Kronecker's divisor theory and the generalization of notions and theorems of classical algebraic number theory to Krull domains

Friedemann Lucius

Georg-August-Universität Göttingen
Mathematisches Institut
Bunsenstraße 3–5
D-37073 Göttingen
e-mail: flucius@aol.com

Introduction

Introductions to algebraic number theory often regard the classical theory of algebraic number fields just as a special case of the theory of Dedekind domains. The level of abstraction can even be more increased by studying *Krull domains* instead of Dedekind domains. Rings of this type, also known as *rings with divisor theory*, still allow some sort of prime factorization, but in general, the corresponding system of prime divisors can no longer be made explicit by the system of prime ideals. It has become standard to describe the prime divisors of a Krull domain by its $\mathfrak{p}$-adic valuations, i. e. by its discrete rank one valuations. Thus, Krull domains are usually studied by means of valuation theory and local-global arguments. This methodical approach, however, has the disadvantage of being more abstract and less graphic than classical ideal theory. Compared to prime ideals discrete rank one valuations are indeed rather abstract algebraic objects. In addition, there is no natural definition of the norm of a divisor or the different of a Krull domain with respect to a finite field extension.

The intention of this paper is to present and propagate a methodical alternative devoid of these inconveniences, namely Kronecker's divisor theory. There have been several attempts to make Kronecker's methods popular, but most of the treatments on Kronecker's divisor theory lack of systematic approach. This may explain

why Kronecker's approach to algebraic number theory is little known and still lives in the shadow of ideal and valuation theory.

In [7] Kronecker's theory was analyzed in modern terms, i. e. by means of the theory of divisorial ideals, Kronecker function rings and Nagata domains. In the present paper we want to show how Kronecker's divisor theory can be used to transfer notions and well-known results from the theory of Dedekind domains to Krull domains thereby giving an alternative approach to the fundamentals of algebraic number theory.

If D is a Krull domain with field of fractions K, the corresponding Kronecker function ring D^v with respect to the v-operation is a principal ideal domain whose elements deliver a complete and (up to association) uniquely determined system of divisors for D in a most natural way. It is well-known that the group of fractional D^v-ideals is isomorphic to the Lorenzen v-group $\Lambda_v(D)$ of D, i. e. the group of fractional divisorial ideals of D. We will show that this isomorphism is given by extending divisorial D-ideals to D^v-ideals and by contracting D^v-ideals to D-ideals. Observing that the integral closure T of D in a finite field extension L/K is again a Krull domain and that the integral closure of D^v in the corresponding extension $L(X)/K(X)$ is given by the Kronecker function ring T^v, we define the norm of a divisor of T with respect to L/K in line with the usual norm with respect to $L(X)/K(X)$. Since the Kronecker function rings D^v resp. T^v are principal ideal domains, hence Dedekind domains, the same translation process can be applied to the definition of the residue class field, the ramification index, the inertial degree, the different, the discriminant etc. Consequently, many results on Dedekind domains such as the different and discriminant theorems can easily be transferred to Krull domains. Finally, we will show that the different of T^v over D^v is generated by an element different $\mathrm{diff}(F)$, $F \in T^v$, which implies that T^v is a simple extension ring of D^v with $T^v = D^v[F]$. From this we will explain, why, whith slight modifications, Kummer's method to factorize rational primes in an algebraic number field is also applicable to common inessential discriminant divisors.

The present paper generalizes several results already obtained by H. Flanders for Dedekind domains (cf. [2]). It is a contribution to an adequate assessment of Kronecker's method. The following passage quoted from the introduction of Flander's paper explains why Kronecker's approach to algebraic number theory deserves being carefully studied even today:

> In many situations it is extremely convenient, indeed almost imperative, to have a principal ideal ring instead of a Dedekind ring. The usual modern device for passing to this technically vastly simpler situation is to localize either by passing to p-adic completions or by forming the quotient ring with respect to the complement of a finite set of prime ideals. [*Kronecker's divisor* ...] theory has not generally been looked upon as a tool for accomplishing this reduction to principal ideals, [...]. In a certain sense it accomplishes the task much better than does localization because with localization the bulk of the structure of the ideal group is lost, whereas with forms [i. e. elements of the Kronecker function ring] this structure is preserved down to the finest detail. [2, 92]

1 Divisorial ideals, Kronecker divisors and the norm

We start this section with a short introduction to the theory of divisorial ideals and Kronecker divisors as outlined in [7]. If not otherwise stated, we always mean fractional ideals with respect to an integral domain when speaking of ideals.

Let D be a domain with quotient field K. If $\mathfrak{a}$ is a D-ideal and if $\mathfrak{a}^{-1}$ means the ideal quotient $(D:\mathfrak{a}) := \{\mu \in K : \mu\mathfrak{a} \subseteq D\}$, we call the fractional D-ideal $\mathfrak{a}_v := (\mathfrak{a}^{-1})^{-1}$ the *divisorial* or *v-ideal* corresponding to $\mathfrak{a}$. The map $\mathfrak{a} \mapsto \mathfrak{a}_v$ is referred to as the *v-operation* with respect to D. It induces the *t-operation*, which is given by

$$\mathfrak{a} \mapsto \mathfrak{a}_t := \bigcap_{\substack{\mathfrak{e}\ \text{f. g.}\\ \mathfrak{e}\subseteq\mathfrak{a}}} \mathfrak{e}_v,$$

where the abbreviation "f. g." stands for "finitely generated D-ideal". The v-operation is said to be *of finite type* if it coincides with the t-operation. Note that v- and t-operation mean the same when restricted to the set of finitely generated D-ideals. If $\mathfrak{a} = \mathfrak{a}_v$, the D-ideal $\mathfrak{a}$ is called *divisorial* or *v-ideal*; if $\mathfrak{a} = \mathfrak{a}_t$, it is called *t-ideal*. In the next paragraph the symbol "$*$" is used to denote both the v- and the t-operation on D.

A $*$-ideal $\mathfrak{a}$ is *$*$-finite* if there is a finitely generated D-ideal $\mathfrak{b}$ with $\mathfrak{a} = \mathfrak{b}_*$. If this ideal $\mathfrak{b}$ is generated by $a_1, \ldots, a_m \in \mathfrak{b}$, we also write $\mathfrak{a} = \mathfrak{a}_* = (a_1, \ldots, a_m)_*$ and refer to $a_1, \ldots, a_m$ as the *$*$-generating system* of $\mathfrak{a}$. The fractional $*$-ideals of D form a partially ordered semigroup by the so-called *$*$-multiplication* "$\times$". It is defined by $\mathfrak{a}_*\times\mathfrak{b}_* := (\mathfrak{a}'\cdot\mathfrak{b}')_*$, where $\mathfrak{a}', \mathfrak{b}'$ denote fractional D-ideals with $\mathfrak{a}'_* = \mathfrak{a}_*$ and $\mathfrak{b}'_* = \mathfrak{b}_*$. The meaning of *$*$-divisibility* and *$*$-invertibility* is obvious. Note that, in general, the v-inverse of a v-invertible v-ideal $\mathfrak{a}$ is not v-finite, even if $\mathfrak{a}$ is v-finite. The t-inverse of a t-invertible t-ideal, however, is always t-finite.

If $f(X) = a_0 + a_1X + \ldots + a_mX^m$ is a polynomial in $K[X]$, the v-ideal

$$\mathrm{c}(f)_v := (a_1, \ldots, a_m)_v$$

is called the *v-content* of f. If $\mathrm{c}(f)_v = D$, f is called *v-primitive*. The set of v-primitive polynomials is denoted by $N_v(D)$. The v-content is said to be *multiplicative* if $\mathrm{c}(f\cdot g)_v = \mathrm{c}(f)_v\times\mathrm{c}(g)_v$ for all $f, g \in K[X]$. The v-content is multiplicative if and only if D is integrally closed. If the v-finite v-ideals of D are v-invertible, the v-content function $\mathrm{c}(\cdot)_v$ can be extended from polynomials to rational functions over K by $\mathrm{c}(f)_v := \mathrm{c}(f_1)_v\times\mathrm{c}(f_2)_v^{-1}$ for all $f := \frac{f_1}{f_2}$, $f_1, f_2 \in D[X]$.

If the v-finite v-ideals of D are v-cancellative with respect to the v-multiplication, which is shown to be equivalent to the v-finite v-ideals being v-invertible, D is called a *v-domain*. The quotient group $\Lambda_v(D)$ of all integral v-finite v-ideals is referred to as the *Lorenzen v-group* of D; $\Lambda_v^+(D)$ denotes the semigroup of all integral v-ideals in $\Lambda_v(D)$. If D is a v-domain, the set

$$D^v := \left\{\frac{f}{g} : f, g \in D[X] \text{ with } \mathrm{c}(f)_v \subseteq \mathrm{c}(g)_v\right\}$$

of rational functions over K becomes an integral domain, the *Kronecker function ring* of D with respect to the v-operation. Any D^v-ideal generated by finitely many rational

functions $\frac{f_1}{g}, \ldots, \frac{f_m}{g}$, $f_i, g \in D[X]$, is a principal ideal of the form $\frac{f}{g}D^v$, where $f(X) = f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m}$ denotes a polynomial in which the exponents r_i are such that in the representation of f no monomials of equal degree occur. This shows that D^v is actually a Bezout domain. It is easy to see that $D^v \cap K = D$. With $\Lambda(D^v)$ (resp. $\Lambda^+(D^v)$) denoting the Lorenzen (semi)group of D^v, i. e. the (semi)group of all (integral) finitely generated, hence principal D^v-ideals, we get the isomorphisms of gcd-(semi)groups $\Lambda_v(D) \cong \Lambda(D^v)$ resp. $\Lambda_v^+(D) \cong \Lambda^+(D^v)$.

If the v-finite v-ideals of D even form a group by v-multiplication, i. e. if the v-inverse of any v-finite v-ideal is v-finite again, D is called *Prüfer v-multiplication domain* (PVMD). In this case, the Kronecker function ring D^v is equal to the quotient ring of $D[X]$ with respect to the multiplicatively closed set $N_v(D)$ of v-primitive polynomials

$$D_v(X) = D[X]_{N_v(D)} = \left\{ \frac{f}{g} : f \in D[X], g \in N_v(D) \right\}.$$

We call $D_v(X)$ the *Nagata domain* of D with respect to the v-operation.

If D is a Prüfer v-multiplication domain in which every v-ideal is v-finite, D is shown to be a Krull domain (and vice versa). Observing that the v-finiteness condition means that v-operation and t-operation coincide, we obtain ideal theoretic characterizations of a Krull domain which are analogue to those of a Dedekind domain. To be precise, D is a Krull domain if and only if any of the following conditions holds: (1) The fractional t-ideals form a group by t-multiplication. (2) Any t-ideal can be uniquely written as the t-product of finitely many prime t-ideals. (3) D is integrally closed, every ascending chain of t-ideals becomes stable (*t-noetherian property*) and any prime t-ideal is maximal in the set of all t-ideals.

We recall that a Krull domain is nothing else than a *ring with divisor theory*, i. e. a domain together with a factorial semigroup $\mathfrak{D}^+$ and a homomorphism $(\cdot) : D^* \to \mathfrak{D}^+$ such that the following conditions hold:
(D 1) $a \mid b$ with respect to $D \Leftrightarrow (a) \mid (b)$ with respect to $\mathfrak{D}^+$.
(D 2) $\{d \in K : \mathfrak{a} \mid (d)\} = \{d \in K : \mathfrak{b} \mid (d)\} \Leftrightarrow \mathfrak{a} = \mathfrak{b}$ for all $\mathfrak{a}, \mathfrak{b} \in \mathfrak{D}^+$.
According to this defintion the second ideal theoretic criterion for Krull domains cited above says that an adequate system of divisors is given by the factorial group of t-ideals, i. e. by the Lorenzen v-group $\Lambda_v(D)$. Up to isomorphism, there is no other divisor theory for D than the homomorphism $(\cdot)_v : D^* \to \Lambda_v^+(D)$ with $a \mapsto (a)_v = aD$.

An alternative to make the divisor theory for D explicit is given by the Kronecker function ring D^v of D with respect to the v-operation. It is well-known that D is a Krull domain if and only if its corresponding Nagata domain $D_v(X)$ is a principal ideal domain. Since $D_v(X) = D^v$ in this case, the order preserving isomorphism $\Lambda_v(D) \cong \Lambda(D^v)$ becomes an isomorphism of factorial groups. Thus, $[\,\cdot\,]_v : D^* \to \Lambda^+(D^v)$ with $a \mapsto [\,a\,]_v := aD^v$ defines another divisor theory for D. It is called *Kronecker's divisor theory* for D. The elements of D^v are referred to as *integral Kronecker divisors*, the elements in $K(X)$ as *fractional Kronecker divisors*. Since any element in D^v is associated to a polynomial over K, we can think of Kronecker divisors as polynomials. Note that

with respect to D^v every polynomial in $K[X]$ can be interpreted as a greatest common divisor of its coefficients.

If T is the integral closure of a Krull domain D in the finite field extension L/K, then T is again a Krull domain whose Kroencker function ring T^v is the integral closure of D^v in the finite field extension $L(X)/K(X)$. Thus, the equalities

$$T^v = T_v(X) = T[X]_{N_v(T)} = T[X]_{N_v(D)}$$

hold. Since the elements of D^v are contained in T^v, Kronecker divisors for D can be regarded as Kronecker divisors for T in a most natural way.

In regard to v-ideal divisors it is well-known that $\mathfrak{d}_v = (\mathfrak{d}T)_v \cap K$ for all D-ideals $\mathfrak{d}$ (cf. [5, Satz 9]). This, however, implies that nothing is lost when we lift v-ideals of D to v-ideals of T. Thus, we may identify the v-ideals of D with the v-ideals they generate in T. Note that, in particular, the gcd-property of a Kronecker resp. v-ideal divisor remains untouched when passing on from one algebraic extension field to another. Informally speaking, "gcd in D stays gcd in T".

Since the algebraic structure of the field extension $L(X)/K(X)$ mimicks that of L/K, we have $[L(X) : K(X)] = [L : K] = m$. In particular, the degrees of separability s and inseparability i are the same. Since every conjugation map over K is equal to the restriction of a conjugation map over $K(X)$, we will denote the K-monomorphisms from L into the normal closure of L/K resp. the $K(X)$-monomorphism from $L(X)$ into the normal closure of $L(X)/K(X)$ uniformly by $\sigma_1, \ldots, \sigma_s$. For the norm function of L/K resp. $L(X)/K(X)$, which is given by $\prod_{k=1}^{s} \sigma_k(\cdot)^i$, we will always use the abbreviated notation $N_{L/K}$, even when applied to $L(X)$.

According to this definition the meaning of the norm of a Kronecker divisor is obvious, at least if it is referred to as an element of $L(X)$. For an element of $\Lambda(T^v)$, i. e. for a principal ideal of the form FT^v, $F \in L(X)$, we define $N_{L/K}(FT^v) := N_{L/K}(F)D^v$. Since the map $\Lambda(T^v) \to \Lambda_v(T)$ with $FT^v \mapsto \mathrm{c}(F)_v$ is a well-defined isomorphism and since any v-ideal of T can be written as the v-content of a polynomial with coefficients in L, this definition induces a well-defined norm function for v-ideal divisors of T by

$$N_{L/K}^{(v)}(\mathfrak{A}) := \mathrm{c}(N_{L/K}(F))_v \quad \text{for all } \mathfrak{A} \in \Lambda_v(T),\ F \in L(X) \text{ with } \mathfrak{A} = \mathrm{c}(F)_v.$$

It is called the *v-ideal norm* or just *v-norm* with respect to L/K. Note that per definitionem the v-norm of a v-ideal of T gives a v-ideal of D.

Proposition 1.1. *Let L/K be an algebraic field extension with degree of separability s and degree of inseparability i. Let further $\mathfrak{A} = \mathfrak{A}_v$ be a v-ideal of T. If $\sigma_k(\mathfrak{A})_v$, $1 \leqslant k \leqslant s$, is the v-ideal generated by $\sigma_k(\mathfrak{A})$ in the normal closure of L/K, we get*

$$N_{L/K}^{(v)}(\mathfrak{A}) = \sigma_1(\mathfrak{A})_v^i \times \ldots \times \sigma_s(\mathfrak{A})_v^i \cap K.$$

Thus, if L/K is a separable finite extension, the v-norm of a v-ideal is just the v-product of its conjugates.

Proof: It has already been mentioned that in case of an arbitary algebraic field extension L/K the equality $\mathfrak{d}_v = (\mathfrak{d}T)_v \cap K$ holds for any D-ideal $\mathfrak{d}$. This, however, implies that nothing is lost when we lift v-ideals in L to v-ideals in the normal closure

of L/K. Thus, we may assume without loss of generality that the finite extension L/K is normal. Let $F \in L[X]$ be a polynomial with v-content $\mathfrak{A}$. Per definitionem, $N^{(v)}_{L/K}(\mathfrak{A}) = \mathrm{c}(N_{L/K}(F))_v$. In addition, we obtain

$$\sigma_k(\mathfrak{A})_v = \sigma_k(\mathfrak{A}) = \sigma_k\big(\mathrm{c}(F)_v\big) = \mathrm{c}\big(\sigma_k(F)\big)_v \quad \text{for } 1 \leqslant k \leqslant s$$

since L/K is normal. Observing that the v-content in an integrally closed domain is always multiplicative we obtain

$$\begin{aligned} N^{(v)}_{L/K}(\mathfrak{A}) &= \mathrm{c}\big(\sigma_1(F)^i \cdot \ldots \cdot \sigma_s(F)^i\big)_v \\ &= \mathrm{c}(\sigma_1(F))^i_v \times \ldots \times \mathrm{c}(\sigma_m(F))^i_v \cap K \\ &= \sigma_1(\mathrm{c}(F)_v)^i \times \ldots \times \sigma_m(\mathrm{c}(F)_v)^i \cap K \\ &= \sigma_1(\mathfrak{A})^i \times \ldots \times \sigma_m(\mathfrak{A})^i \cap K. \end{aligned}$$

□

Proposition 1.2. *Let $F \in L(X)$ be a Kronecker divisor with v-content $\mathfrak{A} = \mathfrak{A}_v$. If "$\sim$" means "is associated to", we have*

$$N_{L/K}(F) \sim \gcd\big(\{N_{L/K}(\alpha)\}_{\alpha \in L,\ F \mid \alpha}\big).$$

In terms of v-ideals we obtain

$$N^{(v)}_{L/K}(\mathfrak{A}) = \big(\{N_{L/K}(\alpha)\}_{\alpha \in \mathfrak{A}}\big)_v.$$

Proof: Making the divisor group of T explicit by the Lorenzen v-group we have $\gcd(\{\alpha_i\}_{i\in I}) = (\{\alpha_i\}_{i\in I})_v$ for any family $\{\alpha_i\}_{i\in I}$ of elements in L (cf. [7, Satz 2.6]). Because of the definition of the v-norm it is therefore sufficient to prove the statement for Kronecker divisors. Obviously, $N_{L/K}(F) \mid N_{L/K}(\alpha)$ for all $\alpha \in L$ with $F \mid \alpha$. Thus, it remains to show $\gcd\big(\{N_{L/K}(\alpha)\}_{\alpha\in L, F\mid\alpha}\big) \mid N_{L/K}(F)$. Let $p \in D^v$ be a Kronecker divisor prime in D^v. Since T is a Krull domain, there exists a Kronecker divisor $G_p \in T^v$ with $\gcd(p, G_p) \sim 1$ in T^v and $F \cdot G_p = \alpha_p \in T$ (cf. [7, Satz 3.1, (G 2.4)]). The condition $\gcd(p, G_p) \sim 1$ in T^v implies that the corresponding norms are relatively prime in D^v, hence $\gcd\big(p, N_{L/K}(G_p)\big) \sim 1$ in D^v. With $v_p(\cdot)$ denoting the p-exponent of a Kronecker divisor we obtain

$$\begin{aligned} v_p\big(N_{L/K}(\alpha_p)\big) &= v_p\big(N_{L/K}(F) \cdot N_{L/K}(G_p)\big) \\ &= v_p\big(N_{L/K}(F)\big) + v_p\big(N_{L/K}(G_p)\big) \\ &= v_p\big(N_{L/K}(F)\big). \end{aligned}$$

Since $\min\big\{v_p\big(N_{L/K}(\alpha)\big)\colon \alpha \in L,\ F \mid \alpha\big\} \leq v_p\big(N_{L/K}(\alpha_p)\big) = v_p\big(N_{L/K}(F)\big)$ for all prime Kronecker divisors $p \in D^v$, it follows that

$$\gcd\big(\{N_{L/K}(\alpha)\}_{\alpha\in L,\ F\mid\alpha}\big) = \prod_{p \in D^v \text{ prime}} p^{\min\left\{v_p\left(N_{L/K}(\alpha)\right)\colon\, \alpha \in L,\ F \mid \alpha\right\}}$$

divides $N_{L/K}(F)$. □

We want to end this section by proving that in the case of a Krull domain D the ismorphism $\Lambda_v(D) \cong \Lambda(D^v)$ is given by extending divisorial D-ideals to principal D^v-ideals and by contracting principal D^v-ideals to divisorial D-ideals. This follows immediately from

Lemma 1.3. *Let D be a v-domain in which the v-operation is of finite type. Then $\mathfrak{a}D^v = \mathfrak{a}_v D^v$ for all D-ideals $\mathfrak{a}$. In particular, $fD^v = \mathrm{c}(f)_v D^v$ for all $f \in K[X]$.*

Proof: Due to $\mathfrak{a} \subseteq \mathfrak{a}_v$ the inclusion $\mathfrak{a}D^v \subseteq \mathfrak{a}_v D^v$ is trivial. Let $\alpha \in \mathfrak{a}_v D^v$. There are $\alpha_1, \ldots, \alpha_m \in \mathfrak{a}_v$ and $f_1, \ldots, f_m \in D^v$ such that $\alpha = \alpha_1 f_1 + \ldots + \alpha_m f_m$. Since the v-operation is of finite type, for every α_i there is a finitely generated D-ideal $\mathfrak{a}^{(i)}$ with $\mathfrak{a}^{(i)} \subseteq \mathfrak{a}$ and $\alpha_i \in \mathfrak{a}_v^{(i)}$. Let $\mathfrak{b}$ be the D-ideal generated by $\mathfrak{a}^{(1)}, \ldots, \mathfrak{a}^{(m)}$. Then, we have $\mathfrak{b} \subseteq \mathfrak{a}$ and $\alpha_i \in \mathfrak{b}_v$ for $1 \leqslant i \leqslant m$. Since $\mathfrak{b}$ is finitely generated, there is a polynomial $f \in K[X]$ whose coefficients generate $\mathfrak{b}$. This implies $\alpha_i \in \mathrm{c}(f)_v$, hence $f \mid \alpha_i$ with respect to D^v. Thus, $f \mid \alpha$, i. e. $\alpha \in fD^v = \mathfrak{b}D^v \subseteq \mathfrak{a}D^v$. □

Theorem 1.4. *Let D be a Krull domain with field of fractions K and T the integral closure of D in the finite field extension L/K. Then the following diagrams are commutative with the horizontal maps being inverse isomorphisms:*

$$\begin{array}{ccc} \Lambda_v(T) & \underset{\cap L}{\overset{\cdot T^v}{\rightleftarrows}} & \Lambda(T^v) \\ {\scriptstyle N_{L/K}^{(v)}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ \Lambda_v(D) & \underset{\cap K}{\overset{\cdot D^v}{\rightleftarrows}} & \Lambda(D^v) \end{array} \qquad \begin{array}{ccc} \Lambda_v(T) & \underset{\cap L}{\overset{\cdot T^v}{\rightleftarrows}} & \Lambda(T^v) \\ {\scriptstyle \cap K}\downarrow & & \downarrow{\scriptstyle \cap K(X)} \\ \Lambda_v(D) & \underset{\cap K}{\overset{\cdot D^v}{\rightleftarrows}} & \Lambda(D^v) \end{array}$$

Proof: Since D and T are Krull domains, the corresponding Kronecker function rings D^v and T^v are principal ideal domains and all divisorial ideals of D resp. T are v-finite. The map $\Lambda(D^v) \to \Lambda_v(D)$, $fD^v \mapsto \mathrm{c}(f)_v$, is known to be a well-defined isomorphism with inverse map $\mathfrak{a}_v \mapsto \mathfrak{b}D^v$, where $\mathfrak{b}$ is a finitely generated D-ideal with $\mathfrak{a}_v = \mathfrak{b}_v$. Since $\mathrm{c}(f)_v = fD^v \cap K$ for all $f \in K[X]$, the isomorphism $fD^v \mapsto \mathrm{c}(f)_v$ is actually given by contracting D^v-ideals to divisorial D-ideals. Vice versa, the isomorphism $\mathfrak{a}_v \mapsto \mathfrak{a}D^v$ is given by extending divisorial D-ideals to D^v-ideals because $\mathfrak{a}D^v = \mathfrak{a}_v D^v$ according to Lemma 1.3. By definition of the v-norm the first diagram is obviously commutative. Let $F \in L[X]$ be a Kronecker divisor of T and $\mathfrak{A}$ the corresponding v-ideal of T such that $\mathfrak{A} = \mathrm{c}(F)_v = FT^v \cap L$ resp. $\mathfrak{A}T^v = FT^v$. Since the contracted ideal $FT^v \cap K(X)$ is a principal D^v-ideal, there is an $f \in K[X]$ with $fD^v = FT^v \cap K(X)$. The corresponding v-ideal of D is given by $fD^v \cap K = \mathrm{c}(f)_v$, and we obtain $FT^v \cap K = FT^v \cap L \cap K = \mathfrak{A} \cap K = \mathrm{c}(f)_v$. This proves that the contraction of a divisorial T-ideal gives a divisorial D-ideal. This means that the map $\Lambda_v(T) \overset{\cap K}{\longrightarrow} \Lambda_v(D)$ is defined and that the second diagram is commutative. □

For the reader familiar with the theory of $*$-operations and $*$-ideals it is a well-known fact that the following conditions are equivalent for a $*$-operation $(\cdot)_*$ of finite type which is *endlich arithmetisch brauchbar*, i. e. for which the Kronecker function ring $D^{(*)}$ resp. the Lorenzen $*$-group is defined: (1) The $*$-finite $*$-ideals form a group by $*$-multiplication. (2) The map $\mathfrak{a}_* \mapsto \mathfrak{a}_* D^{(*)}$ from the semigroup of $*$-ideals of D to the semigroup of $D^{(*)}$-ideals is an isomorphism (cf. [4, II, § 3.1, Théorème 3]). In addition, it is easy to prove the $*$-theoretic analogue to Lemma 1.3, which says that $\mathfrak{a}_* D^{(*)} \cap K = \mathfrak{a}_*$ for any $*$-ideal $\mathfrak{a}_*$ of D if the $*$-finite $*$-ideals are $*$-invertible. If any of

the conditions (1) or (2) hold it can be deduced that the inversve map of $\mathfrak{a}_* \mapsto \mathfrak{a}_* D^{(*)}$ is given by contracting $D^{(*)}$-ideals to $*$-ideals of D. Translating this general result to Krull domains we get an alternative proof of Theorem 1.4.

Notation: To make the reading of this paper easier we will use the following standard of notation: Elements in K are denoted by small Latin letters $(a, b, c, \dots)$, elements in the algebraic extension field L by small Greek letters $(\alpha, \beta, \gamma, \dots)$. D-ideals are denoted by small, T-ideals by capital German letters $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$ resp. $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots)$. Kronecker divisors of D, i. e. elements of the function field $K(X)$, are denoted by small, Kronecker divisors of T by capital Latin letters $(f, g, h, \dots$ resp. $F, G, H, \dots)$. v-Ideals and Kronecker divisors that correspond to each other according to Theorem 1.4 are denoted by corresponding letters: $\mathfrak{a}_v \leftrightarrow f$, i. e. $\mathfrak{a}_v = \mathrm{c}(f)_v$, $\mathfrak{b}_v \leftrightarrow g$, $\dots$ resp. $\mathfrak{A}_v \leftrightarrow F$, $\mathfrak{B}_v \leftrightarrow G$, $\dots$. For D- resp. T-ideals extended to $D_v(X)$ resp. $T_v(X)$ we will also write $\mathfrak{a}_v(X), \mathfrak{b}_v(X), \dots$ resp. $\mathfrak{A}_v(X), \mathfrak{B}_v(X), \dots$, i. e. we will set $\mathfrak{a}_v(X) := \mathfrak{a}_v D^v = \mathfrak{a}_v D_v(X)$ etc. $\mathfrak{a}_v[X], \mathfrak{b}_v[X], \dots$ resp. $\mathfrak{A}_v[X], \mathfrak{b}_v[X]$ denote the set of polynomials in the indeterminate X with coefficients in $\mathfrak{a}_v, \mathfrak{b}_v, \dots$ resp. $\mathfrak{A}_v, \mathfrak{B}_v, \dots$, i. e. we will set $\mathfrak{a}_v[X] := \mathfrak{a}_v D[X]$ etc. Prime ideals or prime Kronecker divisors are denoted by the letter p in its adequate form $(\mathfrak{p}, \mathfrak{P}$ resp. $p, P)$. If not otherwise stated, all ideals in this paper are v-ideals so that the index letter v will usually be omitted.

2 Residue class fields, inertia degree and ramifaction index

Let D be a Krull domain with field of fractions K and $\mathfrak{a} = \mathfrak{a}_v \in \Lambda_v^+(D)$ an integral v-ideal of D that is not v-primitive. Extending the canonical epimorphism $D \to D/\mathfrak{a}$ to the ring of polynomials over D in the indeterminate X we obtain

$$\begin{aligned} \varphi_{\mathfrak{a}} : \quad D[X] \quad &\longrightarrow \quad D/\mathfrak{a}\,[X] \\ a_0 + a_1 X + \ldots + a_m X^m &\longmapsto \overline{a_0} + \overline{a_1} X + \ldots + \overline{a_m} X^m, \end{aligned} \tag{2.1}$$

where the bar stands for taking the residue modulo $\mathfrak{a}$, i. e. $\overline{a_i} := a_i \bmod \mathfrak{a}$. We are interested in the image of the set of v-primitive polynomials over D.

Proposition 2.2. *The canonical epimorphism $\varphi_{\mathfrak{a}} : D[X] \to D/\mathfrak{a}\,[X]$ of (2.1) maps the v-primitive polynomials of D to the non-zero divisors of $D/\mathfrak{a}\,[X]$. To be precise,*

$$\varphi_{\mathfrak{a}}\big(N_v(D)\big) = \big\{\varphi_{\mathfrak{a}}(f) : f \in D[X]^*;\ fg \in \mathfrak{a}(X) \text{ for } g \in D[X] \Leftrightarrow g \in \mathfrak{a}(X)\big\}.$$

Proof: "$\subseteq$" Let $g \in N_v(D)$ and $h \in D[X]$ be polynomials over D with $\varphi_{\mathfrak{a}}(g) \cdot \varphi_{\mathfrak{a}}(h) = \overline{0}$, i. e. $gh \in \mathfrak{a}[X]$. Since $\mathrm{c}(g)_v = D$, it follows $\mathrm{c}(h)_v = \mathrm{c}(g)_v \times \mathrm{c}(h)_v = \mathrm{c}(gh)_v \subseteq \mathfrak{a}$. This, however, means $h \in \mathfrak{a}[X]$, hence $\varphi_{\mathfrak{a}}(h) = \overline{0}$, which proves that $\varphi_{\mathfrak{a}}(g)$ is a non-zero divisor in $D/\mathfrak{a}\,[X]$.

"$\supseteq$" Let $\varphi_{\mathfrak{a}}(h)$ be a non-zero divisor of $D/\mathfrak{a}\,[X]$. First, we prove that the v-ideal generated by $\mathfrak{a}$ and the v-content of h is the unit ideal, i. e. $(\mathrm{c}(h)_v, \mathfrak{a})_v = D$. Assume that $(\mathrm{c}(h)_v, \mathfrak{a})_v \subsetneqq D$. By the v-invertiblity of any v-ideal in D, there is a fractional v-ideal $\mathfrak{b} = \mathfrak{b}_v$ with $D \subsetneqq \mathfrak{b}_v$ such that $\mathfrak{b}_v \times (\mathrm{c}(h)_v, \mathfrak{a})_v = D$. This implies $(\mathfrak{a}_v \times \mathfrak{b}_v) \times (\mathrm{c}(h)_v, \mathfrak{a})_v = \mathfrak{a}_v$ with $\mathfrak{a}_v \times \mathfrak{b}_v \supsetneqq \mathfrak{a}_v$. Since every v-ideal in a Krull domain is

v-finite, there is a polynomial $f \in K[X]$ with v-content $\mathfrak{a}_v \times \mathfrak{b}_v$. It follows

$$\mathrm{c}(f)_v \times (\mathrm{c}(h)_v, \mathfrak{a})_v = (\mathrm{c}(f \cdot h)_v, \mathfrak{a} \cdot \mathrm{c}(f)_v)_v = \mathfrak{a}_v = \mathfrak{a},$$

hence $fh \in \mathfrak{a}[X]$. Since $f, h \notin \mathfrak{a}[X]$, we obtain $\varphi_\mathfrak{a}(f) \cdot \varphi_\mathfrak{a}(h) = \overline{0}$ with $\varphi_\mathfrak{a}(f), \varphi_\mathfrak{a}(h) \neq \overline{0}$. This shows that $\varphi_\mathfrak{a}(f)$ is a zero divisor in $D/\mathfrak{a}\,[X]$, which contradicts our assumption. Thus, $(\mathrm{c}(h)_v, \mathfrak{a})_v = D$. Recalling that any v-ideal in a Krull domain can be v-generated by two elements we conclude that there must be elements $a, b \in \mathfrak{a}$ such that $(\mathrm{c}(h)_v, a, b)_v = D$. Let $g = h + aX^m + bX^{m+1}$ with $m := 1 + \deg h$. Then g is v-primitive, and from $g - h = aX^m + bX^{m+1} \in \mathfrak{a}[X]$ we get $\varphi_\mathfrak{a}(g) - \varphi_\mathfrak{a}(h) = \overline{0}$. Thus, $\varphi_\mathfrak{a}(g) = \varphi_\mathfrak{a}(h)$, which proves that there is a v-primitive polynomial that is mapped onto the non-zero divisor $\varphi_\mathfrak{a}(h)$. □

Proposition 2.3. *Let D be a Krull domain and $\mathfrak{a} = \mathfrak{a}_v$ a v-ideal which is not v-primitive. Writing $D/\mathfrak{a}\,[X]_{\varphi_\mathfrak{a}(N_v(D))}$ for the quotient ring of $D/\mathfrak{a}\,[X]$ with respect to the multiplicative set of non-zero divisors $\varphi_\mathfrak{a}\,(N_v(D))$, we have the isomorphisms*

$$D_v(X)/\mathfrak{a}(X) \cong D[X]_{N_v(D)}/\mathfrak{a}D[X]_{N_v(D)} \cong D/\mathfrak{a}\,[X]_{\varphi_\mathfrak{a}(N_v(D))}.$$

Proof: We prove that the well-defined epimorphism

$$\begin{aligned} \widetilde{\varphi}_\mathfrak{a} : D[X]_{N_v(D)} &\longrightarrow D/\mathfrak{a}\,[X]_{\varphi_\mathfrak{a}(N_v(D))} \\ \frac{f}{g} &\longmapsto \varphi_\mathfrak{a}(f) \cdot \varphi_\mathfrak{a}(g)^{-1}, \qquad f \in D[X],\, g \in N_v(D) \end{aligned}$$

has kernel $\mathfrak{a}(X) = \mathfrak{a}D[X]_{N_v(D)}$. Let $h = \frac{f}{g}$, $f \in D[X]$, $g \in N_v(D)$, be a Kronecker divisor of D. Since $\varphi_\mathfrak{a}(g) \neq \overline{0}$, we have

$$\widetilde{\varphi}_\mathfrak{a}(h) = \overline{0} \quad \Leftrightarrow \quad \varphi_\mathfrak{a}(f) = \overline{0} \quad \Leftrightarrow \quad f \in \mathfrak{a}[X] \quad \Leftrightarrow \quad h \in \mathfrak{a}D[X]_{N_v(D)}. \qquad \square$$

Let $\mathfrak{p}$ be a prime v-ideal of D and p the corresponding Kronecker divisor, i. e. an element of $K(X)$ with $\mathrm{c}(p)_v = \mathfrak{p}$. Note that $\mathfrak{p}$ need not be a maximal D-ideal and consequently the residue class ring of D modulo $\mathfrak{p}$, which is an integral domain, need not be a field. We call the quotient field of $D/\mathfrak{p}$ the *residue class field* of D with respect to $\mathfrak{p}$. It is denoted by $K_\mathfrak{p}$. This terminology is obviously compatible with the one developed for Dedekind domains. Passing on to the Kronecker function ring $D^v = D_v(X) = D[X]_{N_v(D)}$ of D the situation becomes even simpler and clearer. According to Theorem 1.4 the extended $D_v(X)$-ideal $\mathfrak{p}D_v(X) = \mathfrak{p}(X) = pD_v(X)$ gives a prime Kronecker divisor of D. Since principal prime ideals are maximal, the residue class ring $D_v(X)/pD_v(X)$ actually is a field, namely the *residue class field* of $D_v(X)$ with respect to p, denoted by $K(X)_p$.

Theorem 2.4. *Let D be a Krull domain with quotient field K and T the integral closure of D in a finite field extension L/K. Let p be a prime Kronecker divisor of D with v-content $\mathfrak{p}$ and P a prime Kronecker divisor of T with v-content $\mathfrak{P}$, such that $P \mid p$ in $T_v(X)$, i. e. $\mathfrak{P} \cap K = \mathfrak{p}$. Then*

(1) *$K_\mathfrak{p}(X) \cong K(X)_p$ and $L_\mathfrak{P}(X) \cong L(X)_P$.*

(2) *$[L_\mathfrak{P} : K_\mathfrak{p}] = [L(X)_P : K(X)_p] \leqslant L/K$.*

Proof: Ad (1) Since $D/\mathfrak{p}$ is an integral domain, the corresponding polynomial ring $D/\mathfrak{p}\,[X]$ is an integral domain as well. Thus, $D/\mathfrak{p}\,[X]$ contains no zero divisors, which implies $\varphi_{\mathfrak{p}}\,(N_v(D)) = D/\mathfrak{p}\,[X]$ according to Proposition 2.2. Therefore,

$$D/\mathfrak{p}\,[X]_{\varphi_{\mathfrak{p}}\,(N_v(D))} = \mathrm{Quot}\big(D/\mathfrak{p}\,[X]\big) = \mathrm{Quot}(D/\mathfrak{p})(X) = K_{\mathfrak{p}}(X).$$

The isomorphism now follows from Proposition 2.3.

Ad (2) By (1) the equality $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = [L(X)_P : K(X)_p]$ is obvious. It is well-known that $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] \leqslant [L : K]$ holds if D and T are Dedekind domains. Since $D_v(X)$ and $T_v(X)$ are even principal ideal domains we get $[L(X)_P : K(X)_p] \leqslant [L(X) : K(X)] = [L : K]$. □

In line with the usual terminology the *inertia degree* of the prime Kronecker divisor P with respect to L/K, i. e. the degree $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = [L(X)_P : K(X)_p]$, is denoted by $f_{L/K}(P)$. For the ramifaction index of P with respect to L/K we will write $e_{L/K}(P)$. The meaning of the terms inertia degree and ramifacation index for a prime v-ideal in T is obvious. From the theory of Dedekind domains we obtain the following results.

Proposition 2.5. *Let $p \in D_v(X)$ be a prime Kronecker divisor of D whose prime factorization in $T_v(X)$ is given by $p \sim P_1^{e_1} \cdot \ldots \cdot P_n^{e_n}$, where the $P_i \in T_v(X)$ are distinct prime divisors with $e_{L/K}(P_i) = e_i$. Interpreting the residue class ring $T_v(X)/pT_v(X)$ as a vector space over the residue class field $D_v(X)/pD_v(X) = K(X)_p$ of dimension d we obtain:*

(1) *$d = \sum_{i=1}^{n} e_{L/K}(P_i) \cdot f_{L/K}(P_i) \leqslant [L : K]$. If L/K is a separable extension, equality holds.*
(2) *If L/K is a normal extension, then $e_{L/K}(P_i) = e$ and $f_{L/K}(P_i) = f$ for all $1 \leqslant i \leqslant n$. Thus, $d = e \cdot f \cdot n \leqslant [L : K]$.*
(3) *If L/K is a Galois extension, then $d = e \cdot f \cdot n = [L : K]$*

Proposition 2.6. *Let L/K be a finite separable extension. If $P \in T_v(X)$ and $p \in D_v(X)$ are prime Kronecker divisors such that $P \mid p$ with respect to $T_v(X)$ and if $\mathfrak{P}$ and $\mathfrak{p}$ are the corresponding v-ideals, we have*

$$N_{L/K}(P) \sim p^{f_{L/K}(P)} \quad \text{and} \quad N^{(v)}_{L/K}(\mathfrak{P}) = (\mathfrak{p}^{f_{L/K}(\mathfrak{P})})_v.$$

3 Differents, discriminants and fundamental divisors

From now on let L/K be a finite separable extension of degree m. Then $L(X)/K(X)$ is also separable of degree m. We denote the trace function with respect to L/K resp. $L(X)/K(X)$ uniformly by $Tr_{L/K}$. For $A \subseteq L$

$$A^{\frown}_{T/D} := \{\gamma \in L : Tr_{L/K}(\gamma A) \subseteq D\}$$

is called the *complementary set* corresponding to A. Any complementary set is a D-module. If A is a free module with D-basis $\{\omega_1, \ldots, \omega_m\}$, then $A^{\frown}_{T/D}$ is a free D-module with the *complementary basis* $\{\widehat{\omega}_1, \ldots, \widehat{\omega}_m\}$. The complementary basis is determined by $Tr_{L/K}(\omega_i\widehat{\omega}_j) = \delta_{ij}$, $1 \leqslant i, j \leqslant m$, where δ_{ij} means the Kronecker symbol. If $A = \mathfrak{A}$

is a fractional T-ideal, the complementary set $\mathfrak{A}^{\widehat{}}_{T/D}$ is a fractional T-ideal, too. If T is a Krull domain, it even is a v-ideal. This follows from

Lemma 3.1. *Let $\mathfrak{A}$ be an arbitrary fractional ideal of the Krull domain T. Then,*

$$\mathfrak{A}(X)^{\widehat{}}_{T_v(X)/D_v(X)} \cap L = \mathfrak{A}^{\widehat{}}_{T/D}.$$

Proof: Since any element in $T_v(X)$ can be written as the quotient of a polynomial F over T and a v-primitive polynomial g over D and since $Tr_{L/K}(\frac{F}{g}) = \frac{1}{g} \cdot Tr_{L/K}(F)$ for all $F \in T[X]$ and $g \in D[X]$, we have

$$\begin{aligned}
&\mathfrak{A}(X)^{\widehat{}}_{T_v(X)/D_v(X)} \cap L \\
&= \big\{\gamma \in L(X) : Tr_{L/K}(\gamma \cdot \mathfrak{A}(X)) \subseteq D_v(X)\big\} \cap L \\
&= \big\{\gamma \in L : Tr_{L/K}\big(\gamma \cdot \tfrac{F}{g}\big) \in D_v(X) \text{ for all } F \in \mathfrak{A}[X],\, g \in N_v(D)\big\} \\
&= \big\{\gamma \in L : Tr_{L/K}(\gamma \cdot F) \in D_v(X) \cap K[X] = D[X] \text{ for all } F \in \mathfrak{A}[X]\big\} \\
&= \big\{\gamma \in L : Tr_{L/K}(\gamma \cdot \alpha) \in D \text{ for all } \alpha \in \mathfrak{A}\big\} = \mathfrak{A}^{\widehat{}}_{T/D}. \qquad \square
\end{aligned}$$

Proposition 3.2. *If T is a Krull domain, the complementary ideal of an arbitrary T-ideal is always a v-ideal. Two T-ideals generating the same v-ideal have the same complementary ideal.*

Proof: Let $\mathfrak{A}$ be an arbitrary T-ideal. By Theorem 1.4 the contracted T-ideal $\mathfrak{A}_v(X)^{\widehat{}}_{T_v(X)/D_v(X)} \cap L = \mathfrak{A}^{\widehat{}}_{T/D}$ is a v-ideal. If $\mathfrak{B}$ is another T-ideal with $\mathfrak{A}_v = \mathfrak{B}_v$, we have $\mathfrak{A}(X) = \mathfrak{A}_v(X) = \mathfrak{B}_v(X) = \mathfrak{B}(X)$ by Lemma 1.3. Now Lemma 3.1 yields $\mathfrak{A}^{\widehat{}}_{T/D} = \mathfrak{B}^{\widehat{}}_{T/D}$. $\square$

The *different* of the integral ring extension T/D is given by the integral v-ideal $\big(T^{\widehat{}}_{T/D}\big)^{-1}$ and is denoted by $\mathfrak{D}_{T/D}$. Correspondingly, $\mathfrak{D}_v(X)_{T/D} := \big(T_v(X)^{\widehat{}}_{T_v(X)/D_v(X)}\big)^{-1}$ means the different of the integral ring extension $T_v(X)/D_v(X)$. By Lemma 3.1 we have $T^{\widehat{}}_{T/D} = T_v(X)^{\widehat{}}_{T_v(X)/D_v(X)} \cap L$. Theorem 1.4, however, says that contracting $T_v(X)$-ideals to T-ideals is an isomorphism. Thus, we obtain

Proposition 3.3. *Let T be a Krull domain. Then*

$$\mathfrak{D}_{T/D} = \mathfrak{D}_v(X)_{T/D} \cap L.$$

If T is a Krull domain, all we know about differents in Dedekind domains can be applied to the Kronecker function ring $T^v = T_v(X)$, which is a principal ideal domain in this case. Translating the results into the language of divisorial ideals we see that, according to Theorem 1.4 and Proposition 3.3, most of the well-known ideal theoretic statements on differents in Dedekind domains, such as Dedekind's Different theorem or the Different tower theorem, carry over to differents in Krull domains.

The same is true for *discriminants* in Krull domains. It is well known that the discriminant of an extension T/D is the ideal norm of the corresponding different if D resp. T are Dedekind domains. The discriminant of $T_v(X)/D_v(X)$ is therefore given by the integral Kronecker divisor $\mathfrak{d}_v(X)_{T/D} := N_{L/K}(\mathfrak{D}_v(X)_{T/D})$. Correspondingly, we define the discriminant of T/D to be the integral v-ideal $\mathfrak{d}_{T/D} := N^{(v)}_{L/K}(\mathfrak{D}_{T/D})$.

Theorem 1.4 and Proposition 3.3 yield

$$\mathfrak{d}_{T/D} = \mathfrak{d}_v(X)_{T/D} \cap L.$$

Thus, the well-known ideal theoretic statements on discriminants in Dedekind domains, such as Dedekind's discrimiant theorem or the Discriminant tower theorem, remain valid for Krull domains.

In fact, it would be sufficient to know all the results on differents and discriminants in the case of an integral extension of principal ideal domains instead of Dedekind domains. We leave it to the reader to simplify the standard proofs. It is most likely that many proofs do without the methods of localization and completion, which are usually applied.

There is another point which makes things easier in Kronecker's divisor theory. If the finite extensions L/K resp. $L(X)/K(X)$ are separable, the principal ideal domain $T_v(X)$ becomes a free $D_v(X)$-module of degree $[L(X) : K(X)] = m$ (cf. [8, V, § 4, Corollary 2 of Theorem 7]). In particular, the algebraic function field $L(X)$ has an integral basis over $K(X)$. This remarkable fact has not been put much emphasis on yet.

Let $\{F_1, \dots, F_m\}$, $F_i \in T_v(X)$, be an integral basis of $L(X)$ over $K(X)$. Since every element in $T_v(X)$ can be written as the quotient of a polynomial over T and a polynomial over D which is v-primitive, we may assume without loss of generality that the F_i are polynomials with coefficients in T. Let $\alpha_1, \dots, \alpha_r$ be the coefficients of $F_1, \dots, F_m$. Any Kronecker divisor of T whose denominator is a polynomial with exactly these coefficients and whose nominator is v-primitive is called *fundamental Kronecker divisor* with respect to the integral basis $\{F_1, \dots, F_m\}$. The polynomials $\alpha_1 X + \dots + \alpha_r X^r$ and $F := F_1 X^{r_1} + \dots + F_m^{r_m}$ with $r_1 = 0$ and $r_{i+1} = i \cdot \big(1 + \max_{1 \leqslant j \leqslant m}\{\deg f_j\}\big)$ for $1 \leqslant i \leqslant m-1$ are examples of fundamental Kronecker divisors. It will be sufficient to think of fundamental divisors as polynomials of exactly this type.

Note that any fundamental divisor is a greatest common divisor of its corresponding integral basis, but that not any greatest common divisor of an integral basis is fundamental. This is obvious since

$$T_v(X) = F_1 D_v(X) + \dots + F_m D_v(X) \subseteq F_1 T_v(X) + \dots + F_m T_v(X) \subseteq T_v(X),$$

which means that the elements of an integral basis $\{F_1, \dots, F_m\}$ are always relatively prime with respect to $T_v(X)$.

To show that a fundamental divisor is also a primitive element of the separable extension $L(X)/K(X)$ we have to take a look at the element different of F. Remember that if $\chi(t)$ denotes the characteristic polynomial of F over $K(X)$, the element different of F is defined by

$$\operatorname{diff}_{L/K}(F) = \frac{d}{dt}\chi(t)|_{t=F} = \frac{d}{dt} N_{L/K}(t - F)|_{t=F} = \prod_{k=2}^{m} \big(F - \sigma_k(F)\big). \tag{3.4}$$

Proposition 3.5. *Let L/K be a finite separable extension and $F \in L[X]$ a polynomial with the coefficients $\alpha_1, \dots, \alpha_r$. Then the following conditions are equivalent:*

(1) $\mathrm{diff}_{L/K}(F) \neq 0$.
(2) $L(X) = K(X)[F]$.
(3) $L = K[\alpha_1, \dots, \alpha_r]$.

Proof: The equivalence (1) $\Leftrightarrow$ (2) is well-known.

(1) $\Rightarrow$ (3) Let $\mathrm{diff}_{L/K}(F) \neq 0$. Suppose $K' := K(\alpha_1, \dots, \alpha_r) \subsetneqq L$, i. e. $[L : K'] > 1$, in particular. Since the field polynomial of F over K is given by $\chi(t) = N_{L/K}(t - F) = N_{L/K'}\big(N_{K'/K}(t - F)\big) = N_{K'/K}(t - F)^{[L:K']}$,

$$\mathrm{diff}_{L/K}(F) = [L : K'] \cdot N_{L/K'}(F - F)^{[L:K']-1} \cdot \frac{d}{dt} N_{K'/K}(t - f)|_{t=F} = 0,$$

which is a contradiction.

(3) $\Rightarrow$ (1) Let $L = K(\alpha_1, \dots, \alpha_r)$. Assume $\mathrm{diff}_{L/K}(F) = 0$. By (3.4) this means there is a $k \in \{2, \dots, m\}$ such that $\sigma_k(\alpha_i) = \alpha_i$ for all $1 \leqslant i \leqslant r$. This, however, implies $\sigma_k(\alpha) = \alpha$ for all $\alpha \in L$, hence $\sigma_k = \sigma_1 = id_L$, which is impossible. □

To show that the fundamental Kronecker divisor F with the coefficients $\alpha_1, \dots, \alpha_r$ is a primitive element of the separable extension $L(X)/K(X)$, hence a divisor with $\mathrm{diff}_{L/K}(F) \neq 0$, it is therefore sufficient to prove $L = K[\alpha_1, \dots, \alpha_r]$. Since

$$T_v(X) = F_1 D_v(X) + \dots + F_m D_v(X) \subseteq D_v(X)[\alpha_1, \dots, \alpha_r] \subseteq T_v(X)$$

the Kronecker function ring $T_v(X)$ is a finitely generated extension ring of $D_v(X)$ with $T_v(X) = D_v(X)[\alpha_1, \dots, \alpha_r]$. Passing on to the corresponding quotient fields we obtain

$$L = L(X) \cap L = K(X)(\alpha_1, \dots, \alpha_r) \cap L = K(\alpha_1, \dots, \alpha_r).$$

Since the α_i are algebraic over K, this yields $L = K[\alpha_1, \dots, \alpha_r]$.

We will show that even more is true, namely that any fundamental divisor F generates the Kronecker function ring $T_v(X)$ over $D_v(X)$, i. e. $T_v(X) = D_v(X)[F]$. This follows from

Theorem 3.6. *Let D be a Krull domain with quotient field K, T the integral closure of D in the finite separable extension L/K and $F \in T[X]$ a fundamental Kronecker divisor of T with respect to the integral basis $\{F_1, \dots, F_m\}$. If the residue class field extensions $L(X)_P/K(X)_p$ are separable for all prime Kronecker divisors $P \in T_v(X)$, $p \in D_v(X)$ with $P \mid p$, we have*

$$\mathfrak{D}_v(X)_{T/D} = \mathrm{diff}_{L/K}(F)\, T_v(X).$$

We prove this theorem by means of

Lemma 3.7. *Let D be a Krull domain with quotient field K, T the integral closure of D in the finite separable extension L/K and $F \in T[X]$ a fundamental Kronecker divisor of T with respect to the integral basis $\{F_1, \dots, F_m\}$. Then we have*

$$\mathrm{diff}_{L/K}(F) \sim \gcd\Big(\big\{\mathrm{diff}_{L/K}(G) : G \in T_v(X) \text{ with } L(X) = K(X)[G]\big\}\Big).$$

Proof: Let $\alpha_1, \dots, \alpha_r$ be the coefficients of $F_1, \dots, F_m$. Since we have the equality $T_v(X) = D_v(X)[\alpha_1, \dots, \alpha_r]$ any element $G \in T_v(X)$ can be written as

$$G = \sum_{i_1,\dots,i_r \in \mathbb{N}} d_{i_1,\dots,i_r} \alpha_1^{i_1} \cdot \ldots \cdot \alpha_r^{i_r} \quad \text{with} \quad d_{i_1,\dots,i_r} \in D_v(X),$$

where only finitely many $d_{i_1,\dots,i_r}$ are $\neq 0$. Let $G \in T_v(X)$ be a primitive element of the separable field extension $L(X)/K(X)$, i. e. let $\operatorname{diff}_{L/K}(G) \neq 0$. We denote the normal closure of $L(X)/K(X)$ by $\overline{L(X)}$ and the integral closure of $T_v(X)$ in $\overline{L(X)}$ by $\overline{T_v(X)}$. Let σ be a $K(X)$-automorphism of $\overline{L(X)}$. To show $\operatorname{diff}_{L/K}(F) \mid \operatorname{diff}_{L/K}(G)$ we first prove by induction on the number of coefficients r that $G - \sigma(G)$ is a linear combination of $\alpha_1 - \sigma(\alpha_1), \dots, \alpha_r - \sigma(\alpha_r)$ over $\overline{T_v(X)}$. For $r = 1$ we have $G = \sum_{i \in \mathbb{N}} d_i \cdot \alpha_1^i$ with $d_i \in D_v(X)$. This, however, implies

$$G - \sigma(G) = \sum_{i \in \mathbb{N}} d_i \big(\alpha_1^i - \sigma(\alpha_1)^i\big)$$

$$= \big(\alpha_1 - \sigma(\alpha_1)\big) \cdot \sum_{i \in \mathbb{N}} d_i \cdot \big(\alpha_1^{i-1} + \alpha_1^{i-2}\sigma(\alpha_1) + \ldots + \alpha_1\sigma(\alpha_1)^{i-2} + \sigma(\alpha_1)^{i-1}\big),$$

which obviously is an element of the desired form. Suppose now that the statement has been proved for $r \geqslant 1$ and let

$$G = \sum_{i_1,\dots,i_r,i_{r+1} \in \mathbb{N}} d_{i_1,\dots,i_r,i_{r+1}} \cdot \alpha_1^{i_1} \cdot \ldots \cdot \alpha_r^{i_r} \cdot \alpha_{r+1}^{i_{r+1}}$$

$$= \sum_{i_{r+1} \in \mathbb{N}} \alpha_{r+1}^{i_{r+1}} \cdot \sum_{i_1,\dots,i_r \in \mathbb{N}} d_{i_1,\dots,i_r,i_{r+1}} \cdot \alpha_1^{i_1} \cdot \ldots \cdot \alpha_r^{i_r}.$$

We define $G_{i_{r+1}}$ to be the Kronecker divisor $\sum d_{i_1,\dots,i_r,i_{r+1}} \cdot \alpha_1^{i_1} \cdot \ldots \cdot \alpha_r^{i_r}$. Then, by induction hypothesis, $G_{i_{r+1}} - \sigma(G_{i_{r+1}})$ is a linear combination of $\alpha_1 - \sigma(\alpha_1), \dots, \alpha_r - \sigma(\alpha_r)$ over $\overline{T_v(X)}$. Thus,

$$G - \sigma(G) = \sum_{i_{r+1} \in \mathbb{N}} \Big(G_{i_{r+1}} \cdot \alpha_{r+1}^{i_{r+1}} - \sigma(G_{i_{r+1}}) \cdot \sigma(\alpha_{r+1}^{i_{r+1}})\Big)$$

$$= \sum_{i_{r+1} \in \mathbb{N}} \Big(\alpha_{r+1}^{i_{r+1}}\big(G_{i_{r+1}} - \sigma(G_{i_{r+1}})\big) + \sigma(G_{i_{r+1}})\big(\alpha_{r+1}^{i_{r+1}} - \sigma(\alpha_{r+1}^{i_{r+1}})\big)\Big)$$

is a linear combination of $\alpha_1 - \sigma(\alpha_1), \dots, \alpha_{r+1} - \sigma(\alpha_{r+1})$ over $\overline{T_v(X)}$, where we made use of the fact that

$$\alpha_{r+1}^{i_{r+1}} - \sigma(\alpha_{r+1}^{i_{r+1}}) = \big(\alpha_{r+1} - \sigma(\alpha_{r+1})\big) \cdot \big(\alpha_{r+1}^{i_{r+1}-1} + \ldots + \sigma(\alpha_{r+1}^{i_{r+1}-1})\big)$$

and α_{r+1}^{i+1} resp. $\sigma(G_{i_{r+1}})\big(\alpha_{r+1}^{i_{r+1}-1} + \ldots + \sigma(\alpha_{r+1}^{i_{r+1}-1})\big)$ are elements in $\overline{T_v(X)}$. For the fundamental divisor $F = \alpha_1 X^{i_1} + \ldots + \alpha_r X^{i_r}$, $i_k \neq i_l$ for $k \neq l$, with respect to the integral basis $\{F_1, \dots, F_m\}$ we have

$$F - \sigma(F) = (\alpha_1 - \sigma(\alpha_1))X^{i_1} + \ldots + (\alpha_r - \sigma(\alpha_r))X^{i_r}.$$

Since $\overline{T_v(X)}$ is equal to the Kronecker function ring of $\overline{T}$, the Kronecker divisor $F - \sigma(F)$ divides each of its coefficients in $\overline{T_v(X)}$. This however, implies $F - \sigma(F) \mid G - \sigma(G)$ in $\overline{T_v(X)}$ for any $G \in T_v(X)$ with $\operatorname{diff}_{L/K}(G) \neq 0$. Since $\operatorname{diff}_{L/K}(F) = \prod_{\sigma \neq \mathrm{id}_L} \big(F - \sigma(F)\big)$,

we obtain $\mathrm{diff}_{L/K}(F) \mid \mathrm{diff}_{L/K}(G)$ in $\overline{T_v(X)} \cap L(X) = T_v(X)$. Thus, $\mathrm{diff}_{L/K}(F)$ is a greatest common divisor off all element differents $\mathrm{diff}_{L/K}(G) \neq 0$. □

Proof of Theorem 3.6: It is well-known that the different of a Dedekind domain is the greatest common divisor of all element differents $\neq 0$ (cf. [6, III, § 2, Proposition 8] or [3, XII, Satz 4.3]). Thus, by Lemma 3.7

$$\begin{aligned}\mathfrak{D}_v(X)_{T/D} &= \Big(\big\{\mathrm{diff}_{L/K}(G) : G \in T_v(X) \text{ with } L(X) = K(X)[G]\big\}\Big) T_v(X) \\ &= \mathrm{diff}_{L/K}(F)\, T_v(X).\end{aligned}$$ □

Theorem 3.6 is indeed remarkable. Since we have

$$N_{L/K}\big(\mathrm{diff}_{L/K}(G)\big) = (-1)^{\frac{1}{2}n(n-1)}\mathrm{discr}_{L/K}(G)$$

for any primitive element $G \in T_v(X)$ of the separable extension $L(X)/K(X)$, it follows that the discriminant of $T_v(X)/D_v(X)$ is given by

$$\mathfrak{d}_v(X)_{T/D} = \mathrm{discr}_{L/K}(F)\, D_v(X).$$

But we already know $\mathfrak{d}_v(X)_{T/D} = \mathrm{discr}_{L/K}(F_1, \ldots, F_m)$ since the discriminant of the integral extension $T_v(X)/D_v(X)$ is just the discriminant of any integral basis. Thus, $\{1, F, \ldots, F^{m-1}\}$ is shown to be an integral basis of $L(X)/K(X)$, too, and we obtain

Theorem 3.8. *Let D be a Krull domain with quotient field K and T the integral closure of D in the finite separable extension L/K. All residue class field extensions $L(X)_P/K(X)_p$ are supposed to be separable for any pair of prime Kronecker divisors $P \in T_v(X)$, $p \in D_v(X)$ with $P \mid p$. If $F \in T[X]$ is a fundamental Kronecker divisor of T, we have*

$$T_v(X) = D_v(X)[F].$$

In particular, there are no common inessential discriminant divisors $\not\sim 1$ with respect to the integral extension $T_v(X)/D_v(X)$.

4 Factorizing primes in Kronecker's divisor theory

Suppose now that the assumptions of Theorem 3.8 are fulfilled. Since we have $T_v(X) = D_v(X)[F]$ for any fundamental Kronecker divisor F, we can always apply Kummer's decomposition theorem (cf. [6, I, § 8, Proposition 25]) in order to factorize prime Kronecker divisors of $D_v(X)$ in the integral closure $T_v(X)$.

Let $p \in D_v(X)$ be a prime Kronecker divisor of $D_v(X)$. Assume that $F \in D_v(X)$ is a fundamental divisor with minimal polynomial $\mu(t) \in D_v(X)[t]$. Reduction modulo $pD_v(X)$ gives the decomposition

$$\overline{\mu(t)} = \overline{\mu_1(t)}^{e_1} \cdot \ldots \cdot \overline{\mu_n(t)}^{e_n}$$

with $\mu_i \in D_v(X)[t]$ such that $\overline{\mu_i}$ is prime in $D_v(X)/pD_v(X)[t]$. Then the decomposition of p into irreducible factors in $T_v(X)$ is given by

$$p \sim P_1^{e_1} \cdot \ldots \cdot P_n^{e_n},$$

where $P_i \sim \gcd\big(p, \mu_i(F)\big)$ with $f_{L/K}(P_i) = \deg \mu_i(t)$ for all $1 \leqslant i \leqslant n$.

Let us have a look at the classical situation of algebraic number theory, i. e. let D be the ring of rational integers $\mathbb{Z}$ with quotient field $K = \mathbb{Q}$ and T the ring of algebraic integers in the algebraic number field L. Then there is an integral basis $\{\omega_1, \ldots, \omega_m\}$ of L/K which is also an integral basis of $L(X)/K(X)$. Thus, we can choose a fundamental Kronecker divisor of the form $F = \omega_1 X + \ldots + \omega_m X^m$. Note that in the case of an algebraic number field the v-operation is the identity on the system of all ideals. Thus, v-primitivity means primitivity in the usual sense, i. e. a polynomial over $\mathbb{Z}$ resp. T is v-primitive if and only if its coefficients generate the unit ideal. In $\mathbb{Z}$ this is obviously equivalent to the condition that all coefficients are relatively prime. Thus, the Kronecker function rings $\mathbb{Z}_v(X)$ and $T_v(X)$ are given by $\mathbb{Z}_v(X) = \big\{\frac{f}{g} : f, g \in \mathbb{Z}[X],\ \gcd(\text{coefficients of } g) \sim 1\big\}$ and $T_v(X) = \big\{\frac{F}{G} : F, G \in T[X],\ (\text{coefficients of } G)T = T\big\}$.

Suppose that $p \in \mathbb{Z}$ is a rational prime with corresponding prime ideal $\mathfrak{p} = p\mathbb{Z}$. Let $P \in T_v(X)$ be a prime Kronecker divisor of T with corresponding v-ideal $\mathfrak{P}$ such that $P \mid p$ in $T_v(X)$. Since $\mathfrak{p}$ and $\mathfrak{P}$ are maximal ideals the residue class rings $\mathbb{Z}/\mathfrak{p} = \mathbb{Z}_p$ and $T/\mathfrak{P}$ are fields, namely the residue class fields of $\mathfrak{p}$ and $\mathfrak{P}$. Since $\mathbb{Z}_p$ is finite, $T/\mathfrak{P}$ is separable over $\mathbb{Z}_p$. This implies that $T/\mathfrak{P}\ (X)$ is separable over $\mathbb{Z}_p(X)$. By Theorem 2.4.(1) it follows that $T_v(X)/PT_v(X)$ is separable over $\mathbb{Z}_v(X)/p\mathbb{Z}_v(X)$. Thus, the conditions of Theorem 3.8 are fulfilled and we obtain $T_v(X) = \mathbb{Z}_v(X)[F]$.

Let $\mu(t) \in \mathbb{Z}_v(X)[t]$ be the minimal polynomial of the fundamental divisor F. The proof of Proposition 2.3 shows that reducing a Kronecker divisor $\frac{f}{g} \in \mathbb{Z}_v(X)$, $f \in \mathbb{Z}[X]$, $g \in N_v(\mathbb{Z})$, modulo $p\mathbb{Z}_v(X) = \mathfrak{p}(X)$ actually means reducing the coefficients of f and g modulo $p\mathbb{Z} = \mathfrak{p}$. Since $\mu(t)$ has coefficients in $\mathbb{Z}[X] \subseteq \mathbb{Z}_v(X)$, reduction modulo $p\mathbb{Z}_v(X)$ gives the polynomial $\overline{\mu(t)}$ with coefficients in $\mathbb{Z}_p[X] \subseteq \mathrm{Quot}\big(\mathbb{Z}_p[X]\big) \cong \mathbb{Z}_v(X)/p\mathbb{Z}_v(X)$. Note that by Gauss' Lemma any irreducible factor of $\overline{\mu(t)}$ in $\mathbb{Z}_p[X][t]$ remains irreducible over $\mathbb{Z}_v(X)/p\mathbb{Z}_v(X)$. Thus, it is sufficient to determine the prime decomposition of $\overline{\mu(t)}$ over $\mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a finite field, this can be done in a finite number of steps. If $\mu_1, \ldots, \mu_n \in \mathbb{Z}[X][t]$ are such that

$$\overline{\mu(t)} = \overline{\mu_1(t)}^{e_1} \cdot \ldots \cdot \overline{\mu_n(t)}^{e_n} \quad \text{with } \overline{\mu_i(t)} \text{ prime in } \mathbb{Z}_p[X][t],$$

all prime Kronecker divisors of T dividing p in $T_v(X)$ are given by

$$P_i \sim \gcd\big(p, \mu_i(F)\big) \sim p + \mu_i(F) \cdot X,$$

and we obtain the prime decomposition of p in $T_v(X)$ by

$$p \sim P_1^{e_1} \cdot \ldots \cdot P_n^{e_n}.$$

A similar result has also been obtained by H.M. Edwards in the case of algebraic number fields (cf. [1, §§ 2.4–2.7]). Edward's presentation, however, is unfamiliar to the modern reader and sometimes lacks the clarity of modern mathematical language. In my opinion, it does not reveal the real cause why Kronecker divisors make Kummer's factorization method work also for common inessential discriminant divisors.

5 Bibliography

[1] Harold M. Edwards: Divisor Theory. — Boston u. a.: Birkhäuser 1990.
[2] Harley Flanders: The meaning of the form calculus in classical ideal theory. — Transactions of the American Mathematical Society 95 (1960), 92–100.
[3] Karl-Bernhard Gundlach: Einführung in die Zahlentheorie. — Mannheim/Wien/Zürich: Bibliographisches Institut 1972.
[4] Paul Jaffard: Systèmes Idéaux. — Paris: Dunod 1960.
[5] Wolfgang Krull: Beiträge zur Arithmetik kommutativer Integritätsbereiche. II. v-Ideale und vollständig ganz abgeschlossene Integritätsbereiche. — Mathematische Zeitschrift 41 (1936), 665–679.
[6] Serge Lang: Algebraic Number Theory. — New York u. a.: Springer 1996.
[7] Friedemann Lucius: Ringe mit einer Theorie des größten gemeinsamen Teilers. — Mathematica Gottingensis 7 (1997), 1–70.
[8] Oscar Zariski & Pierre Samuel: Commutative Algebra, Vol. 1. — New York/Heidelberg/Berlin: Springer 1958.