

## 12 The different and the discriminant

### 12.1 The different

We continue in our usual *AKLB* setup:  $A$  is a Dedekind domain,  $K$  is its fraction field,  $L/K$  is a finite separable extension, and  $B$  is the integral closure of  $A$  in  $L$  (a Dedekind domain with fraction field  $L$ ). We would like to understand the primes that ramify in  $L/K$ . Recall that a prime  $\mathfrak{q}|\mathfrak{p}$  of  $L$  is unramified if and only if  $e_{\mathfrak{q}} = 1$  and  $B/\mathfrak{q}$  is a separable extension of  $A/\mathfrak{p}$ , equivalently, if and only if  $B/\mathfrak{q}^{e_{\mathfrak{q}}}$  is a finite étale  $A/\mathfrak{p}$  algebra (by Theorem 4.40).<sup>1</sup> A prime  $\mathfrak{p}$  of  $K$  is unramified if and only if all the primes  $\mathfrak{q}|\mathfrak{p}$  lying above it are unramified, equivalently, if and only if the ring  $B/\mathfrak{p}B$  is a finite étale  $A/\mathfrak{p}$  algebra.<sup>2</sup>

Our main tools for studying ramification are the *different*  $\mathcal{D}_{B/A}$  and *discriminant*  $D_{B/A}$ . The different is a  $B$ -ideal that is divisible by precisely the ramified primes  $\mathfrak{q}$  of  $L$ , and the discriminant is an  $A$ -ideal divisible by precisely the ramified primes  $\mathfrak{p}$  of  $K$ . Moreover, the valuation  $v_{\mathfrak{q}}(\mathcal{D}_{B/A})$  will give us information about the ramification index  $e_{\mathfrak{q}}$  (its exact value when  $\mathfrak{q}$  is tamely ramified).

Recall from Lecture 5 the trace pairing  $L \times L \rightarrow K$  defined by  $(x, y) \mapsto \mathrm{T}_{L/K}(xy)$ ; under our assumption that  $L/K$  is separable, it is a perfect pairing. An  $A$ -lattice  $M$  in  $L$  is a finitely generated  $A$ -module that spans  $L$  as a  $K$ -vector space (see Definition 5.9). Every  $A$ -lattice  $M$  in  $L$  has a *dual lattice* (see Definition 5.11)

$$M^* := \{x \in L : \mathrm{T}_{L/K}(xm) \in A \ \forall m \in M\},$$

which is an  $A$ -lattice in  $L$  isomorphic to the dual  $A$ -module  $M^{\vee} := \mathrm{Hom}_A(M, A)$  (see Theorem 5.12). In our *AKLB* setting we have  $M^{**} = M$ , by Proposition 5.16.

Every fractional ideal  $I$  of  $B$  is finitely generated as a  $B$ -module, and therefore finitely generated as an  $A$  module (since  $B$  is finite over  $A$ ). If  $I$  is nonzero, it necessarily spans  $L$ , since  $B$  does. It follows that every element of the group  $\mathcal{I}_B$  of nonzero fractional ideals of  $B$  is an  $A$ -lattice in  $L$ . We now show that  $\mathcal{I}_B$  is closed under the operation of taking duals.

**Lemma 12.1.** *Assume AKLB. If  $I \in \mathcal{I}_B$  then  $I^* \in \mathcal{I}_B$ .*

*Proof.* The dual lattice  $I^*$  is a finitely generated  $A$ -module, thus to show that it is a finitely generated  $B$ -module it is enough to show it is closed under multiplication by elements of  $B$ . So consider any  $b \in B$  and  $x \in I^*$ . For all  $m \in I$  we have  $\mathrm{T}_{L/K}((bx)m) = \mathrm{T}_{L/K}(x(bm)) \in A$ , since  $x \in I^*$  and  $bm \in I$ , so  $bx \in I^*$  as desired.  $\square$

**Definition 12.2.** *Assume AKLB. The different  $\mathcal{D}_{L/K}$  of  $L/K$  (and the different  $\mathcal{D}_{B/A}$  of  $B/A$ ), is the inverse of  $B^*$  in  $\mathcal{I}_B$ . Explicitly, we have*

$$B^* := \{x \in L : \mathrm{T}_{L/K}(xb) \in A \text{ for all } b \in B\},$$

and we define

$$\mathcal{D}_{L/K} := \mathcal{D}_{B/A} := (B^*)^{-1} = (B : B^*) = \{x \in L : xB^* \subseteq B\}.$$

Note that  $B \subseteq B^*$ , since  $\mathrm{T}_{L/K}(ab) \in A$  for  $a, b \in B$  (by Corollary 4.53), and this implies  $\mathcal{D}_{B/A} = (B^*)^{-1} \subseteq B^{-1} = B$ . Thus the different is an ideal, not just a fractional ideal.

<sup>1</sup>Note that  $B/\mathfrak{q}^{e_{\mathfrak{q}}}$  is reduced if and only if  $e_{\mathfrak{q}} = 1$ ; consider the image of a uniformizer in  $B/\mathfrak{q}^{e_{\mathfrak{q}}}$ .

<sup>2</sup>As usual, by a *prime* of  $A$  or  $K$  we mean a nonzero prime ideal of  $A$ , and similarly for  $B$  and  $L$ . The notation  $\mathfrak{q}|\mathfrak{p}$  means that  $\mathfrak{q}$  is a prime of  $B$  lying above  $\mathfrak{p}$  (so  $\mathfrak{p} = \mathfrak{q} \cap A$  and  $\mathfrak{q}$  divides  $\mathfrak{p}B$ ).

The different respects localization and completion.

**Proposition 12.3.** *Assume AKLB and let  $S$  be a multiplicative subset of  $A$ . Then*

$$S^{-1}\mathcal{D}_{B/A} = \mathcal{D}_{S^{-1}B/S^{-1}A}.$$

*Proof.* This follows from the fact that inverses and duals are both compatible with localization, by Lemmas 3.5 and 5.15.  $\square$

**Proposition 12.4.** *Assume AKLB and let  $\mathfrak{q}|\mathfrak{p}$  be a prime of  $B$ . Then*

$$\mathcal{D}_{\hat{B}_{\mathfrak{q}}/\hat{A}_{\mathfrak{p}}} = \mathcal{D}_{B/A}\hat{B}_{\mathfrak{q}},$$

where  $\hat{A}_{\mathfrak{p}}$  and  $\hat{B}_{\mathfrak{q}}$  are the completions of  $A$  and  $B$  at  $\mathfrak{p}$  and  $\mathfrak{q}$ , respectively.

*Proof.* Let  $\hat{L} := L \otimes K_{\mathfrak{p}}$  be the base change of the finite étale  $K$ -algebra  $L$  to  $K_{\mathfrak{p}}$ . By (5) of Theorem 11.23, we have  $\hat{L} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$ . Note that even though  $\hat{L}$  need not be a field, in general, is a free  $K_{\mathfrak{p}}$ -module of finite rank, and is thus equipped with a trace map that necessarily satisfies  $\mathrm{T}_{\hat{L}/K_{\mathfrak{p}}}(x) = \sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{T}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(x)$  that defines a trace pairing on  $\hat{L}$ .

Now let  $\hat{B} := B \otimes \hat{A}_{\mathfrak{p}}$ ; it is an  $A_{\mathfrak{p}}$ -lattice in the  $K_{\mathfrak{p}}$ -vector space  $\hat{L}$ . By Corollary 11.26,  $\hat{B} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}} \simeq \bigoplus_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}$ , and therefore  $\hat{B}^* \simeq \bigoplus_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}^*$ , by Corollary 5.13. It follows that  $\hat{B}^* \simeq B^* \otimes_A \hat{A}_{\mathfrak{p}}$ . In particular,  $B^*$  generates each fractional ideal  $\hat{B}_{\mathfrak{q}}^* \in \mathcal{I}_{\hat{B}_{\mathfrak{q}}}$ . Taking inverses,  $\mathcal{D}_{B/A} = (B^*)^{-1}$  generates the  $\hat{B}_{\mathfrak{q}}$ -ideal  $(\hat{B}_{\mathfrak{q}}^*)^{-1} = \mathcal{D}_{\hat{B}_{\mathfrak{q}}/\hat{A}_{\mathfrak{p}}}$ .  $\square$

## 12.2 The discriminant

**Definition 12.5.** Let  $S/R$  be a ring extension in which  $S$  is a free  $R$ -module of rank  $n$ . For any  $x_1, \dots, x_n \in S$  we define the *discriminant*

$$\mathrm{disc}(x_1, \dots, x_n) := \mathrm{disc}_{S/R}(x_1, \dots, x_n) := \det[\mathrm{T}_{S/R}(x_i x_j)]_{i,j} \in R.$$

Note that we do not require  $x_1, \dots, x_n$  to be an  $R$ -basis for  $S$ , but if they satisfy a non-trivial  $R$ -linear relation then the discriminant will be zero (by linearity of the trace).

In our AKLB setup, we have in mind the case where  $e_1, \dots, e_n \in B$  is a basis for  $L$  as a  $K$ -vector space, in which case  $\mathrm{disc}(e_1, \dots, e_n) = \det[\mathrm{T}_{L/K}(e_i e_j)]_{i,j} \in A$ . Note that we do not need to assume that  $B$  is a free  $A$ -module;  $L$  is certainly a free  $K$ -module. The fact that the discriminant lies in  $A$  when  $e_1, \dots, e_n \in B$  follows immediately from Corollary 4.53.

**Proposition 12.6.** *Let  $L/K$  be a finite separable extension of degree  $n$ , and let  $\Omega/K$  be a field extension for which there are distinct  $\sigma_1, \dots, \sigma_n \in \mathrm{Hom}_K(L, \Omega)$ . For any  $e_1, \dots, e_n \in L$  we have*

$$\mathrm{disc}(e_1, \dots, e_n) = \det[\sigma_i(e_j)]_{i,j}^2,$$

and for any  $x \in L$  we have

$$\mathrm{disc}(1, x, x^2, \dots, x^{n-1}) = \prod_{i < j} (\sigma_i(x) - \sigma_j(x))^2.$$

Such a field extension  $\Omega/K$  always exists, since  $L/K$  is separable ( $\Omega = K^{\mathrm{sep}}$  works).

*Proof.* For  $1 \leq i, j \leq n$  we have  $\mathbb{T}_{L/K}(e_i e_j) = \sum_{k=1}^n \sigma_k(e_i e_j)$ , by Theorem 4.50. Therefore

$$\begin{aligned} \text{disc}(e_1, \dots, e_n) &= \det[\mathbb{T}_{L/K}(e_i e_j)]_{ij} \\ &= \det([\sigma_k(e_i)]_{ik} [\sigma_k(e_j)]_{kj}) \\ &= \det([\sigma_k(e_i)]_{ik} [\sigma_k(e_j)]_{jk}^t) \\ &= \det[\sigma_i(e_j)]_{ij}^2 \end{aligned}$$

since the determinant is multiplicative and  $\det M = \det M^t$  for any matrix  $M$ .

Now let  $x \in L$  and put  $e_i := x^{i-1}$  for  $1 \leq i \leq n$ . Then

$$\text{disc}(1, x, x^2, \dots, x^{n-1}) = \det[\sigma_i(x^{j-1})]_{ij}^2 = \det[\sigma_i(x)^{j-1}]_{ij}^2 = \prod_{i < j} (\sigma_i(x) - \sigma_j(x))^2,$$

since  $[\sigma_i(x)^{j-1}]_{ij}$  is a Vandermonde matrix (rows of the form  $z^0, \dots, z^{n-1}$  for some  $z$ ); see [2, p. 258] for a proof of this standard fact.  $\square$

**Definition 12.7.** For a polynomial  $f(x) = \prod_i (x - \alpha_i)$ , the *discriminant* of  $f$  is

$$\text{disc}(f) := \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

Equivalently, if  $A$  is a Dedekind domain,  $f \in A[x]$  is a monic separable polynomial, and  $\alpha$  is the image of  $x$  in  $A[x]/(f(x))$ , then

$$\text{disc}(f) = \text{disc}(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) \in A.$$

**Example 12.8.**  $\text{disc}(x^2 + bx + c) = b^2 - 4c$  and  $\text{disc}(x^3 + ax + b) = -4a^3 - 27b^2$ .

Now assume *AKLB* and let  $M$  be an  $A$ -lattice in  $L$ . Then  $M$  is a finitely generated  $A$ -module that contains a  $K$ -basis for  $L$ . We want to define the discriminant of  $M$  in a way that does not require us to choose a basis.

Let us first consider the case where  $M$  is a free  $A$ -lattice. If  $e_1, \dots, e_n \in M \subseteq L$  and  $e'_1, \dots, e'_n \in M \subseteq L$  are two  $A$ -bases for  $M$ , then

$$\text{disc}(e'_1, \dots, e'_n) = u^2 \text{disc}(e_1, \dots, e_n)$$

for some unit  $u \in A^\times$ ; this follows from the fact that the change of basis matrix  $P \in A^{n \times n}$  is invertible and its determinant is therefore a unit  $u$ . This unit gets squared because we need to apply the change of basis matrix twice in order to change  $\mathbb{T}(e_i e_j)$  to  $\mathbb{T}(e'_i e'_j)$ . Explicitly, writing bases as row-vectors, let  $e = (e_1, \dots, e_n)$  and  $e' = (e'_1, \dots, e'_n)$  satisfy  $e' = eP$ . Then

$$\begin{aligned} \text{disc}(e') &= \det[\mathbb{T}_{L/K}(e'_i e'_j)]_{ij} \\ &= \det[\mathbb{T}_{L/K}((eP)_i (eP)_j)]_{ij} \\ &= \det[P^t \mathbb{T}_{L/K}(e_i e_j) P]_{ij} \\ &= (\det P^t) \text{disc}(e) (\det P) \\ &= (\det P)^2 \text{disc}(e), \end{aligned}$$

where we have used the linearity of  $\mathbb{T}_{L/K}$  to go from the second equality to the third.

This actually gives us a basis independent definition when  $A = \mathbb{Z}$ . In this case  $B$  is always a free  $\mathbb{Z}$ -lattice, and the only units in  $\mathbb{Z}$  are  $u = \pm 1$ , so  $u^2 = 1$ .

**Definition 12.9.** Assume  $AKLB$ , let  $M$  be an  $A$ -lattice in  $L$ , and let  $n := [L : K]$ . The *discriminant*  $D(M)$  of  $M$  is the  $A$ -module generated by  $\{\text{disc}(x_1, \dots, x_n) : x_1, \dots, x_n \in M\}$ .

**Lemma 12.10.** Assume  $AKLB$  and let  $M' \subseteq M$  be free  $A$ -lattices in  $L$ . The discriminants  $D(M') \subseteq D(M)$  are nonzero principal fractional ideals. If  $D(M') = D(M)$  then  $M' = M$ .

*Proof.* Let  $e := (e_1, \dots, e_n)$  be an  $A$ -basis for  $M$ . Then  $\text{disc}(e) \in D(M)$ , and for any row vector  $x := (x_1, \dots, x_n)$  with entries in  $M$  there is a matrix  $P \in A^{n \times n}$  for which  $x = eP$ , and we then have  $\text{disc}(x) = (\det P)^2 \text{disc}(e)$  as above. It follows that

$$D(M) = (\text{disc}(e))$$

is principal, and it is nonzero because  $e$  is a basis for  $L$  and the trace pairing is nondegenerate. If we now let  $e' := (e'_1, \dots, e'_n)$  be an  $A$ -basis for  $M'$  then  $D(M') = (\text{disc}(e'))$  is also a nonzero and principal. Our assumption that  $M' \subseteq M$  implies that  $e' = eP$  for some matrix  $P \in A^{n \times n}$ , and we have  $\text{disc}(e') = (\det P)^2 \text{disc}(e)$ . If  $D(M') = D(M)$  then  $\det P$  must be a unit, in which case  $P$  is invertible and  $e = e'P^{-1}$ . This implies  $M \subseteq M'$ .  $\square$

**Proposition 12.11.** Assume  $AKLB$  and let  $M$  be an  $A$ -lattice in  $L$ . Then  $D(M) \in \mathcal{I}_A$ .

*Proof.* The  $A$ -module  $D(M) \subseteq K$  is nonzero because  $M$  contains a  $K$ -basis  $e = (e_1, \dots, e_n)$  for  $L$  and  $\text{disc}(e) \neq 0$  because the trace pairing is nondegenerate. To show that  $D(M)$  is a finitely generated  $A$ -module (and thus a fractional ideal), we use the usual trick: make it a submodule of a noetherian module. So let  $N$  be the free  $A$ -lattice in  $L$  generated by  $e$  and then pick a nonzero  $a \in A$  such that  $M \subseteq a^{-1}N$  (write each generator for  $M$  in terms of the  $K$ -basis  $e$  and let  $a$  be the product of all the denominators that appear; note that  $M$  is finitely generated). We then have  $D(M) \subseteq D(a^{-1}N)$ , and  $D(a^{-1}N)$  is a principal fractional ideal of  $A$ , hence a noetherian  $A$ -module (since  $A$  is noetherian), so its submodule  $D(M)$  must be finitely generated.  $\square$

**Definition 12.12.** Assume  $AKLB$ . The *discriminant*  $D_{L/K}$  of  $L/K$  (and the *discriminant*  $D_{B/A}$  of  $B/A$ ) is the discriminant of  $B$  as an  $A$ -module:

$$D_{L/K} := D_{B/A} := D(B) \in \mathcal{I}_A,$$

which is an  $A$ -ideal, since  $\text{disc}(x_1, \dots, x_n) = \det[T_{B/A}(x_i x_j)]_{i,j} \in A$  for all  $x_1, \dots, x_n \in B$ .

**Example 12.13.** Consider the case  $A = \mathbb{Z}$ ,  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}(i)$ ,  $B = \mathbb{Z}[i]$ . Then  $B$  is a free  $A$ -lattice with basis  $(1, i)$  and we can compute  $D_{L/K}$  in three ways:

- $\text{disc}(1, i) = \det \begin{bmatrix} T_{L/K}(1 \cdot 1) & T_{L/K}(1 \cdot i) \\ T_{L/K}(i \cdot 1) & T_{L/K}(i \cdot i) \end{bmatrix} = \det \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} = -4.$
- The non-trivial automorphism of  $L/K$  fixes 1 and sends  $i$  to  $-i$ , so we could instead compute  $\text{disc}(1, i) = \left( \det \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix} \right)^2 = (-2i)^2 = -4.$
- We have  $B = \mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 + 1)$  and can compute  $\text{disc}(x^2 + 1) = -4.$

In every case the discriminant  $D_{L/K}$  is the ideal  $(-4) = (4)$ .

**Remark 12.14.** If  $A = \mathbb{Z}$  then  $B$  is the ring of integers of the number field  $L$ , and  $B$  is a free  $A$ -lattice, because it is a torsion-free module over a PID and therefore a free module. In this situation it is customary to define the *absolute discriminant*  $D_L$  of the number field  $L$  to be the *integer*  $\text{disc}(e_1, \dots, e_n) \in \mathbb{Z}$ , for any basis  $(e_1, \dots, e_n)$  of  $B$ , rather than the ideal it generates. As noted above, this integer is independent of the choice of basis because  $u^2 = 1$  for all  $u \in \mathbb{Z}^\times$ ; in particular, the sign of  $D_L$  is well defined (as we shall see, the sign of  $D_L$  carries information about  $L$ ). In the example above, the absolute discriminant is  $D_L = -4$ .

Like the different, the discriminant respects localization.

**Proposition 12.15.** *Assume AKLB and let  $S$  be a multiplicative subset of  $A$ . Then*

$$S^{-1}D_{B/A} = D_{S^{-1}B/S^{-1}A}.$$

*Proof.* Let  $x = s^{-1} \text{disc}(e_1, \dots, e_n) \in S^{-1}D_{B/A}$  for some  $s \in S$  and  $e_1, \dots, e_n \in B$ . Then  $x = s^{2n-1} \text{disc}(s^{-1}e_1, \dots, s^{-1}e_n)$  lies in  $D_{S^{-1}B/S^{-1}A}$ . This proves the forward inclusion.

Conversely, for any  $e_1, \dots, e_n \in S^{-1}B$  we can choose a single  $s \in S \subseteq A$  so that each  $se_i$  lies in  $B$ . We then have  $\text{disc}(e_1, \dots, e_n) = s^{-2n} \text{disc}(se_1, \dots, se_n) \in S^{-1}D_{B/A}$ , which proves the reverse inclusion.  $\square$

**Proposition 12.16.** *Assume AKLB and let  $\mathfrak{p}$  be a prime of  $A$ . Then*

$$D_{B/A}\hat{A}_{\mathfrak{p}} = \prod_{\mathfrak{q}|\mathfrak{p}} D_{\hat{B}_{\mathfrak{q}}/\hat{A}_{\mathfrak{p}}}$$

where  $\hat{A}_{\mathfrak{p}}$  and  $\hat{B}_{\mathfrak{q}}$  are the completions of  $A$  and  $B$  at  $\mathfrak{p}$  and  $\mathfrak{q}$ , respectively.

*Proof.* After localizing at  $\mathfrak{p}$  we can assume  $A$  is a DVR and  $B$  is a free  $A$ -module of rank  $n$ . As in the proof of Proposition 12.4, we have a trace pairing on the finite étale  $K_{\mathfrak{p}}$ -algebra  $\hat{L} := L \otimes K_{\mathfrak{p}}$  and  $\hat{B} := B \otimes \hat{A}_{\mathfrak{p}} \simeq \bigoplus_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}$  is an  $\hat{A}_{\mathfrak{p}}$ -lattice in the  $K_{\mathfrak{p}}$ -vector space  $\hat{L}$  that is a direct sum of free  $\hat{A}_{\mathfrak{p}}$ -modules, and thus a free  $\hat{A}_{\mathfrak{p}}$ -module of rank  $n = \sum e_{\mathfrak{q}}f_{\mathfrak{q}}$ ; see Corollary 11.26.

We can choose  $\hat{A}_{\mathfrak{p}}$  bases for each  $\hat{B}_{\mathfrak{q}}$  using elements in  $B$ ; this follows from weak approximation (Theorem 8.5) and the fact that  $B$  is dense in  $\hat{B}_{\mathfrak{q}}$  (or see [1, Thm. 2.3]). From these bases we can construct an  $\hat{A}_{\mathfrak{p}}$ -basis  $\hat{e}$  for the direct sum  $\bigoplus_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}} \simeq \hat{B}$  whose elements each have nonzero projections to exactly one of the  $\hat{B}_{\mathfrak{q}}$ , along with a corresponding  $A$ -basis  $e$  for  $B$  obtained from  $\hat{e}$  as the union of these projections.

The matrix  $[T_{\hat{L}/K_{\mathfrak{p}}}(\hat{e}_i\hat{e}_j)]$  is block diagonal; each block corresponds to a matrix whose determinant is the discriminant of the  $\hat{A}_{\mathfrak{p}}$ -basis we chose for one of the  $\hat{B}_{\mathfrak{q}}$ . It follows that  $D_{\hat{B}/\hat{A}_{\mathfrak{p}}} = \prod_{\mathfrak{q}|\mathfrak{p}} D_{\hat{B}_{\mathfrak{q}}/\hat{A}_{\mathfrak{p}}}$  (here we are using the fact that  $\hat{B} \simeq \bigoplus_{\mathfrak{q}|\mathfrak{p}} \hat{B}_{\mathfrak{q}}$  is both an isomorphism of rings and an isomorphism of  $A_{\mathfrak{p}}$ -modules, hence it preserves traces to  $\hat{A}_{\mathfrak{p}}$ ). We now observe that

$$\text{disc}_{B/A}(e_1, \dots, e_n) = \text{disc}_{(B \otimes A_{\mathfrak{p}})/\hat{A}_{\mathfrak{p}}}(e_1 \otimes 1, \dots, e_n \otimes 1)$$

generates  $D_{B/A}$  as an  $A$ -ideal, and also generates  $D_{\hat{B}/\hat{A}_{\mathfrak{p}}}$  as an  $\hat{A}_{\mathfrak{p}}$ -ideal (note that  $\hat{B}$  is a free  $\hat{A}_{\mathfrak{p}}$ -module, so  $D_{\hat{B}/\hat{A}_{\mathfrak{p}}}$  is the principal ideal generated by the discriminant of any  $A_{\mathfrak{p}}$ -basis for  $\hat{B}$ ). It follows that  $D_{B/A}\hat{A}_{\mathfrak{p}} = D_{\hat{B}/\hat{A}_{\mathfrak{p}}} = \prod_{\mathfrak{q}|\mathfrak{p}} D_{\hat{B}_{\mathfrak{q}}/\hat{A}_{\mathfrak{p}}}$ .  $\square$

We have defined two different ideals associated to a finite separable extension of Dedekind domains  $B/A$  in the *AKLB* setup. We have the different  $\mathcal{D}_{B/A}$ , which is a fractional ideal of  $B$ , and the discriminant  $D_{B/A}$ , which is a fractional ideal of  $A$ . We now relate these two ideals in terms of the ideal norm  $N_{B/A}: \mathcal{I}_B \rightarrow \mathcal{I}_A$ , which for  $I \in \mathcal{I}_B$  is defined as  $N_{B/A}(I) := [B : I]_A$ , where  $[B : I]_A$  is the module index (see Definitions 6.1 and 6.5).

**Theorem 12.17.** *Assume AKLB. Then  $D_{B/A} = N_{B/A}(\mathcal{D}_{B/A})$ .*

*Proof.* The different and discriminant are both compatible with localization, by Propositions 12.3 and 12.15, and the  $A$ -modules  $D_{B/A}$  and  $N_{B/A}(\mathcal{D}_{B/A})$  of  $A$  are both determined by the intersections of their localizations at maximal ideals (Proposition 2.6), so it suffices to prove that the theorem holds when we replace  $A$  by its localization  $A$  at a prime of  $A$ . Then  $A$  is a DVR and  $B$  is a free  $A$ -lattice in  $L$ ; let us fix an  $A$ -basis  $(e_1, \dots, e_n)$  for  $B$ .

The dual  $A$ -lattice

$$B^* = \{x \in L : \mathbb{T}_{L/K}(xb) \in A \ \forall b \in B\} \in \mathcal{I}_B$$

is also a free  $A$ -lattice in  $L$ , with basis  $(e_1^*, \dots, e_n^*)$  uniquely determined by  $\mathbb{T}_{L/K}(e_i^* e_j) = \delta_{ij}$ , where  $\delta_{ij}$  is the Kronecker delta function; see Corollary 5.14. If we write  $e_i = \sum a_{ij} e_j^*$  in terms of the  $K$ -basis  $(e_1^*, \dots, e_n^*)$  for  $L$  then

$$\mathbb{T}_{L/K}(e_i e_j) = \mathbb{T}_{L/K} \left( \sum_k a_{ik} e_k^* e_j \right) = \sum_k a_{ik} \mathbb{T}_{L/K}(e_k^* e_j) = \sum_k a_{ik} \delta_{kj} = a_{ij}.$$

It follows that  $P := [\mathbb{T}_{L/K}(e_i e_j)]_{ij}$  is the change-of-basis matrix from  $e^* := (e_1^*, \dots, e_n^*)$  to  $e := (e_1, \dots, e_n)$  (as row vectors we have  $e = e^* P$ ). If we let  $\phi$  denote the  $K$ -linear transformation with matrix  $P$  (or its transpose, if you prefer to work with column vectors), then  $\phi$  is an isomorphism of free  $A$ -modules and

$$D_{B/A} = (\det[\mathbb{T}_{L/K}(e_i e_j)]_{ij}) = (\det \phi) = [B^* : B]_A,$$

where  $[B^* : B]_A$  is the module index (see Definition 6.1). Applying Corollary 6.8 yields

$$D_{B/A} = [B^* : B]_A = N_{B/A}((B : B^*)) = N_{B/A}((B^*)^{-1}) = N_{B/A}(\mathcal{D}_{B/A}).$$

(the last three equalities each hold by definition). □

### 12.3 Ramification

Having defined the different and discriminant ideals we now want to understand how they relate to ramification. Recall that in our *AKLB* setup, if  $\mathfrak{p}$  is a prime of  $A$  then we can factor the  $B$ -ideal  $\mathfrak{p}B$  as

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}.$$

The Chinese remainder theorem implies

$$B/\mathfrak{p}B \simeq B/\mathfrak{q}_1^{e_1} \times \cdots \times B/\mathfrak{q}_r^{e_r}.$$

This is a commutative  $A/\mathfrak{p}$ -algebra of dimension  $\sum e_i f_i$ , where  $f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$  is the residue degree (see Theorem 5.34). It is a product of fields if and only if we have  $e_i = 1$  for all  $i$ , and it is a finite étale-algebra if and only if it is a product of fields that are separable extensions of  $A/\mathfrak{p}$ . The following lemma relates the discriminant to the property of being a finite étale algebra.

**Lemma 12.18.** *Let  $k$  be a field and let  $R$  be a commutative  $k$ -algebra with  $k$ -basis  $r_1, \dots, r_n$ . Then  $R$  is a finite étale  $k$ -algebra if and only if  $\text{disc}(r_1, \dots, r_n) \neq 0$ .*

*Proof.* By Theorem 5.20,  $R$  is a finite étale  $k$ -algebra if and only if the trace pairing on  $R$  is a perfect pairing, which is equivalent to being nondegenerate, since  $k$  is a field.

If the trace pairing is degenerate then for some nonzero  $x \in R$  we have  $\text{Tr}_{R/k}(xy) = 0$  for all  $y \in R$ . If we write  $x = \sum_i x_i r_i$  with  $x_i \in k$  then  $\text{Tr}_{R/k}(xr_j) = \sum_i x_i \text{Tr}_{R/k}(r_i r_j) = 0$  for all  $r_j$  (take  $y = r_j$ ), and this implies that the columns of the matrix  $[\text{Tr}_{R/k}(r_i r_j)]_{ij}$  are linearly dependent and  $\text{disc}(r_1, \dots, r_n) = \det[\text{Tr}_{R/k}(r_i r_j)]_{ij} = 0$ .

Conversely, if  $\text{disc}(r_1, \dots, r_n) = 0$  then the columns of  $\det[\text{Tr}_{R/k}(r_i r_j)]_{ij}$  are linearly dependent and for some  $x_i \in k$  not identically zero we must have  $\sum_i x_i \text{Tr}_{R/k}(r_i r_j) = 0$  for all  $j$ . For  $x := \sum_i x_i r_i$  and any  $y = \sum_j y_j r_j \in R$  we have  $\text{Tr}_{R/k}(xy) = \sum_j y_j \sum_i x_i \text{Tr}_{R/k}(r_i r_j) = 0$ , which shows that the trace pairing is degenerate.  $\square$

**Theorem 12.19.** *Assume AKLB, let  $\mathfrak{q}$  be a prime of  $B$  lying above a prime  $\mathfrak{p}$  of  $A$  such that  $B/\mathfrak{q}$  is a separable extension of  $A/\mathfrak{p}$ . The extension  $L/K$  is unramified at  $\mathfrak{q}$  if and only if  $\mathfrak{q}$  does not divide  $\mathcal{D}_{B/A}$ , and it is unramified at  $\mathfrak{p}$  if and only if  $\mathfrak{p}$  does not divide  $D_{B/A}$ .*

*Proof.* We first consider the different  $\mathcal{D}_{B/A}$ . By Proposition 12.4, the different is compatible with completion, so it suffices to consider the case that  $A$  and  $B$  are complete DVRs (complete  $K$  at  $\mathfrak{p}$  and  $L$  at  $\mathfrak{q}$  and apply Theorem 11.23). We then have  $[L : K] = e_{\mathfrak{q}} f_{\mathfrak{q}}$ , where  $e_{\mathfrak{q}}$  is the ramification index and  $f_{\mathfrak{q}}$  is the residue field degree, and  $\mathfrak{p}B = \mathfrak{q}^{e_{\mathfrak{q}}}$ .

Since  $B$  is a DVR with maximal ideal  $\mathfrak{q}$ , we must have  $\mathcal{D}_{B/A} = \mathfrak{q}^m$  for some  $m \geq 0$ . By Theorem 12.17 we have

$$D_{B/A} = N_{B/A}(\mathcal{D}_{B/A}) = N_{B/A}(\mathfrak{q}^m) = \mathfrak{p}^{f_{\mathfrak{q}} m}.$$

Thus  $\mathfrak{q} | \mathcal{D}_{B/A}$  if and only if  $\mathfrak{p} | D_{B/A}$ . Since  $A$  is a PID,  $B$  is a free  $A$ -module and we may choose an  $A$ -module basis  $e_1, \dots, e_n$  for  $B$  that is also a  $K$ -basis for  $L$ . Let  $k := A/\mathfrak{p}$ , and let  $\bar{e}_i$  be the reduction of  $e_i$  to the  $k$ -algebra  $R := B/\mathfrak{p}B$ . Then  $(\bar{e}_1, \dots, \bar{e}_n)$  is a  $k$ -basis for  $R$ : it clearly spans, and we have  $[R : k] = [B/\mathfrak{q}^{e_{\mathfrak{q}}} : A/\mathfrak{p}] = e_{\mathfrak{q}} f_{\mathfrak{q}} = [L : K] = n$ .

Since  $B$  has an  $A$ -module basis, we may compute its discriminant as

$$D_{B/A} = (\text{disc}(e_1, \dots, e_n)).$$

Thus  $\mathfrak{p} | D_{B/A}$  if and only if  $\text{disc}(e_1, \dots, e_n) \in \mathfrak{p}$ , equivalently,  $\text{disc}(\bar{e}_1, \dots, \bar{e}_n) = 0$  (note that  $\text{disc}(e_1, \dots, e_n)$  is a polynomial in the  $\text{Tr}_{L/K}(e_i e_j)$  and  $\text{Tr}_{R/k}(\bar{e}_i \bar{e}_j)$  is the trace of the multiplication-by- $\bar{e}_i \bar{e}_j$  map, which is the same as the reduction to  $k = A/\mathfrak{p}$  of the trace of the multiplication-by- $e_i e_j$  map  $\text{Tr}_{L/K}(e_i e_j) \in A$ ). By Lemma 12.18,  $\text{disc}(\bar{e}_1, \dots, \bar{e}_n) = 0$  if and only if the  $k$ -algebra  $B/\mathfrak{p}B$  is not finite étale, equivalently, if and only if  $\mathfrak{p}$  is ramified. Thus  $\mathfrak{p} | D_{B/A}$  if and only if  $\mathfrak{p}$  is ramified. There is only one prime  $\mathfrak{q}$  above  $\mathfrak{p}$ , so we also have  $\mathfrak{q} | \mathcal{D}_{B/A}$  if and only if  $\mathfrak{q}$  is ramified.  $\square$

We now note an important corollary of Theorem 12.19.

**Corollary 12.20.** *Assume AKLB. Only finitely many primes of  $A$  (or  $B$ ) ramify.*

*Proof.*  $A$  and  $B$  are Dedekind domains, so the ideals  $D_{B/A}$  and  $\mathcal{D}_{B/A}$  both have unique factorizations into prime ideals in which only finitely many primes appear.  $\square$

## 12.4 The discriminant of an order

Recall from Lecture 6 that an order  $\mathcal{O}$  is a noetherian domain of dimension one whose conductor is nonzero (see Definitions 6.16 and 6.19), and the integral closure of an order is always a Dedekind domain. In our *AKLB* setup, the orders with integral closure  $B$  are precisely the  $A$ -lattices in  $L$  that are rings (see Proposition 6.22); if  $L = K(\alpha)$  with  $\alpha \in B$ , then  $A[\alpha]$  is an example. The discriminant  $D_{\mathcal{O}/A}$  of such an order  $\mathcal{O}$  is its discriminant  $D(\mathcal{O})$  as an  $A$ -module. The fact that  $\mathcal{O} \subseteq B$  implies that  $D(\mathcal{O}) \subseteq D_{B/A}$  is an  $A$ -ideal.

If  $\mathcal{O}$  is an order of the form  $A[\alpha]$ , where  $\alpha \in B$  generates  $L = K(\alpha)$  with minimal polynomial  $f \in A[x]$ , then  $\mathcal{O}$  is a free  $A$ -lattice with basis  $1, \alpha, \dots, \alpha^{n-1}$ , where  $n = \deg f$ , and we may compute its discriminant as

$$D_{\mathcal{O}/A} = (\text{disc}(1, \alpha, \dots, \alpha^{n-1})) = (\text{disc}(f)),$$

which is a principal  $A$ -ideal contained in  $D_{B/A}$ . If  $B$  is also a free  $A$ -lattice, then as in the proof of Lemma 12.10 we have

$$D_{\mathcal{O}/A} = (\det P)^2 D_{B/A} = [B:\mathcal{O}]_A^2 D_{B/A},$$

where  $P$  is the matrix of the  $A$ -linear map  $\phi: B \rightarrow \mathcal{O}$  that sends an  $A$ -basis for  $B$  to an  $A$ -basis for  $\mathcal{O}$  and  $[B:\mathcal{O}]_A$  is the module index (a principal  $A$ -ideal).

In the important special case where  $A = \mathbb{Z}$  and  $L$  is a number field, the integer  $(\det P)^2$  is uniquely determined and it necessarily divides  $\text{disc}(f)$ , the generator of the principal ideal  $D(\mathcal{O}) = D(A[\alpha])$ . It follows that if  $\text{disc}(f)$  is squarefree then we must have  $B = \mathcal{O} = A[\alpha]$ . More generally, any prime  $p$  for which  $v_p(\text{disc}(f))$  is odd must be ramified, and any prime that does not divide  $\text{disc}(f)$  must be unramified. Another useful observation that applies when  $A = \mathbb{Z}$ : the module index  $[B:\mathcal{O}]_{\mathbb{Z}} = ([B:\mathcal{O}])$  is the principal ideal generated by the index of  $\mathcal{O}$  in  $B$  (as  $\mathbb{Z}$ -lattices), and we have the relation

$$D_{\mathcal{O}} = [B:\mathcal{O}]^2 D_B$$

between the absolute discriminant of the order  $\mathcal{O}$  and its integral closure  $B$ .

**Example 12.21.** Consider  $A = \mathbb{Z}$ ,  $K = \mathbb{Q}$  with  $L = \mathbb{Q}(\alpha)$ , where  $\alpha^3 - \alpha - 1 = 0$ . We can compute the absolute discriminant of  $\mathbb{Z}[\alpha]$  as

$$\text{disc}(1, \alpha, \alpha^2) = \text{disc}(x^3 - x - 1) = -4(-1)^3 - 27(-1)^2 = -23.$$

The fact that  $-23$  is squarefree immediately implies that 23 is the only prime of  $A$  that ramifies, and we have  $D_{\mathbb{Z}[\alpha]} = -23 = [\mathcal{O}_L : \mathbb{Z}[\alpha]]^2 D_L$ , which forces  $[\mathcal{O}_L : \mathbb{Z}[\alpha]] = 1$ , so  $D_L = -23$  and  $\mathcal{O}_L = \mathbb{Z}[\alpha]$ .

More generally, we have the following theorem.

**Theorem 12.22.** *Assume AKLB and let  $\mathcal{O}$  be an order with integral closure  $B$  and conductor  $\mathfrak{c}$ . Then  $D_{\mathcal{O}/A} = N_{B/A}(\mathfrak{c})D_{B/A}$ .*

*Proof.* See Problem Set 6. □



## 12.5 Computing the discriminant and different

We conclude with a number of results that allow one to explicitly compute the discriminant and different in many cases.

**Proposition 12.23.** *Assume  $AKLB$ . If  $B = A[\alpha]$  for some  $\alpha \in L$  and  $f \in A[x]$  is the minimal polynomial of  $\alpha$ , then*

$$\mathcal{D}_{B/A} = (f'(\alpha))$$

*is the  $B$ -ideal generated by  $f'(\alpha)$ .*

*Proof.* See Problem Set 6. □

The assumption  $B = A[\alpha]$  in Proposition 12.23 does not always hold, but if we want to compute the power of  $\mathfrak{q}$  that divides  $\mathcal{D}_{B/A}$  we can complete  $L$  at  $\mathfrak{q}$  and  $K$  at  $\mathfrak{p} = \mathfrak{q} \cap A$  so that  $A$  and  $B$  become complete DVRs, in which case  $B = A[\alpha]$  does hold (by Lemma 10.14), so long as the residue field extension is separable (always true if  $K$  and  $L$  are global fields, since the residue fields are then finite, hence perfect). The following definition and proposition give an alternative approach.

**Definition 12.24.** Assume  $AKLB$  and let  $\alpha \in B$  have minimal polynomial  $f \in A[x]$ . The *different* of  $\alpha$  is defined by

$$\delta_{B/A}(\alpha) := \begin{cases} f'(\alpha) & \text{if } L = K(\alpha), \\ 0 & \text{otherwise.} \end{cases}$$

**Proposition 12.25.** *Assume  $AKLB$ . Then  $\mathcal{D}_{B/A} = (\delta_{B/A}(\alpha) : \alpha \in B)$ .*

*Proof.* See [3, Thm. III.2.5]. □

We can now more precisely characterize the ramification information given by the different ideal.

**Theorem 12.26.** *Assume  $AKLB$  and let  $\mathfrak{q}$  be a prime of  $L$  lying above  $\mathfrak{p} = \mathfrak{q} \cap A$  for which the residue field extension  $(B/\mathfrak{q})/(A/\mathfrak{p})$  is separable. Then*

$$e_{\mathfrak{q}} - 1 \leq v_{\mathfrak{q}}(\mathcal{D}_{B/A}) \leq e_{\mathfrak{q}} - 1 + v_{\mathfrak{q}}(e_{\mathfrak{q}}),$$

*and the lower bound is an equality if and only if  $\mathfrak{q}$  is tamely ramified.*

*Proof.* See Problem Set 6. □

We also note the following proposition, which shows how the discriminant and different behave in a tower of extensions.

**Proposition 12.27.** *Assume  $AKLB$  and let  $M/L$  be a finite separable extension and let  $C$  be the integral closure of  $A$  in  $M$ . Then*

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B} \cdot \mathcal{D}_{B/A}$$

*(where the product on the right is taken in  $C$ ), and*

$$D_{C/A} = (D_{B/A})^{[M:L]} N_{B/A}(D_{C/B}).$$

*Proof.* See [4, Prop. III.8]. □

If  $M/L/K$  is a tower of finite separable extensions, we note that the primes  $\mathfrak{p}$  of  $K$  that ramify are precisely those that divide either  $D_{L/K}$  or  $N_{L/K}(D_{M/L})$ .

## References

- [1] A. Jakhar, B. Jhorar, S. K. Khanduja, N. Sangwan, *Discriminant as a product of local discriminant*, J. Algebra App. **16** (2017), 1750198 (7 pages).
- [2] S. Lang, *Algebra*, third edition, Springer, 2002.
- [3] J. Neukirch, *Algebraic number theory*, Springer, 1999.
- [4] J.-P. Serre, *Local fields*, Springer, 1979.
- [5] Stacks Project Authors, *Stacks Project*, <http://stacks.math.columbia.edu>.