11 Completing extensions, different and discriminant ideals

11.1 Local extensions come from global extensions

Let $\hat{L}$ be a local field. From our classification of local fields (Theorem 9.7), we know $\hat{L}$ is a finite extension of $\hat{K} = \mathbb{Q}_p$ (some prime $p \leq \infty$) or $\hat{K} = \mathbb{F}_q((t))$ (some prime power $q$). We also know that the completion of a global field at any of its nontrivial absolute values is such a local field (Corollary 9.5). It thus reasonable to ask whether $\hat{L}$ is the completion of a corresponding global field $L$ that is a finite extension of $K = \mathbb{Q}$ or $K = \mathbb{F}_q((t))$.

More generally, for any fixed global field $K$ and local field $\hat{K}$ that is the completion of $K$ with respect to one of its nontrivial absolute values $| |$, we may ask whether every finite extension of local fields $\hat{L}/\hat{K}$ necessarily corresponds to an extension of global fields $L/K$, where $\hat{L}$ is the completion of $L$ with respect to one of its absolute values (whose restriction to $\hat{K}$ must be equivalent to $| |$). The answer is yes. In order to simplify matters we restrict our attention to the case where $\hat{L}/\hat{K}$ is separable, but this is true in general.

**Theorem 11.1.** Let $K$ be a global field with a nontrivial absolute value $| |$, and let $\hat{K}$ be the completion of $K$ with respect to $| |$. Every finite separable extension $\hat{L}$ of $\hat{K}$ is the completion of a finite separable extension $L$ of $K$ with respect to an absolute value that restricts to $| |$. Moreover, one can choose $L$ so that $\hat{L}$ is the compositum of $L$ and $\hat{K}$ and $[\hat{L} : \hat{K}] = [L : K]$.

**Proof.** Let $\hat{L}/\hat{K}$ be a separable extension of degree $n$. Let us first suppose that $| |$ is archimedean. Then $K$ is a number field and $\hat{K}$ is either $\mathbb{R}$ or $\mathbb{C}$; the only nontrivial case is when $\hat{K} = \mathbb{C}$ and $n = 2$, and we may then assume that $\hat{L} \simeq \mathbb{C}$ is $\hat{K}(\sqrt{-d})$ where $-d \in \mathbb{Z}_{<0}$ is a nonsquare in $K$ (such a $-d$ exists because $K/\mathbb{Q}$ is finite). We may assume without loss of generality that $| |$ is the Euclidean absolute value on $\hat{K} \simeq \mathbb{R}$ (it must be equivalent to it), and uniquely extend $| |$ to $L = K(\sqrt{-d})$ by requiring $|\sqrt{-d}| = \sqrt{d}$. Then $\hat{L}$ is the completion of $L$ with respect to $| |$, and clearly $[\hat{L} : \hat{K}] = [L : K] = 2$, and $\hat{L}$ is the compositum of $L$ and $\hat{K}$.

We now suppose that $| |$ is nonarchimedean, in which case the valuation ring of $\hat{K}$ is a complete DVR and $| |$ is induced by the corresponding discrete valuation. By the primitive element theorem (Theorem 4.33), we may assume $\hat{L} = \hat{K}[x]/(f)$ where $f \in \hat{K}[x]$ is monic, irreducible, and separable. The field $K$ is dense in its completion $\hat{K}$, so we can find a monic $g \in K[x] \subseteq \hat{K}[x]$ that is arbitrarily close to $f$: such that $\|g - f\|_1 < \delta$ for any $\delta > 0$. It then follows from Proposition 10.30 that $\hat{L} = \hat{K}[x]/(g)$ (and that $g$ is separable). The field $\hat{L}$ is a finite separable extension of the fraction field of a complete DVR, so by Theorem 9.25 it is itself the fraction field of a complete DVR and has a unique absolute value that extends the absolute value $| |$ on $\hat{K}$.

Now let $L = \hat{K}[x]/(g)$. The polynomial $g$ is irreducible in $\hat{K}[x]$, hence in $K[x]$, so $[L : K] = \deg g = [\hat{L} : \hat{K}]$. The field $\hat{L}$ contains both $\hat{K}$ and $L$, and it is clearly the smallest field that does (since $g$ is irreducible in $\hat{K}[x]$), so $\hat{L}$ is the compositum of $\hat{K}$ and $L$. The absolute value on $\hat{L}$ restricts to an absolute value on $L$ extending the absolute value $| |$ on $K$, and $\hat{L}$ is complete, so $\hat{L}$ contains the completion of $L$ with respect to $| |$. On the other hand, the completion of $L$ with respect $| |$ contains both $L$ and $\hat{K}$, so it must be $\hat{L}$. \qed

In the preceding theorem, when the local extension $\hat{L}/\hat{K}$ is Galois one might ask whether the corresponding global extension $L/K$ is also Galois, and whether $\text{Gal}(\hat{L}/\hat{K}) \simeq \text{Gal}(L/K)$. As shown by the following example, this need not be the case.
Example 11.2. Let $K = \mathbb{Q}$, $\bar{K} = \mathbb{Q}_7$ and $\bar{L} = \bar{K}[x]/(x^3 - 2)$. The extension $\bar{L}/\bar{K}$ is Galois because $\bar{K} = \mathbb{Q}_7$ contains $\zeta_3$ (we can lift the root 2 of $x^2 + x + 1 \in \mathbb{F}_7[x]$ to a root of $x^2 + x + 1 \in \mathbb{Q}_7[x]$ via Hensel’s lemma), and this implies that $x^3 - 2$ splits completely in $L_w = \mathbb{Q}_7(\sqrt[3]{2})$. But $L = \bar{K}[x]/(x^3 - 2)$ is not a Galois extension of $K$ because it contains only one root of $x^3 - 2$. However, we can replace $K$ with $\mathbb{Q}(\zeta_3)$ without changing $\bar{K}$ (take the completion of $K$ with respect to the absolute value induced by a prime above 7) or $\bar{L}$, but now $L = \bar{K}[x]/(x^3 - 2)$ is a Galois extension of $K$.

In the example we were able to adjust our choice of the global field $K$ without changing the local fields extension $\bar{L}/\bar{K}$ in a way that ensures that $\bar{L}/\bar{K}$ and $L/K$ have the same automorphism group. Indeed, this is always possible.

Corollary 11.3. For every finite Galois extension $\bar{L}/\bar{K}$ of local fields there is a correspon-
ding Galois extension of global fields $L/K$ and an absolute value $| |$ on $L$ such that $\bar{L}$ is the completion of $L$ with respect to $| |$, $\bar{K}$ is the completion of $K$ with respect to the restriction of $| |$ to $K$, and $\text{Gal}(\bar{L}/\bar{K}) \simeq \text{Gal}(L/K)$.

Proof. The archimedean case is already covered by Theorem 11.1 (take $K = \mathbb{Q}$), so we assume $\bar{L}$ is nonarchimedean and note that we may take $| |$ to be the absolute value on both $\bar{K}$ and $\bar{L}$ (by Theorem 9.25). The field $\bar{K}$ is an extension of either $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$, and by applying Theorem 11.1 to this extension we may assume $\bar{K}$ is the completion of a global field $K$ with respect to the restriction of $| |$. As in the proof of the theorem, let $g \in K[x]$ be a monic separable polynomial irreducible in $\bar{K}[x]$ such that $\bar{L} = \bar{K}[x]/(g)$ and define $L := K[x]/(g)$ so that $\bar{L}$ is the compositum of $K$ and $L$.

Now let $M$ be the splitting field of $g$ over $K$, the minimal extension of $K$ that contains all the roots of $g$ (which are distinct because $g$ is separable). The field $\bar{L}$ also contains these roots (since $\bar{L}/K$ is Galois) and $\bar{L}$ contains $K$, so $\bar{L}$ contains a subextension of $K$ isomorphic to $M$ (by the universal property of a splitting field), which we now identify with $M$; note that $\bar{L}$ is also the completion of $M$ with respect to the restriction of $| |$ to $M$.

We have a group homomorphism $\varphi : \text{Gal}(\bar{L}/\bar{K}) \to \text{Gal}(M/K)$ induced by restriction, and $\varphi$ is injective (each $\sigma \in \text{Gal}(\bar{L}/\bar{K})$ is determined by its action on any root of $g$ in $M$). If we now replace $K$ by the fixed field of the image of $\varphi$ and replace $L$ with $M$, the completion of $K$ with respect to the restriction of $| |$ is still equal to $\bar{K}$, and similarly for $L$ and $\bar{L}$, and now $\text{Gal}(L/K) = \text{Gal}(\bar{L}/\bar{K})$ as desired. \qed

11.2 Completing a separable extension of Dedekind domains

We now return to our general $AKLB$ setup: $A$ is a Dedekind domain with fraction field $K$ with a finite separable extension $L/K$, and $B$ is the integral closure of $A$ in $L$, which is also a Dedekind domain. Recall from Theorem 5.11 that if $p$ is a nonzero prime of $A$, each prime $q|p$ gives a valuation $v_q$ of $L$ that extends the valuation $v_p$ of $K$ with index $e_q$, meaning that $v_q|_K = e_q v_p$. Moreover, every valuation of $L$ that extends $v_p$ arises in this way. We now want to look at what happens when we complete $K$ with respect to the absolute value $| |_p$ induced by $v_p$, and similarly complete $L$ with respect to $| |_q$ for some $q|p$. This includes the case where $L/K$ is an extension of global fields, in which case we get a corresponding extension $L_q/K_p$ of local fields for each $q|p$, but note that $L_q/K_p$ may have strictly smaller degree than $L/K$ because if we write $L \simeq K[x]/(f)$, the irreducible polynomial $f \in K[x]$ need not be irreducible over $K_p$. Indeed, this will necessarily be the case if there is more than one prime $q$ lying above $p$; there is a one-to-one correspondence between factors of $f$
in $K_p[x]$ and primes $q|p$. If $L/K$ is Galois, so is $L_q/K_p$ and each $\text{Gal}(L_q/K_p)$ is isomorphic to the decomposition group $D_q$ (which perhaps helps to explain the terminology).

The following theorem gives a complete description of the situation.

**Theorem 11.4.** Assume $AKLB$, let $p$ be a prime of $A$, and let $pB = \prod_{q|p} q^e_q$ be the factorization of $pB$ in $B$. Let $K_p$ denote the completion of $K$ with respect to $|\cdot|_p$, and let $\hat{\mathfrak{p}}$ denote the maximal ideal of its valuation ring. For each $q|p$, let $L_q$ denote the completion of $L$ with respect to $|\cdot|_q$, and let $\hat{q}$ denote the maximal ideal of its valuation ring. The following hold:

1. Each $L_q$ is a finite separable extension of $K_q$;
2. Each $\hat{q}$ is the unique prime of $L_q$ lying over $\hat{p}$.
3. Each $\hat{q}$ has ramification index $e_q = e_q$ and residue field degree $f_q = f_q$.
4. $[L_q : K_p] = e_q f_q$.
5. The map $L \otimes_K K_p \to \prod_{q|p} L_q$ defined by $\ell \otimes x \mapsto (\ell x, \ldots, \ell x)$ is an isomorphism of finite étale $K_p$-algebras.
6. If $L/K$ is Galois then each $L_q/K_p$ is Galois and we have isomorphisms of decomposition groups $D_q \simeq D_q = \text{Gal}(L_q/K_p)$ and inertia groups $I_q \simeq I_q$.

**Proof.** We first note that the $K_p$ and the $L_q$ are all fraction fields of complete DVRs; this follows from Proposition 8.18 (note: we are not assuming they are local fields, in particular, their residue fields need not be finite).

1. For each $q|p$ the embedding $K \hookrightarrow L$ induces an embedding $K_p \hookrightarrow L_q$ via the map $[(a_n)] \mapsto [(a_n)]$ on equivalence classes of Cauchy sequences; a sequence $(a_n)$ that is Cauchy in $K$ with respect to $|\cdot|_p$, is also Cauchy in $L$ with respect to $|\cdot|_q$ because $v_q$ extends $v_p$.

We then view $K_p$ as a subfield of $L_q$, which also contains $L$. There is thus a $K$-algebra homomorphism $\phi_q: L \otimes_K K_p \to L_q$ defined by $\ell \otimes x \mapsto \ell x$, which we may view as a linear map of $K_p$ vector spaces. We claim that $\phi_q$ is surjective.

If $\alpha_1, \ldots, \alpha_m$ is any basis for $L_q$ then its determinant with respect to $\mathcal{B}$, i.e., the $m \times m$ matrix whose $j$th row contains the coefficients of $\alpha_j$ when written as a linear combination of elements of $\mathcal{B}$, must be nonzero. The determinant is a polynomial in the entries of this matrix, hence a continuous function with respect to the topology on $L_q$ induced by the absolute value $|\cdot|_q$. It follows that if we replace $\alpha_1, \ldots, \alpha_m$ with $\ell_1, \ldots, \ell_m$ chosen so that $|\alpha_j - \ell_j|_q$ is sufficiently small, the matrix of $\ell_1, \ldots, \ell_m$ with respect to $\mathcal{B}$ must also be nonzero, and therefore $\ell_1, \ldots, \ell_m$ is also a basis for $L_q$. We can thus choose a basis $\ell_1, \ldots, \ell_m \subseteq L$, since $L$ is dense in its completion $L_q$. But then $\{\ell_j\} = \{\phi_q(\ell_j \otimes 1)\} \subseteq \text{im} \phi_q$ spans $L_q$, so $\phi_q$ is surjective as claimed.

The $K_p$-algebra $L \otimes_K K_p$ is the base change of a finite étale algebra, hence finite étale, by Proposition 4.34. It follows that $L_q$ is a finite separable extension of $K_p$: it certainly has finite dimension as a $K_p$-vector space, since $\phi_q$ is surjective, and it is separable because every $\alpha \in L_q$ is the image $\phi_q(\beta)$ of an element $\beta \in L \otimes_K K_p$ that is a root of a separable (but not necessarily irreducible) polynomial $f \in K_p[x]$, as explained after Definition 4.29; we then have $0 = \phi_q(0) = \phi_q(f(\beta)) = f(\alpha)$, so $\alpha$ is a root of $f$, hence separable.

2. The valuation rings of $K_p$ and $L_q$ are complete DVRs, so this follows immediately from Theorem 9.20.

3. The valuation $v_q$ extends $v_p$ with index $e_q$. The valuation $v_p$ extends $v_p$ with index $e_q$, and it follows that $v_q$ extends $v_p$ with index $e_q$ and therefore $e_q = e_q$. The residue field of $\hat{p}$ is the same as that of $p$: for any Cauchy
sequence \((a_n)\) over \(K\) the \(a_n\) will eventually all have the same image in the residue field at \(p\) (since \(v_p(a_n - a_m) > 0\) for all sufficiently large \(m\) and \(n\)). Similar comments apply to each \(\hat{q}\) and \(q\), and it follows that \(f_{\hat{q}} = f_q\).

(4) It follows from (2) that \([L_q : K_p] = e_q f_{\hat{q}}\), since \(\hat{q}\) is the only prime above \(\hat{p}\), and (3) then implies \([L_q : K_p] = e_q f_q\).

(5) Let \(\phi = \prod_{q|p} \phi_q\), where \(\phi_q\) are the surjective \(K_q\)-algebra homomorphisms defined in the proof of (1). Then \(\phi: L \otimes_K K_p \rightarrow \prod_{q|p} L_q\) is a \(K_q\)-algebra homomorphism. Applying (4) and the fact that base change preserves dimension (see Proposition 4.34):

\[
\dim_{K_p} (L \otimes_K K_p) = \dim_K L = [L : K] = \sum_{q|p} e_q f_q = \sum_{q|p} [L_q : K_p] = \dim_{K_p} \left( \prod_{q|p} L_q \right).
\]

The domain and range of \(\phi\) thus have the same dimension, and \(\phi\) is surjective (since the \(\phi_q\) are), so it is an isomorphism.

(6) We now assume \(L/K\) is Galois. Each \(\sigma \in D_q\) acts on \(L\) and respects the valuation \(v_q\), since it fixes \(q\) (if \(x \in q^n\) then \(\sigma(x) \in \sigma(q^n) = q^n\)). It follows that if \((x_n)\) is a Cauchy sequence in \(L\), then so is \((\sigma(x_n))\), thus \(\sigma\) is an automorphism of \(L_q\), and it fixes \(K_p\). We thus have a group homomorphism \(\varphi: D_q \rightarrow \text{Aut}_{K_p}(L_q)\).

If \(\sigma \in D_q\) acts trivially on \(L_q\) then it acts trivially on \(L \subseteq L_q\), so \(\ker \varphi\) is trivial. Also,

\[e_q f_q = [D_q] \leq \#\text{Aut}_{K_p}(L_q) \leq [L_q : K_p] = e_q f_q,
\]

by Theorem 11.4, so \(\#\text{Aut}_{K_p}(L_q) = [L_q : K_p]\) and \(L_q/K_p\) is Galois, and this also shows that \(\varphi\) is surjective and therefore an isomorphism. There is only one prime \(\hat{q}\) of \(L_q\), and it is necessarily fixed by every \(\sigma \in \text{Gal}(L_q/K_p)\), so \(\text{Gal}(L_q/K_p) \cong D_q\). The inertia groups \(I_q\) and \(I_{\hat{q}}\) both have order \(e_q = e_{\hat{q}}\), and \(\varphi\) restricts to a homomorphism \(I_q \rightarrow I_{\hat{q}}\), so the inertia groups are also isomorphic.

\[\square\]

Corollary 11.5. Assume \(AKLB\) and let \(p\) be a prime of \(A\). For every \(\alpha \in L\) we have

\[N_{L/K}(\alpha) = \prod_{q|p} N_{L_q/K_q}(\alpha) \quad \text{and} \quad T_{L/K}(\alpha) = \prod_{q|p} T_{L_q/K_q}(\alpha),\]

where we view \(\alpha\) as an element of \(L_q\) via the canonical embedding \(L \hookrightarrow L_q\).

Proof. The norm and trace are defined as the determinant and trace of \(K\)-linear maps \(L \xrightarrow{\times \alpha} L\) that are unchanged upon tensoring with \(K_p\); the corollary then follows from the isomorphism in part (5) of Theorem 11.4, which commutes with the norm and trace. \[\square\]

Remark 11.6. Theorem 11.4 can be stated more generally in terms of (equivalence classes of) absolute values (or \(\text{places}\)). Rather than working with a prime \(p\) of \(K\) and primes \(q\) of \(L\) above \(p\), one works with an absolute value \(|\cdot|_v\) of \(K\) (for example, \(|\cdot|_p\) and inequivalent absolute values \(|\cdot|_w\) of \(L\) that extend \(|\cdot|_v\). Places will be discussed further in the next lecture.

Corollary 11.7. Assume \(AKLB\) with \(A\) a DVR with maximal ideal \(p\). Let \(pB = \prod q^e_q\) be the factorization of \(pB\) in \(B\). Let \(\hat{A}\) denote the completion of \(A\), and for each \(q|p\), let \(\hat{B}_q\) denote the completion of \(B_q\). Then \(B \otimes_A \hat{A} \simeq \prod_{q|p} \hat{B}_q\).
Proof. Since $A$ is a DVR (and therefore a torsion-free PID), the ring extension $B/A$ is a free $A$ module of rank $n := [L : K]$, and therefore $B \otimes_A \hat{A}$ is a free $\hat{A}$-module of rank $n$. And $\prod q \hat{B}_q$ is a free $\hat{A}$-module of rank $\sum q|\mathfrak{p} e_q j_q = n$. These two $\hat{A}$-modules lie in isomorphic $K_p$-vector spaces, $L \otimes_K K_p \simeq \prod L_q$, by part (5) of Theorem 11.4. To show that they are isomorphic it suffices to check that they are isomorphic after reducing modulo $\hat{p}$, the maximal ideal of $\hat{A}$.

For the LHS, note that $\hat{A}/\hat{p} \simeq A/p$, so

$$B \otimes_A \hat{A}/\hat{p} \simeq B \otimes_A A/p \simeq B/pB.$$  

On the RHS we have

$$\prod q \hat{B}_q/\hat{p} \hat{B}_q \simeq \prod q \hat{B}_q/p \hat{B}_q \simeq \prod q \hat{B}_q/p B_q = \prod q B_q/q^{e_q} B_q$$

which is isomorphic to $B/pB$ on the LHS because $pB = \prod q q^{e_q}$.  

\[\square\]

11.3 The different ideal

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 $L/K$, that is, the primes $q$ of $B$ for which $e_q > 1$, or, at a coarser level, primes $\mathfrak{p}$ of $A$ that have a ramified prime $q$ lying above them. Our main tool for doing so is the different ideal $\mathcal{D}_{B/A}$, a fractional ideal of $B$ that will give us an exact answer to this question: the primes of $B$ that ramify are exactly those that divide the different ideal, and $v_q(\mathcal{D}_{B/A})$ will give us information about the ramification index $e_q$ (its exact value in the tamely ramified case).

Of course we could just define $\mathcal{D}_{B/A}$ to have the properties we want, but the key is to define it in a way that makes it independently computable, allowing us to determine the primes $q$ that ramify in $B$, which we typically do not know \emph{a priori}.

Recall from Lecture 4 the trace pairing $L \times L \to K$ defined by $(x, y) \mapsto T_{L/K}(xy)$. Since $L/K$ is separable, this pairing is nondegenerate, by Proposition 4.58. For any $A$-module $M \subseteq L$, we defined the dual $A$-module

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

(see Definition 4.59). Note that if $M \subseteq N$ are two $A$-modules in $L$, then it is clear from the definition that $N^* \subseteq M^*$ (taking duals reverses inclusions).

If $M$ is a free $A$-lattice (see Definition 6.1) then it has an $A$-module basis $e_1, \ldots, e_n$ that is also a $K$-basis for $L$. The dual $A$-module $M^*$ is then also a free $A$-lattice, and it has the dual basis $e_1^*, \ldots, e_n^*$, which is the unique $K$-basis for $L$ that satisfies

$$T_{L/K}(e_i^* e_j) = \delta_{ij} := \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise} \end{cases}$$

(see Proposition 4.54) and also an $A$-module basis for $M^*$.

Every $B$-module $M \subseteq L$ (including all fractional ideals of $B$) is also a (not necessarily free) $A$-module in $L$, and in this case the dual $A$-module $M^*$ is also a $B$-module: for any $x \in M^*$, $b \in B$, and $m \in M$ we have $T((bx)m) = T(b \cdot x(m)) \in A$, since $bm \in M$ and $x \in M^*$, so $bx \in M^*$. If $M$ is a finitely generated as a $B$-module, then it is a fractional ideal of $B$ (by definition), and provided it is nonzero, it is invertible, since $B$ is a Dedekind domain, and therefore an element of the ideal group $\mathcal{I}_B$. We now show that $M^* \in \mathcal{I}_B$.  

18.785 Fall 2015, Lecture #11, Page 5
Proposition 11.11. Assume $\text{AKLB}$ and suppose $M \in I_B$. Then $M^* \in I_B$.

Proof. Since $M$ is a $B$-module, so is $M^*$ (as noted above), and $M^*$ is clearly nonzero: if $M = \frac{1}{b}I$ with $b \in B$ nonzero and $I$ a $B$-ideal, then $bm \in B$ and $T_{L/K}(bm) \in A$ for all $m \in M$ so $b \in M^*$. We just need to check that $M^*$ is finitely generated. Here we use the standard trick: find a free submodule of $M$, take its dual to get a free module that contains $M^*$, and then note that $M^*$ is a submodule of a noetherian module.

Let $e_1, \ldots, e_n$ be a $K$-basis for $L$. By clearing denominators, we may assume the $e_i$ lie in $B$ (since $L = \text{Frac} B$). If $m$ is any element of $M$, then $me_1, \ldots, me_n$ is a $K$-basis for $L$ that lies in $M$. Let $C$ be the free $A$-submodule of $M$ generated by $me_1, \ldots, me_n$; this is a free $A$-lattice, and it follows that $M^* \subseteq C^*$ is contained in the free $A$-lattice $C^*$, which is obviously finitely generated. As a finitely generated module over a noetherian ring, the $A$-module $C^*$ is a noetherian module, which means that every $A$-submodule of $C^*$ is finitely generated, including $M^*$. We have $A \subseteq B$, so if $M^*$ is finitely generated as an $A$-module, it is certainly finitely generated as a $B$-module. \qed

Definition 11.9. Assume $\text{AKLB}$. The inverse different ideal (or codifferent) of $B$ is the dual of $B$ as an $A$-module:

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

The different ideal (or different) $D_{B/A}$ is the inverse of $B^*$ as a fractional $B$-ideal.

To justify the name, we should check that $D_{B/A}$ is actually an ideal, not just a fractional ideal. The dual module $B^*$ clearly contains 1, since $T_{L/K}(1 \cdot b) = T_{L/K}(b) \in A$ for all $b \in B$. It follows that

$$D_{B/A} = (B^*)^{-1} = (B : B^*) = \{x \in L : xB^* \subseteq B\} \subseteq B,$$

so $D_{B/A}$ is indeed a $B$-ideal.

We now show that the different respects localization and completion.

Proposition 11.10. Assume $\text{AKLB}$, let $S$ be a multiplicative subset of $A$. Then

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

Proof. Since taking inverses respects localization, it suffices to show that $S^{-1}B^* = (S^{-1}B)^*$, where $(S^{-1}B)^*$ denotes the dual of $S^{-1}B$ as an $S^{-1}A$-module in $L$. If $x = s^{-1}y \in S^{-1}B^*$ with $s \in S$ and $y \in B^*$, and $m = t^{-1}b \in S^{-1}B$ with $t \in S$ and $b \in B$ then

$$T_{L/K}(xm) = (st)^{-1}T_{L/K}(yb) \in S^{-1}A,$$

since the trace is $K$-linear and $S \subseteq A \subseteq K$; this shows that $S^{-1}B^* \subseteq (S^{-1}B)^*$. For the reverse inclusion, let $\{b_i\}$ be a finite set of generators for $B$ as an $A$-module and let $x \in (S^{-1}B)^*$. For each $b_i$ we have $T_{L/K}(xb_i) \in S^{-1}A$, since $(S^{-1}B)^*$ is an $S^{-1}B$-module and therefore a $B$-module. So each $T_{L/K}(xb_i) = s_i^{-1}a_i$ for some $s_i \in S$ and $a_i \in A$. If we now put $s = \prod s_i$ (a finite product), then $T_{L/K}(sxb_i) \in A$ for all $b_i$ (here we are again using the $K$-linearity of $T_{L/K}$). So $sx \in B^*$, and therefore $x \in S^{-1}B^*$ as desired. \qed

Proposition 11.11. Assume $\text{AKLB}$ and let $q \mid p$ be a prime of $B$. Then

$$D_{B_q/A_p} = D_{B/A} \cdot \hat{B}_q.$$
Proof. We can assume without loss of generality that $A$ is a DVR by localizing at $\mathfrak{p}$. Let $\hat{L} := L \otimes \hat{K}$. By (5) of Theorem 11.4, we have $\hat{L} = \prod_{q\mid \mathfrak{p}} \hat{L}_q$. This is not a field, in general, but $T_{L/K}$ is defined as for any ring extension, and we have $T_{L/K}(x) = \sum_{q\mid \mathfrak{p}} T_{L_q/K}(x)$.

Now let $\hat{B} := B \otimes \hat{A}$. By Corollary 11.7, $\hat{B} = \prod_{q\mid \mathfrak{p}} \hat{B}_q$, and therefore $\hat{B}^* \simeq \prod_{q\mid \mathfrak{p}} \hat{B}_q^*$ (since the trace is just a sum of traces). It follows that $B^* \simeq B^* \otimes_A \hat{A}$. Thus $B^*$ generates the fractional ideal $\hat{B}_q^* \subseteq \mathcal{I}_{\hat{A}}$. Taking inverses, $\mathcal{D}_{B/A} = (B^*)^{-1}$ generates $(\hat{B}_q^*)^{-1} = \mathcal{D}_{\hat{B}_q/\hat{A}}$. \(\Box\)

11.4 The discriminant

**Definition 11.12.** Let $B/A$ be a ring extension with $B$ free as an $A$-module. For any $e_1, \ldots, e_n \in B$ we define the discriminant

$$\text{disc}(e_1, \ldots, e_n) = \det[T_{B/A}(e_ie_j)]_{i,j} \in A,$$

where $T_{B/A}(b)$ is the trace from $B$ to $A$ (see Definition 4.40).\(^1\)

We have in mind the case where $e_1, \ldots, e_n$ is a basis for $L$ as a $K$-vector space. In our usual $AKLB$ setup, if $e_1, \ldots, e_n \in B$ then $\text{disc}(e_1, \ldots, e_n) \in A$.

**Proposition 11.13.** Let $L/K$ be a finite separable extension of degree $n$, and let $\Omega/K$ be a field extension for which there are distinct $\sigma_1, \ldots, \sigma_n \in \text{hom}_K(L, \Omega)$. For any $e_1, \ldots, e_n \in L$

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

Furthermore, for any $x \in L$

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

Note that such an $\Omega$ exists, since $L/K$ is separable (just take a normal closure).

**Proof.** For $1 \leq i, j \leq n$ we have $T_{L/K}(e_ie_j) = \sum_{k=1}^n \sigma_k(e_ie_j)$, by Theorem 4.44. Therefore

$$\text{disc}(e_1, \ldots, e_n) = \det[T_{L/K}(e_ie_j)]_{i,j}$$

$$= \det ([\sigma_k(e_i)]_{ik}[\sigma_k(e_j)]_{kj})$$

$$= \det ([\sigma_k(e_i)]_{ik}[\sigma_k(e_j)]_{jk})$$

$$= (\det[\sigma_i(e_j)]_{i,j})^2$$

since the determinant is multiplicative and invariant under taking transposes.

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

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

since $[\sigma_i(x^{j-1})]_{i,j}$ is a Vandermonde matrix. \(\Box\)

\(^1\)This definition is consistent with Definition 4.49 where we defined the discriminant of a bilinear pairing.
**Definition 11.14.** 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

\[
\text{disc}(f) = \text{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \in A.
\]

**Example 11.15.** \( \text{disc}(x^2 + bx + c) = b^2 - 4c \) and \( \text{disc}(x^3 + ax + b) = -4a^3 - 27b^2 \).

Now assume \( AKLB \) and let \( M \) be an \( A \)-lattice in \( L \) (Definition 6.1). Then \( M \) is a finitely generated \( A \)-module that contains a basis for \( L \) as a \( K \)-vector space, but we would like 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 \( e_1, \ldots, e_n \in M \subseteq L \) and \( e'_1, \ldots, e'_n \in M \subseteq L \) are two bases for \( M \), then

\[
\text{disc}(e'_1, \ldots, e'_n) = u^2 \text{disc}(e_1, \ldots, e_n)
\]

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 twice in order to change \( T(e_i e_j) \) to \( T(e'_i e'_j) \). Explicitly, writing bases as row-vectors, let \( e = (e_1, \ldots, e_n) \), \( e' = (e'_1, \ldots, e'_n) \) and suppose \( e' = eP \). We then have

\[
\text{disc}(e') = \det[T_{L/K}(e'_i e'_j)]_{ij} = \det[T_{L/K}(eP_i (eP)_j)]_{ij} = \det[P^t T_{L/K}(e e_j) P]_{ij} = (\det P^t) \text{disc}(e)(\det P) = (\det P)^2 \text{disc}(e),
\]

where we have (repeatedly) used the fact that \( T_{L/K} \) is \( A \)-linear.

This actually gives us an unambiguous definition when \( A = \mathbb{Z} \): the only units in \( \mathbb{Z} \) are \( u = \pm 1 \), so we always have \( u^2 = 1 \) and get the same discriminant no matter which basis we choose. In general we want to take the principal fractional ideal of \( A \) generated by \( \text{disc}(e_1, \ldots, e_n) \), which does not depend on the choice of basis. This suggests how we should define the discriminant of \( M \) in the general case, where \( M \) is not necessarily free.

**Definition 11.16.** Assume \( AKLB \) and let \( M \) be an \( A \)-lattice in \( L \). The **discriminant** \( D(M) \) of \( M \) is the \( A \)-module generated by the set \( \{ \text{disc}(e_1, \ldots, e_n) : e_1, \ldots, e_n \in M \} \).

In the case that \( M \) is free, \( D(M) \) is equal to the principal fractional ideal generated by \( \text{disc}(e_1, \ldots, e_n) \), for any fixed basis \( e = (e_1, \ldots, e_n) \). For any \( n \)-tuple \( e' = (e'_1, \ldots, e'_n) \) of elements in \( L \), we can write \( e' = eP \) for some (not necessarily invertible) matrix \( P \); we will have \( \text{disc}(e') = 0 \) whenever \( e' \) is not a basis.

**Lemma 11.17.** Assume \( AKLB \) and let \( M \subseteq M' \) be free \( A \)-lattices in \( L \). If \( D(M) = D(M') \) then \( M = M' \).
Proof. Fix bases $e$ and $e'$ for $M$ and $M'$. If $D(M) = (\text{disc}(e)) = (\text{disc}(e')) = D(M')$ as fractional ideals of $A$, then the change of basis matrix from $M'$ to $M$ is invertible over $A$, which implies $M' \subseteq M$ and therefore $M = M'$.

In general, $D(M)$ is a fractional ideal of $A$, but it need not be principal.

**Proposition 11.18.** Assume $AKLB$ and let $M$ be an $A$-lattice in $L$. Then $D(M) \in \mathcal{I}_A$.

*Proof. The $A$-module $D(M)$ is nonzero because $M$ contains a $K$-basis $e_1, \ldots, e_n$ for $L$ and $\text{disc}(e_1, \ldots, e_n) \neq 0$ because the trace pairing is nondegenerate, and it is clearly a submodule of the fraction field $K$ of $A$ (it is generated by determinants of matrices with entries in $K$). To show that $D(M)$ is finitely generated as an $A$-module we use the usual trick: show that it is a submodule of a noetherian module. Let $N$ be the free $A$-lattice generated by a $K$-basis of $L$ in $M$. Since $N$ is finitely generated, we can pick a nonzero $a \in A$ such that $M \subseteq a^{-1}N$. Then $D(M) \subset D(a^{-1}N)$, and since $a^{-1}N$ is a free $A$-lattice, $D(a^{-1}N)$ is finitely generated and therefore a noetherian module, since $A$ is noetherian. Every submodule of a noetherian module is finitely generated, so $D(M)$ is finitely generated.*

**Definition 11.19.** Assume $AKLB$. The *discriminant* of $L/K$ is the discriminant of $B$ as an $A$-module:

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

Note that $D_{L/K}$ is a fractional ideal (in fact an ideal, by Corollary 11.24 below), not an element of $A$ (but see Remark 11.21 below).

**Example 11.20.** Consider the case $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $B = \mathbb{Z}[i]$. Then $B$ is a free $\mathbb{Z}$-basis 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 ideal $D_{L/K}$ is $(-4) = (4)$.

**Remark 11.21.** If $A = \mathbb{Z}$ then $B$ is the ring of integers of the number field $L$, and $B$ is a free $\mathbb{Z}$-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* $\text{disc}(e_1, \ldots, e_n) \in \mathbb{Z}$, for any basis $(e_1, \ldots, e_n)$ 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 any $u \in \mathbb{Z}^\times$; in particular, the sign of $D_L$ is well defined. In the example above, the absolute discriminant is $D_L = -4$ (not 4).

We now show that the discriminant respects localization.

**Proposition 11.22.** 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 \( x = s^{-1} \text{disc}(e_1, \ldots, e_n) \in S^{-1}D_{B/A} \) for some \( s \in S \) and \( e_1, \ldots, e_n \in B \). Then \( x = s^{2n-1} \text{disc}(s^{-1} e_1, \ldots, s^{-1} e_n) \) lies in \( D_{S^{-1}B/S^{-1}A} \). This proves the forward inclusion.

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

We have now defined two different ideals associated to a finite separable extension of Dedekind domains \( B/A \) in the AKLB setup. We have the different \( D_{B/A} \), 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 6.2 and 6.5). We recall that \( N_{B/A}(I) \) is also equal to the ideal generated by the image of \( I \) under the field norm \( N_{L/K} \); see Corollary 6.8.

**Theorem 11.23.** Assume AKLB. Then \( D_{B/A} = N_{B/A}(D_{B/A}) \).

Proof. The different respects localization at any prime \( \mathfrak{p} \) of \( A \) (see Proposition 11.10), and we just proved that this is also true of the discriminant. Since \( A \) is a Dedekind domain, the \( A \)-modules on both sides of the equality are determined by the intersections of their localization, so it suffices to consider the case that \( A = A_p \) is a DVR, and in particular a PID. In this case \( B \) is a free \( A \)-lattice in \( L \) (torsion-free over a PID implies free), and we can choose a basis \( e_1, \ldots, e_n \) for \( B \) as an \( A \)-module. The dual \( A \)-module

\[
B^* = \{ x \in L : T_{L/K}(xb) \in A \ \forall b \in B \} \in \mathcal{I}_B
\]

is also a free \( A \)-lattice in \( L \), with basis \( e_1^*, \ldots, e_n^* \) uniquely determined by \( T_{L/K}(e_i^* e_j) = \delta_{ij} \).

If \( M \) is any free \( A \)-lattice with basis \( m_1, \ldots, m_n \), then \( [T_{L/K}(m_i e_j)]_{ij} \) is precisely the change of basis matrix from \( e_1^*, \ldots, e_n^* \) to \( m_1, \ldots, m_n \). Applying this to the free \( A \)-lattice \( B \), we then have

\[
D_{B/A} = (\det[T_{L/K}(e_i e_j)]_{ij}) = (B^* : B)_A
\]

by the definition of the module index for free \( A \)-modules (see Definition 6.2).

For any \( I \in \mathcal{I}_B \) we have \( (B : I) = I^{-1} = (I^{-1} : B) \) as \( B \)-modules, and it follows that \( (B : I)_A = (I^{-1} : B)_A \). Applying this with \( I^{-1} = B^* \) gives

\[
D_{B/A} = (B^* : B)_A = (B : (B^*)^{-1})_A = (B : D_{B/A})_A = N_{B/A}(D_{B/A})
\]

as claimed.

**Corollary 11.24.** Assume AKLB. The discriminant \( D_{B/A} \) is an \( A \)-ideal.

Proof. The different \( D_{B/A} \) is a \( B \)-ideal, and the field norm \( N_{L/K} \) sends elements of \( B \) to \( A \); it follows that \( D_{B/A} = N_{B/A}(D_{B/A}) = (N_{L/K}(x) : x \in D_{B/A}) \) is an \( A \)-ideal.