2k}| \leq \lfloor \frac{n}{2} \rfloor + 1$, so that

$$2r \leq |S| \leq 2\Big(\Big\lfloor \frac{n}{2} \Big\rfloor + 1\Big) + (2k-1)n \leq n + 2 + (2k-1)n = 2(nk+1),$$

  hence $r \leq kn+1$, a contradiction.
- *Each* U_i *for* $1 \leq i \leq 2k$ *is of the form* $U_i = g_i^n$ *for some generator* g_i *of* C_n. Indeed, by maximality of $|S|$, each U_i is non-splittable, and then Theorem 4.23 implies the claim.
- *There are no* U_i, U_j *with* $1 \leq i, j \leq 2k+1$ *such that* $U_i = g^n$ *and* $U_j = (-g)^n$. If there would be, then the maximal choice of l would imply $l \geq n$. Without restriction $V_1 = \cdots = V_n = g(-g)$. Removing U_i and U_j from the left side of 4.1 and $V_1, \ldots, V_n$ from the right side, then shows $\rho_{2k-1}(\mathsf{C}_n) \geq r - n \geq (k-1)n + 2$, contradicting the minimal choice of k.

From the last two items we now conclude $l \leq |U_{2k+1}|$. Furthermore, also $|U_{2k+1}| \leq \lfloor \frac{n}{2} \rfloor + 1$: otherwise, another application of Theorem 4.23 gives $U_{2k+1} = g^n$ for some generator g of C_n. Since $l \geq 1$, this means $g \in \{-g_1, \ldots, -g_{2k}\}$, contradicting the last item.

We now find, from the right side of 4.1,

$$r \leq l + \frac{|S| - 2l}{3} = \frac{|S| + l}{3}.$$

Substituting $|S|$ computed from the left side,

$$\frac{|S| + l}{3} = \frac{2kn + |U_{2k+1}| + l}{3} \leq \frac{2kn + 2|U_{2k+1}|}{3} \leq \frac{2kn + n + 2}{3} \leq kn + \frac{2}{3},$$

contradicting $r \geq kn + 2$. □

Open Problem 4.25. *It is conjectured that the cyclic groups are the only groups for which the lower bound* $\rho_{2k+1}(G) = k\mathsf{D}(G) + 1$ *of Proposition 4.3 is attained for all* $k \in \mathbb{N}_0$.

4.4 Other Results and Open Problems

We mention some more key results and problems without proofs.

4.4.1 Structure Theorem for Sets of Lengths.

In Proposition 4.4, we saw that the unions of sets of length $\mathcal{U}_k(G)$ are intervals. Of course, a more refined question is to ask about the structure of individual sets of lengths $\mathsf{L}(S)$ for $S \in \mathcal{B}(G)$. Recall that if $\{k < l\} \subseteq \mathsf{L}(S)$ then $\{nk, (n-1)k + l, \ldots, (n-1)l + k, nl\} \subseteq \mathsf{L}(S^n)$ for all $n \ge 1$, so we expect arithmetic progressions to play a role. Indeed, there is a precise structure theorem along these lines. We first need a definition.

Definition 4.26. *Let $d \in \mathbb{N}$, l, $M \in \mathbb{N}_0$ and $\{0, d\} \subseteq \mathcal{D} \subseteq [0, d]$.*

(1) *An **arithmetic multiprogression** (**AMP**) with difference d and period $\mathcal{D}$ is a finite nonempty set of the form*

$$L = (\min L + \mathcal{D} + d\mathbb{Z}) \cap [\min L, \max L].$$

*The **length** of L is the maximal l for which $\min L + ld \in L$.*

(2) *An **almost arithmetic multiprogression** (**AAMP**) with difference d, period $\mathcal{D}$, length l,and bound M, is a set of the form*

$$L = y + (L' \cup L^* \cup L'') \subseteq y + \mathcal{D} + d\mathbb{Z},$$

where $y \in \mathbb{Z}$, where L^* is an AMP with difference d, period $\mathcal{D}$, and length l, such that $\min L^* = 0$, such that $L' \subseteq [-M, -1]$, and such that and $L'' \subseteq \max L^* + [1, M]$.

We should think of an AAMP as an AMP with some holes at the beginning and at the end, but with an in general large central part that is an AMP.

Theorem 4.27 (Structure Theorem for Sets of Lengths [Ger09, Chapter 3.2])**.** *If G is a finite abelian group and $G_0 \subseteq G$, then there exists some $M^* \in \mathbb{N}_0$ and a finite nonempty set $\Delta^* \subseteq \mathbb{N}$ such that every $L \in \mathcal{L}(G_0)$ is an AAMP with some difference $d \in \Delta^*$ and bound M^*. If moreover $G = G_0$ and $|G| \ge 3$, then*

$$\Delta^* = \big\{ \min \Delta(G_0) : G_0 \subseteq G \text{ with } \Delta(G_0) \ne \varnothing \big\}.$$

By contrast, in the infinite case, we have the following theorem of Kainrath, that shows that sets of lengths are completely unstructured.

Theorem 4.28 (Kainrath [Kai99])**.** *Let $G = G_0$ be an infinite abelian group. Then, for every finite nonempty set $L \subseteq \mathbb{N}_{\ge 2}$, there exists some $S \in \mathcal{B}(G)$ such that $\mathsf{L}(S) = L$.*

In fact, Kainrath's theorem even allows one to prescribe the multiplicities of the elements of L in $\mathsf{L}(S)$, that is, the number of factorizations of S of each length.

4.4.2 Finiteness of $\rho(G_0)$.

While $\rho(G_0) \le \mathsf{D}(G_0)/2$ is always finite when G_0 is finite, it can be infinite when G_0 is infinite. If G is a finitely generated abelian group, that is, if $G \cong \mathbb{Z}^r \oplus G_{\text{tors}}$ with $r \in \mathbb{N}_0$ and G_{tors} a finite abelian group, Grynkiewicz has recently proven a complete characterization of those subsets $G_0 \subseteq G$ for which $\rho(G_0) < \infty$ [Gry22]. The difficult result uses methods from convex geometry (viewing $G/G_{\text{tors}} \cong \mathbb{Z}^r$ as a lattice in $\mathbb{R}^r$).

4.4.3 Inverse Problem for Sets of Lengths.

Suppose that G and G' are two finite abelian group. A natural question is to what extent arithmetical invariants of $\mathcal{B}(G)$ and $\mathcal{B}(G')$ determine G and G'. Applied to rings of algebraic integers in number fields, this is the question of to which extent the arithmetic of the ring determines the class group.

Let us gather some facts.

- By Carlitz's theorem, the sets of lengths of $\mathcal{B}(G)$ are singletons if and only if $|G| \le 2$. So we can see whether $|G| \le 2$ from $\mathcal{L}(G)$.
- Since $\rho(G) = \mathsf{D}(G)/2$, the Davenport constant is determined by the system of sets of lengths $\mathcal{L}(G)$.
- It is not hard to show that there exist only finitely many non-isomorphic finite abelian groups G with a given Davenport constant $\mathsf{D}(G)$, so $\mathsf{D}(G)$ (and by extension $\mathcal{L}(G)$) determines G up to finitely many possibilities.

Trivially one has $\mathcal{L}(\{0\}) = \mathcal{L}(\mathsf{C}_2)$. One can similarly see $\mathcal{L}(\mathsf{C}_3) = \mathcal{L}(\mathsf{C}_2 \oplus \mathsf{C}_2)$. It is an open problem whether, aside from these trivial exceptions, the system of sets of lengths $\mathcal{L}(G)$ determines G up to isomorphism.

Open Problem 4.29. *If G and G' are finite abelian groups with $\mathcal{L}(G) = \mathcal{L}(G')$, is then $G \cong G'$? (Except for the two trivial exceptions mentioned above).*

This has been proven in the case where G is cyclic, an elementary 2-group [Ger09, Corollary 5.3.3], or has rank two [GS19].

We sketch the proof for cyclic groups and elementary 2-groups, which relies on the following lemma (we skip the proof).

Lemma 4.30 ([Ger09, Corollary 2.3.6])**.** *Let $|G| \ge 3$. The set $\{2, \mathsf{D}(G)\}$ appears as a set of lengths of some $S \in \mathcal{B}(G)$ if and only if G is cyclic or an elementary 2-group (meaning $G \cong \mathsf{C}_2^r$ for some $r \in \mathbb{N}_0$).*

Proposition 4.31. *If G is cyclic or an elementary 2-group and $\mathcal{L}(G) = \mathcal{L}(G')$, then $G \cong G'$ (except for the trivial exception $G \cong \mathsf{C}_3$ and $G' \cong \mathsf{C}_2 \oplus \mathsf{C}_2$, respectively, conversely).*

Sketch of Proof. Since $\mathcal{L}(G)$ determines $\rho(G)$, it determines $\mathsf{D}(G)$. From the previous lemma we immediately see that G' is cyclic or an elementary 2-group. In case G' is cyclic, Theorem 4.24

shows $\rho_3(G') = \mathsf{D}(G') + 1$. On the other hand, if G' is an elementary 2-group, then one can show $\rho_3(G') \ge \lfloor \frac{3\mathsf{D}(G')}{2} \rfloor$ [Ger09, Corollary 3.1.5], and hence $\rho_3(G') > \mathsf{D}(G') + 1$ (unless $\mathsf{D}(G') = 3$, which corresponds to the exceptional case), distinguishing the two cases. The precise order of the group follows from $\mathsf{D}(C_n) = n$ and $\mathsf{D}(\mathsf{C}_2^r) = r + 1$. □

4.5 Exercises

Exercise 4.32. *Find an infinite set $G_0 \subseteq \mathbb{Z}$ for which $\mathcal{B}(G_0)$ is nevertheless factorial.*

Exercise 4.33. *For $G = \mathsf{C}_n$, show that every atom of maximal length is of the form g^n for some generator g of G.*

Exercise 4.34. *For $G = \mathsf{C}_2^r$, determine the structure of maximal-length atoms.*

Exercise 4.35. *Let G be a finite abelian group with $|G| \ge 3$.*

(1) *$\mathsf{D}(G) \ge 3$ and for every $2 \le j \le \mathsf{D}(G)$ there exists $S \in \mathcal{B}(G)$ with $\{2, j\} \subseteq \mathsf{L}(S)$.*

(2) *For every $l \in \mathbb{N}_0$, we have*

$$\lambda_{l\mathsf{D}(G)+j}(G) = \begin{cases} 2l & \text{if } j = 0, \\ 2l+1 & \text{if } j \in [1, \rho_{2l+1(G)} - l\mathsf{D}(G)], \\ 2l+2 & \text{if } j \in [\rho_{2l+1}(G) - l\mathsf{D}(G) + 1, \mathsf{D}(G) - 1], \end{cases}$$

provided that $l\mathsf{D}(G) + j \ge 1$.

5 Krull Monoids and Domains

We already saw that a transfer homomorphism to a monoid of zero-sum sequences provides a powerful tool for studying the arithmetic of a monoid or domain. The applicability of this method is not limited to Dedekind domains. In this chapter we introduce the much more general classes of Krull monoids and Krull domains, where we can again find such a transfer homomorphism.

Indeed, we already saw in Theorem 3.14 that it is enough to have a divisor homomorphism to a free abelian monoid. We can take this as the definition of a Krull monoid.

Definition 5.1. *A **Krull monoid** is a monoid H that admits a divisor homomorphism $\varphi\colon H \to \mathcal{F}(P)$ into a free abelian monoid.*

Examples 5.2. (1) If R is a Dedekind domain, then $R^\bullet$ is a Krull monoid by Proposition 3.2.

(2) The free abelian monoid $(\mathcal{F}(P), \cdot) \cong (\mathbb{N}_0^{(P)}, +)$ is a Krull monoid. In particular, the multiplicative monoid of natural numbers $(\mathbb{N}, \cdot) \cong (\mathcal{F}(\mathbb{P}), +)$ is a Krull monoid.

(3) Every saturated submonoid of a Krull monoid is again a Krull monoid. For instance, the Hilbert monoid $(4\mathbb{N}_0 + 1, \cdot)$, as saturated submonoid of $(\mathbb{N}, \cdot)$, is a Krull monoid.

(4) A **Diophantine monoid** is the set of nonnegative integer solutions to a system of linear homogeneous equations with integer coefficients. Explicitly, a Diophantine monoid H is a submonoid of $\mathbb{N}_0^n$ of the form

$$H = \{ \mathbf{x} \in \mathbb{N}_0^n : A\mathbf{x} = 0 \} = \ker(A) \cap \mathbb{N}_0^n.$$

where $A \in \mathbb{Z}^{m \times n}$ is an integer matrix. As a saturated submonoid of $\mathbb{N}_0^n$, every Diophantine monoid is a Krull monoid. These monoids are also known as **normal affine monoids** in the context of toric geometry and convex geometry.

(5) If G is an abelian group and G_0 is a subset, then $\mathcal{B}(G_0)$ is Krull monoid, because it is a saturated submonoid of $\mathcal{F}(G_0)$, see Lemma 3.12. ○

While we have some examples of Krull monoids, from the definition it is often not clear how to verify that a given monoid is Krull. We therefore seek additional characterizations.

5.1 Divisorial Ideals of a Monoid

Let H be a monoid and $\mathbf{q}(H)$ its quotient group. Analogous to the case of domains, for $X, Y \subseteq \mathbf{q}(H)$ we define

$$(X:Y) \coloneqq \{\, a \in \mathbf{q}(H) : aY \subseteq X \,\}$$

and $X^{-1} \coloneqq (H:X)$.

In particular, we will be interested in the case where $X = I$ is a (semigroup) ideal of H, meaning $HI \subseteq I$. A **fractional ideal** of H is a subset $I \subseteq \mathbf{q}(H)$ such that $HI \subseteq I$, such that $I \neq \emptyset$, and such that $aI \subseteq H$ for some $a \in H$. The last condition is equivalent to $I^{-1} \neq \emptyset$. Every nonempty ideal of H is a fractional ideal, and every fractional ideal is of the form $a^{-1}I$ for some $a \in H$ and some nonempty ideal I of H.

Definition 5.3. *Let $X \subseteq \mathbf{q}(H)$.*

(1) *The **divisorial closure** (or v-**closure**) of X is $X_v \coloneqq (X^{-1})^{-1}$.*

(2) *A (fractional) ideal $I \subseteq H$ is **divisorial** (or a v-**ideal**) if $I = I_v$.*

We note some basic properties of the v-operation.

Lemma 5.4. *Let X, Y, $Z \subseteq \mathbf{q}(H)$.*

(1) *If $X \subseteq Y$, then $Y^{-1} \subseteq X^{-1}$ and $X_v \subseteq Y_v$.*

(2) *$((X:Y):Z) = (X:YZ)$.*

(3) *If $a \in \mathbf{q}(H)$, then $(aX)^{-1} = a^{-1}X^{-1}$ and $(aX)_v = aX_v$. Moreover, we have $(aH)_v = aH$, so principal fractional ideals are divisorial.*

(4) *We have $HX^{-1} = X^{-1}$ and $HX_v = X_v$.*

(5) *$X \subseteq X_v$, and $(X^{-1})_v = X_v^{-1} = X^{-1}$. In particular, then $(X_v)_v = X_v$.*

(6) *$(XY)_v = (X_vY)_v = (X_vY_v)_v$.*

(7) *$(XX^{-1})_v = (X_v:X)^{-1}$.*

Proof. (1), (2), (3), and (4) are immediate from the definitions.

(5) Since $XX^{-1} \subseteq H$, we have $X \subseteq (X^{-1})^{-1} = X_v$. Now

$$\big((X^{-1})^{-1}\big)^{-1} = (X_v)^{-1} \subseteq X^{-1} \subseteq (X^{-1})_v = \big((X^{-1})^{-1}\big)^{-1}$$

shows $(X^{-1})_v = X_v^{-1} = X^{-1}$. Then $(X_v)_v = \big((X_v)^{-1}\big)^{-1} = (X^{-1})^{-1} = X_v$.

(6) By (5) it suffices to show the inclusion $(X_vY_v)_v \subseteq (XY)_v$. Using (1), it suffices to show $(XY)^{-1} \subseteq (X_vY_v)^{-1}$.

Let $a \in (XY)^{-1}$, so that $aXY \subseteq H$. Then we have $axY \subseteq H$ for all $x \in X$, so $axY_v \subseteq H_v = H$, using (3). So $aXY_v \subseteq H$, and thus $aXy \subseteq H$ for all $y \in Y_v$, so $aX_vy \subseteq H$ for all $y \in Y_v$. using (3) again. But then $aX_vY_v \subseteq H$, so $a \in (X_vY_v)^{-1}$.

(7) Using (2), we find $(XX^{-1})^{-1} = (H : XX^{-1}) = ((H : X^{-1}) : X) = (X_v : X)$, so $(XX^{-1})_v = (X_v : X)^{-1}$. □

5.1.1 Divisorial Product and v-Invertibility

Let $\mathrm{Frac}_v(H)$ denote the set of all fractional divisorial ideals of H, and let $\mathcal{I}_v(H)$ denote the set of all nonempty divisorial ideals of H. Thus, we have $I \in \mathcal{I}_v(H)$ if and only if $I \in \mathrm{Frac}_v(H)$ and $I \subseteq H$.

We can define a multiplication on these sets.

Definition 5.5. *The **divisorial product** (or v-**product**) of I, $J \in \mathrm{Frac}_v(H)$ is is defined as $I \cdot_v J = (IJ)_v$.*

Together with this operation, the sets $\mathrm{Frac}_v(H)$ and $\mathcal{I}_v(H)$ are commutative semigroups with identity element H. The only non-trivial property is the associativity, which follows from (6) in Lemma 5.4.

Definition 5.6. *A fractional divisorial ideal $I \in \mathrm{Frac}_v(H)$ is v-**invertible** if it is invertible in the semigroup $\mathrm{Frac}_v(H)$, that is, there exists $J \in \mathrm{Frac}_v(H)$ such that $I \cdot_v J = H$.*

Remark 5.7. The notion of v-invertibility is a relaxation of the notion of invertibility for ideals. Call a fractional ideal I **invertible** if there exists some J such that $IJ = H$ (without the v-closure). As in the case of Dedekind domains, it is easy to see that then $J = I^{-1}$ and that therefore $I = I_v$ is divisorial. Moreover, then $(IJ)_v = H = IJ$, so I is v-invertible with inverse I^{-1}.

More generally, the group of all invertible ideals (with respect to the usual ideal multiplication) is a subgroup of $\mathrm{Frac}_v(H)^\times$, with respect to the divisorial product.

We have the following characterization of v-invertible ideals. Given any fractional ideal I, the set $(I : I)$ is always an overmonoid of H.

Lemma 5.8. *For $I \in \mathrm{Frac}_v(H)$, the following statements are equivalent.*
(a) *I is v-invertible.*
(b) *For J, $J' \in \mathrm{Frac}_v(H)$ if $I \cdot_v J \subseteq I \cdot_v J'$, then $J \subseteq J'$.*
(c) *$(I : I) = H$.*
If I is v-invertible, then its inverse is I^{-1}.

Proof. (a) ⇒ (b): Let I' with $I' \cdot_v I = H$. We get

$$J = H \cdot_v J = I' \cdot_v I \cdot_v J \subseteq I' \cdot_v I \cdot_v J' = H \cdot_v J' = J'.$$

(b)⇒ (c): Clearly $H \subseteq (I : I)$, so it suffices to show $(I : I) \subseteq H$. We have

$$(I : I) \cdot_v I \subseteq I = H \cdot_v I,$$

hence $(I:I) \subseteq H$ by (b).

(c)⇒ (a): Using (7) of Lemma 5.4 and $I_v = I$, we get

$$I \cdot_v I^{-1} = (II^{-1})_v = (I_v:I)^{-1} = (I:I)^{-1} = H^{-1} = H.$$

From the last part of the proof, we also see that the inverse of I is I^{-1}. □

Let $\mathcal{I}_v^*(H) \coloneqq \mathcal{I}_v(H) \cap \mathrm{Frac}_v(H)^\times$ denote the semigroup of all v-invertible divisorial ideals of H. Since $\mathrm{Frac}_v(H)^\times$ is a group, the semigroup $\mathcal{I}_v^*(H)$ is cancellative, and hence a monoid.

Corollary 5.9. *If I, $J \in \mathcal{I}_v^*(H)$, then $I \subseteq J$ if and only if J divides I in $\mathcal{I}_v^*(H)$. In particular, we have $I \cap J = \mathrm{lcm}(I,J)$ and $(I \cup J)_v = \gcd(I,J)$.*

Proof. If J divides I, then $I = J \cdot_v L$ for some $L \in \mathcal{I}_v^*(H)$. Then $I = IH \subseteq IL^{-1} \subseteq (IL^{-1})_v = I \cdot_v L^{-1} = J$. Conversely, if $I \subseteq J$, then $IJ^{-1} \subseteq H$. Then also $(IJ^{-1})_v \subseteq H$, and so $I = (IJ^{-1})_v \cdot_v J$, so J divides I in $\mathcal{I}_v^*(H)$. The statement about the least common multiple and the greatest common divisor now follows from their definitions, as in Lemma 2.15 (observing $(I \cap J)_v = I \cap J$). □

The property of every divisorial ideal being v-invertible corresponds to a generalization of integral closure that we now discuss.

Definition 5.10. (1) *An element $x \in \mathbf{q}(H)$ is **almost integral** over H if there exists some $d \in H$ such that $dx^n \in H$ for all $n \in \mathbb{N}$.*

(2) *The **complete integral closure** $\widehat{H}$ of H consists of all elements of $\mathbf{q}(H)$ that are almost integral over H.*

(3) *The monoid H is **completely integrally closed** if $\widehat{H} = H$.*

The following characterizes complete integrally closed monoids.

Proposition 5.11. *The following statements are equivalent for a monoid H.*

(a) *The monoid H is completely integrally closed.*

(b) *For all $I \in \mathrm{Frac}_v(H)$, we have $(I:I) = H$.*

(c) *Every $I \in \mathrm{Frac}_v(H)$ is v-invertible.*

The last condition is equivalent to $\mathrm{Frac}_v(H)$ being a group, which is in turn equivalent to $\mathcal{I}_v^*(H) = \mathcal{I}_v(H)$, so to every nonempty divisorial ideal being v-invertible.

Proof. The equivalence (b) ⇔ (c) follows from Lemma 5.8.

(a) ⇒ (b): Observe first that $(I:I)$ is an overmonoid of H. Suppose there exists some $I \in \mathrm{Frac}_v(H)$ such that $H \subsetneq (I:I)$, and let $x \in (I:I) \setminus H$. Observe that $(I:I)$ is a fractional ideal of H, because $1 \in (I:I)$ and $(I:I)II^{-1} \subseteq H$. Thus, there exists $d \in H$ such that $d(I:I) \subseteq H$. Since $x^n \in (I:I)$ for all $n \in \mathbb{N}$, we have $dx^n \in H$ for all $n \in \mathbb{N}$, so $x \in \widehat{H} = H$, a contradiction.

(b) ⇒ (a): Let $x \in \mathbf{q}(H)$ be such that there exists $d \in H$ such that $dx^n \in H$ for all $n \in \mathbb{N}$. Let $X = \{ x^n : n \in \mathbb{N}_0 \}$, so that $dX \subseteq H$. Then X_v is a fractional ideal of H, since $dX_v \subseteq H_v = H$ by (3) of Lemma 5.4. Applying (b) gives $(X_v : X_v) = H$. But $xX \subseteq X$ shows $xX_v \subseteq X_v$, so $x \in (X_v : X_v) = H$. □

5.1.2 Mori Monoids (v-Noetherian Monoids)

Aside from the complete integral closure, a chain condition on divisorial ideals will also appear in the characterization of Krull monoids.

Definition 5.12. *A monoid H is v-**noetherian** (or **Mori**) if it satisfies the ascending chain condition on divisorial ideals.*

Proposition 5.13. *The following statements are equivalent.*

(a) *The monoid H is v-noetherian.*

(b) *Every nonempty set of divisorial ideals of H has a maximal element.*

(c) *For every $I \in \mathrm{Frac}_v(H)$, there exists a finite subset $E \subseteq I$ such that $E_v = I$.*

(d) *Every nonempty set of fractional divisorial ideals of H with nonempty intersection has a minimal element.*

Proof. The equivalence of (a), (b), and (d) is the standard one for noetherianity conditions.

(b) ⇒ (d): Let Ω be a nonempty set of fractional divisorial ideals of H such that $\bigcap_{I \in \Omega} I \neq \varnothing$. Let a be an element of the intersection. Then $I^{-1} \subseteq a^{-1}H$ for every $I \in \Omega$, so $\Omega' \coloneqq \{ aI^{-1} : I \in \Omega \}$ is a nonempty set of divisorial ideals of H. Therefore, the set Ω' has a maximal element J. Since $aI^{-1} \subseteq J$ if and only if $J^{-1} \subseteq (aI^{-1})^{-1} = a^{-1}I_v = a^{-1}I$ (using Lemma 5.4), which is equivalent to $aJ^{-1} \subseteq I$, the element aJ^{-1} is a minimal element of Ω.

(d) ⇒ (b): Let Ω be a nonempty set of divisorial ideals of H. Without restriction, we may assume $\varnothing \notin \Omega$, so that every element of Ω is fractional. Let $\Omega' = \{ I^{-1} : I \in \Omega \}$. Then $1 \in H \subseteq I^{-1}$ for every $I \in \Omega$, so $\bigcap_{I \in \Omega'} I \neq \varnothing$. Therefore, the set Ω' has a minimal element J, and then J^{-1} is a maximal element of Ω. □

Analogous to the case of rings, a **prime ideal** of the monoid H is a proper ideal P such that if $ab \in P$ for some $a, b \in H$, then $a \in P$ or $b \in P$. Equivalently, if A, B are sets with $AB \subseteq P$, then $A \subseteq P$ or $B \subseteq P$. The following generalizes a familiar result from commutative algebra.

Lemma 5.14. *Let $S \subseteq H$ be a submonoid. If P is maximal in $\{ I \in \mathcal{I}_v(H) : I \cap S = \varnothing \}$, then P is a prime ideal of H.*

Proof. Suppose that P is not prime. Then there exist $a, b \in H \setminus P$ such that $ab \in P$. By maximality of P, then $S \cap (P \cup \{a\})_v \neq \varnothing$ and $S \cap (P \cup \{b\})_v \neq \varnothing$. Let $s \in (P \cup \{a\})_v \cap S$ and $t \in (P \cup \{b\})_v \cap S$. Then $st \in S$ and

$$st \in (P \cup \{a\})_v (P \cup \{b\})_v \subseteq \big((P \cup \{a\})(P \cup \{b\}) \big)_v \subseteq P_v = P,$$

a contradiction. □

Lemma 5.15. *Let H be v-noetherian.*

(1) *If $I \in \mathcal{I}_v(H)$ and S is a submonoid of H such that $I \cap S = \varnothing$, then there exists a divisorial prime ideal P of H such that $I \subseteq P$ and $P \cap S = \varnothing$.*

(2) *Let $a \in H$ and let P be a prime ideal of H with $a \in P$. Then there exists some divisorial prime ideal P_0 of H such that $a \in P_0 \subseteq P$.*

(3) *Every minimal nonempty prime ideal of H is divisorial.*

Proof. (1) Consider $\Omega = \{ J \in \mathcal{I}_v(H) : I \subseteq J \text{ and } J \cap S = \varnothing \}$, which is nonempty since it contains I. Since H is v-noetherian, the set Ω has a maximal element P, which is prime by Lemma 5.14.

(2) Consider $\Omega \coloneqq \{ I \in \mathcal{I}_v(H) : a \in I \subseteq P \}$. Since $aH \in \Omega$, the set Ω is nonempty. Since H is v-noetherian, there exists a maximal element P_0 of Ω. By Lemma 5.14, the ideal P_0 is a prime ideal of H (keeping in mind that $H \setminus P$ is a monoid).

(3) If Q is a minimal nonempty prime ideal of H, let $a \in Q$ and apply (2) to get a divisorial prime ideal P with $a \in P \subseteq Q$. Then $P = Q$ by the minimality of Q. □

Lemma 5.16. *Let H be v-noetherian. If $a \in H \setminus H^\times$, then the set of divisorial prime ideals containing a is finite and nonempty.*

Proof. Let $\Omega \coloneqq \{ P \in \mathcal{I}_v(H) : P \text{ prime with } a \in P \}$. Since a is a non-unit, we have $aH \cap H^\times = \varnothing$. Now (1) of Lemma 5.15, applied with $I = aH$ and $S = H^\times$, shows $\Omega \neq \varnothing$.

Suppose Ω is infinite. By v-noetherianity, we can construct a sequence $P_1, P_2, \ldots$ in Ω such that P_n is maximal in $\Omega \setminus \{P_1, \ldots, P_{n-1}\}$ for each n. Let $I_n \coloneqq P_1 \cap \cdots \cap P_n$ for $n \in \mathbb{N}$. This is a descending chain of divisorial ideals of H containing a, so by v-noetherianity, there exists some n such that $I_n = I_{n+1}$. Then $P_1 \cdots P_n \subseteq P_1 \cap \cdots \cap P_n \subseteq P_{n+1}$. Since P_{n+1} is a prime ideal, this implies $P_i \subseteq P_{n+1}$ for some $i \in \{1, \ldots, n\}$. This contradicts the maximal choice of P_i. □

Remark 5.17. Using this lemma, one can show that v-noetherian monoids are BF-monoids (**??**).

5.2 Krull Monoids

We can now give a characterization of Krull monoids.

Theorem 5.18. *For a monoid H, the following statements are equivalent.*

(a) *H is a Krull monoid.*

(b) *H is completely integrally closed and v-noetherian.*

(c) *H has a divisor theory.*

(d) *H_{red} is a saturated submonoid of a free abelian monoid.*

Before proving the theorem, we need two additional lemmas.

Lemma 5.19. *Let $\varphi\colon H \to D$ be a divisor homomorphism between two monoids. Let $\mathbf{q}(\varphi)\colon \mathbf{q}(H) \to \mathbf{q}(D)$ be the induced homomorphism between the quotient groups.*

(1) *We have $\mathbf{q}(\varphi)^{-1}(D) = H$.*

(2) *For every $X \subseteq H$, we have $X^{-1} = \mathbf{q}(\varphi)^{-1}\big(\mathbf{q}(\varphi)(X)^{-1}\big)$.*

(3) *For $I \in \mathrm{Frac}_v(H)$, we have $I = \mathbf{q}(\varphi)^{-1}\big(\mathbf{q}(\varphi)(I)_v\big)$.*

(4) *If D is completely integrally closed, then so is H.*

(5) *If D is v-noetherian, then so is H.*

Proof. Set $\overline{\varphi} \coloneqq \mathbf{q}(\varphi)$ for brevity.

(1) Clearly $H \subseteq \overline{\varphi}^{-1}(D)$. Suppose $ab^{-1} \in \overline{\varphi}^{-1}(D)$ with $a, b \in H$, so that $\varphi(a) = \varphi(b)d$ for some $d \in D$. Since φ is a divisor homomorphism, we have $a = bc$ for some $c \in H$, and then $c = ab^{-1}$.

(2) Let $a \in X^{-1}$, so that $aX \subseteq H$. Then $\overline{\varphi}(a)\overline{\varphi}(X) = \overline{\varphi}(aX) \subseteq \overline{\varphi}(H) \subseteq D$, so $\overline{\varphi}(a) \in \overline{\varphi}(X)^{-1}$, and thus $a \in \overline{\varphi}^{-1}(\overline{\varphi}(X)^{-1})$.

Conversely, let $a \in \overline{\varphi}^{-1}(\overline{\varphi}(X)^{-1})$, so that $\overline{\varphi}(a) \in \overline{\varphi}(X)^{-1}$. It follows that $\overline{\varphi}(aX) \subseteq D$, so that $aX \subseteq \overline{\varphi}^{-1}(D) = H$ by (1), and thus $a \in X^{-1}$.

(3) The inclusion $I \subseteq \overline{\varphi}^{-1}(\overline{\varphi}(I)_v)$ is clear. Let $a \in \overline{\varphi}^{-1}(\overline{\varphi}(I)_v)$. Then $\overline{\varphi}(a) \in (\overline{\varphi}(I)^{-1})^{-1}$, so

$$\overline{\varphi}(aI^{-1}) = \overline{\varphi}(a\overline{\varphi}^{-1}(\overline{\varphi}(I)^{-1})) \subseteq \overline{\varphi}(a)\overline{\varphi}(I)^{-1} \subseteq D.$$

We get $aI^{-1} \subseteq H$, and thus $a \in I_v = I$.

(4) By assumption, we have $\widehat{D} = D$. If $x \in \widehat{H}$, then there exists some $d \in H$ such that $dx^n \in H$ for all $n \in \mathbb{N}$. Then $\overline{\varphi}(d)\overline{\varphi}(x)^n \in D$, so $\overline{\varphi}(x) \in \widehat{D} = D$, and thus $x \in \overline{\varphi}^{-1}(D) = H$ by (1).

(5) Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of divisorial ideals of H. Then $\varphi(I_1)_v \subseteq \varphi(I_2)_v \subseteq \cdots$ is an ascending chain of divisorial ideals of D, so there exists some n such that $\varphi(I_n)_v = \varphi(I_{n+1})_v = \cdots$. Since $I_m = \overline{\varphi}^{-1}(\varphi(I_m)_v)$ for all m by (3), the chain $(I_n)_{n\ge 0}$ becomes stationary. □

Proposition 5.20. *Let H be a factorial monoid. Then H is completely integrally closed and v-noetherian. Every nonempty divisorial ideal of H is principal, and is generated by a greatest common divisor of its elements.*

Keep in mind that greatest common divisors in a factorial monoid are only unique up to associates. However, if H is free abelian, then we can speak of *the* greatest common divisor.

Proof. Let H be factorial. Then $H = H^\times \times \mathcal{F}(P)$ for some set P of representatives for the associativity classes of prime elements of H, see Corollary 1.11. For each $p \in P$, let $\mathsf{v}_p\colon \mathbf{q}(H) \to \mathbb{Z}$ be the homomorphism defined by $\mathsf{v}_p(p) = 1$, by $\mathsf{v}_p(q) = 0$ for all $q \in P \setminus \{p\}$, and by $\mathsf{v}_p(H^\times) = 0$.

To check that H is completely integrally closed, let $x \in \mathbf{q}(H)$ be such that there exists a $d \in H$ with $dx^n \in H$ for all $n \in \mathbb{N}$. Then $\mathsf{v}_p(d) + n\mathsf{v}_p(x) \ge 0$ for all n, so $\mathsf{v}_p(x) \ge 0$ for all p, and thus $x \in H$.

We first show that for $a, b \in H$, the ideal $\{a,b\}_v$ is the principal ideal generated by $d \in \mathrm{GCD}(a,b)$. Note $\mathsf{v}_p(d) = \min\{\mathsf{v}_p(a), \mathsf{v}_p(b)\}$ for all $p \in P$. Clearly $\{a,b\}_v \subseteq dH$. For the converse inclusion, it suffices to show $\{a,b\}^{-1} \subseteq d^{-1}H$. Suppose ca, $cb \in H$. Then $\mathsf{v}_p(c) + \mathsf{v}_p(a) \ge 0$ and $\mathsf{v}_p(c) + \mathsf{v}_p(b) \ge 0$, hence $\mathsf{v}_p(c) \ge \max\{-\mathsf{v}_p(a), -\mathsf{v}_p(b)\} = -\min\{\mathsf{v}_p(a), \mathsf{v}_p(b)\} = -\mathsf{v}_p(d)$. So $\{a,b\}_v = dH$, as claimed.

Now let $I \in \mathcal{I}_v(H)$, and fix $a \in I$. Since $\mathrm{GCD}(a,b) \subseteq I$ for all $b \in I$, we can assume that I is generated by divisors of a. Since there are only finitely many divisors of a up to associates, the ideal I is finitely generated, in fact, it is principal, generated by a greatest common divisor of a generating set, which is then also a greatest common divisor of all the elements of I. □

Examples 5.21. (1) The nonempty divisorial ideals of $(\mathbb{N}, \cdot)$ are precisely the principal ideals $d\mathbb{N}$ with $d \in \mathbb{N}$. For instance, we have $\{6, 15\}_v = 3\mathbb{N}$. But note that $3 \notin 6\mathbb{N}_0 \cup 15\mathbb{N}_0$, so the ideal generated by 6 and 15 is not divisorial, and there are many non-divisorial ideals in $(\mathbb{N}, \cdot)$.

Among, the nonempty divisorial ideals, the prime ideals are precisely the ideals of the form $p\mathbb{N}$ with p a prime number (these are also the maximal divisorial ideals).

(2) The monoid $(\mathbb{N}_0, +)$ is factorial with unique prime element 1, and the nonempty divisorial ideals are the sets $d + \mathbb{N}_0$ with $d \in \mathbb{N}_0$, and the unique nonempty divisorial prime ideal is $1 + \mathbb{N}_0$. ○

We can now prove the first characterization of Krull monoids.

Proof of Theorem 5.18. (a)⇒(b): Let $\varphi\colon H \to \mathcal{F}(P)$ be a divisor homomorphism. Proposition 5.20 shows that $\mathcal{F}(P)$ is completely integrally closed and v-noetherian. Lemma 5.19 implies that the same holds for H.

(b)⇒(c): We claim that $(\mathcal{I}_v(H), \cdot_v)$ is a free abelian monoid with basis the set of nonempty divisorial prime ideals of H, and that the map $a \mapsto aH$ is a divisor theory.

Since H is completely integrally closed, every fractional ideal is v-invertible by Lemma 5.8, and so $\mathcal{I}_v^*(H) = \mathcal{I}_v(H)$ is cancellative. If $P \in \mathcal{I}_v(H)$ is a prime ideal, and $P \mid IJ$ in $\mathcal{I}_v(H)$, then $P \supseteq IJ$ and hence $P \supseteq I$ or $P \supseteq J$, say $P \supseteq I$. Corollary 5.9 shows $P \mid I$ in $\mathcal{I}_v(H)$, so P is a prime element of $\mathcal{I}_v(H)$.

It remains to show that every $I \in \mathcal{I}_v(H)$ is a v-product of such prime ideals. Let $I \in \mathcal{I}_v(H)$. If $I = H$, then I is the empty v-product. Otherwise, by v-noetherianity, there exists some maximal v-ideal P of H such that $I \subseteq P$. Again using Corollary 5.9, then $I = P \cdot_v J$ with $I \subsetneq J$. Iterating with J, the process must terminate after finitely many steps by v-noetherianity, and we obtain a factorization of I into prime ideals.

The proof that the map $H \to \mathcal{I}_v(H)$, $a \mapsto aH$ is a divisor theory is now analogous to the one for Dedekind domains (Proposition 3.2).

(c)⇒(d): Let $\varphi\colon H \to \mathcal{F}(P)$ be a divisor theory. Then $\varphi(H)$ is a saturated submonoid of $\mathcal{F}(P)$ and one easily checks $\varphi(H) \cong H_{\mathrm{red}}$.

(d)⇒(a): The inclusion $\iota\colon H_{\red} \to \mathcal{F}(P)$ is a divisor homomorphism. Let $\pi\colon H \to H_{\red}$ be the canonical projection. Then one easily verifies that $\iota \circ \pi\colon H \to \mathcal{F}(P)$ is a divisor homomorphism, so H is a Krull monoid. □

We note the following consequence of the proof of (b)⇒(c).

Corollary 5.22. *If H is a Krull monoid, then the monoid $(\mathcal{I}_v(H), \cdot_v)$ is free abelian with basis the nonempty divisorial prime ideals.*

Let v-spec(H) denote the set of divisorial prime ideals of H, and v-max(H) the set of maximal divisorial ideals of H (that is, the proper divisorial ideals of H that are maximal with respect to set inclusion). Lemma 5.14 shows v-max$(H) \subseteq v$-spec(H). Finally, let $\mathfrak{X}(H)$ denote the set of minimal nonempty prime ideals of H.

In Krull monoids these sets coincide (aside from possibly the empty ideal).

Lemma 5.23. *If H is a Krull monoid, then*

$$v\text{-spec}(H) \setminus \{\varnothing\} = v\text{-max}(H) \setminus \{\varnothing\} = \mathfrak{X}(H).$$

Proof. Every nonempty minimal prime ideal of H is divisorial by Lemma 5.15, showing $\mathfrak{X}(H) \subseteq v$-spec$(H) \setminus \{\varnothing\}$, and we always have v-max$(H) \subseteq v$-spec(H).

Now, suppose $P \subsetneq Q$ are two nonempty prime ideals with Q divisorial. Using Lemma 5.15, there exists a nonempty divisorial prime ideal P_0 with $P_0 \subseteq P$. By Corollary 5.9, then $P_0 = Q \cdot_v I$ with $I \in \mathcal{I}_v(H) \setminus \{H\}$, contradicting the fact that P_0 is a prime element of $\mathcal{I}_v(H)$. This shows v-spec$(H) \setminus \{\varnothing\} \subseteq \mathfrak{X}(H)$, so v-spec$(H) \setminus \{\varnothing\} = \mathfrak{X}(H)$. Then also v-max$(H) \setminus \{\varnothing\} = \mathfrak{X}(H)$ follows. □

The class group of H is by definition the one associated to the divisor theory $H \to \mathcal{I}_v(H)$.

Definition 5.24. *Let H be a Krull monoid. The* (***divisor***) ***class group*** *of H is the quotient*

$$\mathrm{Cl}(H) \coloneqq \mathrm{Frac}_v(H)^\times / \{\, aH : a \in \mathbf{q}(H) \,\}.$$

Compare the following result to Theorem 2.21.

Theorem 5.25. *A monoid H is factorial if and only if it is a Krull monoid with trivial divisor class group.*

Proof. Let first H be a Krull monoid with trivial class group. If $a \in H \setminus H^\times$, then $aH = P_1 \cdot_v \cdots \cdot_v P_r$ for some nonempty divisorial prime ideals $P_1, \ldots, P_r$ of H. Each P_i is principal, say $P_i = p_i H$ with p_i a prime element of H. Hence, we have $a \simeq p_1 \cdots p_r$, and H is factorial.

Now let H be factorial. Then H is a Krull monoid by Proposition 5.20. To show that the class group is trivial, it suffices to show that every $I \in \mathcal{I}_v(H)$ is principal, but this also follows from Proposition 5.20. □

5.3 Uniqueness of Divisor Theories

Theorem 5.26. *Let H be a monoid.*

(1) *Let $\varphi\colon H \to \mathcal{F}(P)$ be a divisor theory. Then there exists an isomorphism $\Phi\colon \mathcal{F}(P) \to \mathcal{I}_v(H)$ such that $\Phi \circ \varphi(a) = aH$ for all $a \in H$. Moreover, we have $\Phi(P) = \{ P_0 : P_0 \in \mathcal{I}_v(H)$ is a prime ideal $\}$ and Φ induces an isomorphism between the class group of H and the class group associated to φ.*

(2) *For $i \in \{1,2\}$, let $\varphi_i\colon H \to F_i$ be two divisor theories. Then there exists a unique isomorphism $\Phi\colon F_1 \to F_2$ such that $\Phi \circ \varphi_1 = \varphi_2$.*

Proof. First observe that it suffices to show (1), since then (2) follows by applying (1) to φ_1 and φ_2 and composing the resulting isomorphisms.

Let $F := \mathcal{F}(P)$. We first check:

(i) For $a \in F$, we have $a = \gcd(aF \cap \varphi(H))$.

(ii) For $I \in \mathcal{I}_v(H)$ and $d = \gcd(\varphi(I))$, we have $I = \varphi^{-1}(dF)$.

For (i), note that $\gcd(\varphi(X_1))\gcd(\varphi(X_2)) = \gcd(\varphi(X_1X_2))$ for all $\varnothing \neq X_1, X_2 \subseteq H$. From the definition of a divisor theory, therefore $a = \gcd(\varphi(X))$ for some $\varnothing \neq X \subseteq H$. Then clearly $\varphi(X) \subseteq aF \cap \varphi(H)$, so $\gcd(aF \cap \varphi(H))$ divides a. On the other hand, every element of $aF \cap \varphi(H)$ is a multiple of a, so $a = \gcd(aF \cap \varphi(H))$.

For the second claim, Proposition 5.20 shows $dF = \varphi(I)_v$. Now (3) of 5.19 shows $I = \varphi^{-1}(\varphi(I)_v) = \varphi^{-1}(dF)$.

With these two claims proven, we can now show (1). Define $\Phi\colon F \to \mathcal{I}_v(H)$ by $\Phi(a) = \varphi^{-1}(aF)$ for $a \in F$. Clearly $\Phi(1) = H$, and we have to check $\Phi(ab) = \Phi(a) \cdot_v \Phi(b)$ for all $a, b \in F$.

We have

$$\Phi(a) \cdot_v \Phi(b) = \big((\varphi^{-1}(aF))_v \varphi^{-1}(bF)_v\big)_v = \big(\varphi^{-1}(aF)\varphi^{-1}(bF)\big)_v \subseteq (\varphi^{-1}(abF))_v = \Phi(ab),$$

showing one inclusion.

For the other inclusion, let $d = \gcd \varphi\big(\Phi(a) \cdot_v \Phi(b)\big)$. Starting from the trivial inclusion $\varphi^{-1}(aF)\varphi^{-1}(bF) \subseteq \Phi(a) \cdot_v \Phi(b)$, we find

$$d \mid \gcd \varphi\big(\varphi^{-1}(aF)\varphi^{-1}(bF)\big) = \gcd(aF \cap \varphi(H))\gcd(bF \cap \varphi(H)) = ab,$$

using (i) in the last step. Therefore $abF \subseteq dF$ and

$$\Phi(ab) = \varphi^{-1}(abF) \subseteq \varphi^{-1}(dF) = \Phi(a) \cdot_v \Phi(b),$$

where the last equality follows from (ii). We have thus shown that Φ is a homomorphism.

The surjectivity of Φ follows from (ii). For the injectivity, let $a \in F$. Then $\varphi(\Phi(a)) = \varphi(\varphi^{-1}(aF)) = aF \cap \varphi(H)$, and hence $a = \gcd(\varphi(\Phi(a)))$ by (i), so $\Phi(a)$ indeed determines a.

For $a \in H$, we have $\varphi(a) = \gcd(\varphi(a))$ and so $\Phi(\varphi(a)) = \varphi^{-1}(\varphi(a)F) = aH$ by (ii). The bijection between P and the nonempty divisorial prime ideals of H follows, because monoid isomorphisms map prime elements to prime elements.

Finally, the isomorphism between the class groups follows from the fact that Φ induces an isomorphism between the quotient groups $\mathbf{q}(F)$ and $\mathbf{q}(\mathcal{I}_v(H))$ that maps $\mathbf{q}(H)$ to $\{ aH : a \in \mathbf{q}(H) \}$. □

While a given monoid can have different divisor homomorphisms into free abelian monoids, giving rise to non-isomorphic class groups, divisor theories are canonical, and their attached class group is uniquely determined by H.

5.4 A Local Characterization of Krull Monoids

Let H be a monoid with quotient monoid $Q \coloneqq \mathbf{q}(H)$, and let $S \subseteq H$ be a submonoid (that is, a multiplicative set). Analogous to the situation for domains (see Section 2.6), we define the localization

$$S^{-1}H \coloneqq \{ ab^{-1} \in Q : a \in H, b \in S \}.$$

This is an overmonoid of H in that $H \subseteq S^{-1}H \subseteq Q$. The most important case is again when $S = H \setminus P$ for some prime ideal P of H, in which case we write $H_P \coloneqq S^{-1}H$.

Again the map $I \mapsto S^{-1}I = \{ xs^{-1} : x \in I, s \in S \}$ induces a monoid homomorphism $\mathrm{Frac}(H) \to \mathrm{Frac}(S^{-1}H)$ (with respect to semigroup ideal multiplication). If I is an ideal of H, then $S^{-1}I = S^{-1}H$ if and only if $I \cap S \neq \varnothing$.

There is also a bijection

$$\{ P \subseteq H : P \text{ prime ideal of } H \text{ with } P \cap S = \varnothing \} \leftrightarrow \{ Q \subseteq S^{-1}H : Q \text{ prime ideal of } S^{-1}H \}$$
$$P \mapsto S^{-1}P$$
$$Q \cap H \hookleftarrow Q.$$

For the notion of v-ideals to work well with respect to localization, we need to work with v-noetherian monoids. For additional clarity, we write $S^{-1}v$ for the v-operation on $S^{-1}H$.

A monoid is **v-local** if it has a unique maximal divisorial ideal.

Proposition 5.27. *Let H be a v-noetherian monoid and let $S \subseteq H$ be a submonoid.*

(1) *For $I \in \mathrm{Frac}_v(H)$ and $J \in \mathrm{Frac}(H)$, we have $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$ and $S^{-1}J_v = (S^{-1}J)_{S^{-1}v}$.*

(2) *If $I \in \mathcal{I}_v(S^{-1}H)$, then $J \coloneqq I \cap H \in \mathcal{I}_v(H)$ and $S^{-1}J = I$.*

(3) *If* $I \in \mathrm{Frac}_v(H)$, *then* $S^{-1}I \in \mathrm{Frac}_v(S^{-1}H)$ *and the map* $\mathrm{Frac}_v(H) \to \mathrm{Frac}_v(S^{-1}H)$, $I \mapsto S^{-1}I$ *is a surjective monoid homomorphism with respect to the divisorial product.*

(4) *The localization* $S^{-1}H$ *is* v*-noetherian.*

(5) *There is a bijection*

$$\{\, P \in v\text{-spec}(H) : P \cap S = \varnothing \,\} \leftrightarrow v\text{-spec}(S^{-1}H), \quad P \mapsto S^{-1}P.$$

(6) *If* P *is a nonzero divisorial prime ideal of* H, *then* H_P *is* v*-local with unique maximal divisorial ideal* P_P.

Proof. (1) If $xJ \subseteq I$, then $xS^{-1}J \subseteq S^{-1}I$, so $S^{-1}(I:J) \subseteq (S^{-1}I : S^{-1}J)$. Conversely, because H is v-noetherian, there exists a finite set $E \subseteq J$ such that $J_v = E_v$. Let $x \in (S^{-1}I : S^{-1}J)$. Then $xE \subseteq S^{-1}I$, and because E is finite there exists a common denominator $s \in S$ such that $sxE \subseteq I$ Therefore $sxJ \subseteq sxJ_v = sxE_v = (sxE)_v \subseteq I_v = I$. So $sx \in (I:J)$ and $x \in S^{-1}(I:J)$.

Now $S^{-1}J_v = S^{-1}(H:(H:J)) = (S^{-1}H:(S^{-1}H:S^{-1}J)) = (S^{-1}J)_{S^{-1}v}$.

(2) The equality $S^{-1}J = I$ is straightforward to check. We check that J is divisorial. By (1), we have

$$(I \cap H)_v \subseteq S^{-1}(I \cap H)_v \cap H = I_{S^{-1}v} \cap H = I \cap H,$$

which shows the claim since the inclusion $I \cap H \subseteq (I \cap H)_v$ is trivial.

(3) If $I = I_v$, then $S^{-1}I = S^{-1}I_v = (S^{-1}I)_{S^{-1}v}$ by (1), so $S^{-1}I \in \mathrm{Frac}_v(S^{-1}H)$. Moreover, we have $S^{-1}(I \cdot_v J) = S^{-1}(IJ)_v = (S^{-1}IJ)_{S^{-1}v} = (S^{-1}I \cdot S^{-1}J)_{S^{-1}v} = S^{-1}I \cdot_v S^{-1}J$, so the map is a monoid homomorphism.

To establish surjectivity, it suffices to show that the restriction to $\mathcal{I}_v(H) \to \mathcal{I}_v(S^{-1}H)$ is surjective. This follows from (2).

(4) Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of divisorial ideals of $S^{-1}H$. For each n, let $J_n := I_n \cap H$. Then $J_1 \subseteq J_2 \subseteq \cdots$ is an ascending chain of divisorial ideals of H (using (2)), so there exists some n such that $J_n = J_{n+1} = \cdots$. Since $I_n = S^{-1}J_n$, also $I_n = I_{n+1} = \cdots$.

(5) This follows from the bijection between prime ideals and (1).

(6) By (5). □

As a first step, we now characterize v-local Krull monoids.

Proposition 5.28. *For a monoid* H, *the following statements are equivalent.*

(a) *The monoid* H *is a* v*-local Krull monoid, but not a group.*

(b) *The monoid* H *is a factorial monoid with a unique prime element (up to associates).*

(c) $H = H^\times \times H_0$ *with* $(H_0, \cdot) \cong (\mathbb{N}_0, +)$.

(d) *There exists a group epimorphism* $\mathsf{v} : \mathbf{q}(H) \to \mathbb{Z}$ *such that* $H = \mathsf{v}^{-1}(\mathbb{N}_0)$.

Proof. (a)⇒(b): Let $P = P_v$ be the unique maximal divisorial ideal of H. Then Corollary 5.22 shows that every nonempty divisorial ideal of H is of the form $(P^n)_v$ for some $n \in \mathbb{N}_0$, and all these ideals are distinct

Choose $p \in P \setminus (P^2)_v$. Then necessarily $P = pH$, and p is a prime element of H. If $a \in H$ is any non-unit, then $aH = (P^n)_v = p^n H$ for some $n \in \mathbb{N}$, so $a \simeq p^n$. Therefore, the monoid H is factorial with a unique prime element p up to associates.

(b)⇒(c): By Corollary 1.11.

(c)⇒(d): Clear.

(d)⇒(a): To show that H is a Krull monoid, we show that v is a divisor homomorphism. Let $a, b \in H$ with $\mathsf{v}(a) \le \mathsf{v}(b)$. Let $c := a^{-1}b \in \mathbf{q}(H)$. Then $\mathsf{v}(c) = \mathsf{v}(b) - \mathsf{v}(a) \ge 0$, so $c \in H$ and $b = ac$.

To see that H is v-local, first note that the nonempty divisorial ideals of $(\mathbb{N}_0, +)$ are precisely the principal ideals $n + \mathbb{N}_0$ with $n \in \mathbb{N}_0$, by Proposition 5.20, and that $1 + \mathbb{N}_0 = \mathbb{N}$ is the unique divisorial maximal ideal. Lemma 5.19 shows that every nonempty divisorial ideal of H is a preimage of a divisorial ideal of $(\mathbb{N}_0, +)$, so it follows that $\{ a \in H : \mathsf{v}(a) \ge 1 \}$ is the unique maximal divisorial ideal of H. □

Definition 5.29. *A monoid H satisfying the equivalent conditions of the previous proposition is a **discrete valuation monoid**.*

We now obtain a local characterization of Krull monoids, analogous to the one for Dedekind domains (Theorem 2.29).

Theorem 5.30. *The following statements are equivalent for a monoid H.*

(a) *The monoid H is a Krull monoid.*

(b) *The monoid H is v-noetherian and H_P is a discrete valuation monoid for every nonempty maximal divisorial ideal P.*

(c) *H is an intersection of finite character of discrete valuation monoids in $\mathbf{q}(H)$.*

Here, an **intersection of finite character** means that $H = \bigcap_{i \in I} H_i$ for some family of overmonoids H_i of H such that for every $a \in H$, the set $\{ i \in I : a \notin H_i^\times \}$ is finite.

Before proving the theorem, we need an additional lemma on v-noetherian monoids.

Lemma 5.31. *If H is v-noetherian, then $H = \bigcap_{P \in v\text{-max}(H)} H_P$.*

Proof. The non-trivial inclusion is $\bigcap_{P \in v\text{-max}(H)} H_P \subseteq H$. Let $x \in \bigcap_{P \in v\text{-max}(H)} H_P$. Then

$$I = \{ d \in H : dx \in H \} = x^{-1}H \cap H$$

is a nonempty divisorial ideal of H. To show $x \in H$, we have to show $I = H$.

Suppose $I \subsetneq H$. Lemma 5.15 shows that there exists a divisorial maximal ideal P of H with $I \subseteq P$. But then $I \cap (H \setminus P) = \emptyset$, so $x \notin H_P$, contradicting the choice of x. □

Proof of Theorem 5.30. (a)⇒(b): Proposition 5.27 shows that H_P is v-noetherian and v-local. To show that H_P is a discrete valuation monoid, it suffices to show that H_P is completely integrally closed, by Proposition 5.28. Let $I \in \mathrm{Frac}_v H_P$. By (3) of Proposition 5.27, there exists some $J \in \mathrm{Frac}_v(H)$ such that $I = S^{-1}J$. By (1) of the same proposition, with $S = H \setminus P$, then

$$(I:I) = (S^{-1}J : S^{-1}J) = S^{-1}(J:J) = S^{-1}H = H_P,$$

so H_P is completely integrally closed (using Proposition 5.11).

(b)⇒(c): Lemma 5.31 shows $\bigcap_{P \in v\text{-max}(H)} H_P = H$. Each H_P is a discrete valuation monoid. Since each $a \in H$ is contained in only finitely many maximal divisorial ideals by Lemma 5.16, we have $a \in H_P^\times$ for all but finitely many $P \in v\text{-max}(H)$, so the intersection is of finite character.

(c)⇒(a): We have $H = \bigcap_{i \in I} H_i$ for some family of discrete valuation monoids H_i in $\mathbf{q}(H)$ such that for every $a \in H$, the set $\{ i \in I : a \notin H_i^\times \}$ is finite. For each $i \in I$, let $\mathsf{v}_i : \mathbf{q}(H) \to \mathbb{Z}$ be a group epimorphism such that $H_i = \mathsf{v}_i^{-1}(\mathbb{N}_0)$ (using Proposition 5.28). We claim that the map $\varphi : H \to \mathbb{N}_0^{(I)}$, $a \mapsto (\mathsf{v}_i(a))_{i \in I}$ is a divisor homomorphism. Let $a, b \in H$ with $\varphi(a) \le \varphi(b)$. Let $c = a^{-1}b \in \mathbf{q}(H)$. Then $\mathsf{v}_i(c) = \mathsf{v}_i(b) - \mathsf{v}_i(a) \ge 0$ for all $i \in I$, so $c \in H_i$ for all $i \in I$. So $c \in \bigcap_{i \in I} H_i = H$, and $a \mid_H b$. □

The following is an immediate consequence of (c) of the previous theorem.

Corollary 5.32. *Intersections of finitely many Krull monoids with a fixed quotient group are again Krull monoids.*

5.5 Krull Domains

We now return to the setting of domains. Let D be a domain with field of fractions K.

Definition 5.33. *The domain D is a **Krull domain** if $D^\bullet$ is a Krull monoid.*

For $X, Y \subseteq K$, we can define $(X:Y) \coloneqq \{ z \in K : zY \subseteq X \}$ and $X_v = (D:(D:X))$. It then makes sense talk about divisorial ideals of D in the obvious way. Almost integrality, the complete integral closure, and the v-noetherian (Mori) properties and other properties and objects are defined analogous to the case of monoids.

The following key observation implies that essentially everything directly carries over from the monoid to the domain setting.

Proposition 5.34. *There is a bijection*

$$\begin{aligned} \mathrm{Frac}_v(D) &\leftrightarrow \mathrm{Frac}_v(D^\bullet), \\ I &\mapsto I \setminus \{0\}, \\ J \cup \{0\} &\mapsfrom J. \end{aligned}$$

With respect to the divisorial product, this is an inclusion-preserving isomorphism.

Proof. The crucial point is that if J is a divisorial fractional ideal of the monoid $D^\bullet$, then $J_0 \coloneqq J \cup \{0\}$ is a divisorial fractional ideal of the domain D. In particular, we need $J_0 + J_0 \subseteq J_0$. But note that if X is any subset of $D^\bullet$, then $(D\colon X) = (D^\bullet\colon X) \cup \{0\}$ is closed under addition. Since $J = (D^\bullet\colon(D^\bullet\colon J))$, this holds for J_0.

The remaining claims are straightforward to check. □

A characterization of Krull domains follows immediately from the characterization of Krull monoids.

Corollary 5.35. *For a domain D, the following statements are equivalent.*

(a) *D is a Krull domain.*

(b) *D is a completely integrally closed v-noetherian domain.*

(c) *For every minimal nonzero prime ideal P of D, the localization D_P is a discrete valuation ring and $\bigcap_{P\in\mathfrak{X}(D)} D_P = D$ is an intersection of finite character.*

(d) *D is a finite character intersection of discrete valuation rings (with quotient field K).*

Proof. The equivalence follows from Theorems 5.18 and 5.30 together with Proposition 5.34. That D_P is a discrete valuation ring follows from the fact that $(D^\bullet)_P$ is a discrete valuation monoid together with $D_P = (D^\bullet)_P \cup \{0\}$ being a domain. □

We take a closer look at almost integrality in the domain setting. Recall that $x \in K$ is integral over D if and only if $D[x] \subseteq K$ is a finitely generated D-module.

Lemma 5.36. (1) *An element $x \in K$ is almost integral over D if and only if there exists a finitely generated D-submodule M with $D[x] \subseteq M \subseteq K$.*

(2) *If $x \in K$ is integral, it is almost integral.*

(3) *If D is noetherian, then $x \in K$ is integral if and only if it is almost integral.*

Proof. (1) Suppose first that x is almost integral over D, and that $d \in D^\bullet$ is such that $dx^n \in D$ for all $n \in \mathbb{N}$. Then $D[x] \subseteq d^{-1}D$, so we can take $M \coloneqq d^{-1}D$.

Conversely, let M be a finitely generated D-submodule of K with $D[x] \subseteq M \subseteq K$. Taking a common denominator of the generators of M, we get a $d \in D^\bullet$ with $dx^n \subseteq D$ for all $n \geq 1$.

(2) If x is integral, then $D[x]$ is a finitely generated D-module.

(3) Now $D[x]$ is a D-submodule of M. Because M is finitely generated and D is noetherian, also $D[x]$ is a finitely generated D-module, so x is integral. □

We see that for noetherian domain, being completely integrally closed is equivalent to being integrally closed.

Corollary 5.37. *A noetherian domain is completely integrally closed if and only if it is integrally closed. Hence, a noetherian domain is Krull if and only if it is integrally closed.*

Compared to Dedekind domains, there is no restriction on the dimension.

Examples 5.38. (1) The ring $\mathbb{Z}[\sqrt{5}]$ is not a Krull domain, because it is not integrally closed.

(2) Coordinate rings of smooth affine irreducible varieties are Krull domains.

Consider the case of an algebraically closed field. The nonzero divisorial prime ideals are the minimal nonzero prime ideals, which geometrically correspond to irreducible subvarieties of codimension one. Divisorial ideals are then $\mathbb{Z}$-linear combinations of these, and hence correspond to Weil divisors (when one writes them additively). Ideal classes correspond to linear equivalence classes of Weil divisors, so the class group is the Weil divisor class group.

(3) Let D be a noetherian domain. If D is one-dimensional, then the integral closure $\overline{D}$ of D is noetherian (by the Krull–Akizuki Theorem) and integrally closed, hence a Krull domain. If $\dim(D) > 1$, then $\overline{D}$ need not be noetherian, but it is still a Krull domain by the Mori–Nagata Theorem. ◯

The following is immediate from the corresponding monoid-theoretic result.

Corollary 5.39. *A domain is factorial if and only if it is a Krull domain with trivial class group.*

Proof. By Theorem 5.25. □

Example 5.40. The polynomial ring in infinitely many variables $\mathbb{C}[x_1, x_2, \dots]$ is factorial (hence a Krull domain) but not noetherian. ◯

The relation between Krull and Dedekind domains can be described precisely.

Corollary 5.41. *A domain is a Dedekind domain if and only if it is a Krull domain of dimension at most one.*

Proof. If D is a Dedekind domain, then it is Krull by Proposition 3.2, and it is at most one-dimensional by Theorem 2.5.

Conversely, let D be a Krull domain of dimension at most one. If D is zero-dimensional, then D is a field and there is nothing to show. So suppose D is one-dimensional, meaning $\max(D) = \mathfrak{X}(D)$. Then every maximal ideal is divisorial, by the ring-theoretic analogue of Lemma 5.23. By Theorem 2.5, it suffices to show that every nonzero ideal is invertible. Let $0 \neq I \subseteq D$ be an ideal. Then I_v is v-invertible, and therefore $(II^{-1})_v = D$. If $(II^{-1}) \subsetneq D$, then there exists a maximal ideal M of D such that $II^{-1} \subseteq M$. Since $M = M_v$, this would contradict $(II^{-1})_v = D$. □

While many theorems about Krull domains can be proved in the setting of Krull monoids, the following result has no counterpart in the monoid setting.

If D is a Krull domain, for each $P \in v\text{-max}(D)$, let $\mathsf{v}_P \colon K \to \mathbb{Z}$ be the discrete valuation associated to the discrete valuation ring D_P.

Theorem 5.42 (Approximation Property for Krull Domains)**.** *Let D be a Krull domain with field of fractions K, and let $P_1, \dots, P_n \in v\text{-max}(D)$ be distinct. For each $i \in \{1, \dots, n\}$, let*

$e_i \in \mathbb{Z}$. Then there exists $x \in K$ such that $\mathsf{v}_{P_i}(x) = e_i$ for all $i \in \{1, \dots, n\}$ and $\mathsf{v}_P(x) \ge 0$ for all $P \in v\text{-max}(D) \setminus \{P_1, \dots, P_n\}$.

Proof. Adapt the proof of Theorem 2.19, replacing ideal multiplication by v-multiplication. □

5.6 Some Classes of Krull Domains and Monoids

We close with a very brief discussion of some additional natural classes of Krull domains and monoids (without proofs).

5.6.1 Monoid Algebras

For monoid algebras the theory is particularly well-developed and elegant. Let D be a domain and H a monoid.

Theorem 5.43. (1) *The monoid algebra $D[H]$ is a Krull domain if and only if D is a Krull domain and H is a torsion-free Krull monoid with $H^\times$ satisfying the ascending chain condition on cyclic subgroups.*

(2) *If $D[H]$ is a Krull domain, then there is a canonical isomorphism $\mathrm{Cl}(D[H]) \cong \mathrm{Cl}(D) \oplus \mathrm{Cl}(H)$.*

(3) *If $D[H]$ is a Krull domain and H is a non-trivial monoid, then every class of $\mathrm{Cl}(D[H])$ contains infinitely many prime divisors.*

The Krull property for monoid algebras was first characterized by Chouinard [Cho81], a standard reference is [Gil84]. The final claim, about the distribution of prime divisors, is a recent result of Fadinger and Windisch [FW22].

As special cases, this class of monoid algebras includes polynomial and Laurent polynomial rings over Krull domains and monoid algebras of normal affine monoids over fields.

5.6.2 Laurent Intersection Rings

Let K be a field, and $Q = K(x_1, \dots, x_n)$ the field of rational functions in n variables. To any tuple of variables $\mathbf{y} = (y_1, \dots, y_n) \in Q^n$ with the property that $Q = K(y_1, \dots, y_n)$, we can associate a polynomial ring $K[\mathbf{y}] = K[y_1, \dots, y_n]$ and a Laurent polynomial ring $K[\mathbf{y}^{\pm 1}] = K[y_1^{\pm 1}, \dots, y_n^{\pm 1}]$, having in the same quotient field Q.

Definition 5.44. *A **Laurent intersection ring** (LIR) is a domain of the form $R = \bigcap_{\boldsymbol{y} \in S} K[\boldsymbol{y}^{\pm 1}]$ for some set S of variables $\boldsymbol{y} = (y_1, \dots, y_n) \in Q^n$ with $Q = K(y_1, \dots, y_n)$ such that $K[\boldsymbol{y}] \subseteq R$ for all $\boldsymbol{y} \in S$. The domain R is a **finite Laurent intersection ring** (FLIR) if S can be chosen to be finite.*

LIRs and FLIRs were introduced in [PS26]. The motivation for this definition is the observation that many upper cluster algebras and their generalizations are FLIRs, and that the FLIR property

is a useful tool for studying their factorization theory. FLIRs give rise to a large class of Krull domains where the class group can be determined algorithmically and the distribution of prime divisors is understood.

Since finite intersection of Krull domains are Krull domains, it is easy to see that every FLIR is a Krull domain. More generally, a LIR is a Krull domain if and only if it is a FLIR [PS26, Proposition 3.4].

The following natural question arises and is open for $n > 1$. A positive answer would imply that every upper cluster algebra, with base ring a Krull domain, is itself a Krull domain.

Open Problem 5.45 ([PS26, Question 7.8])**.** *Is every LIR over a Krull domain a FLIR?*

5.6.3 Monoids of Modules

Let $\mathcal{C}$ be a class of modules over a ring R, such that $\mathcal{C}$ is closed under finite direct sums, direct summands, and isomorphisms. Suppose that the isomorphism classes in $\mathcal{C}$ form a set, denoted by $V(\mathcal{C})$. Then $V(\mathcal{C})$ forms a monoid with respect to the operation $[M] + [N] = [M \oplus N]$. If $\mathcal{C}$ is the class of finitely generated projective right R-modules, we write $V(R)$ instead of $V(\mathcal{C})$.

In several interesting cases, this monoid is known to be a Krull monoid [BW13]. For example, we have the following.

(1) If R is semilocal, then $V(R)$ is a Krull monoid [FH00]. If every module in $\mathcal{C}$ has a semilocal endomorphism ring, then $V(\mathcal{C})$ is a Krull monoid [Fac02].

(2) Let R be a commutative one-dimensional noetherian local ring such that $\widehat{R}$ is reduced. If M is a finitely generated module and $\operatorname{add}(M)$ denotes the class of modules isomorphic to direct summands of finite direct sums of M, then $V(\operatorname{add}(M))$ is a Krull monoid [BW13, Theorem 3.18]. In particular, this applies to $V(R)$, since $V(R) = V(\operatorname{add}(R))$. Similar results are possible if $\mathcal{C}$ is the class of finitely generated torsion-free modules, and in many cases one can determine the class group and the distribution of prime divisors [BG14].

5.7 Exercises

Exercise 5.46. *Every v-noetherian monoid is a BF-monoid* (*use Lemma 5.16*).

Exercise 5.47. *If H is a Krull monoid, then $H = H^\times \times H_0$ with $H_0 \cong H_{\mathrm{red}}$ a reduced Krull monoid.*

Exercise 5.48. *Let $(H_i)_{i\in I}$ be a family of monoids. The coproduct $H \coloneqq \coprod_{i\in I} H_i$ consist of all $(a_i)_{i\in I}$ with $a_i \in H$ such that $a_i = 1$ for all but finitely many $i \in I$.*

(1) *There is a semigroup isomorphism* $\mathrm{Frac}_v(H) \cong \prod_{i\in I} \mathrm{Frac}_v(H_i)$.

(2) *The coproduct H is a Krull monoid if and only if each H_i is a Krull monoid and* $\mathrm{Cl}(H) \cong \bigoplus_{i\in I} \mathrm{Cl}(H_i)$.

This gives another way of showing that factorial monoids are Krull monoids with trivial class group.

Bibliography

[Bel+23] J. P. Bell, K. Brown, Z. Nazemian, and D. Smertnig. *On noncommutative bounded factorization domains and prime rings*. J. Algebra 622 (2023), 404–449. DOI: 10.1016/j.jalgebra.2023.01.023.

[BG14] N. R. Baeth and A. Geroldinger. *Monoids of modules and arithmetic of direct-sum decompositions*. Pacific J. Math. 271.2 (2014), 257–319. DOI: 10.2140/pjm.2014.271.257.

[BW13] N. R. Baeth and R. Wiegand. *Factorization theory and decompositions of modules*. Amer. Math. Monthly 120.1 (2013), 3–34. DOI: 10.4169/amer.math.monthly.120.01.003.

[Car60] L. Carlitz. *A characterization of algebraic number fields with class number two*. Proc. Amer. Math. Soc. 11 (1960), 391–392. DOI: 10.2307/2034782.

[CG24] G. W. Chang and A. Geroldinger. *On Dedekind domains whose class groups are direct sums of cyclic groups*. J. Pure Appl. Algebra 228.1 (2024), Paper No. 107470, 14. DOI: 10.1016/j.jpaa.2023.107470.

[Cha22] G. W. Chang. *The ideal class group of polynomial overrings of the ring of integers*. J. Korean Math. Soc. 59.3 (2022), 571–594. DOI: 10.4134/JKMS.j210419.

[Cho81] L. G. Chouinard II. *Krull semigroups and divisor class groups*. Canadian J. Math. 33.6 (1981), 1459–1468. DOI: 10.4153/CJM-1981-112-x.

[Cla09] P. L. Clark. *Elliptic Dedekind domains revisited*. Enseign. Math. (2) 55.3-4 (2009), 213–225. DOI: 10.4171/LEM/55-3-1.

[Cla66] L. Claborn. *Every abelian group is a class group*. Pacific J. Math. 18 (1966), 219–222.

[Cla68] L. Claborn. *Specified relations in the ideal group*. Michigan Math. J. 15 (1968), 249–255.

[Fac02] A. Facchini. *Direct sum decompositions of modules, semilocal endomorphism rings, and Krull monoids*. J. Algebra 256.1 (2002), 280–307. DOI: 10.1016/S0021-8693(02)00164-3.

[FH00] A. Facchini and D. Herbera. *K_0 of a semilocal ring*. J. Algebra 225.1 (2000), 47–69. DOI: 10.1006/jabr.1999.8092.

[Fos73] R. M. Fossum. *The divisor class group of a Krull domain*. Vol. Band 74. Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]. Springer-Verlag, New York-Heidelberg, 1973, pp. viii+148.

[FW22] V. Fadinger and D. Windisch. *On the distribution of prime divisors in Krull monoid algebras*. J. Pure Appl. Algebra 226.4 (2022), Paper No. 106887, 8. DOI: 10.1016/j.jpaa.2021.106887.

[Ger09] A. Geroldinger. *Additive group theory and non-unique factorizations*. In: *Combinatorial number theory and additive group theory*. Adv. Courses Math. CRM Barcelona. Birkhäuser Verlag, Basel, 2009, 1–86. DOI: 10.1007/978-3-7643-8962-8.

[Ger16] A. Geroldinger. *Sets of lengths*. Amer. Math. Monthly 123.10 (2016), 960–988. DOI: 10.4169/amer.math.monthly.123.10.960.

[GG03a] W. Gao and A. Geroldinger. *Zero-sum problems and coverings by proper cosets*. European J. Combin. 24.5 (2003), 531–549. DOI: 10.1016/S0195-6698(03)00033-7.

[GG03b] A. Geroldinger and R. Göbel. *Half-factorial subsets in infinite abelian groups*. Houston J. Math. 29.4 (2003), 841–858.

[GG98] W. Gao and A. Geroldinger. *Half-factorial domains and half-factorial subsets of abelian groups*. Houston J. Math. 24.4 (1998), 593–611.

[GGZ26] A. Geroldinger, D. J. Grynkiewicz, and Q. Zhong. *Combinatorial Factorization Theory*. Fortcoming monograph. 2026.

[GH06] A. Geroldinger and F. Halter-Koch. *Non-unique factorizations*. Vol. 278. Pure and Applied Mathematics (Boca Raton). Algebraic, combinatorial and analytic theory. Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxii+700. DOI: 10.1201/9781420003208.

[GHS96] R. Gilmer, W. Heinzer, and W. W. Smith. *On the distribution of prime ideals within the ideal class group*. Houston J. Math. 22.1 (1996), 51–59.

[Gil84] R. Gilmer. *Commutative semigroup rings*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1984, pp. xii+380.

[Gra74] A. Grams. *Atomic rings and the ascending chain condition for principal ideals*. Proc. Cambridge Philos. Soc. 75 (1974), 321–329. DOI: 10.1017/s0305004100048532.

[Gry13] D. J. Grynkiewicz. *Structural additive theory*. Vol. 30. Developments in Mathematics. Springer, Cham, 2013, pp. xii+426. DOI: 10.1007/978-3-319-00416-7.

[Gry22] D. J. Grynkiewicz. *The characterization of finite elasticities—factorization theory in Krull monoids via convex geometry*. Vol. 2316. Lecture Notes in Mathematics. Springer, Cham, 2022, pp. xii+280. DOI: 10.1007/978-3-031-14869-9.

[GS19] A. Geroldinger and W. A. Schmid. *A characterization of class groups via sets of lengths*. J. Korean Math. Soc. 56.4 (2019), 869–915. DOI: 10.4134/JKMS.j180467.

[GS92] A. Geroldinger and R. Schneider. *On Davenport's constant*. J. Combin. Theory Ser. A 61.1 (1992), 147–152. DOI: 10.1016/0097-3165(92)90061-X.

[GY12] A. Geroldinger and P. Yuan. *The set of distances in Krull monoids*. Bull. Lond. Math. Soc. 44.6 (2012), 1203–1208. DOI: 10.1112/blms/bds046.

[GZ20] A. Geroldinger and Q. Zhong. *Factorization theory in commutative monoids*. Semigroup Forum 100.1 (2020), 22–51. DOI: 10.1007/s00233-019-10079-0.

[Kai99] F. Kainrath. *Factorization in Krull monoids with infinite class group*. Colloq. Math. 80.1 (1999), 23–30. DOI: 10.4064/cm-80-1-23-30.

[Lee72] C. R. Leedham-Green. *The class group of Dedekind domains*. Trans. Amer. Math. Soc. 163 (1972), 493–500.

[LS08] G. Lettl and Z.-W. Sun. *On covers of abelian groups by cosets*. Acta Arith. 131.4 (2008), 341–350. DOI: 10.4064/aa131-4-3.

[MS86] D. Michel and J.-L. Steffan. *Répartition des idéaux premiers parmi les classes d'idéaux dans un anneau de Dedekind et équidécomposition*. J. Algebra 98.1 (1986), 82–94. DOI: 10.1016/0021-8693(86)90016-5.

[Per23] G. Peruginelli. *Polynomial Dedekind domains with finite residue fields of prime characteristic*. Pacific J. Math. 324.2 (2023), 333–351. DOI: 10.2140/pjm.2023.324.333.

[Pom26] M. Pompili. *Every finitely generated abelian group is the class group of a generalized cluster algebra*. J. Algebra 686 (2026), 566–594. DOI: 10.1016/j.jalgebra.2025.08.017.

[PS26] M. Pompili and D. Smertnig. *Factoriality and Class Groups of Upper Cluster Algebras and Finite Laurent Intersection Rings: A Computational Approach* (2026). Submitted. arXiv: 2601.07520.

[Roi93] M. Roitman. *Polynomial extensions of atomic domains*. J. Pure Appl. Algebra 87.2 (1993), 187–199. DOI: 10.1016/0022-4049(93)90122-A.

[Ros73] M. Rosen. *S-units and S-class group in algebraic function fields*. J. Algebra 26 (1973), 98–108.

[Ros76] M. Rosen. *Elliptic curves and Dedekind domains*. Proc. Amer. Math. Soc. 57.2 (1976), 197–201.

[SC07] S. Savchev and F. Chen. *Long zero-free sequences in finite cyclic groups*. Discrete Math. 307.22 (2007), 2671–2679. DOI: 10.1016/j.disc.2007.01.012.

[Sch16] W. A. Schmid. *Some recent results and open problems on sets of lengths of Krull monoids with finite class group*. In: *Multiplicative ideal theory and factorization theory*. Vol. 170. Springer Proc. Math. Stat. Springer, [Cham], 2016, 323–352. DOI: 10.1007/978-3-319-38855-7_14.

[Sme17] D. Smertnig. *Every abelian group is the class group of a simple Dedekind domain*. Trans. Amer. Math. Soc. 369.4 (2017), 2477–2491. DOI: 10.1090/tran/6868.

[Sze07] B. Szegedy. *Coverings of abelian groups and vector spaces*. J. Combin. Theory Ser. A 114.1 (2007), 20–34. DOI: 10.1016/j.jcta.2005.10.007.

[Tri19] S. Tringali. *Structural properties of subadditive families with applications to factorization theory*. Israel J. Math. 234.1 (2019), 1–35. DOI: 10.1007/s11856-019-1922-2.