DISCRIMINANTS IN TOWERS

JOSEPH RABINOFF

Let A be a Dedekind domain with fraction field F, let K/F be a finite separable extension field, and let B be the integral closure of A in K. In this note, we will define the discriminant ideal $\mathscr{D}_{B/A}$ and the relative ideal norm $\mathrm{N}_{B/A}(\mathfrak{b})$. The goal is to prove the formula

$$\mathscr{D}_{C/A} = \mathrm{N}_{B/A}\big(\mathscr{D}_{C/B}\big) \cdot \mathscr{D}_{B/A}^{[L:K]},$$

where C is the integral closure of B in a finite separable extension field L/K. See Theorem 6.1.

The main tool we will use is localizations, and in some sense the main purpose of this note is to demonstrate the utility of localizations in algebraic number theory via the discriminants in towers formula. Our treatment is self-contained in that it only uses results from Samuel's *Algebraic Theory of Numbers*, cited as [Samuel].

Remark. All finite extensions of a perfect field are separable, so one can replace "Let K/F be a separable extension" by "suppose F is perfect" here and throughout. Note that Samuel generally assumes the base has characteristic zero when it suffices to assume that an extension is separable. We will use the more general fact, while quoting [Samuel] for the proof.

1. Notation and review. Here we fix some notations and recall some facts proved in [Samuel]. Let K/F be a finite field extension of degree n, and let $x_1, \dots, x_n \in K$. We define

$$D(x_1, \dots, x_n) = \det\big(\mathrm{Tr}_{K/F}(x_i x_j)\big)_{i,j=1}^{n}.$$

We write $D_{K/F}$ instead of D if the field extension is not clear from context. If K/F is separable and $x_1, \dots, x_n$ are an F-basis for K, then $D(x_1, \dots, x_n) \neq 0$ by [Samuel, Proposition 2.7.3]. If M is an $n \times n$ matrix with coefficients in F then

$$D(Mx_1, \dots, Mx_n) = \det(M)^2 \cdot D(x_1, \dots, x_n) \tag{1.1}$$

by [Samuel, Proposition 2.7.1]. If M is a permutation matrix then $\det(M) = \pm 1$, so $D(x_1, \dots, x_n)$ is independent of the ordering of its arguments.

Let A be an integrally closed domain with fraction field F, let K/F be a finite extension of degree n, and let $B \subset K$ be a subring which is integral over A. Then for $x_1, \dots, x_n \in B$, we have $\mathrm{Tr}_{K/F}(x_i x_j) \in A$, so $D(x_1, \dots, x_n) \in A$. If B is a free A-module of rank n, with basis $x_1, \dots, x_n$, the *discriminant ideal* is the principal ideal

$$\mathscr{D}_{B/A} := D(x_1, \dots, x_n)A. \tag{1.2}$$

This is independent of the choice of basis by (1.1), as if M is a change of basis matrix for B, then $\det(M) \in A^{\times}$. If K/F is separable then $\mathscr{D}_{B/A}$ is nonzero.

Now we specialize to the case of Dedekind domains. See [Samuel, Theorems 2.7.1 and 3.4.1] for proofs of the following facts.

Proposition 1.3. *Let A be a Dedekind domain with fraction field F, let K/F be a finite separable extension of degree n, and let B be the integral closure of A in K. Then:*

1. *B is a Dedekind domain with fraction field K.*
2. *B is an A-submodule of a free A-module of rank n.*
3. *B is a finitely generated A-module.*
4. *If $\mathfrak{q} \subset B$ is a maximal ideal then $\mathfrak{q} \cap A$ is a maximal ideal.*
5. *If A is a principal ideal domain, then B is a free A-module of rank n, and any A-basis for B is an F-basis for K.*

Let A be a Dedekind domain with field of fractions F. For a nonzero fractional ideal $\mathfrak{a} \subset F$, we have a unique factorization

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

where the product is taken over all nonzero prime ideals of A. Of course, all but finitely many of the integers $v_{\mathfrak{p}}(\mathfrak{a})$ are zero. For fixed $\mathfrak{p}$ we have $v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$, where $\mathfrak{a}, \mathfrak{b} \subset F$ are nonzero fractional ideals. For $x \in F^\times$ we write $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}((x))$.

Remark 1.4. We will follow Samuel's convention that a field is a Dedekind domain. This has the advantage that any localization of a Dedekind domain is Dedekind (see Proposition 2.1 below), but the disadvantage that one has to distinguish between "maximal ideal" and "nonzero prime ideal" throughout.

2. Localizations. For our purposes, the main advantage of localizations is that they produce principal ideal domains from Dedekind domains. This allows us to use the classification of modules over a PID, and facilitates our constructions and proofs. The localization is well-behaved, in that it respects most ring-theoretic constructions, and one can recover information about a ring from its localizations.

Let A be an integral domain with fraction field F, and let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset. Recall that the *localization* of A at S is

$$S^{-1}A := \left\{ \frac{a}{s} \in F \mid a \in A,\, s \in S \right\}.$$

This is a subring of F containing A, and the fraction field of $S^{-1}A$ is F. For a prime ideal $\mathfrak{p} \subset A$, the complement $A \setminus \mathfrak{p}$ is multiplicatively closed, and we write

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A = \left\{ \frac{a}{s} \in F \mid a, s \in A,\, s \notin \mathfrak{p} \right\}.$$

We call $A_{\mathfrak{p}}$ the *localization of A at* $\mathfrak{p}$. If A is a subring of an integral domain B and $\mathfrak{p} \subset A$ is a prime ideal, then $A \setminus \mathfrak{p}$ is also a multiplicatively closed subset of B, and we write $B_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B$. Note that $B_{\mathfrak{p}}$ in general is *not* the localization of B at a prime ideal of B.

Let A be an integral domain, let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset, and let $A' = S^{-1}A$. For an ideal $\mathfrak{a} \subset A$, we define its *extension* $\mathfrak{a}A'$ to be the ideal of A' generated by $\mathfrak{a}$. The *contraction* of an ideal $\mathfrak{a}' \subset A'$ is the ideal $\mathfrak{a}' \cap A$ of A. An ideal of A of the form $\mathfrak{a}' \cap A$ is called *contracted*.

We have the following ideal correspondence for localizations from [Samuel, Proposition 5.1.1]. Note the similarity with the ideal correspondence for quotients.

Proposition 2.1. *Let A be an integral domain, let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset, and let $A' = S^{-1}A$.*

(1) *For every ideal $\mathfrak{a}' \subset A'$ we have $(\mathfrak{a}' \cap A)A' = \mathfrak{a}'$.*
(2) *Extension and contraction give rise to an inclusion-preserving bijection*
$$\big\{\textit{contracted ideals of } A\big\} \longleftrightarrow \big\{\textit{ideals of } A'\big\}.$$
(3) *The bijection of (2) restricts to a bijection*
$$\big\{\textit{prime ideals } \mathfrak{p} \subset A \textit{ such that } \mathfrak{p} \cap S = \emptyset\big\} \longleftrightarrow \big\{\textit{prime ideals of } A'\big\}.$$
In other words, a prime ideal $\mathfrak{p} \subset A$ is contracted if and only if $\mathfrak{p} \cap S = \emptyset$.

Exercise 2.2. Let A be an integral domain, let $\mathfrak{a} \subset A$ be an ideal, let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset, and let $A' = S^{-1}A$. Prove that:

(1) $\mathfrak{a}A' = \left\{ \dfrac{a}{s} \mid a \in \mathfrak{a},\, s \in S \right\}$.
(2) If $\mathfrak{p} \subset A$ is prime with $\mathfrak{p} \cap S = \emptyset$, $a \in A$ and $s \in S$, then $a/s \in \mathfrak{p}A'$ if and only if $a \in \mathfrak{p}$. [Careful: remember that there are multiple ways of expressing an element of $S^{-1}A$ as a fraction.]
(3) The contraction of a nonzero ideal is nonzero.
(4) Extension is compatible with products, in that for any two ideals $\mathfrak{a}, \mathfrak{b} \subset A$,
$$(\mathfrak{a}A')(\mathfrak{b}A') = (\mathfrak{a}\mathfrak{b})A'.$$
(5) $\mathfrak{a}A' = A'$ if and only if $S \cap \mathfrak{a} \neq \emptyset$.
(6) $A = S^{-1}A$ if and only if $S \subset A^{\times}$.

Exercise 2.3. Let A be an integral domain, let $\mathfrak{a} \subsetneq A$ be a proper ideal, and let $S = 1 + \mathfrak{a}$. Verify that S is a multiplicatively closed subset, and show that for a prime ideal $\mathfrak{p} \subset A$, we have $\mathfrak{p} \cap S \neq \emptyset$ if and only if $\mathfrak{p} + \mathfrak{a} = A$.

3. Localizations of Dedekind domains. The localization is an extremely well-behaved construction, in that it is compatible with most of the ring-theoretic constructions we have already encountered. For instance, we have [Samuel, Proposition 5.1.2 and 5.1.3].

Proposition 3.1. *Let A be a Dedekind domain with fraction field F, let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset, let K/F be a finite separable extension, and let B be the integral closure of A in K. Then*

(1) *$S^{-1}B$ is the integral closure of $S^{-1}A$ in K, and*
(2) *$S^{-1}B$ is a Dedekind domain.*

By Exercise 2.2, nonzero prime ideals in $S^{-1}A$ correspond to nonzero prime ideals in A which are disjoint from S. The following lemma relates prime factorizations in A to prime factorizations in $S^{-1}A$.

Lemma 3.2. *Let A be a Dedekind domain, let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset, and let $A' := S^{-1}A$.*

(1) *If $\mathfrak{a}\subset A$ is a nonzero ideal then*
$$\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \implies \mathfrak{a}A'=\prod_{\mathfrak{p}\cap S=\emptyset}(\mathfrak{p}A')^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

(2) *If $\mathfrak{a}'\subset A'$ is a nonzero ideal then*
$$\mathfrak{a}'=\prod_{\mathfrak{p}\cap S=\emptyset}(\mathfrak{p}A')^{v_{\mathfrak{p}A'}(\mathfrak{a}')} \implies \mathfrak{a}'\cap A=\prod_{\mathfrak{p}\cap S=\emptyset}\mathfrak{p}^{v_{\mathfrak{p}A'}(\mathfrak{a}')}.$$

(3) *The nonzero contracted ideals in A are those ideals whose prime factors are disjoint from S.*

In other words, to find the prime factorization of $\mathfrak{a}A'$, one simply deletes the prime factors which do not give rise to prime ideals of A'. By Proposition 2.1(3), every nonzero prime ideal of A' has the form $\mathfrak{p}A'$ for a nonzero prime ideal $\mathfrak{p}\subset A$, and Lemma 3.2 implies the compatibility

$$v_{\mathfrak{p}A'}(\mathfrak{a}A')=v_{\mathfrak{p}}(\mathfrak{a}). \tag{3.3}$$

Proof. By Exercise 2.2(4), extension is compatible with ideal products, so
$$\mathfrak{a}A'=\prod_{\mathfrak{p}}(\mathfrak{p}A')^{v_{\mathfrak{p}}(\mathfrak{a})}=\prod_{\mathfrak{p}\cap S=\emptyset}(\mathfrak{p}A')^{v_{\mathfrak{p}}(\mathfrak{a})}$$
because $\mathfrak{p}A'=A'$ when $\mathfrak{p}\cap S\neq\emptyset$. This gives (1). Now we prove (2). By Proposition 2.1(1), the ideal $\mathfrak{a}:=\mathfrak{a}'\cap A$ extends to $\mathfrak{a}'$, and by (1), the ideal $\mathfrak{b}:=\prod_{\mathfrak{p}\cap S=\emptyset}\mathfrak{p}^{v_{\mathfrak{p}A'}(\mathfrak{a}')}$ extends to $\mathfrak{a}'$ as well. Clearly
$$\mathfrak{b}\subset(\mathfrak{b}A')\cap A=\mathfrak{a}'\cap A=\mathfrak{a},$$
so $\mathfrak{a}\mid\mathfrak{b}$. This implies $v_{\mathfrak{p}}(\mathfrak{a})\leq v_{\mathfrak{p}}(\mathfrak{b})$ for all primes $\mathfrak{p}\subset A$. By construction and (3.3), if $\mathfrak{p}\cap S=\emptyset$ then $v_{\mathfrak{p}}(\mathfrak{b})=v_{\mathfrak{p}A'}(\mathfrak{a}')=v_{\mathfrak{p}}(\mathfrak{a})$, and since $v_{\mathfrak{p}}(\mathfrak{b})=0$ for $\mathfrak{p}\cap S\neq\emptyset$, for such $\mathfrak{p}$ we have
$$0\leq v_{\mathfrak{p}}(\mathfrak{a})\leq v_{\mathfrak{p}}(\mathfrak{b})=0.$$
This means $v_{\mathfrak{p}}(\mathfrak{a})=v_{\mathfrak{p}}(\mathfrak{b})$ for *all* $\mathfrak{p}$, so $\mathfrak{a}=\mathfrak{b}$. This proves (2); part (3) follows from (1) and (2). □

We will produce principal ideal domains from Dedekind domains in the following way.

Definition 3.4. A nonzero ring is called *semi-local* if it has finitely many maximal ideals. A Dedekind domain with exactly one nonzero prime ideal is a called a *discrete valuation ring*, or *DVR*.

Lemma 3.5. *A semi-local Dedekind domain is a PID. In particular, a DVR is a PID.*

Proof. Let A be a semi-local Dedekind domain with nonzero prime ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$. These are distinct maximal ideals, so they are pairwise coprime: $\mathfrak{p}_i+\mathfrak{p}_j=(1)$ for $i\neq j$. Moreover, since $\mathfrak{p}_1^2$ does not share any common factors with $\mathfrak{p}_j$ for $j\geq 2$, we have likewise $\mathfrak{p}_1^2+\mathfrak{p}_j=\gcd(\mathfrak{p}_1^2,\mathfrak{p}_j)=(1)$. Applying the Chinese remainder theorem gives a surjection
$$c\colon A\twoheadrightarrow\frac{A}{\mathfrak{p}_1^2}\times\frac{A}{\mathfrak{p}_2}\times\cdots\times\frac{A}{\mathfrak{p}_r}$$

with kernel $\mathfrak{p}_1^2\mathfrak{p}_2\cdots\mathfrak{p}_r$. Let $\overline{x}\in\mathfrak{p}_1/\mathfrak{p}_1^2$ be a nonzero element, and choose $x\in A$ such that $c(x)=(\overline{x},1,\ldots,1)$. Then $x\in\mathfrak{p}_1$ but not $\mathfrak{p}_1^2$, and for $j\geq 2$ we have $x\equiv 1 \mod \mathfrak{p}_j$ for $j\geq 2$, so $x\notin\mathfrak{p}_j$. In terms of ideals, this says $\mathfrak{p}_1\mid(x)$ but $\mathfrak{p}_1^2\nmid(x)$, and $\mathfrak{p}_j\nmid(x)$ for $j\geq 2$. Hence $(x)=\mathfrak{p}_1$, as this is the only possible prime factorization. It follows that $\mathfrak{p}_1$ is principal, and by the same argument, that $\mathfrak{p}_i$ is principal for all i. As any nonzero ideal in A is a product of prime ideals, A is a principal ideal domain. □

Remark 3.6. Let A be a DVR with maximal ideal $\mathfrak{p}$. Then $\mathfrak{p}=(p)$ is principal, and every nonzero ideal of A has the form $\mathfrak{p}^n$ for some $n\geq 0$, since there are no other possible ideal factorizations. Hence the ideals of A are $(1),(p),(p^2),(p^3),\cdots,(0)$.

Example 3.7. The ring $A=\mathbf{C}[\![t]\!]$ is a DVR with maximal ideal (t).

Lemma 3.8. *If A is a Dedekind domain, then $A_{\mathfrak{p}}$ is a DVR, and $\mathfrak{p}A_{\mathfrak{p}}$ is its maximal ideal.*

Proof. We know that $A_{\mathfrak{p}}$ is Dedekind by Proposition 3.1(2), and by Proposition 2.1(3) that every nonzero prime ideal of $A_{\mathfrak{p}}$ has the form $\mathfrak{q}A_{\mathfrak{p}}$ for a nonzero prime ideal $\mathfrak{q}\subset A$ such that $\mathfrak{q}\cap(A\setminus\mathfrak{p})=\emptyset$. But $\mathfrak{q}\cap(A\setminus\mathfrak{p})=\emptyset$ if and only if $\mathfrak{q}\subset\mathfrak{p}$, so since $\mathfrak{p}$ and $\mathfrak{q}$ are maximal, we must have $\mathfrak{p}=\mathfrak{q}$. □

Lemma 3.9. *Let A be a discrete valuation ring with fraction field F, let K/F be a finite separable extension, and let B be the integral closure of A in K. Then B is semi-local, hence a PID.*

Proof. Let $\mathfrak{q}$ be a maximal ideal of B. Then $\mathfrak{q}\cap A$ is a maximal ideal by Proposition 1.3(4), so $\mathfrak{q}\cap A=\mathfrak{p}$, the unique maximal ideal of A. Thus $\mathfrak{p}\subset\mathfrak{q}$, so $\mathfrak{p}B\subset\mathfrak{q}$, and hence $\mathfrak{q}\mid\mathfrak{p}B$. But $\mathfrak{p}B$ has only finitely many prime factors. □

It follows from Lemmas 3.8 and 3.9 that if A is a Dedekind domain with fraction field F, $\mathfrak{p}\subset A$ is a nonzero prime, K/F is a finite separable extension, and B is the integral closure of A in K, then both $A_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ are PIDs.

We will also use localizations to test if two ideals are equal.

Lemma 3.10. *Let A be a Dedekind domain, and let $\mathfrak{a},\mathfrak{a}'\subset A$ be nonzero ideals. Then $\mathfrak{a}=\mathfrak{a}'$ if and only if $\mathfrak{a}A_{\mathfrak{p}}=\mathfrak{a}'A_{\mathfrak{p}}$ for all nonzero prime ideals $\mathfrak{p}\subset A$.*

Proof. If $\mathfrak{a}A_{\mathfrak{p}}=\mathfrak{a}'A_{\mathfrak{p}}$ then $v_{\mathfrak{p}}(\mathfrak{a})=v_{\mathfrak{p}}(\mathfrak{a}')$ by (3.3). Hence $\mathfrak{a}$ and $\mathfrak{a}'$ have the same prime factorizations. □

Exercise 3.11. Let A be a Dedekind domain, let $S\subset A\setminus\{0\}$ be a multiplicatively closed subset, and let $A'=S^{-1}A$. Prove that for any two ideals $\mathfrak{a}',\mathfrak{b}'\subset A'$, we have

$$(\mathfrak{a}'\cap A)\cdot(\mathfrak{b}'\cap A)=(\mathfrak{a}'\mathfrak{b}')\cap A.$$

In other words, contraction is compatible with products in the case of localizations of Dedekind domains.[1]

Exercise 3.12. Let A be a Dedekind domain, let $S\subset A\setminus\{0\}$ be a multiplicatively closed subset, and let $A'=S^{-1}A$.

[1] I strongly believe this to be false in general, but I cannot find a counterexample when A is an integral domain.

(1) Let $\mathfrak{p} \subset A$ be a nonzero prime ideal such that $\mathfrak{p} \cap S = \emptyset$. Generalize [Samuel, Proposition 5.1.5] to prove that for any $n \geq 0$, the natural homomorphism
$$A/\mathfrak{p}^n \longrightarrow A'/(\mathfrak{p}A')^n$$
is an isomorphism.

(2) Let $\mathfrak{a} \subset A$ be a nonzero contracted ideal. Prove that the natural homomorphism
$$A/\mathfrak{a} \longrightarrow A'/\mathfrak{a}A'$$
is an isomorphism.

Exercise 3.13. Let A be a Dedekind domain and let $\mathfrak{a} \subset A$ be a nonzero ideal.

(1) Prove that every ideal of $A/\mathfrak{a}$ is principal. [Localize at $S = 1 + \mathfrak{a}$ as in Exercise 2.3. Show that $\mathfrak{a}$ is contracted and $S^{-1}A$ is semi-local, then use Exercise 3.12(2).]

(2) Prove that $\mathfrak{a}$ can be generated by two elements. [Apply (1) to the ideal $\mathfrak{a}/aA$ of A/aA for any nonzero element $a \in \mathfrak{a}$.]

Exercise 3.14. Let K be a number field and let $A = \mathscr{O}_K$. Prove that there exists $f \in A \setminus \{0\}$ such that $A_f := \{1, f, f^2, \ldots\}^{-1}A$ is a principal ideal domain. [Choose f to kill all elements of the class group of A.]

Exercise 3.15. Generalize Lemma 3.9 as follows. Let A be a semi-local Dedekind domain with fraction field F, let K/F be a finite separable extension, and let B be the integral closure of A in K. Show B is semi-local.

Exercise 3.16. Suppose that there were finitely many prime numbers. Use Exercise 3.15 to prove that $\mathbf{Z}[\sqrt{-5}]$ is a PID, and derive a contradiction. Thus there are infinitely many prime numbers.[2]

4. The relative ideal norm. In this section we fix a Dedekind domain A with fraction field F. Let K/F be a finite separable extension of degree n, and let B be the integral closure of A in K. For a nonzero ideal $\mathfrak{b} \subset B$ we will define its relative norm $\mathrm{N}_{B/A}(\mathfrak{b})$, which is an ideal of A. This will generalize the (absolute) ideal norm $\mathrm{N}(\mathfrak{b})$ defined when $A = \mathbf{Z}$, and it will also generalize the norm of an element $\mathrm{N}_{K/F}(x)$ for $x \in B$. See Remark 4.2 and Proposition 4.4.

By Proposition 1.3, B is a Dedekind domain and a finitely generated A-module, and for every maximal ideal $\mathfrak{q} \subset B$, the contraction $\mathfrak{p} := \mathfrak{q} \cap A$ is a maximal ideal. Hence $A/\mathfrak{p}$ is a subfield of $B/\mathfrak{q}$. Any set of generators for B as an A-module also generates $B/\mathfrak{q}$ as a vector space over $A/\mathfrak{p}$, so the degree $[B/\mathfrak{q} : A/\mathfrak{p}]$ is finite.

Definition 4.1. Let $\mathfrak{b} = \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{b})}$ be a nonzero ideal of B. The *relative ideal norm* of $\mathfrak{b}$ is defined to be
$$\mathrm{N}_{B/A}(\mathfrak{b}) := \prod_{\mathfrak{q}} (\mathfrak{q} \cap A)^{[B/\mathfrak{q}:A/\mathfrak{p}]\, v_{\mathfrak{q}}(\mathfrak{b})},$$
where $\mathfrak{p} = \mathfrak{q} \cap A$.

For ideals $\mathfrak{b}, \mathfrak{b}' \subset B$, we have $\mathrm{N}_{B/A}(\mathfrak{b}\mathfrak{b}') = \mathrm{N}_{B/A}(\mathfrak{b})\,\mathrm{N}_{B/A}(\mathfrak{b}')$ since $v_{\mathfrak{q}}(\mathfrak{b}\mathfrak{b}') = v_{\mathfrak{q}}(\mathfrak{b}) + v_{\mathfrak{q}}(\mathfrak{b}')$.

[2] Brian Conrad attributes this ridiculous proof to Larry Washington.

Remark 4.2. Suppose that $A = \mathbf{Z}$, so $F = \mathbf{Q}$ and K is a number field with ring of integers $B = \mathscr{O}_K$. The *absolute ideal norm* $\mathrm{N}(\mathfrak{b})$ of a nonzero ideal $\mathfrak{b} \subset B$ is defined to be the (finite) number of elements of the quotient ring, i.e. $\mathrm{N}(\mathfrak{b}) := \#(B/\mathfrak{b})$. We claim that

$$\mathrm{N}_{B/\mathbf{Z}}(\mathfrak{b}) = \mathrm{N}(\mathfrak{b})\mathbf{Z}. \tag{4.3}$$

The absolute ideal norm is multiplicative in $\mathfrak{b}$ by [Samuel, Proposition 3.5.2], so it suffices to prove $\mathrm{N}(\mathfrak{q})\mathbf{Z} = \mathrm{N}_{B/\mathbf{Z}}(\mathfrak{q}) = (\mathfrak{q} \cap \mathbf{Z})^{[B/\mathfrak{q}\,:\,\mathbf{Z}/\mathfrak{q}\cap\mathbf{Z}]}$ for $\mathfrak{q} \subset B$ prime. But it is easily verified that

$$\mathrm{N}(\mathfrak{q}) = \#(B/\mathfrak{q}) = p^{[B/\mathfrak{q}\,:\,\mathbf{F}_p]},$$

where $\mathfrak{q} \cap \mathbf{Z} = p\mathbf{Z}$.

The following proposition says that the relative ideal norm is compatible with the norm of an element. It is surprising because the two kinds of norm are defined in completely different ways: indeed, the norm of an element b is defined as the determinant of multiplication by b.

Proposition 4.4. *Let $b \in B \setminus \{0\}$. Then $\mathrm{N}_{B/A}(bB) = \mathrm{N}_{K/F}(b)A$.*

In order to prove Proposition 4.4, we first need to show that the relative ideal norm is compatible with localizations.

Lemma 4.5. *Let S be a multiplicatively closed subset of A, let $A' := S^{-1}A$, and let $B' := S^{-1}B$. Then for every nonzero ideal $\mathfrak{b} \subset B$, we have*

$$\mathrm{N}_{B/A}(\mathfrak{b})A' = \mathrm{N}_{B'/A'}(\mathfrak{b}B').$$

Proof. As norms and extensions are both multiplicative in $\mathfrak{b}$, we may assume $\mathfrak{b} = \mathfrak{q}$ is prime. Let $\mathfrak{p} = \mathfrak{q} \cap A$, and note that $\mathfrak{p} \cap S = \mathfrak{q} \cap S$ because $S \subset A$. If $\mathfrak{q} \cap S \neq \emptyset$ then $\mathfrak{q}B' = B'$, so $\mathrm{N}_{B'/A'}(\mathfrak{q}B') = A'$. In this case, $\mathfrak{p} \cap S \neq \emptyset$ as well, so $\mathfrak{p}A' = A'$, and

$$\mathrm{N}_{B/A}(\mathfrak{q})A' = \mathfrak{p}^{[B/\mathfrak{q}:A/\mathfrak{p}]}A' = (\mathfrak{p}A')^{[B/\mathfrak{q}:A/\mathfrak{p}]} = A'.$$

Now suppose $\mathfrak{q} \cap S = \mathfrak{p} \cap S = \emptyset$. Then $B/\mathfrak{q} = B'/(\mathfrak{q}B')$ and $A/\mathfrak{p} = A'/\mathfrak{p}A'$ by [Samuel, Proposition 5.2.5]. Moreover,

$$((\mathfrak{q}B') \cap A') \cap A = (\mathfrak{q}B') \cap A = ((\mathfrak{q}B') \cap B) \cap A = \mathfrak{q} \cap A = \mathfrak{p},$$

so $(\mathfrak{q}B') \cap A' = \mathfrak{p}A'$ because they contract to the same ideal of A. Hence we have a commutative square

$$\begin{tikzcd}
A/\mathfrak{p} \arrow[r, hook] \arrow[d, "\cong"'] & B/\mathfrak{q} \arrow[d, "\cong"] \\
A'/\mathfrak{p}A' \arrow[r, hook] & B'/\mathfrak{q}B'
\end{tikzcd}$$

so $[B/\mathfrak{q} : A/\mathfrak{p}] = [B'/\mathfrak{q}B' : A'/\mathfrak{p}A']$. It follows that

$$\mathrm{N}_{B/A}(\mathfrak{q})A' = \mathfrak{p}^{[B/\mathfrak{q}\,:\,A/\mathfrak{p}]}A' = (\mathfrak{p}A')^{[B'/\mathfrak{q}B'\,:\,A'/\mathfrak{p}A']} = \mathrm{N}_{B'/A'}(\mathfrak{q}B').$$

□

Proof of Proposition 4.4. By Lemma 3.10, it suffices to check that for all nonzero prime ideals $\mathfrak{p} \subset A$, we have $\mathrm{N}_{B/A}(bB)A_{\mathfrak{p}} = \mathrm{N}_{K/F}(b)A_{\mathfrak{p}}$. Lemma 4.5 gives that $\mathrm{N}_{B/A}(bB)A_{\mathfrak{p}} = \mathrm{N}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}(bB_{\mathfrak{p}})$, so we may replace A by $A_{\mathfrak{p}}$ and B by $B_{\mathfrak{p}}$ to assume A is a discrete valuation ring. Thus A and B are principal ideal domains by Lemmas 3.8 and 3.9. As ideal and element norms are multiplicative, and since B is a unique factorization domain, it suffices to show that $\mathrm{N}_{B/A}(qB) = \mathrm{N}_{K/F}(q)A$ for $q \in B$ a *prime* element. The contraction $(qB) \cap A$ is the unique maximal ideal of A; let p be a generator. By the classification of finitely generated modules over a PID, we have

$$B/qB \cong A/p^{e_1}A \times \cdots \times A/p^{e_r}A \tag{4.6}$$

for some $1 \le e_1 \le e_2 \le \cdots \le e_r$, since pA is the only maximal ideal of A. But $p \in qB$, so p annihilates B/qB, so $e_1 = \ldots = e_r = 1$, and $B/qB \cong (A/pA)^r$. This means that B/qB is an r-dimensional A/pA-vector space, so by definition, $\mathrm{N}_{B/A}(pB) = (pA)^r = p^r A$. On the other hand, equation (4.6) shows that the Smith normal form for the multiplication-by-q homomorphism $m_q \colon B \to B$ is the diagonal matrix

$$\begin{bmatrix} p & & & & & \\ & \ddots & & & & \\ & & p & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}$$

with r diagonal entries being p and the rest being 1. Hence $\mathrm{N}_{K/F}(p) = \det(m_q) = p^r$, up to units. □

Exercise 4.7. Let $\mathfrak{b}, \mathfrak{b}'$ be nonzero ideals of B, with $\mathfrak{b} \mid \mathfrak{b}'$. Show that $\mathrm{N}_{B/A}(\mathfrak{b}) \mid \mathrm{N}_{B/A}(\mathfrak{b}')$, and that if $\mathrm{N}_{B/A}(\mathfrak{b}) = \mathrm{N}_{B/A}(\mathfrak{b}')$ then $\mathfrak{b} = \mathfrak{b}'$.

Exercise 4.8. Let $\mathfrak{b}$ be a nonzero ideal of B.

(1) Prove that
$$\mathrm{N}_{B/A}(\mathfrak{b}) = \big(\mathrm{N}_{K/F}(x) \mid x \in \mathfrak{b}\big).$$
[Localize at a nonzero prime ideal of A.]

(2) Prove by example that $\mathrm{N}_{B/A}(\mathfrak{b})$ is not necessarily generated by the norms of a given set of generators for $\mathfrak{b}$. [Take $\mathfrak{b} = B$, and suppose that there are two distinct nonzero prime ideals of B which contract to the same ideal of A.]

Exercise 4.9. Let L/K be a finite separable extension and let C be the integral closure of B (or A) in L. Prove that for any nonzero ideal $\mathfrak{c} \subset C$, we have

$$\mathrm{N}_{B/A}\big(\mathrm{N}_{C/B}(\mathfrak{c})\big) = \mathrm{N}_{C/A}(\mathfrak{c}).$$

[It is tempting to use Exercise 4.8(1), but this does not work because of Exercise 4.8(2).]

Exercise 4.10. Let $\mathfrak{a}$ be a nonzero ideal of A. Prove that

$$\mathrm{N}_{B/A}(\mathfrak{a}B) = \mathfrak{a}^{[K:F]}.$$

[Localize to reduce to the case where $\mathfrak{a}$ is principal.]

Exercise 4.11. Suppose that K/F is Galois with Galois group $G = \mathrm{Gal}(K/F)$. Note that $\sigma(B) = B$ for all $\sigma \in G$. Prove that for a nonzero ideal $\mathfrak{b} \subset B$,

$$\mathrm{N}_{B/A}(\mathfrak{b})B = \prod_{\sigma \in G} \sigma(\mathfrak{b}).$$

[The left side is included in the right by Exercise 4.8. Take norms of both sides.]

Remark 4.12. Suppose that $F = \mathbf{Q}$ and $A = \mathbf{Z}$, and that K/F is Galois with Galois group $G = \mathrm{Gal}(K/F)$. By Exercise 4.11 and Remark 4.2, for any nonzero ideal $\mathfrak{b} \subset B = \mathscr{O}_K$, we have

$$\mathrm{N}(\mathfrak{b})\mathscr{O}_K = \prod_{\sigma \in G} \sigma(\mathfrak{b}),$$

where $\mathrm{N}(\mathfrak{b}) = \#(\mathscr{O}_K/\mathfrak{b}) \in \mathbf{Z}_{\geq 1}$ is the absolute ideal norm. This useful observation gives a concrete formula for the inverse fractional ideal:

$$\mathfrak{b}^{-1} = \frac{1}{\mathrm{N}(\mathfrak{b})} \prod_{\sigma \neq 1} \sigma(\mathfrak{b}).$$

The situation becomes particularly simple when $K = \mathbf{Q}(\sqrt{d})$ is a quadratic extension of $\mathbf{Q}$. In this case $K/\mathbf{Q}$ is automatically Galois, with $\mathrm{Gal}(K/\mathbf{Q}) = \{1, \tau\}$, where $\tau(\sqrt{d}) = -\sqrt{d}$. Writing $\bar{\mathfrak{b}} = \tau(\mathfrak{b})$ for a nonzero ideal $\mathfrak{b} \subset \mathscr{O}_K$, we obtain

$$\mathrm{N}(\mathfrak{b})\mathbf{Z} = \mathfrak{b}\bar{\mathfrak{b}}.$$

5. The discriminant. In this section we fix a Dedekind domain A with fraction field F. Let K/F be a finite separable extension of degree n, and let B be the integral closure of A in K. By Proposition 1.3, B is a Dedekind domain with fraction field K, and B is an A-submodule of a free A-module of rank n. However, if A is not a principal ideal domain then B may not itself be a free A-module, so that we cannot use (1.2) to define the discriminant $\mathscr{D}_{B/A}$. We will use localizations in order to *define* the discriminant $\mathscr{D}_{B/A}$ in this case.

By Proposition 3.1(1), for any prime ideal $\mathfrak{p} \subset A$, the integral closure of $A_\mathfrak{p}$ in K is $B_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}B$. Since $A_\mathfrak{p}$ is a principal ideal domain, $B_\mathfrak{p}$ is a *free* $A_\mathfrak{p}$-module of rank n, so the discriminant ideal $\mathscr{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$ of (1.2) is a well-defined nonzero ideal of $A_\mathfrak{p}$. Since $A_\mathfrak{p}$ has only one maximal ideal $\mathfrak{p}A_\mathfrak{p}$, the prime factorization of $\mathscr{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$ has the form

$$\mathscr{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = (\mathfrak{p}A_\mathfrak{p})^{n_\mathfrak{p}(B)} \tag{5.1}$$

for a unique nonnegative integer $n_\mathfrak{p}(B)$.

Lemma 5.2. *We have $n_\mathfrak{p}(B) = 0$ for all but finitely many $\mathfrak{p}$.*

Proof. Since $\mathrm{Frac}(B) = K$, by clearing denominators we can find an F-basis $y_1, \dots, y_n$ for K contained in B. Let $d = D(y_1, \dots, y_n) \in A$. It is enough to show that $n_\mathfrak{p}(B) \leq v_\mathfrak{p}(d)$ for all $\mathfrak{p}$, since the latter is zero for all but finitely many $\mathfrak{p}$. For any prime ideal $\mathfrak{p}$, we have $y_1, \dots, y_n \in B \subset B_\mathfrak{p}$. Let $x_1, \dots, x_n$ be an $A_\mathfrak{p}$-basis for $B_\mathfrak{p}$, and let M be the unique matrix with entries in $A_\mathfrak{p}$ such that $Mx_i = y_i$. Then $\det(M) \in A_\mathfrak{p}$ and

$$d = D(y_1, \dots, y_n) = D(Mx_1, \dots, Mx_n) = \det(M)^2 D(x_1, \dots, x_n)$$

by (1.1). Thus $d \in \mathscr{D}_{B_\mathfrak{p}/A_\mathfrak{p}}$, and $\mathscr{D}_{B_\mathfrak{p}/A_\mathfrak{p}} \mid dA_\mathfrak{p}$. It follows from Lemma 3.2 that $dA_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^{v_\mathfrak{p}(d)}$, and by definition $\mathscr{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = (\mathfrak{p}A_\mathfrak{p})^{n_\mathfrak{p}(B)}$, so $n_\mathfrak{p}(B) \le v_\mathfrak{p}(d)$, as desired. □

Definition 5.3. Let A be a Dedekind domain with fraction field F, let K/F be a finite separable extension of degree n, and let B be the integral closure of A in K. The *discriminant ideal* of B/A is defined to be

$$\mathscr{D}_{B/A} := \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}(B)} \subset A, \tag{5.4}$$

where the product is taken over all nonzero prime ideals of A, and where $n_\mathfrak{p}(B)$ is defined in (5.1).

This product has only finitely many factors by Lemma 5.2. If B happens to be a free A-module, we have now made *two* a priori different definitions of $\mathscr{D}_{B/A}$ in (1.2) and (5.4). The following lemma implies that they are compatible.

Lemma 5.5. *Suppose that B is a free A-module, with A-basis $x_1, \dots, x_n$. Then for all nonzero prime ideals $\mathfrak{p} \subset A$, we have*

$$n_\mathfrak{p}(B) = v_\mathfrak{p}\big(D(x_1, \dots, x_n)\big).$$

Proof. We claim that $x_1, \dots, x_n$ are an $A_\mathfrak{p}$-basis of $B_\mathfrak{p}$ for any nonzero prime ideal $\mathfrak{p} \subset A$. Indeed, the x_i are $A_\mathfrak{p}$-linearly independent (as they are K-linearly independent by Proposition 1.3(5)), and clearly $x_1, \dots, x_n \in B_\mathfrak{p}$, so we only need to show $B_\mathfrak{p} \subset A_\mathfrak{p}x_1 + \cdots + A_\mathfrak{p}x_n$. Let $b/s \in B_\mathfrak{p}$, where $b \in B$ and $s \notin \mathfrak{p}$. Then there exist $a_1, \dots, a_n \in A$ such that $b = \sum_{i=1}^n a_i x_i$, so

$$\frac{b}{s} = \frac{1}{s}\sum_{i=1}^n a_i x_i = \sum_{i=1}^n \frac{a_i}{s} x_i \in A_\mathfrak{p}x_1 + \cdots + A_\mathfrak{p}x_n,$$

as claimed.

It follows that

$$(\mathfrak{p}A_\mathfrak{p})^{n_\mathfrak{p}(B)} = \mathscr{D}_{B_\mathfrak{p}/A_\mathfrak{p}} = D(x_1, \dots, x_n)A_\mathfrak{p},$$

so $n_\mathfrak{p}(B) = v_\mathfrak{p}(D(x_1, \dots, x_n))$ by Lemma 3.2. □

Remark 5.6. Suppose that B/A is a *monogenic* extension, i.e. that there exists $x \in B$ such that $B = A[x]$. Then $1, x, x^2, \dots, x^{n-1}$ is an A-basis for B, so $\mathscr{D}_{B/A} = D(1, x, x^2, \dots, x^{n-1})A$. Hence if $\mathscr{D}_{B/A}$ is not a principal ideal, then A is not a PID and B/A is not monogenic. These conditions are commonly satisfied for number fields, but it takes work to write down an explicit example where $\mathscr{D}_{B/A}$ is not principal.

In order to prove the discriminants in towers formula (6.2), we will (not surprisingly) reduce to the case where A is a PID by localizing. Hence we will need to know that discriminants are compatible with localizations, as the following lemma shows. Compare with Lemma 4.5.

Lemma 5.7. *Let $S \subset A \setminus \{0\}$ be a multiplicatively closed subset, let $A' = S^{-1}A$, and let $B' := S^{-1}B$. Then $\mathscr{D}_{B'/A'} = \mathscr{D}_{B/A}A'$.*

Proof. This amounts to showing that for every nonzero prime ideal $\mathfrak{p}$ of A such that $\mathfrak{p}\cap S = \emptyset$, we have $n_{\mathfrak{p}}(B) = n_{\mathfrak{p}'}(B')$, where $\mathfrak{p}' = \mathfrak{p}A'$. Observe that

$$\begin{aligned} A'_{\mathfrak{p}'} &= \left\{ \frac{a/s}{b/t} \mid a, b, s, t \in A,\ s, t \notin \mathfrak{p},\ \frac{b}{t} \notin \mathfrak{p}' \right\} \\ &= \left\{ \frac{at}{bs} \mid a, b, s, t \in A,\ b, s, t \notin \mathfrak{p} \right\} = A_{\mathfrak{p}}, \end{aligned}$$

where $b/t \notin \mathfrak{p}'$ if and only if $b \notin \mathfrak{p}$ by Exercise 2.2(2). Similarly, $B'_{\mathfrak{p}'} = B_{\mathfrak{p}}$, so

$$(\mathfrak{p}A_{\mathfrak{p}})^{n_{\mathfrak{p}}(B)} = \mathscr{D}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}} = \mathscr{D}_{B'_{\mathfrak{p}'}/A'_{\mathfrak{p}'}} = (\mathfrak{p}'A'_{\mathfrak{p}'})^{n_{\mathfrak{p}'}(B')}.$$

□

Exercise 5.8. Prove that

$$\mathscr{D}_{B/A} = \big(D(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in B\big).$$

[Compare to Exercise 4.8.]

Exercise 5.9. Let $B' \subset B$ be a subring which is a free A-module of rank $n = [K : F]$. Prove that $\mathscr{D}_{B/A} \mid \mathscr{D}_{B'/A}$.

6. Discriminants in towers. We are now in a position to state and prove the discriminants in towers formula.

Theorem 6.1 (Discriminants in towers)**.** *Let A be a Dedekind domain with fraction field F. Let K/F and L/K be finite separable extensions, and let B (resp. C) be the integral closure of A in K (resp. L). Then we have an equality of ideals of A:*

$$\mathscr{D}_{C/A} = \mathrm{N}_{B/A}\big(\mathscr{D}_{C/B}\big) \cdot \mathscr{D}_{B/A}^{[L:K]}. \tag{6.2}$$

We will localize to reduce the proof of Theorem 6.1 to the case when A and B are both PIDs. In this case, the discriminant and norm ideals in (6.2) are principal, so we can work on the level of *elements*. This then becomes a matrix determinant calculation, carried out in Proposition 6.3 below.

Proposition 6.3. *Let F be a field, and let K/F and L/K be finite separable extensions of degrees n and m, respectively. Let $x_1, \ldots, x_n$ be an F-basis for K and let $y_1, \ldots, y_m$ be a K-basis for L, so $\{x_i y_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is an F-basis for L. Then*

$$D_{L/F}(x_1 y_1, \ldots, x_n y_m) = \mathrm{N}_{K/F}\big(D_{L/K}(y_1, \ldots, y_m)\big) \cdot D_{K/F}(x_1, \ldots, x_n)^m. \tag{6.4}$$

Proof. Fix an algebraic closure C of F. Let $\sigma_1, \ldots, \sigma_n \colon K \to C$ be the distinct F-homomorphisms. For $i = 1, \ldots, n$ let $\tau_{i1}, \ldots, \tau_{im} \colon L \to C$ be the distinct embeddings restricting to σ_i on K. Then $\{\tau_{ij} \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is the complete set of F-embeddings of L into C.

Define the following matrices with entries in C:

$$\begin{aligned} S &= (\sigma_i x_j)_{i,j=1}^{n} \\ T_k &= (\tau_{ki} y_j)_{i,j=1}^{m} \qquad (k = 1, \ldots, n) \\ M &= (\tau_{ij}(x_k y_\ell))_{(i,j),(k,l)=(1,1)}^{(n,m)}. \end{aligned}$$

Here and below we order the pairs (i,j) lexicographically. By [Samuel, Proposition 2.7.3], we have

$$\begin{aligned} D_{K/F}(x_1,\dots,x_n) &= \det(S)^2 \\ \sigma_k D_{L/K}(y_1,\dots,y_m) &= \det(T_k)^2 \\ D_{L/F}(x_1y_1,\dots,x_ny_m) &= \det(M)^2. \end{aligned}$$

Let I_m be the $m \times m$ identity matrix. We have $\tau_{ij}(x_k y_\ell) = \sigma_i(x_k)\tau_{ij}(y_\ell)$ because $x_k \in K$, so we can write M in block form as

$$\begin{aligned} M &= \begin{bmatrix} (\sigma_1 x_1)T_1 & (\sigma_1 x_2)T_1 & \cdots & (\sigma_1 x_n)T_1 \\ (\sigma_2 x_1)T_2 & (\sigma_2 x_2)T_2 & \cdots & (\sigma_2 x_n)T_2 \\ \vdots & \vdots & \ddots & \vdots \\ (\sigma_n x_1)T_n & (\sigma_n x_2)T_n & \cdots & (\sigma_n x_n)T_n \end{bmatrix} \\ &= \begin{bmatrix} T_1 & 0 & \cdots & 0 \\ 0 & T_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & T_n \end{bmatrix} \cdot \begin{bmatrix} (\sigma_1 x_1)I_m & (\sigma_1 x_2)I_m & \cdots & (\sigma_1 x_n)I_m \\ (\sigma_2 x_1)I_m & (\sigma_2 x_2)I_m & \cdots & (\sigma_2 x_n)I_m \\ \vdots & \vdots & \ddots & \vdots \\ (\sigma_n x_1)I_m & (\sigma_n x_2)I_m & \cdots & (\sigma_n x_n)I_m \end{bmatrix}. \end{aligned} \tag{6.5}$$

The square of the determinant of the first matrix in the product (6.5) is

$$\begin{aligned} \det(T_1)^2 \cdots \det(T_n)^2 &= \sigma_1\big(D_{L/K}(y_1,\dots,y_m)\big) \cdots \sigma_n\big(D_{L/K}(y_1,\dots,y_m)\big) \\ &= \mathrm{N}_{K/F}\left(D_{L/K}(y_1,\dots,y_m)\right). \end{aligned}$$

By performing a series of row and column exchanges, we transform the second matrix in the product (6.5) into the block matrix

$$\begin{bmatrix} S & 0 & \cdots & 0 \\ 0 & S & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & S \end{bmatrix}.$$

Hence the square of the determinant of the second matrix is

$$(\det(S)^2)^m = D_{K/F}(x_1,\dots,x_n)^m.$$

Taking products yields (6.4). □

Example 6.6. Let us illustrate the proof of Proposition 6.3 by taking $n = m = 2$. In this case,

$$\begin{aligned}
M &= \begin{bmatrix} \sigma_1 x_1 \tau_{11} y_1 & \sigma_1 x_1 \tau_{11} y_2 & \sigma_1 x_2 \tau_{11} y_1 & \sigma_1 x_2 \tau_{11} y_2 \\ \sigma_1 x_1 \tau_{12} y_1 & \sigma_1 x_1 \tau_{12} y_2 & \sigma_1 x_2 \tau_{12} y_1 & \sigma_1 x_2 \tau_{12} y_2 \\ \sigma_2 x_1 \tau_{21} y_1 & \sigma_2 x_1 \tau_{21} y_2 & \sigma_2 x_2 \tau_{21} y_1 & \sigma_2 x_2 \tau_{21} y_2 \\ \sigma_2 x_1 \tau_{22} y_1 & \sigma_2 x_1 \tau_{22} y_2 & \sigma_2 x_2 \tau_{22} y_1 & \sigma_2 x_2 \tau_{22} y_2 \end{bmatrix} \\
&= \begin{bmatrix} \tau_{11} y_1 & \tau_{11} y_2 & 0 & 0 \\ \tau_{12} y_1 & \tau_{12} y_2 & 0 & 0 \\ 0 & 0 & \tau_{21} y_1 & \tau_{21} y_2 \\ 0 & 0 & \tau_{22} y_1 & \tau_{22} y_2 \end{bmatrix} \cdot \begin{bmatrix} \sigma_1 x_1 & 0 & \sigma_1 x_2 & 0 \\ 0 & \sigma_1 x_1 & 0 & \sigma_1 x_2 \\ \sigma_2 x_1 & 0 & \sigma_2 x_2 & 0 \\ 0 & \sigma_2 x_1 & 0 & \sigma_2 x_2 \end{bmatrix} \\
&= \begin{bmatrix} T_1 & 0 \\ 0 & T_2 \end{bmatrix} \cdot \begin{bmatrix} (\sigma_1 x_1) I_2 & (\sigma_1 x_2) I_2 \\ (\sigma_2 x_1) I_2 & (\sigma_2 x_2) I_2 \end{bmatrix}.
\end{aligned}$$

By making one row exchange and one column exchange, we transform:

$$\begin{bmatrix} \sigma_1 x_1 & 0 & \sigma_1 x_2 & 0 \\ 0 & \sigma_1 x_1 & 0 & \sigma_1 x_2 \\ \sigma_2 x_1 & 0 & \sigma_2 x_2 & 0 \\ 0 & \sigma_2 x_1 & 0 & \sigma_2 x_2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} \sigma_1 x_1 & \sigma_1 x_2 & 0 & 0 \\ \sigma_2 x_1 & \sigma_2 x_2 & 0 & 0 \\ 0 & 0 & \sigma_1 x_1 & \sigma_1 x_2 \\ 0 & 0 & \sigma_2 x_1 & \sigma_2 x_2 \end{bmatrix}.$$

Proof of Theorem 6.1. By Lemma 3.10 it suffices to check that both sides of (6.2) extend to the same ideal in $A_\mathfrak{p}$ for all nonzero prime ideals $\mathfrak{p} \subset A$. By Lemmas 5.7 and 4.5, both sides of (6.2) are compatible with localizations, so we may replace A by $A_\mathfrak{p}$, B by $B_\mathfrak{p}$, and C by $C_\mathfrak{p}$ to assume A is a discrete valuation ring. Then A and B are PIDs by Lemmas 3.8 and 3.9, so B is a free A-module and C is a free B-module. Let $x_1, \ldots, x_n$ be an A-basis for B and $y_1, \ldots, y_m$ a B-basis for C. Then $\{x_i y_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$ is an A-basis for C, and

$$\begin{aligned}
\mathscr{D}_{C/A} &= D_{L/F}(x_1 y_1, \ldots, x_n y_m) A \\
\mathscr{D}_{C/B} &= D_{L/K}(y_1, \ldots, y_m) B \\
\mathscr{D}_{B/A} &= D_{K/F}(x_1, \ldots, x_n) A.
\end{aligned}$$

By Proposition 4.4,

$$\begin{aligned}
\mathrm{N}_{B/A}\big(\mathscr{D}_{C/B}\big) \cdot \mathscr{D}_{B/A}^{[L:K]} &= \mathrm{N}_{B/A}\big(D_{L/K}(y_1, \ldots, y_m) B\big) \cdot D_{K/F}(x_1, \ldots, x_n)^m A \\
&= \mathrm{N}_{K/F}\big(D_{L/K}(y_1, \ldots, y_m)\big) \cdot D_{K/F}(x_1, \ldots, x_n)^m A,
\end{aligned}$$

so the theorem follows from Proposition 6.3. □

Corollary 7. *With the notation in Theorem 6.1, we have* $\mathscr{D}_{B/A} \mid \mathscr{D}_{C/A}$.

8. Examples and applications. Here we present some situations in which Theorem 6.1 becomes useful. For a number field K we let $\mathrm{D}_K \in \mathbf{Z}$ denote the absolute discriminant, so $\mathscr{D}_{\mathscr{O}_K/\mathbf{Z}} = \mathrm{D}_K \mathbf{Z}$.

8.1. *Multiquadratic extensions of* $\mathbf{Q}$. Let $d_1, \ldots, d_r$ be squarefree integers, let

$$K = \mathbf{Q}\big(\sqrt{d_1}, \ldots, \sqrt{d_r}\big),$$

and let $F_i = \mathbf{Q}(\sqrt{d_i})$ for $i = 1, \ldots, r$. Then $F_i \subset K$ for each i, so by Corollary 7, we have $\mathrm{D}_{F_i} \mid \mathrm{D}_K$ for all i. The discriminant of a quadratic field is

$$\mathrm{D}_{F_i} = \begin{cases} d_i & \text{if } d \equiv 1 \mod 4, \\ 4d_i & \text{otherwise.} \end{cases} \tag{8.2}$$

Therefore $d_i \mid \mathrm{D}_K$ for each i.

Conversely, we claim that every prime factor of D_K divides $2d_1 \cdots d_r$. We proceed by induction on r, the case $r = 1$ being handled above. Suppose that the claim is true for r. Let $d = d_{r+1}$ be a squarefree integer and let $L = K(\sqrt{d})$, so we need to show that every prime factor of D_L divides $2d_1 \cdots d_r d$. If $L = K$ then we are done by the inductive hypothesis, so suppose $L \neq K$. Then $[L : K] = 2$, so the conjugates of $a + b\sqrt{d}$ over K are $a \pm b\sqrt{d}$. Thus

$$\mathrm{Tr}_{L/K}(1) = 2 \quad \mathrm{Tr}_{L/K}(d) = 2d \quad \mathrm{Tr}_{L/K}(\sqrt{d}) = \sqrt{d} - \sqrt{d} = 0,$$

where the first two identities hold since $1, d \in K$ and $[L : K] = 2$. We compute

$$D_{L/K}(1, \sqrt{d}) = \det\begin{bmatrix} \mathrm{Tr}_{L/K}(1) & \mathrm{Tr}_{L/K}(\sqrt{d}) \\ \mathrm{Tr}_{L/K}(\sqrt{d}) & \mathrm{Tr}_{L/K}(d) \end{bmatrix} = \det\begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d.$$

By Exercise 5.8, we have $4d = D_{L/K}(1, \sqrt{d}) \in \mathscr{D}_{\mathscr{O}_L/\mathscr{O}_K}$, so $\mathscr{D}_{\mathscr{O}_L/\mathscr{O}_K} \mid 4d\mathscr{O}_K$. Applying Theorem 6.1,

$$\begin{aligned} \mathrm{D}_{L/\mathbf{Q}}\,\mathbf{Z} = \mathscr{D}_{\mathscr{O}_L/\mathbf{Z}} &= \mathrm{N}_{\mathscr{O}_K/\mathbf{Z}}\big(\mathscr{D}_{\mathscr{O}_L/\mathscr{O}_K}\big)\,\mathscr{D}^2_{\mathscr{O}_K/\mathbf{Z}} \;\Big|\; \mathrm{N}_{\mathscr{O}_K/\mathbf{Z}}\big(4d\mathscr{O}_K\big)\,\mathscr{D}^2_{\mathscr{O}_K/\mathbf{Z}} \\ &= \mathrm{N}_{K/\mathbf{Q}}(4d)\,\mathscr{D}^2_{\mathscr{O}_K/\mathbf{Z}} = (4d)^{[K:\mathbf{Q}]}\,\mathscr{D}^2_{\mathscr{O}_K/\mathbf{Z}} = (4d)^{[K:\mathbf{Q}]}\,\mathrm{D}^2_{K/\mathbf{Q}}\,\mathbf{Z}, \end{aligned}$$

where we used Exercise 4.7 for $\mathrm{N}_{\mathscr{O}_K/\mathbf{Z}}\big(\mathscr{D}_{\mathscr{O}_L/\mathscr{O}_K}\big) \mid \mathrm{N}_{\mathscr{O}_K/\mathbf{Z}}\big(4d\mathscr{O}_K\big)$, and where $\mathrm{N}_{K/\mathbf{Q}}(4d) = (4d)^{[K:\mathbf{Q}]}$ because $4d \in K$. Hence $\mathrm{D}_{L/\mathbf{Q}} \mid (4d)^{[K:\mathbf{Q}]}\mathrm{D}^2_{K/\mathbf{Q}}$, so by induction, every prime factor of $\mathrm{D}_{L/\mathbf{Q}}$ divides $2d_1 \cdots d_r d$, as claimed. To summarize, we have proved:

Proposition 8.3. *Let $d_1, \ldots, d_r$ be squarefree integers, and let $K = \mathbf{Q}\big(\sqrt{d_1}, \ldots, \sqrt{d_r}\big)$. Then the odd prime factors of D_K are exactly the odd prime factors of $d_1 \cdots d_r$.*

Corollary 8.4. *Let $d_1, \ldots, d_r$ be squarefree integers, let $K = \mathbf{Q}\big(\sqrt{d_1}, \ldots, \sqrt{d_r}\big)$, and let d be a squarefree integer which has a prime factor p which is coprime to $2d_1 \cdots d_r$. Then d is not a square in K.*

Proof. If d were a square in K then $F = \mathbf{Q}(\sqrt{d}) \subset K$, so $\mathrm{D}_F \mid \mathrm{D}_K$ by Corollary 7. But $d \mid \mathrm{D}_F$ and $d \nmid \mathrm{D}_K$ by Proposition 8.3, since p is an odd prime dividing d but not $d_1 \cdots d_r$. This is a contradiction. □

For example, 13 is not a square in $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$.

8.5. *The quadratic subfield of* $\mathbf{Q}(\zeta_p)$. Let p be an odd prime and let ζ_p be a primitive pth root of unity. The minimal polynomial for ζ_p over $\mathbf{Q}$ is the p-cyclotomic polynomial

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

by [Samuel, §2.9]. In particular, $K = \mathbf{Q}(\zeta_p)$ has degree $p-1$ over $\mathbf{Q}$. Moreover, $\mathcal{O}_K = \mathbf{Z}[\zeta_p]$ by [Samuel, Theorem 2.9.2], so

$$\mathrm{D}_K = D(1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-2}) = \pm \mathrm{N}_{K/\mathbf{Q}}(\Phi_p'(\zeta_p))$$

by [Samuel, §2.8], where Φ_p' is the derivative of Φ_p. We have

$$\Phi_p'(X) = \frac{X^p - 1 - pX^{p-1}(X-1)}{(X-1)^2} = \frac{\Phi_p(X) - pX^{p-1}}{X-1}$$

and therefore

$$\begin{aligned} \mathrm{D}_K &= \pm \mathrm{N}_{K/\mathbf{Q}}\left(\frac{-p\zeta_p^{-1}}{\zeta_p - 1}\right) \\ &= \pm \mathrm{N}_{K/\mathbf{Q}}(-p)\, \mathrm{N}_{K/\mathbf{Q}}(\zeta_p)^{-1}\, \mathrm{N}_{K/\mathbf{Q}}(\zeta_p - 1)^{-1} \\ &= \pm p^{p-1} \cdot 1 \cdot p = \pm p^p, \end{aligned}$$

where we used $\mathrm{N}_{K/\mathbf{Q}}(\zeta_p) = 1$ and $\mathrm{N}_{K/\mathbf{Q}}(\zeta_p - 1) = \pm p$, as shown in [Samuel, §2.9].

The extension $K/\mathbf{Q}$ is Galois, being the splitting field of $X^p - 1$, and it has Galois group isomorphic to $(\mathbf{Z}/p\mathbf{Z})^\times$. This group is cyclic of order $p-1$, which is an even number. Therefore it admits a unique subgroup of index 2, so by the Galois correspondence, there is a unique subfield $F \subset K$ of degree two over $\mathbf{Q}$. As $F/\mathbf{Q}$ is quadratic, there is a unique squarefree integer d such that $F = \mathbf{Q}(\sqrt{d})$. By Corollary 7 we have $\mathrm{D}_F \mid \mathrm{D}_K = \pm p^p$, so $\mathrm{D}_F = \pm p$. But $2 \nmid \mathrm{D}_K$, so $\mathrm{D}_F \equiv 1 \mod 4$ and $d = \pm p = \mathrm{D}_F$ by (8.2). Observe that

$$p \equiv 1 \mod 4 \iff -p \equiv 3 \mod 4 \quad \text{and} \quad p \equiv 3 \mod 4 \iff -p \equiv 1 \mod 4,$$

so we have shown:

Proposition 8.6. *Let p be an odd prime. Then*

$$p \equiv 1 \mod 4 \implies \sqrt{p} \in \mathbf{Q}(\zeta_p) \quad \textit{and} \quad p \equiv 3 \mod 4 \implies \sqrt{-p} \in \mathbf{Q}(\zeta_p).$$