THE DIFFERENT IDEAL

KEITH CONRAD

1. Introduction

The discriminant of a number field K tells us which primes p in $\mathbf{Z}$ ramify in $\mathcal{O}_K$: the prime factors of the discriminant. However, the way we have seen how to compute the discriminant doesn't address the following themes:

(a) determine which prime ideals in $\mathcal{O}_K$ ramify (that is, which $\mathfrak{p}$ in $\mathcal{O}_K$ have $e(\mathfrak{p}|p) > 1$ rather than which p have $e(\mathfrak{p}|p) > 1$ for some $\mathfrak{p}$),
(b) determine the multiplicity of a prime in the discriminant. (We only know the multiplicity is positive for the ramified primes.)

Example 1.1. Let $K = \mathbf{Q}(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$. The polynomial $T^3 - T - 1$ has discriminant -23, which is squarefree, so $\mathcal{O}_K = \mathbf{Z}[\alpha]$ and we can detect how a prime p factors in $\mathcal{O}_K$ by seeing how $T^3 - T - 1$ factors in $\mathbf{F}_p[T]$. Since $\mathrm{disc}(\mathcal{O}_K) = -23$, only the prime 23 ramifies.

Since $T^3 - T - 1 \equiv (T-3)(T-10)^2 \bmod 23$, $(23) = \mathfrak{p}\mathfrak{q}^2$. One prime over 23 has multiplicity 1 and the other has multiplicity 2. The discriminant tells us some prime over 23 ramifies, but not which ones ramify. Only $\mathfrak{q}$ does.

The discriminant of K is, by definition, the determinant of the matrix $(\mathrm{Tr}_{K/\mathbf{Q}}(e_i e_j))$, where $e_1, \ldots, e_n$ is an arbitrary $\mathbf{Z}$-basis of $\mathcal{O}_K$. By a finer analysis of the trace, we will construct an ideal in $\mathcal{O}_K$ which is divisible precisely by the ramified primes in $\mathcal{O}_K$. This ideal is called the *different ideal*. (It is related to differentiation, hence the name I think.) In the case of Example 1.1, for instance, we will see that the different ideal is $\mathfrak{q}$, so the different singles out the particular prime over 23 that ramifies. While the discriminant lies downstairs in $\mathbf{Z}$, the different lies upstairs in $\mathcal{O}_K$. The ideal norm of the different is the absolute value of the discriminant, and this connection between the different and discriminant will tell us something about the multiplicity of primes in the discriminant. So the different ideal gives answers to both (a) and (b) above (only a partial answer in the case of (b)).

The main idea needed to construct the different ideal is to do something in number fields that is analogous to the classical notion of a dual lattice in Euclidean space. We will start off in Section 2 describing dual lattices in $\mathbf{R}^n$ and some of their basic properties. Armed with that intuition, we will meet the analogous construction in number fields in Section 3 and then construct the different ideal in Section 4.

2. The $\mathbf{Z}$-dual of a lattice in $\mathbf{R}^n$

In $\mathbf{R}^n$, the standard dot product gives a notion of orthogonal complement: when $V \subset \mathbf{R}^n$ is a subspace, we set

$$V^\perp = \{w \in \mathbf{R}^n : w \perp V\} = \{w \in \mathbf{R}^n : w \cdot V = 0\}.$$

Then $\mathbf{R}^n = V \oplus V^\perp$, $V^{\perp\perp} = V$, and $V_1 \subset V_2 \iff V_2^\perp \subset V_1^\perp$.

A *lattice* in $\mathbf{R}^n$ is, by definition, the $\mathbf{Z}$-span of a basis of $\mathbf{R}^n$.[1] The standard lattice is $\mathbf{Z}^n$, for instance. There is a concept for lattices in $\mathbf{R}^n$ somewhat like the orthogonal complement of a subspace.

Definition 2.1. For a lattice $L \subset \mathbf{R}^n$ its $\mathbf{Z}$-*dual* is

$$L^\vee = \{w \in \mathbf{R}^n : w \cdot L \subset \mathbf{Z}\}.$$

This $\mathbf{Z}$-dual of a lattice is *not* an orthogonal complement. The condition for a vector to lie in the $\mathbf{Z}$-dual of L is to have integral dot product against all elements of L, not to have dot product 0 against all elements of L.[2] Some similarities with properties of orthogonal complements will be seen in Corollary 2.7.

If $e_1, \ldots, e_n$ is a $\mathbf{Z}$-basis of L, then to have $w \cdot v \in \mathbf{Z}$ for all $v \in L$ it suffices to check $w \cdot e_i \in \mathbf{Z}$ for $i = 1, \ldots, n$ since every element of L is a $\mathbf{Z}$-linear combination of the e_i's. Here are three examples of dual lattices in $\mathbf{R}^2$.

Example 2.2. Let $L = \mathbf{Z}^2 = \mathbf{Z}\binom{1}{0} + \mathbf{Z}\binom{0}{1}$. For $w \in \mathbf{R}^2$, $w \in L^\vee$ if and only if $w \cdot \binom{1}{0} \in \mathbf{Z}$ and $w \cdot \binom{0}{1} \in \mathbf{Z}$. Writing $w = \binom{a}{b}$, the two dot products are a and b, so $L^\vee = \mathbf{Z}^2 = L$. The lattice $\mathbf{Z}^2$ is "self-dual."

Example 2.3. Let $L = \mathbf{Z}\binom{1}{0} + \mathbf{Z}\binom{1}{2}$. Then $\binom{a}{b}$ is in $L^\vee$ when $a \in \mathbf{Z}$ and $a + 2b \in \mathbf{Z}$, which is equivalent to $a \in \mathbf{Z}$ and $b \in (1/2)\mathbf{Z}$, so $L^\vee = \mathbf{Z}\binom{1}{0} + \mathbf{Z}\binom{0}{1/2}$.

Example 2.4. Let $L = \mathbf{Z}\binom{2}{1} + \mathbf{Z}\binom{1}{3}$. To say $\binom{a}{b} \in L^\vee$ is equivalent to $2a + b \in \mathbf{Z}$ and $a + 3b \in \mathbf{Z}$. The system of equations

$$\begin{aligned} 2a + b &= x \\ a + 3b &= y \end{aligned}$$

is equivalent to

$$\begin{aligned} a &= \frac{3}{5}x - \frac{1}{5}y \\ b &= -\frac{1}{5}x + \frac{2}{5}y, \end{aligned}$$

so

$$\binom{a}{b} = x\binom{3/5}{-1/5} + y\binom{-1/5}{2/5}.$$

Thus $L^\vee = \mathbf{Z}\binom{3/5}{-1/5} + \mathbf{Z}\binom{-1/5}{2/5}$.

Theorem 2.5. *If $L = \bigoplus_{i=1}^n \mathbf{Z}e_i$ is a lattice in $\mathbf{R}^n$ then its $\mathbf{Z}$-dual is $L^\vee = \bigoplus_{i=1}^n \mathbf{Z}e_i^\vee$, where $\{e_i^\vee\}$ is the dual basis to $\{e_i\}$ relative to the dot product on $\mathbf{R}^n$: $e_i \cdot e_j^\vee = \delta_{ij}$. In particular, $L^\vee$ is a lattice.*

Proof. For $w \in \mathbf{R}^n$, write it in the dual basis $\{e_1^\vee, \ldots, e_n^\vee\}$ as $w = \sum_{i=1}^n c_i e_i^\vee$. Then $w \cdot e_i = c_i$, so to say $w \in L^\vee$ is equivalent to the coefficients c_i being integers. Therefore $L^\vee$ is the $\mathbf{Z}$-span of the $e_i^\vee$'s. □

[1] Topologically, the lattices in $\mathbf{R}^n$ are the subgroups Λ such that Λ is discrete and $\mathbf{R}^n/\Lambda$ is compact.

[2] The $\mathbf{Z}$-dual is the dual space of L as a $\mathbf{Z}$-module: every $\mathbf{Z}$-linear map $L \to \mathbf{Z}$ has the form $v \mapsto w \cdot v$ for a unique $w \in L^\vee$.

Example 2.6. Let $L = \mathbf{Z}\binom{1}{0} + \mathbf{Z}\binom{1}{2}$, as in Example 2.3. The dual basis to $\binom{1}{0}$ and $\binom{1}{2}$ is $\binom{1}{-1/2}$ and $\binom{0}{1/2}$, so by Theorem 2.5, $L^\vee = \mathbf{Z}\binom{1}{-1/2} + \mathbf{Z}\binom{0}{1/2}$. If we do a change of basis, replacing $\binom{1}{-1/2}$ with $\binom{1}{-1/2} + \binom{0}{1/2} = \binom{1}{0}$ and keeping $\binom{0}{1/2}$ then we recover the spanning set for $L^\vee$ in Example 2.3.

Corollary 2.7. *For lattices in $\mathbf{R}^n$, the following properties hold:*

(1) $L^{\vee\vee} = L$,
(2) $L_1 \subset L_2 \iff L_2^\vee \subset L_1^\vee$,
(3) $(L_1 + L_2)^\vee = L_1^\vee \cap L_2^\vee$,
(4) $(L_1 \cap L_2)^\vee = L_1^\vee + L_2^\vee$.

Proof. (1): Theorem 2.5 and double duality of vector spaces tells us $L^{\vee\vee} = L$ since the dual basis of a dual basis is the original basis, whose $\mathbf{Z}$-span is the original lattice.

(2): It is easy to see from the definitions that if $L_1 \subset L_2$ then $L_2^\vee \subset L_1^\vee$. Applying this to the inclusion $L_2^\vee \subset L_1^\vee$ gives us $L_1^{\vee\vee} \subset L_2^{\vee\vee}$, so $L_1 \subset L_2$.

(3): If $v \in (L_1 + L_2)^\vee$ then v has integral dot product with each vector in $L_1 + L_2$, and hence with each vector in L_1 and each vector in L_2. Thus $v \in L_1^\vee$ and $v \in L_2^\vee$, so $v \in L_1^\vee \cap L_2^\vee$. We have shown $(L_1 + L_2)^\vee \subset L_1^\vee \cap L_2^\vee$. The reverse inclusion is just as easy to check.

(4): Rather than directly verify that $(L_1 \cap L_2)^\vee = L_1^\vee + L_2^\vee$, we will check the two sides are equal by checking their dual lattices are equal. That means, by double duality, we want to check $L_1 \cap L_2 = (L_1^\vee + L_2^\vee)^\vee$. From (3), $(L_1^\vee + L_2^\vee)^\vee = L_1^{\vee\vee} \cap L_2^{\vee\vee} = L_1 \cap L_2$, so we are done. □

One property of orthogonal complements that is not shared by dual lattices is $V \oplus V^\perp = \mathbf{R}^n$. The lattices L and $L^\vee$ are *not* complementary in the direct sum sense. Both a lattice and its dual lattice have rank n.

3. Lattices in Number Fields

The ideas about lattices in $\mathbf{R}^n$ will not literally be used, but they are the motivation for what we do now in number fields. Replace $\mathbf{R}^n$ and its dot product $(v, w) \mapsto v \cdot w$ with a number field K and the operation $(x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy)$ on it, which we'll call the *trace product*.[3] The trace product has values in $\mathbf{Q}$. Instead of being concerned with vectors having a *dot product in* $\mathbf{Z}$, we will look at algebraic numbers having a *trace product in* $\mathbf{Z}$.

Definition 3.1. In a number field K of degree n, a *lattice* in K is the $\mathbf{Z}$-span of a $\mathbf{Q}$-basis of K.

Examples of lattices in K include $\mathcal{O}_K$, fractional ideals, and orders.

Definition 3.2. Let L be a lattice in K. Its *dual lattice* is

$$L^\vee = \{\alpha \in K : \mathrm{Tr}_{K/\mathbf{Q}}(\alpha L) \subset \mathbf{Z}\}.$$

As with lattices in Euclidean space, where one can check membership in a dual lattice by checking the dot products with a basis of the lattice are all in $\mathbf{Z}$, to check $\alpha \in L^\vee$ it suffices to check its trace products with a basis of L are all in $\mathbf{Z}$: $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha e_i) \in \mathbf{Z}$ for some $\mathbf{Z}$-basis $e_1, \ldots, e_n$ of L.

[3]The usual term is trace pairing, not trace product. But since we're trying to emphasize the similarity to the dot product on $\mathbf{R}^n$, the term "trace product" seems helpful.

Example 3.3. Let $K = \mathbf{Q}(i)$ and $L = \mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i$. For $a + bi \in \mathbf{Q}(i)$, $a + bi \in L^\vee$ when $\mathrm{Tr}_{\mathbf{Q}(i)/\mathbf{Q}}(a+bi) \in \mathbf{Z}$ and $\mathrm{Tr}_{\mathbf{Q}(i)/\mathbf{Q}}((a+bi)i) \in \mathbf{Z}$. This is equivalent to $2a \in \mathbf{Z}$ and $-2b \in \mathbf{Z}$, so

$$\mathbf{Z}[i]^\vee = \frac{1}{2}\mathbf{Z} + \frac{1}{2}\mathbf{Z}i = \frac{1}{2}\mathbf{Z}[i].$$

Taking $L = (1+2i)\mathbf{Z}[i] = \mathbf{Z}(1+2i) + \mathbf{Z}(-2+i)$, calculations like those in Example 2.4 (but using trace products instead of dot products) lead to

$$L^\vee = \mathbf{Z}\left(\frac{1}{10} - \frac{i}{5}\right) + \mathbf{Z}\left(-\frac{1}{5} - \frac{i}{10}\right) = \mathbf{Z}\frac{1-2i}{10} + \mathbf{Z}\frac{-2-i}{10} = \frac{1-2i}{10}(\mathbf{Z} - \mathbf{Z}i) = \frac{1}{2(1+2i)}\mathbf{Z}[i].$$

This calculation shows a relation between the dual lattice and the inverse ideal. Writing $\mathfrak{a}$ for $L = (1+2i)$, an ideal, the calculation of $L^\vee$ says $\mathfrak{a}^\vee = \frac{1}{2}\mathfrak{a}^{-1}$.

Theorem 3.4. *For a number field K and a lattice $L \subset K$ with $\mathbf{Z}$-basis $e_1, \ldots, e_n$, $L^\vee = \bigoplus_{i=1}^n \mathbf{Z}e_i^\vee$, where $\{e_i^\vee\}$ is the dual basis to $\{e_i\}$ relative to the trace product on $K/\mathbf{Q}$. In particular, $L^\vee$ is a lattice.*

Proof. This is virtually identical to Theorem 2.5, except for the use of the trace product in place of the dot product. □

Corollary 3.5. *For lattices in K, the following properties hold:*

(1) $L^{\vee\vee} = L$,
(2) $L_1 \subset L_2 \iff L_2^\vee \subset L_1^\vee$,
(3) $(L_1 + L_2)^\vee = L_1^\vee \cap L_2^\vee$,
(4) $(L_1 \cap L_2)^\vee = L_1^\vee + L_2^\vee$,
(5) $(\alpha L)^\vee = \frac{1}{\alpha}L^\vee$ *for* $\alpha \in K^\times$.

Proof. The first four properties are proved in the same way as the proof of Corollary 2.7, and the last one is left to the reader. □

Example 3.6. For a quadratic field $K = \mathbf{Q}(\sqrt{d})$, with a squarefree integer d, we use Theorem 3.4 to compute $L^\vee$ for the lattices $\mathbf{Z} + \mathbf{Z}\sqrt{d}$ and $\mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2}$. (The second lattice isn't a ring unless $d \equiv 1 \bmod 4$, but it is a lattice for all d, so we can speak of its dual lattice in all cases.)

The dual basis of $\{1, \sqrt{d}\}$ for $K/\mathbf{Q}$ relative to the trace product on K is $\{\frac{1}{2}, \frac{1}{2\sqrt{d}}\}$, so $(\mathbf{Z} + \mathbf{Z}\sqrt{d})^\vee = \mathbf{Z}\frac{1}{2} + \mathbf{Z}\frac{1}{2\sqrt{d}} = \frac{1}{2\sqrt{d}}(\mathbf{Z}\sqrt{d} + \mathbf{Z}) = \frac{1}{2\sqrt{d}}(\mathbf{Z} + \mathbf{Z}\sqrt{d})$.

The dual basis of $\{1, \frac{1+\sqrt{d}}{2}\}$ relative to the trace product on K is $\{-1 + \frac{\sqrt{d}}{2\sqrt{d}}, \frac{1}{d}\sqrt{d}\}$, and a calculation yields $(\mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2})^\vee = \frac{1}{\sqrt{d}}(\mathbf{Z}\frac{-1+\sqrt{d}}{2} + \mathbf{Z}) = \frac{1}{\sqrt{d}}(\mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2})$.

The next theorem tells us the dual basis of a power basis of K (a basis consisting of powers of a single element). In terms of dual lattices, a tight connection between dual lattices and differentiation is revealed.

Theorem 3.7. *Let $K = \mathbf{Q}(\alpha)$ and let $f(T)$ be the minimal polynomial of α in $\mathbf{Q}[T]$. Write*

$$f(T) = (T - \alpha)(c_0(\alpha) + c_1(\alpha)T + \cdots + c_{n-1}(\alpha)T^{n-1}), \quad c_i(\alpha) \in K.$$

The dual basis to $\{1, \alpha, \ldots, \alpha^{n-1}\}$ relative to the trace product is $\{\frac{c_0(\alpha)}{f'(\alpha)}, \frac{c_1(\alpha)}{f'(\alpha)}, \ldots, \frac{c_{n-1}(\alpha)}{f'(\alpha)}\}$. In particular, if $K = \mathbf{Q}(\alpha)$ and $\alpha \in \mathcal{O}_K$ then

$$(\mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{n-1})^\vee = \frac{1}{f'(\alpha)}(\mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{n-1}).$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the $\mathbf{Q}$-conjugates of α in a splitting field, with $\alpha = \alpha_1$. A beautiful polynomial identity of Euler says

$$\sum_{i=1}^{n} \frac{1}{f'(\alpha_i)} \frac{f(T)}{T - \alpha_i} = 1.$$

Indeed, both sides are polynomials of degree less than n that are equal at n values. By the same argument,

$$\sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} \frac{f(T)}{T - \alpha_i} = T^k$$

for $0 \leq k \leq n-1$. Comparing coefficients of like powers of T on both sides,

$$\sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} c_j(\alpha_i) = \delta_{jk}.$$

The left side is $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha^k(c_j(\alpha)/f'(\alpha)))$, so $\{c_j(\alpha)/f'(\alpha)\}$ is the dual basis to $\{\alpha^j\}$ and

$$(\mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{n-1})^\vee = \frac{1}{f'(\alpha)}(\mathbf{Z}c_0(\alpha) + \mathbf{Z}c_1(\alpha) + \cdots + \mathbf{Z}c_{n-1}(\alpha)).$$

To show

$$\mathbf{Z}c_0(\alpha) + \mathbf{Z}c_1(\alpha) + \cdots + \mathbf{Z}c_{n-1}(\alpha) = \mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{n-1}$$

when $\alpha \in \mathcal{O}_K$, we find a formula for $c_j(\alpha)$, the coefficient of T^j in $f(T)/(T-\alpha)$. Letting $f(T) = a_0 + a_1 T + \cdots + a_{n-1}T^{n-1} + a_n T^n \in \mathbf{Z}[T]$, where $a_n = 1$,

$$\begin{aligned}
\frac{f(T)}{T-\alpha} &= \frac{f(T) - f(\alpha)}{T - \alpha} \\
&= \sum_{i=1}^{n} a_i \frac{T^i - \alpha^i}{T - \alpha} \\
&= \sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} \alpha^{i-1-j} T^j \\
&= \sum_{j=0}^{n-1} \left(\sum_{i=j+1}^{n} a_i \alpha^{i-1-j} \right) T^j,
\end{aligned}$$

so $c_j(\alpha) = \sum_{i=j+1}^{n} a_i \alpha^{i-1-j}$, whose top term is α^{n-j-1} (since $a_n = 1$). A transition matrix from $1, \alpha, \ldots, \alpha^{n-1}$ to $c_{n-1}(\alpha), \ldots, c_1(\alpha), c_0(\alpha)$ is triangular with integral entries and 1's on the main diagonal, so it is invertible over $\mathbf{Z}$ and shows the $\mathbf{Z}$-span of the two sets is the same. □

Example 3.8. Returning to Example 3.6, we recompute $(\mathbf{Z} + \mathbf{Z}\alpha)^\vee$ for $\alpha = \sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$, with $f(T) = T^2 - d$ or $T^2 - T + \frac{1-d}{4}$, respectively. In the first case $f'(\alpha) = 2\sqrt{d}$, and in the second case $f'(\alpha) = 2\frac{1+\sqrt{d}}{2} - 1 = \sqrt{d}$. The formula $(\mathbf{Z} + \mathbf{Z}\alpha)^\vee = \frac{1}{f'(\alpha)}(\mathbf{Z} + \mathbf{Z}\alpha)$ from Theorem 3.7 recovers the formulas for the dual lattices in Example 3.6.

The most interesting lattice in K is $\mathcal{O}_K$. What can we say about

$$\mathcal{O}_K^\vee = \{\alpha \in K : \mathrm{Tr}_{K/\mathbf{Q}}(\alpha \mathcal{O}_K) \subset \mathbf{Z}\}?$$

First of all, $\mathcal{O}_K^\vee$ is *not* the elements of K with integral trace. It is smaller than that. To lie in $\mathcal{O}_K^\vee$, the trace product with all elements of $\mathcal{O}_K$ must lie in $\mathbf{Z}$. This includes the condition the trace of the element is in $\mathbf{Z}$ only as a special case (taking the trace product with 1). Since algebraic integers have integral trace, $\mathcal{O}_K \subset \mathcal{O}_K^\vee$, so $\mathcal{O}_K^\vee$ always contains $\mathcal{O}_K$. We saw earlier that $\mathbf{Z}[i]^\vee = \frac{1}{2}\mathbf{Z}[i]$, for instance.

The next theorem says the dual lattice of $\mathcal{O}_K$ is a fractional ideal that "controls" the dual lattice of every fractional ideal.

Theorem 3.9. *For a fractional ideal $\mathfrak{a}$ in K, $\mathfrak{a}^\vee$ is a fractional ideal and $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathcal{O}_K^\vee$.*

This formula explains $\mathfrak{a}^{\vee\vee} = \mathfrak{a}$ from Corollary 3.5 in the special case of fractional ideals.

Proof. By definition, $\mathfrak{a}^\vee = \{\alpha \in K : \mathrm{Tr}_{K/\mathbf{Q}}(\alpha\mathfrak{a}) \subset \mathbf{Z}\}$. First we check $\mathfrak{a}^\vee$ is a fractional ideal. We know it is finitely generated as a $\mathbf{Z}$-module (a dual lattice is a lattice), so the key point is that it is preserved by multiplication by $\mathcal{O}_K$. For $\alpha \in \mathfrak{a}^\vee$ and $x \in \mathcal{O}_K$, $x\alpha \in \mathfrak{a}^\vee$ since, for all $\beta \in \mathfrak{a}$, $\mathrm{Tr}_{K/\mathbf{Q}}((x\alpha)\beta) = \mathrm{Tr}_{K/\mathbf{Q}}(\alpha(x\beta)) \in \mathbf{Z}$, as $x\beta \in \mathfrak{a}$ and $\alpha \in \mathfrak{a}^\vee$.

To show $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathcal{O}_K^\vee$, pick $\alpha \in \mathfrak{a}^\vee$. For $\beta \in \mathfrak{a}$, $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha\beta\mathcal{O}_K) \subset \mathbf{Z}$ since $\beta\mathcal{O}_K \subset \mathfrak{a}$. Therefore $\alpha\beta \in \mathcal{O}_K^\vee$. Letting β vary in $\mathfrak{a}$ we get $\alpha\mathfrak{a} \subset \mathcal{O}_K^\vee$, so $\alpha \in \mathfrak{a}^{-1}\mathcal{O}_K^\vee$. Thus $\mathfrak{a}^\vee \subset \mathfrak{a}^{-1}\mathcal{O}_K^\vee$. The reverse inclusion is left to the reader. □

Theorem 3.10. *The dual lattice $\mathcal{O}_K^\vee$ is the largest fractional ideal in K whose elements all have trace in $\mathbf{Z}$.*

Proof. For a fractional ideal $\mathfrak{a}$, $\mathfrak{a} = \mathfrak{a}\mathcal{O}_K$. Thus $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{a}) \subset \mathbf{Z}$ if and only if $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{a}\mathcal{O}_K) \subset \mathbf{Z}$, which is equivalent to $\mathfrak{a} \subset \mathcal{O}_K^\vee$. □

This theorem isn't saying $\mathcal{O}_K^\vee$ is the set of all elements in K with integral trace. It's the largest *fractional ideal* whose elements have integral trace. The set of all elements with integral trace is an additive group, but it is not a fractional ideal.

Example 3.11. Since $\mathbf{Z}[i]^\vee = \frac{1}{2}\mathbf{Z}[i]$, a fractional ideal whose elements have integral trace is inside $\frac{1}{2}\mathbf{Z}[i]$. All the elements of $\mathbf{Q}(i)$ with integral trace are $\frac{1}{2}\mathbf{Z} + \mathbf{Q}i$, which isn't a fractional ideal at all.

4. The Different Ideal

The construction of $\mathcal{O}_K^\vee$ provides us with an interesting canonical fractional ideal in K other than $\mathcal{O}_K$. Because $\mathcal{O}_K \subset \mathcal{O}_K^\vee$, the inverse of $\mathcal{O}_K^\vee$ is a fractional ideal inside $\mathcal{O}_K$, hence is an integral ideal.

Definition 4.1. The *different ideal* of K is

$$\mathcal{D}_K = (\mathcal{O}_K^\vee)^{-1} = \{x \in K : x\mathcal{O}_K^\vee \subset \mathcal{O}_K\}.$$

Example 4.2. Since $\mathbf{Z}[i]^\vee = \frac{1}{2}\mathbf{Z}[i]$ by Example 3.3, $\mathcal{D}_{\mathbf{Q}(i)} = 2\mathbf{Z}[i]$.

Theorem 4.3. *If $\mathcal{O}_K = \mathbf{Z}[\alpha]$ then $\mathcal{D}_K = (f'(\alpha))$, where α has minimal polynomial $f(T) \in \mathbf{Z}[T]$.*

Proof. Use Theorem 3.7. □

Example 4.4. For a quadratic field $K = \mathbf{Q}(\sqrt{d})$ with squarefree $d \in \mathbf{Z}$, $\mathcal{O}_K$ is $\mathbf{Z}[\sqrt{d}]$ or $\mathbf{Z}[(1+\sqrt{d})/2]$, depending on d mod 4. Using Example 3.8,

$$\mathcal{D}_{\mathbf{Q}(\sqrt{d})} = \begin{cases} (2\sqrt{d}), & \text{if } d \not\equiv 1 \bmod 4, \\ (\sqrt{d}), & \text{if } d \equiv 1 \bmod 4. \end{cases} \tag{4.1}$$

Remark 4.5. It is not true in general that $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for some α, so the different can't be calculated as a principal ideal $(f'(\alpha))$ all the time. However, the different does divide ideals of this type. Specifically, for all $\alpha \in \mathcal{O}_K$, $\mathcal{D}_K \mid (f'_\alpha(\alpha))$ where $f_\alpha(T)$ is the characteristic polynomial of α in $\mathbf{Q}[T]$. This is automatic if $\mathbf{Q}(\alpha) \subsetneq K$ since $f'_\alpha(\alpha) = 0$, as $f_\alpha(T)$ is a proper power of the minimal polynomial of α. If $\mathbf{Q}(\alpha) = K$ and $\alpha \in \mathcal{O}_K$, then $\mathbf{Z}[\alpha]$ is a lattice in K and the inclusion $\mathbf{Z}[\alpha] \subset \mathcal{O}_K$ implies $\mathcal{O}_K^\vee \subset \mathbf{Z}[\alpha]^\vee$, which is equivalent to $\mathcal{D}_K^{-1} \subset \frac{1}{f'_\alpha(\alpha)}\mathbf{Z}[\alpha]$, so $\mathcal{D}_K^{-1} \subset \frac{1}{f'_\alpha(\alpha)}\mathcal{O}_K$. Inverting ideals, $(f'_\alpha(\alpha)) \subset \mathcal{D}_K$, so $\mathcal{D}_K \mid (f'_\alpha(\alpha))$. If we let α vary then $\mathcal{D}_K$ divides the ideal generated by $f'_\alpha(\alpha)$ as α runs over $\mathcal{O}_K$. It can be shown that $\mathcal{D}_K$ is equal to the ideal generated by all $f'_\alpha(\alpha)$ for $\alpha \in \mathcal{O}_K$. This is in marked contrast to the situation for discriminants: $\mathrm{disc}(\mathcal{O}_K/\mathbf{Z})$ does not always equal the greatest common divisor of all $\mathrm{disc}(f_\alpha(T))$ as α ranges over algebraic integers in K.

Theorem 4.6. *For every number field K, $\mathrm{N}(\mathcal{D}_K) = |\mathrm{disc}(K)|$.*

Proof. Let $e_1, \ldots, e_n$ be a $\mathbf{Z}$-basis for $\mathcal{O}_K$, so $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbf{Z}e_i$. Then $\mathcal{D}_K^{-1} = \mathcal{O}_K^\vee = \bigoplus_{i=1}^n \mathbf{Z}e_i^\vee$. The norm of an ideal is its index in $\mathcal{O}_K$, so

$$\mathrm{N}(\mathcal{D}_K) = [\mathcal{O}_K : \mathcal{D}_K] = {}^{4}\ [\mathcal{D}_K^{-1} : \mathcal{O}_K] = [\mathcal{O}_K^\vee : \mathcal{O}_K].$$

To compute the index $[\mathcal{O}_K^\vee : \mathcal{O}_K]$, recall that for finite free $\mathbf{Z}$-modules $M_1 \subset M_2$ of equal rank, $[M_2 : M_1] = |\det(A)|$ where A is a matrix expressing a $\mathbf{Z}$-basis of M_1 in terms of a $\mathbf{Z}$-basis of M_2. For our application, with $M_1 = \mathcal{O}_K$ and $M_2 = \mathcal{O}_K^\vee$, let's write the e_i's in terms of the $e_i^\vee$'s: if $e_j = \sum_{i=1}^n a_{ij}e_i^\vee$, the meaning of being dual bases relative to the trace product is that $a_{ij} = \mathrm{Tr}_{K/\mathbf{Q}}(e_j e_i) = \mathrm{Tr}_{K/\mathbf{Q}}(e_i e_j)$. Therefore $(a_{ij}) = (\mathrm{Tr}_{K/\mathbf{Q}}(e_i e_j))$. The determinant of this matrix, by definition, is $|\mathrm{disc}(K)|$, so $\mathrm{N}(\mathcal{D}_K) = |\mathrm{disc}(K)|$. □

Theorem 4.6 tells us that in the inclusions of lattices

$$\mathcal{D}_K \subset \mathcal{O}_K \subset \mathcal{O}_K^\vee$$

each successive inclusion has index $|\mathrm{disc}(K)|$. In particular, $\mathcal{O}_K^\vee$ is strictly larger than $\mathcal{O}_K$ if and only if $|\mathrm{disc}(K)| > 1$. That inequality holds for all $K \neq \mathbf{Q}$ (Minkowski's theorem), so $\mathcal{O}_K$ is not its own dual lattice when $K \neq \mathbf{Q}$. The different ideal could be considered a measure of how much $\mathcal{O}_K$ fails to be self-dual as a lattice in K.

Example 4.4 and Theorem 4.6 recover the formulas for (the absolute value of) the discriminant of a quadratic field from the norm of the different of a quadratic field:

$$|\mathrm{disc}(\mathbf{Q}(\sqrt{d}))| = \mathrm{N}(\mathcal{D}_{\mathbf{Q}(\sqrt{d})}) = \begin{cases} 4|d|, & \text{if } d \not\equiv 1 \bmod 4, \\ |d|, & \text{if } d \equiv 1 \bmod 4. \end{cases} \tag{4.2}$$

Theorem 4.6 suggests, from experience with the discriminant, there should be a relation between the different and ramified primes. We will show the prime ideal factors of the different are the ramified primes in K.

Lemma 4.7. *For a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathfrak{a} \mid \mathcal{D}_K$ if and only if $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{a}^{-1}) \subset \mathbf{Z}$.*

Proof. Since divisibility is the same as containment for integral ideals, $\mathfrak{a} \mid \mathcal{D}_K$ if and only if $\mathfrak{a} \supset \mathcal{D}_K = (\mathcal{O}_K^\vee)^{-1}$, which is equivalent to $\mathcal{O}_K^\vee \supset \mathfrak{a}^{-1}$. By Theorem 3.10, this last containment is equivalent to $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{a}^{-1}) \subset \mathbf{Z}$. □

[4]For fractional ideals $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$, with $\mathfrak{a} \supset \mathfrak{b}$, $\mathfrak{ac}/\mathfrak{bc} \cong \mathfrak{a}/\mathfrak{b}$ as $\mathcal{O}_K$-modules. When $\mathfrak{c}$ is a nonzero ideal, using $\mathfrak{a} = \mathfrak{c}^{-1}$ and $\mathfrak{b} = \mathcal{O}_K$ gives us $\mathcal{O}_K/\mathfrak{c} \cong \mathfrak{c}^{-1}/\mathcal{O}_K$. Thus $[\mathcal{O}_K : \mathfrak{c}] = [\mathfrak{c}^{-1} : \mathcal{O}_K]$.

Here is the central theorem about the different ideal. It not only tells us the prime ideal factors of the different, but also the multiplicities in most cases.

Theorem 4.8 (Dedekind)**.** *The prime ideal factors of $\mathcal{D}_K$ are the primes in K that ramify over $\mathbf{Q}$. More precisely, for each prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ lying over a prime number p, with ramification index $e = e(\mathfrak{p}|p)$, the exact power of $\mathfrak{p}$ in $\mathcal{D}_K$ is $\mathfrak{p}^{e-1}$ if $e \not\equiv 0 \bmod p$, and $\mathfrak{p}^e \mid \mathcal{D}_K$ if $p \mid e$.*

When $p \mid e$, the theorem does not tell us the exact multiplicity of $\mathfrak{p}$ in $\mathcal{D}_K$, but only says the multiplicity is at least e.

Proof. If we grant that $\mathfrak{p}^{e-1} \mid \mathcal{D}_K$, every ramified prime in K divides $\mathcal{D}_K$. If $\mathfrak{p}$ is unramified over $\mathbf{Q}$, so $e = 1$, then the last part of the theorem says $\mathfrak{p}$ doesn't divide $\mathcal{D}_K$ since p doesn't divide 1. Therefore it remains to check the two divisibility relations.

To show $\mathfrak{p}^{e-1} \mid \mathcal{D}_K$, write $(p) = \mathfrak{p}^{e-1}\mathfrak{a}$. Since $\mathfrak{p}^e \mid (p)$, $\mathfrak{p} \mid \mathfrak{a}$. To say $\mathfrak{p}^{e-1} \mid \mathcal{D}_K$ is equivalent, by Lemma 4.7, to saying $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{p}^{-(e-1)}) \subset \mathbf{Z}$. Since $\mathfrak{p}^{-(e-1)} = \frac{1}{p}\mathfrak{a}$, $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{p}^{-(e-1)}) \subset \mathbf{Z}$ if and only if $\mathrm{Tr}_{K/\mathbf{Q}}(\mathfrak{a}) \subset p\mathbf{Z}$, which is the same as $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) \equiv 0 \bmod p$ for all $\alpha \in \mathfrak{a}$. This congruence is what we will actually show.

For $\alpha \in \mathfrak{a}$, $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = \mathrm{Tr}_{\mathcal{O}_K/\mathbf{Z}}(\alpha)$ and $\mathrm{Tr}_{\mathcal{O}_K/\mathbf{Z}}(\alpha) \bmod p = \mathrm{Tr}_{(\mathcal{O}_K/(p))/\mathbf{F}_p}(\overline{\alpha})$. This last trace is the trace of multiplication by $\overline{\alpha}$ on $\mathcal{O}_K/(p)$ as an $\mathbf{F}_p$-linear map, and $\overline{\alpha}$ is a general element of $\mathfrak{a}/(p)$. (The quotient $\mathfrak{a}/(p)$ makes sense since $\mathfrak{a} \mid (p)$ by the definition of $\mathfrak{a}$.) Since $\mathfrak{a}$ is divisible by every prime ideal factor of (p) (including $\mathfrak{p}$), a high power of $\mathfrak{a}$ is divisible by (p). Therefore a high power of $\overline{\alpha}$ is 0 in $\mathcal{O}_K/(p)$, which means multiplication by $\overline{\alpha}$ on $\mathcal{O}_K/(p)$ is nilpotent as an $\mathbf{F}_p$-linear map. Nilpotent linear maps have trace 0, so $\mathrm{Tr}_{(\mathcal{O}_K/(p))/\mathbf{F}_p}(\overline{\alpha}) = 0$. That completes the proof that $\mathfrak{p}^{e-1} \mid \mathcal{D}_K$.

Now we want to show $\mathfrak{p}^e \mid \mathcal{D}_K$ if and only if $p \mid e$. Write $(p) = \mathfrak{p}^e\mathfrak{b}$, so $\mathfrak{b}$ is not divisible by $\mathfrak{p}$. To say $\mathfrak{p}^e \mid \mathcal{D}_K$ is equivalent to $\mathrm{Tr}_{\mathcal{O}_K/\mathbf{Z}}(\mathfrak{b}) \subset p\mathbf{Z}$ by Lemma 4.7, which is equivalent to

$$\mathrm{Tr}_{(\mathcal{O}_K/(p))/\mathbf{F}_p}(\overline{\beta}) = 0 \text{ for all } \beta \in \mathfrak{b}. \tag{4.3}$$

We will break up $\mathcal{O}_K/(p)$ into a product of two rings and analyze the trace separately on both.

Since $\mathfrak{p}^e$ and $\mathfrak{b}$ are relatively prime, $\mathcal{O}_K/(p) \cong \mathcal{O}_K/\mathfrak{p}^e \times \mathcal{O}_K/\mathfrak{b}$ as rings by the natural map, so

$$\mathrm{Tr}_{(\mathcal{O}_K/(p))/\mathbf{F}_p}(\overline{x}) = \mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{x}) + \mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{b})/\mathbf{F}_p}(\overline{x}) \tag{4.4}$$

for all $x \in \mathcal{O}_K$, where $\overline{x}$ on the left is x mod (p) and $\overline{x}$ on the right is x mod $\mathfrak{p}^e$ and x mod $\mathfrak{b}$. (Both $\mathcal{O}_K/\mathfrak{b}$ and $\mathcal{O}_K/\mathfrak{p}^e$ contain $\mathbf{F}_p$ since $\mathfrak{p}^e$ and $\mathfrak{b}$ both divide (p), so p is 0 in both rings.) If $x \in \mathfrak{b}$, then $x = 0$ in $\mathcal{O}_K/\mathfrak{b}$, so $\mathrm{Tr}_{(\mathcal{O}_K/(p))/\mathbf{F}_p}(\overline{x}) = \mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{x})$. For $y \in \mathcal{O}_K$, there is an $x \in \mathcal{O}_K$ satisfying $x \equiv y \bmod \mathfrak{p}^e$ and $x \equiv 0 \bmod \mathfrak{b}$, so $\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{y}) = \mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{x}) = \mathrm{Tr}_{(\mathcal{O}_K/(p))/\mathbf{F}_p}(\overline{x})$. Therefore proving (4.3) is equivalent to proving

$$\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{y}) = 0 \text{ for all } y \in \mathcal{O}_K. \tag{4.5}$$

Unlike (4.3), which is quantified over the ideal $\mathfrak{b}$, (4.3) runs over $\mathcal{O}_K$. We will show (4.5) happens if and only if $p \mid e$.

To study the trace down to $\mathbf{F}_p$ of y on $\mathcal{O}_K/\mathfrak{p}^e$, we will filter $\mathcal{O}_K/\mathfrak{p}^e$ by subspaces made from powers of $\mathfrak{p}$:

$$\mathcal{O}_K/\mathfrak{p}^e \supset \mathfrak{p}/\mathfrak{p}^e \supset \mathfrak{p}^2/\mathfrak{p}^e \supset \cdots \supset \mathfrak{p}^{e-1}/\mathfrak{p}^e \supset \mathfrak{p}^e/\mathfrak{p}^e = \{\overline{0}\}.$$

Each power $\mathfrak{p}^i$ is an ideal, so multiplication by y is a well-defined linear operator on each $\mathfrak{p}^i/\mathfrak{p}^e$ $(0 \leq i \leq e)$. We now appeal to a result from linear algebra: if V is a finite-dimensional vector space over a field F, $A\colon V \to V$ is a linear operator and W is a subspace of V such that $A(W) \subset W$, then

$$\mathrm{Tr}(A\colon V \to V) = \mathrm{Tr}(A\colon V/W \to V/W) + \mathrm{Tr}(A\colon W \to W).$$

(This identity is proved by a matrix calculation, using a basis of V/W lifted to V together with a basis of W to form a basis of V. The matrix for A on V in this basis is block triangular.) Taking $F = \mathbf{F}_p$, $V = \mathcal{O}_K/\mathfrak{p}^e$, $W = \mathfrak{p}/\mathfrak{p}^e$, and A to be multiplication by y,

$$\begin{aligned}\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{y}) &= \mathrm{Tr}(m_y\colon \mathcal{O}_K/\mathfrak{p}^e \to \mathcal{O}_K/\mathfrak{p}^e)\\ &= \mathrm{Tr}(m_y\colon \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}) + \mathrm{Tr}(m_y\colon \mathfrak{p}/\mathfrak{p}^e \to \mathfrak{p}/\mathfrak{p}^e).\end{aligned}$$

In a similar way, using multiplication by y on the vector space $\mathfrak{p}^i/\mathfrak{p}^e$ and subspace $\mathfrak{p}^{i+1}/\mathfrak{p}^e$, where $0 \leq i \leq e-1$,

$$\mathrm{Tr}(m_y\colon \mathfrak{p}^i/\mathfrak{p}^e \to \mathfrak{p}^i/\mathfrak{p}^e) = \mathrm{Tr}(m_y\colon \mathfrak{p}^i/\mathfrak{p}^{i+1} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}) + \mathrm{Tr}(m_y\colon \mathfrak{p}^{i+1}/\mathfrak{p}^e \to \mathfrak{p}^{i+1}/\mathfrak{p}^e).$$

Using this recursively for $i = 0, 1, \ldots, e-1$, we get

$$\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{y}) = \sum_{i=0}^{e-1} \mathrm{Tr}(m_y\colon \mathfrak{p}^i/\mathfrak{p}^{i+1} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}). \tag{4.6}$$

The traces in the sum take values in $\mathbf{F}_p$. We will show the traces are all equal. Choosing $\pi \in \mathfrak{p} - \mathfrak{p}^2$, (π^i) is divisible by $\mathfrak{p}^i$ but not by $\mathfrak{p}^{i+1}$, so $\mathfrak{p}^i = (\pi^i) + \mathfrak{p}^{i+1}$. Therefore $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^i/\mathfrak{p}^{i+1}$ as $\mathcal{O}_K$-modules by $x \bmod \mathfrak{p} \mapsto \pi^i x \bmod \mathfrak{p}^{i+1}$. This $\mathcal{O}_K$-module isomorphism commutes with multiplication by y on both sides, so

$$\mathrm{Tr}(m_y\colon \mathfrak{p}^i/\mathfrak{p}^{i+1} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}) = \mathrm{Tr}(m_y\colon \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}).$$

Thus (4.6) becomes

$$\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/\mathbf{F}_p}(\overline{y}) = e\,\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p})/\mathbf{F}_p}(\overline{y}) \tag{4.7}$$

for all $y \in \mathcal{O}_K$, so (4.5) is true if and only if $e\,\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p})/\mathbf{F}_p}(\overline{y}) = 0$ for all $\overline{y} \in \mathcal{O}_K/\mathfrak{p}$. Since $\mathcal{O}_K/\mathfrak{p}$ is a finite field, the trace map from $\mathcal{O}_K/\mathfrak{p}$ to $\mathbf{F}_p$ is *not* identically 0, so (4.5) holds if and only if $e = 0$ in $\mathbf{F}_p$, *i.e.*, $p \mid e$. □

Up to now the fact that the prime numbers dividing $\mathrm{disc}(K)$ are the ramified primes in K hasn't been used (outside of Example 1.1). Theorem 4.8 leads to a new proof of that result.

Corollary 4.9. *The prime factors of* $\mathrm{disc}(K)$ *are the primes in* $\mathbf{Q}$ *that ramify in* K.

Proof. Since $|\mathrm{disc}(K)| = \mathrm{N}(\mathcal{D}_K)$, if p is a prime dividing $\mathrm{disc}(K)$ then $\mathcal{D}_K$ must have a prime ideal factor whose norm is a power of p, which means (p) is divisible by a prime factor of $\mathcal{D}_K$, so p ramifies in K. Conversely, if p ramifies in K then $\mathcal{D}_K$ is divisible by a prime ideal factor of (p), so $\mathrm{N}(\mathcal{D}_K)$ is divisible by p. □

Corollary 4.10. *Write* $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ *and* $f_i = f(\mathfrak{p}_i|p)$. *If no* e_i *is a multiple of* p *then the multiplicity of* p *in* $\mathrm{disc}(K)$ *is*

$$(e_1 - 1)f_1 + \cdots + (e_g - 1)f_g = n - (f_1 + \cdots + f_g).$$

If some e_i *is a multiple of* p *then the multiplicity of* p *in* $\mathrm{disc}(K)$ *is larger than this amount.*

Proof. The multiplicity of p in $\mathrm{disc}(K)$ is determined by the multiplicities of the $\mathfrak{p}_i$'s in $\mathcal{D}_K$, since the norm of the different is the discriminant (in absolute value). By Theorem 4.8, $\mathfrak{p}_1^{e_1-1}\cdots\mathfrak{p}_g^{e_g-1}$ is a factor of $\mathcal{D}_K$. Applying the ideal norm, $p^{(e_1-1)f_1+\cdots+(e_g-1)f_g}$ is a factor of $\mathrm{disc}(K)$. If no e_i is a multiple of p then $\mathfrak{p}_i$ appears in $\mathcal{D}_K$ with multiplicity e_i-1, so this power of p is the full power of p in $\mathrm{disc}(K)$. If some e_i is a multiple of p then $\mathfrak{p}_i$ appears in $\mathcal{D}_K$ with multiplicity larger than e_i-1, so the p-multiplicity of $\mathrm{disc}(K)$ is larger than what we just computed. □

Example 4.11. In $\mathbf{Q}(\sqrt{10})$, the prime numbers that ramify are 2 and 5: $(2) = \mathfrak{p}_2^2$ and $(5) = \mathfrak{p}_5^2$. By Example 4.4, the different of $\mathbf{Q}(\sqrt{10})/\mathbf{Q}$ is $\mathcal{D} = (2\sqrt{10}) = \mathfrak{p}_2^3\mathfrak{p}_5$. The multiplicity of $\mathfrak{p}_5$ in $\mathcal{D}$ is $e(\mathfrak{p}_5|5) - 1 = 1$, and the multiplicity of $\mathfrak{p}_2$ is at least $e(\mathfrak{p}_2|2) = 2$, which is consistent with Theorem 4.8 since $e(\mathfrak{p}_5|5)$ is not a multiple of 5 and $e(\mathfrak{p}_2|2)$ is a multiple of 2. Notice the $\mathfrak{p}_2$-multiplicity in $\mathcal{D}$ is in fact greater than $e(\mathfrak{p}_2|2)$.

Example 4.12. Let $K = \mathbf{Q}(\alpha)$, where $\alpha^3-\alpha-1 = 0$. Since $\mathcal{O}_K = \mathbf{Z}[\alpha]$ and $|\mathrm{disc}(K)| = 23$, $\mathcal{D}_K$ has norm 23. Therefore $\mathcal{D}_K$ is a prime ideal. Since $(23) = \mathfrak{p}\mathfrak{q}^2$ and $\mathfrak{q}$ must divide $\mathcal{D}_K$ by Theorem 4.8, $\mathcal{D}_K = \mathfrak{q}$. The multiplicity of $\mathfrak{q}$ in the different is $1 = e(\mathfrak{q}|23) - 1$, as expected.

Example 4.13. Let $K = \mathbf{Q}(\sqrt[3]{2})$, so $\mathbf{Z}[\sqrt[3]{2}] \subset \mathcal{O}_K$. We will use Theorem 4.8 to prove $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$. Since $\mathrm{disc}(\mathbf{Z}[\sqrt[3]{2}]) = [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{2}]]^2 \mathrm{disc}(\mathcal{O}_K)$ and $\mathrm{disc}(\mathbf{Z}[\sqrt[3]{2}]) = -108 = -4\cdot 27$, it suffices to show $|\mathrm{disc}(\mathcal{O}_K)| = 108$.

The only prime factors of 108 are 2 and 3, so the only primes that can ramify in K are 2 and 3. The polynomials $T^3 - 2$ and $(T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3$ are Eisenstein at 2 and 3 with roots generating K, so both 2 and 3 are totally ramified in $\mathcal{O}_K$: $(2) = \mathfrak{p}^3$ and $(3) = \mathfrak{q}^3$. By Theorem 4.8, $\mathcal{D}_K$ is divisible by $\mathfrak{p}^2\mathfrak{q}^3$. Taking norms, $\mathrm{disc}(\mathcal{O}_K)$ is divisible by $2^2\cdot 3^3 = 108$. We already knew $\mathrm{disc}(\mathcal{O}_K)$ is a factor of 108, so $|\mathrm{disc}(\mathcal{O}_K)| = 108$ and $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$ (and $\mathcal{D}_K = \mathfrak{p}^2\mathfrak{q}^3$).

Example 4.14. If p has exactly one prime lying over it, say $(p) = \mathfrak{p}^e$, then $\mathcal{D}_K$ is divisible by $\mathfrak{p}^{e-1}$, so $\mathrm{disc}(K)$ is divisible by $\mathrm{N}(\mathfrak{p})^{e-1} = p^{f(e-1)}$. If $e \not\equiv 0 \bmod p$ then $p^{f(e-1)}$ is the exact power of p in $\mathrm{disc}(K)$.

Example 4.15. Let $K = \mathbf{Q}(\sqrt[3]{175})$. Using our knowledge of the multiplicity of primes in the discriminant, based on the connection between the different and discriminant, we will determine $\mathcal{O}_K$ and then prove $\mathcal{O}_K$ does not have a power basis.

View K as a subfield of $\mathbf{R}$, so there is no ambiguity about the meaning of cube roots. Set $\alpha = \sqrt[3]{175}$. Since $175 = 5^2\cdot 7$, K also contains $\sqrt[3]{5\cdot 7^2} = 35/\alpha$. Set $\beta = \sqrt[3]{5\cdot 7^2}$. The minimal polynomials for α and β over $\mathbf{Q}$ are $T^3 - 5^2\cdot 7$ and $T^3 - 5\cdot 7^2$, which are Eisenstein at 5 and 7, so 5 and 7 are both totally ramified in $\mathcal{O}_K$: $(5) = \mathfrak{p}^3$ and $(7) = \mathfrak{q}^3$. Therefore $\mathcal{D}_K$ is divisible by $\mathfrak{p}^{3-1}\mathfrak{q}^{3-1} = \mathfrak{p}^2\mathfrak{q}^2$, so $\mathrm{disc}(\mathcal{O}_K)$ is divisible by $\mathrm{N}(\mathfrak{p}^2\mathfrak{q}^2) = 5^2\cdot 7^2$. Moreover, $(T+1)^3 - 175 = T^3 + 3T^2 + 3T - 174$ is Eisenstein at 3, so 3 is totally ramified in K: $(3) = \mathfrak{p}_3^3$. Since $e(\mathfrak{p}_3|3)$ is a multiple of 3, $\mathrm{disc}(\mathcal{O}_K)$ is divisible by 3^3, not just 3^2, so $\mathrm{disc}(\mathcal{O}_K)$ is a multiple of $3^3\cdot 5^2\cdot 7^2$.

The lattice $\mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta$ lies inside $\mathcal{O}_K$ and is a ring:

$$\alpha^2 = 5\beta, \quad \beta^2 = 7\alpha, \quad \alpha\beta = 35. \tag{4.8}$$

Using these equations and the formulas $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = 0$ and $\mathrm{Tr}_{K/\mathbf{Q}}(\beta) = 0$, the matrix of trace products for the $\mathbf{Q}$-basis $\{1, \alpha, \beta\}$ of K is

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 35 \cdot 3 \\ 0 & 35 \cdot 3 & 0 \end{pmatrix},$$

whose determinant is $-3^3 \cdot 5^2 \cdot 7^2$. Therefore

$$-3^3 \cdot 5^2 \cdot 7^2 = \mathrm{disc}(\mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta) = [\mathcal{O}_K : (\mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta)]^2 \,\mathrm{disc}(\mathcal{O}_K).$$

Since we know $\mathrm{disc}(\mathcal{O}_K)$ is a multiple of $3^3 \cdot 5^2 \cdot 7^2$, the index $[\mathcal{O}_K : (\mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta)]$ must be 1, so $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta$ and thus K has discriminant $-3^3 5^2 7^2 = -33075$.

We will now show in two ways that $\mathcal{O}_K$ does not have a power basis.

Method 1. For each $\gamma \in \mathcal{O}_K - \mathbf{Z}$ we will show $\mathrm{disc}(\mathbf{Z}[\gamma]) \neq \mathrm{disc}(\mathcal{O}_K)$ From the computation of $\mathcal{O}_K$, we can write $\gamma = a + b\alpha + c\beta$ with integers a, b, and c, where b and c are not both 0. Using (4.8), the matrix for multiplication by γ relative to the ordered $\mathbf{Z}$-basis $1, \alpha, \beta$ is

$$[m_\gamma] = \begin{pmatrix} a & 35c & 35b \\ b & a & 7c \\ c & 5b & a \end{pmatrix} \tag{4.9}$$

Computing powers of this matrix in PARI we get

$$\mathrm{Tr}_{K/\mathbf{Q}}(\gamma) = 3a, \quad \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^2) = 3a^2 + 210bc, \quad \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^3) = 3a^3 + 525b^3 + 735c^3 + 630abc,$$

and

$$\mathrm{Tr}_{K/\mathbf{Q}}(\gamma^4) = 3a^4 + 2100ab^3 + 2940ac^3 + 22050b^2c^2 + 1260a^2bc,$$

so

$$\mathrm{disc}(\mathbf{Z}[\gamma]) = \det \begin{pmatrix} \mathrm{Tr}_{K/\mathbf{Q}}(1) & \mathrm{Tr}_{K/\mathbf{Q}}(\gamma) & \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^2) \\ \mathrm{Tr}_{K/\mathbf{Q}}(\gamma) & \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^2) & \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^3) \\ \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^2) & \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^3) & \mathrm{Tr}_{K/\mathbf{Q}}(\gamma^4) \end{pmatrix} = -3^3 5^2 7^2 (5b^3 - 7c^3)^2.$$

Since $-3^3 5^2 7^2$ is the discriminant of K, $[\mathcal{O}_K : \mathbf{Z}[\gamma]] = |5b^3 - 7c^3|$. Therefore this index is 1 if and only if $5b^3 - 7c^3 = \pm 1$, which implies $5b^3 \equiv \pm 1 \bmod 7$, but 5 mod 7 is not a cube. We have a contradiction.

Method 2. We will show the different ideal $\mathcal{D}_K$ is not principal, so $\mathcal{O}_K$ can't have the form $\mathbf{Z}[\gamma]$ by Theorem 4.3.

We already saw that $\mathrm{disc}(K) = -3^3 5^2 7^2$ and $(3) = \mathfrak{p}_3^3$, $(5) = \mathfrak{p}^3$, and $(7) = \mathfrak{q}^3$. Since $\mathrm{N}(\mathcal{D}_K) = |\,\mathrm{disc}(K)| = 3^3 5^2 7^2$, $\mathcal{D}_K = \mathfrak{p}_3^3 \mathfrak{p}^2 \mathfrak{q}^2$. Since $(\beta)^3 = (245) = (5)(7)^2 = \mathfrak{p}^3 \mathfrak{q}^6$ we get $(\beta) = \mathfrak{p}\mathfrak{q}^2$, so $\mathcal{D}_K = (3)(\beta)\mathfrak{p}$ (also $\mathcal{D}_K = (3)(\alpha)\mathfrak{q}$). We will prove $\mathfrak{p}$ is not principal, so $\mathcal{D}_K$ is not principal.

The ideal norm of $\mathfrak{p}$ is 5, so to show $\mathfrak{p}$ is not principal it suffices (and actually is equivalent) to show that no γ in $\mathcal{O}_K$ has norm ± 5. Write $\gamma = a + b\alpha + c\beta$ with $a, b, c \in \mathbf{Z}$. Using (4.9),

$$\mathrm{N}_{K/\mathbf{Q}}(\gamma) = \det(m_\gamma) = a^3 + 175b^3 + 245c^3 - 105abc.$$

Set this equal to ± 5 and reduce modulo 7: the coefficients 175, 245, and 105 are multiples of 7, so

$$\pm 5 = a^3 \bmod 7.$$

This has no solution for a in $\mathbf{Z}/(7)$, so we have a contradiction.

The reasoning in Example 4.15 can be generalized: for distinct primes p and q not equal to 3 such that $p^2q \equiv 1 \bmod 3$ and $p^2q \not\equiv 1 \bmod 9$, and p is not a cube in $\mathbf{Z}/(q)$, the cubic field $\mathbf{Q}(\sqrt[3]{p^2q})$ has a different ideal that is not principal. Examples besides $(p,q) = (5,7)$ are $(p,q) = (11,7)$, $(17,7)$, and $(2,13)$; that last example is $\mathbf{Q}(\sqrt[3]{52})$. I learned about this type of construction from [2, pp. 460–462] and [3, Exer. 10B, pp. 101-102].

Theorem 4.8 gives us an exact formula for the multiplicity of $\mathfrak{p}$ in $\mathcal{D}_K$ if $e(\mathfrak{p}|p) \not\equiv 0 \bmod p$, but not if $e(\mathfrak{p}|p) \equiv 0 \bmod p$. Ramification when $e(\mathfrak{p}|p) \not\equiv 0 \bmod p$ is generally easier to study than when $e(\mathfrak{p}|p) \equiv 0 \bmod p$. For this reason, when $e(\mathfrak{p}|p) \not\equiv 0 \bmod p$ we say $\mathfrak{p}$ is *tamely ramified* over p, and when $e(\mathfrak{p}|p) \equiv 0 \bmod p$ we say $\mathfrak{p}$ is *wildly ramified* over p. If every prime over p in K is tamely ramified then we say p is tamely ramified in K. All unramified primes are tamely ramified, but ramified primes can also be tamely ramified. For example, 2 is wildly ramified in $\mathbf{Q}(\sqrt[3]{2})$ (since $(2) = \mathfrak{p}^3$), but 2 is tamely ramified in $\mathbf{Q}(\gamma)$, where $\gamma^3 + \gamma + 4 = 0$ (since $(2) = \mathfrak{p}\mathfrak{q}^2$).

Upper and lower bounds for the multiplicity of a nonzero prime ideal $\mathfrak{p}$ in $\mathcal{D}_K$ are

$$e - 1 \leq \mathrm{ord}_{\mathfrak{p}}(\mathcal{D}_K) \leq e - 1 + e\,\mathrm{ord}_p(e),$$

where $\mathfrak{p} \mid p$ and $e = e(\mathfrak{p}|p)$. The lower bound was proved by Dedekind (Theorem 4.8), who conjectured the upper bound, which was later proved by Hensel as one of the first applications of p-adic fields to number theory.

In the ideal class group of K, Hecke proved the ideal class of $\mathcal{D}_K$ is always a square. For a proof in the number field and function field settings, see [1].

References

[1] J. V. Armitage, *On a theorem of Hecke in number fields and function fields*, Invent. Math. **2** (1967), 238–246.
[2] H. Hasse, "Number Theory," Springer-Verlag, 1980.
[3] P. Samuel, "Algebraic Theory of Numbers," Dover, 2008.