Every Abelian Group is the Class Group of a Dedekind Domain

Jan Henrik Thomm

Geboren am 29. Juni 1999 in Unna

11. August 2020

Bachelorarbeit Mathematik

Betreuer: Dr. Thorsten Heidersdorf

Zweitgutachterin: Prof. Dr. Catharina Stroppel

Mathematisches Institut

Mathematisch-Naturwissenschaftliche Fakultät der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Contents

Abstract

Im Folgenden wird Claborns Beweis, dass jede abelsche Gruppe die Klassengruppe eines Dedekindrings ist, betrachtet und im Detail erläutert. Nach einem Überblick über einige Grundlagen der kommutativen Algebra wird der Monoid der gebrochenen Ideale und die Klassengruppe eines Ringes erläutert. Anschließend werden Krullringe als Verallgemeinerung von Dedekindringen untersucht und schließlich wird gezeigt, dass jede abelsche Gruppe die Klassengruppe eines Krullrings ist. Um abschließend Claborns Theorem zu beweisen, wird für einen beliebigen Krullring ein Dedekindring mit isomorpher Klassengruppe konstruiert.

Abstract

In this thesis Claborn's proof of his Theorem, that every abelian group is the class group of a Dedekind domain, will be re-examined and explained in detail. After revising some basic knowledge from commutative algebra, we will explore the concept of the divisor and class group, as well as Krull domains as a generalisation of Dedekind domains. We will prove, that every abelian group is isomorphic to the class group of a Krull domain, and then show, that for every Krull domain there is a Dedekind domain with an isomorphic class group.

Motivation

While studying algebraic number fields, Dedekind domains naturally occur as the integral closure of the integers. While they are not exactly unique factorisation domains, they have a unique factorisation property for their ideals into powers of prime ideals of height 1. But when is a Dedekind domain factorial? A useful tool, to determine how close a (completely integrally closed) domain is to being factorial, is its class group. Specifically, we will see, that the class group is 0 if and only if the domain is factorial. Moreover, a domain, whose class group is torsion, is also called "almost factorial". Details on this can be seen in [Fos73, p. 33, Chapter II, §6].

Since Dedekind domains fulfil a number of nice properties, one would hope, that these yield certain restrictions on the class group such that any Dedekind domain would not be too far off from being a unique factorisation domain. However, as the title of this thesis suggests, this does not hold true, since every abelian group can occur as the class group of a Dedekind domain. More precisely, the main Theorem of this thesis is the following Theorem by Luther Claborn.

Theorem 0.1 (Claborn).
Every abelian group is isomorphic to the class group of a Dedekind domain.

To prove this Theorem, we will follow the proof he gave in [Cla66]. For this, it will be necessary to consider Krull domains as a useful generalisation of both Dedekind domains and factorial rings.

Krull domains can also be seen as a generalisation of (normal) noetherian rings, as they fulfil a slightly weaker version of the maximality condition, which defines, what it means to be noetherian. This point of view also offers a different take on familiar concepts, such as factorial rings in terms of some sort of maximum condition. Some of this will be explored in Chapter 1.

In comparison to Dedekind domains, Krull domains offer the advantage of superior stability and allow to consider so called subintersections of the associate discrete valuation rings. Let us consider a Krull domain $A = \bigcap_{i \in I} R_{\nu_i}$ for discrete valuation rings R_{ν_i}. Then Nagata's Theorem will give us an epimorphism from the class group of A to the class group of a subintersection $B := \bigcap_{i \in J} R_{\nu_i}$ given by some $J \subseteq I$ along with a complete description of its kernel. This will be a useful tool to compute abstract class groups by finding unique factorisation domains as a subintersection, because then the given kernel will be the entirety of the class group. With this technique it will be possible to construct Krull domains with arbitrary class groups. To complete the main Theorem of this thesis, we will then apply our gained knowledge on Krull domains to construct a Dedekind domain for a pre-existing Krull domain, with the same class group.

However, the constructed Dedekind domain is rather abstract and far from the integers of a number fields, so the result is not directly applicable for algebraic number theory. Nonetheless, our results shows, that the class groups of the integers of a number field are not restricted by the fact, that they are Dedekind domains. If there are restrictions to these class groups, they are given by other constraints these Dedekind domains have. This will be further explored at the end of Chapter 4.

Notation and Requirements

Some basic knowledge in the field of commutative algebra is necessary, such as the notion of localisation and its prime ideals.

We will only consider commutative rings with 1 in this thesis and the units of such a ring R will be denoted by $R^\times$. More precisely R will usually be used for a domain with field of fractions $K := \mathrm{Frac}(R)$. The localization $S^{-1}R$ on a multiplicative set $S \subseteq R$ not containing 0 will be identified with the image of its canonical embedding into K given by $\frac{a}{b} \mapsto \frac{a}{b}$. This also includes $R \cong \{1\}^{-1}R$. For a prime ideal $\mathfrak{p} \subseteq R$ let $R_\mathfrak{p} := (R \setminus \mathfrak{p})^{-1}R$ denote the localisation at the complement of $\mathfrak{p}$. Moreover let R_ν denote the corresponding valuation ring of a valuation ν on a field F.

Some knowledge on polynomial rings over domains (in arbitrary many variables) is required, like the degree of a polynomial. Some details on this can be found in [ZS58, p. 18f., Chapter I, §18]. In particular, the element 0 will have degree $-\infty$. For a domain R and a polynomial $f \in R[X_i \mid i \in I]$ let I_f denote the set of indices of the variables occurring in f.

The span of a subset $U \subseteq M$ of an R-module M will be denoted by

$\langle U \rangle_R$ or just $\langle U \rangle$. This notation also includes submodules of R itself, i.e. ideals, and the set braces may be omitted if U is finite. In the case that U has only one element a, we will also write aR instead of $\langle a \rangle$. If this one element is just 0, we also write 0 instead of $\langle 0 \rangle$. This notation also includes groups. Additionally, if M is an R-algebra, the product of two submodules always references to the span of their pairwise multiplication. Furthermore submodules of R will be called integral ideals, as the term "ideal" will be reserved for fractionary ideals, which will be defined in Chapter 2. Both kinds of ideals will be denoted by $\mathscr{a}$, $\mathscr{b}$ and so forth, while prime ideals will be denoted by $\mathscr{p}$ or $\mathscr{q}$. Divisorial ideals will be denoted by the likes of $\overline{\mathscr{a}}$ and $\bar{\mathscr{b}}$.

The Krull domains considered later on will usually be referred to by A or B, where B often serves as a subintersection of A. For the sake of convenience we will see an empty intersection of discrete valuation rings of a field as the field itself. The reason for this will become apparent in Chapter 3. Last but not least, a Dedekind domain will usually be denoted by D.

We will have $\mathbb{N}$ denote the natural numbers including 0, $\mathbb{Z}$ denote the integers and $\mathbb{Q}$ the rational numbers. Additionally $\mathbb{C}$ will denote the complex numbers.

The axiom of choice will be assumed, but only needed in Chapter 4 to apply the theory of Krull domains to Dedekind domains. In particular we assume that every integral ideal is contained in a maximal ideal.

1 Backgrounds

In this Chapter some concepts from commutative algebra will be re-examined and fleshed out. A reader who is fluent in this language may skip certain sections and refer back to this Chapter if necessary. Nonetheless, this revision might be helpful in getting used to the notation, terminology and the style of this thesis.

1.1 (Partially) Ordered Groups

Partially ordered groups are not only interesting for us in the context of valuation groups of valuation rings. In Chapter 2.1 we will explore the realm of the partially ordered monoid of divisors. These will allow us to define Krull domains in Chapter 3 by demanding the monoid of divisors to be a lattices.

Moreover, the concepts of maximality and minimality will occur many times over the course of this thesis in different, yet similar contexts.

Definition 1.1 (Maxima and Minima).
Let $(S, \leq)$ be a partially ordered set. For a subset $U \subseteq S$ we say $a \in S$ is an upper (or lower) bound of U, if for every $b \in U$ we have $b \leq a$ (or $a \leq b$ respectively). Furthermore $b \in U$ is a greatest element, if it is an upper bound for U. And if $b \in U$ is a lower bound for U, then b is called smallest or lowest element of U. A smallest upper bound is called a *supremum* and a greatest lower bound is called an *infimum*.

We say an element $a \in U$ is *maximal* (or *minimal*) in U if for $b \in U$ $a \leq b$ implies $a = b$ (or if $b \leq a$ implies $a = b$ respectively). In particular, if U has a smallest or greatest element, it is the unique minimal or maximal element of U.

Last but not least, a total order $\leq$ is a *well-ordering* of S, if every subset has a smallest element.

Definition 1.2 (Order embedding).
We say a map $f : S \to T$ is *order embedding*, or an order embedding, if $(S, \leq)$ and $(T, \preceq)$ are partially ordered and for all $a, b \in S$ we get $a \leq b$ if and only if $f(a) \preceq f(b)$.

If $f : S \to T$ only satisfies $f(a) \preceq f(b)$ for $a \leq b$ with $a, b \in S$, we say f is *order preserving*. The map f is called *order reversing*, if for $a, b \in S$ with $a \leq b$ we get $f(b) \preceq f(a)$.

Definition 1.3 (Ordered groups).
A *partially ordered group* (or monoid) is an abelian group (or monoid) $(G, +)$ together with a relation $\leq$, so that $(G, \leq)$ is partially ordered and additionally $\leq$ is invariant under $+$, i.e. if $a \leq b$ for $a, b \in G$, then we have $a+c \leq b+c$ for all $c \in G$. In particular we have $a \leq b$ if and only if $-b \leq -a$.

We say $a \in G$ is *positive* if $0 < a$. The set of positive elements will be denoted by $G_{>0}$. Moreover, let $G_{\geq 0} := G_{>0} \cup \{0\}$ denote the non-negative elements.

Example 1.4.

(1) For a ring R, the set of (integral) ideals with multiplication of ideals is a partially ordered monoid, whose order is given by "$\subseteq$".

(2) The natural numbers $\mathbb{N}$ are well-ordered by the canonical order.

(3) We know that $(\mathbb{Z}, +, \leq)$ and $(\mathbb{Q}, +, \leq)$ are totally ordered groups and the canonical embedding is an order embedding.

(4) If $(G_i, +_i, \leq_i)_{i \in I}$ is a family of partially ordered group for some index set I. Then their direct sum $G := \bigoplus_{i \in I} G_i$ can be considered to be a partially ordered groups, where for $a, b \in G$ we have $a \leq b$ if and only if $a_i \leq b_i$ of for all $i \in I$, where a_i and b_i denote the projection of a and b in to G_i.

In the context of Krull domains there is a certain class of partially ordered groups that we are interested in, namely the following example.

Example 1.5. For an index set I consider the free group

$$\mathbb{Z}^{(I)} := \bigoplus_{i \in I} \mathbb{Z}$$

together with the partial order described above. Such a partially ordered group is called a *lattice* and has the following two properties:

a) Any two elements $a, b \in \mathbb{Z}^{(I)}$ have a supremum $\sup(a, b) = (\max\{a_i, b_i\})_{i \in I}$ and an infimum $\inf(a, b) = (\min\{a_i, b_i\})_{i \in I}$ in $\mathbb{Z}^{(I)}$.

b) Every non-empty subset of positive elements $\mathbb{Z}^{(I)}_{>0}$ has a minimal element, which can be obtained by fixing one element and minimizing any non zero entry, from which there are only finitely many.

In fact these two conditions give a complete characterisation of lattices as the next Theorem will show.

Theorem 1.6. *Let $(G, +, \leq)$ be a partially ordered group. Then G satisfies the following two conditions*

(a) Any two elements $a, b \in G$ have a supremum $\sup(a, b) \in G$ and infimum $\inf(a, b) \in G$.

(b) Every non-empty subset of positive elements has a minimal element.

if and only if

$$G_{\min} := \{a \in G_{\geq 0} \mid a \text{ is a mnimal element of } G_{\geq 0} \setminus \{0\}\}$$

is a free generating set such that the canonical isomorphism $\varphi\colon \mathbb{Z}^{(G_{\min})} \to G$ *is order embedding, i.e.* G *is (order embedding isomorphic to) a lattice.*

Proof. We have seen in Example 1.5 above that every lattice fulfils conditions (a) and (b). Thus we only have to show the converse.

Let $G_{\leq 0} := \{a \in G \mid a \leq 0\} = \{-a \mid a \in G_{\geq 0}\}$. Now for a fixed $a \in G$ we have $\sup(a, 0) \in G_{\geq 0}$ and $\inf(a, 0) \in G_{\leq 0}$. All of these exist by condition (a). Furthermore for $c := a - \sup(a, 0) \in G_{\leq 0}$ and $c' := a - \inf(a, 0) - a \in G_{\geq 0}$ we have

$$\inf(a, 0) = \inf(c + \sup(a, 0), 0) \geq c = a - \sup(a, 0)$$

and

$$\sup(a, 0) = \sup(c' + \inf(a, 0), 0) \leq c' = a - \inf(a, 0),$$

which shows, that $a = \inf(a, 0) + \sup(a, 0) \in G_{\leq 0} + G_{\geq 0}$.

Thus it is sufficient to show that $G_{\min}$ generates $G_{\geq 0}$ to show that $G_{\min}$ is a system of generators. If $G_{\geq 0} \setminus \langle G_{\min} \rangle$ was non-empty then there is a minimal element $a_0 \in G_{\geq 0} \setminus \langle G_{\min} \rangle$ by (b). However, $0 < a_0 \notin G_{\min}$, so there exists $0 < b_0 < a_0$. Because $a_0 < a_0 + b_0$, we have $0 < b_0, a_0 - b_0 < a_0$ and thus by the minimality of a_0 we get $b_0, a_0 - b_0 \in G_{\geq 0} \cap \langle G_{\min} \rangle$. Since this contradicts $a_0 = a_0 - b_0 + b_0 \notin \langle G_{\min} \rangle$, we must have $G_{\geq 0} \subseteq \langle G_{\min} \rangle$. Hence $G_{\min}$ is indeed a system of generators.

Note, that the argument above still works, if we only allow natural numbers as coefficients when generating. Hence $G_{\geq 0}$ can be generated by $G_{\min}$ with only non-negative coefficients.

Now assume there was a non trivial sum $\sum_{g \in G_{\min}} n_g g = 0$ with $n_g \in \mathbb{Z}$ for $g \in G_{\min}$ not all zero. Then splitting off the positive coefficients yields (by a small induction) a positive element

$$\sum_{\substack{g \in G_{\min} \\ n_g > 0}} n_g g = \sum_{\substack{g \in G_{\min} \\ n_g < 0}} -n_g g.$$

with positive coefficients. Take a minimal positive element $a = \sum_{g \in G_{\min}} n_g g = \sum_{g \in G_{\min}} m_g g$ with this property, i.e. for all $g \in G_{\min}$ we have $n_g, m_g \in \mathbb{N}$ not all equal. Then by the minimality of a, if $n_g > 0$, then $m_g = 0$ and vice versa. Since $a > 0$, there are $g_0, g_1 \in G_{\min}$ with $n_{g_0}, m_{g_1} > 0$ respectively. We have $g_0, g_1 \leq a$ and thus $a \geq \sup(g_0, g_1) = g_0 + g_1 > 0$, where the last equality is a consequence of the minimality of g_0 and g_1. Hence $b := a - g_0 - g_1 < a$ is non-negative and thus can be written as a sum of elements in $G_{\min}$. But then

$$0 < \sum_{g_0 \neq g \in G_{\min}} n_g g + (n_{g_0} - 1) g_0 = a - g_0 = g_1 + b < a$$

can be written as a sum of elements in $G_{\min}$ with or without g_1, contradicting the minimality of a.

Hence $G_{\min}$ is a free generating system. Lastly observe, that for $a, b \in G$ we have $\sum_{g \in G_{\min}} n_g g = a \leq b = \sum_{g \in G_{\min}} m_g g$ if and only if

$$0 \leq b - a = \sum_{g \in G_{\min}} (m_g - n_g) g,$$

which by the uniqueness of the (natural) coefficients of non-negative elements is the case if and only if we have $n_g \leq m_g$ for all $g \in G_{\min}$. □

1.2 Integral Ideals

We will generalise the notion of an (integral) ideal to the notion of a fractionary ideal in Chapter 2.1. However, it will be useful to recall some basics about this familiar case, as prime ideals will play a significant role in the divisor group of Krull domains.

Definition 1.7 (Integral ideals)**.**
Let R be a ring and $\mathfrak{a} \subseteq R$. Then $\mathfrak{a}$ is called an *integral ideal* if $\mathfrak{a}$ is an additive subgroup such that for any $a \in \mathfrak{a}$ and for all $b \in R$ we have $ab \in \mathfrak{a}$. In this case, if $\mathfrak{a} \neq R$, we say $\mathfrak{a}$ is proper and distinguish the following kinds of integral ideals:

An integral ideal $\mathfrak{a}$ is called a *prime ideal*, if the product ab of two elements $a, b \in R$ is an element of $\mathfrak{p} \ni ab$ only if a or b was an element of $\mathfrak{p}$.

An integral ideal $\mathfrak{a}$ is called *maximal ideal*, if it is maximal among the proper integral ideals partially ordered by "$\subseteq$".

Lemma 1.8. *For finitely many integral ideals $\{\mathfrak{a}_i\}_{i=0}^n$ of a ring R for some $n \in \mathbb{N}$, their product is contained in their intersection, i.e.*

$$\prod_{i=0}^n \mathfrak{a}_i \subseteq \bigcap_{i=0}^n \mathfrak{a}_i.$$

Proof. For $a := \prod_{i=0}^n a_i$ with $a_i \in \mathfrak{a}_i$ for $0 \leq i \leq n$ and a fixed $0 \leq j \leq n$ we have $a = a_j \cdot \prod_{\substack{i=0 \\ i \neq j}}^n a_i \in \mathfrak{a}_j$. Hence $a \in \bigcap_{i=0}^n \mathfrak{a}_i$. Thus the claim holds, since

$$\prod_{i=0}^n \mathfrak{a}_i = \left\langle \left\{ \prod_{i=0}^n a_i \;\middle|\; \forall i \in I \; a_i \in \mathfrak{a}_i \right\} \right\rangle.$$ □

Lemma 1.9. *Let $\{\mathfrak{a}_i\}_{i=0}^n$ be finitely many integral ideals of a ring R for some $n \in \mathbb{N}$. Then for every prime ideal $\mathfrak{p}$ of R containing the product of the integral ideals*

$$\prod_{i \in I} \mathfrak{a}_i \subseteq \mathfrak{p},$$

there is some $0 \leq j \leq n$ such that $\mathfrak{a}_j \subseteq \mathfrak{p}$.

The same holds true for the intersection of the integral ideals $\bigcap_{i=0}^n \mathfrak{a}_i$.

Proof. If for every $0 \le i \le n$ there is some $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$, then $\prod_{i=0}^n a_i \in (\prod_{i=0}^n \mathfrak{a}_i) \setminus \mathfrak{p}$, since $\mathfrak{p}$ is prime. So the claim is a direct consequence of this contraposition.

The last assertion is a consequence of Lemma 1.8 above. □

Lemma 1.10 (*Prime avoidance*).
Let $\{\mathfrak{p}_i\}_{i=0}^n$ be finitely many prime ideals of a ring R for some $n \in \mathbb{N}$. Then every integral ideal $\mathfrak{a}$ of R contained in the union of these prime ideals

$$\mathfrak{a} \subseteq \bigcup_{i=0}^n \mathfrak{p}_i$$

is already contained in one of the prime ideals $\mathfrak{p}_j \supseteq \mathfrak{a}$ for some $0 \le j \le n$.

Proof. If $n = 0$ there is nothing to show. Otherwise, if for every $0 \le j \le n$ there is some $a_j \in (\mathfrak{a} \cap \mathfrak{p}_j) \setminus \bigcup_{j \ne i \in I} \mathfrak{p}_i$, then

$$\prod_{i=0}^{n-1} a_i + a_n \in \mathfrak{a} \setminus \bigcup_{i \in I} \mathfrak{p}_i$$

since all the $\mathfrak{p}_i$ are prime. Thus, there is some $0 \le i_0 \le n$ with

$$(\mathfrak{a} \cap \mathfrak{p}_{i_0}) \setminus \bigcup_{i_0 \ne i \in I} \mathfrak{p}_i = \mathfrak{a} \setminus \bigcup_{i \ne i_0 \in I} \mathfrak{p}_i = \emptyset.$$

by contraposition. Now the claim holds by the induction hypothesis for

$$\mathfrak{a} \subseteq \bigcup_{\substack{i=0 \\ i \ne i_0}}^n \mathfrak{p}_i.$$ □

1.3 The Maximum Condition

The maximum condition will be a useful tool to generalise certain notions we will encounter over the course of this thesis such as noetherian domains or unique factorisation domains.

Definition 1.11 (Maximum condition).
A ring R satisfies the *maximum condition* for some subset $\mathcal{U} \subseteq \mathfrak{P}(R)$ of the power set of R, if every non-empty subset of $\mathcal{U}$ partially ordered by inclusion has a maximal element.

Definition 1.12 (Noetherian ring).
We say a ring R is *noetherian* if it satisfies the maximum condition for (proper) integral ideals, i.e. every non-empty set of (proper) integral ideals of R has an "$\subseteq$"-maximal element.

Lemma 1.13. *A ring R is noetherian if and only if every ideal is finitely generated. In particular principal ideal domains are noetherian.*

Proof. See [AM69, p.75, Chapter 6, Proposition 6.2] and recall that every ring is a module over itself. □

A first application of the maximum condition will follow in the next section in the form of a characterisation of unique factorisation domains.

1.4 Prime Factorisations

We will see, that prime elements will be very helpful when studying the class group of a (Krull) domain, as they do not directly contribute to said class group. With this in mind, unique factorisations as subintersections of Krull domains will prove to be a very helpful tool at the end of Chapter 3.

Definition 1.14. (Prime and irreducible elements)
Let R be a domain. Then we say $0 \neq a \in R$ is *prime* if aR is a prime ideal. If aR is "$\subseteq$"-maximal among $\{bR \mid b \in R \setminus R^\times\}$ then a is called *irreducible*.

Lemma 1.15. *Let R be a domain and $a, a' \in R$. Then we have:*

i) $aR = R \iff a \in R^\times$

ii) $aR = a'R \iff \exists e \in R^\times \; ae = a'$

iii) If p is prime, then p is irreducible.

Proof.

i) $aR = R \iff 1 \in aR \iff \exists b \in R \; ab = 1$

ii) $aR = a'R \iff e, e' \in R \; ae = a' \wedge a'e' = a \iff e \in R^\times \; ae = a'$

iii) Assume pR to be a prime ideal. If $pR \subseteq aR$, then there is $b \in R$ with $ab = p$. Hence $a \in pR$ and thus $aR = pR$, or $b = cp \in pR$. In the second case $acp = p$ and thus $ac = 1$ as R is a domain. Therefore $aR = R$ by i). Thus pR is maximal among principal ideals. □

Lemma 1.16. *Let R be a domain and let $a = e \prod_{i=1}^n p_i \in R$ be a product of prime elements $p_i \in R$ for $1 \leq i \leq n \in \mathbb{N}$ and some unit $e \in R^\times$.*

Then this product is unique in the sense, that for any other family of primes q_j for $1 \leq j \leq m \in \mathbb{N}$ and a unit e' such that $a = e' \prod_j^m q_j$, we have $m = n$ and there are units $e_i \in R^\times$ for $1 \leq i \leq n$ and a bijection $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $p_i = e_i q_{\sigma(i)}$ for any $1 \leq i \leq n$ and $e = e' \prod_{i=1}^n e_i$.

Proof. We proceed by induction on $n \in \mathbb{N}$. For $n = 0$ and a unit $e \in R^\times$ we have, if $e = e' \prod_j^m q_j$, then $q_j \in R^\times$ for $1 \leq j \leq m$. But by Lemma 1.15 prime elements must not be units, so $m = 0$ and $e = e'$.

Now for $n > 0$ let $e \prod_{i=1}^n p_i = e' \prod_j^m q_j$. Then using Lemma 1.9

$$\prod_{j=1}^m (q_j R) = \left(\prod_j^m q_j \right) R = \left(\prod_{i=1}^n p_i \right) R \subseteq p_1 R$$

shows that there is some $1 \leq k \leq m$ with $q_k R \subseteq p_1 R$. But the prime element q_k is irreducible by Lemma 1.15 and thus $p_1 R = q_k R$. Again by Lemma 1.15, there is some $e_1 \in R^\times$ such that $p_1 = e_1 q_k$. Hence

$$p_1 \left(e' e_1^{-1} \cdot \prod_{\substack{j \\ j \neq k}}^m q_j \right) = e' e_1^{-1} \cdot p_1 \cdot \prod_{\substack{j \\ j \neq k}}^m q_j = e' \prod_j^m q_j = e \prod_{i=1}^n p_i = p_1 \left(e \prod_{i=2}^n p_i \right)$$

and since $p_1 \neq 0$ and R is a domain

$$e' e_1^{-1} \cdot \prod_{\substack{j \\ j \neq k}}^m q_j = e \prod_{i=2}^n p_i.$$

As $e' e_1^{-1}$ is a unit, the rest is a consequence of the induction hypothesis. □

Definition 1.17 (Unique factorisation domains)**.**
Let R be a domain. Then R is a *unique factorisation domain* or factorial, if every non-zero element $0 \neq a \in R$ can be written as a product of a unit and prime elements.

Remark 1.18. The definition above coincides with the usual definition given in [ZS58, p. 21, Chapter I, §14], since if every element has a unique factorisation into irreducible elements, all irreducible elements must be prime. This can also be seen in [ZS58, p. 21f., Chapter I, §14]. The other direction is a consequence of Lemma 1.16 and the fact, that prime elements are irreducible by Lemma 1.15.

Lemma 1.19. *For a domain R the following are equivalent:*

i) R is a unique factorisation domain.

ii) Every irreducible element of R is prime and R satisfies the maximum condition for the set $\{aR \mid a \in R\}$ of principal integral ideals.

Proof.

"⇒" Let $a \in R$. Then $a = e \prod_{i=1}^{n} p_i$ for a natural number $n \in \mathbb{N}$ and prime elements $p_1, \ldots, p_n \in R$. Then by the uniqueness of the factorisation given in Lemma 1.16, aR is only contained in the principal integral ideals $\left(e \prod_{i \in I} p_i\right) R$, where I is a subset of $\{1, ..., n\}$. Thus every principal integral ideal is only contained in finitely many principal integral ideals. Therefore the maximum condition holds. Furthermore a is irreducible if and only if $n = 1$, which is equivalent to a being prime.

"⇐" Consider the set of all non-zero non-units, which cannot be written as a product of irreducible elements,

$$U := \{0 \neq a \in R \setminus R^{\times} \mid a \text{ is not a product of irreduciable elements}\}.$$

If $U \neq \emptyset$ is non-empty, let $a \in U$ be such that aR is "$\subseteq$"-maximal in $\{bR \mid b \in U\}$. As $a \in U$, a is neither irreducible nor a unit and thus it can be written as $a = bc$ for some $b \in R \setminus R^{\times}$ and $c \in R$ with $aR \subsetneq bR$. Hence $c \in R \setminus R^{\times}$ with $aR \subsetneq cR$. Because aR is "$\subseteq$"-maximal in U, we have $b, c \notin U$ and so they can be written as a product of irreducible elements and a unit. But this is a contradiction to $a \in U$, so U must be empty. Therefore every element of R is a product of prime elements and a unit, since every irreducible element is prime. □

Corollary 1.20. *Principal ideal domains are unique factorisation domains.*

Proof. Combine the fact that maximal ideals are prime and that principal ideal domains are noetherian with Lemma 1.19 above. □

Lemma 1.21. *Let $p \in R$ be a prime element of a domain R. Then $p \in R[X]$ is a prime element of the polynomial ring over R.*

Proof. As the degree of a product of polynomials is additive, the polynomial ring $R[X]$ is a domain. Now for two polynomials $f, g \in R[X]$ with $fg \in pR[X]$ we have $f \in pR[X]$ or $g \in pR[X]$ by a small induction over the degree of f and g. So $p \in R[X]$ is again prime. □

Corollary 1.22. *If R is a domain and I is some index set, then a polynomial $f \in R[X_i|i \in I]$ in the polynomial ring is prime if and only if for the index set of variables in f, $I_f \subseteq I$ the polynomial $f \in R[X_i \mid i \in I_f]$ is prime.*

Proof. Consider the ring homomorphism given by the inclusion $R[X_i \mid i \in I_f] \subseteq R[X_i \mid i \in I]$. This shows, that if $fR[X_i \mid i \in I]$ is a prime ideal, then

$$fR[X_i \mid i \in I_f] = fR[X_i \mid i \in I] \cap R[X_i \mid i \in I_f]$$

is also a prime ideal as a preimage of a prime ideal.

Conversely, let $f \in R[X_i \mid i \in I_f]$ be prime and consider $a, b \in R[X_i \mid i \in I]$ such that $ab \in fR[X_i \mid i \in I]$. Hence there is some $g \in R[X_i \mid i \in I]$ with $ab = fg$. Define $J := I_a \cup I_b \cup I_f \cup I_g$ as the union of the index sets of variables for the polynomials a, b, g and f, which is again finite. By a small induction using Lemma 1.21, $f \in R[X_i \mid i \in J]$ is prime and $ab = fg \in fR[X_i \mid i \in J]$. Therefore

$$a \in fR[X_i \mid i \in J] \quad \text{or} \quad b \in fR[X_i \mid i \in J].$$

Now the claim is a consequence of $fR[X_i \mid i \in J] \subseteq fR[X_i \mid i \in I]$. □

Lemma 1.23. *Let R be a domain and $a, b \in R$ with $b \neq 0$ such that $aR \cap bR = abR$. Then $bX - a \in R[X]$ is prime.*

Proof. We base this proof on [Fos73, p.61, Chapter III, §14, Lemma 14.1].

To show, that $bX - a$ is prime, it suffices to verify, that every polynomial $g \in R[X]$, which has $\frac{a}{b} \in \mathrm{Frac}(R)$ as a root, already is an element of $\langle bX - a \rangle$, because the roots of a polynomial are multiplicative. If the degree of g is smaller than 1, $g = 0$ and the claim is true. Now for the degree $n \geq 1$ of $g = \sum_{i=0}^{n} a_i X^i$ with $g(\frac{a}{b}) = 0$ we have

$$0 = b^n g(\frac{a}{b}) = \sum_{i=0}^{n} a_i a^i b^{n-i}.$$

Thus $a_n a^n = -\sum_{i=0}^{n-1} a_i a^i b^{n-i} \in a^n R \cap bR = a^n bR$, where the last equality is the consequence of a small induction on n. Hence $a_n = a'_n b \in bR$ for some $a'_n \in R$ and therefore

$$g = a'_n(bX - a)X^{n-1} + (a'_n a + a_{n-1})X^{n-1} + \sum_{i=0}^{n-2} a_i X^i = a'_n(bX - a)X^{n-1} + g'$$

for some polynomial $g' \in R[X]$ with zero $\frac{a}{b}$ and a smaller degree. So by induction $g' \in \langle bX - a \rangle$ and thus $g \in \langle bX - a \rangle$. □

Theorem 1.24.
Let R be a unique factorisation domain. Then the polynomial ring $R[X]$ is also a unique factorisation domain.

Proof. See [ZS58, p. 32, Chapter I, §17, Theorem 10] □

Corollary 1.25. *If R is a unique factorisation domain and I is some index set, then the polynomial ring $R[X_i \mid i \in I]$ is again a unique factorisation domain.*

Proof. Let $f \in R[X_i \mid i \in I]$ and let $I_f \subseteq I$ be a finite subset of I such that $f \in R[X_i \mid i \in I_f] \subseteq R[X_i \mid i \in I]$. Then by Theorem 1.24 and a small induction on the number of variables, $R[X_i \mid i \in I_f]$ is a unique factorisation domain and thus f can be written as a product of prime elements and a unit. By Corollary 1.22 above, these prime factors are again prime in $R[X_i \mid i \in I]$. □

Example 1.26.

(1) Any field K is a unique factorisation domain as every non-zero element is a unit.

(2) The integers $\mathbb{Z}$ are a unique factorisation domain with the prime numbers as prime elements up to a sign.

(3) Any polynomial over one of the examples above is a unique factorisation domain by Corollary 1.25.

1.5 Completely Integrally Closed Domains

We will see in Chapter 2.1, how we can only really talk about a class group rather than a monoid, if the considered domain is completely integrally closed. Additionally Dedekind domains occur as the integral closure of $\mathbb{Z}$ in finite field extensions over $\mathbb{Q}$, which makes the notion of integral closure even more interesting to us.

Definition 1.27 ((Almost) integral elements)**.**
Let R be a subring of a ring R' and let $a \in R'$.

Then a is *integral* over R, if there is a monic polynomial $p(X) = X^{n+1} + \sum_{i=0}^{n} a_i X^i \in R[X]$ with root a, i.e. $p(a) = 0$.

Furthermore, $a \in R'$ is *almost integral* over R, if for the R-module $R[a] := \langle \{a^n \mid n \in \mathbb{N}\} \rangle \subseteq R'$ there is some $d \in R \setminus \{0\}$ such that $dR[a] \subseteq R$. In other words, there is a $d \in R$ such that $da^n \in R$ for all $n \in \mathbb{N}$. Such a d is called a common denominator of $R[a]$.

Remark 1.28. An element $a \in \mathrm{Frac}(R)$ is almost integral if and only if $R[a]$ is a fractionary ideal over R in the sense of Definition 2.1, which will occur in Chapter 2.

Lemma 1.29. *For a subring R of a ring a R' the set of integral elements over R, $\bar{R} := \{a \in R' \mid a \text{ integral over } R\}$, forms a subring of R' containing R.*

Proof. See [Nag62, p. 29, Chapter I, 10., (10.2) Corollary]. □

Lemma 1.30. *Let R be a domain with field of fractions $K := \mathrm{Frac}(R)$. Let $a \in K$. The following hold:*

i) Every integral element of K is almost integral over R.

ii) If R is noetherian, every almost integral element of K is integral.

Proof.

i) Let $a \in K$ be integral. Then we have for some $n \in \mathbb{N}$ $a^{n+1} = \sum_{i=0}^{n} a_i a^i$. Thus $R[a] = \langle \{a^m \mid m \in \mathbb{N}\} \rangle$ is generated by $\{1, a, ..., a^n\}$. Now assume $a = \frac{c}{d}$ for some $c, d \in R$. Then we have $d^n a^j \in R$ for any $n \in \mathbb{N}$.

ii) Assume R to be noetherian, $a \in K$ to be almost integral and let d be a common dominator of $R[a]$. Then $dR[a]$ is an integral ideal and thus finitely generated. Therefore $R[a]$ is finitely generated and thus there is some $n \in \mathbb{N}$ such that $R[a] = \langle 1, a, \ldots, a^n \rangle$. Hence there are $a_0, \ldots, a_n \in R$ such that $a^{n+1} = \sum_{i=0}^{n} a_i a^i$. From this we get that a is a root of $X^{n+1} + \sum_{i=0}^{n}(-a_i)X^i \in R[X]$. Therefore a is integral over R. □

Definition 1.31 ((Completely) integrally closed domains)**.**
A domain R is called *normal* or integrally closed, if every integral element over R of the fraction field $K := \mathrm{Frac}(R)$ is already an element of R.

It is called *completely integrally closed*, if every almost integral element over R of K is an element of R.

Corollary 1.32. *A completely integrally closed domain is normal.*

Proof. This is a direct consequence of Lemma 1.30i). □

Proposition 1.33. *An normal noetherian domain is completely integrally closed.*

Proof. This is a direct consequence of Lemma 1.30ii). □

Remark 1.34. We will later see, that the converse is not true as $\mathbb{Z}[X_n \mid n \in \mathbb{N}]$ is completely integrally closed but not noetherian.

Another non-noetherian example is a valuation ring with valuation group $\mathbb{Q}$, which is left as an exercise for the interested reader.

Lemma 1.35. *Let $(R_i)_{i \in I}$ be a family of (completely) integrally closed subrings of a domain R'. Then $R := \bigcap_{i \in I} R_i$ is (completely) integrally closed.*

Proof. Let $a \in \mathrm{Frac}(R) \subseteq \mathrm{Frac}(R')$ be (almost) integral over R. Then a is (almost) integral over R_i for any $i \in I$ as $a \in \mathrm{Frac}(R) \subseteq \mathrm{Frac}(R_i)$. As the R_i are (completely) integrally closed, $a \in R_i$ for any $i \in I$, we have $a \in R$. Therefore R is also (completely) integrally closed. □

1.6 (Discrete) Valuation Rings

Discrete valuation rings are an important part of the generalisation of Dedekind domains to Krull domains. While Dedekind domains have the property to be the intersection of discrete valuation rings, Krull domains can be defined to be the intersection of discrete valuation rings with a certain finiteness assumption.

Some claims in this section may stay without proof. These can be found in [ZS60, p.32-35, Chapter VI, §8].

Definition 1.36 (Valuation ring)**.**
Let $(G, +, \leq)$ be a totally ordered group and let K be a field. For later use extend G with an element ∞ such that ∞ is an upper bound for G and for $a \in G$ $a + \infty := \infty + a := \infty$.

Then a *valuation* is a group homomorphism $\nu : K^\times \to G$ such that for $a, -a \neq b \in K^\times$ we have $\min\{\nu(a), \nu(b)\} \leq \nu(a + b)$. In this case we define $\nu(0) := \infty$.

We call the subring $R_\nu := \{a \in K \mid \nu(a) \geq 0\}$ of K a *valuation ring* for a valuation ν on K. Moreover, any domain R, for which there is a field K with a valuation ν such that $R = R_\nu$ is called a valuation ring.

We say R_ν is a *discrete valuation ring* if the *valuation group* $\nu(K^\times)$ is equal to $\mathbb{Z}$ with the canonical ordering. In this manner, a valuation is called a *discrete valuation*, if it maps surjectively into $\mathbb{Z}$.

Lemma 1.37. *Let K be a field with valuation $\nu : K^\times \to G$. Then:*

i) $\forall a \in K^\times\ a \in R_\nu \lor a^{-1} \in R_\nu$

ii) $a \in R^\times \iff \nu(a) = 0$

iii) $\forall a, b \in R_\nu (\nu(a) \leq \nu(b) \iff bR_\nu \subseteq aR_\nu)$

iv) *R_ν has the unique maximal ideal $\mathfrak{m} := \{a \in R \mid \nu(a) > 0\}$.* □

Proposition 1.38. *A ring R is a valuation ring if and only if R is a domain and we have $a \in R$ or $a^{-1} \in R$ for $a \in \operatorname{Frac}(R)^\times$. In this case, a valuation with valuation ring R_ν is given by the projection into $\operatorname{Frac}(R)^\times / R^\times$, where the order is given by $a \leq b$ if and only if $\frac{b}{a} \in R$.* □

Corollary 1.39. *Two surjective valuations on a field K, $\nu\colon K^\times \to G'$ and $\nu'\colon K^\times \to G$, are equal up to an order embedding isomorphism of G and G' if and only if their valuation rings are the same.*

In this case, if both ν and ν' are discrete, we have $\nu = \nu'$, because the identity is the only order embedding automorphism of $\mathbb{Z}$. □

Remark 1.40. Proposition 1.38 and Corollary 1.39 above show, that a valuation ring R_ν of a valuation ν encodes the valuation in sufficient detail.

Proposition 1.41. *Let $(G, +, \leq)$ be a totally ordered group and let $K := \mathrm{Frac}(R)$ be the fraction field of a domain R. Then it is sufficient to to define a valuation $\nu\colon K^\times \to G$ on $R \setminus \{0\}$ as a monoid homomorphism satisfying $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$ for $a \neq -b \in R \setminus \{0\}$ and extend it uniquely to K by $\nu(\frac{a}{b}) := \nu(a) - \nu(b)$.*

Proof. Assume $\nu\colon R \setminus \{0\} \to G$ was defined as required. As the map $\nu\colon K^\times \to G$ is supposed to be a valuation, the extension described above is the only possibility. It is well defined, since for two fractions $\frac{a}{b}, \frac{c}{d} \in K^\times$, we have $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$ and thus $\nu(a) + \nu(d) = \nu(ad) = \nu(bc) = \nu(b) + \nu(c)$. This is equivalent to $\nu(a) - \nu(b) = \nu(c) - \nu(d)$.

Moreover for $\frac{a}{b}, \frac{c}{d} \in K^\times$ we get

$$\nu\Big(\frac{a}{b} \cdot \frac{c}{d}\Big) = \nu\Big(\frac{ac}{bd}\Big) = \nu(ac) - \nu(bd) = \nu(a) - \nu(b) + \nu(c) - \nu(d)$$

and

$$\nu\Big(\frac{a}{b} + \frac{c}{d}\Big) = \nu(\frac{ad+bc}{bd}) = \nu(ad+bc) - \nu(bd) \geq \nu(ad) - \nu(bd) = \nu\Big(\frac{a}{b}\Big),$$

where without loss of generality $\nu(ad) \leq \nu(bc)$. □

Lemma 1.42. *Let K be a field and let $\nu\colon K^\times \to \mathbb{Z}$ be a discrete valuation. Then the discrete valuation ring R_ν is an "$\subseteq$"-maximal subring of K.*

Proof. Let $R_\nu \subsetneq R \subseteq K$ be a subring of K strictly containing R_ν. Then there is some $a \in R \backslash R_\nu$ and thus $\nu(a) < 0$. As ν is discrete, pick some $b \in R_\nu$ with $\nu(b) = -\nu(a) - 1$ so that $\nu(ab) = -1$. Now for any $c \in R_\nu \setminus \{0\}$ we have $c \in R^\times$, since $\nu(c(ab)^{\nu(c)}) = 0$. Thus, by Lemma 1.37, $c(ab)^{\nu(c)} \in R_\nu^\times \subseteq R^\times$. Now as for every $d \in K^\times$, again by Lemma 1.37, we have $d \in R_\nu \subseteq R$ or $d^{-1} \in R_\nu \subseteq R$, so we must have $R = K$. □

Lemma 1.43. *A valuation ring R is discrete valuation ring if and only if it is noetherian and not a field.*

Proof. As an easy consequence of Lemma 1.37 every finitely generated ideal is principal. Thus R is a principal ideal domain if and only if R is noetherian.

Now if R is a discrete valuation ring, then every integral ideal $\mathfrak{a}$ is generated by some $a \in \mathfrak{a}$ with $\nu(a) = \min_{b \in \mathfrak{a}}\{\nu(b)\}$, which exists since $\mathbb{N}$ is well-ordered.

Conversely if R is a principal ideal domain, then R is a unique factorisation domain by Corollary 1.20. Furthermore every prime element generates the unique maximal ideal of R, since every prime element is irreducible. So Example 1.46 will show us, how to construct a discrete valuation with valuation ring R. □

Lemma 1.44. *Let R be a valuation ring. Then R is normal.*

Proof. Let $a \in \operatorname{Frac}(R)$ be integral over R, i.e. there is an $n \in \mathbb{N}$ and $a_i \in R$ for $0 \leq i \leq n$ such that $a^{n+1} = \sum_{i=0}^{n} a_i a^i$. Now by Lemma 1.37, we have $a \in R$ or $a^{-1} \in R$. In the first case there is nothing to show. In the second case, we get

$$a = a^{-n} a^{n+1} = \sum_{i=0}^{n} a_i (a^{-1})^{n-i} \in R,$$

which shows, that R is normal. □

Corollary 1.45. *Discrete valuation rings are completely integrally closed.*

Proof. By Lemma 1.43 and 1.44 above any discrete valuation ring is noetherian and normal. Hence by Proposition 1.33 any discrete valuation ring is completely integrally closed. □

Example 1.46. Let R be a unique factorisation domain with field of fractions $K := \operatorname{Frac}(R)$. Then for a prime $p \in R$ there is a valuation

$$\begin{aligned} \nu_p : K^\times &\to \mathbb{Z} \\ \frac{a}{b} &\mapsto \nu_p(a) - \nu_p(b) \end{aligned}$$

where for $a \in R$ the valuation $\nu_p(a) := \max_{n \in \mathbb{N}}\{n \mid a \in p^n R\}$ is the maximal natural number for which a power of p can occur in a prime factorisation of a.

The valuations obtained in such a way are called essential valuations of R and and we have the equality $R_{\nu_p} = R_{\langle p \rangle}$ for the discrete valuation ring R_{ν_p}.

Furthermore any element of R is a unit in almost all R_{ν_p}, i.e. has valuation 0 for almost all prime elements of R and

$$R = \bigcap_{\substack{p \in R \\ p \text{ prime}}} R_{\nu_p} = \bigcap_{\substack{p \in R \\ p \text{ prime}}} R_{\langle p \rangle}.$$

2 The Class Group

The class group of a domain measures, in a certain manner, how far away a domain is from being a unique factorisation domain. We will establish this connection at the end of Chapter 3.1 in more detail. As we not only plan to study the class groups of Dedekind domains, but also the class groups of Krull domains, we will now define the notion in a more general manner for a certain class of domains. For this, we will follow the first two sections of the first Chapter of [Sam64, p.1-4, Chapter I, §1-2].

From now on let R be a domain with field of fractions $K := \mathrm{Frac}(R)$ if not stated otherwise.

2.1 Divisor Groups

Contrary to Dedekind domains, for a general domain it is not sufficient to consider the monoid of fractionary ideals to define the class group. Therefore we will now develop the notion of a divisorial ideal and the partially ordered monoid of divisors. Furthermore we will explore, in which cases this monoid is a group. We will see in Chapter 4 why this notion is redundant for Dedekind domains. However, it will be important for studying Krull domains in Chapter 3.

Definition 2.1 (Fractionary Ideals)**.**
A fractionary ideal, or *ideal*, of a domain R is an R-module $\mathfrak{a} \subseteq K := \mathrm{Frac}(R)$ such that there is some $d \in R \setminus \{0\}$, so that $d\mathfrak{a} \subseteq R$. Such a d is called a common denominator of $\mathfrak{a}$.

A fractionary ideal $\mathfrak{a}$ is called *principal*, if there is some $a \in K$ generating $\mathfrak{a}$, i.e. $\mathfrak{a} = aR = \langle a \rangle_R$. Non-zero fractionary ideals, which are the intersection of principal ideals, are called *divisorial ideals*.

For a non-zero fractionary ideal $\mathfrak{a}$ define

$$\overline{\mathfrak{a}} := \bigcap_{\substack{a \in K \\ \mathfrak{a} \subseteq aR}} aR$$

to be the smallest divisorial ideal containing $\mathfrak{a}$. This intersection exists, as we have $\mathfrak{a} \subseteq \frac{1}{d}R$ for any common denominator d .

Example 2.2. Let R be a domain with field of fration $K := \mathrm{Frac}(R)$.

(1) Every integral ideal $\mathfrak{a} \subseteq R \subseteq K$ is a module over R, so the common denominator 1 shows that integral ideals are (fractionary) ideals. Conversely, every fractionary ideal $\mathfrak{a} \subseteq R$ is an integral ideal.

(2) Any module of the form aR for $a \in K^\times$ is a fractionary ideal, where the denominator of a is a common denominator of aR. Thus, all modules of this kind are principal ideals.

(3) Intersections, sums and finite product of submodules of the R-module K are again submodules.

Hence, finite sums and products of ideals are ideals by multiplying one common denominator each. Moreover, arbitrary intersections of ideals are ideals, where one can simply take one common denominators of any one of the intersected ideals as a common denominator of the intersection.

(4) Any non-zero submodule of K, that is an intersection of principal ideals, is an ideal and thus divisorial.

(5) Consider the polynomial ring in two variables $R := F[X,Y]$ over a field F together with the (integral) ideal $\langle X, Y\rangle$. Then

$$\begin{aligned}\mathfrak{a} :=&\{a \in K := \mathrm{Frac}(R) \mid a\langle X, Y\rangle \subseteq R\} \\ =&\{a \in K \mid aX \in R \ni aY\} = R.\end{aligned}$$

We will see in Lemma 2.4 that

$$\overline{\langle X, Y\rangle} = \{a \in K \mid a\mathfrak{a} \subseteq R\} = \{a \in K \mid a \cdot 1 \in R\} = R,$$

so generally, ideals cannot be assumed to be divisorial.

We will see in Example 3.42 a more interesting example of an integral ideal contained in an "$\subseteq$"-minimal non-zero prime ideal, which is not divisorial.

Lemma 2.3. *Let $\mathfrak{a}$ be a (fractionary) ideal of a domain R and $\mathfrak{b} \neq 0 \neq \mathfrak{b}'$ be submodules of $K := \mathrm{Frac}(R)$. Then $(\mathfrak{a} : \mathfrak{b}) := \{x \in K \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$ defines an ideal. Furthermore the following relations hold:*

i) For I and J index sets and ideals $\mathfrak{a}_i$ for $i \in I$ and submodules $0 \neq \mathfrak{b}_j \subseteq K$ for $j \in J$ we have

$$\left(\left(\bigcap_{i\in I} \mathfrak{a}_i\right) : \left(\sum_{j\in J} \mathfrak{b}_j\right)\right) = \bigcap_{\substack{i\in I\\ j\in J}} (\mathfrak{a}_i : \mathfrak{b}_j).$$

ii)

$$(\mathfrak{a} : \mathfrak{b}\mathfrak{b}') = \big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{b}'\big)$$

iii) If $0 \neq a \in K$, then

$$(\mathfrak{b} : aR) = a^{-1}\mathfrak{b}.$$

iv) If $\mathfrak{b}$ is also a fractionary ideal, then $(\mathfrak{a} : \mathfrak{b}) = 0$ if and only if $\mathfrak{a} = 0$.

v) If $\mathfrak{a}$ is divisorial and $\mathfrak{b}$ is an ideal, then $(\mathfrak{a} : \mathfrak{b})$ is divisorial.

Proof. First of all, we need to establish, that $(\mathfrak{a} : \mathfrak{b})$ is in fact a submodule. It is closed under the addition of $(K, +)$ as for $x, y \in (\mathfrak{a} : \mathfrak{b})$

$$(x + y)\mathfrak{b} \subseteq x\mathfrak{b} + y\mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{a} = \mathfrak{a}$$

and $0\mathfrak{b} = 0 \subseteq \mathfrak{a}$. Moreover, for $x \in (\mathfrak{a} : \mathfrak{b})$ and $r \in R$ the equation $(xr)\mathfrak{b} = x(r\mathfrak{b}) \subseteq x\mathfrak{b} \subseteq \mathfrak{a}$ shows that $(\mathfrak{a} : \mathfrak{b})$ is indeed a submodule.

If $0 \neq \mathfrak{b} \subseteq K$ is an R-module, then $\mathfrak{b} \cap R \neq 0$, since for $0 \neq \frac{b}{a} \in \mathfrak{b}$ we have $0 \neq b = a \cdot \frac{b}{a} \in \mathfrak{b} \cap R$. So if d is a common denominator of the fractional ideal $\mathfrak{a}$ and $0 \neq b \in \mathfrak{b} \cap R$, then

$$db(\mathfrak{a} : \mathfrak{b}) \subseteq d\mathfrak{b}(\mathfrak{a} : \mathfrak{b}) \subseteq d\mathfrak{a} \subseteq R$$

shows, that $(\mathfrak{a} : \mathfrak{b})$ is a fractional ideal with common denominator db.

Now it remains to verify the relations.

i) From Example 2.2 above we know, that $\Big(\big(\bigcap_{i\in I} \mathfrak{a}_i\big) : \big(\sum_{j\in J} \mathfrak{b}_j\big)\Big)$ is well defined and the computation

$$\begin{aligned}\Bigg(\Big(\bigcap_{i\in I} \mathfrak{a}_i\Big) : \Big(\sum_{j\in J} \mathfrak{b}_j\Big)\Bigg) &= \left\{ x \in K \;\middle|\; \forall i \in I\ x\Big(\sum_{j\in J} \mathfrak{b}_j\Big) \subseteq \mathfrak{a}_i \right\} \\ &= \bigcap_{i\in I} \left\{ x \in K \;\middle|\; x\Big(\sum_{j\in J} \mathfrak{b}_j\Big) \subseteq \mathfrak{a}_i \right\} \\ &= \bigcap_{i\in I}\bigcap_{j\in J} \{x \in K \mid x\mathfrak{b}_j \subseteq \mathfrak{a}_i\} = \bigcap_{\substack{i\in I\\ j\in J}} (\mathfrak{a}_i : \mathfrak{b}_j)\end{aligned}$$

yields the result.

ii) The product of two non-zero submodules is again non-zero. So everything is well defined and furthermore

$$\begin{aligned}\big(\mathfrak{a} : \mathfrak{b}\mathfrak{b}'\big) &= \big\{x \in K \mid x\mathfrak{b}\mathfrak{b}' \subseteq \mathfrak{a}\big\} \\ &= \big\{x \in K \mid x\mathfrak{b}' \subseteq (\mathfrak{a} : \mathfrak{b})\big\} = \big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{b}'\big)\end{aligned}$$

holds.

iii) For $0 \neq a \in K$

$$\begin{aligned}(\mathfrak{b} : aR) &= \{x \in K \mid x \cdot aR \subseteq \mathfrak{b}\} = \{x \in K \mid ax \in \mathfrak{b}\} \\ &= \big\{x \in K \mid x \in a^{-1}\mathfrak{b}\big\} = a^{-1}\mathfrak{b}\end{aligned}$$

holds.

iv) If $\mathfrak{a} = 0$, then $(\mathfrak{a} : \mathfrak{b}) = 0$ because K is a domain and $\mathfrak{b} \neq 0$. On the other hand, if $0 \neq \mathfrak{a}$, then $0 \neq a \in \mathfrak{a} \cap R$. So if d is a common denominator of $\mathfrak{b}$, then $ad \in (\mathfrak{a} : \mathfrak{b})$, since $ad\mathfrak{b} \subseteq aR \subseteq \mathfrak{a}$.

v) Let $\mathfrak{a} = \bigcap_{i\in I} a_iR$ be divisorial and $\mathfrak{b}$ be an ideal. Then by iv) $(\mathfrak{a} : \mathfrak{b}) \neq 0$ already holds and

$$
\begin{aligned}
(\mathfrak{a} : \mathfrak{b}) &= \left(\left(\bigcap_{i\in I} a_iR\right) : \left(\sum_{0\neq b\in\mathfrak{b}} bR\right)\right) \\
&\overset{i)}{=} \bigcap_{\substack{i\in I\\ 0\neq b\in\mathfrak{b}}} (a_iR : bR) \overset{iii)}{=} \bigcap_{\substack{i\in I\\ 0\neq b\in\mathfrak{b}}} a_ib^{-1}R
\end{aligned}
$$

shows, that $(\mathfrak{a} : \mathfrak{b})$ is in fact divisorial. □

Lemma 2.4. *Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \neq 0$ be non-zero ideals. Then the following additional relations hold.*

i) $\mathfrak{b} \subseteq \mathfrak{a} \implies (\mathfrak{c} : \mathfrak{a}) \subseteq (\mathfrak{c} : \mathfrak{b})$

ii) $\overline{\mathfrak{a}} = (R : (R : \mathfrak{a}))$

iii) $(R : (R : (R : \mathfrak{a}))) = (R : \mathfrak{a})$

iv) $\overline{\mathfrak{a}} = \overline{\mathfrak{b}} \iff (R : \mathfrak{a}) = (R : \mathfrak{b})$

Proof.

i) Let $\mathfrak{b} \subseteq \mathfrak{a}$. Let $x \in K$ such that $x\mathfrak{a} \subseteq \mathfrak{c}$. Then $x\mathfrak{b} \subseteq x\mathfrak{a} \subseteq \mathfrak{c}$. Hence $(\mathfrak{c} : \mathfrak{a}) \subseteq (\mathfrak{c} : \mathfrak{b})$.

ii) By Lemma 2.3 v) above, the ideal $(R : (R : \mathfrak{a}))$ is divisorial as $R = 1R$ is principal and thus divisorial. Furthermore

$$
\begin{aligned}
(R : (R : \mathfrak{a})) &= \{x \in K \mid x(R : \mathfrak{a}) \subseteq R\} \\
&= \{x \in K \mid \forall y \in K\ y\mathfrak{a} \subseteq R \Rightarrow xy \in R\} \supseteq \mathfrak{a}
\end{aligned}
$$

and therefore $\overline{\mathfrak{a}} \subseteq (R : (R : \mathfrak{a}))$.

Now let $a \in K$ such that $\mathfrak{a} \subseteq aR$. Applying i) two times yields

$$
(R : (R : \mathfrak{a})) \overset{i)}{\subseteq} (R : (R : aR)) \overset{2.3\,iii)}{=} (R : a^{-1}R) \overset{2.3\,iii)}{=} aR
$$

and therefore

$$
\overline{\mathfrak{a}} \subseteq (R : (R : \mathfrak{a})) \subseteq \bigcap_{\substack{a\in K\\ \mathfrak{a}\subseteq aR}} aR = \overline{\mathfrak{a}}.
$$

iii) As before $(R : \mathfrak{a})$ is divisorial by Lemma 2.3v). Hence

$$
(R : \mathfrak{a}) = \overline{(R : \mathfrak{a})} \overset{ii)}{=} (R : (R : (R : \mathfrak{a}))).
$$

iv) If $(R : \mathfrak{a}) = (R : \mathfrak{b})$ then

$$\overline{\mathfrak{a}} \overset{ii)}{=} (R : (R : \mathfrak{a})) = (R : (R : \mathfrak{b})) \overset{ii)}{=} \bar{\mathfrak{b}}.$$

If on the other hand $\overline{\mathfrak{a}} = \bar{\mathfrak{b}}$, applying iii) yields

$$(R : \mathfrak{a}) \overset{iii)}{=} (R : (R : (R : \mathfrak{a}))) \overset{ii)}{=} (R : \overline{\mathfrak{a}}) = (R : \bar{\mathfrak{b}}) \overset{ii)+iii)}{=} (R : \mathfrak{b}),$$

which proves the equivalence. ☐

Corollary 2.5. *For non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a domain R the smallest divisorial ideal containing their product*

$$\overline{\mathfrak{a}\mathfrak{b}} = \overline{\overline{\mathfrak{a}}\bar{\mathfrak{b}}}$$

is also the smallest divisorial ideal containing the products of the smallest divisorial ideals containing $\mathfrak{a}$ or $\mathfrak{b}$ respectively.

Proof.

$$\begin{aligned}\overline{\mathfrak{a}\mathfrak{b}} &\overset{2.4ii)}{=} (R : (R : \mathfrak{a}\mathfrak{b})) \overset{2.3ii)}{=} (R : ((R : \mathfrak{a}) : \mathfrak{b})) \\ &\overset{2.4iii)}{=} (R : ((R : (R : (R : \mathfrak{a}))) : \mathfrak{b})) \\ &\overset{2.3ii)}{=} (R : (R : (R : (R : \mathfrak{a}))\mathfrak{b})) \\ &\overset{2.4ii)}{=} (R : (R : (R : \overline{\mathfrak{a}}\mathfrak{b})) \overset{2.4ii)}{=} \overline{\overline{\mathfrak{a}}\mathfrak{b}}\end{aligned}$$

Therefore

$$\overline{\mathfrak{a}\mathfrak{b}} = \overline{\overline{\mathfrak{a}}\mathfrak{b}} = \overline{\overline{\mathfrak{a}}\bar{\mathfrak{b}}}.$$ ☐

Definition 2.6 (Divisors)**.**
Let $\mathtt{I}(R)$ denote the set of all non-zero (fractionary) ideals of a domain R. Then $(\mathtt{I}(R), \cdot, \subseteq)$ is a partially ordered monoid, where $\cdot$ denotes the multiplication of ideals, with neutral element R. There is an equivalence relation $\sim$ on $\mathtt{I}(R)$ given by

$$\mathfrak{a} \sim \mathfrak{b} \iff \overline{\mathfrak{a}} = \bar{\mathfrak{b}} \overset{2.4}{\iff} (R : \mathfrak{a}) = (R : \mathfrak{b})$$

for ideals $\mathfrak{a}$ and $\mathfrak{b}$. In this case $\mathfrak{a}$ and $\mathfrak{b}$ are called (Artin) equivalent or "quasi gleich". Define the *divisors* of R to be $\mathtt{D}(R) := {}^{\mathtt{I}(R)}/_{\sim}$. As two divisorial ideals are equivalent if and only if they are equal, the divisors $\mathtt{D}(R)$ will be identified with the set of divisorial ideals of R.

Additionally, the abelian monoid structure of $\mathtt{I}(R)$, $\cdot : \mathtt{I}(R) \to \mathtt{I}(R)$, is compatible with $\sim$ by Corollary 2.5. So an abelian monoid structure

$$\begin{aligned}+ : \mathtt{D}(R) \times \mathtt{D}(R) &\to \mathtt{D}(R) \\ (\overline{\mathfrak{a}}, \bar{\mathfrak{b}}) &\mapsto \overline{\mathfrak{a}} + \bar{\mathfrak{b}} := \overline{\overline{\mathfrak{a}}\bar{\mathfrak{b}}}\end{aligned}$$

arises on $\mathtt{D}(R)$ from it.

Moreover, applying Lemma 2.4 yields that $\sim$ is order preserving if the divisors are partially ordered by $\subseteq$. However, a slightly different partial order is more suitable. For divisorial ideals $\overline{\mathfrak{a}}$ and $\bar{\mathfrak{b}}$ define

$$\overline{\mathfrak{a}} \leq \bar{\mathfrak{b}} \iff \bar{\mathfrak{b}} \subseteq \overline{\mathfrak{a}} \overset{2.4}{\iff} (R : \overline{\mathfrak{a}}) \subseteq (R : \bar{\mathfrak{b}}) \overset{2.4}{\iff} (R : \mathfrak{a}) \subseteq (R : \mathfrak{b}),$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are representatives of their respective equivalence classes $\overline{\mathfrak{a}}$ and $\bar{\mathfrak{b}}$. In particular, if there are representatives $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{b} \subseteq \mathfrak{a}$, then already $\overline{\mathfrak{a}} \leq \bar{\mathfrak{b}}$ holds, i.e. $\sim$ is order reversing.

All in all, $(\mathtt{D}(R), +, \leq)$ is a (partially) ordered monoid, for which the set of positive elements $\mathtt{D}(R)_{>0}$ is the set of proper divisorial integral ideals. From now on, the relation $+$ will only be used in this sense for divisorial ideals.

Lemma 2.7. *Finite intersections of divisorial ideals of a domain R are divisorial.*

Proof. By induction, it suffices to show, that the claim holds for two divisorial ideals $\overline{\mathfrak{a}}$ and $\bar{\mathfrak{b}}$. As the intersection of intersections of principal ideals are an intersection of principal ideals, it suffices to show that the intersection is non-zero.

Let a and b be common denominators of $\overline{\mathfrak{a}}$ and $\bar{\mathfrak{b}}$ respectively. Then $d := ab$ is a common denominator of both ideals. Hence

$$0 \neq d\overline{\mathfrak{a}} \cdot d\bar{\mathfrak{b}} \overset{1.8}{\subseteq} d\overline{\mathfrak{a}} \cap d\bar{\mathfrak{b}} = d(\overline{\mathfrak{a}} \cap \bar{\mathfrak{b}})$$

and thus $\overline{\mathfrak{a}} \cap \bar{\mathfrak{b}}$ must not be zero. □

Proposition 2.8. *For any two divisorial ideals $\overline{\mathfrak{a}}$ and $\bar{\mathfrak{b}}$ of a domain R there is a supremum* $\sup(\overline{\mathfrak{a}}, \bar{\mathfrak{b}})$ *and an infimum* $\inf(\overline{\mathfrak{a}}, \bar{\mathfrak{b}})$ *within* $(\mathtt{D}(R), \leq)$.

Proof. Define $\sup(\overline{\mathfrak{a}}, \bar{\mathfrak{b}}) := \overline{\mathfrak{a}} \cap \bar{\mathfrak{b}}$ and $\inf(\overline{\mathfrak{a}}, \bar{\mathfrak{b}}) := \overline{\langle \overline{\mathfrak{a}}, \bar{\mathfrak{b}} \rangle}$. By Lemma 2.7 above $\sup(\overline{\mathfrak{a}}, \bar{\mathfrak{b}})$ is indeed divisorial. Hence the claim is a consequence of $\sim$ being order reversing. □

Definition 2.9 (Invertible ideals)**.**
An ideal $\mathfrak{a} \subseteq \mathrm{Frac}(R)$ of a domain R is called *invertible*, if there is an ideal $\mathfrak{a}^{-1} \subseteq \mathrm{Frac}(R)$ such that $\mathfrak{a} \cdot \mathfrak{a}^{-1} = R$.

Lemma 2.10. *Let $\mathfrak{a}$ be an ideal of a domain R with field of fraction $K :=$* $\mathrm{Frac}(R)$. *If $\mathfrak{a}$ is invertible, then $\mathfrak{a}^{-1} = (R : \mathfrak{a})$ and $\mathfrak{a}$ is divisorial.*

Additionally $\mathfrak{a}$ is finitely generated.

Proof. Let $\mathfrak{a}$ be an invertible ideal together with an ideal $\mathfrak{a}^{-1} \subseteq K$ such that $\mathfrak{a} \cdot \mathfrak{a}^{-1} = R$. Then $\mathfrak{a}^{-1} \subseteq (R : \mathfrak{a})$ holds by the definition of $(R : \mathfrak{a})$. Thus

$$R = \mathfrak{a} \cdot \mathfrak{a}^{-1} \subseteq \mathfrak{a} \cdot (R : \mathfrak{a}) \subseteq R$$

shows that $(R : \mathfrak{a})$ is inverse to $\mathfrak{a}$. However, the inverse in a monoid like $\mathtt{I}(R)$ is unique, so that $\mathfrak{a}^{-1} = (R : \mathfrak{a})$.

On the other hand, $\mathfrak{a}$ is inverse to $(R : \mathfrak{a})$, so that

$$\mathfrak{a} = (R : (R : \mathfrak{a})) \overset{2.4}{=} \overline{\mathfrak{a}},$$

which is divisorial.

Lastly, since $\mathfrak{a} \cdot (R : \mathfrak{a}) = R$, we know, that $1 = \sum_{i=0}^{n} a_i b_i$ for some $n \in \mathbb{N}$ with $a_i \in \mathfrak{a}$ and $b_i \in (R : \mathfrak{a})$ for $0 \leq i \leq n$. Hence

$$\langle a_0, ..., a_n \rangle \cdot (R : \mathfrak{a}) = R$$

and, again by the uniqueness of the inverse, $\langle a_0, ..., a_n \rangle = \mathfrak{a}$. Therefore $\mathfrak{a}$ is finitely generated. □

Remark 2.11. Lemma 2.10 above justifies the consideration of the monoid of divisors $\mathtt{D}(R)$ of a domain R instead of the monoid of ideals $\mathtt{I}(R)$. Because of this Lemma, only $\mathtt{D}(R)$ has any hope of being a group. In the following Theorem we will examine, in which cases $\mathtt{D}(R)$ is a group.

Theorem 2.12.
For a domain R, the monoid of divisors $\mathtt{D}(R)$ is a group if and only if R is completely integrally closed.

Proof. Recall from Definition 1.27, that an element $a \in K := \mathrm{Frac}(R)$ is almost integral, if $R[a]$ is a fractionary ideal, i.e there is some $d \in R$ such that for every $n \in \mathbb{N}$ $da^n \in R$, and that R is completely integrally closed, if every almost integral element is already an element of R.

"⇒" Assume $\mathtt{D}(R)$ to be a group and let $a \in K^\times$ be almost integral with common denominator d. Consider the divisorial ideals

$$\overline{\mathfrak{a}} := \bigcap_{n \in \mathbb{N}} a^{-n} R \ni d \text{ and } a^{-1} R \overset{2.10+2.3}{=} -(aR).$$

Then

$$\overline{\mathfrak{a}} - (aR) = \overline{\overline{\mathfrak{a}} \cdot a^{-1} R} = \overline{\Big(\bigcap_{n \in \mathbb{N}} a^{-(n+1)} R \Big)} = \bigcap_{n \in \mathbb{N}} a^{-(n+1)} R \supseteq \overline{\mathfrak{a}}$$

shows, that

$$\overline{\mathfrak{a}} = \overline{\mathfrak{a}} - (aR) + aR \leq \overline{\mathfrak{a}} + aR.$$

Since $\mathtt{D}(R)$ is a group there is some some divisorial ideal $-\overline{\mathfrak{a}}$. Hence

$$R = \overline{\mathfrak{a}} - \overline{\mathfrak{a}} \leq aR + \overline{\mathfrak{a}} - \overline{\mathfrak{a}} = aR$$

and thus $a \in R$, as $aR \subseteq R$. Since $a \in K$ was arbitrary among non-zero almost integral elements, R is completely integrally closed.

"$\Leftarrow$" Assume R to be completely integrally closed and let $\overline{\mathfrak{a}} \subseteq R$ be a divisorial integral ideal.

Consider the integral ideal $\overline{\mathfrak{a}} \cdot (R : \overline{\mathfrak{a}}) \subseteq R$ and let $a \in K$ such that $\overline{\mathfrak{a}} \cdot (R : \overline{\mathfrak{a}}) \subseteq aR$. Then $a \neq 0$ since $\overline{\mathfrak{a}} \cdot (R : \overline{\mathfrak{a}}) \neq 0$. As $a^{-1}\overline{\mathfrak{a}} \cdot (R : \overline{\mathfrak{a}}) \subseteq R$, we get that

$$a^{-1}\overline{\mathfrak{a}} \subseteq (R : (R : \overline{\mathfrak{a}})) \overset{2.4ii)}{=} \overline{\mathfrak{a}}$$

holds by definition. Therefore, by a simple induction,

$$(a^{-1})^n \overline{\mathfrak{a}} = a^{-n}\overline{\mathfrak{a}} \subseteq \overline{\mathfrak{a}}$$

holds for any natural number $n \in \mathbb{N}$. So for any $0 \neq b \in \overline{\mathfrak{a}}$ we have

$$ba^{-n} \in a^{-n}\overline{\mathfrak{a}} \subseteq \overline{\mathfrak{a}} \subseteq R,$$

which shows, that a^{-1} is almost integral over R. Since R is completely integrally closed, $a^{-1} \in R$ and thus $R \subseteq aR$.

All in all,

$$R \supseteq \overline{\mathfrak{a}} + (R : \overline{\mathfrak{a}}) = \bigcap_{\substack{a \in K \\ \overline{\mathfrak{a}} \cdot (R : \overline{\mathfrak{a}}) \subseteq aR}} aR \supseteq R$$

proves that $\overline{\mathfrak{a}}$ is invertible.

If $\overline{\mathfrak{a}}$ is divisorial but not necessarily integral, take any common denominator $d \in R$ of $\overline{\mathfrak{a}}$ and define $\overline{\mathfrak{b}} := dR + \overline{\mathfrak{a}} = \overline{d\mathfrak{a}} \subseteq R$, so that

$$\overline{\mathfrak{a}} + (dR - \overline{\mathfrak{b}}) = \overline{\mathfrak{b}} - \overline{\mathfrak{b}} = R.$$

This shows, that $\mathtt{D}(R)$ is a group. $\square$

Corollary 2.13. *A domain R is completely integrally closed if and only if for every divisorial ideal $\overline{\mathfrak{a}}$*

$$(\overline{\mathfrak{a}} : \overline{\mathfrak{a}}) = R$$

holds.

Proof. Theorem 2.12 states that R is completely integrally closed if and only if $\mathtt{D}(R)$ is a group and by the proof, this is the case if and only if for any divisorial ideal $\overline{\mathfrak{a}}$

$$R = (R : (R : (R : \overline{\mathfrak{a}}) \cdot \overline{\mathfrak{a}})) \overset{2.3ii)}{=} (R : ((R : (R : \overline{\mathfrak{a}})) : \overline{\mathfrak{a}})) \overset{2.4ii)}{=} (R : (\overline{\mathfrak{a}} : \overline{\mathfrak{a}})).$$

This is the case if and only if

$$R = (R : R) = (R : (R : (\overline{\mathfrak{a}} : \overline{\mathfrak{a}}))) \overset{2.4ii)}{=} (\overline{\mathfrak{a}} : \overline{\mathfrak{a}}),$$

since $(\overline{\mathfrak{a}} : \overline{\mathfrak{a}})$ is divisorial by 2.3v). □

Remark 2.14. Studying almost integral elements a little more, it becomes apparent, that a ring R is completely integrally closed if and only if for any fractionary ideal $\mathfrak{a}$, $(\mathfrak{a} : \mathfrak{a}) = R$ holds. This can be seen in [Fos73, p. 12f., Chapter I, §3, Lemma 3.1 and Corollary 3.3] in more detail. So Corollary 2.13 above is another instance of divisorial ideals carrying similar information as fractionary ideals. This further justifies the consideration of divisorial ideals over fractionary ones.

2.2 Class Groups

Whether or not the monoid of divisors is a group, it always contains the group of principal ideals. We will now establish the notion of the class group to be a measure of the difference between the divisorial ideals and the principal ideals. In Chapter 3.1 we will even show, that the class group is 0 if and only if the considered domain is factorial. Because of this, we are especially interested in the class group of Dedekind domains.

Proposition 2.15. *For a domain R let $\mathtt{Prin}(R) := \{aR \mid a \in \mathrm{Frac}(R)^\times\}$ be the set of non-zero principal ideals. This defines an abelian subgroup of $\mathtt{D}(R)$.*

Proof. As principal ideals are divisorial $R = 1R \in \mathtt{Prin}(R) \subseteq \mathtt{D}(R)$ and $aR \cdot bR = (ab)R$ for $a, b \in K := \mathrm{Frac}(R)$, $\mathtt{Prin}(R)$ is indeed a submonoid. Furthermore $aR \cdot a^{-1}R = (aa^{-1})R = R$ for $a \in K^\times$, so that $\mathtt{Prin}(R)$ is indeed a group. □

Definition 2.16 (Class group)**.**
Let R be a completely integrally closed domain and consider the subgroup $\mathtt{Prin}(R)$ from Proposition 2.15 above. Then the *class group*

$$\mathtt{Cl}(R) := {}^{\mathtt{D}(R)}\!\big/_{\mathtt{Prin}(R)}$$

of R is defined as the quotient of $\mathtt{D}(R)$ and $\mathtt{Prin}(R)$. For a divisorial ideal $\overline{\mathfrak{a}} \in \mathtt{D}(R)$ let $\boldsymbol{c}(\overline{\mathfrak{a}}) := \overline{\mathfrak{a}} + \mathtt{Prin}(R) \in \mathtt{Cl}(R)$ denote the class of $\overline{\mathfrak{a}}$, ie.e the corresponding element in the class group.

Example 2.17. Consider a discrete valuation ring R with surjective valuation $\nu\colon K := \mathrm{Frac}(R) \to \mathbb{Z} \cup \{\infty\}$. Recall the basic properties of a valuation ring given in Lemma 1.37, as well as, that R is completely integrally closed by Corollary 1.45. So $\mathtt{D}(R)$ is a group by Theorem 2.12 and we can compute the class group $\mathtt{Cl}(R)$.

For $a \in K^\times$ the principal ideal aR is comparable to R, because if $a \in R$, then $aR \subseteq R$, and $R \subseteq aR$, if $a^{-1} \in R$, one of which is true. Hence, the same holds true for arbitrary intersections of principal ideals and thus for any divisorial ideal. Therefore, it suffices to consider the non-negative, i.e. integral, ideals in $\mathtt{D}(R)_{\geq 0}$ as the other divisorial ideals are just the inverses of these.

Note that for any two elements $a, b \in R$, $\nu(a) = \nu(b)$ if and only if $aR = bR$, so the unique maximal ideal $\mathscr{m}$ is generated by any $a \in \nu^{-1}(1)$. Fix such an a_0.

Furthermore, for any subset $U \subseteq R \setminus \{0\}$ there is a $b \in U$ with $\nu(b) = \min_{a \in U}\{\nu(a)\}$ since $\mathbb{N}$ is well-ordered. Thus

$$\bigcap_{a \in U} aR = bR = a_0^{\nu(b)} R = (a_0 R)^{\nu(b)}$$

for any $U \subseteq R$. This shows, that

$$\mathtt{D}(R) = \{a_0^n R \mid n \in \mathbb{Z}\} = \mathtt{Prin}(R)$$

is the monoid of divisors. Therefore, up to an order embedding isomorphism, $\mathtt{D}(R) \cong \mathbb{Z}$ and $\mathtt{Cl}(R) \cong 0$.

3 Theory of Krull Domains

In this Chapter we want to study Krull domains as a useful generalisation of Dedekind domains. The connection between Dedekind domains and Krull domains will be discussed in Chapter 4. Krull domains can also be considered to be generalisations of other important concepts including unique factorisation domains, which we will see over the course of this Chapter. After establishing some basic properties, we will proceed to study stability properties of Krull domains. Ultimately, we will proof, that every abelian group can be realised as the class group of a Krull domain, up to some isomorphism.

Throughout this Chapter let A be a Krull domain with $F := \mathrm{Frac}(A)$ as its fraction field, if not stated otherwise.

3.1 Krull Domains

We will start of by describing Krull domains, in a possibly unusual fashion, as completely integrally closed domains with a particularly nice divisor group. Later on, we will see this definition coinciding with the usual definition of Krull domains as certain intersections of discrete valuation rings. Nevertheless, this point of view will be helpful in developing the notions, which are relevant to the theory of Krull domains. Again we will follow [Sam64, p. 4-9, Chapter I, §3].

Definition 3.1 (Krull domain)**.**
A *Krull domain* A is a completely integrally closed domain, such that its divisor group is order embedding isomorphic to a lattice, i.e.

$$\mathtt{D}(A) \cong \mathbb{Z}^{(I)}$$

via an embedding the order for some index set I.

Example 3.2. The easiest example of a Krull domain is a field. To account for this, we will consider an empty intersection of discrete valuation rings of the field as the field itself. It will become apparent over the course of this section, why this is useful.

Additionally, we have seen in Example 2.17, that every discrete valuation ring is a Krull domain.

Proposition 3.3. *A completely integrally closed domain A is a Krull domain if and only if it satisfies the maximum condition for (proper) divisorial integral ideals, i.e. any non-empty subset $\emptyset \neq U \subseteq \mathtt{D}(A)_{>0}$ of positive divisorial ideals has an "$\subseteq$"-maximal element.*

In that case, the set $\mathtt{P}(A)$ of minimal positive divisorial ideals is a free generating set of $\mathtt{D}(A)$ and the canonical isomorphism

$$\varphi\colon \mathtt{D}(A) \to \mathbb{Z}^{(\mathtt{P}(A))}$$
$$\mathtt{P}(A) \ni \mathfrak{p} \mapsto (\delta_{\mathfrak{p}\mathfrak{q}})_{\mathfrak{q}\in\mathtt{P}(A)}$$

is order embedding.

Proof. By Theorem 1.6, for every partially ordered group G there is an order embedding isomorphism to some lattice $\mathbb{Z}^{(I)}$ if and only if the following two conditions are met:

(a) For any two elements $a, b \in G$ there is a supremum $\sup(a, b) \in G$ and an infimum $\inf(a, b) \in G$.

(b) Every subset of positive elements has a minimal element.

Proposition 2.8 states that $\mathtt{D}(A)$ always satisfies condition (a). Hence $\mathtt{D}(A)$ is a lattice if and only if condition (b) is met, which by the definition of "$\leq$" is equivalent to the maximum condition for positive divisorial ideals.

The rest of the statement is a direct application of Theorem 1.6. □

Remark 3.4. The condition given in Proposition 3.3 is not equivalent to being noetherian, because the maximum condition is only required for divisorial ideals. A possible example for this phenomenon is the non-noetherian domain $\mathbb{Z}[X_n \mid n \in \mathbb{N}]$, for which we will show, that it is a Krull domain.

Corollary 3.5. *A normal noetherian domain is a Krull domain.*

Proof. By 1.33 a normal noetherian domain is completely integrally closed. Furthermore, a noetherian domain satisfies the maximum condition for every set of integral ideals and thus particularly for any set of positive divisorial ideals. Hence the claim is a consequence of Proposition 3.3 above. □

Definition 3.6 (Prime divisors and essential valuations)**.**
Let $\mathtt{P}(A)$ denote the set of minimal divisorial ideals above a Krull domain A, i.e.

$$\mathtt{P}(A) := \{\bar{\mathfrak{a}} \in \mathtt{D}(A)_{>0} \mid \forall \bar{\mathfrak{b}} \in \mathtt{D}(A)\ A < \bar{\mathfrak{b}} \leq \bar{\mathfrak{a}} \Rightarrow \bar{\mathfrak{b}} = \bar{\mathfrak{a}}\}.$$

The elements of $\mathtt{P}(A)$ are called the *prime divisors* of A.

Note that $\mathtt{P}(A)$ consists only of proper ideals, which form a free generating set for $\mathtt{D}(A)$, as mentioned in Proposition 3.3. Hence, if $F := \mathrm{Frac}(A)$ is the fraction field of A, then for $x \in F^\times$ there is a unique presentation of xA in terms of the free generating set $\mathtt{P}(A)$

$$xA = \sum_{\mathfrak{p} \in \mathtt{P}(A)} \nu_{\mathfrak{p}}(x)\mathfrak{p}$$

with $\nu_{\mathfrak{p}}(x) \in \mathbb{Z}$ for every $\mathfrak{p} \in \mathtt{P}(A)$, almost all of which are zero. Since for $x, y \in F^\times$ $xyA = xA + yA$ and $(x + y)A \geq \overline{\langle x, y\rangle} = \inf(xA, yA)$, the following relations

i) $\nu_{\mathfrak{p}}(xy) = \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y)$ and

ii) $\nu_{\mathfrak{p}}(x+y) \overset{3.3}{\geq} \inf\{\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y)\} = \min\{\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y)\}$ for $x+y \neq 0$

hold for all $\mathfrak{p} \in \mathtt{P}(A)$. Defining $\nu_{\mathfrak{p}}(0) := \infty$ yields, that for every prime divisor $\mathfrak{p}$, $\nu_{\mathfrak{p}}$ defines a discrete valuation on F. We will see in Corollary 3.9, that these valuations are in fact surjective, which justifies, that they are discrete. These valuations are called the *essential valuations* of A.

Lemma 3.7. *For a divisorial ideal $\overline{\mathfrak{a}} = \sum_{\mathfrak{p}\in\mathtt{P}(A)} n_{\mathfrak{p}}\mathfrak{p}$ of a Krull domain A we have*

$$\overline{\mathfrak{a}} = \{x \in \mathrm{Frac}(A) \mid \forall \mathfrak{p} \in \mathtt{P}(A)\ n_{\mathfrak{p}} \leq \nu_{\mathfrak{p}}(x)\}.$$

Proof. For any $x \in \mathrm{Frac}(A)$

$$x \in \overline{\mathfrak{a}} \iff xA \subseteq \overline{\mathfrak{a}} \iff \overline{\mathfrak{a}} \leq xA \overset{3.3}{\iff} \forall \mathfrak{p} \in \mathtt{P}(A)\ \mathfrak{n}_{\mathfrak{p}} \leq \nu_{\mathfrak{p}}(x). \qquad \square$$

For this reason divisorial ideals are also said to be "defined by essential valuation conditions ", as it is done by Claborn in [Cla66].

Corollary 3.8. *If $\mathfrak{p} \in \mathtt{P}(A)$ is a prime divisor of a Krull domain A, then $\mathfrak{p}$ is a prime ideal. Because of this, the prime divisors are also called* prime divisorial ideals.

Proof. Since $\mathtt{P}(A) \subseteq \mathtt{D}(A)_{>0}$ the prime divisor $\mathfrak{p}$ is a proper integral ideal. Now let $x, y \in A$ such that $xy \in \mathfrak{p}$. Then by Lemma 3.7 $1 \leq \nu_{\mathfrak{p}}(x) = \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y)$. Hence $1 \leq \nu_{\mathfrak{p}}(x)$ or $1 \leq \nu_{\mathfrak{p}}(y)$ and thus again by Lemma 3.7 $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. So $\mathfrak{p}$ is prime. $\square$

Corollary 3.9. *For any prime divisorial ideal $\mathfrak{p} \in \mathtt{P}(A)$ of a Krull domain A there is some $x_{\mathfrak{p}} \in A$ with $\nu_{\mathfrak{p}}(x_{\mathfrak{p}}) = 1$.*

Proof. Consider a prime divisorial ideal $\mathfrak{p} \in \mathtt{P}(A)$. As the divisors $\mathtt{D}(A)$ form a lattice, $2\mathfrak{p} \overset{1.8}{\subsetneq} \mathfrak{p}$. So Lemma 3.7 shows, that

$$\begin{aligned}\emptyset \neq \mathfrak{p} \setminus 2\mathfrak{p} &\overset{3.7}{=} \{a \in A \mid \nu_{\mathfrak{p}}(a) \geq 1\} \setminus \{a \in A \mid \nu_{\mathfrak{p}}(a) \geq 2\} \\ &= \{a \in A \mid \nu_{\mathfrak{p}}(a) = 1\}\end{aligned}$$

is non-empty. Hence any $x \in \mathfrak{p} \setminus 2\mathfrak{p}$ fulfils the requirements to be $x_{\mathfrak{p}}$. $\square$

Lemma 3.10. *Let $0 \neq \mathfrak{q}$ be a prime ideal of a Krull domain A. Then*

i) the prime ideal $\mathfrak{q}$ contains some prime divisorial ideal and

ii) the prime ideal $\mathfrak{q}$ is a prime divisorial ideal if and only if it is of height 1, *i.e. there is no non-zero prime ideal $\mathfrak{p}$ strictly contained in $\mathfrak{q}$.*

Proof.

i) For $0 \neq x \in \mathfrak{q}$ the principal ideal $xA = \sum_{\mathfrak{p} \in \mathrm{P}(A)} \nu_{\mathfrak{p}}(x)\mathfrak{p}$ is a finite sum with only non-negative summands. Thus

$$\prod_{\substack{\mathfrak{p} \in \mathrm{P}(A) \\ \nu_{\mathfrak{p}}(x) > 0}} \mathfrak{p}^{\nu_{\mathfrak{p}}(x)} \subseteq xA \subseteq \mathfrak{q}$$

and by Lemma 1.9 there is $j \in J$ such that $\mathfrak{p}_j \subseteq \mathfrak{q}$ as $\mathfrak{q}$ is prime.

ii) Assume $\mathfrak{q}$ was of height 1. By i) there is a prime divisorial ideal $\mathfrak{p}$ such that $0 \neq \mathfrak{p} \subseteq \mathfrak{p}$ and thus $\mathfrak{p} = \mathfrak{q}$.

On the other hand, if $\mathfrak{q}$ was prime divisorial and $0 \neq \mathfrak{p} \subseteq \mathfrak{q}$ for some prime ideal $\mathfrak{p}$, then again by i), there is some prime divisorial ideal $\mathfrak{q}_0 \subseteq \mathfrak{p}$. Thus

$$\mathfrak{q} = \mathfrak{q}_0 \subseteq \mathfrak{p} \subseteq \mathfrak{q}$$

holds by the minimality of $\mathfrak{q}_0$. □

Corollary 3.11. *A divisorial ideal of a Krull domain A is prime divisorial if and only if it is a prime ideal. In particular, a prime element spans a prime divisorial ideal.*

Proof. Applying Corollary 3.8, it suffices to show, that divisorial ideals, which are prime, are prime divisorial.

So assume $\mathfrak{p}$ to be prime and divisorial. By Lemma 3.10 there is a prime divisorial ideal $\mathfrak{q} \subseteq \mathfrak{p}$ and by the minimality of $\mathfrak{q}$ they must be equal, i.e. $\mathfrak{q} = \mathfrak{p}$.

As prime elements span principal prime ideals, the second claim is a direct consequence. □

Lemma 3.12. *We have $A_{\mathfrak{p}} = R_{\nu_{\mathfrak{p}}}$ for a $\mathfrak{p}$ prime divisorial ideal of a Krull domain A.*

Proof. Since by Corollary 3.8 $\mathfrak{p}$ is a prime ideal, $(A \setminus \mathfrak{p})$ is indeed multiplicatively closed. Let $F := \mathrm{Frac}(A)$ denote that field of fractions of A.

"$\subseteq$" Let $\frac{a}{b} \in A_{\mathfrak{p}} \subseteq F$, so that without loss of generality $b \notin \mathfrak{p}$. By applying Lemma 3.7 $\nu_{\mathfrak{p}}(b) = 0$. Hence

$$\nu_{\mathfrak{p}}\left(\frac{a}{b}\right) = \nu_{\mathfrak{p}}(a) - \nu_{\mathfrak{p}}(b) = \nu_{\mathfrak{p}}(a) \geq 0$$

shows, that $\frac{a}{b} \in A_{\nu_{\mathfrak{p}}}$.

"$\supseteq$" Let $x \in R_{\nu_{\mathfrak{p}}} \subseteq F$ with $xA = \sum_{\mathfrak{q} \in \mathrm{P}(A)} \nu_{\mathfrak{q}}(x)\mathfrak{q}$ and define

$$\overline{\mathfrak{a}} := \sum_{\substack{\mathfrak{q} \in \mathrm{P}(A) \\ \nu_{\mathfrak{q}}(x) < 0}} -\nu_{\mathfrak{q}}(x)\mathfrak{q} \subseteq A.$$

Since $0 \leq \nu_{\mathfrak{p}}(x)$, the divisorial ideal $\mathfrak{p}$ and $\overline{\mathfrak{a}}$ are not comparable. Thus for $s \in \overline{\mathfrak{a}} \setminus \mathfrak{p} \neq \emptyset$ and $\mathfrak{q} \in \mathrm{P}(A)$

$$\nu_{\mathfrak{q}}(sx) = \nu_{\mathfrak{q}}(x) + \nu_{\mathfrak{q}}(s) \geq \nu_{\mathfrak{q}}(x) - \nu_{\mathfrak{q}}(x) = 0.$$

Hence $A \leq sxA$ and therefore $sx \in A$, which shows, that $x \in A_{\mathfrak{p}}$. □

Corollary 3.13. *A Krull domain A is an intersection of discrete valuation rings,*

$$A = \bigcap_{\mathfrak{p} \in \mathrm{P}(A)} R_{\nu_{\mathfrak{p}}} = \bigcap_{\substack{\mathfrak{p} \text{ prime ideal} \\ \text{of height } 1}} A_{\mathfrak{p}}.$$

Proof. For $x \in \mathrm{Frac}(A)$ the equivalence

$$\forall \mathfrak{p} \in \mathrm{P}(A)\ 0 \leq \nu_{\mathfrak{p}}(x) \iff A \leq xA \iff xA \subseteq A \iff x \in A$$

holds. The rest is a consequence of Lemma 3.10 and 3.12 above. □

In fact Corollary 3.13 yields a characterisation of Krull domains as the following Theorem will show.

Theorem 3.14 (*Valuation Criterion*).
Let A be a domain. Then the following statements are equivalent:

i) A is a Krull domain

ii) There is a family $(\nu_i)_{i \in I}$ of discrete valuations of $F = \mathrm{Frac}(A)$ for some index set I such that the following two conditions hold:

(a) For $x \in K$ we have $x \in A$ if and only if $0 \leq \nu_i(x)$ for all $i \in I$, i.e.

$$A = \bigcap_{i \in I} R_{\nu_i}.$$

(b) For every $0 \neq x \in A$ we have $\nu_i(x) = 0$ for almost any $i \in I$.

If a family of discrete valuations $(\nu_i)_{i \in I}$ satisfies condition ii) for a domain A, we also say, that $(\nu_i)_{i \in I}$ satisfies the Valuation Criterion for A.

Proof.

"$\Rightarrow$" Taking the essential valuations of A as the family of valuations yields condition (b) by definition. Then condition (a) is a direct application of Corollary 3.13 above.

"$\Leftarrow$" Lemma 1.35 states, that intersections of completely integrally closed domains are completely integrally closed. Thus, by condition (a), A is completely integrally closed due to discrete valuation rings being completely integrally closed, as shown in Corollary 1.45.

By Proposition 3.3, it suffices to verify that A satisfies the maximum condition for sets of (proper) integral divisorial ideals. Now take $x \in F^\times$. By definition there is some $a \in A$ for $y \in xA$ with $ax = y$ and thus

$$\nu_i(y) = \nu_i(x) + \nu(a) \geq \nu_i(x)$$

for every $i \in I$, as $0 \leq \nu_i(a)$ by (a). On the other hand, if for $y \in F$ there is some $i \in I$ such that $\nu_i(x) \leq \nu_i(y)$, then $0 \leq \nu_i(x^{-1}y)$ and thus $x^{-1}y \in R_{\nu_i}$. So if for every $i \in I$ $\nu_i(x) \leq \nu_i(y)$ then condition (a) yields, that $x^{-1}y \in A$ and thus $y = x(x^{-1}y) \in xA$. Hence for $x \in F$

$$xA = \{y \in F \mid \forall i \in I \ \nu_i(x) \leq \nu_i(y)\}.$$

Therefore, we have for any integral divisorial ideal $\overline{\mathfrak{a}}$ given by $U \subseteq F^\times$

$$\begin{aligned}\overline{\mathfrak{a}} = \bigcap_{x \in U} xA = \bigcap_{x \in U} &\{y \in F \mid \forall i \in I \ \nu_i(x) \leq \nu_i(y)\} \\ &= \{y \in F \mid \forall i \in I \ n_i := \sup_{x \in U}\{\nu_i(x)\} \leq \nu_i(y)\},\end{aligned}$$

where without loss of generality $n_i \geq 0$ by condition (a). Now by condition (b) $(n_i)_{i \in I} \in \mathbb{Z}^{(I)}$. Otherwise, i.e. if $n_i \neq 0$ almost all $i \in I$ or one of the $n_i = \infty$, the corresponding ideal must be 0 by condition (b) and thus is not divisorial.

Therefore, there are only finitely many integral divisorial ideals smaller than, and thus containing, any given divisorial ideal $\overline{\mathfrak{a}} = \{a \in A \mid n_i \leq \nu_i(a)\}$. Hence for every non-empty set of integral divisorial ideals $\mathscr{U} \subseteq \mathtt{D}(A)_{\geq 0}$ and any $\overline{\mathfrak{a}} \in \mathscr{U}$, there are only finitely many integral divisorial ideals containing $\overline{\mathfrak{a}}$ in $\mathscr{U}$. For a fixed $\overline{\mathfrak{a}} \in \mathscr{U}$, the inclusion maximal among these is automatically "$\subseteq$"-maximal in $\mathscr{U}$. Therefore, A satisfies the maximum condition for integral divisorial ideals. □

Corollary 3.15. *A discrete valuation $\nu : F \to \mathbb{Z}$ is an essential valuation of a Krull domain A with field of fractions* $\operatorname{Frac}(A) =: F$ *if and only if for every family $(\nu_i)_{i \in I}$ of discrete valuations satisfying the Valuation Criterion for A, there is some $i \in I$ such that $\nu = \nu_i$.*

Proof. It is apparent, that if ν appears in any family of valuations displaying A as a Krull domain, then it appears in $(\nu_{\mathfrak{p}})_{\mathfrak{p} \in \mathtt{P}(A)}$ and thus is an essential valuation.

Conversely, let $\mathfrak{p} \in \mathtt{P}(A)$ and let $\mathfrak{q}_i = A \cap \mathfrak{m}_i$, where $\mathfrak{m}_i$ is the unique maximal ideal of R_{ν_i} for $i \in I$. The integral ideal $\mathfrak{q}_i$ is prime, since $\mathfrak{m}_i$ is prime and A is a subring of R_{ν_i}. Like in the proof of the Valuation Criterion above, $\mathfrak{p} = \{x \in K \mid \forall i \in I \; \nu_i(x) \geq n_i\}$ for some $(n_i)_{i \in I} \in \mathbb{Z}^{(I)}$. Hence

$$\prod_{\substack{i \in I \\ n_i > 0}} \mathfrak{q}_i^{n_i} \subseteq \mathfrak{p}.$$

By Lemma 1.9 there is some $j \in I$ with $n_j > 0$ and $0 \neq \mathfrak{q}_j \subseteq \mathfrak{p}$. Note that $\mathfrak{q}_j \neq 0$, because $n_j \neq 0$. Now $\mathfrak{p}$ is of height 1 by Lemma 3.10 and thus $\mathfrak{q}_j = \mathfrak{p}$. Therefore

$$R_{\nu_{\mathfrak{p}}} \overset{3.12}{=} A_{\mathfrak{p}} \subseteq R_{\nu_j}.$$

Since by Lemma 1.42 discrete valuation rings are maximal proper subrings of F, both discrete valuation rings are equal, i.e. $R_{\nu_{\mathfrak{p}}} = R_{\nu_j}$. Hence by Corollary 1.39 $\nu_{\mathfrak{p}} = \nu_j$. □

Corollary 3.16. *A family of discrete valuations $(\nu_i)_{i \in I}$, that satisfies the Valuation Criterion for a domain A, such that no valuation can be omitted from the family $(\nu_i)_{i \in I}$ without destroying this property, is the family of essential valuations.*

Proof. Any family of valuations presenting A as a Krull domain contains the family of essential valuations by Corollary 3.15 above. On the other hand, we know, that the family of essential valuations is sufficient to present A as a Krull domain by Corollary 3.13. □

Remark 3.17. The Valuation Criterion and its Corollaries yield an equivalent definition of a Krull domain and its essential valuation.

Corollary 3.18. *Any unique factorisation domain R is a Krull domain. In this case its class group is trivial, i.e.* $\mathtt{Cl}(R) \cong 0$.

Proof. Condition ii) from the Valuation Criterion is an immediate application of 1.46 . Taking Corollary 3.15 into account, the prime divisorial ideals of R are all principal, as they are generated by one of the prime elements of R each. In fact, the valuations given in Example 1.46 are the essential valuations of R as an easy consequence of Corollary 3.11.

Hence $\mathtt{D}(R) \subseteq \mathtt{Prin}(R)$ and thus $\mathtt{Cl}(A) \cong 0$. □

Recalling Example 1.26 we have finally shown, that $\mathbb{Z}[X_i \mid i \in \mathbb{N}]$ is indeed a non-noetherian Krull domain, which is completely integrally closed. In fact, the characterisation of unique factorisation domains as Krull domains yields many more examples of Krull domains. However, these examples are not very interesting for us at the moment, because they have a trivial class group. Nevertheless, the next Theorem will generalise our observation into a characterisation of unique factorisation domains.

Theorem 3.19. *For a domain R the following are equivalent:*

i) R is a Krull domain with $\mathtt{Cl}(R) \cong 0$.

ii) R is a Krull domain and every prime divisorial ideal is principal.

iii) R is a Krull domain and the intersection of any two (integral) principal ideals is principal.

iv) Every irreducible element of R is prime and R satisfies the maximum condition for every set of integral principal ideals, ie. every set of integral principal ideals has an "$\subseteq$"-maximal element.

v) R is a unique factorisation domain.

Proof.

i) ⇔ ii) This is an immediate consequence of $\mathtt{Prin}(R)$ being the subgroup of of principal ideals and therefore $\mathtt{Cl}(R) \cong 0$ if and only if $\mathtt{Prin}(R) = \mathtt{D}(R)$.

ii) ⇒ iv) Since every divisorial ideal is principal, any proper integral principal ideal $aR \neq R$ is "$\leq$"-minimal among proper integral divisorial ideals if and only if it is "$\subseteq$"-maximal among those. Hence the principal ideals spanned by the irreducible elements are prime divisorial and thus by Corollary 3.8 prime. Therefore, every irreducible element is prime.

Moreover, because we have seen in Proposition 3.3, that the Krull domain R satisfies the maximum condition for the set of integral divisorial ideals, R satisfies the maximum condition for integral principal ideals.

iv) ⇔ v) This is Lemma 1.19.

v) ⇒ i) This is Corollary 3.18 above.

The proof of ii) $\iff$ iii) can be found in (the proof of) [Sam64, p. 16f., Chapter I, §5, Theorem 5.3], as well as further equivalences. □

3.2 Stability Properties of Krull Domains

In this section we will develop the notion of a subintersection of a Krull domain and establish a connection between the class groups, namely Nagata's Theorem. This relation will turn out to be very useful when constructing Krull domains with arbitrary class groups. Moreover, we will show, that any Polynomial ring over a Krull domain is again a Krull domain with an isomorphic class group.

Proposition 3.20. *Let K be a field and $(A_\alpha)_\alpha$ a family of Krull domains, all of which are contained in K, and let $B := \bigcap_\alpha A_\alpha$. Assume every $0 \neq x \in B$ is a unit in almost all of the A_α, then B is a Krull domain.*

In particular finite intersections of Krull domains are Krull domains.

Proof. Any discrete valuation on $K_\alpha := \mathrm{Frac}(A_\alpha)$ restricts to a valuation on $F := \mathrm{Frac}(B) \subseteq K_\alpha$ with valuation group (isomorphic to) $\mathbb{Z}$ or 0 by restricting it to the subfield. Now consider the family of valuations, which restrict from the essential valuations of the A_α's to discrete valuation on F after applying some isomorphism. Then the intersection of the corresponding discrete valuation rings is still B. Since $0 \neq x \in B$ is a unit in almost all A_α, x is a unit in almost all of these valuation rings. So B is in fact a Krull domain by the Valuation Criterion. □

Proposition 3.21. *Let A be a Krull domain with field of fractions $F :=$ $\mathrm{Frac}(A)$. Let K be a finite field extension of F and let B denote the integral closure of A in K. Then B is also a Krull domain.*

Proof. As this Theorem is not necessary for our main Theorem, and some notions from Galois Theory are required for this proof, we will just sketch the proof of [Sam64, p.12, Chapter I, §4, Proposition 4.5].

First note, that without loss of generality the field extension is normal, because by [ZS58, p. 77, Chapter II, §6, Theorem 14] there is a finite field extension L of K such that the finite field extension of L over F is normal. (The finiteness can be seen in the proof on p. 76.) Now if the integral closure B' of A in F is a Krull domain, then $B = B' \cap K$ is a Krull domain by Proposition 3.20.

So let K be normal over F. In [ZS60, p.13, Chapter VI, §4, Theorem 5'] it is shown, that any valuation of F can be extended to a valuation of K with the same valuation group. Furthermore, by [ZS60, p.29, Chapter VI, §7, Corollary 4 to Theorem 12] there are at most finitely many different extensions of such a valuation, since the field extension is finite. (Note that to connect the concept of a place and a valuation [ZS60, p.35-39, Chapter VI, §9] might be helpful.)

Let Φ denote the set of all discrete valuations that are extensions of the essential valuations of A. Then only the verification, that the valuations in Φ satisfy the Valuation Criterion for B, remains. □

Proposition 3.22. *Let $T \subseteq \mathtt{P}(A)$ be a set of prime divisorial ideals of a Krull domain A and define $B := \bigcap_{\mathfrak{p} \in T} R_\mathfrak{p}$. Then B is a Krull domain with fraction field $\mathrm{Frac}(B) = \mathrm{Frac}(A) =: F$. Furthermore the essential valuations are given by the prime divisorial ideals $\mathfrak{p} \in T$.*

We will call Krull domains such as B subintersections *of A coinciding with [Fos73].*

Proof. The concept of a subintersection as well as this proof are based on [Cla66, p.219, Proposition 1].

Since $A \subseteq B \subseteq F$, we have $F = \mathrm{Frac}(A) \subseteq \mathrm{Frac}(B) \subseteq \mathrm{Frac}(F) = F$. Now, as a consequence of the Valuation Criterion, B is a valuation ring, as almost all essential valuations ν of A vanish on any given element $\frac{a}{b} \in F^\times$, because $\nu\left(\frac{a}{b}\right) = \nu(a) - \nu(b)$.

Lastly, if any of the valuations $\nu_{\mathfrak{q}}$ for $\mathfrak{q} \in T$ could be omitted from this family of valuations, then $\nu_{\mathfrak{q}}$ could be omitted from the family of essential valuations $(\nu_{\mathfrak{p}})_{\mathfrak{p} \in \mathtt{P}(A)}$ of A, which is not possible by Corollary 3.15. So by Corollary 3.16, $(\nu_{\mathfrak{p}})_{\mathfrak{p} \in T}$ is the family of essential valuations of B. □

Remark 3.23. With the notation of Proposition 3.22, the subintersection $B := \bigcap_{\mathfrak{p} \in T} A_{\mathfrak{p}}$ actually defines a superset of $A := \bigcap_{\mathfrak{p} \in \mathtt{P}(A)} R_{\mathfrak{p}}$. So one might talk about a *supintersection* instead of a *subintersection*. However, to be consistent with the literature, we will stick to the name subintersection.

Example 3.24. Let us examine subintersections of $\mathbb{Z}$. Let $\mathbb{P}$ denote the set of positive prime elements and take a prime number $p_0 \in \mathbb{P}$. Let $T := \{p\mathbb{Z} \mid p_0 \neq p \in \mathbb{P}\}$. Then we have for the subintersection given by T

$$B := \bigcap_{\mathfrak{p} \in T} R_{\nu_{\mathfrak{p}}} = \left\{ \frac{a}{p_0^n} \;\middle|\; a \in \mathbb{Z} \text{ and } n \in \mathbb{N} \right\} = \{p_0^n\}_{n \in \mathbb{N}}^{-1}\mathbb{Z}.$$

Generally if $T_0 \subseteq \mathbb{P}$ and $T = \{p\mathbb{Z} \mid p \in \mathbb{P} \setminus T_0\}$ and S is the multiplicatively generated set by the elements of T_0, then

$$B := \bigcap_{\mathfrak{p} \in T} R_{\mathfrak{p}} = S^{-1}\mathbb{Z}.$$

Are these localisations again unique factorisation domains? Is there a connection between subintersections and localisations? Both of these questions will be answered soon.

From now on B will be used to describe a subintersection of a given Krull domain A given by some $T \subseteq \mathtt{P}(A)$, if not stated otherwise.

Proposition 3.25. *Let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset. Then the localisation $S^{-1}A$ is again a Krull domain and the essential valuations are given by $\{\mathfrak{p} \in \mathtt{P}(A) | S \cap \mathfrak{p} = \emptyset\}$.*

In other words, a non-trivial localisation of a Krull domain can be treated as a subintersection of A.

Proof. Using Proposition 3.22, it suffices (and is necessary) to verify

$$S^{-1}A = \bigcap_{\substack{\mathfrak{p} \in \mathtt{P}(A) \\ \mathfrak{p} \cap S = \emptyset}} R_{\nu_{\mathfrak{p}}}.$$

"$\subseteq$" Let $\mathfrak{p} \in \mathtt{P}(A)$ such that $\mathfrak{p} \cap S = \emptyset$. Then for $d \in S$, $\nu_{\mathfrak{p}}(d) = 0$ by Lemma 3.7. Thus we have for $a \in A$ and $d \in S$

$$\nu_{\mathfrak{p}}(\frac{a}{d}) = \nu_{\mathfrak{p}}(a) - \nu_{\mathfrak{p}}(d) = \nu_{\mathfrak{p}}(a) \geq 0.$$

Hence $S^{-1}A \subseteq R_{\nu_{\mathfrak{p}}}$.

"$\supseteq$" Let $x \in \bigcap_{\substack{\mathfrak{p} \in \mathtt{P}(A) \\ \mathfrak{p} \cap S = \emptyset}} R_{\nu_{\mathfrak{p}}}$ and consider $Q(x) := \{\mathfrak{q} \in \mathtt{P}(A) \mid \nu_{\mathfrak{q}}(x) < 0\}$. By definition, there is some $s_{\mathfrak{q}} \in \mathfrak{q} \cap S$ for any $\mathfrak{q} \in Q(x)$ and therefore

$$S \ni s := \prod_{\mathfrak{q} \in Q(x)} s_{\mathfrak{q}}^{-\nu_{\mathfrak{q}}(x)} \in \sum_{\mathfrak{q} \in Q(x)} -\nu_{\mathfrak{q}}(x)\mathfrak{q} =: \overline{\mathfrak{a}} \subseteq A.$$

As for any $a \in \overline{\mathfrak{a}}$ and $\mathfrak{p} \in \mathtt{P}(A)$ we have $\nu_{\mathfrak{p}}(a) \geq -\nu_{\mathfrak{p}}(x)$ the following relations

$$\nu_{\mathfrak{p}}(sx) = \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(s) \geq \nu_{\mathfrak{p}}(x) - \nu_{\mathfrak{p}}(x) = 0$$

holds for any $\mathfrak{p} \in \mathtt{P}(A)$. Hence $sx \in A$ and thus

$$\bigcap_{\substack{\mathfrak{p} \in \mathtt{P}(A) \\ \mathfrak{p} \cap S = \emptyset}} R_{\nu_{\mathfrak{p}}} \subseteq S^{-1}A \subseteq \bigcap_{\substack{\mathfrak{p} \in \mathtt{P}(A) \\ \mathfrak{p} \cap S = \emptyset}} R_{\nu_{\mathfrak{p}}}. \qquad \square$$

Lemma 3.26. *Let B be a subintersection of a Krull domain A given by $T \subseteq \mathtt{P}(A)$. Then there is a bijection $\pi \colon T \to \mathtt{P}(B)$ defined by*

$$T \ni \mathfrak{p} \mapsto \{a \in B \mid \nu_{\mathfrak{p}}(a) \geq 1\} \in \mathtt{P}(B).$$

Proof. Let $\mathscr{P} \in \mathtt{P}(B)$ with $\nu_{\mathscr{P}} = \nu_{\mathfrak{p}}$ for some $\mathfrak{p} \in T$ as by Proposition 3.22, the family of essential valuations of $\mathtt{P}(B)$ is given by T. Now Lemma 3.7 shows the surjectivity and well definedness of π via

$$\mathscr{P} = \{a \in B \mid \nu_{\mathscr{P}}(a) \geq 1\} = \{a \in B \mid \nu_{\mathfrak{p}}(a) \geq 1\}.$$

The injectivity holds since $\mathfrak{p} = \pi(\mathfrak{p}) \cap A$ by Lemma 3.7 combined with Corollary 3.13. $\square$

Lemma 3.27. *Let B be a subintersection of a Krull domain A given by $T \subseteq \mathtt{P}(A)$. Consider $\mathfrak{p} \in \mathtt{P}(A)$. Then the following hold:*

i) If $\mathfrak{p} \notin T$ then $\overline{\mathfrak{p}B} = B$.

ii) If $\mathfrak{p} \in T$ then $\overline{\mathfrak{p}B} = (B : (B : \mathfrak{p}B)) = \{a \in B \mid \nu_{\mathfrak{p}}(a) \geq 1\} \in \mathtt{P}(B)$.

Proof. Considering $\mathfrak{p} \in \mathtt{P}(A)$, we know that for every $\mathfrak{q} \in T' := T \setminus \{\mathfrak{p}\}$, there is some $x \in \mathfrak{p} \setminus \mathfrak{q}$, since by their minimality they must not contain one another. By Lemma 3.7 $\nu_{\mathfrak{q}}(x) = 0$ for such an x. Now let us consider $(B : \mathfrak{p}B)$.

i) For $\mathfrak{p} \notin T$ we have

$$(B : \mathfrak{p}B) = \{x \in K \mid \forall \mathfrak{q} \in T\ \nu_{\mathfrak{q}}(x) \geq 0\} = B = (B : B)$$

by the argument above. This shows $\overline{\mathfrak{p}B} = B$ using Lemma 2.4.

ii) By Corollary 3.9 there is some

$$x_{\mathfrak{p}} \in \mathfrak{p} \subseteq \mathfrak{p}B \subseteq \{a \in B \mid \nu_{\mathfrak{p}}(a) \geq 1\} =: \mathscr{P}$$

with $\nu_{\mathfrak{p}}(x_{\mathfrak{p}}) = 1$. Hence

$$(B : \mathfrak{p}B) = \{x \in K \mid \forall \mathfrak{q} \in T'\ \nu_{\mathfrak{q}}(x) = 0 \wedge \nu_{\mathfrak{p}}(x) \geq -1\} = (B : \mathscr{P})$$

and applying Lemma 2.4 again shows, that $\overline{\mathfrak{p}B} = \overline{\mathscr{P}}$. Lastly, $\overline{\mathscr{P}} = \mathscr{P} \in \mathtt{P}(B)$ by Lemma 3.26 above. □

Theorem 3.28 (*Nagata's Theorem*).
For a Krull domain A and a subintersection $B = \bigcap_{\mathfrak{p} \in T} R_{\nu_{\mathfrak{p}}}$ given by $T \subseteq \mathtt{P}(A)$ the map

$$\begin{aligned} \pi \colon \mathtt{D}(A) &\to \mathtt{D}(B) \\ \overline{\mathfrak{a}} &\mapsto \overline{\overline{\mathfrak{a}}B} \end{aligned}$$

is a surjective group homomorphism sending principal ideals to principal ideals. Furthermore, π induces a surjective group homomorphism.

$$\begin{aligned} \bar{\pi} : \mathtt{Cl}(A) &\to \mathtt{Cl}(B) \\ \boldsymbol{c}(\overline{\mathfrak{a}}) &\mapsto \boldsymbol{c}(\overline{\overline{\mathfrak{a}}B}) \end{aligned}$$

The kernel of π and $\bar{\pi}$ is generated by (the equivalence classes) of the prime divisorial ideals $\mathfrak{p} \in \mathtt{P}(A) \setminus T$.

Proof. This proof is based on the proof given in [Fos73, p. 35, Chapter II, §7, Theorem 7.1]. Corollary 2.5 shows that

$$\overline{\overline{\mathfrak{a}}B} + \overline{\overline{\mathfrak{b}}B} = \overline{\overline{\mathfrak{a}}B\overline{\mathfrak{b}}B} = \overline{\overline{\mathfrak{a}}\overline{\mathfrak{b}}B}$$

for two divisorial ideals $\overline{\mathfrak{a}}, \overline{\mathfrak{b}} \in \mathtt{D}(A)$. Hence π is indeed a group homorphism.

Now Lemma 3.26 and 3.27 above state, that $\mathfrak{p} \in \mathtt{P}(A) \setminus T$ is in the kernel of π and T is mapped bijectively to the free generating set $\mathtt{P}(B)$ of $\mathtt{D}(B)$. Hence π is a surjective group homomorphism with kernel $H := \langle \{\mathfrak{p} \mid \mathfrak{p} \in \mathtt{P}(A) \setminus T\} \rangle$.

Next consider the restriction of π to $\mathtt{Prin}(A)$. For $x \in K^\times$

$$\pi(xA) = \overline{xAB} = \overline{xB} = xB \in \mathtt{Prin}(B).$$

So the restriction yields a group homomorphism

$$\pi\mid_{\mathtt{Prin}(A)}\colon \mathtt{Prin}(A) \mapsto \mathtt{Prin}(B),$$

which is surjective as for $x \in K^{\times}$ xA is a preimage for xB.

Hence the kernel of

$$\begin{aligned} \tilde{\pi} : \mathtt{D}(A) \to \mathtt{D}(B) &\to {}^{\mathtt{D}(B)}\!\big/_{\mathtt{Prin}(B)} = \mathtt{Cl}(B) \\ \overline{a} \mapsto \overline{\overline{a}B} &\mapsto \boldsymbol{c}(\overline{\overline{a}B}) \end{aligned}$$

is $\ker(\tilde{\pi}) = H + \mathtt{Prin}(A)$, since if $\pi(\overline{a}) = xB$ we have $\overline{a} - xA \in \ker(\pi) = H$. Therefore, $\tilde{\pi}$ induces a map $\bar{\pi}\colon \mathtt{Cl}(A) = {}^{\mathtt{D}(A)}\!\big/_{\mathtt{Prin}(A)} \to \mathtt{Cl}(B)$ since $\mathtt{Prin}(A) \subseteq \ker(\tilde{\pi})$ for which the kernel is

$$\ker(\bar{\pi}) = {}^{(H + \mathtt{Prin}(A))}\!\big/_{\mathtt{Prin}(A)} = {}^{H}\!\big/_{\mathtt{Prin}(A)}. \qquad \square$$

Corollary 3.29. *The class group of a subintersection B of a Krull domain is a homomorphic image of the class group of A.* □

Example 3.30. Subintersections of unique factorisation domains are again unique factorisation domains, in particular the localisations of $\mathbb{Z}$ considered in Example 3.24.

Remark 3.31. Nagata studied Krull domains as they occur as the integral closure of noetherian domains ([Nag62, p. 118, Chapter V, 33., (33.10) Theorem]). In this context, he proved, that the localisation at a multiplicatively closed set $S \not\ni 0$ of a Krull domain is again a Krull domain, which can be seen in [Nag62, p.116f., Chapter V, 33., (33.6) Theorem].

Samuel contributes to Nagata a version of this Theorem, which is more similar to our own, namely [Sam64, p. 21, Chapter I, §6,Theorem 6.3]. This will be our second version of Nagata's Theorem.

Theorem 3.32 (Nagata's Theorem second version)**.**
Let $B := S^{-1}A$ be the localisation of a Krull domain A on a multiplicatively closed subset $S \subseteq A$, multiplicatively generated by prime elements. Then the group homomorphism

$$\begin{aligned} \pi\colon D(A) &\to D(B) \\ \overline{a} &\mapsto \overline{\overline{a}B} \end{aligned}$$

induces an isomorphism

$$\begin{aligned} \bar{\pi} : \mathtt{Cl}(A) &\to \mathtt{Cl}(B) \\ \boldsymbol{c}(\overline{a}) &\mapsto \boldsymbol{c}(\overline{\overline{a}B}) \end{aligned}$$

on the class groups, i.e. $\mathtt{Cl}(A) \cong \mathtt{Cl}(B)$.

Proof. By the first version of Nagata's Theorem above and the characterisation of localisations as subintersections from Proposition 3.25, the map $\bar{\pi} : \mathtt{Cl}(A) \to \mathtt{Cl}(B)$ is a surjective group homomorphism with kernel

$$\ker(\bar{\pi}) = {\langle \{ \mathfrak{p} \in P(A) \mid \mathfrak{p} \cap S \neq \emptyset \} \rangle} \big/ {\mathtt{Prin}(A)}.$$

Here we used, that $0 \notin S$, because 0 is no product of prime elements.

Now, as described in [Sam64, p. 21, Chapter I, §6, Theorem 6.3], consider such a prime divisorial ideal $\mathfrak{p} \in \mathtt{P}(A)$ with $\mathfrak{p} \cap S \neq \emptyset$. Then there are some prime elements $s_0, \ldots, s_n \in S$ for some $n \in \mathbb{N}$ such that $\prod_{i=0}^{n} s_i \in \mathfrak{p} \cap S$. Since $\mathfrak{p}$ is prime, there is some $0 \leq j \leq n$ with $s_j \in \mathfrak{p}$. But $s_j A$ and $\mathfrak{p}$ are both prime divisorial ideals and thus $\mathfrak{p} = s_j A \in \mathtt{Prin}(A)$ is principal. Therefore

$$\ker(\bar{\pi}) = {\langle \{ \mathfrak{p} \in P(A) \mid \mathfrak{p} \cap S \neq \emptyset \} \rangle} \big/ {\mathtt{Prin}(A)} \subseteq {\mathtt{Prin}(A)} \big/ {\mathtt{Prin}(A)} \cong 0$$

shows that $\bar{\pi}$ is also injective. $\square$

Theorem 3.33. *For an index set I the polynomial ring $A[X_i \mid i \in I]$ is again a Krull domain. Furthermore*

$$\begin{aligned} \iota \colon \mathtt{D}(A) &\to \mathtt{D}(A[X_i | i \in I]) \\ \overline{\mathfrak{a}} &\mapsto \overline{\overline{\mathfrak{a}} A[X_i \mid i \in I]} \end{aligned}$$

is an injective group homomorphism sending prime divisors to prime divisors and principal ideals to principal ideals. Furthermore ι induces an isomorphism

$$\begin{aligned} \bar{\iota} \colon \mathtt{Cl}(A) &\to \mathtt{Cl}(A[X_i \mid i \in I]) \\ \boldsymbol{c}(\overline{\mathfrak{a}}) &\mapsto \boldsymbol{c}(\overline{\overline{\mathfrak{a}} A[X_i \mid i \in I]}) \end{aligned}$$

of class groups.

Proof. To show that $A[X_i \mid i \in I]$ is again a Krull domain we will follow the proof of [Sam64, p. 11, Chapter I, §4, Proposition 4.3]. With this in mind, define for a prime divisorial ideal $\mathfrak{p} \in \mathtt{P}(A)$ the map

$$\begin{aligned} \tilde{\nu}_{\mathfrak{p}} \colon F[X_i \mid i \in I] \setminus \{0\} &\to \mathbb{Z} \\ \sum_{j=1}^{n} a_j \prod_{i \in I_j}^{n_j} X_i^{n_{ij}} &\mapsto \min_{1 \leq j \leq n} \{ \nu_{\mathfrak{p}}(a_j) \} \end{aligned}$$

where $F = \mathrm{Frac}(A)$ is the field of fractions of A. It is easy to see, that $\tilde{\nu}_{\mathfrak{p}}$ is a monoid homomorphism satisfying the conditions to be a discrete valuation as $\nu_{\mathfrak{p}}$ was a discrete valuation. Thus it can be uniquely extended to a discrete valuation on $F(X_i \mid i \in I) := \mathrm{Frac}(F[X_i \mid i \in I]) = \mathrm{Frac}(A[X_i \mid i \in I])$ by Proposition 1.41.

Any given polynomial has only finitely many coefficients, for which only finitely many valuations $\nu_{\mathfrak{p}}$ are non-trivial for $\mathfrak{p} \in \mathtt{P}(A)$. Thus almost all of the valuations $\tilde{\nu}_{\mathfrak{p}}$ vanish on any given element of $F(X_i \mid i \in I)$. So the Valuation Criterion states that $\bigcap_{\mathfrak{p}\in\mathtt{P}(A)} R_{\tilde{\nu}_{\mathfrak{p}}}$ is a Krull domain.

By Example 1.26, $F[X_i \mid i \in I]$ is a a unique factorisation domain and thus a Krull domain by Theorem 3.19. Hence by Proposition 3.20

$$A[X_i \mid i \in I] = F[X_i \mid i \in I] \cap \bigcap_{\mathfrak{p}\in\mathtt{P}(A)} R_{\tilde{\nu}_{\mathfrak{p}}} = \bigcap_{\mathfrak{q}\in\mathtt{P}(F[X_i|i\in I])} R_{\nu_{\mathfrak{q}}} \cap \bigcap_{\mathfrak{p}\in\mathtt{P}(A)} R_{\tilde{\nu}_{\mathfrak{p}}}$$

is a Krull domain. This equality holds, because in the ring on the right hand side, there are only the polynomials in $F[X_i \mid i \in I]$, whose coefficients are in $A = \bigcap_{\mathfrak{p}\in\mathtt{P}(A)} R_{\nu_{\mathfrak{p}}}$.

In fact the valuations $\tilde{\nu}_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathtt{P}(A)$ are essential valuations by Corollary 3.16, because none of the valuations can be omitted from the intersection above. Otherwise, the elements of $-\mathfrak{p} \not\subseteq A$ are an element of the intersection, if any $\tilde{\nu}_{\mathfrak{p}}$ was omitted for some $\mathfrak{p} \in A$, or for a prime polynomial

$$\sum_{j=1}^{n} \frac{a_j}{b_j} \prod_{i\in I_j}^{n_j} X_i^{n_{ij}} = p \in F[X_i \mid i \in I]$$

the element $\left((\prod_{j=1}^{n} \frac{1}{a_j})p\right)^{-1} \notin A[X_i \mid i \in I]$ was in the intersection, if the valuation $\nu_{\langle p\rangle}$ was omitted. (Recall that every prime divisorial ideal of a unique factorisation domain is principal.)

Now by similar methods as for the proof of Nagata's Theorem and its corresponding Lemmata 3.26 and 3.27, the map ι is indeed a group homomorphism sending principal ideals to principal ideals. Furthermore, for a prime divisorial ideal $\mathfrak{p} \in \mathtt{P}(A)$

$$\overline{\mathfrak{p}A[X_i \mid i \in I]} = \{x \in A[X_i \mid i \in I] \mid \tilde{\nu}_{\mathfrak{p}}(x) \geq 1\} \in \mathtt{P}(A[X_i \mid i \in I]),$$

since $\tilde{\nu}_{\mathfrak{p}} |_A = \nu_{\mathfrak{p}}$. That ι is injective is again a consequence of $\mathfrak{p} = \overline{\mathfrak{p}A[X_i \mid i \in I]} \cap A$.

For a prime divisorial ideal $\mathfrak{p} \in \mathtt{P}(A)$ let $\mathscr{P} := \{x \in A[X_i \mid i \in I] \mid \tilde{\nu}_{\mathfrak{p}}(x) \geq 1\}$ be the corresponding prime divisorial ideal in $A[X_i \mid i \in I]$. Then every principal ideal in the image of ι

$$fA[X_i|i \in I] \in \mathrm{im}(\iota) = \langle \{\mathscr{P} \mid \mathfrak{p} \in \mathtt{P}(A)\}\rangle =: H$$

meets A non-trivially, because this holds true for the generators. Hence $\deg(f) = 0$ so that $f \in A$ and $fA[X_i|i \in I] = \iota(fA)$. Therefore

$$\begin{aligned} \bar{\iota} : \mathtt{Cl}(A) = \mathtt{D}(A)/\mathtt{Prin}(A) &\to H/\mathtt{Prin}(A[X_i|i \in I]) \\ \boldsymbol{c}(\overline{\mathfrak{a}}) &\mapsto \boldsymbol{c}(\overline{\overline{\mathfrak{a}}A[X_i|i \in I]}) \end{aligned}$$

is an isomorphism.

Last but not least, the unique factorisation domain $F[X_i \mid i \in I]$ is a subintersection of $A[X_i \mid i \in I]$ with trivial class group by Theorem 3.19. Hence

$$\begin{aligned}\mathtt{Cl}(A[X_i \mid i \in I]) &= \ker\Big(\bar{\pi}\colon \mathtt{Cl}(A[X_i \mid i \in I]) \to \mathtt{Cl}(F[X_i \mid i \in I])\Big) \\ &= H\big/\mathtt{Prin}(A[X_i \mid i \in I])\end{aligned}$$

where the last equality and $\bar{\pi}$ come from Nagata's Theorem. Recall that $\bar{\pi}(\boldsymbol{c}(\mathfrak{p})) = \boldsymbol{c}(\overline{\mathfrak{p}F[X_i \mid i \in I]})$ for $\mathfrak{p} \in \mathtt{P}(A[X_i \mid i \in I])$. Hence

$$\bar{\iota}\colon \mathtt{Cl}(A) = \mathtt{D}(A)\big/\mathtt{Prin}(A) \to H\big/\mathtt{Prin}(A[X_i \mid i \in I]) = \mathtt{Cl}(A[X_i \mid i \in I])$$

is an isomorphism of class groups. □

Remark 3.34. In general, we cannot assume for an arbitrary subring R of a polynomial ring, that the elements of R, which are prime elements of the polynomial ring, are again prime in R. An instance of this can be seen in Example 3.37.

So what happens with the additional prime divisorial ideals gained by considering the polynomial ring $A[X]$ instead of A? A partial answer of this will be given in Proposition 3.40.

Remark 3.35. In a similar fashion, it can be shown, that the ring of formal power series $A[[X]]$ over a Krull domain A is again a Krull domain. For this see [Sam64, p. 12, Chapter I, §4, Proposition 4.4]. However, in this case we generally just have an injective homomorphism $\mathtt{Cl}(A) \to \mathtt{Cl}(A[[X]])$. For this, see [Fos73, p. 35, Chapter II, §6, Corollary 6.13].

3.3 Class Groups of Krull Domains

With our developed tools, we will now be able to construct a Krull domain with a free class group of arbitrary rank. Afterwards, we will complete our notion of the class group of a subintersection as a homomorphic image of the class group of a given Krull domain. In particular, we will show that every homomorphic image of a class group can itself be realised as the class group of a subintersection of the polynomial ring in one variable over the Krull domain. Ultimately, this means, that every abelian group can be realised as the class group of a Krull domain.

Proposition 3.36. *Every free abelian group is the class group of a Krull domain.*

Proof. This proof is based on the proof of [Cla66, p. 221, Proposition 6]. Let I be some index set and K be an arbitrary field. Consider the unique factorisation domain $B := K[X_i, Y_i, Z_i \mid i \in I]$ (1.26) and the subrings

$$R_j := K[X_i, Y_i, Z_i \mid j \neq i \in I][X_j, Y_j, X_jZ_j]$$

for $j \in I$. Note that for every $j \in I$ we have $\mathrm{Frac}(R_j) = \mathrm{Frac}(B) =: F$. For every index $j \in I$ define the map

$$\begin{aligned} \nu_j \colon R_j &\to \mathbb{Z} \\ f &\mapsto \max\{n \in \mathbb{N} \mid f \in \langle X_j, Y_j\rangle_{R_j}^n\} \end{aligned}$$

where the maximum always exists, because the elements of $\langle X_j, Y_j\rangle_{R_j}^n \subseteq R_j$ have at least degree n. It is easy to see, that ν_j is a homomorphism of monoids meeting the requirements to be a discrete valuation, so ν_j extends uniquely to a discrete valuation ν_j on F by Proposition of 1.41. As every polynomial $f \in B$ has only finitely many variables, almost all the valuations ν_i with $i \in I$ vanish on any given polynomial. Therefore, the same holds true for the elements of F. Hence $\bigcap_{i\in I} R_{\nu_i}$ is a Krull domain by the Valuation Criterion.

Now, in a similar fashion to what we did in the proof of Theorem 3.33,

$$A := B \cap \bigcap_{i\in I} R_{\nu_i} = \bigcap_{\mathfrak{q}\in \mathrm{P}(B)} R_{\nu_\mathfrak{q}} \cap \bigcap_{i\in I} R_{\nu_i}$$

is a Krull domain by Proposition 3.20, whose essential valuations are the ones given in the intersection. For the last part note that $\mathrm{Frac}(A) = F$, as for any $i \in I$, $R_i \subseteq A$, and then utilise Corollary 3.16:

1. If for some $i \in I$ the valuation ν_i is omitted from the intersection, then $Z_i \notin A$ is an element of the intersection, since

$$\nu_i(Z_i) = \nu_i(\frac{X_i Z_i}{X_i}) = \nu_i(Z_i X_i) - \nu_i(X_i) = 0 - 1 = -1.$$

2. If for $i \in I$ the valuation $\nu_{X_i B}$ is omitted from the intersection, then $\frac{Y_i}{X_i} \notin A$ is an element of the intersection.

3. If for a prime element $p \in B$ with $pB \neq X_i B$ for all $i \in I$ the valuation ν_{pB} is omitted, then

$$\prod_{\substack{i\in I \\ \nu_i(p)>0}} X_i^{\nu_i(p)} \frac{1}{p} \notin A$$

is an element of the intersection, since p is a unit in all other essential valuation rings of B.

As every prime divisorial ideal of the unique factorisation domain B is principal, the case distinction above is complete. Hence none of the valuations can be omitted from the intersection.

Now B is a subintersection of A with trivial class group by Theorem 3.19 and thus by Nagata's Theorem

$$\mathtt{Cl}(A) = (\ker(\bar{\pi}) \colon \mathtt{Cl}(A) \to \mathtt{Cl}(B)) = \langle\{\mathfrak{p}_i \mid i \in I\}\rangle / \mathtt{Prin}(A)$$

where $\mathfrak{p}_i$ is the prime divisorial ideal corresponding to ν_i for $i \in I$. Recall that $\bar{\pi}(\mathfrak{c}(\mathfrak{p})) = \mathfrak{c}(\overline{\mathfrak{p}B})$ for $\mathfrak{p} \in \mathtt{P}(A)$ as it was defined in Nagata's Theorem.

Assume for some finite $J \subseteq I$ and integers $n_j \in \mathbb{Z}$ for $j \in J$ that

$$\sum_{j \in J} n_j \mathfrak{p}_j = fA \in \mathtt{Prin}(A)$$

was principal with $f \in F^\times$. Now by definition of the valuations, $\nu_{\mathfrak{q}}(f) = 0$ for every prime divisorial ideal $\mathfrak{q} \in \mathtt{P}(B)$ and thus f is a unit in B, i.e.

$$f \in B^\times = K[X_i, Y_i, Z_i \mid i \in I]^\times = K^\times \subseteq A^\times.$$

Hence $n_j = 0$ for all $j \in J$ as $fA = A$ and $\{\mathfrak{p}_i \mid i \in I\}$ is a free generating set of $\langle \{\mathfrak{p}_i \mid i \in I\} \rangle$. All in all,

$$\mathtt{Cl}(A) = {\langle \{\mathfrak{p}_i \mid i \in I\} \rangle}/{\mathtt{Prin}(A)} \cong \langle \{\mathfrak{p}_i \mid i \in I\} \rangle \cong \mathbb{Z}^{(I)}.$$

Since I was arbitrary, any free abelian group can be realised as the class group of a Krull domain up to isomorphism. □

Example 3.37. Let us construct a Krull domain whose class group is $\mathbb{Z}$. Consider the index set $\{0\}$ and leave out the index of the variables X_0, Y_0 and Z_0. Define $R_0 := K[X, Y, XZ]$ and recall that the discrete valation ν_0 was defined for $a \in R_0$ by the maximal power $n \in \mathbb{N}$ for which $a \in \langle X, Y \rangle_{R_0}^n$.

Proceeding in the vein of the proof of Proposition 3.36 above, we are interested in the $f \in K[X, Y, Z] = K[X, Y][Z]$ with $\nu_0(f) \geq 0$. For the sake of convenience, let us express everything in terms of R-modules with $R := K[X, Y]$. In this manner, let $f = \sum_{i=0}^n f_i Z^i \in R[Z]$ with $f_i \in R$ for $0 \leq i \leq n$ and some $n \in \mathbb{N}$. Then

$$(*) \qquad \nu_0(f) = \nu_0\left(\frac{X^n f}{X^n}\right) = \nu_0\left(\sum_{i=0}^n f_i X^{n-i} (XZ)^i\right) - n.$$

Hence $\nu_0(f) \geq 0$ if and only if $\nu_0(X^n f) \geq n$, which by the definition of ν_0 and $X^n f \in R_0$ is equivalent to $\nu_0(f_i X^{n-i}) \geq n$ for $0 \leq i \leq n$. This is the case if and only if

$$f_i \in \langle X, Y \rangle_{R_0}^i \cap R = \langle X, Y \rangle_R^i$$

for every $0 \leq i \leq n$. This yields

$$A := R_{\nu_0} \cap K[X, Y, Z] = \sum_{n \in \mathbb{N}} Z^n \langle X, Y \rangle_R^n = K[X, Y, XZ, YZ],$$

which is a Krull domain as described in the proof of Proposition 3.36 with a class group isomorphic to $\mathbb{Z}$.

Let us do a "sanity check". What is the prime divisorial ideal corresponding to ν_0? Equation $(*)$ yields

$$\mathfrak{p}_0 := \{a \in A \mid \nu_0(a) \geq 1\} = \sum_{n\in\mathbb{N}} Z^n \langle X, Y\rangle_R^{n+1} = \langle X, Y\rangle_A.$$

More generally, we have $k \cdot \mathfrak{p}_0 = \langle X, Y\rangle_A^k$ for $k \in \mathbb{N}$.

Note that $XA \neq A \cap XK[X, Y, Z]$ since $XYZ^2 \in (A \cap XK[X, Y, Z]) \setminus XA$. So the above does not contradict Example 2.2 (5). In particular X and in a similar fashion Y, are not prime in A. This can also be seen by computing $\nu_0(X) = 1 = \nu_0(Y)$. Nonetheless, since X and Y are prime in $K[X, Y, Z] \supseteq A$, no positive multiple of $\mathfrak{p}_0$ can be principal.

For the sake of completion and later use, let us compute $-\mathfrak{p}_0$. First note that by definition ν_0 is the only essential valuation of A, which may become negative. Thus, we are still looking for a subset of $K[X, Y, Z]$. Consulting equation $(*)$ again, we get

$$-\mathfrak{p}_0 = \{f \in K[X, Y, Z] \mid \nu_0(f) \geq -1\} = \sum_{n\in\mathbb{N}} Z^{n+1} \langle X, Y\rangle_R^n + R = \langle Z, 1\rangle_A.$$

More generally, we get

$$-k\mathfrak{p}_0 = \sum_{n\in\mathbb{N}} Z^{k+n} \langle X, Y\rangle_R^n + \sum_{l=0}^{k-1} Z^l R = \langle Z^n \mid 0 \leq n \leq k\rangle_A$$

for $k \in \mathbb{N}$. It straight forward to check, that every essential valuation of A vanishes on one of the three elements $Z^k X^k$, $Z^k Y^k$ and X^k for every $k \in \mathbb{N}$. Hence

$$1 \in \overline{\langle Z^k X^k, Z^k Y^k, X^k\rangle_A} \subseteq k\mathfrak{p}_0 + (-k\mathfrak{p}_0) \subseteq A$$

after applying Lemma 3.7. Recall that $Z \notin A$. Hence no positive multiple of $-\mathfrak{p}_0$ can be principal, as we expected.

Theorem 3.38 (*Approximation Theorem*).
For a Krull domain A and any finite subset $Q \subseteq \mathsf{P}(A)$ of the prime divisors and $n = (n_{\mathfrak{q}})_{\mathfrak{q}\in Q} \in \mathbb{N}^Q$, there is some $x_Q \in A \setminus \{0\}$ such that for the prime divisors $\mathfrak{q} \in Q$ $\nu_{\mathfrak{q}}(x_Q) = n_{\mathfrak{q}}$. The element x_Q is called an approximation of Q.

Proof. Our proof will be loosely based on the proof of [Fos73, p. 26, Chapter I, §5, Theorem 5.8], using the notions we developed in this Chapter.

If Q is empty, $x_Q := 1$ has the desired property. Otherwise, it is sufficient to show that for every $\mathfrak{p} \in Q$ there is some $x_{\mathfrak{p};Q} \in A$ such that for $\mathfrak{q} \in Q$

$$\nu_{\mathfrak{q}}(x_{\mathfrak{p};Q}) = \begin{cases} 1 & \text{if } \mathfrak{q} = \mathfrak{p} \\ 0 & \text{else} \end{cases}$$

as then $x_Q := \prod_{\mathfrak{q} \in Q} x_{\mathfrak{q};Q}^{n_\mathfrak{q}}$ is the desired element.

So for a fixed $\mathfrak{p} \in Q$ take an $x_\mathfrak{p}$ with $\nu_\mathfrak{p}(x_\mathfrak{p}) = 1$ as in Corollary 3.9 and let $Q_\mathfrak{p} := \{\mathfrak{q} \in Q \setminus \{\mathfrak{p}\} \mid \nu_\mathfrak{q}(x_\mathfrak{p}) > 0\}$. As a contraposition of prime avoidance $\mathfrak{p}^2 \setminus \bigcup_{\mathfrak{q}' \in Q_\mathfrak{p}} \mathfrak{q}' \neq \emptyset$, because $\overline{\mathfrak{p}^2}$ is not comparable with any of the elements of $Q_\mathfrak{p}$. Hence, we may take $y_\mathfrak{p} \in \mathfrak{p}^2 \setminus \bigcup_{\mathfrak{q}' \in Q_\mathfrak{p}} \mathfrak{q}'$ and for $\mathfrak{p} \neq \mathfrak{q}' \in Q \setminus Q_\mathfrak{p}$ some $y_\mathfrak{q} \in \mathfrak{q} \setminus \bigcup_{\mathfrak{q}' \in Q_\mathfrak{p}} \mathfrak{q}' \neq \emptyset$ by a similar argument. As any ideal in $Q_\mathfrak{p}$ is prime, the following holds for any $\mathfrak{q} \in Q \setminus \{\mathfrak{p}\}$

$$\mathfrak{q} \not\ni x_{\mathfrak{p};Q} := x_\mathfrak{p} + \prod_{\mathfrak{q}' \in Q \setminus Q_\mathfrak{p}} y_{\mathfrak{q}'} \in \mathfrak{p}$$

as only one of the summands is an element of $\mathfrak{q}$. Last but not least, $x_{\mathfrak{p};Q} \in \mathfrak{p} \setminus \overline{\mathfrak{p}^2}$, since $x_\mathfrak{p} \in \mathfrak{p} \setminus \overline{\mathfrak{p}^2}$ and $\prod_{\mathfrak{q}' \in Q \setminus Q_\mathfrak{p}} y_{\mathfrak{q}'} \in \mathfrak{p}^2$. So by Lemma 3.7

$$\nu_\mathfrak{q}(x_{\mathfrak{p};Q}) = \begin{cases} 1 & \text{if } \mathfrak{q} = \mathfrak{p} \\ 0 & \text{else} \end{cases}$$

for any $\mathfrak{q} \in Q$. □

Corollary 3.39. *For any integral divisorial ideal $\overline{\mathfrak{a}}$ there are some $a_0, a_1 \in A \setminus \{0\}$ such that*

$$\overline{\mathfrak{a}} = \overline{\langle a_0,\, a_1 \rangle}.$$

In this case, a_0 and a_1 are called an approximation of $\overline{\mathfrak{a}}$.

Proof. For $\overline{\mathfrak{a}} = \sum_{\mathfrak{p} \in \mathtt{P}(A)} n_\mathfrak{p} \mathfrak{p}$ let a_0 be an approximation of $Q_0 := \{\mathfrak{p} \in \mathtt{P}(A) \mid n_\mathfrak{p} > 0\}$ and $(n_\mathfrak{p})_{\mathfrak{p} \in Q_0} \in \mathbb{N}^{Q_0}$. Furthermore, let a_1 be an approximation of $Q_0 := \{\mathfrak{p} \in \mathtt{P}(A) \mid \nu_\mathfrak{p}(a_0) > 0\}$ with $(n_\mathfrak{p})_{\mathfrak{p} \in Q_0} \times (0)_{\mathfrak{p} \in Q_1 \setminus Q_0} \in \mathbb{N}^{Q_1}$. Then

$$\overline{\langle a_0,\, a_1 \rangle} = \inf(a_0 A,\, a_1 A) \overset{3.3}{=} \overline{\mathfrak{a}}.$$ □

Proposition 3.40. *Every element $\boldsymbol{c} \in \mathtt{Cl}(A)$ of the class group of $A[X]$ has a prime divisorial ideal as its representative.*

Proof. For this proof, we will follow the proof of [Fos73, p. 63, Chapter III, §14, Theorem 14.3].

By Theorem 3.33 there is some divisorial ideal $\overline{\mathfrak{a}} \in \mathtt{D}(A)$ of A such that $\boldsymbol{c} = \boldsymbol{c}(\overline{\overline{\mathfrak{a}} A[X]})$ and thus $-\boldsymbol{c} = \boldsymbol{c}(\overline{-\overline{\mathfrak{a}} A[X]})$. Without loss of generality $-\overline{\mathfrak{a}}$ is integral, since for a common denominator $d \in A$

$$\boldsymbol{c}(\overline{-\overline{\mathfrak{a}} A[X]}) = \boldsymbol{c}(dA[X] - \overline{\overline{\mathfrak{a}} A[X]}) = \boldsymbol{c}(\overline{d(-\overline{\mathfrak{a}}) A[X]})$$

and $d(-\overline{\mathfrak{a}})$ is integral. So $\overline{\mathfrak{a}}$ and $-\overline{\mathfrak{a}}$ can be replaced by $d^{-1}\overline{\mathfrak{a}}$ and $d(-\overline{\mathfrak{a}})$. By Corollary 3.39 above, there are $a_0, a_1 \in A$ such that $-\overline{\mathfrak{a}} = \overline{\langle a_0,\, a_1 \rangle}$. Consider the prime element $(a_1 X - a_0) \in F[X]$ where $F = \mathrm{Frac}(A)$ is the field of fractions of A and by construction $a_0 \neq 0 \neq a_1$. By the proof of

Theorem 3.33 $\mathfrak{p} := (a_1X - a_0)F[X] \cap A[X]$ is a prime divisorial ideal of $A[X]$. Note that $\overline{\mathfrak{a}} = -\overline{\langle a_0, a_1 \rangle} = (A\colon \langle a_0, a_1 \rangle) = \{x \in F \mid a_0x, a_1x \in A\}$. Thus

$$(a_1X - a_0)F[X] \supseteq (a_1X - a_0)\overline{\mathfrak{a}}A[X] \subseteq A[X]$$

shows that $(a_1X - a_0)\overline{\mathfrak{a}}A[X] \subseteq \mathfrak{p}$. On the other hand, if we have $(a_1X - a_0)f \in \mathfrak{p}$ for some $f = \sum_{i=0}^{n} b_iX^i \in F[X]$ with $n := \deg(f)$, then $f \in \overline{\mathfrak{a}}A[X]$ by the following induction on the degree n of f.

If $n \leq 0$ and therefore $f = b_0$ then $a_1b_0X - a_0b_0 = (a_1X - a_0)b_0 \in A[X]$ and thus $b_0 \in \overline{\mathfrak{a}}$. For $n \geq 1$ use that $\overline{\mathfrak{a}}A[X]$ is an ideal and thus $f \in \overline{\mathfrak{a}}A[X]$ if and only if $b_i \in \overline{\mathfrak{a}}$ for $0 \leq i \leq n$. Hence it is sufficient to show that $b_n \in \overline{\mathfrak{a}}$, as then

$$(a_1X - a_0)(f - b_nX^n) = (a_1X - a_0)f - (a_1X - a_0)(b_nX^n) \in A[X],$$

so that the claim holds for the other b_i by the induction hypothesis.

Since

$$(a_1X - a_0)f = b_na_1X^{n+1} + \sum_{i=1}^{n}(a_1b_{i-1} - a_0b_i)X^i + a_0b_0 \in A[X],$$

all the coefficients are in A and thus $a_1b_n \in A$. It remains to verify that $a_0b_n \in A$. Now as A is completely integrally closed and thus by Corollary 1.32 normal, it is enough to show that a_0b_n is integral over A. For this consider the polynomial

$$q(X) := X^{n+1} + \sum_{i=1}^{n} \left((b_na_1)^{n-i}(a_1b_{i-1} - a_0b_i)X^i\right) - a_0b_0(a_1b_n)^n \in A[X]$$

for which $q(a_0b_n) = 0$, since

$$\begin{aligned}
&\sum_{i=1}^{n} \left((b_na_1)^{n-i}(a_1b_{i-1} - a_0b_i)(a_0b_n)^i\right) \\
=&b_n^n \sum_{i=0}^{n}(a_0^i a_1^{n-i+1} b_{i-1} - a_0^{i+1}a_1^{n-i}b_i) \\
=&b_n^n \left(\sum_{i=0}^{n-1}(a_0^{i+1}a_1^{n-i}b_i) - \sum_{i=1}^{n}(a_0^{i+1}a_1^{n-i}b_i)\right) \\
=&b_n^n \left(a_0a_1^nb_0 - a_0^{n+1}b_n\right) = -\left(a_0^{n+1}b_n^{n+1} - a_0b_0(a_1b_n)^n\right).
\end{aligned}$$

Hence $a_0b_n, a_1b_n \in A$ and thus $b_n \in \overline{\mathfrak{a}}$. Hence the claim is a consequence of induction as described above. Therefore

$$\overline{\overline{\mathfrak{a}}A[X] + (a_1X - a_0)A[X]} \overset{2.5}{=} \overline{(a_1X - a_0)\overline{\mathfrak{a}}A[X]} = \overline{\mathfrak{p}} = \mathfrak{p},$$

which shows that $\boldsymbol{c}(\overline{\overline{\mathfrak{a}}A[X]}) = \boldsymbol{c}(\overline{\overline{\mathfrak{a}}A[X] + (a_1X - a_0)A[X]}) = \boldsymbol{c}(\mathfrak{p})$. This finishes the proof. □

Proposition 3.41. *If G is the class group of a Krull domain A and G' is a homomorphic image of G, then there is a Krull domain B, whose class group is isomorphic to G'.*

Proof. We will proceed as in [Cla66, p. 221, Proposition 5].

Consider a surjective group homomorphism $\varphi\colon G \to G'$ which exists by assumption and let H be the isomorphic image of the kernel

$$\ker(\varphi) \subseteq G \cong \mathtt{Cl}(A) \overset{3.33}{\cong} \mathtt{Cl}(A[X])$$

in the class group of $A[X]$. Then φ induces an isomorphism $\mathtt{Cl}(A[X])/H \cong G/\ker(\varphi) \cong G'$. Now let $B := \bigcap_{\mathfrak{p} \in T_H} R_{\mathfrak{p}}$ be the subintersection given by

$$T_H := \{\mathfrak{p} \in \mathtt{P}(A[X]) \mid \boldsymbol{c}(\mathfrak{p}) \notin H\}.$$

Then by Nagata's Theorem the kernel of $\bar{\pi}\colon \mathtt{Cl}(A) \to \mathtt{Cl}(B)$ is given by

$$\begin{aligned} \ker(\bar{\pi}) &= \langle\{\boldsymbol{c}(\mathfrak{p}) \mid \mathfrak{p} \in \mathtt{P}(A) \setminus T_H\}\rangle \\ &= \langle\{\boldsymbol{c}(\mathfrak{p}) \mid \mathfrak{p} \in \mathtt{P}(A) \wedge \boldsymbol{c}(\mathfrak{p}) \in H\}\rangle \\ &\overset{3.40}{=} \langle H\rangle = H. \end{aligned}$$

Recall that $\bar{\pi}(\boldsymbol{c}(\mathfrak{p})) = \boldsymbol{c}(\overline{\mathfrak{p}B})$ for $\mathfrak{p} \in \mathtt{P}(A)$ as it was defined in Nagata's Theorem. Thus, as $\bar{\pi}$ is surjective, it induces an isomorphism

$$\mathtt{Cl}(B) \cong \mathtt{Cl}(A[X])/\ker(\bar{\pi}) = \mathtt{Cl}(A[X])/H \cong G'.$$

So B is a Krull domain with class group G'. □

Example 3.42. Let us construct a Krull domain with class group $\mathbb{Z}/n\mathbb{Z}$ for some positive $n \in \mathbb{N}$. Fix a field K and recall the Krull domain $A = K[X, Y, XZ, YZ]$ from Example 3.37 with essential valuation ν_0 and corresponding prime divisorial ideal $\mathfrak{p}_0 = \langle X, Y\rangle$.

Consider the polynomial ring $A[V]$ and the field of fractions $F := \mathrm{Frac}(A)$. In contrast to our approach for the proof of Proposition 3.41, it is sufficient to find a prime divisorial ideal of $F[V]$ with the same class group as $\overline{n\mathfrak{p}_0 A[V]}$. Then the subintersection leaving out the corresponding prime divisorial ideal already must have class group $\mathbb{Z}/n\mathbb{Z}$, because this class already generates the desired kernel.

To find such a prime divisorial ideal, we want to approximate $-n\mathfrak{p} = \langle Z^i\rangle_{i=0}^n$ or rather $X^n A + (\langle Z^i\rangle_{i=0}^n) = \overline{\langle X^n Z^i\rangle_{i=0}^n} \subseteq A$. Note that the only essential valuations not vanishing on all of these generators are ν_0 and the valuations $\nu_X := \nu_{\langle X\rangle}$ and $\nu_Z := \nu_{\langle Z\rangle}$ coming from $K[X, Y, Z]$. In particular we have for $0 \le i \le n$:

$$i = \nu_Z(X^n Z^i) \ge \nu_Z(X^n) = 0 \qquad n = \nu_X(X^n Z^i) \ge \nu_X(X^n) = n$$

$$n - i = \nu_0(X^n Z^i) \geq \nu_Z(X^n Z^n) = 0$$

This shows

$$\overline{\langle X^n Z^i \rangle_{i=0}^n} \subseteq \overline{\langle Z^n X^n, X^n \rangle} \subseteq \overline{\langle X^n Z^i \rangle_{i=0}^n} = X^n A - n\mathfrak{p}_0$$

after applying Lemma 3.7. Therefore

$$\mathfrak{c}(\overline{(-n\mathfrak{p}_0)A[V]}) = \mathfrak{c}(A[V] \cap (X^n V - X^n Z^n)F[V])$$

by the proof of Proposition 3.40. Let $T := \mathtt{P}(A[V]) \setminus \{A[V] \cap (X^n V - X^n Z^n)F[V]\}$ and define $B = \bigcap_{\mathfrak{p} \in T} R_{\nu_\mathfrak{p}}$.

Then the elements of B are of the form $\frac{f}{(X^n V - (XZ)^n)^r}$ for some $r \in \mathbb{N}$ and $f \in F[V]$. These are restricted by the lifts of the essential valuations of A described in the proof of Theorem 3.33. Out of these, only the valuations $\tilde{\nu}_X$, $\tilde{\nu}_Z$ and $\tilde{\nu}_0$ are of special interest. We have:

$$\tilde{\nu}_Z\big((X^n V - (XZ)^n)^r\big) = r \cdot 0 = 0 \qquad \tilde{\nu}_0\big((X^n V - (XZ)^n)^r\big) = r \cdot 0 = 0$$

$$\tilde{\nu}_X\big((X^n V - (XZ)^n)^r\big) = -rn$$

Since all other lifted essential valuations $\tilde{\nu}$ yield $\tilde{\nu}(f) \geq 0$, we get $f \in A[V]$. More precisely, this shows, that

$$B = \sum_{r \in \mathbb{N}} \frac{X^{rn}}{(X^n V - (XZ)^n)^r} A[V] \subseteq \operatorname{Frac}(F[V]).$$

Theorem 3.43. *For every abelian group G there is a Krull domain with an isomorphic class group.*

Proof. By Proposition 3.36 every free abelian group is the class group of a Krull domain. So in light of Proposition 3.41, it suffices to show that every abelian group is a homomorphic image of a free group. Now any given abelian group G can be realised as the image of the surjective homomorphism

$$\begin{aligned} \varphi_G \colon \mathbb{Z}^{(G)} &\to G \\ (n_g)_{g \in G} &\mapsto \sum_{g \in G} n_g g, \end{aligned}$$

whose domain is a free group. □

4 Class Groups of Dedekind Domains

In this Chapter, we will define Dedekind domains and explain their connection to Krull domains. Then we will proceed to construct, for a given Krull domain, a Dedekind domain with an isomorphic class group. Together with Theorem 3.43, this will prove the main Theorem of this thesis.

4.1 Dedekind Domains

Up until now, we have only really seen examples of Krull domains with a trivial class group in the form of unique factorisation domains, apart from our artificial construction. This is going to change, as with Dedekind domains we will obtain an important class of examples for Krull domains, for some of which it is easy to check, that they are not factorial. Additionally we will establish some basic properties of Dedekind domains, which are consequences of our Theory of Krull domains.

Definition 4.1 (Dedekind domains)**.**
A *Dedekind domain* is a Krull domain D such that every non-zero prime ideal is maximal.

Theorem 4.2. *For a domain D the following are equivalent:*

i) D is a Dedekind domain.

ii) D is a Krull domain and every non-zero prime ideal is of height 1.

iii) Every non-zero fractionary ideal of D is invertible.

iv) D is a Krull domain and every non-zero fractionary ideal is divisorial.

v) D is noetherian, every non-zero prime ideal $\mathfrak{p}$ of D is of height 1 and the localisation $D_{\mathfrak{p}}$ is a discrete valuation ring.

vi) D is a normal noetherian domain and every non-zero prime ideal is maximal.

Proof.

i) ⇔ ii) If every non-zero ideal is maximal, then no non-zero prime ideal can contain another one. Conversely, if none non-zero prime ideal contains another, then every non-zero prime ideal is bound to be maximal.

i) ⇒ iii) Let $\mathfrak{a} \subseteq \mathrm{Frac}(D)$ be a non-zero ideal of D. Then $\mathfrak{a}(D : \mathfrak{a}) \subseteq D$ is an integral ideal with $\overline{\mathfrak{a}(D : \mathfrak{a})} = D$, because $\mathtt{D}(D)$ is a group. But then $\mathfrak{a}(D : \mathfrak{a})$ must not be contained in any prime divisorial ideal, which by assumption are the maximal ideals. Thus $\mathfrak{a}(D : \mathfrak{a}) = D$ and so $\mathfrak{a}$ is invertible.

iii) ⇒ iv) We have seen in Lemma 2.10, that invertible ideals are divisorial and finitely generated. Hence $\mathtt{D}(D)$ is in fact a group, as every divisorial ideal is invertible, and D is noetherian, since every ideal is finitely generated. Therefore D is a Krull domain as a consequence of Proposition 3.3.

iv) ⇒ v) By Proposition 3.3, A satisfies the maximum condition for integral divisorial ideals. Since every ideal is divisorial, D satisfies the maximum condition for all integral ideals and thus is noetherian.

Furthermore, as any every non-zero ideal is divisorial, every non-zero prime ideal is divisorial and thus a prime divisorial ideal by Corollary 3.11. Now by Lemma 3.10, every prime divisorial ideal is of height 1.

Lastly, for every prime divisorial ideal $\mathfrak{p}$, i.e. non-zero prime ideal, we have $D_{\mathfrak{p}} = R_{\nu_{\mathfrak{p}}}$ is a discrete valuation ring by Lemma 3.12.

v) ⇒ vi) Since every non-zero prime ideal of D is of height 1, every non-zero prime ideal is maximal. Now, since every non-invertible $a \in D$ is element of some maximal ideal we have, that $D = \bigcap_{\mathfrak{p} \text{ maximal ideal}} D_{\mathfrak{p}}$ is an intersection of valuation rings. (Note that if $\langle 0 \rangle$ is maximal, D is a field and thus a valuation ring.) Now by Lemma 1.44 valuation rings are normal and by Lemma 1.35 their intersection D is normal.

vi) ⇒ i) By Corollary 3.5 normal noetherian domains are Krull domains. □

Remark 4.3. 4.2iii) and iv) shows, that for a Dedekind domain D, it is sufficient to consider the monoid of non-zero fractionary ideals $\mathtt{I}(D)$ to define the class group.

Corollary 4.4. *Every non-zero ideal of a Dedekind domain D has a unique factorisation into (possibly negative) powers of prime ideals up to permutation. For integral ideals these powers are always positive.*

Proof. This is an immediate consequence of $\mathtt{P}(D)$ being a basis of $\mathtt{D}(D) \overset{4.2iv)}{=} \mathtt{I}(D)$. □

Corollary 4.5. *A Dedekind domain D is a unique factorisation domain if and only if it is a principal ideal domain.*

Proof. By Theorem 3.19, D is a unique factorisation domain if and only if $\mathtt{Cl}(D) = 0$ which is the case if an only if $\mathtt{Prin}(D) = \mathtt{D}(D) \overset{4.2iv)}{=} \mathtt{I}(D)$. For the converse, recall from Corollary 1.20, that principal ideal domains are always unique factorisation domains. □

Corollary 4.6. *Any non-zero integral ideal $\mathfrak{a}$ of a Dedekind domain is generated by at most two elements.*

Proof. Let $a_0, a_1 \in D$ be an approximation of $\overline{\mathfrak{a}}$ by Corollary 3.39 of the Approximation Theorem. Then

$$\mathfrak{a} \overset{4.2iv)}{=} \overline{\mathfrak{a}} = \overline{\langle a_0, a_1 \rangle} \overset{4.2iv)}{=} \langle a_0, a_1 \rangle. \qquad \square$$

Example 4.7. The integers $\mathbb{Z}$ are a Krull domain for which every non-zero prime ideal is maximal. Thus $\mathbb{Z}$ is a Dedekind domain.

Now consider a finite field extension K over $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ and let D denote the integral closure of the integers $\mathbb{Z}$ in K. Then by Proposition 3.21 D is a Krull domain. Furthermore going-up and going-down Theorem ([AM69, p.61-64, Chapter 5, Theorem 5.11 and 5.16]) yield, that every non-zero prime ideal $\mathfrak{p}$ is of height 1, just like $\mathbb{Z} \cap \mathfrak{p}$. Note, that D is an integral extension of $\mathbb{Z}$ and that both domains are normal, because Krull domains are normal as a consequence of Corollary 1.32. In other words, D is a Dedekind domain.

What about the class group of D? Let us examine a specific example.

Example 4.8. Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-5})$. One can show that in this case, the Dedekind domain described above is

$$D = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C},$$

see for example [Mar77, p. 11, Chapter 2, Corollary 2 to Theorem 1].

Note, that the smallest (complex) absolute value of elements in D, that is not 0 or 1, is 4 and that the only elements with this absolute value are ± 2. So 2 must be irreducible, since the absolute value is multiplicative and the only non-zero elements with smaller absolute value are the units ± 1.

However, $\langle 2 \rangle \subsetneq \langle 2, 1 + \sqrt{-5} \rangle$ is not a maximal ideal and thus must not be prime, as every non-zero prime ideal of D is maximal. Note, that $\mathfrak{p} := \langle 2, 1 + \sqrt{-5} \rangle \neq D$ and that $\mathfrak{p}$ is in fact prime, since

$$\begin{aligned} D/\mathfrak{p} \cong \mathbb{Z}[X]/\langle X^2 + 5, 2, X + 1 \rangle &= \mathbb{Z}[X]/\langle X^2 + 5 - X(X+1), 2, X + 1 \rangle \\ &= \mathbb{Z}[X]/\langle 2, X + 1 \rangle \cong \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Therefore, 2 is irreducible but not prime and D must not be a unique factorisation domain by Lemma 1.19.

In fact, it can be shown that the size of the class group of the integers of a number field is always finite, see [Neu99, p. 36, Chapter I, §6, (6.3) Theorem], and the bound given in [Neu99, p. 36, Chapter I, §6, Exercise 3] yields, that the class group of our Dedekind domain has less then three elements. Since D is no unique factorisation domain by the above, $\mathtt{Cl}(D)$ must have precisely two elements. Hence, up to some isomorphism, the class group of our Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ is $\mathbb{Z}/2\mathbb{Z}$ with generator $\mathfrak{c}(\langle 2, 1 + \sqrt{-5} \rangle)$, because this prime ideal $\langle 2, 1 + \sqrt{-5} \rangle$ is not principal, as 2 is irreducible.

4.2 Class Groups

Dedekind domains seem rather outstanding among Krull domains, especially when considering their close connection to discrete valuation rings. One would hope, that this yields certain restrictions on their class group. However, for every Krull domain there is a Dedekind domain with an isomorphic class group, which we will construct. This indicates, that Dedekind domains might not be as exceptional among Krull domains as they seem.

Proposition 4.9. *For every Krull domain there is a Dedekind domain with isomorphic class group.*

Proof. For this proof we follow the proof of [Cla66, p.222, Theorem 7].

Let A be a Krull domain and consider the polynomial ring $A_{\mathbb{N}} := A[X_n \mid n \in \mathbb{N}]$. By Theorem 3.33 $\mathtt{Cl}(A) \cong \mathtt{Cl}(A_{\mathbb{N}})$. For every non-zero prime ideal $\mathfrak{q}$ that is not of height 1, choose some $0 \neq a \in \mathfrak{q}$ and

$$b \in \mathfrak{q} \setminus \bigcup_{\substack{\mathfrak{p} \in \mathrm{P}(A_{\mathbb{N}}) \\ \nu_{\mathfrak{p}}(a) > 0}} \mathfrak{p} \neq \emptyset$$

which exists by a contraposition of prime avoidance and is non-zero. Furthermore choose a variable not occurring in a or b and define $f_{\mathfrak{q}} := bX_{\mathfrak{q}} - a$. Now by construction $abA_{\mathbb{N}} = \sup\{aA_{\mathbb{N}}, bA_{\mathbb{N}}\} = aA_{\mathbb{N}} \cap bA_{\mathbb{N}}$ and this equality restricts to $A[X_i \mid i \in I_a \cup I_b]$, where I_a and I_b denote the sets of indices of variables occurring in a or b respectively. Therefore $f_{\mathfrak{q}} \in A[X_i \mid i \in I_a \cup I_b][X_{\mathfrak{q}}]$ is prime by Lemma 1.23. So Corollary 1.22 shows that $f_{\mathfrak{q}} \in A_{\mathbb{N}}$ is prime.

Now let S be the multiplicatively closed subset of $A_{\mathbb{N}}$ generated by the $f_{\mathfrak{q}}$ and define $D := S^{-1}A_{\mathbb{N}}$ as the localisation. As every prime ideal $\mathfrak{q}$ that is not of height 1 meets S non-trivially as $f_{\mathfrak{q}} \in S \cap \mathfrak{q}$, every non-zero prime ideal of D is of height 1. Thus D is a Dedekind domain. Moreover, by the second version of Nagata's Theorem

$$\mathtt{Cl}(D) = \mathtt{Cl}(S^{-1}A_{\mathbb{N}}) \cong \mathtt{Cl}(A_{\mathbb{N}}) \cong \mathtt{Cl}(A). \qquad \square$$

Theorem 4.10 (*Claborn*)**.**
For every abelian group G there is a Dedekind domain D such that $G \cong \mathtt{Cl}(D)$.

Proof. By Theorem 3.43 there is a Krull domain A such that $\mathtt{Cl}(A) \cong G$. Furthermore, by Proposition 4.9 there is a Dedekind domain D with

$$\mathtt{Cl}(D) \cong \mathtt{Cl}(A) \cong G. \qquad \square$$

4.3 Outlook

We have seen, that every abelian group occurs as the class group of a Dedekind domain. But what about the Dedekind domains, which occur in number theory? The Dedekind domains we constructed for arbitrary class groups are rather artificial as a localisation of a polynomial ring over a field in infinitely many variables. Yet, we have seen that not all integers of number fields are unique factorisation domains, so which class groups occur in this case? Clark has shown with tools from algebraic geometry in [Cla09], that every abelian group can be realised as the class group of the algebraic closure of a principal ideal domain in a separable field extension. Clearly, this construction is a lot closer to the number theoretic case.

Nevertheless, we know that the class group of the integers of a number field is countably generated, as we have seen in the sketch of the proof of Proposition 3.21, that these have at most countably many more essential valuations than $\mathbb{Z}$, which in turn has countably many essential valuations. As indicated before, a main result of number theory is that every class group of this kind is not only countably generated, but even finite, see [Neu99, p. 36, Chapter I, §6, (6.3) Theorem]. Still, these finite class groups behave rather unpredictable in both their size and structure, as described in [Neu99, p. 37, Chapter I, §6]. So let us restrict our question to finite class groups of a field extension of degree two.

Unfortunately, even in this restricted case, the answer to which finite abelian groups can or cannot occur as class groups is unknown to this day, as discussed in [hv]. At the very least, restricting even further to imaginary quadratic number fields yields some restrictions to the possible class groups. In this case, it is possible to find lower bounds for the size of the class group depending on the discriminant. Building up on that, some brute force calculations can show that certain abelian groups do not occur as the class group of the algebraic integers of an imaginary quadratic field extension. The smallest example of this phenomenon is $\left(\mathbb{Z}/3\mathbb{Z}\right)^3$. This and further examples are explored in [hb]. Nonetheless, not much is known about the possible class groups of the integers of number fields, even in this theoretically computable case.

References

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Comutative Algebra.* Addison-Wesely Publishing Company, Boston, 1969.

[Cla66] Luther Claborn. Every Abelian group is a class group. *Pac. J. Math.*, 18:219–222, 1966.

[Cla09] Pete L. Clark. Elliptic Dedekind domains revisited. *Enseign. Math. (2)*, 55(3-4):213–225, 2009.

[Fos73] Robert M. Fossum. *The divisor class group of a Krull domain.*, volume 74. Springer-Verlag, Berlin, 1973.

[hb] Dietrich Burde (https://mathoverflow.net/users/32332/dietrich burde). Why is $(\mathbb{Z}/3\mathbb{Z})^3$ not a class group of an imaginary quadratic number field ? MathOverflow. URL:https://mathoverflow.net/q/132838 (version: 2013-06-05). URL: `https://mathoverflow.net/q/132838`, `arXiv:https://mathoverflow.net/q/132838`.

[hv] Kevin Ventullo (https://math.stackexchange.com/users/546/kevin ventullo). Finite abelian groups as class groups. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/10949 (version: 2010-11-19). URL: `https://math.stackexchange.com/q/10949`, `arXiv:https://math.stackexchange.com/q/10949`.

[Mar77] Daniel A. Marcus. *Number Fields.* Springer-Verlag, New York, 1977.

[Nag62] Masayoshi Nagata. *Local Rings.* John Wiley & Sons, New York, London, 1962.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory.* Springer-Verlag, Berlin, 1999.

[Sam64] Pierre Samuel. *Lectures on Unique Factorisation Domains.* Tata Institute of Fundamental Research, Bombay, 1964.

[ZS58] Oscar Zariski and Pierre Samuel. *Commutative Algebra Volume I.* D. Van Nostrand Company, Princeton, 1958.

[ZS60] Oscar Zariski and Pierre Samuel. *Commutative Algebra Volume II.* D. Van Nostrand Company, Princeton, 1960.

Index